European Telecom Capabilities for Defence Readiness

October 2026

Executive Summary

Maximizing telecoms capabilities for defence purposes

1. Telecom operators are critical defence enablers: Telecom operators provide a trusted digital backbone, operational understanding for end-users and open innovation dual-use tech ecosystems that have become essential in today's defence landscape. With reliable and secure connectivity, critical actors are able to carry out key operational tasks under difficult conditions. Telecom operators also offer new and emerging technologies that will be key to a rapidly-evolving environment.

2. European telecom operators' capabilities for defence: There are several areas where the sector offers unique capabilities for defence. This spans from enabling critical connectivity and sophisticated cybersecurity protections to non-terrestrial connectivity, drone connectivity, cloud and AI and distributed sensing, among others.

3. Policy measures to strengthen defence readiness: The defence policy framework should establish clear requirements, incentives and procurement pathways while removing operational barriers. Telecom operators should be integrated into defence planning and explore shared testbeds for dual-use innovation. The EU should pursue initiatives that support critical areas.

4. The way forward for the EU, NATO and Member States: All actors have a role to play to support this vision. The EU, NATO and Member States all have different ways in which they can support telecom operators in delivering services for defence purposes.

Telecom capabilities can strengthen defence, but can also become targets. European readiness therefore requires threat modelling, electromagnetic resilience, safeguards against malicious exploitation and common-mode failures, and validated, interoperable national architectures.

Europe's defence readiness depends on secure, resilient communications and digital services that remain operational during disruption and attack. European telecom operators bring extensive infrastructure, operational expertise and capabilities for terrestrial and satellite connectivity, cybersecurity, and cloud and edge computing, among other things. These capabilities should be systematically integrated into defence planning, exercises and procurement. The EU, NATO and Member States should take action by establishing the operational requirements, investment

mechanisms and contractual arrangements needed to turn commercial capabilities into assured defence capabilities.

Defence and security have been established as strategic priorities in Europe. The geopolitical context has accelerated the transformation of the European industrial ecosystem, with the European Commission[1] taking on a more active role in shaping industrial policy, technological priorities and defence capabilities, supported by a significant increase in funding. The European telecom industry, which makes up the entire geographic scope of the EU and its borders with non-EU countries, is uniquely positioned to help governments and European Institutions address these challenges. Telecom networks already provide essential infrastructure and services, and have extensive geographic reach, operational capabilities, data assets and expertise in secure connectivity.

Europe's defence readiness will increasingly depend on the resilience and sovereignty of its digital infrastructure. Modern military operations, civil preparedness and critical infrastructure protection depend on networks, software and data. They require secure connectivity, cloud-edge processing, cybersecurity, satellite integration, and rapid restoration under attack. This dependence is yet another reason why telecom operators are calling for better overall conditions to support investment in strengthening and upgrading their networks, alongside additional funding where necessary.

To reap the full benefits of the unique capacity of the telecoms sector for defence, they must be considered not only as connectivity suppliers but as digital defence enablers.

1. Telecom operators are critical defence enablers

Trusted European telecom operators are critical defence enablers, and should be integrated into defence planning, procurement, exercises and resilience frameworks. They provide a trusted digital backbone that allows Europe's armed forces, governments, emergency services and critical operators to remain connected, protected and operational under all circumstances.

Defence operations increasingly rely on digital continuity under degraded conditions, making the role of telecom operators highly important. **Armed forces, public authorities and critical operators need secure and resilient communications.** This requires more

[1] Some examples: EU Action Plan on Drone and Counter Drone Security (February 2026): Quantum Act (expected Q4 2026); Five joint defence projects to strengthen Europe's industrial capabilities (July 2026); European Defence Fund; Commission makes available €200 million for submarine cable and digital infrastructure projects

than ordinary connectivity; it requires redundancy, a wide variety of cybersecurity methods, rapid restoration, trusted data-sharing, interoperability and operational support before, during and after a crisis. Operators are investing in research, development of products and integrating solutions and operations increasingly needed for strategic autonomy and industrial goals alike, despite limited regulatory support for investment; a more supportive framework would enable them to do more.

Telecom operators are also uniquely positioned to support coalition operations and military mobility. Defence mobility requires secure connectivity along transport corridors, at logistics hubs, ports, airports and border crossings, as well as the ability to exchange information on routes, authorisations, asset tracking, infrastructure status and cybersecurity threats. They can provide the cross-border digital layer that enables effective military mobility.

Their contribution extends to emerging defence domains, including drones, counter-drone, distributed sensing and edge processing. Telecom infrastructure can host sensors, connect detection systems, provide alternatives and redundancy to GPS/Galileo PNT (Position, Navigation and Timing) signals, integrate other bearers into hyperconnectivity secure networks, support low-latency processing and help integrate data into command-and-control platforms. Secure connectivity also goes hand in hand with space and non-terrestrial networks in today's day and age as well.

2. European telecom operators' capabilities for defence

Telecom operators have unique capabilities that can complement dedicated military activities through their nationwide infrastructure, spectrum, connectivity, edge and cloud platforms, cybersecurity operations and real-time network intelligence. These capabilities must also be assessed and protected against cyber, physical and electromagnetic threats, malicious exploitation and shared dependencies that could undermine resilience.

Below, we outline some of the key capabilities that telcos can offer in support of defence. Though the capabilities listed are non-exhaustive, they offer a broad overview of the wide variety of defence capabilities that telecom operators possess. We share further specific examples linked to each of the below areas within the annex at the end of this paper.

2.1 Enabling critical connectivity

Defence users need to maintain connectivity even during congestion, cyberattack, physical damage or wider network degradation. Defence users need to maintain connectivity among headquarters, deployed units, logistics nodes, sensors, platforms,

command centres, public authorities and critical-infrastructure operators. Connectivity capabilities need to be maintained in difficult conditions, such as congestion, cyberattack, physical damage or wider network degradation.

By leveraging advanced mobile networks, mission-critical voice, video and data services, priority and pre-emption mechanisms, cyber-resilient infrastructure, and the integration of satellite and other complementary connectivity platforms, critical communications can enhance communications continuity during crises, natural disasters and security incidents. European telecom operators have a critical role to play in delivering these capabilities, providing the secure, resilient and geographically extensive infrastructure required to support mission-critical communications across Europe.

2.2 Cybersecurity and cryptographic resilience

Connect Europe's members protect large-scale national infrastructure and maintain continuous security operations against cyberattacks, fraud, service disruption and unauthorised access and often extend their security services to both businesses and government.

Operators are also exploring quantum-safe measures (i.e. Post-Quantum Cryptography, Symmetric Key Infrastructure and Quantum Key Distribution among others), to avoid quantum-related threats to security that could exploit cryptographic vulnerabilities. Connect Europe's members provide dedicated services for events with high security needs, and help governments and businesses with a variety of services dedicated to bolster cybersecurity (including 24/7 security operations, threat detection, advanced analytics, data protection and beyond).

2.3 Space, satellite and non-terrestrial connectivity

Space is a core layer of future resilient telecom infrastructure. Defence users increasingly require communications that remain available when terrestrial networks are degraded, unavailable, congested or attacked. This makes satellite and non-terrestrial networks essential for resilience, military mobility, crisis response, maritime security, remote operations and critical infrastructure.

European telecom operators are best positioned to provide mobile satellite services, in cooperation with space-segment operators, as they combine technological, operational and regulatory capabilities. They have established terrestrial infrastructure, unique expertise in efficient spectrum management and coordination, the ability to integrate terrestrial and satellite networks seamlessly, and provide a sovereign European solution. This includes data control, emergency solutions and capabilities to restore service, reduce critical technologies and reduce supply chain dependencies.

European telecom operators can also deliver sovereign, secure, resilient and fully integrated mobile satellite services in cooperation with providers of the space segment.

2.4 Drone connectivity and counter-UAS support

Uncrewed aerial systems are becoming central to modern security and defence. Telecom operators can support both drone operations and counter-drone capabilities, especially where drones rely on commercial or private mobile connectivity, low-latency data links, edge processing and secure transfer, analysis and reporting of sensor data.

Counter-drone measures are increasingly linked to telecommunications capabilities. ISAC technologies will enable mobile networks to function as sensors for the detection, localisation, and tracking of Unmanned Aircraft System (UAS)

Other technologies, such as Remote ID, allow for the identification and classification of UAS, while RF jamming systems enable their neutralisation. Additionally, connectivity-based business models allow telecom operators to offer new services—such as "drone flights as a service" or integration with secure public safety and emergency networks.

2.5 Sovereign cloud, edge and AI infrastructure

A shared sovereign, secure and interoperable European cloud architecture would enable the resilient exchange and protection of classified data across European nations.

Modern operations require processing close to the mission, especially where latency, bandwidth constraints or degraded connectivity make centralised processing unreliable. Collective European defence capabilities can be strengthened by harmonising security standards, ensuring data sovereignty, enabling secure cross-border interoperability and providing distributed resilience against cyber and physical disruptions. Furthermore, European strategic autonomy in AI for defence and security depends not only on sovereign computing infrastructure but also on the availability of trusted and sovereign datasets. Secure sharing of training, testing and validation datasets among Member States would enable the development of European AI models tailored to defence and security use cases, reducing dependence on non-European technologies and data sources. Such a framework would facilitate common standards for data quality, model evaluation and certification, ensuring that AI systems deployed in operational environments are reliable, interoperable and aligned with European security requirements.

2.6 ISR data support, distributed sensing and sensor fusion

Telecom infrastructure can contribute to intelligence, surveillance and reconnaissance (ISR) by providing additional, lawfully authorised data feeds and by connecting geographically distributed sensors.

Potential sources include network-status and outage information, radio frequency interference and anomaly data, mission-specific network or cellular metadata, timing-integrity alerts and fibre-based distributed sensing.

When available, Integrated Sensing and Communication (ISAC) capabilities could provide an additional sensing layer to detect, locate and track assets across large geographic areas. This would be particularly valuable in remote and hard-to-reach regions that require persistent situational awareness and continuous surveillance, enhancing the ability to monitor critical infrastructure, borders and other strategically important locations.

Edge nodes can process and filter inputs close to the source before they are combined with other sensor data and sent to military command & control.

3. Policy measures to strengthen defence readiness

Europe needs a policy framework that enables telecom infrastructure and capabilities to be planned, funded and used effectively for defence and civil preparedness. The goal should not be to create another layer of regulation. **The goal should be to establish clear operational requirements, incentives and procurement pathways for dual-use telecom capabilities**.

The Defence Readiness Roadmap 2030, the European Defence Fund, the European Defence Industry Programme and other current and future EU instruments provide the foundation. Their implementation should explicitly recognise telecom services as essential to European defence readiness, while establishing dedicated flagship initiatives and funding mechanisms to support the development, deployment and scaling of strategic communications, connectivity and digital infrastructure capabilities across Europe.

3.1 Integrate telecom operators into defence and preparedness planning

Telecom operators should become an integral part in relevant EU and national defence, civil-protection and critical-infrastructure planning. Cooperation should include infrastructure and dependency mapping, continuity and restoration proposals, cross-border mutual assistance, and emergency spectrum and site-access arrangements.

In this regard, a successful approach to European telecom operator resilience would allow trusted telecom operators to provide coordinated cross-border support and services, including during major crises, with the aim of avoiding regulatory or legal burdens. It could cover a number of useful areas, such as rapid restoration of cross-border connectivity, mutual assistance between operators, coordinated incident escalation and situational reporting, as well as common security and resilience baselines. The framework should build on existing national structures and commercial capabilities rather than create a new administrative body. Clearly defined roles, responsibilities and activation procedures should be agreed before a crisis rather than negotiated after disruption has occurred.

3.2 Harmonize regulation and remove operational barriers

Defence-related measures should be coherent with the EU's broader simplification agenda. New requirements should reuse existing security assessments, audits and reporting mechanisms wherever possible and should avoid duplicating obligations under overlapping telecom, cybersecurity and critical-infrastructure frameworks. Any further regulatory or legal burdens should be avoided.

Removing practical obstacles should be a main priority, including:

- lengthy deployment and permitting procedures
- inconsistent national security-clearance processes
- uncertainty over crisis access to spectrum and infrastructure
- incompatible data-handling and classification requirements
- unclear liability and cost-recovery arrangements
- regulatory barriers to cross-border mutual assistance

Accelerated procedures should be available for authorised deployment, infrastructure restoration and emergency capacity activation, while maintaining appropriate security and oversight.

Finally, EU-supported defence and dual-use telecom capabilities should meet common technical, security and operational requirements. EU requirements should also remain coherent with relevant NATO standards, architectures and programmes where this supports cooperation between EU Member States and Allied forces.

3.3 Fund defence readiness and modernise procurement

Commercial investment alone will not deliver all the capabilities required for national and European defence readiness. Certain measures produce broad public-security benefits but have limited commercial returns. EU and national funding should support the

additional cost of capabilities such as hardened and redundant power, diverse national and cross-border routes, protected network and edge facilities, and participation in exercises, to name a few examples. Funding should be linked to measurable availability, resilience and interoperability outcomes. Cross-border projects and capabilities shared by several Member States should receive particular consideration.

The proposed European Competitiveness Fund could become an important financing channel for such investments. Until it is adopted, however, current instruments should be used more effectively, and telecom eligibility should be made explicit wherever it supports recognised defence needs. Moreover, more visibility and clarity in the EU funding instruments addressing the civil-defence domain is required and should be streamlined.

Building on this, at the 2025 Hague Summit, NATO Allies committed to investing 5% of GDP annually in defence and security by 2035. Up to 1.5% may cover wider defence and security-related investment, and progress was subsequently reviewed at the 2026 Ankara Summit. NATO and national authorities should provide clear eligibility and reporting guidance for telecom investments that contribute to this broader category. Finally, procurement frameworks should allow public authorities to acquire resilient telecom capabilities, data and managed services, not only equipment. Mechanisms could include multi-year frameworks, joint and cross-border procurement, lifecycle security and maintenance obligations, and rapid procedures for urgent capability gaps. Security-critical procurement should apply proportionate European and trusted-supplier criteria. Assessments should consider establishment, ownership and control, data jurisdiction, supply-chain risk, intellectual-property rights, maintainability and the proportion of value created within Europe. European preference should be applied where justified by security and resilience requirements, while preserving effective competition, interoperability and cooperation with trusted partners.

3.4 Scale innovation through shared testbeds and cross-industry collaboration

European operators should be able to combine their infrastructure, innovation ecosystems and test environments with the expertise of defence users and industry, research organisations, and technology providers. Shared testbeds and cross-industry collaboration programmes could accelerate the development and validation of several areas already mentioned. Initiatives such as ALAIAN demonstrate how operators can jointly identify and test emerging technologies, but defence applications require additional security, accreditation and operational-validation pathways.

Furthermore, European policymakers should leverage existing telecommunications innovation assets, including Open Gateway and operator-led testbeds, as strategic enablers of the European defence innovation ecosystem. Their integration with initiatives such as NATO DIANA and EUDIS would provide innovators with access to trusted infrastructures, advanced connectivity services, edge computing capabilities and realistic operational environments. This would strengthen collaboration between the defence, telecommunications and technology sectors, improve the validation of dual-use technologies and support the creation of a more agile and resilient European defence industrial and technological base.

Large-scale European compute capacity should be made available to support AI, model development and experimentation. Secure operational deployment, however, should be addressed separately through accredited cloud and edge architectures and aligned, where relevant, with NATO initiatives such as Allied Software for Cloud and Edge Services.

3.5 EU-level initiatives

There are already a number of relevant activities related to defence ongoing at an EU level. To name one example, through EDPCI (European Defence Projects of Common Interest) there are already five flagship initiatives[2] that European telecom operators can contribute to through their unique capabilities detailed throughout this paper.

In our view, there are a few areas where further initiatives should be established and existing initiatives can be built upon. Implementing existing initiatives and exploring new areas of activity would demonstrate how trusted European telecom operators can contribute to defence readiness, civil preparedness and strategic autonomy. Find below some areas that should be implemented through EDPCIs and beyond:

- **European Secure Defence Connectivity Layer:** The EU, Member States and trusted telecom operators should develop a federated capability for secure, resilient and interoperable defence connectivity across Europe (secure 5G and private network capabilities, cross-border service continuity, emergency roaming and failover, priority and pre-emption mechanisms, satellite backup,...)
- **Digital Military Mobility Corridors:** The EU should create pilot digital corridors for military mobility that combine physical infrastructure with secure digital services. This initiative should be aligned with EU military mobility work, NATO requirements and Member State national plans.

[2] Commission proposes five joint defence projects to strengthen Europe's industrial capabilities - European Commission

- **Space-terrestrial resilience:** Establish an initiative involving trusted telcos, satellite operators, defence users, emergency services and critical-infrastructure operators.

European telecom defence innovation network: European operators should combine their infrastructure, innovation ecosystems and test environments with defence users, research organisations, primes and technology providers. These initiatives could be translated into EU, NATO and MS instruments. At EU level the use of the upcoming European Competitiveness Fund and different flagships and European Defence Projects of Common Interest (EDPCIs) would be a natural way to enable these proposals. Telecom operators should be involved from the design stage of these initiatives, including in the definition of operational requirements, governance and implementation models.

Finally, **Connect Europe proposes to create a new flagship initiative to be implemented through an EDPCI for European secure communications, sensing & digital battlespace** to develop sovereign European capabilities in secure communications, borderless and resilient connectivity framework, spectrum dominance and AI-enabled defence systems. We think this would be a valuable addition and address a key area where EU-level activity would be instrumental.

4. The way forward for the EU, NATO and Member States

The EU should explicitly recognise trusted telecom operators as part of Europe's digital defence and resilience ecosystem. Telecom capabilities should be integrated into the Defence Readiness Roadmap implementation, and operators should be included in European Defence Industry Programme (EDIP), European Defence Fund (EDF) and Security Action for Europe (SAFE)-related national plans. The EDPCIs definition and implementation should consider telecom operators, especially for Eastern Flank Watch, Space, Maritime and Seabed Defence, DECODER and military mobility-related actions. Telecom operators should be supported in their resilience efforts, and the applicable regulatory framework should have an enabling role rather than introducing barriers.

NATO should translate resilience commitments into operational telecom requirements and investment initiatives. NATO should include telecom operators in resilience planning and exercises where appropriate, provide testing within NATO exercises, and form a collaborative relationship with operators.

Defence, public safety, spectrum, national security and critical infrastructure are deeply national responsibilities. Therefore, **Member States** should include trusted telecom operators in national defence and preparedness planning and collaborate on crisis

activation procedures and dependency mapping. They should take action to ensure a strong level of funding is made available for resilience capacities and modernise procurement frameworks.

Annex

European telecom operators' capabilities for defence

This annex is linked to section 2, on European telecom operators' capabilities for defence. Here, we list in more detail some of the different capabilities that operators can provide for the different areas mentioned.

Enabling critical connectivity

- National fixed and mobile networks.
- Fibre and cross-border routes.
- Private 4G/5G networks for defence facilities.
- High-capacity radio spectrum portfolio (low-, mid-, high-band spectrum), complementing the military's own typically narrow band spectrum.
- Secure 5G network slices.
- Deployable cells and temporary networks (i.e. 5G bubbles).
- Satellite backhaul: MNOs' spectrum could be dual-used both on the terrestrial network and on Non-Terrestrial solutions (from LEO satellites, such as D2D) and in the hybrid combination of terrestrial and non-terrestrial networks.
- Emergency roaming and mutual assistance.
- Traffic prioritisation and quality-of-service mechanisms.
- Field maintenance and rapid-restoration teams.
- Cross border service continuity.
- Mission-critical push-to-talk, data and video services.
- Hyperconnectivity for disaster management.

Cybersecurity and cryptographic resilience

- 24/7 security operations centres.
- Managed detection and response.
- Cyber threat intelligence.
- DDoS protection.
- Incident response.
- Critical-infrastructure cyber protection.
- Identity and access management.
- Secure service monitoring.
- Protection of telecom and cloud infrastructure.
- Post-quantum cryptography and quantum-safe measures.
- Dedicated services for events with high security needs.

- Deception awareness/detection via identifying spoofed identities, rogue base stations, anomalous network behaviour and more.

Space, satellite and non-terrestrial connectivity

- Integrated terrestrial and satellite connectivity.
- Hybrid terrestrial / non-terrestrial services.
- Integrate direct-to-device and satellite IoT.
- Emergency connectivity.
- Military mobility connectivity.
- Maritime and remote-area services.
- Integration with private 5G and MCX.
- Cyber protection of satellite-ground interfaces, including the security and authenticity of space data.
- Protection of the space signals (SATCOM and GNSS).
- Service assurance for governmental and critical users.

Drone connectivity and counter-UAS support

- Secure 4G and 5G connectivity, including dedicated SIM or eSIM services (e.g secure identity).
- Network-based coverage and flight-planning information.
- Low-latency edge processing for navigation, control and payload data.
- APIs supporting device identity, connectivity management and flight operations.
- Network-assisted remote drone capabilities including identification and traffic-management services.
- Managed drone fleets and automated “drone-in-a-box” services for infrastructure inspection, emergency response and public safety.
- Drone detection as a service to protect sensitive sites.
- These capabilities can improve beyond-visual-line-of-sight operations, fleet management and the secure transfer of sensor and mission data.
- A country-wide passive base station site grid can with both power supply and power backup (which may be hardened) would be able to place military equipment, counter UAV radars, etc.
- Infrastructure for counter-UAS systems
- Support countering network-connected drones (using identity controls, geofencing, or by disabling an authorised connectivity module

Sovereign cloud, edge and AI infrastructure

- Distributed edge infrastructure.

- Sovereign & tactical cloud-to-edge services.
- AI capabilities including local AI inference, GPU factories, EU-based models.
- Sensor-data pre-processing.
- Secure data exchange.
- Cloud and edge portability.
- Classified or restricted-domain hosting where accredited.
- Resilient recovery infrastructure.
- Integration with NATO and EU interoperability requirements.
- Defense & security focused AI TestRanges

ISR data support, distributed sensing and sensor fusion

- Connecting distributed sensors to provide lawfully authorised data sources and connectivity for geographically distributed sensors (i.e. mission-specific information on network availability, radio-frequency interference and timing integrity).
- Fibre-based sensing and sensors hosted at network sites can filter and combine inputs to authorised defence systems and provide supplementary detection of physical activity, vibration or infrastructure disturbance along fibre routes.RF and spectrum-related inputs: interference, anomalies and mission-specific radio-frequency observations can complement dedicated military sensors.
- Protection measures against cybersecurity and sovereign cloud storage and processing of data ensuring the full chain of the data is secured.
- C4ISR capabilities angling different data sources to be integrated in a comprehensive way for further analyais and decision making.
- Mission-specific metadata and timing integrity: authorised cellular/network metadata and timing-integrity alerts can contribute additional contextual indicators.
- Distributed edge fusion: edge nodes can filter, correlate and prioritise inputs close to the source before forwarding relevant information for fusion with other sensor data and integration into military C2 systems.