

Commanding Sovereignty: Comparative Public Law of Defence Contracts and Capability Maturity

Original article

Received: 2026-06-29

Revised: 2026-07-27

Accepted: 2026-08-03

Final review: 2026-08-01

Peer review: 2026-07-15

Double blind

Keywords:

comparative public law,
defence procurement, defence
contracts, technological
sovereignty, capability
sovereignty.

This work is licensed under the
Creative Commons
Attribution-NonCommercial-
NoDerivatives 4.0 License

GAIE Christophe^{1,2, A-F}

[ORCID !\[\]\(3342c215b2a8b663596a81468d5dc314_img.jpg\) 0000-0002-8252-5278](https://orcid.org/0000-0002-8252-5278)

Langlois-Berthelot Jean^{3, D}

[ORCID !\[\]\(1f56542a42e2413e44a2b2023033aa2e_img.jpg\) 0009-0001-2397-5930](https://orcid.org/0009-0001-2397-5930)

A - Research concept and design, B - Collection and/or assembly of data,
C - Data analysis and interpretation, D - Writing the article, E - Critical revision of the
article, F - Final approval of the article

¹Assistance publique - Hôpitaux de Paris French Paris Hospitals,
France

²Laboratoire Magellan CNRS Université Lyon 3, France

³Invited Professor au Center for Advanced Studies
University of Palermo, Italy

Abstract

Objectives: The article proposes a comparative public law theory of defence procurement based on the concept of capability sovereignty. The main objective is to show that defence contracts are no longer merely instruments of acquisition, but legal architectures through which the state governs dependence, technological maturity, operational availability, and future options. It aims to demonstrate how formal state ownership can easily mask material operational captivity in an era where sovereignty is lost through proprietary lock-in, software dependence, or inaccessible source code.

Results: Analysis of Article 346 TFEU, Directive 2009/81/EC, and the 2025 SAFE/EDIP frameworks reveals that public law has transitioned from enforcing security exceptions to proactively enabling industrial readiness. Comparing French, EU, US, and NATO frameworks demonstrates that modern defence sovereignty is increasingly compromised by contractual, proprietary lock-ins and supply chain obfuscation rather than treaties or war. To mitigate these long-term risks across software, data, and modification rights, this article introduces a Sovereign Contract Audit Matrix.

Conclusions: The findings argue that the relevant question is no longer whether sovereignty is national, European, transatlantic, or contractual, but at which level legal arrangements maximize the state's effective freedom of action. By defining capability sovereignty as the legally, industrially, and technologically organized capacity to act without excessive dependence or delay, the article concludes that managing these contractual frameworks is essential to maintaining true strategic control during a crisis.

1. Introduction: Sovereignty Is Also Lost Through Contracts

Public law has traditionally understood defence sovereignty through three categories: sovereign competence, security exception and secrecy. These categories remain necessary. No theory of defence procurement can ignore the constitutional location of military decision, the specific protection of essential security interests, or the need to protect classified information.

Yet these categories are now insufficient. In an environment shaped by the war in Ukraine, shortage of critical components, software-defined capabilities, artificial intelligence, cyber dependence, space infrastructure, cloud architectures, data rights and industrial mobilisation, a state may remain formally sovereign while becoming materially dependent (Hellberg, 2026). It may retain the legal power to decide, while lacking the technical, industrial and contractual means to execute the decision. This gap between formal sovereignty and effective sovereignty is now the central blind spot of defence procurement law.

Defence procurement is usually analysed as a specialised branch of public procurement: a regime for defence and security contracts, adapted procedures, exceptions for essential security interests, specific rules on security of information and security of supply, and particular constraints linked to strategic goods. This view is correct but incomplete.

The real object of the defence contract has changed. A defence contract is no longer only the administrative instrument by which the state acquires equipment, works or services. It is a legal device for organising the state's future ability to understand, maintain, adapt, reconfigure and use a capability.

The problem is therefore not simply whether the state may derogate from ordinary competition rules. The deeper problem is whether public law still allows the state to preserve freedom of action in a technologically unstable environment. A contract for drones, cloud infrastructure, command and control software, simulation systems, cyber tools, battlefield connectivity, intelligence processing or space services never concerns only an object.

It allocates access rights, maintenance obligations, source-code rights, data ownership, update powers, supply-chain risks, interface standards, sub-contracting controls, security obligations, intellectual property, export constraints, audit capacities and rights of modification. It determines not only what the state buys, but what the state will later be able to do. The defence contract is therefore an operator of sovereignty. It may increase state freedom of action, but it may also reduce it. A legally impeccable tender can create a long-term dependence. A cheap offer can generate strategic captivity. A highly mature technology can be sovereignly weak if it is closed, unmodifiable and dependent on a foreign supplier. Conversely, a less mature system may have greater sovereign value if it preserves access, learning, modularity, reversibility and public control. The legal issue is not only the regularity of the procedure. It is the strategic trajectory produced by the contractual arrangement.

This transformation requires a shift in legal reasoning. The question is no longer: under what conditions may the state protect sovereignty against the market? It is: how can public procurement law produce effective sovereignty within markets, alliances, technological ecosystems and industrial interdependence? Sovereignty is no longer only a vertical legal competence. It is also a dynamic property of a system composed of public authorities, prime

contractors, software architectures, standards, suppliers, research organisations, financial instruments, industrial bottlenecks and operational deadlines.

Recent EU law makes this shift explicit. Directive 2009/81/EC aimed to coordinate procurement procedures in the defence and security sectors while taking their specific characteristics into account. Article 346 TFEU, in turn, allows Member States to take measures necessary to protect their essential security interests. As noted by academic and institutional literature, this mechanism was traditionally interpreted to provide legal certainty and limit the potential for abuse of the security exemption (European Parliament & Council, 2009; European Commission, 2006; Perrotto, 2023; European Commission, 2026).

Yet the 2025 instruments change the scale of the problem. The SAFE Regulation establishes a loan-based instrument to reinforce the European defence industry (Council of the European Union, 2025). The EDIP Regulation creates a European Defence Industry Programme and a framework of measures to ensure timely availability and supply of defence products (European Parliament & Council, 2025). This shift toward central mechanisms for financing through institutions represents an operational move towards enabling the Union's strategic autonomy via common purchasing models (Marin, 2026). The Joint White Paper for European Defence Readiness 2030 sets a readiness agenda (EDR2030, 2025), while the Defence Readiness Omnibus proposes to remove bottlenecks in procurement, permitting, reporting and cross-border cooperation (Omnibus, 2025).

The legal meaning of this evolution is considerable. EU defence law is no longer only a law of market opening and exception control. It is becoming a law of industrial readiness, security of supply and capability acceleration. This does not mean that the Union has become a federal defence state. It means that defence sovereignty is now distributed among several legal levels: national authorities, EU funding instruments, NATO standards, industrial consortia, private platforms, supply chains and software ecosystems. Comparative public law must therefore ask where freedom of action is actually produced.

This article defends a simple claim: defence procurement law should be reconstructed as a law of capability sovereignty. Capability sovereignty refers to the institutional, technical and industrial processes of a state or political community to acquire, maintain, alter, and use critical capabilities free from excessive dependence, within a timeframe not unduly constrained by crisis conditions, and while maintaining strategic control.

The concept does not replace existing legal categories. It reorganises them. Article 346 TFEU becomes a rigorous protection clause rather than a rhetorical escape route. Directive 2009/81/EC becomes a competition framework for sensitive capabilities rather than a normalisation tool detached from strategy. French public procurement law becomes an instrument for structuring long-term dependence. EDIP and SAFE become legal mechanisms for European capability scaling. US and NATO innovation frameworks become laboratories for agility and adoption, but also warnings against uncontrolled private dependence.

The argument proceeds in six steps. First, it distinguishes formal sovereignty, industrial sovereignty, technological sovereignty and capability sovereignty. Secondly, it rereads defence contracts as legal architectures of dependence. Thirdly, it analyses the European shift from procurement regulation to industrial readiness. Fourthly, it compares four models of defence

acquisition: French, European, American and NATO. Fifthly, it proposes a legal matrix for assessing the sovereign value of a defence contract. Finally, contemporary public law must become a legal framework for dependencies, not just for competencies.

2. From Sovereignty as Competence to Sovereignty as Capability

Traditional legal definitions of sovereignty are built around competency. All forms of sovereign authority involve deciding, directing, creating laws, enforcing laws, collecting taxes, deploying forces and protecting. Furthermore, the military's significant authority reinforces its position of expedited treatment when it comes to sovereignty. Traditional definitions of sovereignty and the military's ability to use extreme violence in limited geographical areas increase the need for procurement law to recognize the need for modified use of regular market rules in the defence sector. This need will be made even more critical by the transition from ordinary defence funding to urgent defence purchasing secondary to responses to immediate geopolitical crises (Chrzyński, 2023).

Yet competence is not capability. A State may have some classified information but rely on a foreign cloud service, proprietary model or otherwise inaccessible component or update process. In such a case, the state remains legally sovereign, but it has become operationally dependent upon another entity.

This distinction requires a more precise vocabulary:

- **Formal sovereignty** is the legal power to make a decision. It was historically understood from the standpoint of a single, top-down authority of a state as a unitary entity. Recently, formal sovereignty has been increasingly transformed by the requirement to comply with multi-layered national and international governance frameworks (Vercauteren, 2014).
- **Industrial sovereignty** is the ability to produce or secure industrial inputs required for production. In many cases, industrial sovereignty will attempt to relocate key phases in the manufacturing process toward providing countries with strategic autonomy for areas of high sensitivity, such as military, energy, and communication industries. All of this requires some effort to be made to evaluate and quantify the risks versus the benefits associated with each component and function in order to minimize the ramifications of disruption to their supply chains and reduce their overall risk when faced with unintended consequences due to a geopolitical conflict (Hérault, 2021).
- **Technological sovereignty** is the ability to understand, control, modify and develop the key technologies that support capabilities or operations. It is critical that technological sovereignty be understood not as an absolute economic self-sufficiency but as an active and relational ability to avoid structural dependencies while remaining actively engaged in global technological ecosystems (March & Schieferdecker, 2023).
- **Capability sovereignty** is the ability to transform these elements into operational freedom of action over time. This is the point where legal control, industrial base, technological comprehension, logistic support and operational availability come together. In the digital age, capability sovereignty is structurally challenged by hyper-connected global infrastructures and cross-border digital technologies and cross-border digital technologies (Timmers, 2024).

While the four concepts are connected, they are not interchangeable. One can have formal sovereignty without industrial sovereignty and one can have industrial sovereignty without technological sovereignty if the production of goods relies on intellectual property developed abroad or the use of foreign manufactured components or an outside definition of standard. One can attain technological sovereignty (in a research laboratory environment) without having capability sovereignty, if the system cannot be developed, verified, maintained, funded, installed or supported outside of the lab. Of all these concepts, capability sovereignty is the most difficult to establish, because it requires one to ask whether a political decision can still be executed under duress.

In order to have this level of autonomy, architectural frameworks need to be established that proactively incorporate cyber-resilience and secure digital data flows from the outset and secure the flow of digital data from the outset while avoiding full dependence on jurisdictions outside of information ecosystems. With the flow of big data and artificial intelligence, this will require a comprehensive operating and regulatory framework that combines comprehensive cybersecurity with effective data protection to safeguard high-priority national resources (Kaczmarek et al., 2024a). In addition, a supporting resilient defensive posture based on "sovereignty by design" within the acquisition process must exist. Specifically, fiscal risk intelligence must be embedded into all regional defence-digital strategies. This would help ensure that financial pipelines, supply-chain vulnerabilities, and the hyper-connected software infrastructures supporting these capabilities remain transparent and protected from adversarial leverage (Bierecki et al., 2026).

The contract is the mechanism through which these types of sovereignty are converted into legally enforceable duties. Contracts can ensure access to source code, establish escrow arrangements, require open interfaces, control the use of subcontractors, provide for security of supply, distribute intellectual property, set out maintenance rights, protect data portability, allow public audits, allow for incremental upgrades, establish deadlines for delivery, and set out the procedures for producing in the event of a crisis.

A theory of capability sovereignty therefore changes the legal reading of defence procurement. The legal value of a contract is not exhausted by compliance with procedure. A defence contract is not only valid or invalid, competitive or non-competitive, transparent or secret. It is also enabling or disabling. It preserves or destroys options. It reduces or increases dependence. It accelerates or slows adaptation. It produces or prevents learning. It gives the state time, or it consumes time.

This argument does not abolish the rule of law. On the contrary, it strengthens it. If sovereignty is invoked too easily, it becomes a pretext for opacity, protectionism or administrative comfort. Article 346 TFEU illustrates the danger. It permits Member States to protect essential security interests, but it cannot be used as a general exemption from EU law. The Court of Justice has repeatedly treated security exceptions as provisions requiring justification, necessity and proportionality (European Commission, 2006; Court of Justice of the European Union, 2008).

A capability-sovereignty approach does not invite lazy derogation. It requires a more demanding demonstration: what exact dependence would ordinary procurement create? Which function would become unmaintainable? Which information would be exposed? Which supply chain would be compromised? Which future option would be lost?

This systematic defence review must focus on cyber resilience and strong data protection; both of which highlight potential threats to structural freedom of action through vulnerabilities in algorithms and data manipulation (Kaczmarek et al, 2024b).

This method also avoids the opposite error: reducing defence procurement to competition for competition's sake. Competition may strengthen sovereignty when it prevents captivity to an incumbent supplier, reveals alternatives, disciplines prices and forces technical transparency. But competition may weaken sovereignty when award criteria ignore long-term lock-in, software dependence, operational deadlines, data control, critical sub-contracting or security of supply. The right legal question is not whether competition is good or bad. It is whether the competitive arrangement preserves the state's future freedom of action.

The same reasoning applies to technological maturity. In defence acquisition, maturity is often associated with readiness levels, proven performance, certification, integration and operational reliability. These are indispensable. But maturity should not be confused with sovereignty. An off-the-shelf system may be technically mature and sovereignly weak. A national prototype may be sovereignly interesting and operationally immature. A European consortium may increase scale while reducing clarity of responsibility. A US or NATO-compatible standard may improve interoperability while generating dependence on external update cycles. Capability sovereignty therefore requires not one measure, but a matrix.

The practical conclusion is clear. Public lawyers, procurement officers, engineers, operational planners and industrial strategists must evaluate defence contracts as trajectories. What does the contract allow the state to do in one year, five years and ten years? What happens if the supplier fails? What happens if export authorisations are withdrawn? What happens if a component becomes unavailable? What happens if the operational doctrine changes? What happens if a software vulnerability appears during war? What happens if the state must produce, repair or modify at speed? The law of defence contracts must become a law of these questions.

To illustrate this idea, take an example of proprietary lock-in. An analysis of recent major procurement programmes demonstrates that mere asset ownership no longer guarantees operational freedom of action. The case of the American fifth-generation F-35 fighter jet, deployed by several European militaries, is the archetype of this shift (Langford, 2025). The aircraft is structurally dependent on a centralised IT infrastructure for logistics and maintenance known as ODIN (Operational Data Integrated Network). Acquirer states, while formally owning their fleets, cannot plan a mission or perform deep maintenance without their aircraft data being routed back to servers managed by the American prime contractor. The state owns the physical "shell," but capability sovereignty escapes it, legally transferred by contract to the operator of the software infrastructure.

Similarly, the deployment of Storm Shadow / Scalp cruise missiles highlights this gap (Bellais, 2022): the formal political competence to donate these weapons to a third party (Ukraine) faced contractual and regulatory barriers for months (specifically US ITAR regulations) due to the presence of foreign critical sub-components and proprietary mapping data indispensable to the targeting system.

3. Defence Contracts as Legal Architectures of Dependence

A defence contract is often presented as an acquisition instrument. This description is too narrow. A modern defence contract is an architecture of dependence. It defines how the state depends, on whom, for what, for how long, under which conditions, and with which exit options. In strategic sectors, the object purchased matters less than the structure of dependence created around it. A platform contract may allocate property over a physical system while leaving the decisive software layer outside public control (Wydler, 2014). A maintenance contract may give the supplier a quasi-monopoly over operational availability. A cloud or data contract may transfer the centre of gravity from equipment to access rights. An artificial-intelligence contract may make the state dependent on datasets, model updates, evaluation methods and audit rights. A simulation contract may appear pedagogical while structuring the way future officers perceive the battlefield. A cyber contract may create dependence on proprietary detection logic. A drone contract may be less about airframes than batteries, chips, communications, navigation, counter-jamming, payload interfaces, software updates and repair chains.

This is why the doctrine of the public contract must be connected to a doctrine of strategic systems. In ordinary procurement, the contract is often evaluated through price, technical merit, deadlines, compliance and performance. In defence procurement, these elements remain necessary but are insufficient. The public buyer must ask whether the contract gives the state a living capability or a frozen asset. It must ask whether performance is reproducible in wartime, whether maintenance is possible under sanctions, whether the system can be adapted to new threats, whether data can be transferred, whether sub-contractors are controlled, and whether the state can still act if the original supplier becomes unavailable.

The concept of security of supply already moves in this direction. Directive 2009/81/EC recognises that defence and security procurement may require guarantees concerning supply chains, maintenance, spare parts, crisis response and classified information (European Parliament & Council, 2009). French public procurement law contains specific provisions for defence and security contracts, including security of information, security of supply and controls over sub-contracting (French Republic, 2019). These rules are essential. But they should be understood not as isolated safeguards, but as elements of a general legal theory of dependence.

Intellectual property is a decisive example. Public authorities often accept restrictive intellectual property arrangements because they reduce immediate cost, accelerate delivery or reflect market practice. In defence, such arrangements can become strategic vulnerabilities. If the state cannot access technical documentation, reproduce parts, audit code, modify software, train personnel, transfer data or permit a third party to maintain the system, ownership of the equipment becomes secondary. The state may own the physical asset while lacking effective control over the capability. The same applies to software and data. A software-defined capability is never finished. It evolves through patches, updates, modules, interfaces and data flows (McQuade et al., 2019). A contract that does not organise public rights over these elements risks freezing the state into a technological path chosen by the supplier. In artificial intelligence, the issue is even sharper. Data provenance, model evaluation, adversarial robustness, explainability, auditability and update rights are not peripheral technical points. They define whether the state understands and controls the decision-support system it deploys.

Sub-contracting is another central issue. Defence prime contractors often rely on complex supply chains. The legal relationship between the public buyer and the prime contractor may not reveal the true points of dependence (Paulus, 2025). Critical components may be produced abroad. Software modules may come from third parties. Export controls may affect availability. Industrial bottlenecks may lie several levels below the main contract. Public law must therefore look beyond the first contractual layer. The sovereign value of a contract depends on the visibility and controllability of the chain behind it.

Time must also be treated as a legal variable. In peacetime procurement, delay is often treated as an administrative inconvenience, a financial risk or a performance issue. In defence, delay can destroy sovereignty. If the legal procedure is incompatible with the tempo of technological change or with the urgency of the threat, the state may obtain a lawful capability too late. The 2025 Defence Readiness Omnibus explicitly recognises this problem by seeking to remove bottlenecks in procurement, permitting, reporting and cross-border cooperation (Omnibus, 2025). The point is not to abolish legal control, but to align legal time with strategic time.

Capability sovereignty therefore does not mean that every defence contract must be national, closed or secret. It means that every critical defence contract should contain an explicit theory of dependence. Some dependencies are acceptable. Some are even desirable. Interoperability with allies is a dependence, but it may increase freedom of action. European pooling is a dependence, but it may create scale that no state can achieve alone. Reliance on a commercial technology may accelerate adoption. The legal question is whether the dependence is visible, reversible, proportionate, governable and strategically justified.

The digitization of the battlefield shifts the core of the defence contract from physical asset acquisition to service subscriptions (Cloud computing, satellite connectivity, and AI models). The conflict in Ukraine exposed the strategic vulnerability of these new contractual links with non-traditional private tech actors. The Ukrainian military, heavily reliant on SpaceX's Starlink satellite network for command-and-control and drone guidance, saw its access unilaterally restricted during major offensive operations by a private corporate decision (Aiken et al., 2025).

This event demonstrates that a standard commercial service contract—devoid of state requisition clauses, absolute continuity-of-service guarantees in wartime, or structural data portability—amounts to an act of strategic alienation. Capability sovereignty requires public procurement law to engineer permanent code-access guarantees, native interoperability protocols, and software escrow mechanisms that can be triggered immediately if a breach of strategic trust occurs.

4. The European Shift: From Exception Control to Defence-Industrial Readiness

EU defence procurement law has long been structured around a tension. On the one hand, the Union seeks to limit fragmentation, protectionism and abusive exclusion of competition. On the other hand, defence is tied to national security, classified information, military capability and state survival.

Directive 2009/81/EC was adopted to create a specialised procurement regime for defence and sensitive security contracts. Article 346 TFEU remains the constitutional safety valve for essential security interests. The Commission's interpretative approach

has consistently sought to prevent Article 346 from becoming a general opt-out (European Commission, 2006; European Commission, 2026). This approach was legally coherent. Without discipline, the invocation of sovereignty can conceal industrial protection, administrative inertia or political favouritism. The Court of Justice has therefore required Member States to justify reliance on security derogations. In cases such as *Commission v Italy* and *InsTiimi*, the Court made clear that defence-sensitive contexts do not automatically remove procurement from the scope of EU law (Court of Justice of the European Union, 2008; Court of Justice of the European Union, 2012). Sovereignty must be demonstrated, not merely asserted.

Yet the post-2022 strategic environment has changed the function of EU defence law. The Union is no longer concerned only with opening defence markets. It is concerned with whether Europe can produce, procure and supply enough defence products in time. The shift is visible in the White Paper for European Defence Readiness 2030, which frames readiness as a matter of deterrence, capability gaps, industrial mobilisation and financing (EDR2030, 2025). It is visible in SAFE, which uses Article 122 TFEU to establish a loan instrument for reinforcing the European defence industry (Council of the European Union, 2025). It is visible in EDIP, which creates a programme and a framework of measures to ensure timely availability and supply of defence products (European Parliament & Council, 2025). It is also visible in the Defence Readiness Omnibus, which targets administrative and regulatory bottlenecks.

The legal consequence is decisive. EU defence law is becoming a law of readiness. Competition remains important, but it is no longer the only organising principle. Security of supply, joint procurement, industrial scaling, common projects, access to finance, eligibility rules, Ukraine's integration into the European defence-industrial base and simplification of procedures are now part of the legal grammar. The Union is not merely regulating procurement. It is shaping the industrial conditions under which procurement can produce military effects.

This raises a new problem for public law. European integration can either increase or decrease capability sovereignty. It increases sovereignty when it aggregates demand, reduces fragmentation, secures supply chains, supports production capacity, creates interoperable standards and avoids wasteful duplication. It decreases sovereignty when it produces slow compromises, unclear responsibilities, industrial bargaining, excessive dependence on non-European components or legal uncertainty over eligibility and control. The level of integration is not sovereign in itself. Its sovereign value depends on the capabilities and options it creates. The subsidiarity question must therefore be reformulated. Traditional subsidiarity asks whether action should be taken at EU level or Member State level. Capability subsidiarity asks where a given capability can be controlled, sustained, modified and deployed most effectively. Nuclear deterrence, national command authority, intelligence sources and certain cryptographic functions may require national control. Ammunition production, air defence, drones, critical components, logistics, space services and cyber resilience may benefit from European scale. Interoperability, standards, deterrence posture and operational compatibility may require NATO alignment. The legal problem is not ideological. It is functional: what level best preserves freedom of action?

The EDIP and SAFE instruments should be judged by this criterion. Their importance lies not only in money, but in the legal structuring of time, demand, supply and eligibility. SAFE is significant because it mobilises EU borrowing capacity for defence investment and encourages joint procurement. EDIP is significant because it tries to create a more structural European defence-industrial framework.

The EPRS briefing on EU joint defence procurement notes that collaborative procurement has remained below collective targets, which shows that legal and financial instruments must overcome a persistent gap between political declarations and procurement behaviour (Tothova, 2026). The IAI analysis of EDIP similarly emphasises that EDIP's budget is modest but that its framework could become scalable after 2028 (Murgia & Marrone, 2026).

This confirms the central thesis. Defence sovereignty is now partly a matter of legal engineering. It is not enough to proclaim strategic autonomy. Public law must design the contractual, financial and institutional mechanisms that make autonomy executable. A public-law theory of capability sovereignty therefore treats EU law neither as a threat in itself nor as a solution in itself. It treats EU law as one possible architecture for governing dependence.

This fundamental pivot of EU defence law toward "industrial readiness" has materialized through unprecedented emergency legal instruments. The ASAP (Act in Support of Ammunition Production) initiative, structurally scaled up by the 2025 EDIP (European Defence Industry Programme) regulation, perfectly illustrates this mutation (Lóránt, 2025). Historically, EU law strictly prohibited or heavily restricted direct subsidies to national defence industries to prevent market distortions.

Today, the Union actively deploys financial leverage to directly fund the scaling of production lines for gunpowder and 155mm shells leveraging manufacturers like Nexter or Rheinmetall (Blockmans & Fiott, 2026; Schnitzler, 2024). Crucially, these legal frameworks introduce "priority-rated orders" into European law, granting the legal authority to mandate that military production takes precedence over commercial contracts on the factory floor. EU public law no longer merely regulates market opening; it increasingly shapes the legal conditions for industrial speed and readiness in crisis scenarios.

5. Comparative Models: France, the European Union, the United States and NATO

Comparative public law helps avoid a false alternative between national sovereignty and European integration. Defence contracts are governed by different legal cultures, institutional histories and industrial structures. Four models are particularly useful: the French state-strategist model, the European integration model, the American agile-acquisition model and the NATO rapid-adoption model. The French model is based on the state as strategist. Defence procurement is linked to military programming, the Direction générale de l'armement, long-term relations with prime contractors, the defence industrial and technological base, and a strong understanding of sovereign functions. The Code de la commande publique provides a specific regime for defence and security contracts, while the 2024-2030 Military Programming Law sets the financial and capability trajectory of the armed forces (French Republic, 2019; French Republic, 2023).

The advantage of this model is coherence. The state can align doctrine, industrial policy, procurement, secrecy and operational requirements. It can preserve critical competences and maintain continuity in strategic sectors. The weakness of the French model is the risk

of rigidity. Strategic coherence can become procedural heaviness. Long relationships with major industrial actors can become dependence. Detailed specifications can slow adoption of dual-use technologies. Programme logic may absorb tanks, aircraft, submarines or missiles better than software, drones, cyber tools, artificial intelligence or command-and-control simulation. The state-strategist model is strong when the problem is long-cycle sovereign equipment. It is weaker when the problem is rapid adaptation to fast-moving commercial technology.

The French Army's SCORPION programme (Magnuson, 2022; Revue Fantassins, 2025), featuring the Griffon and Jaguar armored vehicles, perfectly illustrates the strengths and limits of this state-strategist model. It is a remarkable success of doctrinal and contractual coherence, establishing a unified collaborative combat information system developed hand-in-hand with the DGA (Direction Général de l'Armement, or Directorate General of Armaments in English). However, its heavy contractual governance, inherited from a tradition of major programs spread over fifteen years, struggles legally to integrate "short-loop" dual-use and low-cost innovations (such as commercial micro-drones). The obsolescence cycles of these digital technologies are measured in months, not decades, running faster than traditional administrative programming timelines.

The European model is based on sovereignty through integration. The Union does not command armies in the same way as a state, but it has regulatory power, market power, budgetary instruments and the ability to structure industrial cooperation. The EDIP and SAFE instruments show that the Union is trying to move from coordination to industrial mobilisation (European Parliament & Council, 2025; SAFE, 2025). The advantage of this model is scale. Many defence problems exceed national industrial capacity. Joint procurement, common standards and coordinated financing can reduce fragmentation and increase bargaining power. The weakness of the European model is dilution. A European project may be legally elaborate but strategically slow. Divergent threat perceptions, national industrial interests and procurement calendars can reduce effectiveness. An integrated project can produce political compromise instead of operational clarity. European sovereignty is therefore not automatic. It must be measured by its effect on availability, maintainability, supply security and time-to-field.

The multinational Eurodrone programme (Kunertova, 2019) highlights how complex European defence cooperation can lead to institutional paralysis. Managed by OCCAR under the just return principle, the contract transformed into a vehicle for industrial bargaining rather than optimised engineering. Diverging national requirements, specifically Germany's demand for a heavy twin engine system for domestic airspace versus France's preference for a lighter, cost-effective expeditionary platform, increased the project's weight, cost and development timeline.. Consequently, this rigid framework has delayed delivery beyond 2030, threatening to field a platform that is technologically obsolete upon arrival.

The American model is based on acquisition pluralism and ecosystem mobilisation. US defence acquisition law includes classic procurement, but also instruments designed to accelerate experimentation and attract non-traditional contractors. The Department of Defence Other Transactions Guide, updated in 2023 and made available in revised form in 2025, presents Other Transactions as flexible instruments outside standard procurement

contracts, grants or cooperative agreements, especially for research and prototyping (U.S. Department of Defence, 2025).

The Adaptive Acquisition Framework and the Software Acquisition Pathway recognise that software-intensive systems require iterative development, continuous delivery and different governance from traditional hardware programmes (Defence Acquisition University, 2026). The strength of the American model is speed and technological depth. It can connect defence needs to venture capital, start-ups, universities and commercial platforms. It can prototype quickly and absorb dual-use innovation. The weakness is dependence on private architectures. Agility can become outsourcing. If the state loses audit rights, software control, data access or architectural understanding, rapid acquisition may produce rapid captivity. The American model teaches Europe that procurement law must diversify instruments. It also warns that legal flexibility without public technical mastery can weaken sovereignty.

The NATO model is not a procurement state model. It is an adoption and interoperability model. NATO seeks to accelerate the transition from innovation to allied use, strengthen interoperability and connect industry with operational needs. DIANA and NATO's rapid adoption agenda illustrate this orientation (NATO, 2025; NATO, 2026). The value of the NATO model lies in adoption speed, allied standards and operational relevance. Its limit is that it does not solve the problem of national or European industrial sovereignty. NATO can help capabilities circulate; it does not necessarily ensure that a particular state controls the underlying technology. These four models show that capability sovereignty cannot be reduced to ownership, origin or legal competence. France offers coherence but risks slowness.

Europe offers scale but risks dilution. The United States offers agility but risks private dependence. NATO offers interoperability but not full control. A mature public law of defence contracts must combine these lessons. It must preserve sovereign control where necessary, Europeanise where scale is decisive, use agile instruments where technology requires speed, and align with NATO where interoperability is operationally indispensable.

6. A Legal Matrix for Capability Sovereignty

This section details a very concrete approach to making capability sovereignty real. It provides an explicit risk-assessment toolkit to verify long-term reliance dimensions before entering into a binding contract. The approach relies on a matrix that helps public buyers identify operational captivity before a deal is signed through a simple list of questions. This structural oversight shifts the procurement process from analysing the immediate price and performance to analysing systemic dependence with a rigorous method. The method relies on the following matrix that is intended as a legal and strategic assessment tool for defence contracts. It does not replace legality review, financial analysis or technical evaluation. It complements them by identifying the dependence profile of a contract.

Table 1. Legal and strategic assessment matrix for capability sovereignty

Criterion	Legal question	Clauses and instruments to examine
Control	Does the state understand and audit the critical architecture?	Technical documentation, audit rights, interface access, transparency obligations, control of critical sub-contractors.
Reversibility	Can the state exit the contract without losing the capability?	Migration clauses, open formats, data transfer, escrow, continuity plans, third-party maintenance rights.
Maintainability	Can the capability be sustained in crisis?	Through-life support, spare parts, repair rights, training, local competences, crisis stocks.
Adaptability	Can the system evolve quickly when threats change?	Incremental lots, modular architecture, upgrade clauses, experimentation, framework agreements.
Interoperability	Does allied integration preserve critical control?	Standards, interfaces, security of information, NATO or EU dependencies, certification rules.
Security of supply	Are critical inputs available under stress?	Component origin, sub-supply mapping, stock obligations, continuity plans, industrial ramp-up duties.
Data and code	Who controls data, models and software?	Intellectual property, licences, source-code access, algorithmic audit, data portability.
Time	Is the legal procedure compatible with the threat tempo?	Urgency tools, joint procurement, off-the-shelf purchase, prototype pathways, simplified procedures.
Financial resilience	Does the contract preserve long-term options?	Price revision, inflation clauses, option lots, termination rights, cost of switching, upgrade financing.
Strategic effect	Does the contract increase freedom of action?	Capability gap analysis, operational availability, doctrine fit, crisis-use assumptions, risk allocation.

Source: Author's own elaboration

This matrix changes the interpretation of existing law. Article 346 TFEU should remain exceptional, but the capability-sovereignty approach makes its use more rigorous. A Member State should not merely invoke defence sensitivity. It should demonstrate the precise dependence that ordinary procurement would create: exposure of classified information, loss of maintenance control, dependence on unavailable components, impossibility of rapid modification, or compromise of essential operational functions.

Capability sovereignty therefore strengthens proportionality analysis instead of bypassing it. Directive 2009/81/EC should be read as a framework for disciplined sensitivity. It allows defence-specific procurement while limiting arbitrary closure. It should not be treated as an enemy of sovereignty. Properly used, it can protect sovereignty by forcing the public buyer to define requirements, justify restrictions and organise security of supply.

The decisive point is the quality of the award criteria and performance clauses. Price and immediate technical performance must be complemented by maintainability, reversibility, data control, supply security and adaptability. French public procurement law already provides relevant tools, but they must be used at the right stage. The definition of need is not a neutral administrative step.

In defence, to define the need is to define the acceptable dependence profile. If the buyer defines only the immediate performance requirement, it may lose control over architecture. The legal analysis of dependence must therefore be integrated upstream, before the tender documents freeze the wrong questions. EDIP and SAFE should be evaluated in the same way. Their value is not reducible to budget. They can create capability sovereignty if they finance projects that improve European supply security, common standards, industrial depth and crisis production. They can fail if they merely accelerate fragmented purchases or subsidise systems without control over components, data and maintenance.

European funding should therefore be tied to dependence analysis, not only to eligibility criteria. The American and NATO models enrich the matrix. The American lesson is that different technological maturities require different legal instruments. Software, drones, cyber

tools and AI cannot always be purchased through long linear programmes. Prototype agreements, incremental acquisition, continuous delivery and experimentation are necessary. The NATO lesson is that adoption is a legal problem. Innovation has no strategic value if it cannot cross the valley between demonstration and operational use.

7. Toward a Public Law of Dependencies

Capability sovereignty leads to a broader doctrinal proposition: contemporary public law must become a law of dependencies. The modern state no longer commands only through hierarchy, ownership and regulation. It acts within systems that only partly controls: networks, platforms, supply chains, standards, cloud infrastructures, industrial ecosystems, alliances, financial instruments and data architectures.

Public law must therefore organise the dependencies that make public power executable. In defence procurement, this proposition has three consequences. First, legality must include trajectory. A contract is not only assessed at signature. It creates long-term effects. Legal analysis should therefore consider lock-in, real duration, exit costs, modification rights, maintenance dependencies and future loss of options. Secondly, sovereignty must not be confused with the nationality of the supplier. A domestic supplier can produce opaque proprietary dependence. An allied or European supplier can sometimes offer more transparency, modularity and reversibility. Origin matters, but control matters more. Thirdly, capability maturity should become part of the most economically advantageous tender.

The best offer is not only cost-effective, technically compliant and capable of delivering immediate performance. It must also be sustainable, modifiable, auditable, secure in supply and resilient over time. This approach avoids two errors. The first is the sovereignist illusion: the belief that the state recovers power by withdrawing from markets, Europe or alliances. For most contemporary technologies, autarky is impossible. The second is the integrationist illusion: the belief that the European scale automatically produces sovereignty. Integration is sovereign only when it increases effective freedom of action.

In Europe, the operation of defence supply chains illustrates this paradigm shift particularly clearly. Strategic autonomy is increasingly understood not as complete independence but as the management of multiple and varying degrees of dependence. Research on the EU defence industry demonstrates that European capabilities continue to rely on non-EU ownership structures, foreign suppliers and external sources for critical technologies and components (Kleczka et al., 2024). Consequently, the ownership of defence assets does not automatically confer autonomous action. A state may possess sophisticated military systems while remaining dependent on external actors for maintenance, spare parts, software updates and other essential inputs. Procurement law is therefore insufficient if it treats acquisition as a one-time transaction. It must instead assess the long-term trajectory of dependencies and incorporate considerations of reversibility, substitutability and control over critical supply chains in order to preserve effective freedom of action.

Between these illusions, capability sovereignty offers a practical criterion: identify which legal level best preserves control, maintenance, modification and use. The implications extend beyond procurement. They affect administrative law, competition law, intellectual-property law, export control, investment screening, data governance and public finance. A defence

capability is not a single legal object. It is a bundle of rights, obligations, technical interfaces, supply chains and operational assumptions.

Public law must learn to govern the bundle rather than the isolated contract. This also creates a research agenda. Comparative public lawyers should study intellectual property clauses in major defence contracts, reversibility obligations in military digital systems, audit rights for algorithmic capabilities, the legal treatment of software updates in operational systems, the interaction between EU eligibility rules and NATO interoperability, and the procurement consequences of industrial mobilisation. They should compare Other Transactions with European innovation procurement, analyse the legal status of prototype-to-production pathways, and investigate how public buyers evaluate technological maturity. Defence procurement law should become a science of public options.

8. Conclusion

Defence sovereignty can no longer be understood simply as a form of legal immunity. A state cannot be considered sovereign merely because it invokes Article 346 TFEU, closes its market to foreign companies, or designates a national supplier in support of strategic autonomy.. A state is sovereign if it can preserve its ability to perform functions, comprehend actions taken by others, sustain and change its status, and determine the course of action when faced with duress.

Defence contracts are now among the main sites where this sovereignty is produced or destroyed. They distribute control, structure dependence, allocate rights, define delays, organise maintenance, regulate access to data and shape future options. Defence procurement law must therefore be assessed by its capacity to preserve freedom of action, not only by its capacity to organise a regular procedure. The European transformation of defence law makes this conclusion unavoidable. EDIP, SAFE, the White Paper for European Defence Readiness 2030 and the Defence Readiness Omnibus show that sovereignty is increasingly a matter of financing, industrial cadence, security of supply, joint procurement and legal simplification.

The Union does not abolish national sovereignty, but it changes how sovereignty must be measured. Sovereignty is no longer only located in the decision. It is located in the ability to make the decision executable. Capability sovereignty names this transformation. It does not abolish existing legal categories. It gives them a stronger function. Article 346 TFEU becomes a rigorous protection clause. Directive 2009/81/EC becomes a framework for disciplined defence competition. French procurement law becomes a tool for governing dependence. EDIP and SAFE become instruments of European scaling. US and NATO models become laboratories for agility and adoption, but only if public control is preserved.

This paradigm shift is further reflected in the broader legislative pivot of European Union law toward defence-industrial mobilization and tangible crisis readiness. Unprecedented regulatory actions, such as the direct financial scaling of munitions production lines and the integration of emergency "priority-rated orders" on the factory floor, demonstrate that public law is no longer restricted to policing market competition. Instead, modern legal frameworks are being actively deployed to architect industrial velocity, ensuring that formal constitutional authority is backed by the immediate physical capacity to execute decisions under severe geopolitical duress.

In the 21st century, the sovereign state does not just make decisions, it retains its options. It understands when to defend, open up, Europeanise, partner with another nation, advance its position, try a new approach, and refuse to be dependent on another nation. The sovereign state distinguishes ownership from control, nationality from effective sovereignty, technological maturity from independence, and routine public procurement from strategic capability. The sovereign state recognizes that law is not separate from power, but rather, law is one of the frameworks of power that allows for its continued existence.

Sovereign states do not equate ownership with control; nationality with sovereignty; maturity with independence; or how often they engage in procurement as being effective from a long-term strategic perspective. They perceive that law will always be one of the structures that enable the existence of power because it will always be related to its source.

References

- Aiken, E., Allen, P., Baudin, A., Finkel, J., Fischer, E., Goldberg, L., Salam, J., & Schmollinger, R. (2025). *The technopolar world: Do tech companies matter as geopolitical actors?* Columbia University, School of International and Public Affairs.
- Bellais, R. (2022). MBDA's industrial model and European defence. *Defence and Peace Economics*, 33(7), 876–893. <https://doi.org/10.1080/10242694.2021.1926176>
- Bierecki, D., Czuryk, M., Gaie, C., & Langlois-Berthelot, J. (2026). Sovereignty by design: Embedding fiscal risk intelligence in Europe's defence-digital strategy. *Prawo i Więż*, 2026(1), 89–112. <https://doi.org/10.36128/priw.vi50.1741>
- Blockmans, S., & Fiott, D. (2026). *European defence projects of common interest: From concept to practice* (PE 775.284). European Parliament, Directorate-General for External Policies of the Union. <https://doi.org/10.2861/0345335>
- Chyrzyński, R. (2023). Programming and financing of development forces: The old and new approach on the basis of Poland's experience. *Defence Science Review*, 28–49. <https://doi.org/10.37055/pno/165876>
- Hellberg, R. (2026). Reconfiguring defence supply chains: Procurement dynamics, inter-organizational dependence, and resilience under geopolitical uncertainty. *Defence and Peace Economics*, 1–40. <https://doi.org/10.1080/10242694.2026.2655381>
- Hérault, P. (2021). *Strengthening sovereignty in the era of global value chains*. Institut Français des Relations Internationales.
- Kaczmarek, K., Karpiuk, M., & Melchior, C. (2024a). A holistic approach to cybersecurity and data protection in the age of artificial intelligence and big data. *Prawo i Więż*, 4(47), 104–122. <https://doi.org/10.36128/priw.vi50.907>
- Kaczmarek, K., Karpiuk, M., & Melchior, C. (2024b). Disinformation as a threat to state security. *Defence Science Review*, 20, 45–54. <https://doi.org/10.37055/pno/205780>
- Klecza, M., Vandercruysse, L., Buts, C., & Du Bois, C. (2024). The spectrum of strategic autonomy in EU defence supply chains. *Defence and Peace Economics*, 35(4), 427–447. <https://doi.org/10.1080/10242694.2023.2180588>
- Kunertova, D. (2019). *Military drones in Europe: The European defense market and the spread of military UAV technology*. Center for War Studies.
- Langford, C. (2025). Experts warn UK faces software dependency risks with F-35s. *UK Defence Journal*.

- Lóránt, S. (2025). Strengthening Europe's defence industrial base: Analysis of the EDIP framework. *Honvédségi Szemle*, 153(Special Issue 1), 25–39. <https://doi.org/10.35926/hdr.2025.1.3>
- Magnuson, S. (2022). Ally upgrades: France plots long-term Army modernization plans. *National Defense*, 107(826), 22–23.
- March, C., & Schieferdecker, I. (2023). Technological sovereignty as ability, not autarky. *International Studies Review*, 25(2), viad012. <https://doi.org/10.1093/isr/viad012>
- Marin, L. (2026). Common procurement in defence and the strategic autonomy of the Union: A first appraisal. In M. Butti, G. Corsetti, & A. Peychev (Eds.), *Reconfiguring Europe in a fractured global economy: The 2026 EMU Lab Florence report* (pp. 423–439). European University Institute.
- McQuade, J. M., Murray, R. M., & Defense Innovation Board. (2019). *Software is never done: Refactoring the acquisition code for competitive advantage*. Defense Innovation Board.
- Murgia, N., & Marrone, A. (2026). *The European Defence Industry Programme: The last piece of the EU defence puzzle?* Istituto Affari Internazionali.
- Paulus, A. (2025). *An Achilles heel of today's armed forces: Managing software supply chain risk in the military sector* (SWP Research Paper No. 6/2025). Stiftung Wissenschaft und Politik. <https://doi.org/10.18449/2025RP06>
- Perotto, G. (2023). The legal framework of the EU defence industry and the pursuit of strategic autonomy. *European Papers – A Journal on Law and Integration*, 2023(2), 475–486. <https://doi.org/10.15166/2499-8249/668>
- Revue Fantassins. (2025). *Fantassins No. 36: Le magazine d'information de l'infanterie*. Armée de Terre.
- Schnitzler, G. (2024). “Wartime economy”: From buzzword to reality? *Changes in European defence industrial strategies since February 2022*. Institut de Relations Internationales et Stratégiques.
- Timmers, P. (2024). Sovereignty in the digital age. In H. Werthner et al. (Eds.), *Introduction to digital humanism*. Springer. https://doi.org/10.1007/978-3-031-45304-5_36
- Tothova, L., Clapp, S., & European Parliamentary Research Service. (2026). *EU joint defence procurement* (Report PE 785.665). European Parliamentary Research Service.
- Vercauteren, P. (2014). Which state for which sovereignty? *Carta Internacional*, 9(2), 125–136. <https://doi.org/10.21539/2526-9038/v9n2a10>
- Wydler, V. (2014). *Gaining leverage over vendor lock to improve acquisition performance and cost efficiencies*. Defense Technical Information Center.

EU legal and policy documents

- Council of the European Union. (2025). *Council Regulation (EU) 2025/1106 of 27 May 2025 establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument*.
- Court of Justice of the European Union. (2008). *Case C-337/05, Commission v Italy, judgment of 8 April 2008*.
- Court of Justice of the European Union. (2012). *Case C-615/10, Insinööritoimisto InsTiimi Oy, judgment of 7 June 2012*.
- European Commission. (2006). *Interpretative Communication on the application of Article 296 of the Treaty in the field of defence procurement, COM(2006) 779 final, 7 December 2006*.

European Commission. (2025). *Defence Readiness Omnibus*.

European Commission. (2026). *Defence procurement*. Directorate-General for Defence Industry and Space.

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2025). *Joint White Paper for European Defence Readiness 2030, JOIN(2025) 120 final, 19 March 2025*.

European Parliament, & Council of the European Union. (2009). *Directive 2009/81/EC of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security*.

European Parliament, & Council of the European Union. (2025). *Regulation (EU) 2025/2643 of 16 December 2025 establishing the European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products*.

Other legal documents

French Republic. (2019). *French Public Procurement Code. Second Part, Book III: Provisions applicable to defence or security contracts, Articles L. 2300-1 to L. 2397-3*.

French Republic. (2023). *Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense. Journal Officiel de la République Française, No. 0177*.

Other official and institutional documents

Defense Acquisition University. (2026). *Adaptive Acquisition Framework: Software Acquisition Pathway*.

North Atlantic Treaty Organization. (2025). *Summary of NATO's Rapid Adoption Action Plan*.

North Atlantic Treaty Organization. (2026). *Defence Innovation Accelerator for the North Atlantic (DIANA)*.

U.S. Department of Defense. (2025). *Other Transactions Guide* (July 2023, revised public version 2025). Office of the Under Secretary of Defense for Acquisition and Sustainment.