Linklaters

Aerospace, Defence and Security

A new era of hard power



linklaters.com

Contents. A new era of hard power.

Introduction p3
Market dynamics p5
Scalability: the race to consolidate p5
Safeguarding supply p7
Technology and the changing face of war p9
Legal issues p12
ESG: friend or foe – or both? p12
Private capital and financing tools p14
Competition law and defence: challenges and opportunities p16
Contracting with government p19
Sanctions, ethics and compliance: managing key risks p20
Cyber security in the grey zone p21
Digital sovereignty p23
AI, technology regulation and LAWS p24
Intellectual property rights p26
A contentious horizon p27
Our sector team p28
Our global experience p30
Sources p31

Introduction

The first duty of the state is security. That principle has moved from theory to balance sheet reality. A decade of underinvestment, shifting allegiances and challenging geopolitics, alongside the relentless pace of technology is reshaping our understanding of the defence and security landscape. Three key points arise. For boards and investors, this is not a cyclical uplift. It is a structural reset shaped by three forces:

$2.88tn **Global military spending reached US$2.88tn in 2025,** the highest level ever recorded, rising 2.9 per cent year-on-year and increasing for the eleventh consecutive year.

55% **NATO members now account for 55 per cent of global defence expenditure.**

5% With NATO allied leaders committing in 2025 to spend up to 5 per cent of GDP by 2035 following sustained US pressure[1].

14% Military spending across Europe rose 14 per cent in 2025 alone.

1. Eroding international frameworks accelerates deterrence

The erosion of multilateral constraint and the return of great-power competition have changed how deterrence is measured. Strategic autonomy, industrial capacity and military readiness now rank alongside fiscal stability as tests of sovereign credibility.

Europe's response has been decisive. Military spending across Europe rose 14 per cent in 2025 alone, driven primarily by Ukraine and reinforced by Russia's 5.9 per cent increase in defence outlays to an estimated 7.5 per cent of GDP[2]. These numbers explain the pace of procurement reform, emergency financing tools and accelerated contracting timelines now confronting defence suppliers.

Boards are increasingly exposed not just to defence demand but to political delivery risk, budget execution risk and public law scrutiny tied to speed and scale.



View sources

2. The economics of defence and security are being rewritten by technology

Ukraine has demonstrated that combat advantage no longer tracks unit cost. **First-person-view (FPV) strike drones assembled for US$400 to US$1,000 are destroying armoured assets worth millions**[3].

While low-cost interceptor drones now neutralise threats that previously required US$3m to US$4m Patriot missiles[4].

This has forced defence ministries and investors to confront uncomfortable questions:

- How do legacy primes adapt to mass, attributable systems?
- How should procurement rules accommodate rapid iteration and software-defined capability?
- What governance applies when civilian supply chains, dual-use components and AI-driven systems merge?

This transition is legally complex and capital intensive, demanding new approaches to IP strategy, export controls, product liability and public-private partnering.

"To be prepared for war is one of the most effective means of preserving peace." **George Washington**

3. Sovereign control of supply chains is now non-negotiable

Globalised defence supply chains have delivered efficiency but at the cost of resilience. Governments now accept that extended, opaque supplier networks are a national security vulnerability.

The US Government Accountability Office estimates that the **Department of War depends on over 200,000 suppliers,** with limited visibility below tier one and growing exposure to foreign dependency risk[5].

NATO has responded with a formal defence-critical supply chain roadmap aimed at reducing adversarial influence, enforcing resilience standards and mandating strategic stockpiling.

The EU has gone further. The €150bn SAFE programme, launched in 2025[6], ties access to long-term, low-cost financing to common procurement and strict local content thresholds, **capping non-EU components at 35 per cent for funded programmes.**

For defence companies and investors, supply chain strategy is now a legal issue, a financing issue and a regulatory issue. Failures will increasingly trigger contractual default, foreign investment intervention and reputational damage.

Capital is flowing, but margins for error are narrowing. Governments are demanding faster delivery, deeper localisation and greater compliance assurance, often simultaneously.

The central question is no longer whether to invest in defence, but how to do so without tripping regulatory, ethical, procurement or execution risks that can derail programmes and impair value.

Over the course of this handbook, we consider the dynamic environment for defence and security investment and wider legal framework for investment and procurement.

View sources

Market dynamics

The imperative for modern governments to build more capable, resilient, and technologically advanced defences is generating a broad and diverse range of transactional activity.

Scalability: the race to consolidate

The defence sector suffers from significant supplier fragmentation, with critical capabilities dispersed across numerous small and mid-sized businesses ill-equipped to meet the surge in sovereign demand. The response is consolidation, and it is already under way and strategic buyers are moving decisively. Rheinmetall's US$950m acquisition of Loc Performance Products in the United States, completed in November 2024[7], illustrates how European primes are urgently building scale, localisation and production depth to compete for high-volume programmes and to satisfy domestic content requirements in allied markets. Similar logic is driving transactions across land systems, naval shipbuilding, munitions and unmanned platforms.

This consolidation is not confined to trade buyers. Defence-focused private equity has emerged as a meaningful force, attracted by long-duration demand and increasingly predictable order books.

In 2025, private equity deal value in aerospace and defence reached US$55.6bn globally, up 19 per cent on 2024[8], with defence transactions the fastest-growing segment.

Average defence deal volume in Europe over the past five years has almost doubled compared with the previous period.

Where scale-up pressures collide with fixed-price contracts, workforce shortages and supply chain bottlenecks, financial stress is becoming visible. Distressed and opportunistic M&A is therefore a feature, not a tail-risk. Strategically critical suppliers that fail to finance rapid expansion are increasingly becoming acquisition targets, often where governments are unwilling to tolerate operational failure but reluctant to provide direct support.

Scalability now raises hard legal questions around national security screening, procurement continuity, workforce transfer and long-term capital structure. Getting this wrong could result in strategic delays to delivery and depreciation in market value.

Supply chain resilience: security, separation, and disputes

Supply chain resilience has become a defining strategic and legal issue. Governments and primes are under mounting pressure to ensure supply chains are free from non-allied influence. Reshoring initiatives, mandatory localisation thresholds and targeted acquisitions of strategic suppliers are becoming the norm. Governments are also pushing for the deliberate separation of military and civilian production lines where mixed operations weaken security assurance or complicate export control and clearance regimes.

As a result of all this, carve-outs and spin-offs are being used to restructure businesses with mixed defence and commercial operations into ring-fenced entities capable of holding security clearances and meeting government contracting requirements. The surging demand for a relatively narrow set of critical minerals that underpin defence materials are making the supply of scarce raw materials and minerals one of the most strategically significant and commercially active areas of M&A globally.

View sources

At the same time, governments and prime contractors are actively seeking new sources of capital to support rapid capacity build-out across defence and adjacent critical industries. This includes institutional investors and private equity sponsors with limited or no prior exposure to defence.

This matters. New capital brings balance sheet depth and execution speed, but it also introduces unfamiliarity with defence-specific risks, including national security review, ethical constraints, classified contracts and restricted exit routes. As a result, transaction structures are becoming more complex, with greater emphasis on governance rights, compliance undertakings and contingent separation mechanics.

Private capital is already responding. **Private equity and venture-backed investment in aerospace and defence in early 2025 almost matched the entirety of 2024**[9] – a signal that capital is adjusting to defence as a long-duration, policy-anchored sector rather than a cyclical outlier.

Supply chain resilience is not confined to manufacturing footprint. The surge in demand for a relatively narrow set of critical raw materials underpinning modern defence materiel has made minerals and upstream processing one of the most strategically contested arenas for both governments and investors.

NATO and allied governments now explicitly identify strategic materials and minerals as defence-critical assets, with policies directed at stockpiling, allied sourcing and substitution to reduce dependency risk. This has translated into heightened M&A activity across mining, processing and recycling, often accompanied by export controls, investment screening and public funding support.

For corporates, this upstream exposure introduces unfamiliar disputes risks, from offtake enforcement and force majeure claims to state intervention and contract frustration. For investors, it raises questions about jurisdictional exposure, political risk and long-term monetisation.

The common thread is friction. As supply chains are unwound, re-engineered or sold under political pressure, disputes are rising across procurement, joint ventures, termination rights and distressed exits.

Technological innovation: acquiring the edge

The pace of technological change is the most transformative force in defence M&A today. Autonomy, artificial intelligence, electronic warfare, cyber capabilities, and the data infrastructure underpinning them are now central to military advantage. Primes and sovereign wealth funds are acquiring dual-use technology companies, IP-rich start-ups, and data centre assets (often businesses with no prior defence exposure) that hold capabilities in AI, quantum computing, cybersecurity, and advanced materials. This convergence is consistent with broader capital flows. Venture capital investment in defence and dual-use technology has increased more than ten-fold over the past decade, reaching an estimated US$8.7bn in 2024[10]. The implication for incumbents is clear: proprietary data, software and talent are as strategically valuable as physical assets, and increasingly scarce.

Beyond outright acquisition, complex cross-border joint ventures and teaming arrangements (e.g. under programmes such as AUKUS and the European Defence Fund) are becoming a condition of major contract awards, raising nuanced questions around IP ownership, governance, liability, and exit.

Within the EU, the European Defence Fund has earmarked €1bn for collaborative defence R&D in 2026[11], requiring multinational consortia and shared governance as a prerequisite for funding.

Large-scale infrastructure investment in shipyards, munitions facilities, and satellite networks is also driving project finance structures and, increasingly, access to public capital markets.

View sources

Safeguarding supply

Financial resilience

Suppliers throughout the supply chain have had to contend with a serious run of financial pressures in recent years. The costs and disruption associated with the Covid-19 pandemic globally, the energy price volatility that has persisted since 2021, and the challenge of keeping pace with surging demand for military equipment as nations ramp up defence spending have all taken their toll. In the US, defence primes and their sub-contractors have faced analogous pressures – fixed-price contract structures, labour shortages, and materials cost inflation have combined to erode margins across major programmes, with notable high-profile losses on key US government contracts in recent years.

In the UK, these pressures have hit the steel industry particularly hard – a sector that is fundamental to defence manufacturing, ultimately requiring direct government intervention at British Steel's Scunthorpe site. In the EU, the European Defence Industry Reinforcement through Common Procurement Act (EDIRPA) and the broader European Defence Industrial Strategy reflect a recognition that the industrial base underpinning European defence capability requires urgent and sustained investment. Against this backdrop, a solid understanding of government intervention mechanisms, distressed M&A, and distressed debt has become increasingly important for those operating in the defence sector and that is unlikely to change while current economic and geopolitical conditions persist.

Suppliers have responded by focusing hard on protecting their financial resilience. Aside from restructurings and carve-outs to streamline defence businesses, as businesses and their shareholders look to protect and improve margins, they have undertaken supply chain reviews to identify more cost-effective options, outsourced lower-margin work, and sought to use contractual time and cost relief mechanisms more actively. The increased reliance on contractual relief mechanisms has, inevitably, brought disputes in its wake. As parties look to extract maximum value from their contracts, claims for force majeure and change of law have become increasingly common (albeit that in the defence space, the concept of force majeure is markedly different).



Intra-government activity and procurement

As governments increase defence spending, closer collaboration between allies and their supply chains has become a defining feature of the sector. This has resulted in a marked increase in intra-government procurements as allies look to deliver shared strategic outcomes, including the protection of critical infrastructure and efforts to counter reconnaissance by hostile states.

In the United States, AUKUS, the trilateral security partnership between Australia, the UK, and the United States, represents perhaps the most ambitious example of intra-government programme collaboration, with profound implications for supply chain structure, technology transfer, and export control compliance across all three nations. At the EU level, the European Defence Fund is financing collaborative research and development programmes across member states, creating new multi-jurisdictional supply chain relationships and the contractual complexity that comes with them. The UK, Canada, Australia and Norway have considerable supply chain overlap across their frigate programmes for the Type 26 and its derivatives, and there are broader efforts to align anti-submarine warfare capability across NATO's northern flank.

The practical consequence for suppliers is that they are increasingly being asked to get to grips with other nations' contracting frameworks, policy requirements, and legislative and governance processes. An international outlook is no longer a differentiator: it is a baseline expectation. Cross-border contracting arrangements, joint ventures, and M&A activity are becoming routine, and the demands on supply chain management, financial management, and cross-border trade compliance have grown in response.

Supply chain compliance

For businesses already in the defence sector, compliance obligations are intensifying. Enhanced cyber and other standards are being embedded into prime contracts and cascaded to sub-contractors, many of whom are ill-equipped to meet them without investment and specialist support. Sanctions screening, export control compliance, and ethical supply chain requirements are all increasing in scope and complexity. More than ever, compliance is a genuine operational priority and one that carries real contractual and regulatory consequences for those who treat it otherwise.

Compliance across defence supply chains is rapidly evolving from a legal obligation to a gatekeeper for contract eligibility and capital access.

Cyber is now a contractual baseline. Mandatory frameworks are now embedded into defence procurement, with compliance becoming a pre-condition to bid and deliver contracts. However, readiness is materially lagging, with less than 1 per cent of contractors consider themselves fully prepared for audit, with many lacking basic controls[12].

While approximately 80% of SMEs have initiated compliance programmes, many struggle to reach certification due to cost, complexity and capability gaps.

This is creating programme delivery risk for primes, alongside credit and diligence risk for lenders and investors.

Export controls and sanctions regimes have become systemic and extraterritorial, with enforcement now targeting the entire supply chain – not just end users. Post-2022 geopolitical shifts have driven unprecedented scale and coordination of controls, materially increasing compliance burden and transaction friction.

Traceability and ESG are also moving into core procurement, including critical minerals traceability and ESG certification which are becoming prerequisites for market access, driven by regulation and investor pressure.

View sources

Technology and the changing face of war

Move fast and break things

The defence industry will continue to be characterised by long-term and large-scale development projects for key defence assets. However, this is increasingly supplemented by a growing number of defence "start-ups" who are taking the rapid and agile concepts from the tech industries and applying them to defence.

Up-and-coming military tech firms had a high profile at the Munich Security Conference pitching European delegations on drones, the means to stop them and AI-enabled battlefield software.

European defence tech start-ups raised €2.6bn in 2025, up sharply from €200m in 2021[13].

One example is drone technology. Warfighting using drones is safer, more effective and cheaper than conventional operations.

It is also an area marked by the breakneck development. This is most apparent in Ukraine where there has been an evolutionary arms race as each side applies countermeasures against enemy drones and adapts its own drone fleet to evade those countermeasures. Radio jamming has led to drones controlled by physical fibre optic cables with ranges of tens of kilometres. GPS blocking or spoofing has led to the creation of generations of increasingly smart drones capable of orientating themselves from multiple inputs. Sometimes the solution is low-tech – such as the use of netting to create anti-drone corridors – but there are also high-tech solutions such as the development of autonomous drone operations. We consider the difficult questions about the use of fully autonomous lethal weapons systems below.



View sources

Alongside the testing of these systems in theatre, there is likely to be a growth of simulated testing using "digital twins". This provides a high-fidelity virtual replica of a physical object, such as a new drone design, that exists in a simulated environment. This is more than a static three-dimensional model; it applies real-world physics and operational parameters, to allow the digital drone to behave exactly like its physical counterpart. Simulated design, testing and warfighting can drastically reduce the time and expense associated with building and flying physical prototypes. This could accelerate the development cycle from years to months.

This requires a change in mindset. Long-term procurement process delivering static goods and services may need to be supplemented by dynamic and agile continuous development model, with more flexible payment models and outcomes. Years of experience with agile IT contracts show these models work but require much greater day-to-day input and management by the customer.

Companies that invest now in understanding defence and security requirements, align their products with dual use and critical infrastructure needs, and build partnerships with governments and prime contractors will be better placed to secure funding, win procurement opportunities and shape emerging regulatory standards.



Industrial capacity

Wars are sometimes won through tactics on the battlefield but just as often the outcome is dictated by each protagonist's financial and industrial base, and political will. Wars often end because one party cannot afford the cost of continuing.

Drones have the capacity to reshape the battlefield through economics. Using a sophisticated multi-million-dollar missile interceptor to take out a low-tech drone that costs tens of thousands of dollars is an operational success, but an accounting disaster. Part of the solution is to develop low-cost interception solutions. This might mean fighting fire with fire with low-cost interceptor drones, or higher-tech solutions, such as laser directed-energy weapons.

Similarly, the low-cost designs open the way to high-volume commodity production using dual-use technology. Much of the early drone warfighting in Ukraine was carried out using repurposed consumer drone technology, though these are increasingly being replaced by home-grown replacements. Russia has also adopted the Iranian-designed Shahed drones and ramped up its own manufacturing base to produce thousands of drones every month.

Western countries face a dual challenge: maintaining a qualitative edge in defence technology and rapidly expanding industrial capacity. Future conflicts may well depend on the manufacturing capacity, logistical capability and strategic deployment of high-volume, low-cost drone fleets.

> "It is not the strongest that survives; but the species that survives is the one that is able best to adapt and adjust to the changing environment in which it finds itself." **Leon C. Megginson**[14]

View sources



Cyber and the grey zone

No one needs to be reminded of the risks of cyber-attacks. The Munich Security Index 2026[15] shows that cyber risks now top public concern across G7 countries, and they are having a significant and ongoing commercial and economic impact. The global cost of the Russian-backed NotPetya attack in 2017 was over US$10bn[16].

The attack on Jaguar Land Rover in 2025 cost the UK economy over £2bn, according to the Cyber Monitoring Centre (CMC)[17].

Most attacks originate – ostensibly – from financially motivated ransomware gangs. However, state actors are becoming increasingly active by providing tacit support for the ransomware gangs and directly engaging in hybrid warfare. One of the key attractions for nation states is the difficulty in attributing cyber-attacks making it a prime 'grey zone' theatre to either erode counterparties' ability to function or, more seriously, to establish footholds in the computer systems for future use in any overt conflict.

Critical infrastructure providers are particularly exposed to cyber-attacks and grey zone conflict. This has resulted in political and regulatory pressure for a step change in the security and resilience of critical infrastructure providers. We discuss those below but, importantly, those measures also need to be viewed through the lens of threats from nation state actors.

Digital sovereignty

Given the rising significance of electronic and data-related warfare, investment in digital infrastructure (including data centres, fibre networks and satellite systems) is set to grow.

Data centres, satellites, and AI and quantum capabilities are now explicitly national security issues. There will be growing obligations on operators of critical and important entities, and additional scrutiny of cloud, data centre and telecoms arrangements. There have been direct threats to this infrastructure such as attempts to map and interfere with subsea fibre networks.

One important consideration is "digital sovereignty" – the need for states to maintain control of their digital infrastructure. The starting point is data centre location. If critical data for that state is held and processed on servers in a third country, that creates an unavoidable risk of that other country meddling with that data or simply cutting off access entirely.

However, the problem is complex. Even if a data centre is within a state's jurisdiction, it might well depend on support from third countries, and that remote access could still be a significant security concern. Equally, building an entirely sovereign data centre with no third country support is a challenging and expensive option, and may be less secure given it may need to rely on locally-supported security measures. Further challenges arise from the scarcity of local data centre capacity in many states – largely driven by electricity supply constraints as a result of the current AI boom.

Regulation in this area has historically been driven by the need to protect personal data under the GDPR. However, businesses should be alert to the question of digital sovereignty increasingly being driven by implicit, or even express, national security concerns, such as a growing list of data localisation laws like the new US rules restricting and prohibiting certain bulk sensitive data transfers to so-called "countries of concern", including China.

View sources

Legal issues

We have set out some of the key challenges to consider when investing in the defence industries and in relation to defence procurement.

ESG: friend or foe – or both?

There is a common misconception that ESG and investment in the defence sector are fundamentally at odds – this isn't necessarily the case. Investors are starting to recognise that a robust understanding of ESG factors can play a meaningful role in managing the risks and opportunities the sector presents.

As more investors enter the defence space for the first time, getting up to speed on the fast-moving ESG regulatory landscape, stakeholder expectations and geopolitical backdrop is essential.

Perceived barriers

ESG and sustainable investment policies have historically been perceived by some to be a barrier to investment. However, the European Commission has been clear that defence investments are compatible with EU sustainable finance regulation (including the SFDR), which does not impose limitations on the financing of any sector and encourages the case-by-case assessment of defence sector investments just like those in any other sector. Similarly, the UK FCA has also acknowledged that its sustainable finance rules do not prevent investment in or finance for defence companies and confirmed that it is up to individual lenders and investors whether to provide capital.

Robust, well-documented due diligence and governance frameworks are the tools that will determine whether a defence investment can credibly sit within an ESG mandate. These will bring a more structured approach to investment decisions.

Investor Checklist

Some of the considerations investors will need to address.

Strategy & Governance

- [ ] Do we have a clear and board-approved position on defence investment?
- [ ] How do we define "defence"?
- [ ] Is our governance framework fit for purpose?
- [ ] Are our exclusion and inclusion policies clearly defined?
- [ ] Are we aligned with our clients' and LPs' expectations?

Risk Management

- [ ] Have we conducted robust due diligence on end-use risk?
- [ ] Are we exposed to sanctions and export control risk?
- [ ] How are we managing reputational risk?
- [ ] What is our exposure to sovereign and political risk?

ESG & Responsible Investments

- [ ] Are we aligned with evolving defence principles and the likes of GRID?
- [ ] How do we reconcile defence investment with our ESG commitments?
- [ ] Are we prepared for increased disclosure requirements?

Legal & Regulatory Compliance

- [ ] Are we compliant with applicable investment screening regimes?
- [ ] Do our financing and security structures hold up in a defence context?
- [ ] Are we monitoring the regulatory horizon?

Understanding your investment

Investors need to understand the specific nature of each underlying investment: the technologies involved and their uses (including dual use), customer base and end-users, the jurisdiction of operations, ESG requirements in government head contracts. The sector does present particular challenges such as restricted access to information and security sensitivities, but these should not be treated as barriers. Instead, they should be viewed as a reason to build more specialised assessment capabilities.

Investors also need to look beyond the current profile of the target business and consider how it may evolve over time. Clarity over business plans and any shifts in customer base and technology usage is key. Ongoing monitoring and risk management are critical, as is understanding the target's sales and distribution policies and controls, oversight of where products and services are ultimately deployed, and the governance mechanisms that sit around management-level decisions. Investors need to be realistic about how quickly they can disengage, if at all, if things don't go to plan.

Emerging guidance

As sector exposure grows, so will the appetite for common industry frameworks to help guide investors and signal to prospective investees where investor expectations lie. Institutional investors and subject matter experts are currently developing the Guidance for Responsible Investment in Defence-related Companies (GRID)[18] which builds on existing international frameworks and guidance and aims to give investors a principled way to navigate the sector's complexity.

The emerging guidance represents a significant development in the regulatory and reputational landscape for investors and financial institutions operating in the defence sector. Designed to guide responsible investment in defence-related companies, GRID seeks to align investment practices with international humanitarian law and broader ethical standards, while acknowledging the legitimacy of the defence industry as a whole. There is a particular emphasis on robust risk management – including the potential misuse of defence products and exposure to conflict-related risks – as well as enhanced transparency and accountability across investment portfolios.

As these principles gain traction among institutional investors, banks, and regulators, financial institutions will need to consider how their investment and lending policies, due diligence frameworks, and ESG strategies align accordingly.

Investors who successfully embed ESG risk and opportunity considerations into their approach to defence will likely be better placed to appropriately value their investments, address reputational and legal risks, withstand stakeholder scrutiny and keep pace with shifting regulatory expectations.



Private capital and financing tools

As policymakers converge on the need to mobilise private investment, investors are beginning to recalibrate their approach to the defence sector and finance providers are developing tools to support and scale capital deployment. For private capital clients – PE sponsors, pension funds, and asset managers – the opportunity set spans a broad and increasingly interconnected value chain from fundraising to deployment.

Europe's defence investment gap, estimated to be US$1-2bn in debt and US$1-3bn in equity for defence SMEs by the European Commission[19], presents a significant opportunity for private capital providers.

Carve-outs and equity stakes: The most established entry point is direct equity ownership of defence businesses, typically targeting tier-two and tier-three supply chain companies where prime contractors are driving outsourced production at scale. PE, and an increasingly a broader set of investment funds, are particularly active in maintenance, repair and overhaul (MRO) businesses, electronic warfare, radar and sensor systems, cyber software, unmanned and autonomous systems, as well as logistics and simulation companies.

Whilst most activity is US-led, **deal value in European PE and VC-backed aerospace and defence transactions rose approximately 4.8 times year-on-year in 2025, reaching US$658.8m**[20].

Meanwhile, European defence primes are rationalising non-core assets as they concentrate capital on high-demand hardware programmes. This is generating a pipeline of carve-outs suited to PE acquisition.

Private credit – a timely opportunity: Where investor appetite allows, private credit funds are well positioned to provide an important and flexible source of financing for the defence sector. As seen in the European leveraged finance market more broadly over the past few years, the role of private credit funds has evolved to become a significant source of financing for private equity funds – both for leveraged buyouts and for the ongoing management of portfolio companies throughout the lifecycle of private equity investment. This trend is now starting to extend into the defence sector. Over the past twelve months, a number of European private credit funds have provided financing for leveraged buyouts of defence-related assets across the supply chain and this is expected to remain a key area of strategic focus. Beyond private equity-backed transactions, certain private credit funds are also broadening their strategies to include lending to corporates, further expanding the range of defence and dual-use companies that may be able to access flexible private credit solutions to address their financing needs.

Infrastructure funding: Pension funds and infrastructure-focused asset managers are increasingly looking at defence through an infrastructure lens. This covers secure communications networks, satellite ground stations, naval dockyards, airbase facilities, and, critically, military mobility and logistics. The attraction is long-dated, government-backed cash flows with inflation linkage – precisely the profile that large pension allocators seek.

View sources

Financing – constraints and evolution: The availability of bank financing for the defence sector has historically been constrained by internal policies, regulatory uncertainty and ESG-related sensitivities. Although some constraints are likely to remain, the landscape is beginning to shift.

A number of banks are actively revising their internal frameworks and engaging with policymakers and regulators to develop a more supportive approach to lending to parts of the defence sector that are aligned with agreed political and security priorities.

For bank lenders and arrangers, greater clarity on the regulatory treatment of defence lending and its interaction with ESG and sustainability frameworks will be critical to unlocking the availability of bank financing at scale to support investment in the defence sector, across the lending and capital market arenas.

ECA boost: There has been a notable rise in deals related to export credit agency (ECA) involvement. ECAs are increasingly being called upon to support allied nations' procurement of vessels, patrol craft, and offshore security platforms.

One example came last year, when **the UK unveiled a £2bn funding boost, up from £8bn to £10bn for the direct lending capacity of UK Export Finance (UKEF)**[21].

As the landscape for investment in defence continues to evolve, so too will the financing tools available to enable and accelerate capital deployment. In the near term, the most accessible opportunities are likely to lie in financing to support investment in dual-use technologies and supply chain assets, where investor mandates, bank policies and regulatory expectations are beginning to align.



View sources

Competition law and defence

Investing in defence means navigating an increasingly complex and fragmented regulatory landscape. Traditional antitrust and merger control review has given way to a much broader screening environment in recent years, with the proliferation of foreign direct investment (FDI) regimes driven by national security considerations, as well as the introduction of the EU's Foreign Subsidies Regulation (FSR) targeting the distortive effects of foreign subsidies on EU markets. Government stimulus – central to ramping up defence production – may also engage state aid and subsidy control rules, while the award of defence contracts by government may be subject to public procurement rules.

At the same time, governments are actively seeking to strengthen defence "readiness" and have been explicit in tasking competition authorities with supporting that agenda. In the EU, the European Commission has adopted the Defence Readiness Omnibus – a comprehensive package aimed at strengthening EU defence capabilities and resilience. Meanwhile, in the UK, the Competition and Markets Authority (CMA) has received a "strategic steer" from the Government to prioritise innovation and growth, focusing on eight key industrial sectors, including defence. And, in the US, the administration has been focused on increasing production capacity and removing chokepoints in the defence industrial supply chain.

The result is a complex, multi-layered regulatory environment but one in which there is increasing potential for a more permissive, flexible, and expedited approach to enforcement. A coordinated strategy across regulations – and across jurisdictions – is key.



Merger control

Merger control is increasingly relevant not only to consolidation in the defence industry but also investments by outside players such as sovereign wealth funds, banks and PE firms. Even smaller stakes can trigger merger control filings in certain jurisdictions, with minority stakes in competing companies under the regulatory spotlight. Broader collaboration through, for example, partnerships or joint ventures may also be notifiable depending on the exact structure.

While competition authorities are principally tasked with examining the anticompetitive effects of a merger, they do not operate in a vacuum. Authorities will take account of the specificities of defence markets as part of their assessment, as well as broader industrial policy around building sovereign defence capabilities within the boundaries of their remit. In the EU, the Commission may go further with a proposal to include "defence readiness" as a positive factor it can consider when conducting merger reviews.

That said, with significant potential for AI to transform the sector, M&A in defence may attract significant scrutiny in particularly dynamic and innovation-driven markets. Acquisitions – where dominant players acquire highly-innovative emerging competitors to defend against future competition – remain a hot topic for authorities worldwide.

Antitrust

Collaborations that fall outside the scope of merger control review, remain subject to general competition rules – in particular, the prohibition on anticompetitive agreements. While regulators recognise that "good" collaboration will play an important role in scaling defence capabilities, they also view competition oversight as part of the solution in fostering well-functioning and resilient markets.

Collaboration between competitors may give rise to competition concerns due to the collaboration itself – for example, joint bidding between players who could credibly bid alone – or if the collaboration leads to anticompetitive sharing of competitively sensitive information.

Parties must ensure that appropriate information sharing safeguards are in place and scope any pro-competitive objective of any collaboration are clear, legitimate and maintained throughout its duration.

FDI

Globally, the FDI landscape remains in flux: new regimes continue to "go live" while more established (and active) jurisdictions develop and refine scope. In the EU, unlike merger control, there is no "one stop shop" for review – almost all member states operate their own regimes, albeit with some cooperation as a result of the EU's Foreign Direct Investment Screening Regulation.

While sensitive sectors vary by jurisdiction, defence is generally a core sensitive sector attracting scrutiny, with dual-use goods and even suppliers to the defence sector often caught. A number of regimes – including the UK – are "investor agnostic" i.e. screening is not limited to foreign investors. Filings will also often require detailed disclosure of ownership structures, extending to ultimate beneficial owners including board members. Most regimes often lack transparency, operating as a "black box" given national security considerations. FDI rules may also be used in unconventional ways to further political agendas.

Subsidy control, state aid and FSR

The involvement of Government support brings regulation that targets "distortive" state subsidies into play. In the EU, state aid rules may apply. The Commission has however emphasised in its Defence Readiness Omnibus the potential availability of Article 346 TFEU (concerning Member State measures necessary to protect essential security interests) as an exemption. Article 346 aside, the Commission has also highlighted the existing "compatibility possibilities" under state aid rules including through the application of the general "block exemption" or via direct approval by the Commission. On the latter, the Commission has indicated it will take account of a measure's contribution to defence readiness as part of its assessment and will prioritise cases with that objective.

In the UK, the subsidy control regime relies on self-assessment by public bodies (and recipients) – in contrast to its EU equivalent – in principle allowing for a more flexible and efficient approach to awarding subsidies in the defence space. Potentially applicable exemptions include an exemption for subsidies given to safeguard national security.

Finally, in respect of non-EU government subsidies, in an M&A context – as well as public procurement in certain circumstances – the FSR may apply, adding a further layer of review.

Public procurement

Significant procurement opportunities will continue to arise as governments continue to look to grow their defence capabilities. These opportunities may however be subject to public procurement rules – rules which govern the lifecycle of a procurement from initial advertisement through to contract award and beyond.

In the EU, targeted amendments to the Defence Procurement Directive have been proposed through the Defence Readiness Omnibus, including streamlined rules for joint procurement (across member states) and doubled thresholds for supply and service contracts. The Commission is also undertaking an "impact assessment" to determine what further changes are needed to simplify and speed up defence procurement in the EU.

In the UK, defence procurement is governed by the relatively new Procurement Act 2023, with the Government indicating in its Defence Industrial Strategy that it will rely on the "existing flexibilities in the Act" to drive effective defence procurement – including through direct award (awards without a competitive process), permitted contract modifications and exemptions (including on national security grounds).

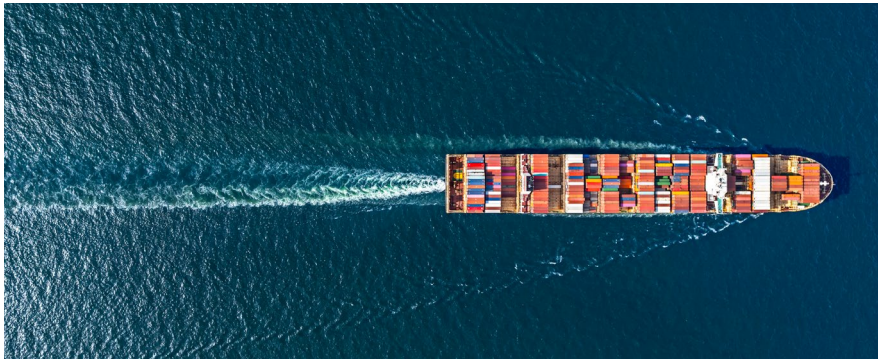
The Ministry of Defence (MoD) is permitted to appoint a contractor by direct award, bypassing any competitive process altogether, if only one contractor can deliver the goods or services required – for example, for national security reasons or because a unique capability is needed.

Where a direct award is made and the prime contract is worth £5,000,000 or more, the contract will be a Qualifying Defence Contract (QDC) and will be subject to the Single Source Contracts Regulations 2014 (SSCR)[22].

A similar regime applies further down the supply chain: a sub-contract worth at least £25,000,000 will be a Qualifying Sub-Contract (QSC) if at least 50% of the value of the obligations under it are in support of a QDC or another QSC[23].

The practical consequences of QDC or QSC status are worth understanding clearly. QDCs are limited to the regulated pricing methods set out in the SSCR: firm pricing, fixed pricing, cost-plus pricing, estimate-based fee pricing, volume-driven pricing, and target pricing. There is no flexibility to use other pricing structures. The allowable baseline profit rate under QDCs and QSCs is also capped, with the cap reviewed and set each year by the Single Source Regulations Office (SSRO). On top of that, QDCs and QSCs are open to scrutiny by the SSRO, which is tasked with assessing value for money under QDCs and QSCs.

Contractors working within this framework must be alert to the need to have their cost management and reporting practices in good shape from day one. Understanding the permissible pricing regimes and what costs can be recovered under the contract is also essential for both investors and contractors.



View sources

Contracting with government

Every supplier in the defence sector is, ultimately, providing goods or services to a government or government body. This structural reality shapes the entire legal and commercial environment. Operating within a supply chain of this sensitivity carries a bespoke set of obligations: compliance with applicable national and international legislation; adherence to government-mandated contractual frameworks and reporting requirements; and, in some cases, integrating private sector goods and services with government-supplied assets and information essential to project delivery.

Government contracting frameworks

Navigating defence procurement requires familiarity with bespoke terminology and standard-form documentation. In the UK, central to this are DEFCONs – standard defence conditions published by the Ministry of Defence for incorporation into defence contracts, spanning technical requirements, security and cyber security obligations, insurance, financial reporting, and legal provisions including indemnities and governing law (among other things). DEFCONs are routinely flowed down from head contracts to sub-contracts and are frequently accompanied by DEFFORMs (standard administrative and reporting forms) and DEFSTANs (specifications setting baseline safety, quality, and operability requirements).

In the US, federal government contractors must comply with specific cybersecurity and confidentiality requirements under various frameworks intended to protect federal contract information (FCI) and the more sensitive, controlled unclassified information (CUI). These include the recent Cybersecurity Maturity Model Certification (CMMC) 2.0 Program requirements for CUI (subject to a phased implementation) and the US General Services Administration's IT Security Procedural Guide.

Of particular significance across all jurisdictions are government-mandated termination provisions and relief clauses. Government contracts typically afford the relevant authority broad termination rights and, in certain cases, operate bespoke termination compensation regimes. Understanding these provisions alongside often complex pricing structures and incentivisation mechanisms is essential to managing risk across the supply chain.

Government-supplied assets, equipment, and information

It is standard practice for governments to supply certain key assets, equipment, and information to prime contractors. In the UK, these are designated as Government Furnished Assets, Government Furnished Equipment, and Government Furnished Information – collectively referred to as GFX. Title ordinarily remains vested in the authority, and GFX is typically provided free of charge pursuant to a pre-agreed contractual schedule.

GFX is integral to programme delivery and can have an impact on payment milestones and supply chain risk management: delays or deficiencies in GFX provision can have cascading consequences for the authority, contractors and sub-contractors alike. Where timely delivery is at risk, parties will typically be required to explore mitigation options before any entitlement to cost or time relief crystallises. On receipt, contractors bear responsibility for inspection; where defects are identified, the obligation to repair or replace items falls on the authority. Responsibility for safe custody, maintenance, and return subsequently passes to the contractor, with the authority retaining rights of inspection and audit throughout.

Legislation and international supply chains

The international nature of defence supply chains, with an ever-increasing need for cohesion between allies, means that one nation's defence legislation can have an impact on the supply chain for and delivery of defence projects in another nation. For example, the US International Traffic in Arms Regulations (ITAR) and the US Export Administration Regulations (EAR) impose stringent limitations on sharing technical information with foreign nationals without US government approval. In these circumstances, the head contract may include a contractual obligation for the authority to provide support to the prime contractor and/or its sub-contractors to obtain relevant export control clearances.

Sanctions, ethics and compliance

The expansion of global defence activity will bring with it a continued focus on an increasingly complex compliance environment. For those in the Defence space, sanctions, ethical risk, and regulatory compliance are not peripheral concerns: they sit at the heart of every transaction, contract, and partnership.

Sanctions

The weaponisation of sanctions as a tool of foreign policy has accelerated dramatically since 2022. Defence players must navigate overlapping and sometimes conflicting sanctions regimes – including those of the UK, EU, US, and UN – when structuring transactions, engaging suppliers, and entering new markets. The risk of inadvertent sanctions exposure is particularly acute in complex supply chains where beneficial ownership and the ultimate destination of goods or technology are not always transparent. Robust sanctions screening and ongoing monitoring are essential.

Export controls

The transfer of defence goods, technology, and technical data across borders is tightly regulated. Clients must ensure compliance with the UK's Export Control Joint Unit framework, US ITAR and EAR requirements, EU rules and equivalent regimes in partner jurisdictions. Missteps can result in criminal liability, significant fines, debarment from government contracting, and severe reputational damage.

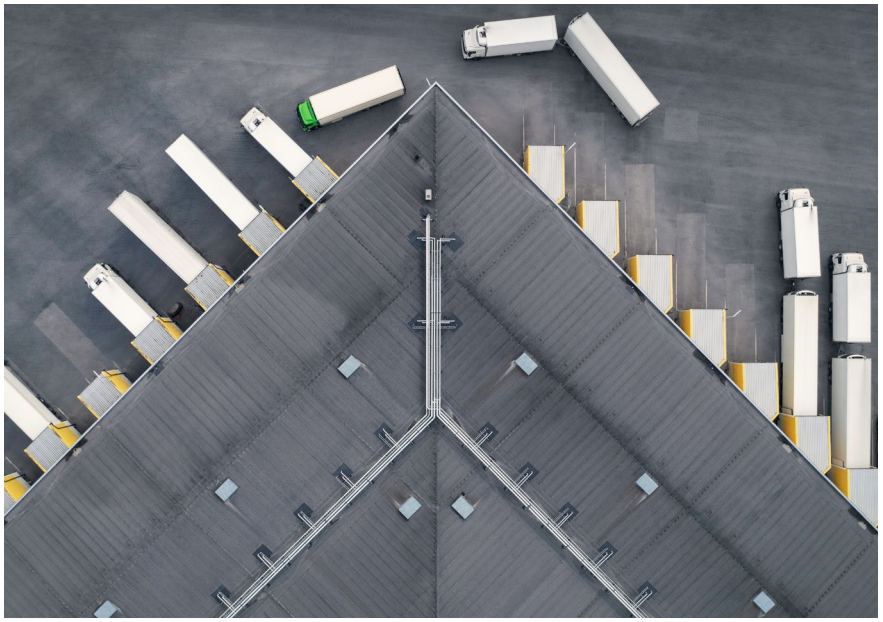
Licensing regimes

Operating in the defence sector requires clients to navigate a demanding framework of licensing obligations. Licence portability, change-of-control provisions, and government consent requirements must therefore be identified and managed early.

Anti-corruption and ethical risk

Defence procurement, particularly in emerging markets and through intermediary arrangements, carries elevated exposure to bribery and corruption risk under the FCPA, UK Bribery Act and equivalent legislation.

As programme values increase and procurement is accelerated, the pressure points multiply. This will inevitably lead to a rise in fraud investigations, export control enforcement actions, sanctions compliance reviews, and anti-corruption inquiries, particularly in cross-border and multi-jurisdictional defence programmes.



Cyber security in the grey zone

The cyber security framework has grown progressively stricter as each year passes. The approach in the EU can be traced back to the NotPetya attack. Alongside the growing risk of nation-state cyber-attacks, this highlights two broader points – the impact of these attacks on a wide range of critical and important companies, and the need for software and hardware providers to secure their systems.

NotPetya – Cyber conflict in a hybrid threat environment

The NotPetya attack arose out of a software updated issue by M.E.Doc, a Ukrainian company that produced accounting software. Russian-backed threat actors had infiltrated M.E.Doc's systems and inserted a virus into that software update.

When M.E.Doc's customers downloaded and installed the software, that activated the virus which then traversed those customers' international networks using the EternalBlue exploit. This caused a large global outage at many critical and important private sector companies such as Maersk, Merck and Mondelez. The total cost is estimated to have exceeded US$10bn[24].



View sources

Regulation of critical sectors

To address the risk to critical and important entities, the EU has passed the NIS II Directive[25]. This significantly enhances the cyber security obligations applicable to critical national infrastructure. In summary:

- **Expanded scope:**
  The obligations in NIS II apply to a much broader range of entities. Alongside entities in "traditional" critical sectors, such as energy, transport and water; it will also encompass sectors such as data centre providers, manufacturing, chemical production and distribution, food production, processing and distribution and research.
- **Enhanced cyber obligations:**
  NIS II contains general obligations to apply appropriate technical and organisational measures to prevent cyber-attacks, and to report incidents to the relevant regulator. This is supplemented by the very detailed security obligations under the Commission Implementing Regulation[26] and applies very extensive and specific cyber security obligations.

The EU Digital Operational Resilience Act, known as DORA[27], contains similar provisions applicable to the financial services sector, with other states taking similar measures, such as the Cyber Security and Resilience (Network and Information Systems) Bill. Meanwhile, the US Cybersecurity and Infrastructure Agency (CISA) is in the process of finalising new rules under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) to require critical infrastructure players to make prompt reporting of major cyber incidents to the federal government.

Once the implementing rules are finalised, CISA will require covered critical infrastructure entities to report covered cyber incidents within 72 hours of discovery and report any ransomware payments within 24 hours of making the payment. Like NIS II, CIRCIA applies broadly to 16 critical infrastructure sectors[28].

Security of software and hardware

The EU Cyber Resilience Act[29] addresses the need to tackle security issues at source and imposes an obligation on producers of software and hardware products to build in security to their products and to then continue to support those products through updates and vulnerability reporting. This principle also applies in the United States, where security is regarded as a fundamental requirement for software and hardware supporting critical or defence-related functions. Federal regulations and guidelines promote development practices that are "secure by design and by default," accompanied by continuous obligations to patch, monitor, and manage vulnerabilities.

None of these new laws are directly applicable to military activities, but companies operating in related sectors, such as defence manufacturing, may be caught. In any event, grey zone cyber attacks are already spilling over to affect private sector organisations meaning that the protection of critical infrastructure is a core national security concern.

For business, the message is clear: cyber risk is now becoming a board-level, macro risk. Companies are expected to harden critical systems, secure digital supply chains and meet security standards that go beyond minimum regulatory compliance. Boards should be able to demonstrate active oversight of cyber and AI risk, including governance structures, incident response plans and investment in resilience.

View sources

Digital sovereignty

As set out above, there is an increasing focus on "digital sovereignty" – the need for states to maintain control of their digital infrastructure.

The approach in the EU to this issue has historically been based not on national security but instead around the fundamental right to data protection. The seminal decision of the EU Court of Justice in *Schrems I* (C-362/14) and *Schrems II* (C-311/18) address the question of whether personal data will be subject to essentially equivalent protection once transferred to a third country.

In practice, there is a correlation between the states that raise fundamental rights concerns and those that raise national security concerns. This is reflected in the EU Commission finding[30] that many traditional allies – such as Canada, the UK and the US – are at least partially adequate for data transfers. At the least, these general restrictions on transfers of personal data have incentivised EU companies to use data centres in the EU.

However, transfers of personal data to third countries are coming under increasing legal pressure and there is an ongoing challenge to the EU Commission's decision to permit transfers to entities in the US subject to EU-US Data Privacy Framework[31]. The loss of that framework could have catastrophic impacts for EU-US data transfers and wider commerce.

There is also likely to be increasing political and legal pressure to localise digital infrastructure for national security reasons. The EU's proposed Cyber Security Act 2[32] contains express powers for the EU Commission to third countries as "high-risk" with suppliers from those jurisdictions excluded from cybersecurity standardisation work and public procurement. This trend to apply national security considerations to data transfers is likely to accelerate in all jurisdictions.

There are significant technical and practical challenges for businesses looking to fully implement "sovereign" digital infrastructure. For example, even if a data centre is physically based in a particular state, it may well be dependent on remote support from a third country. Regardless of these challenges, businesses should anticipate increased pressure to minimise digital dependency on potentially unfriendly third countries.



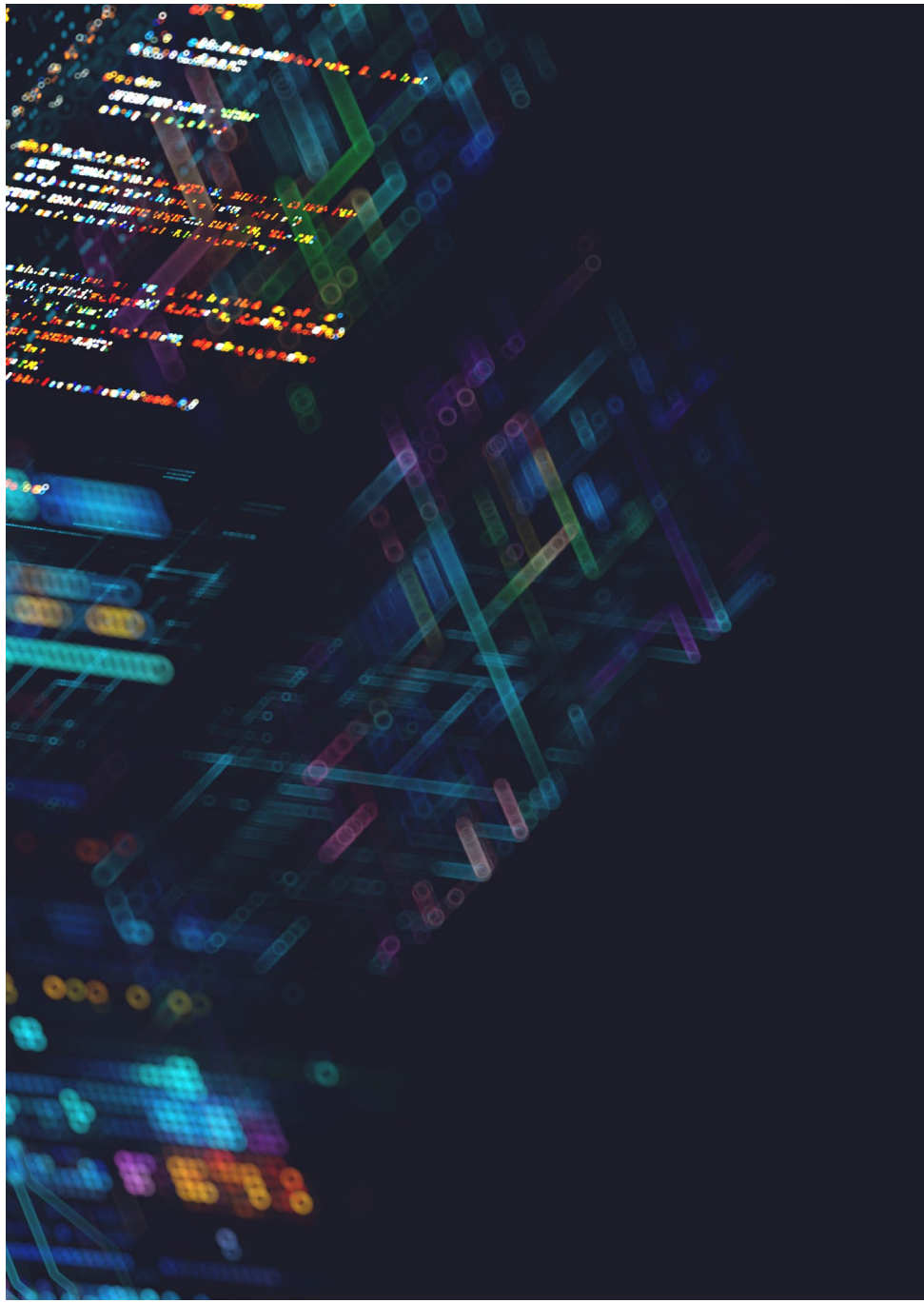
View sources

AI, technology regulation and LAWS

The growth of cyber security laws has been accompanied by wider technology and digital regulation – most notably attempts to regulate artificial intelligence through measures such as the EU AI Act and a slew of state-level AI statutes in the US. That Act directly regulates the development of general-purpose AI models but otherwise has limited direct relevance to defence industries.

It does however highlight the intense focus on artificial intelligence. It is very likely that artificial intelligence will become an increasingly important tool for defence and deterrence but will also compress decision-making time, complicate attribution and strain classical deterrence doctrines. Questions remain about how states can maintain human control, avoid inadvertent escalation at “machine speed”, and build cooperative frameworks for responsible military AI and cyber operations.

Artificial intelligence is continuing to develop at a rapid pace and is likely to have an important role in defence. However, some uses raise significant ethical and legal concerns. Those deploying artificial technology in defence solutions should consider whether this is appropriate in principle but also whether the right framework is in place to train and test that technology. They should also consider whether any controls should be placed on downstream use of that technology.



Lethal autonomous weapon systems (LAWS)

Artificial intelligence has many potential defence uses. For example, Anthropic's Claude has been used as part of Palantir's Maven Smart System to provide real-time targeting for military operations against Iran.

However, most attention has been on the use of artificial intelligence to create LAWS. They have been a possibility for many years but recent advances in artificial intelligence have made this a reality, even for relatively low-cost systems. There would also be significant tactical advantages in drone warfighting – the extensive use of jamming and other drone-countermeasures making the remote operation of these drones increasingly difficult and greatly increases the benefits of autonomous operation.

The international community has been debating the regulation of LAWS for several years, particularly the extent to which it complies with basic principles of humanitarian law such as necessity, humanity, distinction and proportionality.

The principles of distinction and proportionality are particularly problematic as they often require difficult and subjective judgments to be made in the context of complex and rapidly evolving military scenarios. Even if these judgments can be delegated to a machine in principle – there is concern that it may be very difficult to demonstrate this given the difficulties in training and testing these systems in true battlefield conditions.

Some LAWS are already in service, such as the ship-based Phalanx system, which has been in use since 1973 and automatically targets and engages targets such as incoming missiles or aircraft. This raises limited concerns because it operates at sea where the presence of civilians is less of a factor and functions within narrow parameters.

An autonomous drone traversing a town or city to identify hostile targets is inherently riskier.

In 2019, the parties to the Conventional Weapons Convention endorsed 11 Guiding Principles about the application of international humanitarian law to the development and use LAWS, including that humanitarian law continues to apply in full and that "*human responsibility for decisions on the use of weapon systems must be retained since accountability cannot be transferred to machines*".

Little further progress has been made, and recent developments suggest that some states have limited appetite for further controls.

For example, the US Department of War is evidently intending to develop LAWS and became embroiled in a major dispute with Anthropic when Anthropic prohibited military use of its AI tools without human responsibility for the use of force.

> "Partially autonomous weapons, like those used today in Ukraine, are vital to the defense of democracy. Even fully autonomous weapons – those that take humans out of the loop entirely and automate selecting and engaging targets – may prove critical for our national defence.
>
> But today, frontier AI systems are simply not reliable enough to power fully autonomous weapons … without proper oversight, fully autonomous weapons cannot be relied upon to exercise the critical judgment that our highly trained, professional troops exhibit every day."
> **Dario Amodei, Anthropic**

Intellectual property rights

Intellectual property is among the most strategically sensitive and legally complex issues in the defence sector. As governments and primes race to acquire and deploy cutting-edge capability, the ownership, protection, and exploitation of IP has never been more significant.

Patents and technology protection

Patents protect innovations in weapons systems, platform design, materials science, and dual-use technologies, but also raise unique challenges in a defence context. In the UK, Crown use provisions that allow the state to exploit patented technology without consent, subject to compensation. In the US, the Bayh-Dole Act governs rights over federally-funded inventions, permitting contractors to retain ownership whilst granting the government a licence to use them. The scope of these rights is a critical due diligence issue in any acquisition of US defence technology assets. The US International Trade Commission also provides a powerful forum for asserting patent rights against imported defence products.

Jointly developed IP

Joint ventures and collaborative programmes create significant uncertainty over ownership of background IP, foreground IP and improvements. Careful contractual drafting at the outset is essential, particularly where parties from different jurisdictions are collaborating under different legal frameworks.

Technology transfers and licensing

In the US, licensing International Traffic in Arms Regulations (ITAR)-controlled technology requires government approval through Technical Assistance Agreements or Manufacturing Licence Agreements. Arrangements must also address change-of-control scenarios and the divergence between military and commercial applications of shared technology. Similarly, Export Administration Regulations (EAR)-controlled software and technology can be subject to restrictions on technology transfers and licensing to safeguard national security and foreign policy interests.

Trade secrets and know-how

Where patent protection is unavailable or undesirable, trade secret protection becomes critical. Trade secrets play a critical role in the defence sector, as defence programmes frequently depend on highly sensitive know-how that is not patented to prevent public disclosure, which could compromise military advantage or facilitate replication by adversaries or competitors.

The US Defend Trade Secrets Act provides a federal civil remedy for misappropriation: an important tool where unauthorised transfer of proprietary knowledge carries national security consequences.

Government rights

In the US, the government can often obtain specific rights in IP and technical know-how that go beyond a typical commercial licence, especially where government funds contribute to development. In many instances (for example, under the Bayh-Dole Act or US Federal Acquisition Regulation), based on the funding received from the government, the underlying IP rights may be subject to disclosure or government “march-in” rights as well as non-exclusive licences, “unlimited rights” or “government-purpose rights”. These rights can include broad use, reproduction, modification and disclosure within government and, in some cases, to third-party contractors for maintenance, competition or follow-on work.

A contentious horizon

As defence spending accelerates and transactional activity intensifies, a significant wave of disputes and investigations looms. The pressure to reshore, restructure, and rapidly scale production will generate substantial contractual litigation. Delivery failures, force majeure claims, price escalation disputes, and the consequences of supplier substitution are already emerging – and will increase in frequency as governments demand faster output from supply chains not yet equipped to deliver it.

Rise in disputes

The pace and complexity of defence deal-making is creating fertile ground for post-completion M&A disputes. These are likely to include warranty and indemnity claims, earn-out disagreements, material adverse change arguments, and disputes arising from regulatory clearance failures – particularly under foreign investment screening regimes such as the UK's National Security and Investment Act.

The risk of procurement challenges brought by unsuccessful bidders also increases materially as governments accelerate and expand procurement programmes, often under political pressure and with reduced process rigour. Similarly, parties may rely on contentious routes to help determine their rights under hastily implemented joint development arrangements, licensing agreements, particularly in relation to IP ownership, know-how boundaries, and data. These disputes will be particularly acute where military and commercial applications of jointly developed technology diverge.

The cross-border nature of modern defence programmes and transactions will also raise complex questions about where disputes will, and should, be resolved. Parties must navigate competing jurisdictions, differing attitudes to confidentiality, and the particular sensitivities that arise where classified information or national security considerations are in play.



Our sector leaders

We advise major industry players, investors and governments navigating this highly complex regulatory environment.

Linklaters is a global law firm focused on bringing legal certainty in a changing world. Our global network combines local expertise and spans 30 offices and in 20 countries. We have over 2.500 lawyers who advise on multi-jurisdictional projects and transactions around the world.

With a deep understanding of the sector and a presence in key jurisdictions, we excel in navigating the complexities in strategic transactions and cooperations, technological advancements and the protection of related intellectual property and systems. The number and variety of mandates we have advised on gives us an invaluable pool of experience and ensures we are at the forefront of developing innovative solutions to support your strategic objectives.

For more insights, visit our Aerospace, Defence & Security Insights Hub: Aerospace, Defence and Security



Simon Branigan
Global Head of Corporate
Partner, London
Tel: +44 20 7456 3309
simon.branigan@linklaters.com



Kristina Klaaßen-Kaiser
Corporate and M&A
Partner, Düsseldorf
Tel: +49 211 22977 598
kristina.klaassen@linklaters.com



Dr Timo Engelhardt
Corporate and Global Industrials Sector Lead
Partner, Munich
Tel: +49 89 41808 447
timo.engelhardt@linklaters.com



Georgina Kon
Digital, Data and Commercial
Partner, London
Tel: +44 20 7456 5532
georgina.kon@linklaters.com



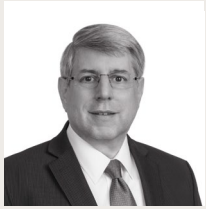
Jason Manketo
U.S. Corporate Finance Partner
London & Dubai
Tel: +44 20 7456 4654
jason.manketo@linklaters.com



George Casey
Global Chairman of Corporate
Chairman of the Americas, New York
Tel: +1 212 903 9300
george.casey@linklaters.com



Anna Mitchell
Antitrust & Foreign Investment
Partner, London
Tel: +44 20 7456 2801
anna.mitchell@linklaters.com



Jonathan Gafni
Head of U.S. Foreign Investment
Partner, Washington, D.C.
Tel: +1 202 654 9278
jonathan.gafni@linklaters.com



Rachel Barrett
Head of ESG
Partner, London
Tel: +44 20 7456 5414
rachel.barrett@linklaters.com



Richard Coar
Energy & Infrastructure
Partner, London
Tel: +44 20 7456 5189
richard.coar@linklaters.com



Satindar Dogra
Litigation, Arbitration & Investigations
Partner, London
Tel: +44 20 7456 4316
satindar.dogra@linklaters.com



Shruti Chopra
Intellectual Property
Partner, New York
Tel: +1 212 903 9448
shruti.chopra@linklaters.com



Silke Bernard
Investment Funds
Partner, Luxembourg
Tel: +352 2608 8223
silke.bernard@linklaters.com



Victoria Wright
Leveraged Finance
Partner, London
Tel: +44 20 7456 3076
victoria.wright@linklaters.com

Our global experience

An overview of some of the transactions we have been supporting clients on.

- Thyssenkrupp: ongoing advice on the spin-off of Thyssenkrupp Marine Systems.
- Renk Group: (i) advising investment banks on the initial public offering (IPO) of Renk Group AG on the Frankfurt Stock Exchange and (ii) advising on entering into a binding agreement for the acquisition of David Brown Defence.
- Safran.AI: advising on the acquisition of technologies from Kayrros.
- Raspberry Pi: advising the British microcomputer maker on its £541.6m IPO and listing on the Premium Segment of the LSE.
- Heidelberger Druckmaschinen AG: advising the global leader in technology and mechanical engineering and its wholly owned subsidiary HD Advanced Technologies GmbH on forming a joint venture for drone defence with US-based Ondas, Inc. and Ondas Autonomous Systems in Europe.
- European Investment Bank: assisting the EIB on a venture debt financing for Optics11, a Dutch deep tech company advancing fibre-optic sensing systems for critical energy and defence.
- Heckler & Koch: advising on (i) corporate matters (also cross-European) and (ii) comprehensive advice in connection with various actions for annulment of resolutions.
- Rheinmetall AG: advising Rheinmetall, inter alia, on (i) its issuance of €500m 1.875% Convertible Bonds due 2028 and (ii) on its issuance of €500m 2.250% Convertible Bonds due 2030.
- HENSOLDT AG: advising the joint bookrunners on the capital increase (ABB) and private placement of shares of HENSOLDT.
- Airbus: advising (i) the defence and space business of Airbus regarding the potential acquisition of a listed German entity (aborted) and (ii) on various dispute matters.
- Volkswagen: advising on the sale of its (indirect) 76% stake in the listed Renk AG.



- John Cockerill: advising on its proposed acquisition of the French leading manufacturer of defence vehicles Arquus from Volvo group.
- Private Equity Investor: advising in relation to an investment into the fibre network operator serving the German army barracks.
- B/E Aerospace: advising on (i) the acquisition of the aerospace manufacturer F+E Fischer + Entwicklungen GmbH & Co. KG, (ii) its acquisition of E-Mug Technologies' aerospace engineering and research and development business in India, (iii) the US$1.05bn acquisition of the consumables solutions business from Honeywell International, (iv) the spin-off of its consumables management segment businesses to KLX Inc.
- BAE Systems: advising on (i) its issue of £400m bonds to be admitted to the Official List of the UK Listing Authority and to trade on the regulated market of the London Stock Exchange plc., (ii) the disposal of its remaining 10% stake in Saab AB, (iii) its Eurosystems JV with Finmeccanica in numerous jurisdictions, (iv) the long-term partnering agreement with the Ministry of Defence to reduce the costs and rationalise the UK munitions sector, and (v) the recapitalisation of a joint venture in the area of case telescoped weapons and ammunition.
- Theon International: advising the underwriters on the IPO of Theon International plc on Euronext Amsterdam.
- A French multinational aerospace, defence and security corporation: advising on (i) their strategy regarding a global patent question in connection and (ii) the potential acquisition of Survitec Aerospace & Defence (aborted).
- Praesidiad and Carlyle: advising on the sale of the Praesidiad Group to Alcentra Limited and Cheyne European Strategic Value Credit RAIF. The project included investment control procedures in Belgium, Germany, Slovakia, the UK, the Czech Republic and the United States.
- Serco: advising on (i) the disposal of the majority of its operations in Germany, (ii) the sale of its nuclear consultancy business to AMEC and (iii) the UK Ministry of Defence's Future Provision of Marine Services (FPMS).
- German Government: advising on a cornerstone investment in an international venture capital fund investing in technology start-ups for defence and security.
- UK Ministry of Defence: advising on (i) its £4.2bn acquisition of a further five Type 26 Frigates from BAE Systems Surface Ships Ltd . (ii) on the competitive tender for, and construction of, the UK's new Type 31 class of naval warship.
- The largest construction PPP in France: advising Natixis on the hedging of the financing of the PPP for the construction of the new French Ministry of Defence complex on the Balard site in Paris.
- Kongsberg Gruppen: advising on its £500m acquisition of the marine products, systems and aftermarket services businesses of Rolls-Royce.
- Safran Aero Booster: advising the subsidiary of the Safran Group, and the Belgian State with respect to a joint venture for an innovative compressor test centre.
- RTX Corporation: advising on the sale of its actuation business to Safran, a French multinational in the aerospace sector for US$1.8bn.
- An US company in the technology sector: advising on the acquisition of 100% of a UK defence contractor. Due to the activities of the target business in the area of dual-use goods and suppliers to various European arms companies and armies it included notification requirements in Germany, the UK, France and Italy.
- United Technologies Corporation: advising on (i) its US$16.5bn acquisition of Goodrich Corporation – UTC's biggest deal in a decade, (ii) its US$3.46bn disposal of its pumps and compressors business and (iii) the disposal of an aircraft engine repair business to Metal Technology Co., Ltd.
- Montagu: advising the London-based private equity house on the acquisition by its portfolio company Jane's, the aerospace and defence information business, of RWR Advisory Group.
- British multinational arms, security, and aerospace company: providing strategic advice in respect of their US$5.6bn acquisition of Ball Aerospace.

- Advent International: advising on its recommended £4bn cash offer for Cobham plc.
- Viasat, Inc: advising on the UK merger control aspects of its US$7.3bn acquisition of Inmarsat. After an in-depth Phase 2 inquiry, the CMA granted unconditional clearance for the transaction.
- OGMA: advising OGMA on the structuring and implementation of a joint venture with a Portuguese engineering company, EEA – Empresa de Engenharia Aeronáutica, to supply selected components to Embraer of its new military aircraft KC-390.
- Kellogg Brown & Root Limited as sponsor: advising on strategic options following the insolvency of Carillion as its joint venture counterparty and then on its acquisition of Carillion's interest in the Aspire Defence project.
- British multinational arms, security, and aerospace company: advising on its appeal to the EU General Court, seeking annulment of the European Commission's decision of April 2019 which concluded that the group financing exemption provided under the UK's controlled foreign company (CFC) rules partly contravened EU State aid rules.
- A satellite technology company: advised on the acquisition by a Canadian strategic investor, which was ultimately cleared unconditionally in Phase II after the implementation of certain ring-fencing measures.
- Krauss-Maffei-Wegmann: advising on (i) its acquisition of MAN Mobile Bridges Business and (ii) on the procurement of 472 Multi Role Armoured Vehicles BOXER by the German and Dutch Ministries of Defence from ARTEC GmbH.
- Tinicum and Blackstone: advising on the £1.275bn recommended offer for Senior plc, a FTSE 250 constituent that designs and manufactures high-tech components and systems for equipment manufacturers across aerospace, defence, land vehicle, power and energy markets.
- Blackstone and Draken International: advising on the acquisition of Cobham's UK aviation services business (CAvS UK) as part of a competitive auction process.
- Wespavia SA: advising on the €100m equity financing of public takeover of LMI Aerospace, Inc., a US aerospace supplier listed on Nasdaq.



Sources

1 Global military spending rise continues as European and Asian expenditures surge | SIPRI
2 Global military spending rise continues as European and Asian expenditures surge | SIPRI
3 How $400 FPV Drones Are Destroying Tanks and Rewriting the Rules of War | Military Machine
4 Ukraine's low-cost interceptor drones rewrite rules of air defense | AP News
5 GAO, DEFENSE INSUSTRIAL BASE: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers | GAO
6 EU Policies SAFE | Consilium Europa.EU
7 Rheinmetall completes acquisition of Loc Performance in the USA | Rheinmetall
8 M&A in Defense: Why All Eyes Are on Europe | Bain & Company
9 S&P Global Market Intelligence's Annual Private Equity and Venture Capital Outlook Indicates Optimism Amid Macroeconomic Caution | S&P Global Market Intelligence
10 https://www.bain.com/insights/aerospace-and-defense-m-and-a-report-2025/ | Bain & Company
11 European Defence Fund (EDF) – Official Webpage of the European Commission | Defence Industry and Space
12 2025 State of the DIB report on CMMC Compliance | cybersheath.com
13 McKinsey & Company: Scaling Security – Munich Security Conference | McKinsey report
14 This quote is often wrongly attributed to Charles Darwin, though does paraphrase the concepts in *On The Origin of Species*.
15 Munich Security Index 2026 | Munich Security Conference
16 https://cybercrim.com/case-study/notpetya-cyberattack/ | cybercrim
17 Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025 | CMC
18 Principles for Responsible Defence Investment Concept Note – November 2025
19 Study results: Access to equity financing for European defence SMEs | Defence Industry and Space
20 https://www.spglobal.com/market-intelligence/en/news-insights/articles/2026/2/europe-outpaces-global-rise-in-private-equity-aerospace-defense-investments-98858635 | S&P Global Market Intelligence
21 £2bn boost for defence sector to unlock orders from allies | GOV.UK
22 Guidance: Direct Award | GOV.UK
23 Guidance: Direct Award | GOV.UK
24 NotPetya: The Most Expensive Cyberattack in History | Cybercrim
25 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).
26 Regulation (EU) 2024/2690. This regulation only directly applies to a subset of essential and important entities providing digital infrastructure and services, including managed service providers, but is likely to set a benchmark for all entities subject to NIS II.
27 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.
28 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA
29 Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).
30 The EU Commission can make a finding that state's data protection laws are adequate which allows personal data to be freely transferred to that state.
31 See *Latombe v Commission* (C-703/25 P).
32 Proposal for a Regulation on ENISA, the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

linklaters.com

This content is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions on issues reported here, please get in touch. © 2026 Linklaters.

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of the LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, 20 Ropemaker Street, London, EC2Y 9AR, England or on **www.linklaters.com** and such persons are either solicitors or registered foreign lawyers. Please refer to **www.linklaters.com/regulatory** for important information on our regulatory position.

CD724_F/09.26