GLOBSEC
IDEAS SHAPING THE WORLD

GeoTech Center

Public–Private Relationships in European Defence Tech

Noah Sylvia

As Europe watched Ukrainians and Russians deploy hordes of drones to decimate armour and AI-enabled decision cycles to overwhelm enemies, a new buzzword began to define defence capabilities: 'defence tech'. This term is used to refer to the growing importance of modern technology (and technology companies) to modern operations.

By now, Western doctrine of modern warfare has embedded defence tech deeply into their concepts of operation in a style called 'multi-domain operations' (MDO). MDO requires capabilities to be integrated across the military domains to enable synchronised and convergent effects on the battlefield. The war in Ukraine has strengthened the centrality of this doctrine in Western military planning, and especially emphasising the need for relatively inexpensive, iterative, software-defined capabilities that maintain relevance given the rapid pace of battlefield adaptation in Ukraine.[1]

Furthermore, while the Ukrainian armed forces have had success integrating many of their capabilities up to operational level, Western militaries envision their forces as needing a more cohesive, wider-ranging integration, from tactical to enterprise level, especially if they maintain air-power-centric manoeuvre as their preferred style of warfare. Such a task is an ambitious one, requiring European forces to operate at a high-intensity in a sensor- and platform-saturated environment with a contested and congested electromagnetic spectrum, where massive, disaggregated data flows must be integrated and managed to enable joint and combined arms targeting across and deep behind enemy lines.

Every element of this style of warfare requires private sector contractors as suppliers, integrators, iterators, technical consultants, and even operators. The war in Ukraine has further demonstrated how essential commercial actors are to modern military operations.[2] For this reason, modern defence capabilities require an unprecedented level of involvement between the public and private sectors, radically reshaping the dynamics of these relationships.

This article is intended as a briefer for the non-expert policymaker that speaks to the changes in the public-private relationships brought by a new era of defence tech, elucidating the changes in power dynamics, the geopolitical dependencies, sector-wide vulnerabilities, and considerations for modern defence systems integration. Such a discussion is especially relevant given the changing nature of US-Europe relations and the reliance by Europe upon US providers of defence tech capabilities.

Defence Tech

'Defence tech' is a term used to describe the role of novel or emerging technology in the defence sector. This paper defines companies in 'defence tech' as those that sell products or services to the defence sector—either directly or indirectly—that include the following areas of advanced technology: advanced materials, robots and autonomy, space, digital technologies (e.g., cybersecurity, networks and connectivity, data processing, hosting, etc.), energy, CUAS, simulation, and advanced sensing. Many of these technologies are dual-use, with innovations brought between the defence and civilian sectors. The insights in this paper stem primarily from research and experience related to those companies which support C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance) functions.

Relationship with civilian sectors

Companies in defence tech are best understood through further differentiation into two broad categories: (1) technology companies selling into the defence sector and (2) defence tech companies.

Civilian technology companies are companies that were created to sell to the civilian sector, which comprise the majority of their revenue. Examples include Amazon Web Services (AWS), Cisco, Alphabet (Google), IBM, Microsoft, and Oracle. Due to a number of factors described in greater depth below, civilian technology companies have been providing an increasing quantity of products and services to the defence sector for around 15 years. A significant proportion, if not a majority, of the digital infrastructure for the defence sector is provided by civilian technology companies.

1 Further reading on software-defined capabilities and the 'cheap mass' debate include Bundesministeriums der Verteidigung (BMVg), 'Software Defined Defence Position Paper from BDSV, BDLI, Bitkom and BMVg', October 2023, **https://www.bdsv.eu/themen/cyber-it.html?file=files/meldungen/2023/11/GK4-EK1_Positionspapier%20SDD_ENG.pdf**; Sidharth Kaushal and Paul O'Neill, 'The Role of Dissimilar Rearmament in Allied Deterrence', Whitehall Papers, 102(1), 2024, **https://www.tandfonline.com/toc/rwhi20/102/1**.

2 Emily Bienvenue et al., 'Private Tech Companies, the State, and the New Character of War', Carnegie Endowment, 01 December 2025, **https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies?lang=en**; Emma Schroeder, 'Building the digital front line: Understanding big tech decision-making in Ukraine', Atlantic Council, 15 November 2025, **https://www.atlanticcouncil.org/in-depth-research-reports/report/building-the-digital-front-line/**.

Defence's Civilian Backbone: The defence sector's digital infrastructure relies heavily on civilian technology firms.

However, while these companies often service contracts worth billions, the scale of these companies means that defence revenue typically provides a mere fraction of civilian technology companies' revenue.

Defence tech companies are technology companies created to primarily sell into the defence sector. They should be differentiated from traditional defence companies (BAE Systems, Lockheed Martin, General Dynamics, Thales, etc.), despite the latter also often providing significant tech products and services to the defence sector, for a number of reasons.

Defence tech companies have grown in their significance due to prioritising software, software-defined hardware, and relatively inexpensive products, although traditional defence companies now compete in these areas as well. The most significant distinction between the two categories is the level of integration of defence tech companies with civilian sectors. Defence tech companies trace their heritage to Silicon Valley,[3] which these companies reflect in their communications, business models, and business in numerous civilian sectors. The rhetoric of defence tech companies has been explored in depth elsewhere, and even been described as 'aggressive marketing', including assertive, sometimes belligerent, geopolitical rhetoric that often revolves around nationalistic and tech-evangelist themes.[4]

Defence tech companies have been intimately involved in the digitalisation of the defence sector in the past decade and use Silicon Valley's experience in digitalising civilian sectors in defence. Much of this relationship stems from the increasing role of technology often originally developed in civilian sectors to military capability, including uncrewed vehicles, advanced sensors, and, perhaps most importantly, digital technologies, due to their importance in MDO. Similar to their provision in civilian sectors, these companies frequently adopt service-based contracts, where government funds are spent as operating expenses, rather than mainly capital expenditure into large platforms.

Procurement Transformation: Defence tech procurement has shifted to rely on more operating expenditure, mainly service-based contracts.

Such contracts mean that militaries pay for a continued relationship with companies that allows them continuous support and sustainment. Critics have described this business model as anticompetitive and 'rent-seeking', the evaluation of which lies outside the scope of this piece, but the complexity of modern defence capabilities in addition to the proliferation of software-defined capabilities does necessitate some manner of persistent contractual relationship between public and private sectors.[5]

Finally, while traditional defence companies often retain some non-defence clients, defence tech companies are often involved in a far greater number of non-defence sectors and relationships. These companies frequently sell products and services to non-defence sectors of government, from intelligence agencies to government health departments, but also many private civilian sectors, including insurance, finance, logistics, and healthcare. Crucially, expertise, products, and deployment lessons flow between their defence and non-defence business arms.

Dependencies and Power

As many countries in Europe reinvest heavily into their defence sectors, some are beginning to examine how the rise of defence tech reshapes existing power dynamics. Much of their concern for the growing influence of the private sector power revolves around a changing relationship with the US.

In recent years—particularly since Trump's re-election—European countries have become increasingly aware of their reliance upon the US for key military capabilities. Several European governments have sought to reduce this

3 A detailed source on this history is Anthony King, AI, Automation, and War: The Rise of a Military-tech Complex, Princeton University Press, August 2025.

4 This rhetoric has been discussed frequently in journalistic pieces, but more in-depth research on the topic includes 'Startups Envisioning Algorithmic Warfare: The Discourses of US Tech Companies in Defense AI' by Anna Nadibaidze and 'Unicorns for Uniforms: On the Problematic Allure of VC Investments in Defence' by Elke Schwarz.

5 Susannah Glickman, 'The War Over Defense Tech', The New York Review, 04 October 2025, **https://www.nybooks.com/online/2025/10/04/the-war-over-defense-tech/**; Jonathan Panter, 'A Skeptic's View of the Hype Machine and Business Model of Neo-Defense Tech', 26 August 2025, War on the Rocks, **https://warontherocks.com/2025/08/a-skeptics-view-of-the-hype-machine-and-business-model-of-neo-defense-tech/**; Mahmoud Javadi, 'Infrastructural Entanglement and Cloud Hyperscalers in Contemporary Warfare: Insights from Ukraine, Israel and Taiwan', Contemporary Security Policy, November 2025, **https://doi.org/10.1080/13523260.2025.2593247**.

dependence upon US companies by investing vast sums in domestic, or at least European, defence firms. This has borne some successes in building a more sovereign defence base, but is far insufficient to replace dependency. The following section examines the balance of power between public authorities and private defence companies, especially through the lens of European dependencies on US companies.

Balancing Public-Private Power

European defence capabilities have long relied on strong relationships between government ministries and private companies. Yet—as described above—the rise of defence technology is reshaping defence industry, including how these relationships function. The balance of power in these relationships has shifted, requiring policymakers, practitioners, and civil society to understand the new vulnerabilities and limitations shaping their ability to procure and field modern capabilities.

This section elaborates on power dynamics between defence tech industry and government, especially through the lens of concentration and dependence.

Concentration and Dependence

European defence technology capabilities are increasingly concentrated and dependent upon a select number of companies, many of which are non-European. The concentration and dependency paradigms have been explored elsewhere for specific classes of technologies,[6] but this section elaborates on these dynamics regarding the broader class of defence tech capabilities, mainly those related to C4ISR functions.

Concentration is when a small number of companies provide most of the products or services. Market share is often dominated by a small number of companies for certain capabilities, especially when these companies possess significant capital expenditure abilities, niche technical expertise, and/or history and knowledge of navigating political and regulatory bureaucracy. Some examples of defence tech concentration are the cloud service provider (CSP) market, which is dominated in North America and Europe by three US hyperscalers, and space, which, despite gaining new competitors in recent years, is concentrated upon a few companies, namely SpaceX.

Market Concentration:
The defence-relevant cloud ecosystem in Europe is largely dominated by three US hyperscalers - AWS, Microsoft and Google.

In areas where capital expenditure is less burdensome to market entry, such as, for example, uncrewed aerial vehicles (UAVs), the market typically more dispersed and democratised. Historically many more areas like UAVs were concentrated, but the desire for inexpensive, often attritable capabilities has enabled a greater number of market actors to compete for contracts. Data processing is another relevant area. While firms like Palantir garner headlines and many large contracts, they are facing a growing number of smaller firms in Europe aiming to win large-scale analytics and data integration contracts. Notably, many of these companies highlight Palantir's US links in an attempt to sell themselves as a localised alternative (a topic explored in greater depth below), although the success of this effort varies by country.[7]

Dependence is the use 'of a service where there are limited or no alternatives, and/or where the cost of change is prohibitive'.[8] Government dependence upon private companies can impact power dynamics between the two, shifting the balance of power strongly towards the latter. However, the dependence paradigm is arguably most relevant to policymakers geopolitically due to the European dependence on US companies for defence tech capabilities. The manner that this dependence came into being is outside the realm of this piece but includes the combination of decades of global dominance by US defence and technology companies, close military and geopolitical alignment, and European decisions to not invest in their own technological and military-industrial bases.[9]

6 Joseph Jarnecki, 'European Cloud Adoption for National Security', Royal United Service Institute, November 2025, **https://www.rusi.org/explore-our-research/publications/research-papers/european-cloud-adoption-national-security**.

7 For different European relationships with Palantir, see 'US tech firm Palantir extends deal with French intelligence agency', Le Monde, 15 December 2025, **https://www.lemonde.fr/en/france/article/2025/12/15/us-tech-firm-palantir-extends-deal-with-french-intelligence-agency_6748523_7.html**; Joseph Bambridge, 'Palantir lands biggest ever UK defense deal', Politico, 02 January 2026, **https://www.politico.eu/article/palantir-lands-biggest-ever-uk-defense-deal/**; Aurélie Pugnet et al., 'Palantir is well on its way to conquering Europe', Euractiv, 08 August 2025, **https://www.euractiv.com/news/palantir-is-well-on-its-way-to-conquering-europe/**; Adrienne Fichter et al., 'Why Palantir is becoming a risky bet for Switzerland', swissinfo.ch, 22 December 2025, **https://www.swissinfo.ch/eng/war-peace/why-palantir-is-becoming-a-risky-bet-for-switzerland/90666335**.

8 Jarnecki, 'European Cloud Adoption for National Security', 2025.

9 See, for example, Peter Schaefer, 'Europe's defence reliance on the US runs deeper than hardware', The Parliament, 02 December 2025, **https://www.theparliamentmagazine.eu/news/article/europes-defence-reliance-on-the-us-runs-deeper-than-hardware**.

Public-Private Power Effects

Anthony King, in his 2025 book 'AI, Automation, and War', coined the term 'military-tech complex'—an evolution of the Cold War-era 'military-industrial complex'—to describe the integration of tech companies into military structures, operations, and procurement.[10] Viewing the merging of the private tech sector with the public defence sector into a single 'complex' is among the most crucial frameworks for understanding the contemporary Western defence sector. While criticism of the military-tech complex includes doubts about its viability in terms of developing and sustaining military capabilities,[11] this section will begin to describe the implications of this phenomenon both inside and outside the defence sector.

Defence Procurement

The rise of the military-tech complex has disrupted many procurement functions over the past decade, often with the intention of providing faster, and more iterative development cycles. This disruption coincides with the cementation of 'software-defined' platforms and 'cheap mass' as core to modern thinking, both of which require continued delivery relationships with industry, rather than platform-delivery based contracts. Combining these concepts with Silicon Valley's experience with these business models, service-based contracts became an essential part of defence procurement, where companies provide engineering and technical support, continued software updates and upgrades, and lifecycle maintenance and sustainment. Such a model reduces capital expenditure for militaries in favour of operational expenditure, as well as ensuring the fielding of the latest capabilities, but increases governments' dependence upon industry.

Both concentration and dependency increase a company's leverage, both political and commercial, over the government and other market actors.

Power Dynamic Shift:
Market concentration + technological dependence → increased leverage for defence tech providers.

The leverage can be used to obtain contracts, dictate contract terms more favourable to the company, and create conditions of vendor lock-in. In other words, the concentration and dependence of the defence tech market places even greater power in the hands of these market actors at the cost of government autonomy and control.

Sovereignty

As seen in Table 1, C4ISR functions in modern operations (broadly sorted into data collection, transfer, storage, processing, analysis functions) across domains and levels of command are disproportionately represented by US providers. Increases in concentration and dependency from capability providers can threaten states' ability to exert control and choice in their domestic and international processes—a quality for which this paper uses the term 'sovereignty'.

European rearmament following Russia's invasion of Ukraine, and especially since the reelection of Donald Trump, has brought questions of sovereignty to the forefront of policy circles.

Sovereignty fundamentally revolves around questions of national control but lacks an agreed-upon description of its characteristics, leading to states and ministries to disagree on what they consider 'sovereignty'. The types of sovereignty might include:

- Operational autonomy
- Physical localisation
- Legal and jurisdictional authority
- Commercial flexibility
- Industrial benefits
- Supply chain
- Unbroken availability
- Access and security control

Companies, ministries, governments, and multinational entities in Europe are in the midst of a heated debate about what sovereignty can and/or should entail, especially in terms of digital technologies like cloud and AI.[12]

10 King, AI, Automation, and War, 2025. More critical descriptions of this complex offer competing terms, such as Francesca Bria's 'authoritarian stack', **https://monde-diplomatique.de/artikel/!6113232** and authoritarian-stack.info.

11 Panter, 'A Skeptic's View of the Hype Machine and Business Model of Neo-Defense Tech', 26 August 2025.

12 Further reading on this topic includes Filippo Gualtiero Blancato and Madeline Carr, 'The Trust Deficit. EU Bargaining for Access and Control over Cloud Infrastructures,' Journal of European Public Policy, December 2024, **https://doi.org/10.1080/13501763.2024.2441418**; Matthias Bauer and Dyuti Pandya, 'Europe's Cloud Debate Is Looking the Wrong Way: It's Not Concentration – It's Lock-In', ECIPE, December 2025, **https://ecipe.org/insights/europes-cloud-debate-looking-wrong-way/**; Daniel Mügge, 'EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?', Journal of European Public Policy 31 (8), February 2024, **https://doi.org/10.1080/13**

Table 1: Major Companies in European C4ISR

Data Collection	*Storage and Processing*	*Data Transfer/Networking*	*Large Scale Analytics*
Airbus BAE **Boeing** Hensoldt Indra **L3Harris** Leonardo **Lockheed Martin** **Northrup Grumman** **RTX** Thales Saab Systematic	Atos **AWS** BAE **IBM** **Google** **L3Harris** **Microsoft** **Oracle** OVH Rheinmetall SAP Thales	Atos Airbus BAE **Boeing** BT **Cisco** **Fujitsu** **General Dynamics** **L3Harris** Rheinmetall Rohde & Schwarz **SpaceX** Sopra Steria Systematic Thales Viasat	Atos BAE **Booz Allen Hamilton** **Leidos** Leonardo **Palantir** SAP **Splunk** Thales

A sample of major suppliers for C4ISR functions at tactical, operational, and enterprise levels. Non-European providers are bolded.

These efforts for sovereignty have been piecemeal, from the 'EuroStack' initiative to the European Cybersecurity Certification Scheme for Cloud Services (EUCS) controversy,[13] but most pushes for 'sovereignty' are at the national level, with mixed success. Resistance to sovereign tech pushes mainly stem from the perceived trade-off between capability and sovereignty, as large, US-centred multinational corporations are able to offer advanced capabilities, availability, and scaling that their European competitors cannot easily match. Nowhere is this balance more acutely felt than in Ukraine, which relies on US tech companies like AWS, Microsoft, Palantir, and SpaceX. Their dependence was seen as necessary in the early stages of the war to maintain continuity in government services and to counter Russia through modern digitalised operations, but this has come at a cost of Ukrainian sovereignty. One Ukrainian official put their dilemma bluntly: 'We will either be destroyed or be controlled'.[14]

Strategic Reality:
Europe remains structurally dependent on US providers for core defence tech capabilities.

No matter the definition chosen, Europe cannot be understood as truly sovereign in the defence tech sector. Despite attempts at stimulating alternatives to US companies, European countries have not been able to scale their tech companies to the point of competitiveness.[15] Table 1 provides a visualisation of US overrepresentation in defence tech, but the reality is even more stark when considering these US companies' market share and contracting for core military functions.[16] Dependence upon US companies permits the US significant leverage over European governments, while leaving Europeans vulnerable to the whims of the US government. The US sanction of the ICC judges also sent shockwaves through Europe, where European citizens upholding international law are prevented from banking, accessing their

501763.2024.2318475. This author is also engaged in a project exploring and assessing approaches to cloud sovereignty: https://www.rusi.org/explore-our-research/projects/sovereignty-cloud.

13 Clotilde Bômont, 'Technical is political: When a cloud certification scheme divides Europe', EUISS, 03 November 2025, https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe.

14 Conversation with the author, December 2025.

15 For a deep dive into a country approach to tech in the national security space, see Pia Hüsch and Natasha Buckley, 'UK National Security Advantage from Disruptive Technologies', RUSI, 08 October 2025, https://www.rusi.org/explore-our-research/publications/research-papers/uk-national-security-advantage-disruptive-technologies.

16 Sebastian Clapp, 'United States Defense Industrial Base', European Parliament, October 2025, https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/777967/EPRS_BRI%282025%29777967_EN.pdf.

email, and even using virtual assistants while still residing in Europe.[17]

Furthermore, even when US companies market 'sovereign solutions', it is sovereignty *through* these companies, rather than sovereignty *from* these companies, with policy circles still debating to what degree technical solutions can mitigate fundamentally political concerns about sovereignty.[18]

Outside Defence

Companies in defence tech are distinct specifically because of their integration with the civilian sectors, causing feedback between the defence and civilian sectors that is mediated by these companies. As a result, this military-tech complex includes impacts outside the defence sector. While this topic still merits further research, the societal impacts should be understood as impacting the economy, governance, and public opinion, and are often not one-way, but instead part of a feedback loop.

These impacts can be seen economically in terms of disruption to capital flows, especially venture capital, and changing patterns of carbon emissions.[19] The market effects of concentrated sectors and/or sector with high dependencies remain outside the remit of this piece, but does include risks of stagnation, inefficiency, and difficulty innovating due to the lack of widespread competition mechanisms, to say nothing of the effects upon actors forced out of the market by such companies.[20] The military-tech complex affects governance by reducing digital sovereignty (see above), reducing governments' ability to exert control over multinational companies due to regulatory capture, and in how dual use tech (and the companies that provide it) becomes framed as fundamental to national security.[21] Finally, companies in defence tech are far more media savvy than their traditional predecessors and shape public opinion of their own companies while also changing how society perceives the defence sector. They have followed—and, oftentimes, led—rhetoric intended to increase tolerance for military action, to increase the need for the military to take a 'whole of society' approach to defence, and to promote increased defence spending as a strong contributor to economic growth.[22]

Other Concerns

Vulnerability

Simultaneously concentrated and dependent capabilities leave that military particularly vulnerable to disruptions, which can result in a disproportionate effect on military readiness and efficacy. IT outages have become more prominent in recent years, especially those affecting customers of commercial providers such as the CSPs and Cloudflare.[23]

---

17 'Cut off by their banks and even iced out by Alexa, sanctioned ICC staffers remain resolute', AP News, 12 December 2025, **https://apnews.com/video/cut-off-by-their-banks-and-even-iced-out-by-alexa-sanctioned-icc-staffers-remain-resolute-cf0b6083b-6c941898b47b94731092eaa**.

18 Rafael Grohmann and Alexandre Costa Barbosa, 'Sovereignty-as-a-service: How big tech companies co-opt and redefines digital sovereignty' Media, Culture & Society, 11 November 2025, **https://doi.org/10.1177/01634437251395003**; Filippo Gaultiero Blancato and Madeline Carr, 'The trust deficit. EU bargaining for access and control over cloud infrastructures', Journal of European Public Policy, 18 December 2024, **https://www.tandfonline.com/doi/full/10.1080/13501763.2024.2441418**.

19 For venture capital shifts, see Branka Marijan, 'Venture Capital and the Militarization of Innovation', Ploughshares, 29 September 2025, **https://ploughshares.ca/venture-capital-and-the-militarization-of-innovation/**; Elke Schwarz, 'From blitzkrieg to blitzscaling: Assessing the impact of venture capital dynamics on military norms', Finance and Society, 2025, **https://www.cambridge.org/core/services/aop-cambridge-core/content/view/S2059599924000189**. For changes in energy requirements, see Murielle Delaporte, 'From Algorithms to Kilowatts: The Energy Challenge of Military AI', Eurosatory, 09 October 2025, **https://www.eurosatory.com/en/from-algorithms-to-kilowatts-the-energy-challenge-of-military-ai/**; Wichuta Teeratanabodee, 'The Environmental Impact of Military AI', RSIS, 15 July 2022, **https://rsis.edu.sg/rsis-publication/idss/ip22039-the-environmental-impact-of-military-ai/**.

20 Sabrina T. Howell et al., 'Opening up military innovation: causal effects of reforms to U.S. defense research', Centre for Economic Performance, March 2023, **https://eprints.lse.ac.uk/114430/5/dp1760.pdf**; Gregory C. Allen and Doug Berenson, 'Why Is the U.S. Defense Industrial Base So Isolated from the U.S. Economy?', CSIS, 20 August 2024, **https://www.csis.org/analysis/why-us-defense-industrial-base-so-isolated-us-economy**.

21 See, for example, James Andrew Lewis, 'Tech Regulation Can Harm National Security', CSIS, 28 November 2022, **https://www.csis.org/analysis/tech-regulation-can-harm-national-security**; Jieli Li, 'Governing High-Risk Technologies in a Fragmented World: Geopolitical Tensions, Regulatory Gaps, and Institutional Barriers to Global Cooperation', Fudan Journal of the Humanities and Social Sciences, 2025, **https://doi.org/10.1007/s40647-025-00445-4**.

22 Glickman, 'The War Over Defense Tech', 2025; Robin Vanderborght and Anna Nadibaidze, 'Demonstrating the Future of War: Tech Companies and Claims of Epistemic Authority on Military AI', OpinioJuris, 19 November 2025, **https://opiniojuris.org/2025/11/19/demonstrating-the-future-of-war-tech-companies-and-claims-of-epistemic-authority-on-military-ai/**; Anna Nadibaidze, 'Startups Envisioning Algorithmic Warfare: The Discourses of US Tech Companies in Defense AI', Global Policy, 2025, **https://doi.org/10.1111/1758-5899.70047**.

23 Jarnecki, 'European Cloud Adoption for National Security', 2025, 32-33.

Operational Risk:
Dependence on individual suppliers increases exposure to external disruptions.

Technology companies have also been vulnerable to political controversy, with examples including Google's 2018 Maven staff walkout, Microsoft cutting some services to the Israeli military in 2025, and even the aforementioned sanctioning of ICC judges. In each case, the company withdrew services from their government customers due to pressure from the public and/or other governments. Mitigating these political vulnerabilities has become a core policy concern, especially since the start of 2025, but solutions remain piecemeal. Most mitigation efforts include redundancy in service providers and/or dispersing services across providers to enhance resilience in the event of provider outages.[24]

Values

European governments and the US government have clashed for years over US tech companies operating in Europe, but these tensions have only grown since Trump's second presidential term began. US tech companies have clashed with European regulators for years in matters of data protection and national sovereignty, and European countries are beginning to recognise that this schism may represent a fundamental divergence in values. The 2025 National Security Strategy, the US threats over Greenland, and the illegal US/Israeli attacks on Iran have only exacerbated this trend.[25] Even when the private sector is willing to align with European *interests*, alignment on *values* is of equal importance.

The American tech sector is no stranger to European political controversy, but the scale and frequency of recent disputes have been staggering, from Palantir's contracts with US Immigration and Customs Enforcement (ICE), to X's disinformation and image generation scandals, to numerous contracts with the Israeli Defence Force, to the close ties between America's powerful tech leaders and its political leadership. Furthermore, the recent controversy between Anthropic and the US Department of War highlights the deference expected of companies by the current US administration as well as the latter's willingness to weaponise the regulatory and economic levers against those who resist.

Ultimately, European policymakers must consider to what degree these companies should be entrusted with providing the defence of Europe.

Public-Private considerations for System Integration

In the modern defence sector, there is no area more relevant to this topic than systems integration, especially due to the centrality of this concept to the vision of a fully integrated force. Specific discussion of systems integration has been sparse in policy circles outside digital specialists, but has whole-of-force implications. Put simply, system integration in defence is the governance and engineering of technical and operational interoperability between systems and technologies while managing risk across both government and industry.

Modern military concepts revolve around enabling MDO, requiring capabilities to be integrated across domains for instantaneous and seamless awareness, decision-making, and execution of operations. Combined with the complexity of modern digitally-defined systems and the sheer quantity of sensors, deciders, and effectors on the modern battlefield, system integration has become a crucial focus for militaries. Detailing the complexities of systems integration methods remains outside the remit of this piece, but merits further work, especially in breaking down the complexity of these processes to policymakers and non-expert practitioners.

Western militaries have struggled with system integration in recent decades, with integration failures cited as among the most common reasons for programme failures. Programmes that have

24 See, for example, Alena Kudzko and Alexandre Burilkov, 'Private Tech for Resilience: Geopolitical Shifts and Government-Tech Relations', GLOBSEC, April 2025, **https://www.globsec.org/what-we-do/publications/private-tech-resilience-geopolitical-shifts-and-government-tech-relations**.

25 See, Pierre-Yves Hénin, 'The 2025 national security strategy: A different worldview', IRIS, 12 January 2026, **https://www.iris-france.org/en/la-strategie-2025-de-securite-nationale-une-autre-vision-du-monde/**; Emily Benson, 'Why Greenland Could Spur Europe's Digital Awakening', CSIS, 14 January 2026, **https://www.csis.org/analysis/why-greenland-could-spur-europes-digital-awakening**; Nathalie Tocci, 'Europe's reaction to Trump's war on Iran is a disaster – for Europe itself', The Guardian, 16 March 2026, **https://www.theguardian.com/commentisfree/2026/mar/16/europe-reaction-donald-trump-war-iran-legal-iraq**; and Anthony Dworkin, 'War over law: Europe's unforced errors over the use of force in Iran', European Council on Foreign Relations, 12 March 2026, **https://ecfr.eu/article/war-over-law-europes-unforced-errors-over-the-use-of-force-in-iran/**.

significantly struggled with system integration include the UK's 'digital backbone' (especially its NGCN programme),[26] the UK's Morpheus tactical radio programme,[27] Germany's D-LBO,[28] NATO's 'Digital Backbone',[29] sixth-generation fighter programmes,[30] and various other national and multinational digitalised acquisition efforts. The difficulties vary, given the complexity of the task, but a number of public/private sector considerations are relevant to current and future successful integration.

Architecting

Any discussions of integration must begin with architectural considerations. The choice of system integrator—the company, ministry, or organisation responsible for outlining and managing how the integration will occur, as well as the integration itself—underpins public-private sector relations for a given programme.

The integration of a system with another system is made possible through the adherence to common standards that mandate certain protocols, formats, and benchmarks. In the Western defence sector, digital standards are often set by NATO to enable standardisation for the purpose of multinational interoperability. Yet countries often deviate from Allied standard-setting, as initiatives like Federated Mission Networking (FMN) are slow and unwieldy, with any rules passed by a consensus of 32 governments. These efforts also struggle to keep up with many modern capabilities given the current speed of technological development and iteration.

The fragmented solutions landscape inhibits interoperability, with the dominance of large NATO countries (namely the US) often leading to de facto alliance adoption of their standards. Efforts to resolve these challenges involve a combination of adopting commercial standards or relying on bilateral or minilateral interoperability, both of which have their limitations in a military alliance context. Some military services, governments, and multinational bodies demand varying degrees of integration/interoperability 'by design' from these companies, with varied success.[31]

Many of these efforts are also stymied by systemic challenges in defence enterprises. Foremost among these is the lack of visibility by both policymakers and practitioners into their digital estates, with one official describing the navigation their networks as 'recce by fire'.[32] Defence ministries also suffer from significant legacy estates which constrain modernisation efforts as well as daily operations.[33]

Modernisation Barrier:
Legacy infrastructure and estate opacity constrain defence transformation across Europe.

Lock-In

As discussed above, modern defence capabilities must be iterative and more integrated, meaning that defence ministries have been increasingly mandating architectures that are open, meaning that other systems can integrate into the architecture using non-proprietary standards. In addition to permitting greater interoperability and integration, the open architecture is intended to counter a significant detrimental effect often arising from commercial architectural ownership—lock-in.

26 Noah Sylvia, 'European Digital Defence Priorities in an Uncertain World', RUSI, 25 March 2025, **https://www.rusi.org/explore-our-research/publications/emerging-insights/european-digital-defence-priorities-uncertain-world**.

27 Noah Sylvia, 'Upgrading the British Army's Tactical Communications: What Next?', RUSI Commentary, 05 April 2024, **https://www.rusi.org/explore-our-research/publications/commentary/upgrading-british-armys-tactical-communications-what-next**.

28 Enrico Dani, 'The Digitisation of Bundeswehr Land Operations', European Security & Defence, 02 December 2022, **https://euro-sd.com/2022/12/articles/28418/the-digitisation-of-bundeswehr-land-operations/**; Europäische Sicherheit & Technik, 'Der IT-Report 2024 – Digitalisierung in der Bundeswehr' ['IT Report 2024 – Digitalisation in the Bundeswehr'], Mittler Report, June 2024, **https://esut.de/en/2024/06/meldungen/50878/der-it-report-2024-digitalisierung-in-der-bundeswehr/**.

29 Joe Fay, 'NATO's battle for cloud sovereignty: Speed is existential', The Register, 17 December 2025 **https://www.theregister.com/2025/12/17/sovereign_cloud_is_existential_nato/**; Hans Horan, 'Securing the Digital Backbone: NATO's Quest for Interoperability in the Age of Emerging Disruptive Technologies', The Hague Centre for Strategic Studies, June 2025, **https://hcss.nl/report/securing-the-digital-backbone-natos-quest-for-interoperability-in-the-age-of-emerging-disruptive-technologies/**.

30 'FCAS at Risk: Dassault Calls Out Dysfunction in Europe's €100B Fighter Project', Großwald, 17 April 2025, **https://www.grosswald.org/fcas-governance-crisis-dassault-warns/**; Alessandro Marrone, 'The New Partnership among Italy, Japan and the UK on the Global Combat Air Programme (GCAP)', Istituto Affari internazionali, 14 March 2025, **https://www.iai.it/en/publications/c04/new-partnership-among-italy-japan-and-uk-global-combat-air-programme-gcap**.

31 All multinational considerations are inhibited by a discernible lack of metrics or methods for measuring interoperability within NATO. See John Deni et al., 'Measuring Interoperability Within NATO: Adapted Off-the-Shelf or Bespoke Solution?', US Army War College Quarterly: Parameters, 2025, **https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3331&context=parameters**; Noah Sylvia, 'Cloud Interoperability Between Allies During Crisis', RUSI, 05 November 2025, **https://www.rusi.org/explore-our-research/publications/insights-papers/cloud-interoperability-between-allies-during-crisis**.

32 Sylvia, 'European Digital Defence Priorities in an Uncertain World', RUSI, 2025, 7.

33 Ibid.

Commercial lock-in is where the government cannot change providers without accruing unacceptable costs, and is therefore reliant upon the companies, granting the latter increased power over the former. Such power can be used to dictate terms to the government on *what* or *who* can be integrated into the architecture, *how* it can be integrated, and how much such integration will cost, in addition to imposing additional costs to prevent the government from shifting to a new commercial provider. A number of companies in defence tech have been campaigning in recent years to embed themselves into national and multinational concepts of operations exactly in this manner, with their products forming a core of the military capabilities, into which other providers must integrate.[34]

However, governments have not had great success historically of themselves acting as the system integrator. Given their relative lack of technical expertise compared to the private sector (which is only widening given the pace of technological development), government-led integration has led to unrealistic requirement burdens upon suppliers and poor management of architectural integration and iteration. Perhaps most critically, government bodies in charge of integration often lack sufficient budgetary and organisational authority to cohere the disparate functions across military services. This is true even when the government is not themselves acting as the system integrator.

Managing Risk and Authority

Decision-making when integrating or iterating capabilities revolves fundamentally around risk management by involved stakeholders. An open architecture changes the risk management considerations considerably. In an open system, the integrator must account for a variety of actors and systems, complicating accreditation, diffusing responsibility and blame, and demanding constant government coordination. In a closed system, a single owner has a greater degree of control over who integrates and how it occurs, allowing government to manage a single point of responsibility.

Besides continuing capability functionality, system integration and iteration must consider risks including but not limited to cyber vulnerabilities, security accreditation, IP constraints, backwards compatibility, supply chain vulnerabilities, multinational interoperability, and resilience. The management of these risks involves coordination between the public and private sectors at different stages of capability lifecycles, technical integration, operational testing and deployment, and architectural iteration. Without proper management of risk, procurement cycles and defence modernisation will fall short, resulting in slow iteration cycles, lock-in, siloed capabilities, budget overruns, and/or total capability failures.

Recent success cases for complex military integration often been due to specific industry circumstances, where companies leveraged existing contacts to coordinate with various government stakeholders and assuage fears. Private sector actors frequently describe the incohesive nature of working with government entities, with companies often acting as the connective tissue for different parts of the government. Yet ad-hoc coordination should not be relied upon while hoping many Western militaries begin the systematic changes necessary to consistently manage integration risk in open, multi-domain architectures.

34 See Javadi, 'Infrastructural Entanglement and Cloud Hyperscalers in Contemporary Warfare', November 2025, for a discussion of technical lock-in, operational leverage, industrial influence in the context of CSPs.

Policy Directions Forward

European governments are pushing strongly into militarisation, but are struggling to create a cohesive, strong position in managing their relationships with the private sector. This paper highlights a number of key areas for policymaking given the problem set outlined above.

1. Skills and Knowledge

a. The public sector needs to develop the expertise to contract, procure, integrate, deploy, and iterate digital technologies without overreliance upon the private sector. Admittedly, the public sector will never be able to match the expertise of the private sector when innovation and development stems from commercial technologies, but pursuing a minimum of digital literacy can ensure a more capable and efficient force. Building capability and reducing dependence on non-European skills requires a combination of developing technical talent at the national level while simultaneously upskilling existing policymakers and service members.[35]

2. Sovereignty

a. European countries have recognised the centrality of sovereignty in their policymaking, but conversations begin to falter when discussing the specifics of sovereignty. For coordinated, coherent actions on sovereignty, Europe needs a common framework and language for describing sovereignty across a number of political, technical, and economic dimensions.

b. To have any hope of building alternatives to concentration in and dependence on US providers, sovereignty must be prioritised in defence tech procurement.

   i. Sovereign (whether defined in national or European terms) companies should be prioritised in procurement cycles. Many European militaries are understandably prioritising capability and speed in their tech adoption; however, this often means that US firms retain primacy in procurement. Sovereign defence tech offerings can only present competitive capability offerings if governments allow them to grow and develop through investment and contracting experience.

c. Admittedly, some level of dependence upon US providers cannot be avoided in the near future, so attempts at promoting sovereign alternatives must be matched with proper risk management. When US companies are chosen for bids, governments must minimise companies' ability translate this into geopolitical leverage. The means for reining in the power of non-European companies varies, but includes means that are technical (client-side encryption, air-gapping, identity and access management policies, architectural openness, etc), legal (IP restrictions, data protection regulations, tech transfer regimes, etc), industrial (mandating jobs, skills, and economic benefits are concentrated in Europe), and commercial (pro-competition guidelines, multi-vendor resilience, requiring foreign vendors pairing with national vendors, etc.).

3. Integration

a. Modern defence capabilities require flexible, modular models of systems integration, with architectural authority, risk ownership, and interoperability obligations clearly defined at programme inception.

   i. The system integrator must have explicit architectural authority, with control over interfaces, data standards, and integration sequencing. Government must designate these measures at the outset, relying on trusted partners to ensure requirements are reasonable and desirable, focusing on acceptable levels of capability rather than requiring perfection.

   ii. Interoperability with key allies must be mandatory and measurable in national procurement programmes. NATO-first in practice requires both adherence to and creation of alliance-level standards, but also bilateral and minilateral interoperability efforts based on these policies.

35 For specific policy recommendations, see 'Closing the talent gap: Priorities for Europe's skills agenda', DigitalEurope, August 2025, **https://cdn.digitaleurope.org/uploads/2025/08/2025-08-20_Closing-the-Talent-Gap_Digital-Skills-Agenda-Priorities.pdf**, and Pia Hüsch and Natasha Buckley, 'UK National Security Advantage from Disruptive Technologies: Understanding UK Assets, Needs and Dependencies', RUSI, October 2025, **https://static.rusi.org/rp_uk-national-security-advantage-oct-2025.pdf**.

iii. Open architectures should be mandated in capability development initiatives when possible, but should be balanced against government security, commercial, and trust concerns. These architectures must include modular integration strategies to allow for capability additions, modifications, and removals, supported by flexible accreditation paths and user feedback loops.

b. As risk calculations for large, digitalised capabilities are changing, the public sector needs to reenvision how it manages risk. Many of these policy changes are part of broader procurement reforms necessary for defence, which is outside the remit of this piece, but there are several relevant directions.

   i. Trust is lacking between the public and private sectors due to budget and timeline nonalignment, frequent mutual perception of lacking 'skin in the game', and insufficient expectation management. Building trust is slow, and will require consistent spending and streamlined bureaucracy from government, while industry will have to burden share on procurement risks.

   ii. A lack of expertise also contributes to a trust deficit, as government officials often lack the knowledge to set requirements, mitigate various types of risk, and account for actors and systems in open models of integration (see above for recommendations on skills).

   iii. While not an issue unique to risk management, the lack of public sector institutional cohesion arrests the ability for capabilities to be developed, integrated, and iterated. Defence organisations must develop commands and institutions that have the authority (both organisational and budgetary) to cohere the various bodies, subcommands, and agencies through specific integrative functions while simultaneously possessing clear diagrammatic knowledge of the authorities, risk ownerships, and relationships of the other defence organisations.

4. Commercial

a. Europe needs better strategies for dealing with the dominant private sector actors. Large multinational corporations have long been recognised as subverting traditional notions of nation-state sovereignty.[36] National or multinational approaches to interacting with these firms in the defence-tech space must be part of larger conversations about power between the public and private (tech) sectors in Europe, especially regarding companies that diverge from Europe's values. These conversations are currently fragmented, with policy mitigations piecemeal and reactive. Only by recognising these corporations as foreign multinational entities more powerful than most states can countries more readily protect their citizens' rights and state power itself.

5. Strategic

a. Perhaps most importantly, Europe is reconsidering its place in a rapidly changing world. As countries recognise their dated perceptions of national geopolitical heft and the fragility of overseas alliances, they need to decide a clear, unified path forward. Regional security relationships have become more important, and Europe will likely need to reorient solidly towards regional defence rather than international power projection. This requires increased cooperation between European countries on mission-specific planning and exercises, rather than the piecemeal efforts that indicate a loose coalition, rather than a tight-knit, credible defensive alliance.

36 See, for example, Hongfei Gu, 'Data, Big Tech, and the New Concept of Sovereignty', Journal of Chinese Political Science, May 2023, **https://pmc.ncbi.nlm.nih.gov/articles/PMC10155150/** and Atal et al., 'Oligarchic sovereignty: Technology and the future of global order', Review of International Studies, Dec 2025, **https://www.cambridge.org/core/journals/review-of-international-studies/article/oligarchic-sovereignty-technology-and-the-future-of-global-order/1E8CA6E567E56FB8CE93FC835A6ED60D**.

Conclusion

European defence is entering a period of accelerated militarism at precisely the moment when the traditional boundaries between state power, industrial capability, and technological control are eroding. As this paper has argued, capability alone will not deliver credible security unless European governments develop the skills, authority, and coherence required to manage their relationships with increasingly powerful private-sector actors. Addressing gaps in technical expertise, clarifying what sovereignty means in practice, reforming approaches to systems integration and risk, and engaging strategically with dominant technology firms are not discrete challenges, but interdependent choices that will shape Europe's ability to act autonomously and collectively. With deliberate action, there is a narrow but viable path toward a more integrated, sovereign, and credible European defence posture.

GLOBSEC
IDEAS SHAPING THE WORLD

Prague, Czechia
Brussels, Belgium
Bratislava, Slovakia
Kyiv, Ukraine
Vienna, Austria,
Washington, DC, United States

+421 2 3213 7800
info@globsec.org
www.globsec.org