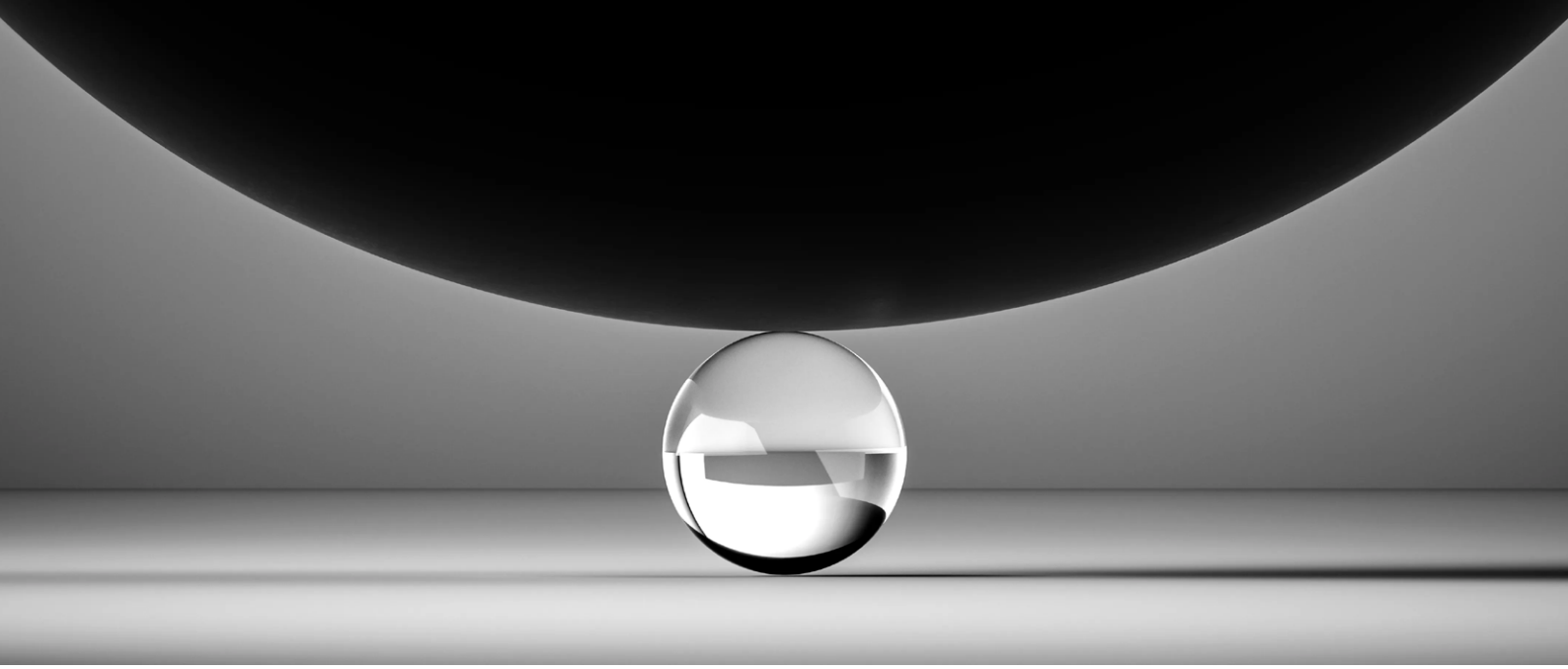
A&O SHEARMAN

PRIVATE CAPITAL PERSPECTIVES

Resilient returns: *investing in defense*

Contents



Resilient returns: how drive for defense autonomy is creating demand for private capital investment

Geopolitical volatility and the desire for defense resilience are creating a powerful new investment cycle, with governments looking to mobilize private capital to scale industrial capacity, particularly in dual-use and technology-led assets. But this is not a conventional market: complex regulation, political oversight and constrained deal dynamics demand a fundamentally different approach from investors seeking to participate.

BY MAGDA NASILOWSKA, HENDRIK ROEHRICHT AND JEAN LEE

SUMMARY

- Recent increases in budgets and NATO spending commitments are driving significant opportunities for private investors in the defense sector.
- Private equity investment has surged, with record deal values over the past year.
- Europe's defense expansion is supported by political consensus and industrial policy tools like SAFE and ReArm Europe, which aim to mobilize private capital alongside public funds.
- Despite clear policy encouragement, defense investing remains complex due to strict regulations, compliance obligations and unique government involvement, requiring investors to adopt fundamentally different approaches.

Rapidly evolving geopolitical conflicts and the pivot towards greater strategic autonomy, particularly in Europe, are driving historic levels of spending on defense.

The U.S. defense budget rose over 7% to USD962 billion for 2026, with proposals to push it to USD1.5 trillion by 2027. NATO members have pledged to allocate 5% of their GDP to defense, while research from Carlyle suggests that European defense and infrastructure spending could reach EUR14tn over the next decade.

In response, an increasing number of private capital providers are loosening historic constraints to launch dedicated defense strategies.

PRIVATE EQUITY INVESTMENT IN AEROSPACE AND DEFENSE HITS NEW HIGH

Private equity deal value in the aerospace and defense sector hit a record USD55.6bn in 2025. Public markets have followed: the Stoxx Europe Aerospace and Defense index has more than tripled since 2022.

This is a structural shift rather than a cyclical trend. Europe's defense expansion is underpinned by political consensus across EU institutions and member states that strategic autonomy requires sustained industrial investment. Order backlogs at Europe's largest defense companies have risen by around 15%, creating pressure to expand production capacity.

Meanwhile, EU industrial policy tools (including the Security Action for Europe (SAFE) funding program) are using public money to mobilize private capital as a core element of the buildout. This approach is further reinforced by the EU's ReArm Europe strategy.

These trends present a significant and sustainable opportunity for private capital investors and for portfolio companies planning to enter the market, particularly those with technologies that have both civilian and military applications.

However, despite clear signals from policymakers in the U.S. and across Europe encouraging greater private capital participation in the sector, there are significant trade-offs that must be addressed, not least that defense is a complex, tightly governed industry, with extensive regulation and strict compliance obligations.

WHY INVESTING IN DEFENSE ASSETS IS DIFFERENT

The emergence of specialist PE funds, defense-focused private credit vehicles and private capital firms entering into joint ventures with primes reflects growing institutional comfort with the sector.

However, investors new to the sector need to understand that defense investments are not like other deals. The defense industry operates under a unique set of economic, regulatory and political rules with governments at the center: as customer, regulator, funder and gatekeeper.

Revenues are often indirect, with government contracts held by prime manufacturers (e.g., Lockheed Martin, RTX, BAE Systems, Safran, Rheinmetall and Leonardo), and value flowing through tightly controlled supply chains.

In response, investors must build extensive relationships with primes, defense authorities and local champions. They must also be prepared for sector-specific processes: long and sometimes opaque procurement cycles, states seeking broad rights over intellectual property, and extensive and closely audited compliance obligations throughout the supply chain; end-to-end traceability of components, stringent cybersecurity protections, auditability, certified quality management and lawful sourcing. Private capital investors must engineer compliance via flow-down clauses, verification rights and offset governance arrangements.

DEAL PROCESSES FACE INTENSE REGULATORY SCRUTINY

Defense M&A due diligence takes substantially longer than in other sectors, often requiring security clearances and multijurisdictional approvals. Foreign Direct Investment (FDI) screening is intense. Government spending programs often impose minimum content requirements: Europe's SAFE program, for example, aims to cap components sourced outside the EU and a subset of associated countries at 35% of contract value.

This creates structural disadvantages for non-EU-domiciled funds. Critically, it is not just where a fund is raised but where the investment committee sits and decisions are made that can determine eligibility.

Similar dynamics are at play in the U.S., where the federal administration is focused on onshoring defense supply chains. Here, the Department of War, through the Office of Strategic Capital, is expanding its budgetary and loan authority to support domestic manufacturing, particularly in critical minerals. A notable emerging structure involves government debt financing alongside private equity. However, this state money can carry conditions, including that products developed with public support must be dual- or multi-use.

ESG NOT THE BARRIER TO INVESTMENT IT ONCE WAS

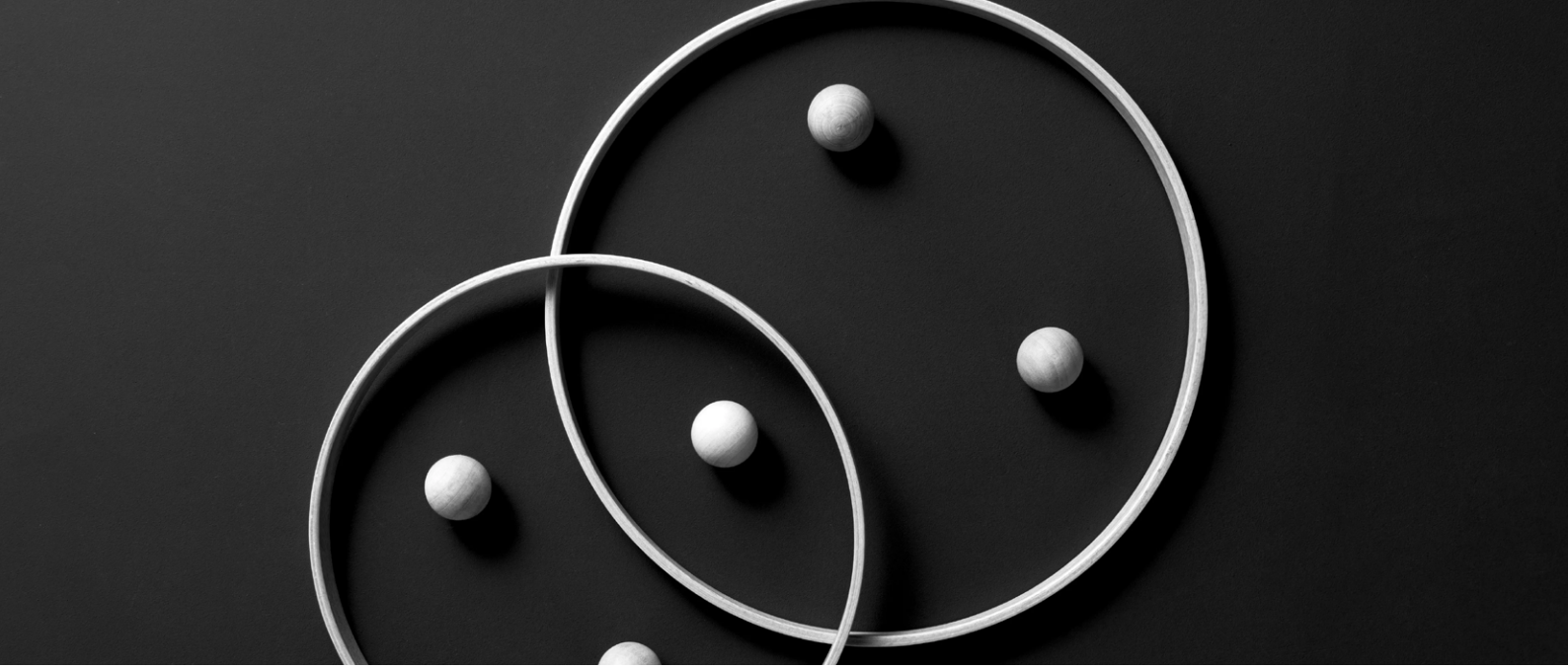
ESG considerations remain a source of debate: while both the UK's FCA and the EU have clarified that sustainability rules do not prevent defense investment, a NATO Innovation Fund study found exclusion policies still in place at 75 of Europe's largest banks.

At the same time, the definition of "defense" itself is expanding. Dual-use technologies, critical infrastructure, and enabling capabilities (including AI, quantum, cybersecurity, drones and semiconductors) are increasingly drawn into the defense perimeter. These assets are increasingly attractive to private capital sponsors, given that they lack the entrenched supplier relationships of traditional military domains and offer a larger pool of potential buyers outside of pure-play defense contractors.

PROCUREMENT DYNAMICS CREATE ASSET VALUATION CHALLENGES

Despite the trajectory of the sector, asset valuations are complicated by volatile procurement cycles. Sales pipelines can spike sharply with new orders and then flatten, so investors must time their entry and exit with care. Reputational risk is also a factor, as is litigation, which can arise from a variety of sources. Eligibility tests, local-content rules, tighter foreign investment screening, and lengthy procurement and approval procedures add further complexities.

However, demand-side signals from governments in the U.S., across the EU and beyond show a tangible commitment to strengthen defense spending and, crucially, to support the industry. To do so, private capital is increasingly recognized as essential by policymakers, regulators and the wider market.



What defense investors need to know about FDI and antitrust screening regimes

Defense deals are subject to overlapping regulatory screening regimes, each with distinct triggers and remedies. Here we explore how early regulatory mapping, coordinated filings and carefully calibrated deal terms are critical to navigating an approval landscape that is both complex and increasingly interventionist.

BY DANIEL HARRIS, CATHERINE HEIN, DOMINIC LONG, FRANCESCA MIOTTO, KEN RIVLIN, JAMES FORD AND MARIO GARCIA

SUMMARY

- FDI screening requirements vary by jurisdiction, with regulators in the U.S., UK, EU, Spain, and Australia enforcing strict controls on foreign investments in businesses with defense applications.
- National regulations often capture minority stakes and may require remedies such as co-investors, firewalls, or nationality restrictions for directors to protect sensitive information and assets.
- Investors should conduct rigorous early self-assessment of regulatory requirements and develop sophisticated government affairs strategies, as regulators may scrutinize fund structures and underlying limited partners.

The acquisition of an interest in defense or dual-use businesses could trigger reporting and approval requirements under applicable FDI regimes, depending on the nature and level of investment. FDI reviews consider whether a transaction could pose national security risks, including in relation to the reduction of critical capabilities and the leakage of classified information.

In the U.S., the FDI screening process is administered by the Committee on Foreign Investment in the United States (CFIUS), which has broad authority to review transactions that could result in foreign control of a U.S. business.

CERTAIN NON-CONTROLLING BUT NON-PASSIVE INVESTMENTS IN SCOPE FOR CFIUS

CFIUS screening also applies to certain non-controlling but non-passive investments in "TID U.S. businesses" (which involve critical technologies, covered investment critical infrastructure (e.g., critical telecommunications, financial systems etc.) or sensitive personal data), and transactions that involve real estate in proximity to certain U.S. government and military facilities. A CFIUS filing may be mandatory when a foreign investor acquires an interest in a TID U.S. business.

The Defense Counterintelligence and Security Agency (DCSA) addresses FOCI (foreign ownership, control or influence) when a foreign person has the power, directly or indirectly (whether exercised or not) to direct or decide matters affecting the management or operations of a U.S. company that possesses a facility clearance, classified information, or classified contracts (we explore the issues surrounding classified information and security clearances in more detail here). A U.S. company determined to be under FOCI is unable to perform classified work unless and until effective security measures have been put in place to negate or mitigate FOCI to the satisfaction of the DCSA.

The International Traffic in Arms Regulations (ITAR), administered by the Directorate of Defense Trade Controls (DDTC) within the U.S. Department of State, impose specific requirements (including registration) on U.S. companies that manufacture, export, or broker defense articles, defense services, or related technical data listed on the United States Munitions List (USML). When there is a material change in registration information, or a foreign person or entity acquires ownership or control of a DDTC-registered company, the company must notify the DDTC in writing.

UK REGULATIONS IMPOSE MANDATORY REPORTING REQUIREMENTS

In the UK, the National Security and Investment Act (NSIA) governs the screening of foreign (and domestic) investments in sensitive sectors. Certain acquisitions of targets that deal in or manufacture defense items fall within the scope of reporting requirements under the NSIA and are subject to mandatory notification to, and prior clearance by, the UK government, coordinated through the UK's Investment Security Unit. Transactions that do not obtain requisite clearance in advance are deemed legally void in the eyes of the UK courts, with acquiring parties potentially subject to fines, and in certain circumstances, criminal sanctions. Transactions considered to give rise to a risk to UK national security may be unwound if already completed, cleared subject to remedies or prohibited.

In the European Union, Regulation (EU) 2019/452 establishes a cooperation and coordination framework for the screening of FDI on security or public order grounds, which specifically includes defense and dual-use items such as AI, quantum computing and semiconductors. Screening decisions remain the exclusive competence of member states, but the regulation enables the Commission and other EU countries to review and comment on transactions that raise cross-border concerns. In response to the regulation, all member states have incorporated FDI screening mechanisms into their national legislation. Failing to comply with the applicable requirements could result in transactions being prohibited or unwound.

MANY EU MEMBER STATES' RULES CAPTURE MINORITY INVESTMENTS

Across EU member states, many national screening protocols capture minority stakes. Spain for example has a dedicated defense FDI regime triggered at a 5% ownership threshold that is applicable to any non-Spanish investor, including EU nationals. The Spanish government may impose a diverse range of remedies in defense transactions, including requiring foreign buyers to accept Spanish co-investors, implement firewalls to protect sensitive information or assets, and mandating that directors be Spanish nationals.

In Australia, the country's Foreign Investment Review Board (FIRB) conducts enhanced reviews of overseas investments into businesses with defense or military applications, particularly for foreign-government-linked investors. Here, a mandatory notification and approval may be required prior to acquiring stakes as low as 10%, with no minimum dollar investment threshold, and for certain investors prior to starting a business which proposes to operate in the defense space.

The identity of private equity funds' limited partners presents a potential regulatory obstacle. Many FDI regulators look through a fund's structure to examine the nationality and profile of underlying LPs, on the basis that those providing capital may exercise influence regardless of formal voting rights.

EARLY ASSESSMENT OF POTENTIAL RISKS IS VITAL FOR INVESTORS

Investors exploring opportunities in the defense sector should conduct early, rigorous self-assessment via scoping out likely FDI requirements and modeling the range of possible outcomes, including governance restrictions that may limit synergies or information flow. Particularly in the U.S., a sophisticated government affairs strategy, including lobbyists engaged before the deal, has become a feature of the market under the current administration.

Conditionality in transaction documents must be carefully drafted: hell-or-high-water clauses applying to FDI notifications are generally resisted by acquirers given the unpredictability of government-imposed conditions, and sellers and buyers must negotiate how to distribute regulatory uncertainty accordingly. Investors must also think about their exit options from the outset; the pool of eligible buyers for businesses considered relevant to national security is likely to be narrower than in other sectors, with FDI restrictions imposing an additional hurdle. As a result, we are seeing increasing interest in public listings as an exit option, an issue we explore in more detail here.

MERGER CONTROL PROCESSES ADD FURTHER COMPLEXITY

Alongside FDI screening, merger reviews and, in the EU, the Foreign Subsidies Regulation (FSR), may also be applicable.

For private capital investors, merger control assessments may apply to firms pursuing bolt-on strategies. At one level, defense deals are assessed like any other transaction, with antitrust authorities focused on the impact of transactions on competition.

However, in Europe the focus on defense preparedness has seen the EU Commission become more receptive to arguments about resilience when analyzing deals (i.e., also considering the impact of transactions on the robustness of the European defense supply chain, access to key inputs and the ability of companies to withstand shocks).

The Commission is currently conducting a review of its merger guidelines, with competitiveness, innovation and supply chain resilience identified as core themes.

The recently published draft revised guidelines go further than prior practice by explicitly recognizing that, in certain circumstances, consolidation may contribute to security of supply, industrial scale and the ability of European firms to compete effectively in global and technologically dynamic markets, including in strategically sensitive sectors such as defense.

This represents a shift in emphasis from the traditional framework, under which such considerations were primarily assessed as efficiencies invoked to rebut identified harm. While the draft guidelines do not change the underlying legal standard, they suggest a more integrated approach in which potential pro-competitive effects are assessed alongside theories of harm as part of the overall competitive analysis.

As we explored in our recent alert, this evolution may allow parties to proactively frame transactions in terms of their contribution to scale, innovation and resilience, rather than relying on these arguments only at a later stage.

With that said, merger assessments remain anchored in established principles, and the Commission continues to require robust, verifiable evidence demonstrating that any claimed benefits are merger-specific and sufficient to offset a reduction in competition. In practice, the evidentiary bar remains high.

In defense transactions, this evolving approach is also reflected in longer pre-notification phases and earlier engagement on potential remedies, particularly where markets are already concentrated and/or strategic capabilities or supply chains are at issue.

In In the U.S., the Hart-Scott-Rodino merger filing process underwent a significant overhaul in early 2025 with the introduction of a revised form that required substantially more information than under the previous regime.

Earlier this year the old, shorter form was temporarily reintroduced as the Federal Trade Commission (FTC) appealed a lower court decision that it had overstepped its rulemaking authority.

At the same time, merger filings for qualifying transactions (which include some technology deals) are now sent to the Department of War as well as being reviewed by the Department of Justice and FTC. It is not yet clear how the DOW uses the information it receives.

GLOBAL COORDINATION ACROSS APPLICABLE REGIMES IS CRITICAL TO SUCCESSFUL EXECUTION

The FSR review process is designed to investigate and counteract distortive subsidies granted by non-EU governments. The term "foreign subsidy" covers any financial contribution from a non-EU government or public entity that confers a selective benefit on a business operating within the EU single market. "Financial contributions" is defined broadly to include grants, loans, tax incentives and even the provision of goods or services at market terms.

FSR mandates pre-notifications for large mergers (where the target or one of the merging parties has a turnover within the EU of more than EUR500m and the parties received combined foreign financial contributions (FFCs) of more than EUR50m in the previous three years) and significant public tenders (more than EUR250m in contract value, with the bidder receiving FFCs exceeding EUR4m).

Against this backdrop, global coordination is critical: FDI, merger control and FSR filings across jurisdictions must not fall out of step, and remedies across regimes and countries must be aligned.

Presence of classified information imposes constraints on defense deal execution

Investing in targets that hold sensitive government information can introduce layers of complexity when executing deals. Here we explore the issues investors need to look for, and how potential risks can be mitigated.

BY KEN RIVLIN, ADAM SCHWARTZ, CATHERINE HEIN, RAVI DE FONSEKA, ARTHUR SAUZAY, JAMES FORD, MARIO GARCIA, LUC LAMBLIN AND LARA FONTAINE

SUMMARY

- Investments involving classified data face strict national security regulations, with risks including contract cancellation, loss of clearances, and potential criminal liability if mishandled.
- Security clearance requirements exist at multiple levels, including facility, personnel and site clearances, and a change in ownership may require structural safeguards to be implemented.
- Many jurisdictions have specialised screening regimes for defense investments, often requiring governance changes, firewalls and commitments to protect sensitive information from foreign influence.
- The due diligence process is complicated by information gaps, as deal teams may need clearances to access sensitive contracts, and the scope of possible regulatory conditions is broader than in other investment contexts.

For private capital firms investing in the defense sector, dealing with classified information and security clearances presents distinct challenges that can fundamentally shape deal execution.

Defense investments are often subject to strict national security restrictions that govern the disclosure, handling, exchange and dissemination of sensitive information, and which operate independently of, and in addition to, FDI screening regimes. Here the consequences of missteps can range from the loss of government contracts and security clearances to criminal liability.

Security clearances operate at multiple levels: facility clearances (formal certifications verifying that an organization can securely handle, store and process classified government information on their own premises and that physical, IT and personnel security procedures meet government standards); personnel clearances for key individuals and board members; and in some jurisdictions, clearances specific to physical sites.

CHANGE OF CONTROL CAN RESULT IN GOVERNMENT CONTRACTS AND SECURITY CLEARANCES BEING LOST

A change in ownership can trigger two distinct consequences. First, contractual change of control clauses may cause the cancellation or non-renewal of sensitive government contracts held by the target. Second, security clearances themselves may be lost if a new owner does not meet national security requirements. To mitigate these risks, investors may need to implement structural measures such as voting trusts or proxy agreements to address potential foreign ownership, control or influence (FOCI) concerns.

In the United States, investors targeting businesses with access to classified government information must navigate a process outside of the CFIUS FDI screening regime administered by the Defense Counterintelligence and Security Agency (DCSA).

The DCSA process addresses concerns surrounding foreign ownership, control or influence (FOCI) over companies in the defense supply chain. Mitigating identified FOCI risks may require structural governance changes such as carving out the U.S. business; restricting board access; or entering into national security agreements that limit interaction between the U.S. operations and the non-U.S. acquirer. Parties must scope out what the DCSA (if it applies) and the CFIUS process will entail and potentially propose governance or structural changes in advance to secure the necessary approvals. Importantly, ensuring that the right individuals are in the room to help negotiate these measures is essential.

These issues are not unique to the U.S. Some EU member states are eyeing America's FOCI model as a way to protect national security and industrial secrets. France for example is looking to place restrictions on foreign-controlled businesses to limit access to confidential information, including via governance mechanisms such as proxy boards.

In Spain, a specific screening regime for defense investments exists which sits outside the country's general FDI screening framework. Here, investments in which a foreign buyer purchases 5% of a target's share capital, or which allow a foreign investor to directly or indirectly form part of the company's management body, are subject to scrutiny, with the regime giving authorities broad discretion to request remedies or negotiate commitments on inbound investors.

Measures may entail establishing firewalls to protect sensitive information or assets; remedies to protect the "Spanish-hood" of the company's management (potentially with mandates that directors be Spanish nationals); commitments regarding the provision of services to the Spanish market or clients; and the inclusion of domestic co-investors to enable local board-level oversight of how sensitive information is handled.

DEAL TEAMS MAY REQUIRE SECURITY CLEARANCES TO CONDUCT DUE DILIGENCE

The mere presence of classified information in defense transactions presents additional complexities. Deal teams involved in M&A processes may be required to obtain security clearances to review certain contracts, and in some situations, it may not be possible for all sensitive agreements to be diligenced. This creates a fundamental information gap: when a buyer submits an application for investment approvals, the process may trigger concerns that it could not have known about in advance.

The sheer scope of potential conditions is also materially different from other types of investment reviews. In an antitrust context, for example, investors can generally anticipate regulatory challenges and propose "fix it first" solutions such as carve-outs or disposals to address overlapping product markets.

In defense transactions, not only could a government's potential concerns be invisible due to the relevant information being restricted, but the range of conditions that could be imposed is also unpredictable. As a result, the degree of uncertainty in defense transactions is structurally greater than in other regulated sectors.

Given these dynamics, purchasers should avoid accepting "hell-or-high-water" clauses in deals that involve conditions precedent relating to government approvals. Standard representations and warranties regarding completeness of disclosures may need to be adjusted to account for classified information controls.

Case study: classified information and data center deals

Classified information can also present challenges for private capital investors targeting assets that sit adjacent to the defense sector itself.

In Australia, any entity seeking to host or process government data must obtain government credentials, while data center operators in the government and defense space face a further layer of regulation under Australia's hosting certification framework.

Data centers must be individually certified by the government before they can host classified material, through an application process that is both extensive and costly. Applicants are required to provide detailed information not only about the physical assets proposed for hosting, but about their entire ownership structure (traced up the chain) to ensure there is no foreign government or sovereignty risk.

This can present issues to potential investors who cannot have certainty prior to the closing of a transaction that the Australian government will approve their hosting certification framework application.

In response, some operators maintain dedicated sites for government or defense purposes, though not all do; in either case, the operator must be structured to satisfy Australia's regulatory requirements before it can host both government and non-government data.

Amid rising interest in defense, IPOs are an increasingly viable exit route for investors

Public listings are becoming an attractive path to liquidity in a sector where trade buyers may be constrained by national security considerations. However, defence IPOs bring distinctive challenges, from handling classified information and export controls to addressing compliance gaps and reputational risk.

BY TIM STEVENS, JEFF HENDRICKSON AND MAGDA NASILOWSKA

SUMMARY

- Defense IPOs are gaining traction as exit routes for investors. However, defense listings face unique legal, diligence, and compliance challenges.
- Government contracts and geopolitical factors are central to defense companies' business models, requiring careful alignment with political priorities for success in public markets.
- The Czechoslovak Group's recent EUR3.8bn IPO on Euronext Amsterdam, the biggest defense IPO to date, exemplified these trends, highlighting the importance of a strong order backlog and secure supply chain.

IPOs are an increasingly viable exit route for equity investors with defense-related businesses in their portfolios. The universe of potential trade buyers for defense assets is likely to be limited in a world where governments have a significant say in any change of ownership, and therefore flotations are a good option for sponsors seeking a liquidity event.

Defense IPOs present distinctive legal and diligence challenges that set them apart from conventional listings. Government contracts are central to defense companies' business models but are not standard commercial agreements; while they are often long-term, defense procurement requirements give government buyers significant negotiating power as well as the right to alter commercial terms. Potential investors will therefore want to carefully diligence these agreements in order to take a view on the quality and security of the company's order book.

CHALLENGES OF HANDLING CLASSIFIED INFORMATION ADD COMPLEXITY TO LISTINGS

The challenges of handling classified information add a further degree of complexity. As we explain in more detail here, it may not be possible for certain agreements to be fully disclosed in the run-up to a listing. Export controls bring additional challenges as the required permissions can be withdrawn at short notice, meaning contractual certainty is never absolute. Defense companies pursuing IPOs therefore need to develop frameworks for managing these risks.

Compliance is another key focus area. Founder-led and fast-growing companies in the defense supply chain (i.e., the sort of businesses that private equity and growth capital investors are increasingly targeting) often do not have the mature compliance processes of defense primes. Any gaps in anti-bribery and sanctions controls should be addressed by investors at the point of commitment in preparation for an eventual exit.

PR risk is equally significant and demanding of early attention. Ensuring that a company's end-users are in countries that investors and the public would be comfortable with is an important consideration in advance of a listing. A clean compliance record and a defensible customer base are not things that can be built retroactively.

ESG CHALLENGES NEED TO BE CAREFULLY HANDLED DURING BOOK-BUILD

Defense IPOs also face a structurally narrower investor universe than most sectors, with many ESG-mandated funds, sovereign wealth funds and values-based investors excluding or restricting defense holdings. A traditional book-build that reveals uneven demand from certain investor categories during the price discovery process could create negative signaling effects. However, a fixed-price offering avoids this dynamic: demand is assessed privately through the pre-placement, and the public offering proceeds at this price without the transparency (and potential for negative headlines) of an open book.

Geopolitical instability and the desire among governments to build "strategic autonomy" will ensure that government budgets will continue to flow into the sector for the foreseeable future. But private capital sponsors must pay close attention to governments and their advisers to ensure their portfolio investments remain aligned with political priorities and can continue to access public funds. The companies that succeed in public markets will be those that understand the political landscape from the outset and position themselves accordingly.

Case study: the Czechoslovak Group IPO

Our global team recently advised the underwriters on the EUR3.8bn IPO of Czechoslovak Group (CSG) on Euronext Amsterdam. The transaction was, according to Euronext, the largest defense IPO in history both in terms of the amount raised and market capitalization, the biggest European IPO since 2022 and the most significant listing on Euronext Amsterdam in more than a decade. The market cap of CSG upon IPO was EUR25bn.

CSG is a key supplier to Ukraine, which accounted for around a quarter of CSG's sales in the first nine months of 2025. The IPO proceeds will contribute to the company's international expansion, including via further acquisitions following CSG's purchase of U.S. ammunition maker Kinetic from Remington in 2024.

CSG's equity story was based around three core pillars: macro tailwinds from increased defense spending globally; the company's EUR14bn order backlog; and a secure supply chain for critical components. NATO countries' public commitment to rebuild their ammunition stockpiles was an important factor, with CSG's products (primarily ammunition) not vulnerable to rapid technological obsolescence.

Investor expectations of forward-looking guidance for defense companies led to CSG preparing a profit forecast, which may set a precedent for future defense listings. A pre-placement with key anchor investors, an accelerated timetable (to mitigate exposure to headline risk), a fixed price rather than a traditional book-build, and conservative pricing of the stock led to the IPO being oversubscribed by a factor of ten. In response, CSG's share price rose 31% on debut to value the business at around EUR33bn.

A conservative fixed price serves important strategic purposes for defense companies. First, it generates strong aftermarket performance, which builds long-term investor confidence in a sector that may be unfamiliar to many institutional investors. Second, oversubscription at a fixed price allows the issuer to allocate shares selectively, prioritizing long-term holders, strategically aligned investors, and those comfortable with the defense sector's unique risks, including its PR and ESG dimensions.

Amsterdam served CSG as a neutral, EU-based listing venue that reinforced the company's positioning as an international business. The choice of venue, the abbreviation of the company name from Czechoslovak Group to CSG, and the emphasis on global sales were all part of a deliberate strategy to broaden the investor base. CSG's successful listing demonstrates investor appetite for defense-related assets but also underscores the importance of robust preparation.

Dual-use technologies offer attractive defense entry point for private capital firms

Technologies with both civilian and frontline applications are drawing significant investor interest as the definition of defense broadens beyond traditional hardware. These assets are often easier to square with ESG commitments and offer strong exit pathways, but remain subject to the same regulatory scrutiny as pure-play defense companies.

BY JESSE DEBBAN AND DANIEL HARRIS

SUMMARY

- Dual-use technologies, which serve both civilian and frontline purposes, are increasingly attractive to private capital firms.
- However, despite their appeal, dual-use companies remain subject to close government scrutiny, including under FDI screening regimes.
- Personal data is now classified as a dual-use asset with national security implications, leading to tighter controls and contractual obligations regarding data transfers to certain countries.
- Private investors are increasingly splitting portfolio companies into military and non-military divisions to maximise exit value and broaden acquisition options.

Dual-use technologies (i.e., items that are designed for commercial/civil use but that can also be used in battlefield, security or weapons proliferations purposes, such as drones, artificial intelligence, cybersecurity systems and quantum computing) are a rapidly expanding area of investment focus for private capital firms.

The broadening definition of defense beyond traditional hardware is creating significant value creation opportunities, but it also brings legal, regulatory, and practical challenges that require careful consideration.

DUAL-USE PORTFOLIO COMPANIES ATTRACT INTEREST FROM PRIMES AND PRIVATE EQUITY

The rising interest in dual-use investments is in part a response to increasing government investment in defense. But it also reflects the fact that dual-use companies are often easier to reconcile with LP ESG mandates and ethical sensitivities than direct munitions manufacturers (an issue we explore in more detail here).

They also offer a more diverse set of exit options, with dual use assets potentially of interest to both defense primes and private equity buyers. For the latter we see particular interest in commercial-first, defense-adaptable technology under AUKUS Pillar II, which covers cyber, AI, electronic warfare, quantum, hypersonic/counter-hypersonic missiles and undersea systems.

The principal deal execution challenge for investors is regulatory. Dual-use companies are subject to the same scrutiny that applies to munitions manufacturers in areas including FDI reviews and export controls.

PERSONAL DATA NOW TREATED AS A DUAL-USE ASSET

Sensitive personal data is also now expressly treated as a dual-use asset with national security implications. In the U.S., the Committee on Foreign Investments in the United States examines whether transactions may expose personally identifiable information, genetic details or other sensitive data of U.S. citizens to access by foreign governments or persons.

The Department of Justice's Data Security Program (which prohibits, with some exceptions, the transfer of "bulk" sensitive personal data and government-related information to countries of concern including China, Hong Kong, and Russia), goes further, requiring any U.S. business that shares such data with a non-U.S. entity to have in its contracts a provision to stop it being transferred to the countries of concern.

ROBUST DILIGENCE REQUIRES DETAILED ASSESSMENT OF FINANCING STRUCTURES

Diligencing a dual use company (which may be relatively early in its growth journey) requires a detailed understanding of their financing structures. Again in the U.S., government-affiliated investors such as In-Q-Tel (the CIA's investment fund) often inject capital into early-stage businesses developing technologies in aligned areas.

These stakes are credentializing for the business but are likely to come with extensive governance rights which may include board observer seats, information rights, and rights to negotiate future use of the technology. This is the case even where the initial investment may be relatively small.

In preparation for an eventual exit we are seeing private capital investors split dual-use portfolio companies into separate military and non-military arms connected by inter-group licensing agreements. The separation is designed to maximize exit value by broadening the potential acquirer base for the civilian business while preserving the higher-value military component for a more targeted sale.

And as the definition of what constitutes a defense asset expands, private capital investors need to assess the profile of their existing portfolio companies with this in mind when considering their exit options. As we explore here, IPOs are an increasingly attractive option given investor interest in defense-related assets, and the fact that national security restrictions mean the universe of trade buyers for such businesses is likely to be limited.

Why diligencing compliance processes is critical in defense and dual-use investments

Close interaction with governments and intermediaries places defense companies at heightened risk of bribery, corruption and related financial crime. Here we explain how investors must assess not only the existence of compliance frameworks, but whether they are effective in practice and aligned with evolving enforcement expectations.

BY ADAM SCHWARTZ AND AMY EDWARDS

SUMMARY

- Effective due diligence of defense targets requires assessing not only the existence but also the practical effectiveness of anti-bribery and anti-corruption (ABAC) frameworks, including strong controls over third parties and board-level governance.
- Regulatory bodies like the UK Serious Fraud Office (SFO) and U.S. Department of Justice (DOJ) demand data-driven evidence that compliance systems are actively functioning, not just formally in place.
- Legal and regulatory landscapes are rapidly evolving, with new EU directives and continued U.S. enforcement requiring defense companies to keep ABAC policies current and aligned to local requirements.
- Investors must also address broader risks including sanctions, export controls, anti-money laundering, and proliferation financing, conducting thorough due diligence on ownership and financial flows to avoid regulatory penalties.

The defense sector is an inherently higher-risk environment for corruption, bribery, and financial crime. Governments are the ultimate buyers of defense equipment and therefore the degree of interaction with state actors (including politically exposed persons or PEPs) is high.

Taking Europe as an example, the market has 27 end customers (the EU member state governments), with funds flowing either through contracts directly with governments or via subcontracting arrangements with prime defense manufacturers. These dynamics present a heightened risk of corruption and fraud, with the UK government's anti-corruption strategy specifically identifying the global defense sector as a focus for enforcement.

GOOD ABAC COMPLIANCE REQUIRES BOARD-LEVEL GOVERNANCE

For private capital firms, whether investing through equity or lending, robust due diligence of a target's anti-bribery and anti-corruption (ABAC) compliance is essential. Good ABAC compliance requires an up-to-date and comprehensive policy framework; strong controls around third parties such as agents and intermediaries who deal with governments on the company's behalf; evidence of proper due diligence and robust approval processes before engaging with third parties; a well-functioning internal reporting and whistleblowing system; and board-level governance showing that the framework is operating effectively.

These governance checks should examine what data is being reported at board level, for example around the number of third parties being onboarded, any internal reporting on identified issues, and what measures have been implemented to mitigate risks. Both the UK SFO and the U.S. DOJ demand data-led evidence that compliance processes are working, not just that businesses have a framework in place.

WHERE RISKS ARE IDENTIFIED, EARLY REMEDIATION IS ESSENTIAL

A key consideration for investors is the maturity of a target given that early-stage businesses may lack robust compliance infrastructure. Where a target is found to have immature ABAC processes, investors should implement robust compliance and mitigation measures as early as possible post-acquisition.

In the U.S., an M&A safe harbor exists such that if a buyer discovers post-completion bribery issues that did not surface during due diligence, prompt self-reporting to the authorities provides significant mitigation with regard to enforcement.

Compliance risks may be exacerbated by the practical limits of due diligence in the sector; defense contracts and company information may be classified and therefore cannot be disclosed to prospective buyers ahead of closing, meaning that potential issues could remain invisible at the point of commitment (an issue we explore in more detail here).

As far as legal developments are concerned, the EU anti-corruption directive, approved by the European Parliament in March 2026, will require some member states to tighten their bribery laws, meaning defense companies operating across Europe will need to keep their ABAC policies aligned with evolving local requirements.

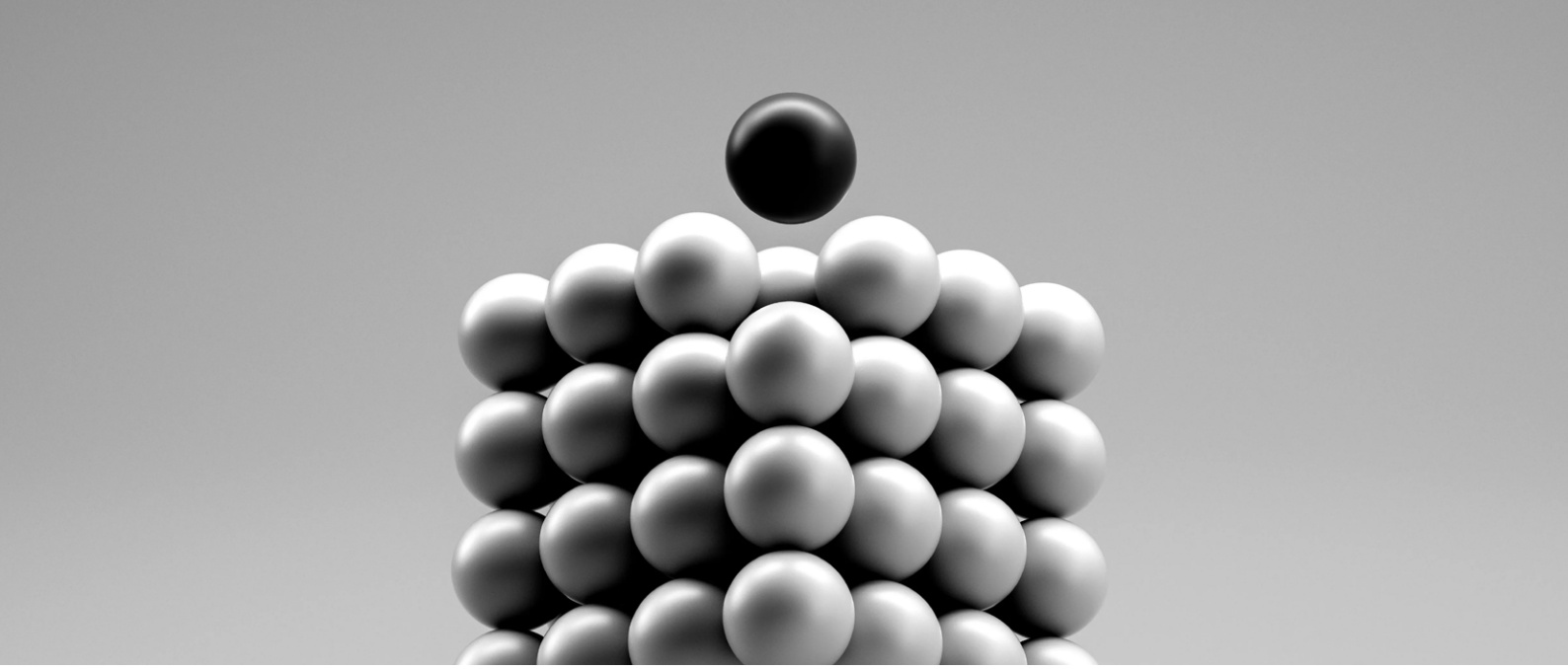
While the current U.S. federal administration announced a retreat from FCPA enforcement after the 2024 presidential election, no notable decline in activity has materialized, and the limitation period for anti-bribery offenses outlasts any single government's term.

SANCTIONS AND EXPORT CONTROL REGIMES PRESENT ADDED COMPLEXITIES

Beyond bribery and corruption, the defense sector raises heightened compliance risks around sanctions and export controls (an issue we explore in more detail here), anti-money laundering, and counterterrorism and proliferation financing. Private capital investors must conduct due diligence on the ultimate beneficial ownership of targets and subcontractors to confirm they are not sanctioned or linked to prohibited parties. The prevalence of cross-border transactions can complicate efforts to trace where funds are flowing to, with the use of complex ownership structures and shell companies important red flags.

The Financial Action Task Force has published specific guidance on proliferation financing, warning that support networks use the international financial system through indirectly connected intermediaries and front companies; involvement in proliferation financing, even unknowingly, can result in severe regulatory penalties and inclusion on sanctions lists. Ongoing portfolio screening for emerging legal and regulatory risks is critical.

Finally, investors must be mindful of the reputational consequences of exposure to the defense sector. Association with controversial weapons or unethical arms sales can lead to divestment by limited partners and public backlash, and multinational banks have historically been reluctant to lend to defense companies for fear of these risks. Proactive compliance, rigorous due diligence, and ongoing monitoring remain the most effective safeguards.



Upscaling production and investment in the Netherlands

In March 2026, A&O Shearman convened a group of financial sponsors, commercial banks, policymakers, government officials, defense primes and defense tech startups in Amsterdam to share perspectives on how best to scale production in the Netherlands. Here we summarize the key themes.

BY PETER HUIZING

SUMMARY

- Private investors and banks have become more open to funding defense companies in the Netherlands, but early-stage innovators still face challenges due to insufficient revenue certainty and traditional bank risk models.
- Structural issues in government procurement, including reluctance to commit to long-term orders for rapidly evolving technology, hinder companies' ability to secure financing.
- Hybrid venture capital/private equity funding models are emerging, enabling earlier-stage investment and sustainable scaling for defense tech companies.
- Institutional investors and public private partnership (PPP) models are increasingly interested in defense-adjacent assets like infrastructure and cybersecurity, where risk profiles are more familiar.

For a generation, the Dutch defense sector was defined by shrinking budgets and limited appetite from private investors, partly due to reputational caution driven by ESG concerns. That era is over. Today, banks report no reservations on lending to defense companies, and institutional investors have shifted their internal policies to permit defense allocations. However, there are still constraints on capital deployment, including in relation to banks' standard risk models; many of the early-stage innovators that are driving the sector's evolution do not have guaranteed offtakes or the type of revenue certainty that lenders and investors require to build a credible investment case.

The root of the problem lies in a structural tension within traditional government procurement processes. Battlefield technology is evolving at extraordinary speed, and governments, understandably, are reluctant to lock in large volume commitments to technologies that may be superseded quickly. But that same flexibility deprives companies of the revenue visibility they need to secure financing.

BANKS CALL FOR MORE TRANSPARENCY FROM THE STATE

In response, banks have called for greater transparency from the government. This is not necessarily in the shape of firm orders, but instead clearer indications of how ministries view particular companies, their management teams and their products. There have also been requests for policymakers to do more on pre-financing, including by relaxing bank guarantee requirements that are difficult for lenders to provide to early-stage companies with minimal balance sheets.

The profile of defense companies attractive to private equity remains relatively narrow: proven suppliers to major primes or dual-use businesses with stable cash flows, a credible pipeline and a viable exit horizon. Companies that fit this profile and that are available for investment are now attracting major interest from potential investors, resulting in highly competitive auctions and substantial valuation premiums. Dual-use capabilities are particularly valued because they have a larger addressable market and a potentially bigger pool of possible buyers on exit.

Venture capital faces a different challenge. Strong entrepreneurs are needed to translate knowledge and technological innovation into viable businesses, but this process can be hindered when knowledge institutions retain IP without focusing on its economic application. The gap between early-stage innovation and production-ready scale remains a persistent problem in defense technology.

THE EMERGENCE OF HYBRID VENTURE CAPITAL/PRIVATE EQUITY STRUCTURES

One emerging trend in defense is the rise of hybrid investment structures. We are now seeing venture capital and private equity financing being deployed within the same funding round. PE firms are also beginning to invest one or two rounds earlier than the pre-IPO stage at which they would typically commit, often taking governance positions in the process. Combined with public co-investment, these hybrid models offer a potential path to allow defense technology companies to scale sustainably.

Institutional investors, meanwhile, have shifted their policies but are not yet seeing enough concrete investment proposals to deploy capital at scale. They also depend on fund managers having both the ability and the willingness to identify opportunities in defense and related sectors.

There is significant interest in adapting PPP models, already proven in infrastructure and energy, to defense-supporting assets such as military barracks. Even investors hesitant about frontline production can participate in adjacent capabilities (infrastructure, energy, IT, cybersecurity, and real estate) where the investment thesis is more familiar and the risk profile more conventional.

STRUCTURAL SOLUTIONS TO DE-RISK INVESTMENTS

Beyond PPPs, several structural approaches were discussed to de-risk investment and create scale. Financing demand could be channeled through special purpose vehicles and multilateral financing mechanisms, including securitization-style approaches. The U.S. market offers an alternative solution: there, banks extend riskier credit to smaller defense companies but package it off-balance-sheet as an investable product, akin to a collateralized debt obligation (CDO) structure. Major OEMs can also play a role, reducing risk and improving financing options for SME suppliers through supply-chain financing solutions.

Joint procurement at EU or NATO level, along with export arrangements, can increase both the scale and certainty of offtake rather than relying on individual governments.

GOVERNMENTS EXPLORE 'PRODUCTION AS A SERVICE' MODELS

The rapid pace of battlefield innovation is challenging the traditional model of multi-billion-dollar, decades-long procurement contracts for heavy manufacturing products. In its place, some governments are beginning to explore "production as a service" arrangements whereby trusted companies with flexible production capabilities are provided with a threshold level of support as they continually adapt their products to maintain an edge. The emphasis shifts from fixed specifications to problem sets, combining flexibility with reliability.

For investors, this model requires a different kind of diligence. The value proposition is less about a guaranteed product order and more about a company's production agility, its relationship with the relevant ministry, and its ability to iterate quickly in response to evolving requirements.

CALL FOR MORE DIALOGUE BETWEEN STAKEHOLDERS

The Dutch government has taken early institutional steps, including by establishing a new financing unit within the Ministry of Defence. But decisions about which companies to back, how to combine public and private financing, and how to structure selection processes remain in very early stages. The planned creation of a "Dutch DARPA" has been discussed as a potential catalyst for innovation and co-investment, though its precise set-up, responsibilities and relationship with the envisaged National Agency for Disruptive Innovation remain unclear.

A recurring theme was the need for better dialogue between public and private stakeholders. The French Ministry of Defence's working-group model, which convenes government, industry, and financiers around specific financing challenges, was highlighted as a potential template.

Why ESG frameworks are not a barrier to investing in defense assets

Shifting geopolitical realities are prompting investors to reassess how defense assets fit within established ESG commitments. While certain regulatory frameworks continue to impose constraints, evolving policy guidance increasingly recognizes defense as compatible with social sustainability objectives. Here we explain how investors are responding with structuring solutions to balance their fiduciary duties with emerging opportunities.

BY KEN RIVLIN, MATT TOWNSEND, DANIEL HARRIS, JESSE DEBBAN, MAAMEYAA KWAFO-AKOTO AND JOHN ADAMS

SUMMARY

- Western governments are prioritizing defense and energy security, which is influencing capital allocation and policy decisions.
- Strict ESG regulations, such as the EU's Sustainable Finance Disclosure Regulation, still pose limitations for certain funds, particularly those labeled as "dark green" under Article 9.
- Recent guidance from the UK government and European Commission asserts that defense investments can support ESG objectives, provided they meet criteria for social sustainability and resilience—although some would disagree.
- Investors are employing structuring solutions like investing in dual-use technologies and using side letters to navigate ESG restrictions.

Defense and energy security have become significant political priorities for most Western governments and are overtaking ESG as the primary lens through which policy and capital allocation are assessed.

The forces driving this are well understood: Russia's invasion of Ukraine, which prompted a fundamental reassessment of the merits of defense-related investments; the challenge to NATO allies and its Enhanced Opportunity Partners to increase defense spending, which has intensified pressure on national budgets; and a growing desire for sovereignty amid a changing international order. For private capital firms, the question now is how to navigate existing ESG commitments while capturing the opportunity that defense presents.

SUSTAINABLE FINANCE DISCLOSURE REGULATION CONSTRAINS WHAT ASSETS FUNDS CAN HOLD

Funds and institutional investors considering opportunities in the defense supply chain must examine their investment criteria carefully. Under the EU's Sustainable Finance Disclosure Regulation, fund classifications ("dark green", "light green" or otherwise) constrain what assets a fund may hold.

Here, the strictest limitations apply to Article 9 ("dark green") funds: controversial weapons banned by international treaty are subject to zero-tolerance exclusions, conventional weapons are often capped at low revenue thresholds, and investments must pass "Do No Significant Harm" and Principal Adverse Impact tests.

At the same time, the EU Taxonomy, the classification tool for labeling investments as sustainable, continues to evolve. There is also wider discussion around whether ESG needs to become ESSG (environmental, social, security and governance) given current geopolitical volatility.

Both the UK government and the European Commission have provided helpful arguments that defense investments can align with ESG goals, particularly in supporting social sustainability by promoting peace and national security. The EU's Defence Readiness Omnibus also clarifies that the EU Taxonomy does not automatically exclude defense provided that investments bolster national resilience.

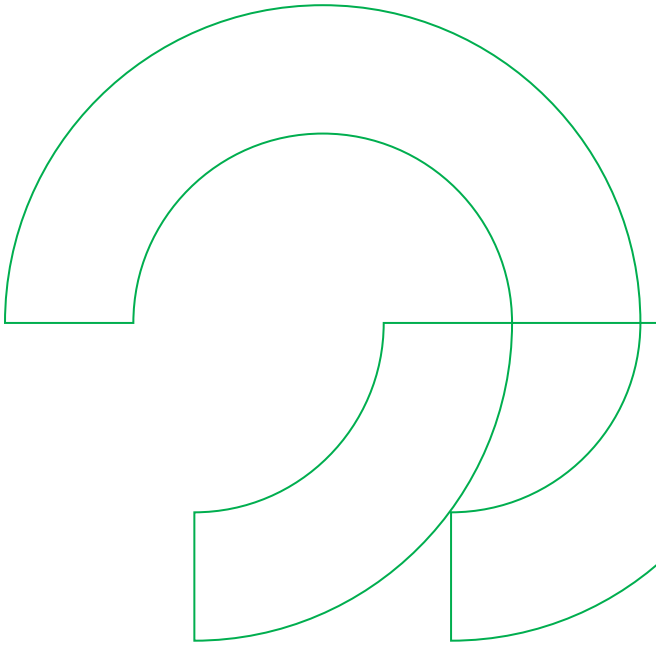
HOW DUAL-USE ASSETS AND SIDE-LETTERS CAN HELP ADDRESS ESG LIMITATIONS

Against this backdrop funds are exploring how to gain exposure to the sector, including by revisiting current restrictions in their limited partnership agreements and sustainable investment principles.

Investing in dual-use technologies (which we explore in more detail here) is one potential path through ESG limitations for many investors, with defense-adjacent infrastructure, hypersonics, cybersecurity and AI assets facing fewer sustainability obstacles than kinetic defense goods.

Side letters are another way for investors to navigate potential ESG limitations at the investor level rather than the fund level. Article 9-classified investors or those with equivalent restrictions (for example sovereign wealth funds subject to national security restrictions or pension funds with fiduciary and stakeholder concerns) can use side letter provisions such as tailored investment restrictions or excuse rights to opt out of specific defense-related investments that would breach their regulatory classification, allowing fund managers to accommodate their wishes while pursuing defense-related opportunities on behalf of other LPs. They also support enhanced sustainability reporting by creating an auditable trail that the fund has honored its commitments to ESG-mandated investors.

The operational implications, however, should not be underestimated. Where investors hold excuse rights their committed capital may not be available for certain deals, and if too much capital is excused it could trigger default provisions in subscription credit lines secured against those commitments.



Why Europe's "buy EU" principle has more opportunities for third country businesses than might appear

As the European Union accelerates efforts to strengthen its defense sector, new initiatives are reshaping procurement policies and supply chain strategies. Here we explore what this shift towards "Buy EU" requirements means for member states and private capital firms exploring opportunities in the EU defense market.

BY GAUTHIER VAN THUYNE, UDO OLGEMOELLER AND EMANUELE TRUCCO

SUMMARY

- The EU's "Buy EU" principle is being strengthened as part of broader efforts to enhance the region's defense sector and supply chain autonomy.
- New procurement policies allow member states more flexibility to exclude non-EU suppliers, tying the award of EU funds to compliance with these rules.
- However despite these measures, member states can still invoke national security exemptions to award contracts to local or certain third-country suppliers.

Amid the desire to rapidly upscale EU defense investment, and thereby to promote the EU's own defense industrial capabilities as well as boost collaboration between member states, the European Commission is pushing to establish a European defense supply chain. This is seen in Brussels as an essential step towards greater sovereignty, autonomy and resilience in an increasingly complex geopolitical environment.

"Buy EU" incentives and requirements are the critical means to achieve this goal. Here, the EU's approach is twofold. First, to provide greater flexibility for member states to exclude from procurement processes any suppliers, goods, components and services that do not meet EU qualification criteria. And second, to tie the award of EU funds to strict conditions that require member states to cooperate and comply with Buy EU rules. The Security Action for Europe (SAFE) financial instrument is arguably the best-known example in this space.

"BUY EU" APPROACH MARKS SIGNIFICANT SHIFT FROM HISTORIC NEO-LIBERAL PROCUREMENT MODEL

Allowing national governments the flexibility to pursue Buy EU policies is a significant shift away from Europe's neo-liberal public procurement directives that were launched in the mid-1990s. These focused on awarding contracts to the most economically advantageous bid (typically the cheapest).

Since then, Europe's procurement rules have been paying greater attention to environmental and social factors in the awarding of public contracts, with the question of whether member states were entitled or even obliged to exclude non-EU bidders from public tenders only really becoming a relevant concern when trade tensions with China grew in the 2020s.

Against this backdrop, the Court of Justice of the European Union (ECJ) clarified that national governments were principally allowed to exclude third-country bidders simply because they were from outside the EU. This approach is likely to be reinforced with the forthcoming recast of the EU's public procurement directives.

EMERGING LAW AT MEMBER STATE LEVEL IS TESTING LIMITS OF LOCAL PROCUREMENT FOCUS

Defense procurement in the EU already operates under a separate directive that affords member states greater flexibility to exclude foreign bidders, and there is more legislation emerging at national level (such as Germany's Armed Forces Planning and Procurement Acceleration Act) that is adding detail and testing the limits of the concept.

At the same time, member state governments are able to act independently of all EU rules (e.g., procurement, state aid, merger control etc.) by invoking national security interests under Article 346 of the Treaty on the Functioning of the European Union (TFEU). This exemption enables them to award defense contracts to local champions or technologically leading third-country suppliers, such as those from the U.S.

The dilemma from an EU perspective has been that, while there has been de facto freedom for member states to exclude non-EU suppliers, goods, components or services from defense procurement processes, this has in fact led to a nationally fragmented rather than integrated EU defense market. Indeed, a number of member states are now more or less dependent on non-EU suppliers that may not be as reliable as they have been considered in the past.

WHAT DOES THE EU'S SAFE PROGRAM MEAN FOR PRIVATE CAPITAL PROVIDERS?

SAFE provides EU funding to member state governments to boost military investment. The program is designed to support joint procurement of defense equipment and onshore the highest-value elements of the defense supply chain by promoting EU control over defense contractors and subcontractors. As outlined above, the Buy EU principle it supports is set to be a central feature of Europe's reformed procurement framework and the proposed Industrial Accelerator Act, among other things.

The European Defense Fund (2021), the Act in Support of Ammunition Production (ASAP, 2023), the European Defence Industry Reinforcement Through Common Procurement Act (EDIRPA, also 2023), and the proposed European Defence Industry Program (EDIP, 2025) similarly include eligibility criteria that function as European preference requirements.

For financial sponsors, this "buy local" focus must be taken into account when considering investments in the EU defense sector. It will play a significant role in determining which companies can access procurement opportunities and where value will accrue across the European supply chain. But the EU's regulatory frameworks must also be scrutinized closely, with more opportunities available for third-country businesses than might first be apparent, including under SAFE.

IMPORTANT EXEMPTIONS OFFER OPPORTUNITIES FOR NON-EU SUPPLIERS

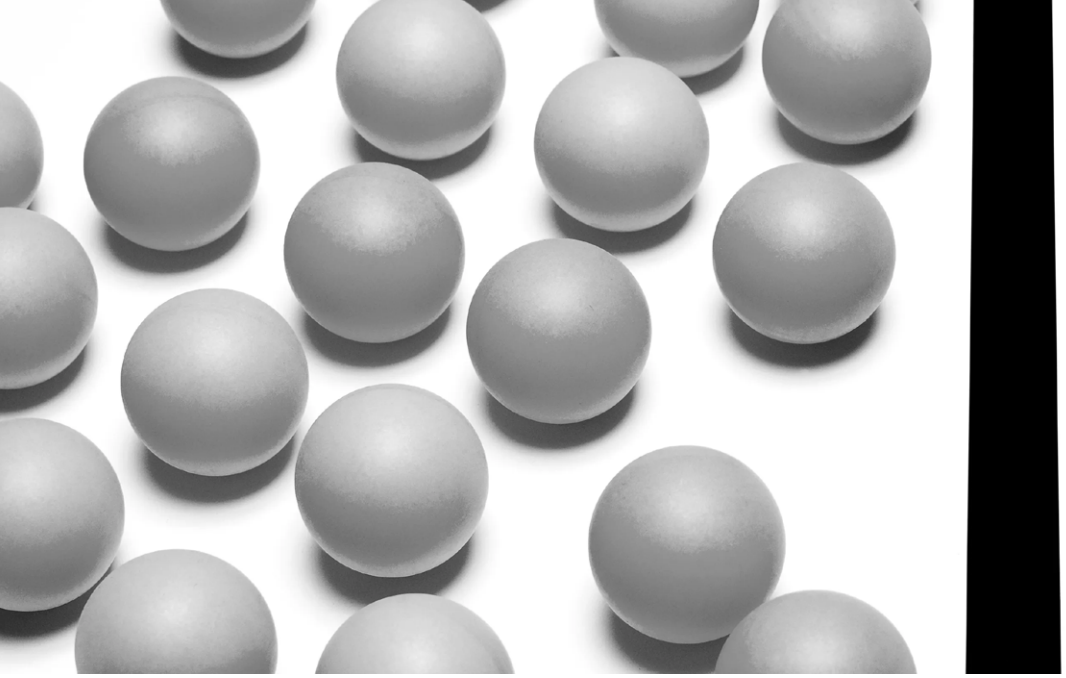
SAFE is the most significant EU funding instrument in the defense arena. It provides up to EUR150bn in low-cost, long-term loans for military investment.

On its face, SAFE is designed to support joint procurement of defense equipment between EU member states; Ukraine; countries in the European Economic Area (EEA) and European Free Trade Area (EFTA); EU candidate and potential candidate nations; and states that have signed security and defense partnerships with the EU (e.g., Canada, India, Japan, South Korea and the UK). Since its launch in May 2025, 18 countries have been approved to receive SAFE funds.

No more than 35% of the value of a contract funded under SAFE can originate from entities that are established or have their executive management outside the EU, EEA, EFTA or Ukraine. In practice, however, the eligibility rules contain important exemptions that open the door wider.

- A foreign-located-or-controlled subcontractor that has a relationship with an in-territory contractor which predates SAFE can participate in defense contracts up to 35% of the contract value outside the joint procurement context.
- Subcontractors located within the defined territories but controlled from outside can also participate above the 35% limit if they have passed an FDI screening or have security guarantees in place with the government of an approved jurisdiction.
- As a result, there may be more SAFE-eligible companies for private capital firms to invest in than a first reading of SAFE would suggest.

However, governance structures are critical. If a foreign parent exercises board-level control over an in-territory subsidiary, that subsidiary may lose SAFE eligibility absent FDI screening approval. Investors must therefore either carefully structure the governance of their portfolio companies or opt for debt finance instruments, minority participations or preferential non-voting shares, to preserve eligibility.



Export controls and sanctions shape boundaries of defense deal-making

Export control regimes define not only how defense technologies move across borders, but who can invest in them and on what terms. With extraterritorial reach, strict licensing requirements and the potential for severe civil and criminal penalties, compliance is fundamental to a target's viability. Here we explore how detailed diligence and careful deal structuring are essential to manage risks.

BY KEN RIVLIN, MATT TOWNSEND, CATHERINE HEIN, ARTHUR SAUZAY, JAMES FORD, LUC LAMBLIN AND LARA FONTAINE

SUMMARY

- Export controls apply to military and dual-use goods, services, and technology.
- Investors must conduct detailed due diligence and carefully structure deals to manage export control risks, which can arise without physical technology transfers.
- Evaluating a target's historic and ongoing compliance with export control regulations, including licensing and program maturity, is essential and should be performed alongside FDI due diligence.

Export controls govern the export of military and dual-use goods, services and technology (g/s/t). Investing in the defense sector presents a particular set of export control challenges, including navigating trade controls restrictions and having to comply with relevant FDI regimes (an issue we explore in more detail here).

Compliance with applicable export control regulations is at the core of a defense company's license to operate; a failure to adhere to export controls could result in civil and criminal penalties both for companies and individuals, as well as reputational damage.

DILIGENCE SHOULD CLOSELY SCRUTINIZE A TARGET'S DEALINGS IN CONTROLLED GOODS AND TECHNOLOGIES

When diligencing targets, investors should closely scrutinize a target's dealings in controlled goods and technologies, including whether the export of controlled items has been properly licensed, who has access to controlled items within the organization, and the maturity of the target's export compliance program.

Depending on the findings of the DD process and the risk profile of the target, it may be appropriate to include in the deal agreement tailored export control representations, warranties and/or indemnities to address export control risks connected with the proposed acquisition. However, it should also be noted that export control risks may not be covered under certain W&I policies. Post-acquisition, an investor may consider requiring a target company to conduct a review of the effectiveness of its export compliance program.

"DEEMED EXPORT" RULE CREATES RISK WITHOUT PHYSICAL TECHNOLOGY TRANSFERS

It is also important to understand that in some cases, export controls can be triggered even where goods are not transferred across borders. In the U.S., the "deemed export" rule can apply to information-sharing with foreign nationals involved in an investment.

A deemed export occurs when controlled technology, technical data or software is released to a foreign national within the United States. This is treated as an export to that person's country of origin, even though the relevant items do not physically leave the country.

As a broader point, U.S. export control jurisdiction has extensive extraterritorial reach. Military g/s/t are generally governed by the International Traffic in Arms Regulations (ITAR). If an item incorporates any other item that is subject to ITAR, that "taints" the product such that it also becomes subject to ITAR, regardless of how small the other item is or where the original item is manufactured.

Additionally, any item that is "U.S. origin" is subject to the Export Administration Regulations (EAR). This includes both dual-use items and EAR99 items (which are U.S. origin, but not dual-use). Any item that is subject to the EAR remains subject to U.S. export control jurisdiction going forwards, including where that item is re-exported from one non-U.S. country to another.

CFIUS USES EXPORT CONTROL CLASSIFICATIONS TO DETERMINE FILING OBLIGATIONS

The Committee on Foreign Investment in the United States (CFIUS) also uses export control classifications to determine filing obligations, treating the investment itself as a national security-relevant transaction even absent any actual export. Mandatory notifications are necessary when a foreign investor acquires an interest in a U.S. business involved in critical technologies, critical infrastructure or sensitive data (so-called "TID" businesses) and a U.S. government license would hypothetically be required to export the relevant TID items to the foreign investor.

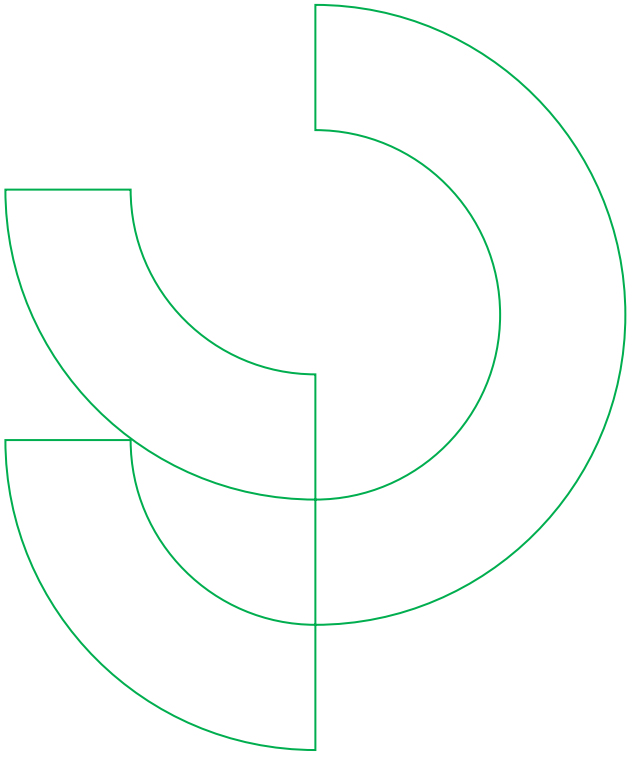
The UK has a similar mandatory notification requirement to the Investment Security Unit (ISU) under the National Security and Investment Act (NSIA) in connection with certain acquisitions of target companies that hold military and/or dual-use assets, among other things. (We explore the dynamics surrounding foreign investments in the defense sector in more detail here).

Against this backdrop, investors must evaluate a target's historic compliance with applicable export control regulations as well as any future licensing requirements. This includes understanding the robustness of the target's existing export compliance program, establishing the target's dealings with military and dual-use goods and technologies, and assessing whether the target has obtained all necessary licenses and registrations to deal in such goods and technologies. This analysis should take place alongside FDI due diligence.

SANCTIONS COMPLIANCE REQUIRES CAREFUL CHECKS

Sanctions compliance is another important consideration. Defense companies frequently operate in geopolitically sensitive markets and may have historical trading relationships with countries or entities that have since become subject to sanctions.

Arms embargoes (which prohibit or restrict the sale, supply or transfer of arms and related materials to specified countries or non-state actors) are a prominent feature of sanctions regimes. In addition, many sanctions programs include sectoral measures specifically targeting military and defense activities (for example, the EU and UK sanctions regimes targeting Russia's defense sector). Investors should therefore assess whether a target company has adequate sanctions compliance programs in place covering OFAC (U.S.), UK, EU and other international sanctions regimes.



Investors pay close attention to unique treatment of IP in defense contracts

Intellectual property (IP) is critical to the value proposition of defense and dual-use businesses, but government procurement models can significantly shape how that value is realised. Here we explore how broad state rights over foreground and background IP, combined with evolving approaches to incentivise private innovation, create a complex negotiation landscape for investors.

BY RAVI DE FONSEKA AND NIGEL PARKER

SUMMARY

- The treatment of IP in defense contracts can impact investors and innovators by diluting potential commercial returns.
- Regulations like the U.S. Defense Federal Acquisition Regulation Supplement (DFARS) and policies prescribed by governments on defense contracting, such as the UK Ministry of Defence's "DEFCONS" (Defence Conditions), generally allow governments broad rights of use with respect to both foreground and background IP developed by contractors, and potentially the ability to on-license that IP to competitors of the contractor.
- Governments may also exercise compulsory licenses over IP deemed critical to national security.
- Contractors need to manage IP policy and strategy across multiple legal and contracting frameworks in the various countries in which they operate, which will have different implications for ownership and control of IP rights. These factors can lead some tech companies, small/medium-sized entities (SMEs) and investors to avoid participation in the defense sector altogether.
- However recent reforms aim to incentivize innovation and encourage competition by providing greater flexibility and giving defense contractors more leverage in negotiations.

For investors and acquirers pursuing targets specializing in the development and supply of defense and dual-use technologies, understanding the dynamics that surround ownership and control of IP (including rights in technical data and knowhow) within the defense sector is vital. Defense procurement frameworks often allocate IP ownership and usage rights in ways that can materially impact long-term commercial upside if not managed carefully.

As the nature of battlefield technology evolves from heavy engineering to weapons systems whose efficacy is defined by software, AI and robotics, how the interests of governments to protect national security are balanced against innovators' need to benefit from their investment in R&D has emerged as an important challenge.

IP ARRANGEMENTS ARE LEGACY OF HARDWARE-DRIVEN DEFENSE ERA

Defense contracts typically give governments broad rights over IP created by contractors (including both background and foreground IP); a legacy of the hardware-dominated era where R&D was largely the preserve of prime manufacturers developing equipment that was funded entirely by its government customer.

As well as funding, traditional approaches have also been informed by security concerns, a desire to protect any background IP contributed by the government customer, the need to retain control and flexibility within complex supply chains, and to ensure access to technical developments in the national interest.

In the U.S. for example, the Defense Federal Acquisition Regulation Supplement (DFARS, which we explore in more detail here, gives the U.S. government "Unlimited Rights" (affording rights to use developments for any purposes in programs fully funded by the Department of War) and "Government Purpose Right", affording broad rights to use, modify, reproduce and disclose "government purposes" (including purposes of the U.S. government, foreign states and international defense organizations).

After five years the government purposes limitation falls away and unlimited rights kick in. Once these rights vest, inventions can be shared with anyone for any reason, including the creator's competitors. Similar government purposes rights are a feature of UK defense agreements.

GOVERNMENTS TRADITIONALLY SOUGHT BROAD IP RIGHTS TO PRESERVE OPTIONALITY

Defense contracts and policies also generally give states broad rights over background IP that forms part of a contract deliverable. From a government's perspective, these provisions are necessary to preserve optionality for future defense programs, but in practice they can dilute the economic incentives that underpin private investment in innovation-led defense technologies.

Where a contractor risks losing control of valuable background IP, it needs to be careful what pre-existing technology is utilized in delivering under the contract. To the extent a government acquires different usage rights as between background and foreground IP, the contractor must clearly distinguish between background and foreground technology to avoid background IP being swept up in broader usage rights granted in relation to foreground IP.

Where sensitive technologies or inventions that have been specifically commissioned by a government are concerned, either IP ownership will vest in the government customer, or a broad, perpetual, freely-transferable and royalty-free license will be granted to the government customer.

Contractors will typically bear the contractual burden of securing the same expansive IP rights from their subcontractors and supply chain as they commit to provide to the government customer. Failure to effectively "flow down" these rights can lead to breach of contract. The contractor may be required to identify any restrictions on the government customer's ability to use or disclose background IP.

In scenarios where defense products are developed through cross-border collaborations and joint ventures (an issue we explore in more detail here), these dynamics can create commercial challenges in relation to foreground IP created from innovations contributed to the alliance that are either controlled or owned by a JV party's home state.

In addition, governments will often have statutory rights to exercise compulsory licenses over IP deemed critical to national security under mechanisms such as "Crown Use" powers in the UK and Australia. These rights allow governments (or their contractors) to use IP without the IP owner's permission, usually limited to purposes vital to the national interest (including defense).

NEW APPROACHES EMERGE IN LINE WITH EVOLUTION OF THE SECTOR

As the universe of businesses that comprise the modern defense supply chain has broadened, some states have re-evaluated their IP practices to incentivize greater participation and innovation, and to acknowledge that the R&D programs of this new generation of suppliers may have been entirely funded by the business or its investors.

It is increasingly acknowledged that by allowing contractors greater scope to own foreground IP, this may result in more competitive pricing, encourage delivery of better solutions and potentially provide the possibility for royalty-sharing opportunities foe government contractors (whereby a levy is imposed on further commercial exploitation by the contractor).

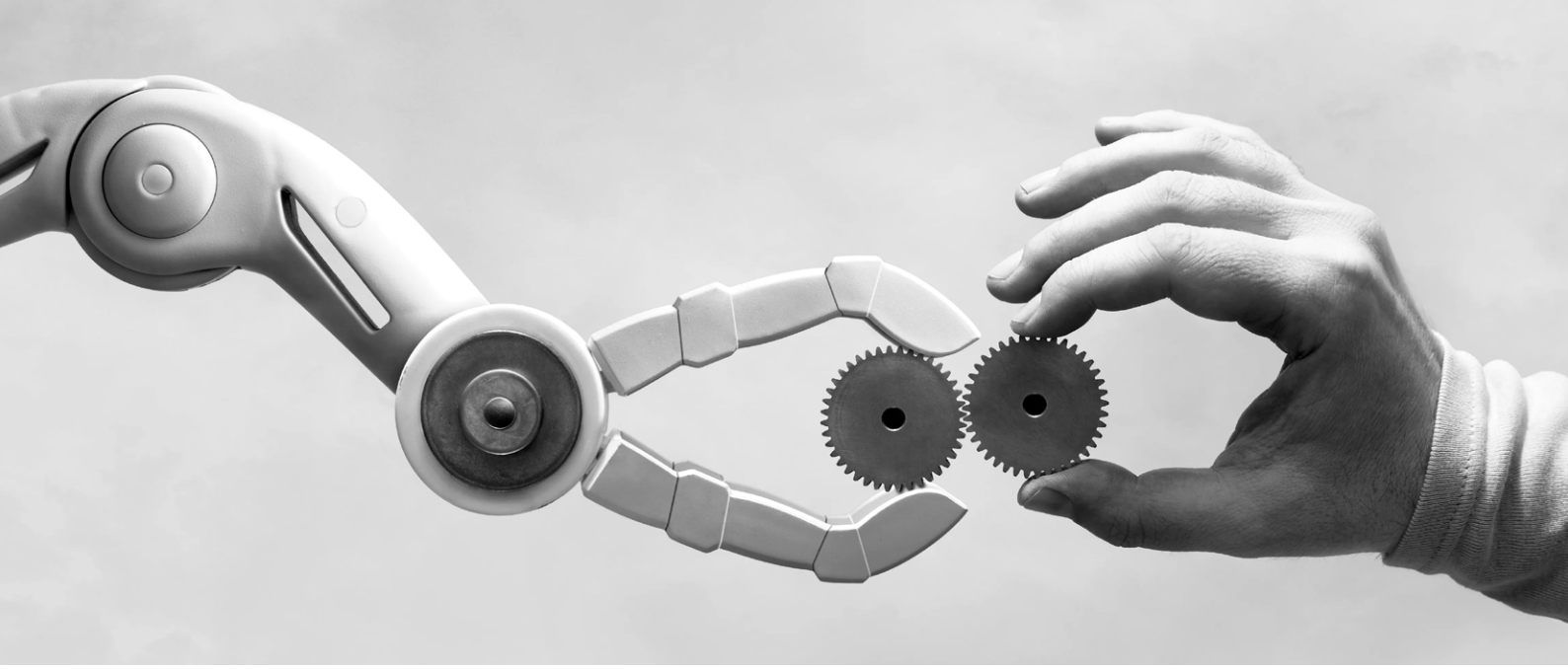
The U.S. government's approach to defense IP has been revised several times in recent years. The DFARS framework has been amended to give contractors more IP rights in certain technology areas, while the DOW can also now use structures such as Cooperative Research and Development Agreements (CRADAs) to create bespoke IP agreements outside of DFARS. This more flexible approach was further reinforced in the 2025 Intellectual Property Guidebook, giving defense suppliers greater leverage in contract negotiations.

In the UK, recent institutional reforms such as the launch of UK Defence Innovation (UKDI), signal a growing recognition that traditional IP models may need to adapt, although how this translates into commercial outcomes remains highly deal-specific.

Data and AI compliance

Compliance with EU legislation such as the AI Act and NIS2 Directive is not required for AI systems developed or used solely for national security or military purposes, consistent with Article 4(2) TFEU. However, the exemption falls away when the technology is placed on the commercial market or deployed for mixed civilian and military purposes.

By contrast, data protection rules, including GDPR, do apply to defense innovations. National security exemptions (such as Section 26 of the UK Data Protection Act 2018) are qualified, not automatic, and require case-by-case demonstration that compliance would negatively affect national security.



New joint ventures accelerate evolution of battlefield technology

Joint ventures have become a key feature of the rapidly evolving defense landscape. Flexible structures that often prioritize operational outcomes over technology ownership are enabling collaborations between primes, disruptors and financial sponsors. However, export controls, FDI rules and long investment horizons make careful structuring essential.

BY ALAIN DERMARKAR, ROMAIN DAMBRE AND BENJAMIN CRAWFORD

SUMMARY

- Modern warfare's shift toward technology-driven and autonomous systems is accelerating JV formation, with partners combining complementary strengths like intellectual property, manufacturing, and supply chains.
- The defense supply chain is now characterized by diverse partnerships, such as disruptor-disruptor and disruptor-prime relationships alongside traditional prime-prime alliances.
- Many new JVs prioritize operational advantage over ownership, featuring light governance and flexible structures designed for future exits and regional expansions.
- Export controls, foreign investment screening, and local partnering requirements are central to structuring cross-border defense JVs, directly impacting equity arrangements and operational control.

Defense companies are forming joint ventures at a rate that would have been difficult to imagine even five years ago, as the focus of modern warfare moves from heavy engineering to tech-enabled, often autonomous systems.

Advanced engines, AI-enabled drones and next-generation sensors demand capital commitments and technical capabilities that no single firm can marshal alone. One partner may contribute intellectual property in the form of software or AI technology, while the other brings manufacturing capability, supply chains, government certifications and customer access.

For decades the archetypal defense JV involved partnerships between defense primes, for example the Lockheed Martin/Raytheon Javelin missile program. That model still exists, but the landscape has shifted in response to demand surges driven by the wars in Ukraine and the Middle East, NATO rearmament commitments and the rise of defense-tech disruptors.

DIVERSE PARTNERSHIPS EMERGE THAT ARE DRIVING INNOVATION

Recent deal activity illustrates this diversity. The partnership between EDGE and Anduril combines the UAE state-backed defense group's manufacturing strength and regional market access with the U.S. autonomy provider's technology. The JV launched with an anchor customer and is targeting full-rate production by the end of 2028.

The AIRO Group–Bullet alliance brings battlefield-tested Ukrainian interceptor drone technology into U.S. manufacturing and NATO procurement channels, functioning as a conduit between frontline innovation and U.S. contracting. Meanwhile, the Raytheon-Rafael JV is a more traditional prime-to-prime model founded on a major government contract, in this case a USD1.25bn deal to supply Israel with Iron Dome interceptors.

Alongside formal equity joint ventures, a spectrum of strategic alliances is also emerging. Disruptor-disruptor partnerships, for example Anduril/OpenAI, Shield AI/Palantir, EagleNXT/ThirdEye Systems and Lantronix/Unusual Machines combine AI, autonomy and data capabilities.

Elsewhere, disruptor-prime partnerships such as Anduril's deal with Rheinmetall allow primes to inject momentum into their legacy platforms while giving disruptors the procurement credibility and manufacturing scale they need to compete for larger contracts. Prime-prime alliances such as Airbus/Northrop Grumman address production bottlenecks and share risk across jurisdictions.

ARRANGEMENTS ARE OFTEN GOVERNANCE-LIGHT

What distinguishes many of these arrangements is the fact that they prioritize operational advantage over ownership. Governance tends to be light, while alignment between parties comes through customer pull and shared roadmaps rather than board mechanics. Here, structures are deliberately designed to preserve optionality for future exits, whether buy-outs, acquisitions or regional spin-outs.

Export controls and foreign investment screening lie at the heart of every cross-border defense JV. U.S. ITAR and EAR rules, alongside other jurisdictions' export controls (an issue we explore in more detail here), govern any transfer of technology, while CFIUS and broader FDI screening regimes (which we explore in more detail here) will apply wherever a foreign entity takes a significant stake in a JV with a non-domestic partner. Many countries also impose local partnering requirements on such arrangements.

In practice, these dynamics shape the way JVs are structured. EDGE Group's joint ventures, for example, feature 49:51 equity stakes whereby EDGE controls the alliance in the UAE but takes a minority position in the partner's home jurisdiction.

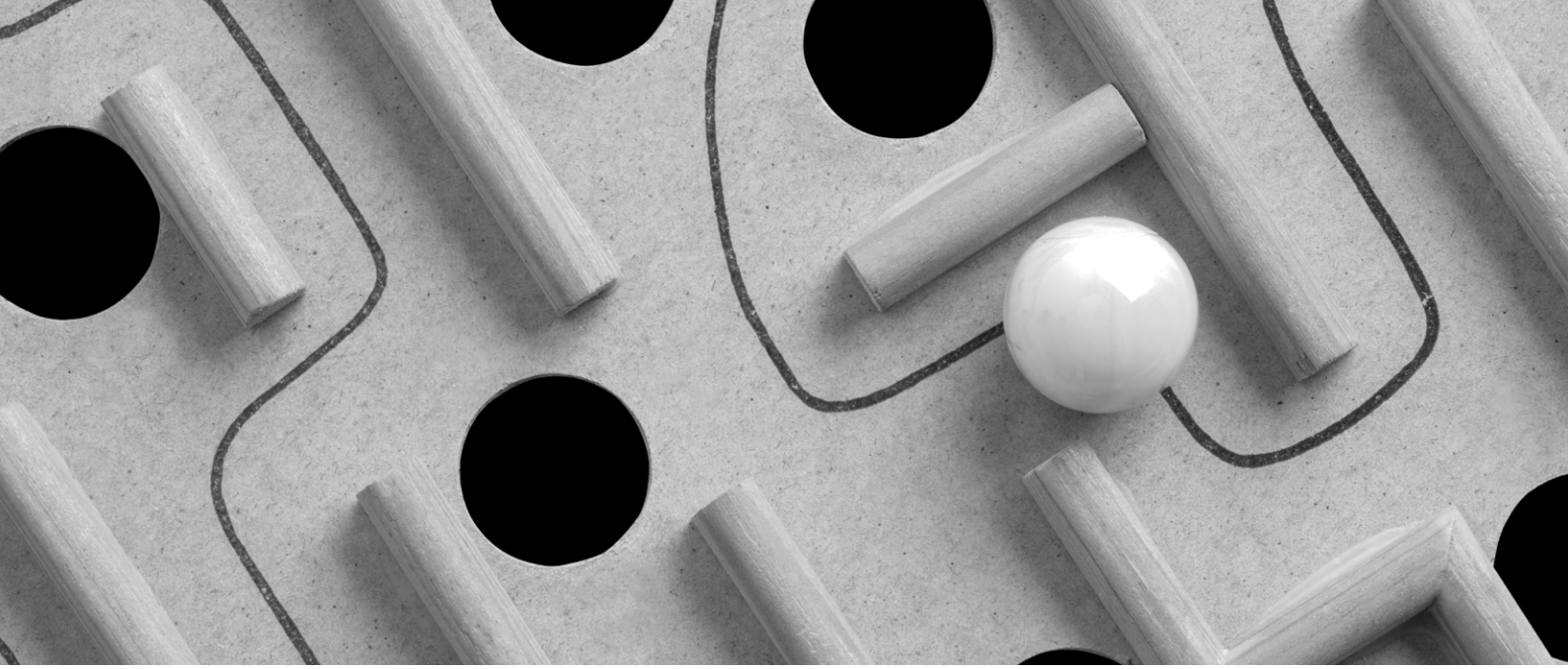
INNOVATIVE STRUCTURING SOLUTIONS HELP MITIGATE COMMERCIAL RISKS

Equity commitments are staggered in tranches aligned with technology-transfer milestones, and termination rights are baked in at each phase. The latter point (i.e., how to unwind an alliance if the geopolitical or regulatory landscape shifts) is a critical consideration. Resolution mechanisms must be built into the agreement such as call or put rights, clauses that support forced sales to third parties, mandatory listings or measures to convert equity arrangements into arm's-length contractual collaborations.

One creative solution we have seen involves structuring a commercial collaboration agreement alongside the JV to extract value contractually rather than through equity. This addresses the challenge that arises when liquidating the JV is impractical because the shares are worth more to one party than the other.

Private capital firms are also increasingly teaming up with primes manufacturers (e.g., Carlyle's deal with Raytheon) to co-invest, share risk and tap into domain expertise. Here it's important that financial sponsors do not rely too heavily on their partner's sectoral expertise and connections, and instead take steps to independently understand the economics of government contracting and the foreign investment landscape.

They also need to get comfortable with the fact that defense JVs often run over many years. This requires patient capital and the ability to adapt as budgets, threats and the geopolitical landscape evolve. Investors must enter the space cognizant that conventional PE hold periods and exit timelines may not apply. Those who approach defense JVs with the right structure, partners and time horizon will be best placed to succeed.



Why defense companies are exposed to litigation risk on multiple fronts

From False Claims Act exposure and DFARS compliance to export controls and human rights claims, defense companies face the threat of litigation from myriad sources. For investors, rigorous diligence and ongoing risk monitoring are critical to preserving value in an increasingly contested legal environment.

BY ADAM SCHWARTZ AND MAEVE HANNA

SUMMARY

- The litigation risk profile of businesses in the defense supply chain is complex.
- In the U.S., the False Claims Act is a major driver of disputes, which are often triggered by contractual ambiguities rather than intentional fraud.
- DFARS regulations impose extensive compliance requirements, making thorough regulatory diligence essential for investors.
- Intellectual property disputes and shifting geopolitical factors, such as U.S. export controls, introduce additional risks, as do human rights-related lawsuits.

Companies in the defense value chain are exposed to the threat of litigation from many angles.

For U.S. defense contractors and their suppliers, the False Claims Act is one of the primary drivers of litigation. The Act permits the federal government to recover triple the value of any false claim, and also has a provision that allows private whistleblowers to initiate cases and share in recoveries. In 2025 alone, the government recovered USD5bn in False Claims fines.

What makes the False Claims Act particularly challenging for investors is that claims frequently arise not from deliberate fraud by contractors but from the ambiguities inherent in government contracts, such as allegations that a company has failed to meet its cybersecurity obligations, or that a component's performance falls marginally short of contractual standards (provided that the alleged non-compliance is material to the agreement).

FLOW-DOWN REQUIREMENTS IMPOSE EXTENSIVE DFARS COMPLIANCE OBLIGATIONS

Layered on top of this is the burden applied by the Defense Federal Acquisition Regulation Supplement (DFARS—a supplement to the Federal Acquisition Regulations (FAR)), a set of obligations that apply to Department of War (DOW) contractors that handle sensitive information or provide certain defense components. Through flow-down requirements, government contractors are required to include DFARS clauses in their subcontracts, making the regulations binding for businesses across the defense supply chain.

While the title "supplement" might suggest a relatively limited set of rules, in reality DFARS runs to several thousand pages. U.S. defense contracts typically incorporate DFARS obligations by reference, often condensing this extensive body of requirements into a single page of listed provisions. For private capital firms conducting due diligence on defense-related targets (including those outside America that rely on U.S. components and are therefore also subject to DFARS) assessing whether the business is in full compliance is a significant challenge. Even inadvertent non-compliance can expose investors to substantial litigation risk, making specialist regulatory diligence an essential component of any defense sector transaction.

Intellectual property rights present a further source of litigation risk. Governments across the world will look to assert control over technologies they deem critical to national security (an issue we explore in more detail here), and when they do, it often leads innovators to sue to protect their inventions.

EXPORT CONTROLS CREATE CASCADING RISKS ACROSS INTERNATIONAL SUPPLY CHAINS

Geopolitical shifts are another driver. U.S. export controls create cascading risks through international supply chains. U.S. primes will typically provide in their contracts that if the U.S. government changes its export control position, the contract will terminate with no mitigation available.

For investors acquiring companies dependent on U.S. suppliers, the risk of contract termination or delivery delays due to export control changes is a material due diligence issue. European defense contracts (many of which rely on U.S.-manufactured components) increasingly include substantial contractual penalties for late delivery, and the recent surge in European defense orders is expected to generate significant disputes as companies struggle to meet delivery schedules, whether or not export controls are a factor in non-performance.

ESG FRAMEWORKS AMPLIFY REPUTATIONAL THREATS

Defense investments also carry inherent reputational sensitivities, amplified by ESG frameworks and institutional investors' exclusionary policies. Against this backdrop we are seeing an emerging body of litigation grounded in human rights law, in which defendants, including victims of armed conflict and non-governmental organizations, seek to hold defense companies liable for alleged complicity in human rights abuses committed using their products.

In the United States, Yemeni civilians have sued U.S. primes over weapons which were subsequently deployed in attacks on the country by the Saudi-led coalition. Lawsuits have also been filed against U.S. chipmakers over the use of their products in Russian weapons allegedly used to target civilian neighborhoods, schools and evacuation routes.

In the UK, the key cases that have come before the courts involve challenges to government export licensing decisions through judicial review rather than commercial lawsuits, as illustrated by the Campaign Against Arms Trade's challenge over Saudi Arabia and the Al-Haq/GLAN case involving Israel.

CONTROVERSIAL USES CASES CREATE EXPOSURE

Involvement in a value chain can also generate significant publicity and cause companies to become the target of pressure or litigation from campaign groups. This is relevant not only when investing in prime contractors, but also for subcontractors and dual-use businesses. Investors need to understand that reputational risk can crystallize through litigation not directly aimed at them, but in which their name or products become publicly associated with a controversial use case.

Investors may be able to reduce their exposure by favoring companies with comprehensive end-user monitoring programs, clear policies on sales to high-risk jurisdictions and demonstrated adherence to international humanitarian law standards. Assessing insurance coverage for product liability claims and monitoring legislative developments in corporate accountability is also prudent.

The litigation landscape that surrounds the defense sector is complex, and in many respects unique. The investors best placed to succeed are those that understand the multifaceted sources of risk, conduct sophisticated due diligence of targets prior to committing capital, and continue to monitor potential threats throughout their asset hold periods.

Private capital firms target emerging opportunities in space sector

Space is rapidly emerging as a core domain of defense capability, attracting private capital as manufacturing models industrialize and costs fall. Here we explore how investors are backing assets that underpin critical functions such as intelligence and communications, but must navigate complex regulatory regimes, procurement constraints and technology risk.

BY ARTHUR SAUZAY

SUMMARY

- Private capital is increasingly investing in the space sector, where the rise of reusable rockets and vertical integration has disrupted traditional, government-led space manufacturing models.
- Space infrastructure, especially satellites, is now vital to military operations across domains, leading to increased government focus on sovereign assets.
- Recent years have seen large private equity investments in space-related companies as well as some notable failures, highlighting the need for thorough due diligence on scalability, management, and revenue stability.
- Space investments face complex regulatory and procurement challenges, including FDI screening and compliance with export control regimes.

Space assets are attracting significant interest from venture capital (VC) as well as private equity investors.

Two primary developments underlie this shift. The first is the industrialization of space manufacturing. Historically, spacecraft were capital-intensive, often single-use, government-commissioned systems.

That model has been disrupted by companies such as SpaceX, which has imported manufacturing methods used in the automotive industry (e.g., in-house production and vertical integration, which provide significant efficiency benefits with fewer dependencies) to develop reusable rockets. By focusing on returning the most valuable sections of its spacecraft to Earth rather than abandoning them in orbit, SpaceX has dramatically reduced the cost of launch.

Businesses are also creating new markets in space, such as low earth orbit (LEO) internet, which operates using satellites that fly much closer to the earth than traditional geostationary systems. LEO satellites can deliver fiber-like connection speeds and serve needs that require lower latencies such as gaming and in-flight Wi-Fi, generating billions of dollars in revenues for operators. SpaceX's IPO prospectus points to potential future commercial opportunities, including orbital data centers powered by solar energy.

SPACE INFRASTRUCTURE IS INCREASINGLY ESSENTIAL TO MILITARY STRENGTH

The second is the importance of space infrastructure to modern defense capabilities. Satellites are integral to air, land, sea, and cyber defenses, underpinning real-time intelligence, secure communications, navigational support and early warning systems.

In 2023 more than 100 defense and dual-use satellites were launched by 14 nations, a 40% increase year-on-year. Amid the focus by governments on self-reliance in a more volatile geopolitical environment, sovereign space assets are seen as essential. The sector is also pulling in prime manufacturers: Rheinmetall has entered into a joint venture with Finnish satellite manufacturer ICEYE, while Safran is also growing its space program. For investors, these moves are a further signal of the space sector's growing maturity.

Space remains a largely state-funded sector, with research putting total government spending in 2024 at around USD135bn globally. Even Starlink relies heavily on contracts with NASA and the U.S. Department of War.

With that said, the patterns of private capital investment are changing. VC funding has long been central to early-stage innovators, and increasingly significant amounts of new money are flowing into the sector (ICEYE's recent EUR450m primary Series F round is a prime example). We are also seeing more big-ticket private equity investments; KKR acquired a 28% stake in the German satellite manufacturer OHB in 2024, and is now reportedly pursuing a share sale with OHB's majority owner.

INVESTORS MUST SEPARATE HYPE FROM SUBSTANCE

Investors targeting space-related assets have several important issues to consider.

When assessing targets, it's vital to separate substance from noise. The sector has seen some significant failures in recent years, including several unsuccessful SPAC deals and the collapse of startups such as UK-based rocket manufacturer Orbex. Rigorous diligence on the scalability of innovations, the capability of management teams and the robustness of contracts and revenue pipelines is therefore essential.

Space investments are also complex from a regulatory perspective. Transactions are subject to FDI screening processes in nearly every jurisdiction, with space assets (both satellites and ground systems) classified as critical infrastructure in many countries. These include the UK, Australia and larger EU member states such as Germany, while the Space Infrastructure Act, introduced to Congress in 2025, proposes doing the same in the U.S. Critical infrastructure transactions often require mandatory filings, are triggered at lower investment thresholds, involve heightened regulatory scrutiny and are more likely to be subject to risk mitigation.

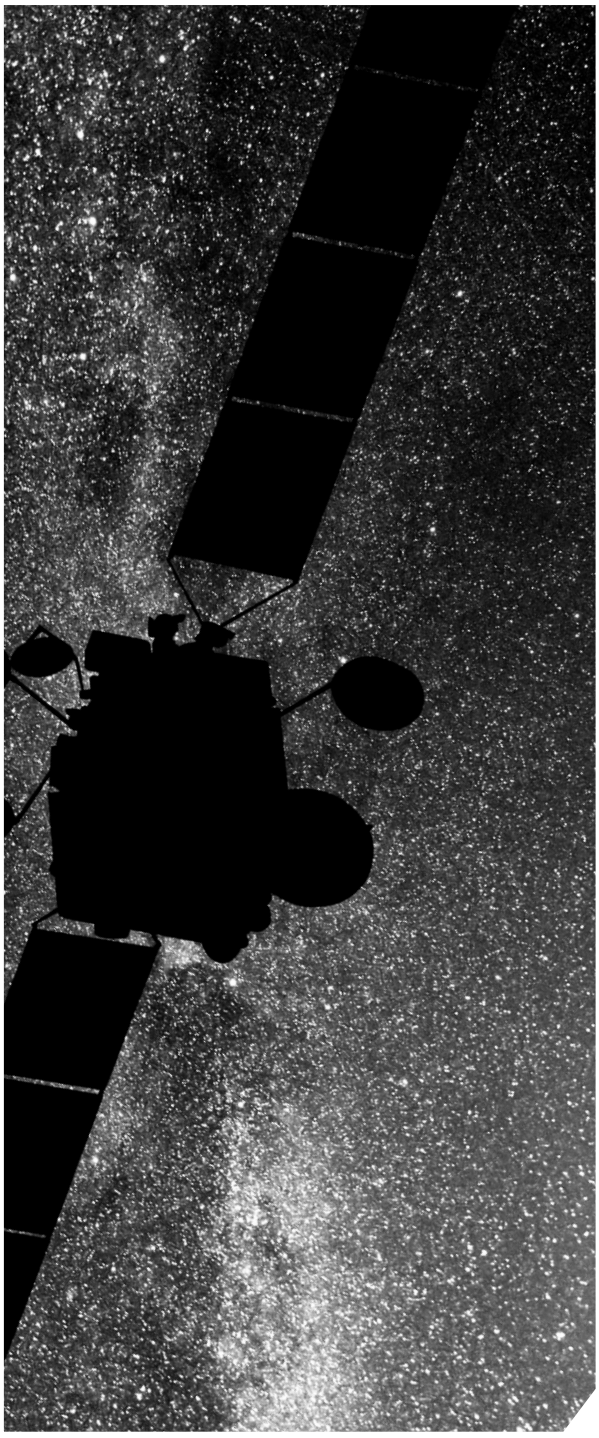
As the sector evolves, new issues are emerging: satellite frequencies are becoming increasingly scarce, while the risk of collisions—which raise the threat of potential litigation down the line—is trending upwards as the number of satellites grows. Earth orbit is also an increasingly contested zone, with military activity and risks rising as a result.

SPACE PROCUREMENT PROCESSES ARE COMPLEX

Alongside these dynamics, space businesses may be exposed to complex government procurement processes. In Europe for example, the IRIS² sovereign satellite constellation program is governed by a dedicated procurement regulation that imposes limits on non-EU-controlled entities participating as major contractors.

In addition, many space assets appear on dual-use technology lists, which could bring them into scope of regimes such as the U.S. International Traffic in Arms Regulation (ITAR). ITAR controls the manufacture, sale and distribution of physical weapons, defense services, software and technical data, with government licenses needed to export in-scope items to foreign persons. Financial sponsors must thoroughly diligence a target's ITAR compliance procedures, although the regulation itself can pose challenges to diligence processes that require clean teams limited to U.S. persons. (We explore the ITAR regime in more detail here).

Beyond these frameworks, entering the sector also exposes parties to space law, under which specific authorizations are required to launch and operate spacecraft, and operators are subject to strict liability regimes. Financial sponsors should take care to ensure their contracts are structured so they can own individual assets without assuming responsibility for their operation, or behavior, in orbit, which carries significant financial and litigation risks.



Venture capital reshapes how defense innovation is funded and developed

Venture capital is transforming the defense ecosystem and accelerating the shift toward software-led, dual-use technologies with rapid deployment cycles. Here we explore how investors are deploying capital earlier and across the full growth lifecycle, and how political risk demands a more nuanced, thesis-driven approach to value creation.

BY WILL SAMENGO-TURNER AND ADAM SCHWARTZ

SUMMARY

- Venture capital has become a major driver of defense innovation, with investment in 2025 nearly doubling to USD49bn.
- Investor interest is shifting from traditional hardware to software, AI, robotics, drones and cybersecurity, with Ukraine serving as a proving ground for new solutions.
- In the U.S., VC and private equity funds often target small businesses qualified under the SBA 8(a) program, which provides preferential access to defense contracts.
- Private capital strategies include minority control deals and joint ventures, reflecting increased involvement of PE firms with VC arms throughout the growth lifecycle.
- Defense innovators' cap tables feature diverse governance arrangements, with a mix of active and passive investors.

Venture capital (VC) is now a significant force in the defense supply chain. In 2025, USD49bn of venture capital investment flowed into defense and dual-use assets, almost double the total for the previous 12 months.

The structural shift in the sector from hardware-oriented munitions to software, AI- and data-driven technologies has powered investor interest. Robotics, drones, cybersecurity and autonomous systems offer a range of opportunities to enter a sector experiencing historic levels of investment. Ukraine has served as a testing ground for these cutting-edge innovations, while their dual-use potential offers a broader universe of potential buyers for fund managers focused on their exit path. However political risk remains a live issue for investors, as Anthropic's ongoing dispute with the U.S. Department of War demonstrates.

FINANCIAL SPONSORS TARGET EARLY INVESTMENT IN BUSINESSES PRIMED FOR ACQUISITIONS

In the United States, many VC and private equity funds frequently target businesses that are qualified small business entities under the U.S. Small Business Administration (SBA) 8(a) Business Development Program, a designation that gives them preferential access to defense contracts.

U.S. prime manufacturers are given certain set-asides in their contracts to use 8(a) suppliers, and once these businesses grow to the point where they are no longer classed as legally "small", primes will often look to acquire them. For financial sponsors, investing early in these companies gives a clear route to liquidity.

These strategies echo the early internet and social media era, when VC firms targeted founder-led startups that were positioning themselves for a buyout by one of the U.S. tech giants. Forming joint ventures with primes, or accepting minority investments carrying acquisition rights, offer alternative routes for private capital investors to de-risk their exit paths, although these approaches may also compress valuations.

MINORITY CONTROL DEALS ON THE RISE

One of the more notable recent trends we have seen has been the growth of minority control deals, whereby early-stage private capital investors acquire between 20% and 30% of a company's share capital but also negotiate veto rights and other governance controls that more closely resemble controlling investments.

This reflects the rising number of PE firms with VC arms that are investing across the growth lifecycle. The same firms that support seed or series A financing rounds will continue deploying through to the pre-IPO phase, often investing a round or two before the typical PE entry point.

Other private capital investors, particularly sovereign wealth funds, provided they can navigate potential FDI restrictions (an issue we explore in more detail here), remain passive. The spectrum of governance arrangements among defense innovators' cap tables is therefore unusually wide.

As with other VC-driven industries, for every Anduril or Helsing there are many businesses that fail to reach their potential. But the risks in defense investments are arguably greater than in many other sectors given that once a new capability appears on the battlefield, efforts will immediately begin to neutralize it.

As a result, innovations may have short lifespans, and can go from viable to obsolete almost overnight. For this reason, experienced defense investors invariably look not for the latest system to gain adoption on the front line, but for the businesses developing ways to counter it.

For more information, please get in touch with your usual A&O Shearman contact.

Global presence

A&O Shearman is an international legal practice with nearly 4,000 lawyers, including some 750 partners, working in 29 countries worldwide. A current list of A&O Shearman offices is available at aoshearman.com/en/global-coverage.

A&O Shearman means Allen Overy Shearman Sterling LLP and/or its affiliated undertakings. Allen Overy Shearman Sterling LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen Overy Shearman Sterling (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen Overy Shearman Sterling LLP (SRA number 401323) and Allen Overy Shearman Sterling (Holdings) Limited (SRA number 557139) are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen Overy Shearman Sterling LLP or a director of Allen Overy Shearman Sterling (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen Overy Shearman Sterling LLP's affiliated undertakings. A list of the members of Allen Overy Shearman Sterling LLP and of the non-members who are designated as partners, and a list of the directors of Allen Overy Shearman Sterling (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

A&O Shearman was formed on 1 May 2024 by the combination of Shearman & Sterling LLP and Allen & Overy LLP and their respective affiliates (the legacy firms). This content may include material generated and matters undertaken by one or more of the legacy firms rather than A&O Shearman.

aoshearman.com

GB

CDD-0526-133081-ADD-0626-139693