Telecommunications at the heart of the new defence strategy

December 2025

Contents

1. Executive Summary

The transformation of conflicts and security architectures now places telecom operators at the heart of defence capabilities. Mobile networks, fibre optics, submarine cables, data centres and satellite constellations are no longer just civilian infrastructure: they form the digital backbone on which the command, intelligence, logistics, resilience, and continuity of the state depend. This shift is driven by three major dynamics.

1. Defence is becoming more reliant on civilian networks.

Tactical needs are rapidly expanding: real-time video, drones, tactical cloud, embedded AI, IoT sensors, distributed communications. Traditional military networks (TETRA/Tetrapol, microwave links, sovereign satcom) are reaching their limits. As a result, armed forces are increasingly relying on commercial infrastructure to handle this "mass of connectivity, as demonstrated in Ukraine, the Middle East and European programs (RRF, BOSNet, ESN). Consequently, operators are taking shared responsibility for sovereign communications, with obligations regarding availability, supervision, and hardening.

2. Telecommunications operators (telcos) are becoming strategic players, but their position remains fragile.

Their infrastructure (fibre optics, mobile sites, submarine cables, backbones, clouds) forms the core of critical communications. This integration expands their role to include functions similar to those of a sovereign operator: 24/7 supervision, cybersecurity, energy resilience, continuity of priority services. But this hybridisation also introduces vulnerabilities: non-European technological dependencies, increased cyber risks, fragmentation of national models, and the lack of a unified doctrine to ensure coexistence between civil and sovereign layers.

3. Europe is moving forward, but in a scattered way.

The United States has centralised governance (FirstNet), a dedicated spectrum and consistent federal oversight. Europe, on the other hand, remains fragmented: each country is developing its own critical architecture, standards and industrial partnerships.
The European Defence Fund is attempting to initiate convergence, but telcos still represent only a marginal share (<1% of budgets). This under-integration contrasts with the central role that telecoms infrastructure already plays in military operations.

The outcome is a strategic paradox.

Telcos provide speed, capacity, coverage, and innovation, but they are also becoming a new critical point of dependence for states. Digital sovereignty cannot be considered independently of commercial networks or their global supply chains.

Ultimately, telecom operators are now essential links in the chain of information power. The question is no longer whether they will be part of European defense, but under what conditions, with what level of public control, what degree of technological sovereignty, and according to what common doctrine.

The decade from 2025 to 2035 will be decisive: it will determine whether Europe transforms this dependence into a strategic advantage... or whether it allows a new point of structural fragility to develop.op.

2. Introduction

Modern warfare no longer relies solely on firepower, operational doctrines or traditional industrial capabilities: it now depends on a continuous, distributed and resilient digital foundation. In this model, telecom operators occupy an unexpected strategic position. Their infrastructure (mobile networks, fibre optics, data centres, submarine cables, cloud platforms and satellite capabilities) is becoming an essential component of military sovereignty and operational continuity.

For a long time, the contribution of telcos was limited to the field of public safety: emergency networks, traffic prioritisation, continuity of service in the event of a crisis. But recent conflicts, in Ukraine and the Middle East, have accelerated a structural shift: the same technological building blocks used for civil security are now being called upon to support tactical communications, command system resilience, threat detection, critical infrastructure protection and operational support. The boundary between security and defence is blurring. The role of operators now extends to the heart of the military ecosystem, where they are sought after as technology partners and no longer just as second-tier service providers.

This convergence is creating a two-way movement.

On the one hand, armed forces are increasingly relying on civilian capabilities that have become indispensable: 4G/5G, critical MCx networks, edge computing, LEO constellations, cloud security, cyber surveillance and 24/7 monitoring services. Traditional military networks (TETRA, Tetrapol, microwave links, dedicated satcom) are no longer sufficient to absorb the mass of connectivity generated by real-time video, drone swarms, distributed sensors and embedded AI.

On the other hand, operators are discovering a sovereign market with characteristics that are very different from their traditional consumer or B2B activities: multi-year contracts, resilience and availability requirements, increased state control, direct exposure to geopolitical risks and defence regulations.

At the same time, the strategic framework is evolving. NATO is explicitly expanding the scope of defence to include critical infrastructure, networks and civil resilience. European states are increasing their budgets, tightening NIS2 requirements, launching dedicated programmes (RRF, BDBOS, ESN, IRIS²) and seeking to structure their industrial base through the European Defence Fund. However, telecom operators remain only marginally integrated into these industrial policies, even though their networks form the backbone of distributed command and information superiority.

In this context, this white paper has three objectives

- To explain how operators are moving from the role of connectivity providers to that of sovereignty actors;
- • Compare American and European governance models in critical communications;
- • Analyse the economic and industrial implications of this evolution for telcos and for Europe.

The central issue can be summarized as follows: telcos have already become critical links in command, intelligence and resilience. The question is therefore no longer whether they will be part of European defence, but under what conditions, with what level of public control, what

degree of technological sovereignty, and according to what articulation among states, operators, and manufacturers.

3. From access provider to strategic player

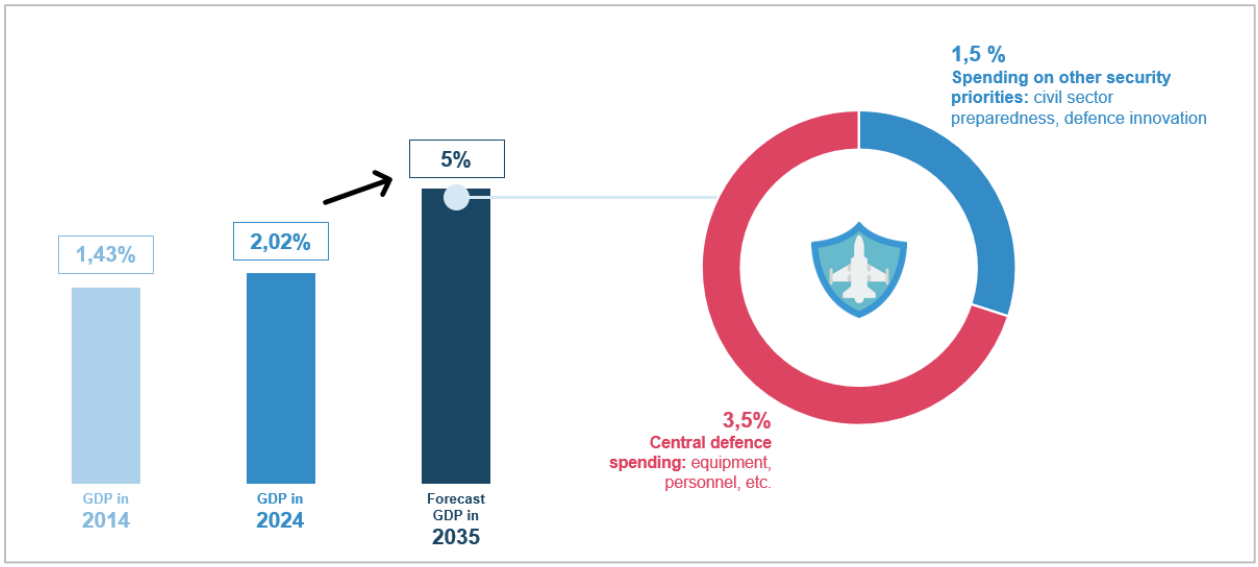
From civil connectivity to a defence issue

Historically, telecom operators were seen as mere access providers. Their role was limited to providing fixed and mobile connectivity for individuals and businesses, far removed from military issues. This separation no longer exists. Attacks on submarine cables, hybrid operations and geopolitical crises have revealed that civilian networks are now a critical component of state continuity. NATO's "Baltic Sentry" operation, focused on protecting damaged cables, illustrates this shift: telecoms are no longer peripheral, but strategic.

NATO expands defence to digital infrastructure

At the 2025 summit in The Hague, the Allies decided to increase defence and security spending to 5% of GDP by 2035. Of this total, 3.5% is dedicated to defence in the strict sense and up to 1.5% is targeted at protecting critical infrastructure, network defence, civil resilience, innovation and strengthening the defence industrial base.

This expansion explicitly includes digital infrastructure, cybersecurity and telecom networks within the Alliance's strategic scope. This development places operators at the heart of an unprecedented budgetary effort, with the prospect of rapid expansion of the European sovereign market.



Resilience and security: a new scope of responsibility

In this context, operators must ensure the continuity of critical communications, protect networks against attacks or jamming, and provide real-time monitoring for national authorities. ENISA reports show a significant increase in network attacks: 3.5% of incidents in 2022, 10% in 2023 and 8% in 2024. Telecoms are becoming both a strategic target and a defence asset.

Monitoring, detection and cybersecurity

Operators now play a key role in detecting anomalies, cyberattacks and influence operations. Their permanent monitoring capabilities provide visibility that the armed forces cannot replicate on their own. Some are even developing advanced cybersecurity offerings for government

agencies. In Norway, the "Bukleap" exercise, led by Telenor, brings together the military, public authorities and private companies to simulate cyberattacks on a national scale. This reflects a clear increase in responsibility.

An industrial pivot for national resilience

Operators have a wealth of infrastructure that the armed forces could not rebuild: national fibre networks, thousands of mobile sites, transnational backbones, submarine cables, data centres and distributed clouds. These assets have become indispensable for meeting rapidly growing tactical needs: real-time video, autonomous drones, tactical cloud, embedded AI and swarm sensors. Sovereign military networks are no longer sufficient to support this "mass of connectivity.

From service providers to co-architects of sovereignty

This repositioning is transforming the very nature of telcos' role. They no longer just provide connectivity services: they are involved in building national resilience, protecting critical infrastructure and ensuring the continuity of military operations. Their network expertise is becoming a key component of states' digital power.

This transition logically opens the following chapters: the structuring of governance models (part 7) and how Europe is attempting to further integrate operators into its industrial base via the European Defence Fund (part 8).

4. Why operators are getting involved in defence

An operational need that has become too massive for military networks alone

Today's armed forces generate a volume of data that is difficult for sovereign networks alone to handle: tactical videos, drone swarms, telemedicine, intelligence fusion, IoT sensors and the tactical cloud.

Civilian infrastructure (fibre, commercial 4G/5G, and LEO constellations) has become indispensable for maintaining command, coordination, and operational continuity. Ukraine has shown that without civilian networks, several critical functions would have collapsed.

In France, the Radio Network of the Future (RRF) illustrates this shift, relying on 4G/5G antennas from Orange and Bouygues Telecom.

This choice confronts states with a structural trade-off: rebuild very costly sovereign networks, or embrace a faster civil-military hybridization that requires security and resilience guarantees.

An industrial lever that cannot be replicated by the armed forces alone

Operators have a unique asset base: national fibre networks, tens of thousands of mobile sites, submarine cables, distributed data centres and transnational backbones.
No defence ministry can replicate this infrastructure. Relying on telcos is like benefiting from a "major programme" without bearing the full cost.

FirstNet in the United States and the RRF in France illustrate this model: massive public investment coupled with private sector operation.

This outsourcing provides immediate capacity but increases dependence on non-European supply chains, particularly for radio equipment, servers, network operating systems and certain cloud components.

The central issue then becomes effective control of critical data, in a context of non-European components and extraterritorial jurisdictions, such as the Cloud Act.

A strategic function at the heart of national resilience

Resilience is no longer theoretical: jamming, cyberattacks, sabotage of submarine cables and attacks on cellular infrastructure in Ukraine have shown that civilian networks are military targets.

Operators have teams and 24/7 monitoring centres that the armed forces cannot replicate in the short term.

NATO has formalised this in the NATO Warfighting Capstone Concept: "*civilian networks are now an integral part of military planning".*

This recognition places telcos as direct players in resilience, responsible for cyber hardening, continuous monitoring and interconnection with tactical networks.

A major economic opportunity in a growing sovereign market

For operators, the "defence and sovereignty" market is becoming a strategic vertical. Critical networks (RRF, ESN, BDBOS) mobilise budgets of €1 to €2 billion over 10 to 15 years, with performance obligations and enhanced state control.

Orange, Deutsche Telekom and Telefonica are repositioning themselves with dedicated defence and security divisions.

In 2025, Orange created its Defence & Security Division, which leverages its 45,000 km of terrestrial fibre, 450,000 km of jointly operated submarine cables, and satellite infrastructure to provide connectivity, cybersecurity and real-time analysis solutions. Deutsche Telekom is developing hybrid networks integrating fibre, satellite and 5G to ensure continuity of communications in civil and military environments, while Nokia is partnering with Kongsberg (a Norwegian public company specialising in defence) to deploy tactical 5G networks and prepare for the arrival of 6G for defence operations.

This move upmarket provides access to higher-value revenues than the traditional telecoms market but requires compliance with military standards for security and resilience, effectively excluding smaller or less capitalised players.

A strategic paradox: increased efficiency, increased dependence

Civil-military hybridisation increases deployment speed, reduces costs and increases available capacity. But it creates direct dependence on networks that are exposed to the vulnerabilities of the civil market: power failures, cyberattacks, saturation, disruptions to the industrial chain, or supplier unavailability.

The model is effective but fragile, and no European doctrine yet fully regulates this interdependence.

The challenge is no longer whether to integrate telcos into defence – they already are – but how to secure this integration through robust governance, consistent standards and clear separation between civilian and sovereign layers.

5. Cross-cutting themes: when telcos become defence players

5.1. Telcos as new "national security operators"

A role that goes beyond simple connectivity

Telecom operators are becoming central players in national security. Their networks, often more extensive and modernised than certain historical sovereign infrastructures, are gradually being integrated into critical government communications. This is not about pitting public and sovereign networks against each other – certain systems, such as Germany's TETRA, remain highly secure – but about recognising that commercial infrastructure is now an essential part of the national capability base.

This shift marks a structural change: connectivity is no longer a civil service, but an essential strategic capability. The priority, pre-emption and hardening mechanisms deployed on initially commercial networks bear witness to this.

In the United States, FirstNet is an integrated model; in Europe, equivalents exist (RRF, BOSNet, secure services in the United Kingdom), but in a fragmented context, without a common doctrine.

Civil-military hybridisation: increased responsibility

With this integration, operators' responsibilities are changing profoundly. They must now ensure complete national resilience: 24/7 supervision, proactive detection, cyber and physical hardening, coordination with security authorities. Managing submarine cables, data centres, network cores, and cloud platforms places them directly at the heart of digital sovereignty, yet their status and regulation often do not reflect these quasi-sovereign responsibilities.

A capacity lever... but a strategic dependency

For states, relying on telcos avoids costly and time-consuming deployment of sovereign infrastructure. But this strategy creates a major dependency: commercial networks remain exposed to vulnerabilities of the civilian market, including saturation, power outages, coordinated cyberattacks, logistical disruptions, and sabotage. The hybrid model enhances capabilities but relies on infrastructure not designed for high-intensity conflict or advanced electronic warfare.

This fragility is amplified by non-European technological dependencies: Asian radio equipment, American cloud computing, and components subject to extraterritorial regulations. The state therefore delegates a sovereign function to private actors whose technological chain depends on external powers. This is one of the structural dilemmas of the European model.

A model that is only viable under certain conditions

This model is sustainable only if several conditions are met: multi-operator redundancy, interoperability with tactical and satellite networks, massive hardening of network cores and sensitive sites, a strengthened regulatory framework and clear governance of priorities in emergencies. Without these safeguards, civil-military hybridisation can become a systemic risk rather than a capability advantage.

At the European level, the lack of standardization is a major obstacle. Each country is developing its own model, which limits NATO/EU interoperability and collective management of hybrid crises. Europe cannot claim to have a coherent defence without interoperable communications.

In this context, telcos have become essential partners in national security. But this strategic importance requires a political response: strengthening the resilience of critical telecom infrastructure, reducing technological dependencies, and building a coherent European framework for sovereign communications. Without this, operators risk becoming not a pillar but a potential breaking point for sovereignty.

Their role now goes beyond the technical: it determines the state's ability to communicate, command and act in all circumstances. Telcos have become an essential link in digital power, yet they can also become a "single point of failure" if governance does not evolve at the same pace.

5.2. The technological triptych: private 5G, edge computing and Satcom/NTN

The digital modernisation of armed forces increasingly relies on three complementary technical building blocks: private 5G, edge computing and Satcom/NTN satellite communications. Their combination shapes the way telecom operators contribute to military operations: controlled local connectivity, autonomous processing in degraded environments and continuity of command in the event of terrestrial network failure.

Private 5G: connecting and securing tactical operations

Private 5G offers controlled high-speed connectivity in areas of operation, suitable for critical uses such as tactical video, distributed sensors and autonomous systems. Experiments conducted by Nokia/LMT, Ericsson/Telia and the US Department of Defence (DoD) show a gradual replacement of less flexible proprietary solutions.

The DoD is currently the main investor in defence 5G, with approximately £400-500 million committed between 2020 and 2023. Applying a proportional extrapolation, with the DoD accounting for around half of global spending on emerging technologies, we arrive at an order of magnitude of around £1.4 billion for the global defence 5G market in 2023.

Driven by the modernisation of tactical communications and the digitisation of operations, this market is expected to grow rapidly. Assuming a CAGR of 22-24%, justified by increased military spending, the growing need for autonomous systems and the rise of 5G tactical networks, the global market could reach £4-4.5 billion by 2032. The segment is still limited in value, but it occupies an increasingly strategic position in next-generation military communications.

Edge computing: ensuring continuity in contested environments

Edge computing brings computing power closer to the units involved: vehicles, outposts, drones, autonomous sensors, to maintain critical functions even in the event of jamming, saturation, or the interruption of long-distance links. By distributing capabilities as close as possible to the field, it limits the impact of a central failure and enhances operational continuity.

For European operators, this development aligns with investments in distributed architectures. Edge computing provides a concrete response to degraded environments, but its implementation remains complex: multiple suppliers, integration constraints, enhanced cybersecurity requirements, and the difficulty of maintaining consistency in multi-stakeholder ecosystems.

Satcom/NTN: the ultimate in command continuity

Satellite solutions are the last line of resilience when terrestrial networks become unavailable. Europe is seeking to secure this capability through the IRIS² constellation, scheduled for 2030, with a total budget of around €10.6 billion over twelve years as part of a public-private partnership, a significant portion of which is dedicated to government and defence communications.

This European initiative is complemented by major national programmes: SpainSat NG I/II for Spain (over €2 billion), as well as Syracuse (France), Skynet (United Kingdom), SATCOMBw (Germany) and SICRAL (Italy), each costing between €1 billion and €3 billion per generation cycle.

When these investments are aggregated, the defence Satcom segment represents approximately €3.5 billion per year in Europe in 2025, with momentum likely to reach €7 to €7.5 billion by 2030. This growth, representing an average annual increase of around 15%, is driven by:

- The accumulation of programmes (new generation of national satellites + IRIS²) rather than simple "one-for-one" replacement;
- The structural increase in defence budgets in Europe since 2022;
- The increasing militarisation of satellite uses (tactical links, back-up for terrestrial networks, integration with 5G/NTN architectures).

On a global scale, if we consider that around a quarter of the global satellite communications market (with a total market value of around £30 billion) is directly related to defence and government uses, this leads to an order of magnitude of £7 billion for defence Satcom in 2025 and a scenario of around £14 billion in 2030, representing a similar growth rate of close to 15% per annum.

The acceleration in satellite investment reflects a structural change: the Satcom segment is becoming an essential sovereign capability, whereas previously it was merely a complement to terrestrial networks. The simultaneous rise of national programmes and IRIS² shows that Europe is seeking to secure an independent orbital chain, while aligning its capabilities with NATO standards.

This dynamic confirms that future architectures will be hybrid, combining 5G, edge and Satcom to ensure operational continuity in all circumstances.

A hybrid architecture offering opportunities... and new vulnerabilities

The combination of private 5G, edge computing, and Satcom forms a local, autonomous and resilient architecture suited to modern military operations. It automatically strengthens the role of telecom operators in tactical and strategic resilience. But it also introduces new constraints: complex integration, increased exposure to cyber risks, fragmented interfaces and dependence on supply chains that are often based outside Europe.

The challenge is therefore as much technological as it is strategic. As this architecture becomes the basis for distributed operations, the role of operators is evolving toward a more central position. For Europe, the question is how to regulate this hybridisation: whether to make it a lever for sovereignty or to allow additional dependence to take hold in an area that has become critical.

5.3. Digital sovereignty and critical infrastructure security

Sovereignty that now depends on telcos

Digital sovereignty has become a central defence issue in Europe. For European states, it is not about internalising everything but about guaranteeing three fundamental capabilities: deciding on their rules, choosing their technologies and suppliers without being subject to imposed dependencies, and maintaining continuity, i.e., ensuring the continuity of essential services even in the event of a geopolitical, cyber, or industrial shock.

This sovereignty increasingly relies on infrastructure operated by telecoms companies, which control a growing share of the state's networks, data and connectivity capabilities. They are becoming essential gateways for the continuity of state authority: if operators falter, government communications, security forces and military supply chains are now directly exposed.

Critical infrastructure under geopolitical pressure

Telecom operators occupy a strategic position: they control a large share of critical infrastructure, including terrestrial networks, submarine cables, Internet exchanges, data centres, satellites, 4G/5G network cores, and cloud platforms. More than 95% of European intercontinental traffic passes through submarine cables owned, co-financed, or operated by telcos, creating a major exposure in times of crisis. Within national borders, they also provide virtually all connectivity for government agencies, security forces and critical operators.

These assets are essential to the flow of sovereign data, government communications, the coordination of emergency services and, increasingly, the command and intelligence capabilities of the armed forces. A failure of a network core, the corruption of an Internet exchange point, or the cutting of an undersea cable can now directly affect the continuity of the state, as demonstrated by incidents in the Baltic Sea and attacks targeting landing stations in 2022–2023.

For governments, controlling these infrastructures means limiting technological and geopolitical dependencies. Debates over non-European 5G equipment, restrictions on certain suppliers, and data localisation requirements are evidence of this desire for greater control.

However, the reality remains fragile: a significant proportion of critical technologies, radio equipment, network software, cloud solutions and cybersecurity still come largely from non-European suppliers.

This vulnerability is exacerbated by the fact that these strategic infrastructures are operated by private operators who do not always control their own dependencies. Recent incidents – sabotage of cables in the Baltic Sea, hybrid attacks on landing stations, transcontinental outages – have shown that this exposure is very real. Telecoms companies are thus becoming, despite themselves, potential points of disruption for public authorities: a failure or external pressure can now directly affect sovereign and military communications.

The shift to mission-critical services: sovereignty in transition

Added to this is a major technological challenge: the rise of "Mission Critical" services defined by 3GPP (MCPTT, MCVideo, MCData). These services, which include priority communications, real-time tactical video, and sensitive data sharing, are now based on hardened 4G/5G infrastructures operated by telcos, gradually replacing the dedicated TETRA/Tetrapol networks historically under direct state control.

This shift transfers part of operational sovereignty to commercial and software architectures managed by private actors. The governance of critical communications has been profoundly transformed: states no longer have complete control over the technical layers that once guaranteed the autonomy of security forces and armies. Sovereign communications now rely on sensitive software platforms and sometimes on non-European cloud environments. The risk is no longer just that of failure but also that of technological dependence: updates, vulnerability management, prioritisation, cryptography, service availability.In response to these risks, Europe has launched several initiatives (trusted clouds, protection of submarine cables, 5G Toolbox, 6G programmes, cybersecurity funds). But the effort remains fragmented: each country is moving forward according to its own priorities and industrial alliances, preventing the emergence of a coherent European framework comparable to the American federal model. This fragmentation reduces the ability to pool investments, hinders interoperability and limits the creation of a genuine European industrial base for critical communications.

But this technical effort will not be enough: digital sovereignty is as much a political and industrial issue as it is an operational one. Without political harmonisation and a European industrial strategy, no amount of technical robustness can compensate for the structural dependencies that currently undermine sovereign communications.

As long as Europe relies on dispersed private infrastructure, opaque supply chains and non-EU technologies, it will remain exposed to systemic disruptions. In this context, telcos are becoming not only critical operators, but also potential points of disruption for public authorities: a failure, external pressure or supply disruption can now directly affect the state's ability to command, communicate and act.

5.4. Critical communications: Europe in transition, the United States in integration

Critical communications are entering a new era. TETRA and Tetrapol networks, long considered benchmarks for robustness and security, are now reaching their technical limits. They must now support uses that were previously impossible: real-time tactical video, multi-agency coordination, massive IoT flows, autonomous operations, and sensor fusion. This change is not a simple technological upgrade: it is profoundly transforming how states design their sovereign communications.

A transformation that repositions operators at the centre of sovereign functions

The gradual migration to MCx services (MCPTT, MCVideo, MCData) on commercial 4G/5G networks is redefining the role of operators. Sovereign communications are relying less and less on dedicated state infrastructure and increasingly on critical software layers operated over civilian networks. The consequence is direct: operators are becoming jointly responsible for sovereign capacity, whether in terms of availability, security, supervision or continuity of access.

The change is not only technical. It is institutional. Commercial networks, which are by nature shared and exposed to the vagaries of civilian traffic, global industrial dependencies and energy tensions, are not designed to absorb sovereign responsibilities on their own. The real debate is therefore not "should we use operators' networks?", but " ***can we guarantee operational sovereignty when the critical layer relies on private and shared infrastructure?"***

Two different paths: American centralisation, European plurality

The United States has opted for a centralised model with FirstNet: a single operator (AT&T), dedicated spectrum (Band 14), initial federal funding, and a uniform contractual framework. This model ensures national consistency and institutional simplification, but, as in Europe, it is based on a hardened commercial network. The difference lies more in governance than in technology.

Europe is following a different approach. There is no common doctrine, no harmonised spectrum, and no shared model.

France is moving forward with the RRF, Germany is modernising BOSNet while introducing critical 4G/5G capabilities, and the United Kingdom is restructuring its ESN. Each country is developing its own architecture and industrial ecosystem. This diversity complicates interoperability between Member States, slows operational convergence and creates strategic uncertainty in a context of cross-border hybrid crises.

Clear gains, risks still poorly addressed

The promise of MCx is real: greater capabilities, controlled costs, better sensor integration, and enhanced operational continuity. But each technological advantage also introduces new vulnerabilities.

What will happen when a disaster causes a massive influx of civilian traffic at the very moment when emergency teams need absolute priority? How can service continuity be guaranteed if a cyber breach or power outage affects the 5G core? How can digital sovereignty be ensured if some of the critical equipment, software or cloud services come from non-European players?

These questions are not theoretical. They are at the heart of the trade-offs that each country will face over the next five years.

A strategic challenge for the coming decade

Critical communications are becoming the backbone of distributed command, emergency response, armed forces coordination and civil resilience. They place operators at the centre of a sovereign function... but they also make states dependent on their infrastructure, their cybersecurity, and sometimes their own global technological dependencies.

Europe will have to choose between three paths: maintaining a fragmented sovereign approach, converging towards a form of centralisation inspired by the American model, or building a controlled hybridisation based on enhanced requirements for resilience, oversight and redundancy.

For the moment, no model stands out. And one question remains: ***how much sovereignty is a state prepared to delegate in order to gain capacity and speed?***

Beyond critical communications, the rise of drones is giving rise to a new field of capability in which telecommunications operators could play a key role: **the detection and management of low airspace**.

5.5. Telcos facing new threats: drones and countermeasures

Beyond critical communications, the rise of drones is creating a new capability field in which telecommunications players could play a structuring role: the detection, surveillance and management of low airspace.

The rapid rise of drones, whether civilian, commercial or military, has created a new theatre of operations. Long marginalized, low airspace has become a dense environment that is difficult to monitor and susceptible to malicious exploitation. Attacks on airports, critical infrastructure and military positions, particularly in Ukraine, have highlighted the limitations of current systems. States do not yet have robust, continuous and generalisable architectures to effectively control this airspace. In this context, telecommunications operators appear to be potential contributors to the detection and management of these threats.

Why control of low airspace is becoming a strategic issue for states

The proliferation of drones is profoundly reshaping the security balance. These systems are inexpensive, easy to deploy, and difficult to detect. They can be used for surveillance, sabotage, or the saturation of sensitive sites. Unlike traditional airspace, low airspace does not yet rely on large-scale integrated surveillance architectures.

Telecommunications networks are introducing a structural disruption. They are already densely deployed across the entire territory and offer continuous data collection and processing capabilities. By becoming spectrum sensors and distributed processing platforms, 4G and 5G networks can contribute to the detection, identification and tracking of low-altitude aerial threats. They complement conventional military systems without replacing them. For governments, the challenge is clear: to build a sovereign surveillance capability for low-altitude airspace using existing infrastructure integrated into security and defence architectures.

Mobile networks becoming spectrum sensors

Mobile infrastructure comprises a dense network of sensors already deployed on a national scale.

Each radio site offers unique visibility into the spectrum: emission variations, abnormal signals, remote commands, and the trajectories of connected drones.

This approach complements conventional radars, which are often less effective at detecting small, slow-moving targets flying at low altitude. Several European countries are already experimenting with "detection layers" based on existing networks, in partnership with operators and the defence industry.

In Germany, Deutsche Telekom, via the Droniq platform developed with civil air traffic control, is already using mobile networks for remote identification, tracking and management of drone trajectories as part of the European U-space system. These civil architectures foreshadow uses that can be transposed to the security and protection needs of critical infrastructure.

5G SA: a technical lever for the detection and management of low airspace

5G Standalone enhances this capability:

- more accurate location thanks to synchronised signals;
- high density of radio sites;
- slicing to isolate a surveillance function;
- native integration of IoT sensors or ground relays.

This increased responsibility also creates a risk: if mobile networks become essential for detection and neutralisation, they automatically become priority targets, particularly for hybrid operations aimed at blinding a defence system.

Experiments conducted by Nokia with several European authorities have shown that 5G networks, combined with edge computing and radio spectrum analysis, can contribute to the detection, identification and tracking of drones in the vicinity of sensitive infrastructure, complementing radars and optical sensors.

Europe still in the experimental stage

Europe is advancing in a piecemeal way. A few national initiatives are emerging, but there is still no common doctrine for integrating operators into anti-drone systems. The United States, Israel, and certain Asian countries have already incorporated these capabilities into their defence architectures and are investing in integrated platforms combining radar, radio, optics, 5G, and AI.

Europe is still exploring its options. Without coordination, it risks multiplying incompatible systems, making it difficult to manage cross-border threats or coordinate the protection of critical infrastructure.

As these capabilities grow in power, telecommunications networks are no longer just a means of connectivity but are becoming a component of situational awareness and territorial protection, effectively expanding the scope of operators' sovereign powers.

Control of low airspace is becoming a central aspect of digital and operational sovereignty, with operators playing an increasingly important role.

6. Governance, economic models and the strategic role of operators

Two political architectures shaping the role of telcos

The modernization of critical communications has accelerated in response to recent conflicts, but the American and European trajectories are grounded in opposing institutional foundations. In the United States, public security is under the control of a single federal agency that can impose national standards and mobilize massive budgets: the Department of Defence (DoD) spends more than $66 billion a year on IT and cyber activities. In Europe, internal security remains a strictly national prerogative, creating a mosaic of 27 policies, 27 historical networks, and 27 doctrines of use. This divergence directly shapes how telecom operators are integrated into critical communications ecosystems.

Multi-year contracts that redefine the relationship with the state

Sovereign partnerships are now part of a very long-term horizon. In the United States, the FirstNet model is the most emblematic example.

AT&T operates under a 25-year contract, combining $6.5 billion in initial federal funding and nearly $40 billion in investments to deploy and operate the national public safety network. In Europe, programmes such as RRF in France, BDBOS in Germany and ESN in the United Kingdom are based on similar commitments in terms

of availability, service continuity and state supervision. These mechanisms place the operator in a structural position that goes far beyond that of a simple capacity provider.

The American model: federal efficiency and assumed dependence

The creation of FirstNet reflects the American response to two decades of crises that exposed the fragmentation of emergency networks: 9/11, Katrina, and the California wildfires. The federal government opted for a centralised architecture, with reserved spectrum (Band 14), national governance, and a key operator: AT&T. The FirstNet contract provides exceptional visibility and enables the rapid industrialisation of a network covering 99% of the population. This approach maximises efficiency: immediate interoperability between agencies, pooling of investments, and strict priority and preemption mechanisms in crisis situations. But it also concentrates risks: a single operator becomes a systemic vulnerability in the event of a cyberattack or major failure.

The European model: national sovereignty, technological inertia and fragmentation

Europe approaches critical communications from a different heritage. Since the 1990s and 2000s, each Member State has financed its own TETRA or Tetrapol network, representing several tens of billions of euros in total. This strategic asset, robust but costly to renew, generates strong structural inertia. Russia's invasion of Ukraine has accelerated national efforts without creating continental convergence. France is banking on a sovereign architecture (RRF), Germany on TETRA-5G coexistence (BDBOS), and the United Kingdom on a difficult transition to a broadband network.

This fragmentation imposes high entry costs on European operators: each market functions as an autonomous ecosystem with its own standards, integrators and sovereignty requirements. It reduces economies of scale, limits the reproducibility of solutions and slows modernisation. This dispersion is precisely what the European Defence Fund (EDF) seeks to correct by stimulating transnational projects that gradually integrate operators.

Two different philosophies: centralise or disperse?

The American model is based on a logic of unification: a critical national network, a pivotal operator, federal governance. This approach promotes speed, technical consistency and the deep integration of telcos into sovereign missions. But it automatically concentrates resilience on a limited number of players, exposing the entire system to common vulnerabilities.

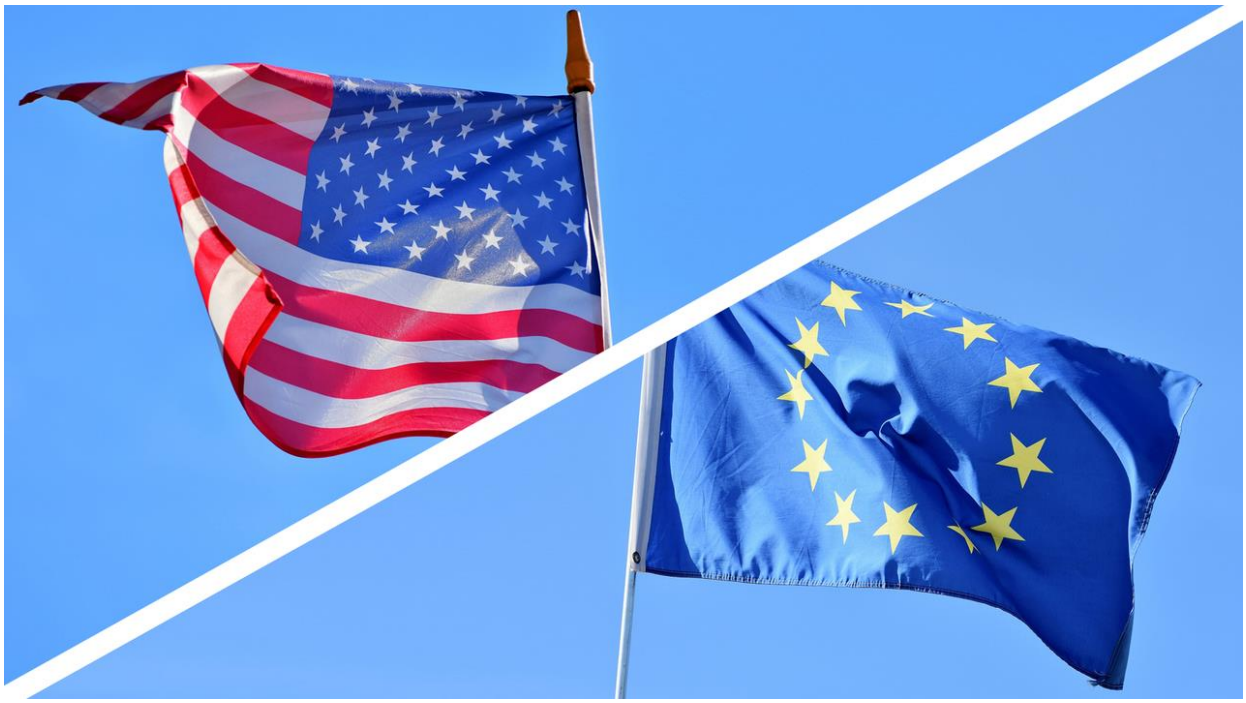
The European model takes the opposite approach: prioritising national sovereignty, preserving local industries and maintaining independent decision-making chains. This approach reduces the risk of centralised failure, but at the cost of slower, more expensive and more difficult to harmonise modernisation. Telecoms companies must adapt their solutions to 27 different markets, which dilutes investment and reduces speed of execution.

Which model will withstand the next digital crisis?

The challenge is not to determine which model is "best", but to understand their structural trade-offs.

- An attack targeting a pivotal operator would weaken the American model.
- Simultaneous destabilisation of several segments would weaken an overly dispersed European model.

Future crises (cyber, saturation, jamming, spectrum fragmentation, etc.) will test not only the technology, but above all the organisation of sovereign communications.



A gradual convergence around the role of telcos

Despite their historical differences, the two models are converging on one essential point: telecom operators are becoming indispensable to the continuity of military and civil operations. Whether through FirstNet, the RRF, BDBOS, or ESN, telcos are no longer peripheral service providers but key contributors to sovereign missions. This development paves the way for broader industrial restructuring, which will be analysed in the next section through the role of the European Defence Fund.

A structural repositioning towards sovereignty

The entry of telecom operators into the defence ecosystem is profoundly transforming their business model. As armed forces shift toward hybrid digital architectures combining sovereign capabilities and commercial infrastructure, operators are becoming major contributors to critical communications. This evolution is creating a new revenue stream distinct from traditional telecom markets: higher margins, multi-year commitments, enhanced resilience requirements and greater integration into state decision-making chains.

A move upmarket towards integrated critical solutions

This transformation is accompanied by a major evolution in the scope of services provided by operators. The sale of connectivity is gradually giving way to comprehensive solutions integrating 24/7 monitoring, cyber hardening, trusted cloud, edge computing tactics, multi-technology maintenance, GEO/LEO satellite services and traffic prioritisation mechanisms.

In the case of the RRF, Orange and Bouygues Telecom are now contributing to the very backbone of national command. This move upmarket allows operators to capture a greater share of value in a market where resilience, security and performance take precedence over volume.

A more integrated but more demanding defence ecosystem

The ecosystem no longer operates in silos: telecom operators now work closely with traditional defence manufacturers. Partnerships such as Vodafone-Airbus, BT-ESN and Telefonica-Indra

demonstrate the rise of complex arrangements in which operators contribute their infrastructure and network expertise, while manufacturers handle the integration of critical layers.

This close cooperation is accompanied by increased state involvement in governance, technological choices and sometimes even the strategic direction of operators, a sign of a market where margins and visibility are traded for a high degree of public oversight.

A long-term approach that brings telecoms and sovereignty closer together

Sovereign space and digital programs, such as IRIS² (more than €10 billion over twelve years), illustrate this enduring convergence among telecoms, space and defence. Operators involved in these projects gain access to long-term, stable and protected revenue streams, which are particularly valuable in a telecoms market facing competitive pressure and margin erosion. Secure communications and sovereign cloud solutions offer new growth opportunities in a sector seeking structural economic drivers.

An interdependence that will need to be structured by public governance

However, this development creates a new interdependence between states and private operators. By entrusting the latter with capabilities that affect the command, resilience, and continuity of military operations, states strengthen their digital sovereignty while exposing themselves to a technological and industrial dependence that only precise governance can control.

7. Europe is structuring its industrial base: the European Defence Fund (EDF)

A major budget, but still a marginal presence in telecoms

The European Defence Fund (EDF) has a budget of €7.3 billion for 2021-2027, of which around €4 billion has already been committed to 224 projects between 2021 and 2024. It is now the main tool for shaping the European defence industrial base.

In this context, telcos are involved in only 14 projects, with a combined budget of around €34 million, or less than 1% of the total financial volume. Their role remains limited, with telcos seen more as providers of technological building blocks than as genuine contributors to capabilities.

This participation is concentrated among a few players (Nokia, Ericsson, Telefonica, Telenor, Eutelsat, LMT) and in five areas: information superiority, cyber, tactical communications, space and disruptive technologies. The peak observed in 2024 around tactical 5G, secure communications and interoperability shows the beginnings of integration, but no operator is leading a strategic project. Europe has not yet defined a clear doctrine on the place of telecoms infrastructure in defence capabilities.

The dynamics of the EDF (new projects, rise of manufacturers, dual innovation) are progressing faster than the integration of telecoms, which are essential to the connectivity and resilience of modern operations.

Year	EDF budget (EUR)	# Projects	Development budget (EUR)	Research budget (EUR)	#Projects with Telcos	Estimated Telcos budget (EUR)
2021	1.2 billion	60	845 million	322 million	4	12.78 million
2022	832 million	41	514 million	317 million	1	2.4 million
2023	1.154 billion	61	850 million	304 million	1	0.51 million
2024	910 million	62	539 million	369 million	8	17.87 million

Why telcos remain on the sidelines of the EDF

Several structural obstacles explain this low presence.

The requirements of the EDF (multi-country consortia, industrial sovereignty, defence governance) are high, and operators must manage market pressure and the need for rapid returns on investment.

Industrial cultures differ profoundly:

- BITDs work on long-term, highly standardised programmes focused on sovereignty;
- Telecom operators favour agility, short cycles and CAPEX/OPEX optimisation.

Added to this are the lack of a clear business model for dual services, the difficulty of promoting highly specialised components on the consumer or B2B markets, and European fragmentation (regulatory, doctrinal, industrial) that prevents the emergence of pan-European solutions.

This fragmentation makes it impossible, at this stage, for a European equivalent of FirstNet to emerge, as each country has its own priorities, employment doctrines, and budget cycles.

What this situation reveals for Europe

The EU is investing heavily in dual innovation, but has not yet fully integrated its telecoms industry into this trajectory. The EDF aims to transform capabilities, but European defences remain dominated by traditional prime contractors, while telecoms operators appear to be occasional contributors rather than key players.

This discrepancy creates a paradox: Europe is aiming for strategic autonomy while underinvesting in the critical infrastructure (networks, cloud, edge, 5G/6G) that forms the backbone of modern warfare.

The risk is clear: long-term dependence on American technologies for digital capabilities and military connectivity.

A direct strategic impact on European sovereignty

In the short term, the limited integration of telcos limits the emergence of sovereign solutions in key areas: 5G tactical communications, defence edge, resilient networks, critical connectivity for drones, and hybrid space architectures.

In the medium term, the European Union risks missing out on the convergence of defence and telecoms, which is already underway in the United States, China, and Korea.

NATO is now encouraging the development of tactical MCx and 5G capabilities: if European telcos remain on the sidelines, Member States will depend on non-European ecosystems to meet these standards.

A still marginal but rapidly expanding market

Over the period 2021-2024, it is estimated that telcos' share of the European Defence Fund and the national defence budgets of the United Kingdom, France, Germany, Spain, and Italy will be around 1% (~0.8%-1.2%). By way of comparison, telcos accounted for approximately 3.2% to 3.5% of the defense budget in the United States, more than four times as much, despite a much larger total defence budget. This structural difference shows that operators are already considered important players in the pursuit of information superiority in the United States, which is not yet the case in Europe, where operators still play a secondary role.

Today, the amounts allocated to telecom operators in the European defense market remain low, and the share of contracts awarded to them remains marginal. However, we can expect the spending structure of European countries to evolve in the coming years to resemble that of the United States. The defence budgets of NATO member countries are expected to grow significantly in the coming years, in part as a result of the call by the administration of US President Donald Trump for member countries to invest 5% of their GDP in defence by 2035. In this context, the defence telcos market could reach nearly €18.2 billion by 2030, accounting for around 2.5% of European countries' defence budgets. The trajectory of the EDF and the various national defence budgets is already consistent with this trend.

Telcos-defence market (Europe) – EUR billion

Year	2024	2027	2030
Value	2.6	6.6	18.2
Period	**2021–2024**	**2024-2027**	**2027-2030**
CAGR %*	*11.4*	*37.1*	*40.1*

*Average annual growth rate

The geopolitical situation in Europe continues to exert strong pressure on defence and positions this sector as a major strategic issue. Several concrete initiatives illustrate this dynamic, such as the collaboration between Nokia and the German armed forces to develop tactical networks in 2025, and the Swedish armed forces' participation in Ericsson and Telia's 5G innovation programme, which aims to strengthen military communications and interoperability within NATO.

A clear conclusion: Europe is moving forward, but (too) slowly

The EDF is a major lever for structuring a modern defence industrial base. But the late integration of telecom players creates a strategic vulnerability: without progressive investment in digital infrastructure, Europe risks becoming permanently dependent on non-European ecosystems for sovereign communications.

The decade from 2025 to 2035 will be decisive. The question is no longer whether telecoms should become capability players, but ***how to effectively integrate them into European defence industrial policy***.

8. Strategic outlook and challenges

The analysis in the previous chapters shows a clear shift: telecom operators are no longer peripheral players in defence, but structural components of military power and digital sovereignty. Their infrastructure now forms the backdrop to modern operations: without networks, there is no real-time intelligence, distributed command or digitalised logistics. Telcos are thus becoming nerve centres of informational power and redefining their strategic role.

An unstable balance between efficiency and vulnerability

Civil-military hybridisation brings immediate gains in capacity and agility. It reduces costs and draws on innovations in the civil sector. Examples such as FirstNet in the United States, the RRF in France and critical German architectures show that such a model can reach a considerable scale, with millions of critical users integrated.

However, this approach also creates growing industrial and geopolitical dependence on private actors and technologies that are often non-European. Neither the hyper-centralised American model nor the fragmented European model offers a fully satisfactory solution at this stage.

European sovereignty still incomplete

Europe has launched numerous initiatives: 5G Toolbox, NIS2, IRIS², trusted cloud, 6G programmes, submarine cable protection, and the European Defence Fund. Despite their importance, these efforts do not yet constitute a coherent strategy. Critical communications are migrating to MCPTT, MCVideo and MCData services running on commercial 4G/5G networks, but software platforms, critical equipment, and cloud environments often remain non-European. The European telecom industrial base exists but has not yet been mobilised as a pillar of defence capability, particularly in EDF programmes, where the presence of telcos remains weak. This gap limits Europe's ability to align sovereignty, innovation, and technological autonomy.

Until Europe clarifies what truly needs to be sovereign – core networks, satellite segments, MCx platforms, combat cloud, cryptography, and supervision – and what can remain open to global interdependence, it will continue to build its defence architectures on a partially controlled foundation. The risk is not theoretical: a disruption in access to a hyperscaler, the blacklisting of a critical supplier, or the sabotage of infrastructure could be enough to degrade command and coordination capabilities.

Telcos, from service providers to co-architects of defence

For operators, entering the sovereign domain represents a major economic opportunity but also a change in nature. They are moving from

- from a commodity model, focused on selling connectivity in volume,
- to a role as co-architects of critical systems, engaged in multi-year contracts with obligations to deliver results, resilience and security at the highest level.

This evolution is part of the transformation of the sovereign economic model described in part 6: higher margins, long contracts, increased responsibilities.

This repositioning opens up opportunities for growth in managed services, private 5G, edge, satcom, cybersecurity and critical communications, but in return requires:

- alignment with security standards close to those of the military
- acceptance of increased state control over certain components
- the ability to invest in hardening, redundancy and 24/7 supervision on a scale greater than the commercial market.

For European telcos, the central question becomes: do they want to and can they take on this role of "quasi-sovereign operators"? Those who choose this path will have to accept a more restrictive framework, but will have access to more stable revenue streams and a unique strategic position in defence value chains.

What course should Europe take?

Between the lines, this document highlights a series of structural choices for European decision-makers:

- Should each Member State continue to develop its own critical communications model, or should there be a minimum level of European convergence on certain technical foundations (MCx, 5G/NTN, combat cloud)?
- To what extent should dependence on non-European technologies in sovereign networks be accepted, and in which segments should a European industrial base be an absolute priority?
- Which service and infrastructure areas should be considered non-outsourceable, even to trusted national operators?
- What role should telcos play in crisis governance: simply executing public orders, or acting as strategic partners integrated into planning and operations centres?

These questions have yet to be definitively answered, but they lie at the heart of the strategic challenges of the next ten years. If Europe does not quickly develop a clear doctrine on the relationship between defence and telecoms, it risks being forced to accept the architectures that are put in place rather than choosing them.

Ultimately, there are two sides to the coin. On the one hand, telcos represent a historic opportunity: they enable the armed forces to be equipped with a modern, agile and scalable digital foundation without having to start from scratch. On the other, they represent a new critical dependency: without a robust governance framework, a coherent industrial policy and a shared European vision, the integration of operators into defence could become the Achilles heel of digital sovereignty.

The question is therefore no longer whether telecoms will be part of European defence, but under what conditions: with what level of control, what depth of integration, what degree of technological sovereignty, and in the service of what common strategic vision.

These are the trade-offs that governments, operators and manufacturers will now have to address if they want to turn potential dependence into a real strategic advantage.

9. What should we take away from this?

Modern defence is shifting toward a model in which connectivity, digital resilience, and control of critical infrastructure are as crucial as traditional military platforms. In this context, telecom operators now occupy a central place: their networks have become essential foundations of command, intelligence, joint coordination, and government continuity capabilities.

This document highlights a structural change: telcos are no longer on the periphery of defence; they have become co-architects.

Three dynamics run throughout the document.

❖ Growing dependence of the armed forces on civilian infrastructure

Operational requirements (tactical video, drone swarms, tactical cloud, military IoT sensors, and embedded AI) have reached a level that exceeds the capabilities of traditional sovereign networks. Armed forces now rely heavily on fibre, 4G/5G, edge, and LEO constellations to maintain continuity of operations. Operators are therefore becoming key players in oversight, cybersecurity, and resilience in crisis situations. Without their networks, some modern command capabilities would be inoperative today.

This development is not limited to communications: the management of low airspace amid the proliferation of drones is a new strategic field where operators could become key players in national security and resilience.

❖ A major economic repositioning for operators

Entering the sovereign domain is profoundly transforming telcos' economic model. The defence and security market is opening a new structural vertical, based on long-term contracts, heightened resilience requirements and a higher level of responsibility than in commercial telecoms. Operators no longer just provide connectivity; they deploy comprehensive solutions that include 24/7 monitoring, cyber hardening, critical communications, tactical edge, or satellite services. This move upmarket creates a major economic opportunity but requires long-term alignment with security standards that approach those of the military.

❖ Europe in transition, still far from the integrated American model

Europe is making progress, but within a fragmented framework. Each country is developing its own critical architecture: RRF in France, BOSNet in Germany, and ESN in the United Kingdom. The European Defence Fund is financing 224 projects, but less than 1% of the funding goes to telecoms, even though they are essential to modern military connectivity. By 2030, however, current budgetary trajectories suggest a change of scale: the share of telecommunications in European defence budgets could more than double, bringing the telecoms-defence market to tens of billions of euros at the European level, or a share of up to around 2.5% of defence budgets by 2030.

In contrast, the United States has structured a coherent, centralised and heavily funded model that fully integrates operators into sovereign communications.

The difference lies not in technology but in governance and institutional coherence.

General conclusion

Telecommunications networks are now the backbone of modern military power. They support everything: real-time intelligence, distributed command, multi-domain operations, civil resilience and cybersecurity.
Europe has real industrial assets but is not yet fully mobilising them.
To transform this structural dependence into a strategic advantage, it will need to develop a clear doctrine, coordinate its investments, reduce its technological dependencies and integrate operators as full-fledged capability providers.

The role of telcos in European defence is no longer a question for the future: it is an established fact.

The decisive question now becomes: **with what level of sovereignty, what governance model and what industrial ambitions?**