

# The Defence Tech Readiness Pivot

## From Legal Limits to AI-Enabled Capability: Europe’s Industrial and Governance Roadmap

di Gordon A. Mensah

### Abstract

This paper argues that Europe’s path to credible defence lies not in creating a supranational army, but in building a tech- and AI-enabled capability stack anchored in a stronger European Defence Technological and Industrial Base (EDTIB). Starting from the EU’s legal framework—TEU/TFEU provisions that preserve national sovereignty while enabling collective action—the paper shows how treaty constraints can catalyse an industrial pivot: aggregating demand via joint procurement (ASAP, EDIRPA), deploying EDIP’s market-shaping tools (including SEAP and EDPCIs), and leveraging the Readiness 2030/ReArm package (escape clause + SAFE loans) to generate bankable, multi-year orders. In comparative perspective, it distils the United States’ “innovative advantage” in independent systems integration (FFRDCs/UARCs, interface stewardship, architecture-first design) and translates these lessons into a European governance model that separates integration from production and standardises open, modular architectures. The paper operationalises Mario Draghi’s competitiveness lens—treat defence as a strategic industry—and prioritises defence-relevant AI applications (C2, multi-sensor fusion, air/missile defence, secure cloud, digital twins, drones/autonomy, space-based ISR, resilient cyber). It proposes “rule-of-law-by-design” guardrails (objective security-of-supply, sovereignty-preserving standards, lifecycle TEVV for AI, export-control coherence, parliamentary/independent oversight). National strategies (Italy’s DPP; UK’s SDR/UKDI) and the post-2022 surge in European defence-tech investment underscore urgency. The result is a roadmap to turn EU rearmament into fielded, interoperable capability—at speed, and under law.

Il paper sostiene che la competitività della difesa europea non dipende dalla creazione di un esercito sovranazionale, bensì dalla costruzione di una capability stack abilitata da tecnologia e IA, fondata su una EDTIB (European Defence Technological and Industrial Base) più coesa. Muovendo dal quadro giuridico dell’UE—disposizioni TUE/TFUE che preservano la sovranità nazionale pur consentendo l’azione collettiva—mostra come i vincoli dei Trattati possano accelerare un pivot industriale: aggregare domanda tramite appalti congiunti (ASAP, EDIRPA), utilizzare gli strumenti market-shaping di EDIP (incluse SEAP ed EDPCI), e sfruttare il pacchetto Readiness 2030/ReArm (clausola di salvaguardia + prestiti SAFE) per creare portafogli ordini pluriennali bancabili. In chiave comparata, distilla il vantaggio

innovativo statunitense nell'integrazione indipendente dei sistemi (FFRDC/UARC, stewardship delle interfacce, design "architecture-first") e lo traduce in un modello europeo che separa integrazione e produzione e standardizza architetture aperte e modulari. Operazionalizzando la lente della competitività di Mario Draghi—trattare la difesa come industria strategica—il paper priorizza applicazioni di IA per la difesa (C2, fusione multi-sensore, difesa aerea/missilistica, cloud sicuro, digital twins, droni/autonomia, ISR spaziale, cyber resiliente). Propone garanzie di legalità "by design" (security-of-supply oggettiva, standard aperti ma sovereignty-preserving, TEVV ciclo-vita per l'IA, coerenza del controllo export, supervisione parlamentare/indipendente). Strategie nazionali (DPP Italia; SDR/UKDI Regno Unito) e il boom di investimenti post-2022 confermano l'urgenza. Ne deriva una roadmap per tradurre il riarmo UE in capacità dispiegate e interoperabili—rapidamente e nel rispetto del diritto.

## 1. Introduction

The geoeconomics challenges alongside great power competition have prompted Europe to reassess both its global stance and internal industrial strategy. Europe's revival of the industrial age echoes a simple axiom Friedrich List shared over two centuries ago: power depends on productive forces. As Grégoire Roos, director of the Chatam House European Program, notes, Europe's post-industrial comfort zone—supported by economic influence and regulatory strength—has shifted to a world where platform economics, AI computing, critical minerals, resilient grids, and low-carbon manufacturing now determine strategic importance; without a move from rules to capabilities, the EU cannot maintain geopolitical relevance or establish a "third way" between the United States and China. The challenge is a radical economic transformation that rebuilds industrial depth and speed. In prioritising efforts, Antonio Calcara and Riccardo Bosticco, professor and researcher at the Vrije Universiteit Brussel, warn that Europe risks following the wrong path: investing billions in "sovereign" chips and data centres while its true comparative advantage lies in industrial AI applications—particularly in defence and similarly to sectors such as education and healthcare where public investments are key in reducing the initial capex—where innovation capacity, rather than raw computing power, offers leverage. From digital twins for sixth-generation fighter production (e.g., GCAP) to multi-sensor data fusion in air defence, demand-driven adoption can strengthen the European Defence Technology Industrial Base(EDTIB) and promote dual-use spillovers. Equally important, this must be combined with a deliberate EU rearmament cycle: multi-year joint procurement and credible demand signals that expand munitions and air-defence lines, replenish stockpiles, and increase surge capacity across shipyards, aerospace,

electronics, and secure software—backed by common standards, workforce development, permitting reform, and resilient supply chains for critical inputs. The practical outcome is a more pragmatic approach to infrastructure—such as portability and data protection across clouds; aggregation of high-value industrial datasets—and targeted incentives that facilitate adoption across companies and sectors. In summary, Europe’s power will be built in factories, laboratories, and data centres only if it synchronises capital, standards, and rearmament-led procurement around defence-relevant AI applications—shifting from regulatory leadership to capability-building at industrial speed.

Europe’s industrial rearmament, however, cannot take place in a legal vacuum. To understand where and how the EU can act swiftly, this article proceeds in three steps. First, it clarifies the legal framework—EU treaties and Member State constitutions—that set strict limits on establishing a supranational European army while still allowing for collective action. Second, it shows how these constraints can catalyse—not block—a pivot towards defence technology: consolidating the EDTIB, pooling demand through joint procurement, and accelerating AI-enabled, system-of-systems capabilities—comparing it with the United States’ “innovative advantage” in integrating independent systems (FFRDCs/UARCs, interface stewardship, architecture-first design) that turns technological advances into operational effectiveness. Third, it outlines the governance needed to ensure that progress does not outpace the law. We argue that defence technology is the key lever because it connects Europe’s strategic autonomy to tangible industrial capacity: it reduces external dependencies, shortens innovation cycles, promotes dual-use spillovers, and ensures accountability by design. With this perspective, we examine the legal foundations that define the EU’s scope for manoeuvre.

This paper explains how Europe can turn defence tech into the practical engine of strategic autonomy by aligning law, finance, and industry. It starts from the legal architecture—TEU/TFEU limits that preclude a supranational army yet enable collective action—and shows why the centre of gravity must shift to the industrial domain: consolidating the EDTIB through EDIP’s “Buy European” rule-set, joint procurement (ASAP, EDIRPA), and the Readiness 2030/ReArm Europe package (escape clause + SAFE loans) to create credible multi-year demand. Framed by the Draghi agenda and Europe’s quest for digital sovereignty, the argument prioritises applications over raw compute: AI-enabled C2, multi-sensor fusion and air/missile defence, trusted cloud and secure software, digital twins for next-gen platforms, drones/autonomy, space-based ISR, and resilient cyber showing how these

technologies convert industrial scale into operational effect. In comparative perspective, the paper draws on the U.S. innovative advantage in independent systems integration (FFRDCs/UARCs, interface stewardship, architecture-first design) to illuminate the capabilities and governance Europe must build (SEAPs, EDPCIs, catalogue and sales mechanisms, supply-chain stress tests). It then proposes rule-of-law-by-design guardrails—objective security-of-supply and cybersecurity criteria, open-yet-sovereignty-preserving standards, lifecycle TEVV for AI, export-control coherence, and parliamentary/independent oversight—so that acceleration never outruns legality. National strategies (Italy’s DPP; the UK’s SDR/UKDI) and capital formation trends (venture surge post-2022) underscore urgency. The contribution is a roadmap to translate EU rearmament from policy to fielded capability: a legally disciplined procurement strategy that scales European industry, shortens innovation cycles, reduces external dependencies, and delivers interoperable, AI-centred defence systems at speed.

## **2. EU’s Legal Constraints**

The latest Joint Communication of 16 October 2025 — Preserving Peace: Defence Readiness Roadmap 2030 — reaffirms that Member States are, and will remain, sovereign in matters of national security and defence. They are responsible for defining capability objectives to ensure the readiness of their national armed forces, including for missions undertaken within NATO. National objectives and timelines are therefore sovereign choices, confirming that national security remains a Member State competence.

This intergovernmental logic, rather than a supranational defence union, is embedded in the Treaties. Article 42(2) TEU safeguards the specific character of certain Member States’ security and defence policies, including constitutional neutrality or non-alignment. Article 42(7) TEU establishes a mutual-assistance obligation in the event of armed aggression against a Member State, while respecting each country’s existing commitments, particularly within NATO. Article 222 TFEU (the solidarity clause) addresses joint responses to terrorist attacks or natural and man-made disasters without encroaching on national competences. Collectively, these provisions confirm the intergovernmental nature of the Common Security and Defence Policy (CSDP), which enhances collective security while preserving Member State primacy. They also delineate the CSDP’s scope: joint disarmament operations;

humanitarian and rescue missions; military advisory and assistance; conflict prevention; and post-conflict stabilisation.

Given these legal and constitutional constraints, a fully-fledged European army with integrated, interoperable command-and-control remains out of reach. The centre of gravity thus shifts to the industrial domain, notably through the ReARm–Readiness 2030 package, which seeks to reduce fragmentation within the EU defence industrial base via targeted funding and joint purchasing.

### **3. USA’s Innovative Advantage**

This industrial pivot is best understood in comparative perspective—set against the benchmark of the United States’ defence industrial base, whose scale and organisation illustrate both the ambition and the gaps Europe must address.

The United States’ defence industrial base (DIB) is the world’s largest, comprising over 60,000 companies and 1.17 million employees, and dominated by five prime contractors—Lockheed Martin, RTX, General Dynamics, Boeing and Northrop Grumman—that account for roughly one third of DoD contracts and half of the revenue of the top 100 global defence firms. While underpinning US technological dominance, the DIB faces consolidation, supply-chain and workforce challenges that the 2023 National Defense Industrial Strategy seeks to address through supply-chain resilience, workforce development and more flexible acquisition. According to SIPRI, the US delivered about 43% of global major arms exports in 2020–2024, many to Europe—an interdependence that is deepening as AI-enabled defence ecosystems increasingly rely on tools from large US technology companies. Crucially, America’s enduring “innovative advantage” is not scale alone but a distinctive capacity for “system-of-systems integration” — the first and defining step that turns scientific advances into military innovation by setting architectures, stewarding interfaces and interoperability, and orchestrating trade-offs across heterogeneous platforms. This “systems approach” to warfare has deep roots and is explicitly framed as the key initial step in transformation in Eugene Gholz’s “America’s Innovative Advantage: Systems Integration in the U.S. Defense Industry”.

That advantage is “institutionalised” in a diversified organisational landscape—Federally Funded Research and Development Centres (FFRDCs) such as Aerospace Corporation, MITRE and Johns Hopkins APL; specialised government laboratories; and primes—paired with governance that separates “architecture/system integration”

from “production” to preserve independence and trust. The classic case is the 1959 TRW investigation, which led to spinning off Space Technology Laboratories into the independent Aerospace Corporation, thereby insulating technical direction from production conflicts of interest and pioneering an advisory model later replicated across FFRDCs and UARCs.

Within this model, “independent advisors” maintain credibility by promising not to compete for production, safeguarding proprietary information, and offering equal access—features that foster high-quality, objective advice and enable rigorous interface stewardship across complex networks. At the same time, lack of bias and trust are protected by keeping prime contractors’ systems-integration roles at arm’s length; where primes act as integrators, customers reasonably fear biased trade-off analyses. Hence the emphasis on independent SI houses and FFRDCs in defining network standards, interfaces and requirements.

Performance in this ecosystem is assessed through “technical awareness” (continuous scanning of state-of-the-art subsystems; access to contractor and academic expertise; making cross-component trade-offs), “project-management discipline” (accurate schedules, realistic technical goals, and minimized transaction costs across many actors), and “customer understanding” (deep knowledge of service doctrine and operational practice). These metrics—long embedded in the US system—become even more salient with unmanned systems and network-centric operations. Finally, the US innovation model leverages “pluralist competition” among integrators (FFRDCs, UARCs, and for-profit SI houses) to stress-test architectures and mitigate organisational bias—an arrangement aligned with broader American “clash-of-ideas” governance and particularly valuable for network-centric warfare.

This design—-independent integration, rigorous interface stewardship and conflict-of-interest safeguards—underpins the United States’ ability to absorb new technologies quickly and at scale.

#### **4. Defence Tech in the EU**

The EDTIB, by contrast, remains fragmented after decades of under-investment. In 2024, EU defence expenditure reached €343 billion—around 2.5 times less than US spending (circa €864 billion)—with a substantial share of EU procurement sourced from the US. The 2024 European Defence Industrial Strategy (EDIS) and the European Defence Industry Programme (EDIP) aim to strengthen industrial sovereignty, promote collaborative procurement and prioritise a “Buy European” approach. The European

Parliament supports close EU–US cooperation but underscores that EU programmes must primarily reinforce the EDTIB and increase strategic autonomy. Quantified collective targets for 2030 include: intra-EU defence trade at or above 35% of the EU market; at least 50% of national procurement budgets directed to the EDTIB (rising to 60% by 2035); and 40% of equipment acquisitions conducted collaboratively—measures designed to create a more cohesive, resilient internal market for defence.

EU instruments are expanding to support this shift. The European Defence Fund (EDF) has become the EU’s third-largest defence R&D investor. With relatively limited outlays, ASAP and EDIRPA have helped address critical shortfalls and leveraged over €12 billion in additional public–private investment. Once adopted, EDIP will add tools for capability delivery, including flagships such as European Defence Projects of Common Interest (EDPCIs) and Structures for European Armament Projects (SEAP). Activation of the national escape clause has provided additional fiscal space to 16 Member States to raise defence spending. The Security Action for Europe (SAFE) has been fully subscribed by 19 Member States, committing its €150 billion envelope. Following the mid-term review of cohesion policy, Member States and regions may reprogramme cohesion funds toward defence-relevant investments—including military mobility—with higher flexibility and pre-/co-financing rates; regions adjacent to Ukraine, Russia and Belarus will receive targeted support.

This industrial turn echoes Mario Draghi’s “Report on the Future of European Competitiveness”, which argues that without a strong industrial and technological base, Europe cannot ensure either its security or its autonomy. Identifying defence as an area where fragmentation and under-investment threaten both security and competitiveness, the report urges the EU to treat defence as a strategic industry backed by EU-level financing, long-term programmes and Single Market rules. A robust, innovative industrial base rooted in the EU is simultaneously an engine of growth, given market size, employment potential and spill-overs. Efforts to close capability gaps should become an opportunity for the EDTIB to enhance competitiveness, deepen cooperation and accelerate innovation—benefiting start-ups, scale-ups, SMEs and mid-caps, as well as regional economies and smaller Member States.

Innovation is central to defence readiness. Disruptive technologies, rapid testing and integration, and agile engagement with the tech community are essential for modern warfare. EU funding will therefore stimulate R&D and innovative production, catalysing private investment and supporting dual-use start-ups, scale-ups, SMEs and mid-caps; simplified procurement pathways for younger firms should be considered.

The cohesion policy mid-term review incentivises reprogramming toward critical technologies and capability enhancement. The future EU Competitiveness Fund will focus on novel technologies and disruptive solutions from new tech actors, while the next Horizon Europe — especially the European Innovation Council—will back deep-tech from research to scale-up, including defence applications. The forthcoming European Defence Transformation Roadmap will propose mechanisms to boost innovation with industry — particularly scale-ups and SMEs—driven by greater agility, speed and risk-taking. Europe must remain ahead of the defence-tech curve, notably in AI, and reinforce investment in critical systems—drones, satellites, command-and-control and a secure European cloud—where AI will be decisive.

## 5. The Way Ahead

Recent national strategies reinforce this trajectory. Italy's Ministry of Defence "Documento Programmatico Pluriennale 2025–2027" underscores the rapid advance of technology, the expanding role of unmanned systems across all operational domains, and the opportunities and challenges posed by integrating AI and other emerging technologies to enhance efficiency, precision and resilience in complex, multi-domain operations. The United Kingdom's Strategic Defence Review prioritises technological innovation—AI, autonomy (including drones), cyber operations and digital integration via architectures such as the Digital Targeting Web—paired with accelerated procurement through the new UK Defence Innovation (UKDI) agency, compressing development cycles from years to months. A recent UK–Palantir strategic partnership aims to unlock roughly 1.5 billion in defence-AI and dual-use innovation—illustrative of the competitive pace at which the EU must position itself.

In parallel, European defence innovation can no longer be assessed solely through traditional procurement. As Ricardo González argues in "Militarising Big Tech: The Rise of Silicon Valley's Digital Defence Industry" (2023), major digital platforms—Amazon, Microsoft, Google, Palantir and others—are increasingly co-designing command, surveillance and AI systems for militaries. Although AI is currently applied in military contexts, it does not achieve full autonomy. Its development focuses on planning and logistics, cyber warfare—including sabotage, espionage, hacking, and information operations—and, most controversially, weapons targeting. This intensifies enduring concerns about transparency and accountability identified by Ashley Deeks

in “The Double Black Box”, which interrogates how to ensure democratic oversight, legality and effectiveness in the use of AI within national-security processes.

Set against Ashley Deeks’s warning that AI intensifies a “double black box” of opacity in national-security decision-making — where consequential choices are least transparent, and accountability can erode — John Yoo advances a contrasting claim: that attempts to pre-emptively ban or heavily constrain robotics and cyber weapons are misguided and counterproductive. In Yoo’s analysis, these technologies leverage real-time information and communications to increase precision, reduce casualties and overall destructiveness, and may actually create more opportunities to settle disputes with less force; categorical bans would perversely push states back toward more indiscriminate, higher-cost methods of warfare and are unlikely to succeed given realist incentives in the international system.

## **6. Governance Model and Conclusion**

Against this backdrop, governance must keep pace with technology. The priority is “rule-of-law-by-design”: (i) procurement frameworks that embed transparency, competition and security-of-supply while operationalising the “Buy European” principle in a WTO- and Treaty-compliant manner; (ii) interoperable technical standards, secure data-sharing and lifecycle cyber-resilience across supply chains; (iii) AI assurance regimes—testing, evaluation, verification and validation, audit trails and human-in-the-loop controls—aligned with fundamental-rights safeguards; (iv) oversight and accountability through parliamentary scrutiny, independent supervisory bodies and effective remedies; and (v) export-control compliance and due diligence consistent with CFSP commitments, cohesion objectives and sustainable sourcing.

In conclusion, acceleration is both necessary and underway—principally through cooperation and procurement—while debates persist around a robust “Buy European” principle, including elements reflected in Germany’s rearmament-related procurement reforms. Stabilised public demand is drawing unprecedented private capital into Europe’s defence-tech sector: venture investment has surged since Russia’s full-scale invasion of Ukraine, with companies raising about €2.4 billion since early 2022 (including €1.4 billion in the first seven months of this year), up from €30 million in 2020 and €150 million in 2021. The task ahead is to sustain this momentum while ensuring that accountability and Treaty compliance govern arms trade, cohesion and

the sustainability of sourcing—so that speed, decisiveness and legality advance together.

## Bibliography

Council of the European Union. (2025). *Final compromise text of the Regulation establishing the European Defence Industry Programme (EDIP) (Document 14814/25)*. Brussels: Council of the European Union.

Council of the European Union. (2025). *EDIP—general provisions, legal bases and objectives (Budget 2025–2027; Ukraine Support Instrument)*. Brussels: Council of the European Union.

Council of the European Union. (2025). *EDIP—security-of-supply toolbox and crisis activation (alerts, preventive action, crisis termination)*. Brussels: Council of the European Union.

Deeks, A. (n.d.). *The double black box: AI, accountability, and national security*. [Book].

Draghi, M. (2024). *Report on the future of European competitiveness*. Brussels: European Commission.

European Commission. (2024, March). *Proposal for a Regulation establishing the European Defence Industry Programme (EDIP)*. Brussels: European Commission.

European Commission. (2025, March). *White Paper for European Defence – Readiness 2030 and the ReArm Europe/Readiness 2030 package*. Brussels: European Commission.

European Commission. (2023–2024). *European Defence Fund work programmes and awards (selected calls)*. Brussels: European Commission.

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2025, October 16). *Preserving peace – Defence Readiness Roadmap 2030*. Brussels: European External Action Service.

European Union. (2009). *Directive 2009/81/EC on the coordination of procedures for the award of certain works, supply and service contracts in the fields of defence and security*. Official Journal of the European Union.

European Union. (Consolidated version). *Treaty on European Union; Treaty on the Functioning of the European Union* (selected provisions: Art. 42 TEU; Arts. 107, 114, 173, 212, 322, 346 TFEU).

Gholz, E. (n.d.). *America's innovative advantage: Systems integration in the U.S. defense industry*. [Paper].

González, R. (2023). *Militarising Big Tech: The rise of Silicon Valley's digital defence industry*. [Working paper].

HM Government. (2025). *Strategic Defence Review (SDR)*. London: Cabinet Office.

Ministero della Difesa. (2025). *Documento programmatico pluriennale della Difesa 2025–2027 (DPP)*. Rome: Governo Italiano.

Roos, G. (2025, November). *The industrial age returns: Is Europe ready?* London: Chatham House – International Affairs Think Tank.

SIPRI. (2025). *Trends in international arms transfers, 2024*. Stockholm International Peace Research Institute.

U.S. Department of Defense. (2023). *National Defense Industrial Strategy*. Washington, DC: Office of the Secretary of Defense.

Yoo, J. (2017). Embracing the machines: Rationalist law of war for autonomous weapons and cyber warfare. *California Law Review*, 105, 443–516.