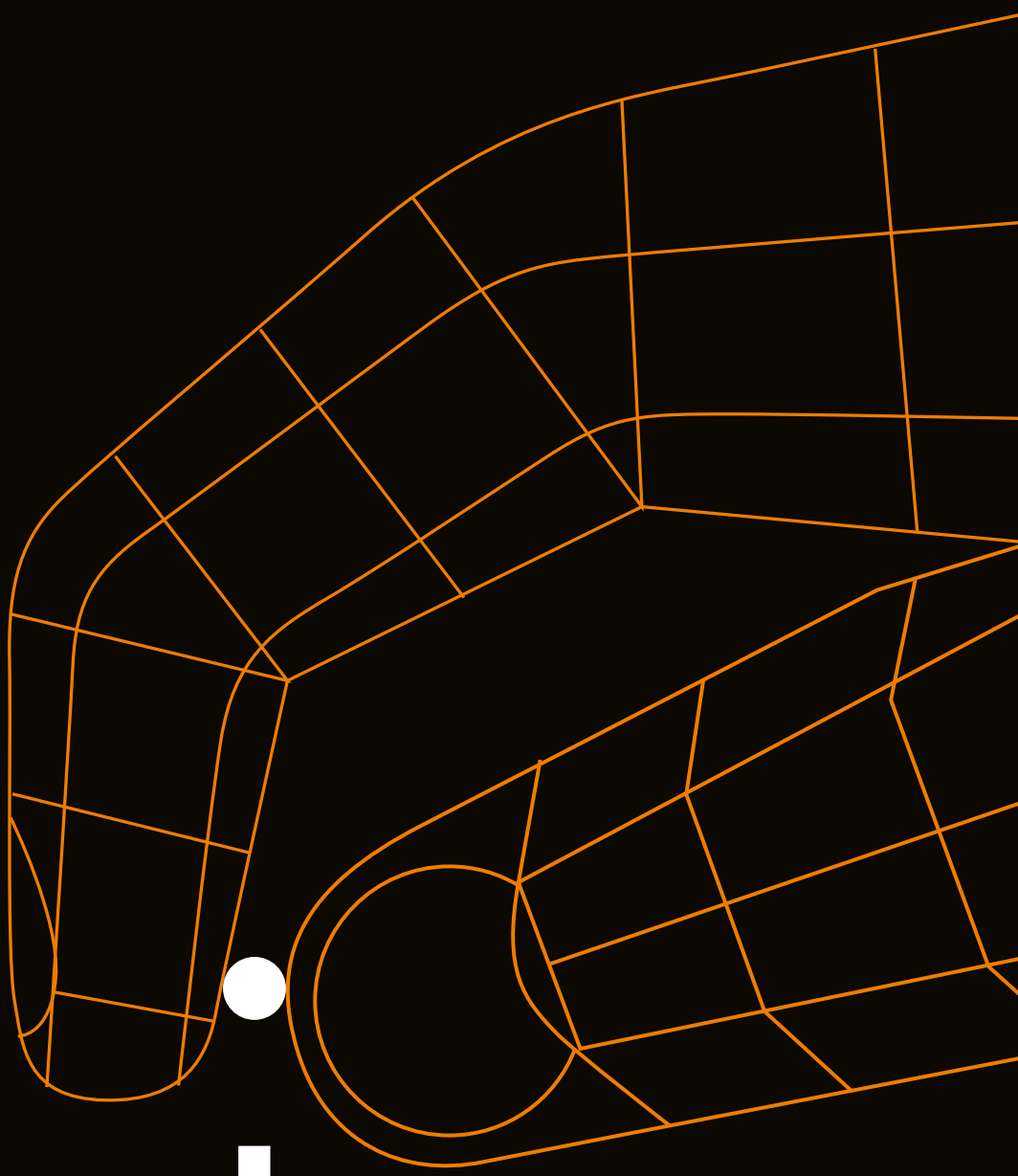
orange™



1st Edition

2026 – 2027

Innovation report

Julien Ducarroz



CEO, Orange Romania

Innovation starts with a question

Technology is moving fast. Artificial intelligence is reshaping the way we work and solve problems. Networks are becoming more intelligent, cloud and edge computing are bringing processing closer to where it is needed, and 5G is opening the door to entirely new ways of connecting people. Some of these developments are already changing the way we work and live.

With that in mind... what if the next big technological breakthrough comes from seeing familiar problems in a completely different way?

The good news is that we do not have to wait to see what happens next. We can experiment. We can explore new possibilities. And because some of the best ideas emerge when different worlds meet, we work closely with talented people across startups, research institutions, universities, technology partners, businesses and public institutions.

This first edition of the Orange Romania Innovation Report is a snapshot of a story built on collaboration and curiosity. Inside, you will find projects exploring AI, next-generation connectivity, cybersecurity, cloud, energy, immersive technologies and much more. They are different in ambition and application, but they share one important idea: they take ideas that once seemed like possibilities and turn them into solutions that can improve people's lives.

So, consider this report an invitation to explore bold applications that started with a simple question:

what if?

Table of Contents

01

Innovation at Orange Romania 2
- Beyond state of the art – Our vision for a tech-driven society 3
- Connectivity as the Layer Everything Else Runs On 3
- Networks That Are Starting to Reason 4
- Security as a Precondition for Trust 4
- An Ecosystem, Not Just a Company 5
- What We Mean by "Beyond" 5

A.I. and the 5th Industrial Revolution: The Human-Centric Shift 6

02

5G Advanced Networks 10
- 5G RedCap 11
- 5G mmWave 12
- Network exposure through standardized APIs 13
- Cellular NTN 14
- Integrated Sensing and Communications (ISAC) 16

03

Wi-Fi 7: An Ultra High-Speed Future 18

04

Education 26

05

Entrepreneurship 38
- Innovation Ecosystems: Where Entrepreneurship Creates the Greatest Value 39
- Open Innovation: Redefining Corporate Competitiveness 41
- Corporate Accelerators: From Startup Support to Strategic Business Value 43
- Orange Fab: Accelerating Startup Collaboration 46

06

Research and Innovation Actions at Orange 54

Our Facilities – Orange 5G Lab Network 55

Smart Networks and Services 56
- AMAZING-6G 57
- 6G-PATH 58
- FLECON-6G 59
- 6G-INTENSE 60
- 6G-MUSICAL and iSEE-6G 61
- TrialsNet 62
- 6Green 63
- ADROIT6G 64
- Agentic6G 65
- SOVEREIGN-6G 66

Civil Security for Societies 67
- SECASSURED 67
- RECITALS 68
- CASTOR 69

Digital, Industry and Space 70
- Euro-3C 70
- HEAT 71

The Digital Europe Programme 72
- CTIS4NIS 72
- 5G-TACTIC 74
- SOCCER 75

Connecting Europe Facility 76
- 5G-CDD 77
- WAVEO 78
- X_HeERO – eCall Next Generation 79

07

The A.I. Frontier 80
- Supercomputers, data centres, EDGE & Clouds 81
- The Telco Use-Case and the Industrial Approach 82
- Challenges, Uncertainties and Ethics 83
- Knowledge Creation 83
- Quantum-Safe Foundations in the 6G Era 85

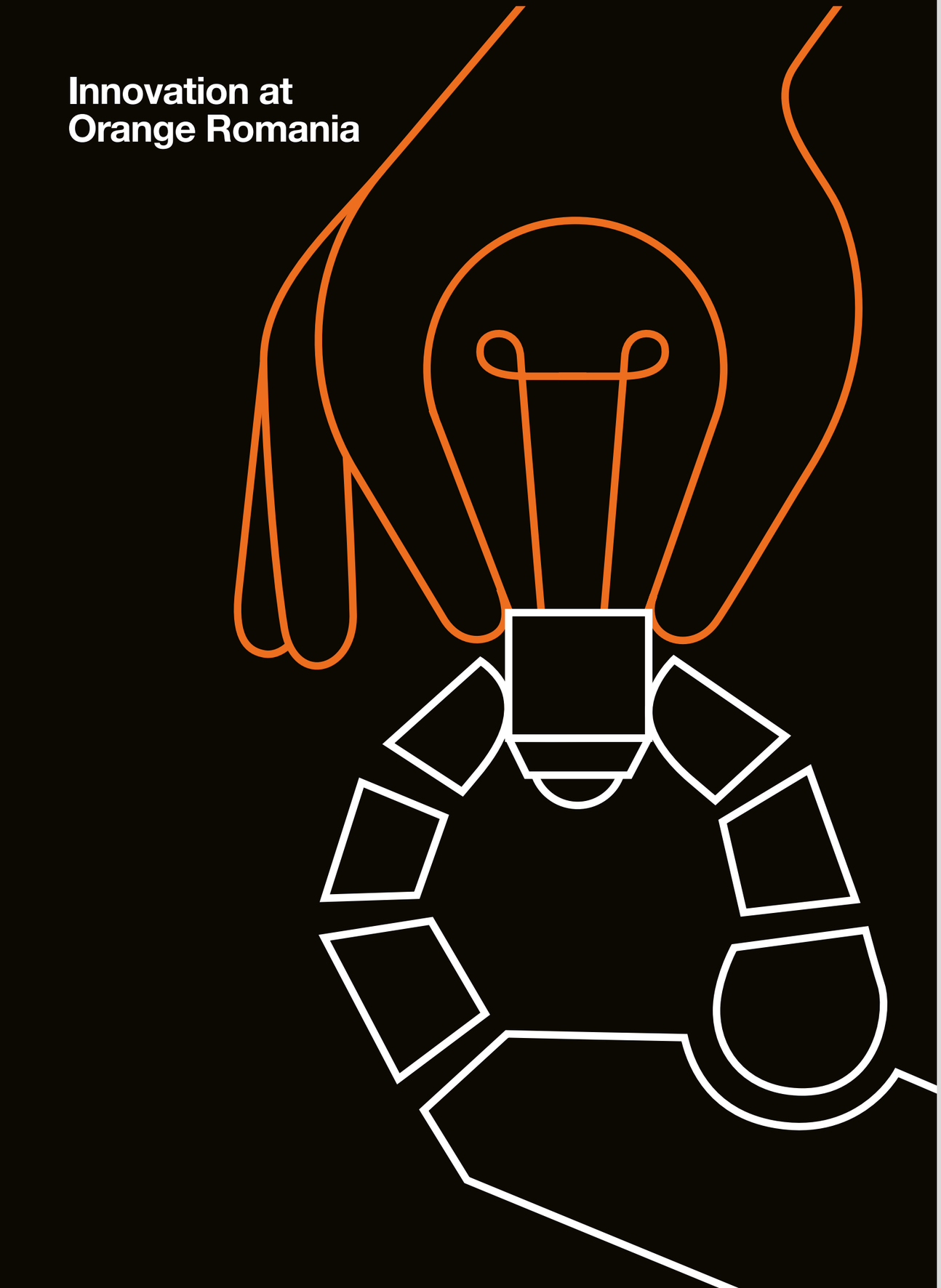
08

Predictions for 2027 86
- Networks of the Future 87
- Wi-Fi 8: Building the Intelligent Indoor Network 88
- Cybersecurity - The Era of Algorithmic Warfare 90
- Claude Mythos and the Art of the Cybersecurity Plot Twist 92
- The Bottom Line 98

09

Glossary of terms 99

Innovation at Orange Romania



01

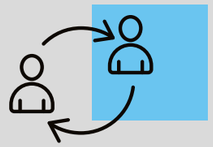
Beyond state of the art – Our vision for a tech-driven society

The scope of this report can be summed up in a single question: what did Orange Romania build, test, and learn over the past twelve months? The sections that follow answer it in detail — network architectures, research projects, proof-of-concept results, and several technologies still years from commercial maturity. Read one way, they describe spectrum, latency, and silicon. Read another way, they describe the country these tools are meant to serve.

We wanted to introduce that second reading before the technical details take over.

For a telecom operator, “innovation” can mean an R&D budget line, a slide in an investor presentation, or a lab full of prototypes that never leave the building.

Over the past several years we tried to make it more concrete: a set of commitments to the people and institutions around us: students who need a way into a technical career, startups that need a first paying customer, companies and cities that need infrastructure they can trust, and a country that needs far more cybersecurity professionals than its universities currently train. Everything described in this report was built to serve those commitments.

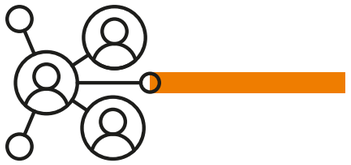


Connectivity as the layer everything else runs on

Most of what Orange Romania does starts with connectivity, so it is worth being clear about what that word means today. A decade ago, a good network meant fast downloads, and few dropped calls. The research chapters ahead describe something different: networks that sense their environment as well as carry data, that increasingly blend Wi-Fi and mobile access instead of treating them as separate services, and that will soon reach places terrestrial infrastructure cannot, through satellite links and Non-Terrestrial Networks. Multi-country research efforts such as EURO-3C and 6Green are testing what a genuinely sustainable, pan-European edge-cloud infrastructure looks like, while 5G Connect Danube Delta is bringing 5G coverage to 23 communities across the Danube Delta that had little of it before.

None of this is abstract to us. Much of it runs today inside the Orange 5G Lab, split between Bucharest, built with Politehnica University of Bucharest and Iași, built with Technical University “Gheorghe Asachi”. These are not showcase spaces; they are where a researcher, a startup founder, or a partner company’s engineer can test a 5G-based idea before betting a product roadmap on it. VITAL-5G proved out assisted navigation and IoT integration at the harbour of Galați under exactly this kind of testing. 5G Smart Intersection, built with Continental Automotive and the Technical University of Iași, brought AI-assisted traffic management to a real intersection rather than a simulation.

We describe this work in technical terms elsewhere in the report, because that is how engineers talk to each other. The underlying idea is simpler: connectivity is now the layer everything else in a digital economy runs on top of, from a hospital’s telemetry to a farmer’s irrigation sensors to a city’s traffic signals. Getting that layer right, quietly and reliably, is one of the more consequential things a company like ours can do for the country it operates in.



Networks That Are Starting to Reason

A second shift running through this report is that networks are no longer just plumbing for data; they are starting to reason about it. Radio resource management, threat detection, and customer service are all moving from fixed rules toward systems that learn from what they observe and act on it directly, often without waiting for a person to approve each step. Our Mobile Data Analytics product turns anonymized network signals into insight for retailers and local authorities that previously had no visibility into how people move through a space. Our work with GSMA Open Gateway and the CAMARA APIs is opening parts of the network itself to outside developers, so a startup can build on our infrastructure without needing to understand it at the protocol level.

We take the caution around this shift seriously, and the cybersecurity chapters later in this report reflect that: the same AI techniques that make networks more capable also make attackers faster and harder to detect, and we would rather describe that risk plainly than understate it. But caution does not mean standing still. It means building the expertise to use these tools responsibly before they are forced on us by competitors, or by attackers who show no such restraint. Several of the projects described later — from AI-assisted radio access networks to autonomous threat-hunting concepts — are our attempt to build that expertise now, deliberately, rather than later, under pressure.

Security as a Precondition for Trust

The third commitment we want to name directly is security, because it is where the other two stories in this report — about intelligent networks and about the country's technical workforce — meet most clearly.

The numbers are not encouraging on their own. In 2025, cyberattacks against Romanian businesses rose 19% year-on-year, according to our data. Across Europe, the 2025 ISC2 Cybersecurity Workforce Study put the sector's workforce shortage at an alarming rising pace. This is a gap that has been growing faster than universities can close it. The AI-driven threats described later in this report will not make that gap smaller.

We have chosen to treat this as a problem we can help solve directly. Orange Romania was the first local telecom operator involved in building, running, and funding Romania's major cybersecurity competitions for students, an involvement that goes back to 2020: UNbreakable România, which we run together with Bit Sentinel and which, in 2026 alone, drew more than 4500 young competitors nationwide; the Romanian Cyber Security Challenge, where we have served as Gold partner since 2017 and which sends the country's top ten competitors to the European Cyber Security Challenge; DefCamp, the largest cybersecurity conference in Central and Eastern Europe; and the National Cybersecurity Olympiad for high school students, launched in 2024 with Orange among its initiators. Through Orange Fab, we also backed CyberEdu, a training platform that surpassed 20,000 registered users within its first four years.

These programs work alongside the technical defenses described elsewhere in this report. The premise is simple: the most durable answer to a growing attacker capability is a growing base of defenders, and a company with our reach carries some responsibility for helping build it.



An Ecosystem, Not Just a Company

The same logic runs through how we think about talent and entrepreneurship, which the Entrepreneurship chapter of this report explores in more depth. Put plainly: a company our size creates more value by opening doors than by keeping them closed.

The Orange Educational Program has been doing exactly that since 1998, longer than most of the technologies described in this report have existed. Twenty-eight years in, it counts more than 1,400 alumni, has funded over 425 scholarships, placed more than 650 students in paid internships, and built partnerships with 13 universities across seven Romanian cities. Several of the engineers leading our technical teams today, including contributors to this report, came through the program themselves. It is, in a real sense, how Orange Romania renews its own technical capability, one cohort at a time.

Orange Fab addresses the same problem from the other direction. Conceived as the first corporate accelerator network of its kind, it runs in Romania as a one-year program with no participation fee and no equity taken, offering young companies what they usually cannot afford on their own: access to Orange's commercial network, proof-of-concept funding of up to €20,000, the 5G Lab's infrastructure in Bucharest and Iași, and, through the wider Orange Fab network active in twenty countries, a route to distribution partners well beyond Romania. A startup working on connectivity, digital health, smart cities, or cybersecurity does not need to convince us its market is real. It needs a first serious partner willing to test the idea under real conditions, and that is the role we try to play.

We think of the 5G Lab, Orange Fab, and the Orange Educational Program as one system rather than three separate programs, because the people who move through them usually do too. A student on an OEP scholarship works alongside a 5G Lab researcher. That researcher's project sometimes becomes the technical foundation for an Orange Fab startup. That startup's founders occasionally return, years later, to mentor the next cohort of UNbreakable competitors. Each program is more useful because the others exist alongside it.

What We Mean by "Beyond"

While some of the technologies presented in this report, including Wi-Fi 8, our 6G research initiatives, and AI-driven cybersecurity solutions, are still evolving and may take years to reach widespread adoption, they represent important steps toward the future.

This is precisely why we chose the title "Beyond State of the Art." We believe that the true value of an innovation program goes beyond the number of solutions brought to market today. It lies in its ability to anticipate future needs, explore emerging technologies, and develop solutions that will help shape Romania's digital future.

Our answer, based on everything in this report, is that Romania needs networks resilient and capable enough to carry a genuinely digital economy, a cybersecurity workforce large enough to defend it, and enough founders, researchers, and engineers trained today to keep building on top of it tomorrow.
That is the tech-driven society we are working toward: not one defined by how advanced any single technology is, but by how widely its benefits reach.

A.I. and the 5th Industrial Revolution: The Human-Centric Shift



Industry 4.0 was built around automation, connectivity, and large-scale data collection: production lines instrumented end-to-end, decisions increasingly delegated to control systems, efficiency treated as the primary metric of success. The "Smart Factory" model optimized throughput but gave little weight to the people working alongside the machines.

The 5th Industrial Revolution (5IR) builds on 4.0 rather than replacing it. It reintroduces the human element into the automated landscape, adding sustainability, resilience, and human-centricity as design goals alongside efficiency.

In this model, AI functions less as a replacement for human labour and more as a collaborator: systems designed to support human decision-making rather than replace it.

If Industry 4.0 was about the "How," Industry 5.0 is about the "Why." In practice: a 4.0 system optimizes the process; a 5IR system also accounts for the person operating within it — workload, safety, and fatigue alongside throughput.

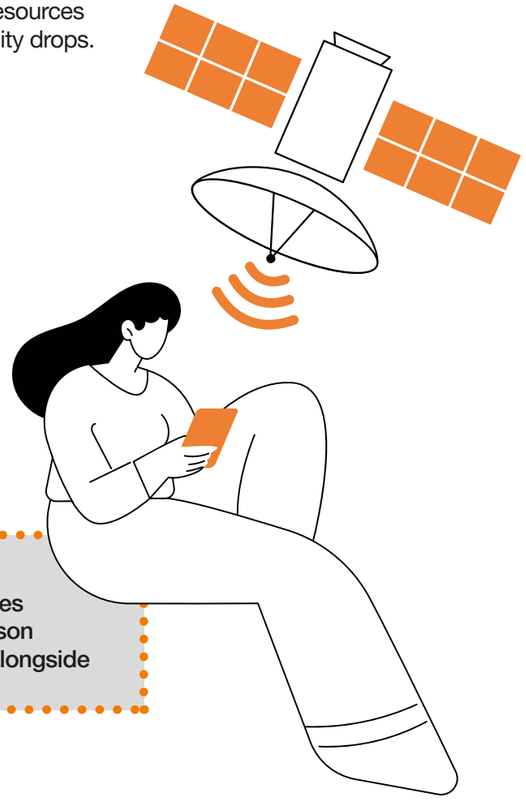
From Automation to Augmentation: The Era of Agentic AI

In previous technological cycles, AI was largely reactive: a prompt in, a result out, with no persistence beyond that exchange. In 5IR, we are seeing a transition toward Agentic AI: systems capable of autonomous reasoning and goal setting within predefined guardrails. In an industrial context, this means AI is moving from "observing" to "orchestrating." This shows up in a few concrete ways:

Cognitive Network Management: instead of reacting after a link fails, the network predicts congestion from local signals and reconfigures resources before service quality drops.

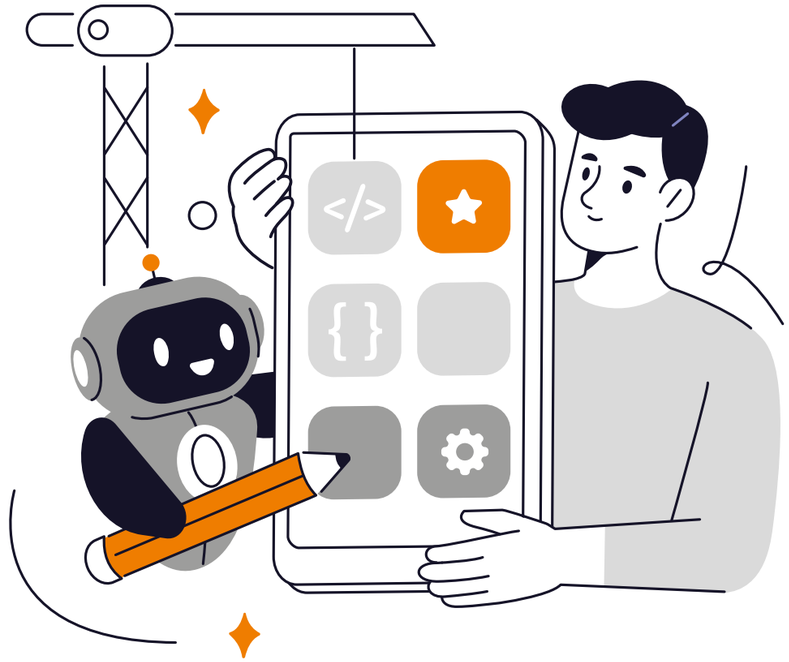
Hyper-Personalization: in 5IR, the "mass production" model of 4.0 gives way to "mass personalization": production lines that switch from one thousand identical units to one thousand unique units without stopping the line.

The goal is Augmented Intelligence: delegating continuous monitoring of large data volumes to AI so human experts can focus on strategy and exceptions rather than routine surveillance.



The Symbiosis of 5G, Edge Computing, and AI

The 5th Industrial Revolution depends on a high-performance connectivity layer, provided by the convergence of 5G/5G-Advanced and Multi-access Edge Computing (MEC). This is part of the broader shift of telcos such as Orange from connectivity providers toward AI-driven technology companies. For AI to support real-time decisions, processing needs to happen close to where the data is generated. If a robot in a smart warehouse must send data to a data centre hundreds of kilometres away before deciding whether to stop for a person crossing its path, the resulting latency becomes a safety problem. 5IR addresses this by moving inference to the network edge.



Three Enabling Technologies

Network Slicing: partitioning the network into dedicated virtual "slices" — one reserved for emergency services with 99.999% reliability, another carrying lower-priority consumer traffic such as 4K video streaming.

Edge Inference: running AI models locally at the network edge to achieve sub-10ms response times for real-time human-robot interaction.

Real-Time Data Streams: a continuous feedback loop between physical assets and their digital controllers.

Digital Twins and the Virtual Testing Ground

A cornerstone of the 5IR strategy is the use of Digital Twins: highly accurate, real-time virtual replicas of physical assets, whether a single machine, a factory floor, or an entire city's communication grid. By integrating real-time telemetry from IoT devices, a Digital Twin lets engineers test changes without risking the physical system: what happens if traffic on this node doubles, or if a solar event disrupts the signal environment?

In practice, this lets teams catch failure modes — grid overload during a heatwave, for instance — in simulation rather than in production, at a fraction of the cost of a real incident.

The Leap to 6G: The AI-Native Network

5G provided the connectivity basis for 5IR; 6G research goes further by building intelligence into the network itself. Rather than AI merely running on top of the network, the network increasingly functions as a sensor.

Using Joint Communication and Sensing (JCAS), 6G base stations can detect the position and movement of people and objects without those objects carrying any device.

Why AI Matters for 6G

AI-Native Air Interface: in 5G, waveform design is fixed by human engineers in advance. In 6G, AI can adapt the waveform in real time to the current environment such as walls, weather, or physical obstructions.

Self-Synthesizing Networks: 6G research is exploring AI that generates network protocols on the fly, so two machines can establish a working communication scheme even when no existing protocol covers their specific exchange.

Sub-terahertz Frequencies: 6G targets very high data rates using frequency bands that are impractical to manage manually. AI is needed to handle beam-steering at the precision and speed these frequencies require.



Sustainability: The Green Imperative

Industry 5.0 places significant emphasis on the “Triple Bottom Line”: profit, people, and planet. AI is often framed as an environmental cost, but within 5IR it is also used as a tool for energy optimization.

Through Green AI practices such as model distillation (compressing large models into smaller, more efficient ones) and AI-driven power management, industrial players can meaningfully reduce their carbon footprint.

In 5IR, technology shifts from being simply a consumer of resources to also acting as their auditor and optimizer — continuously identifying and eliminating waste that would go unnoticed at human scale.

Predictive Cooling: AI manages data centre cooling systems by predicting heat spikes before they occur.

Deep Sleep Modes: AI puts 5G/6G towers into a low-power state during idle periods, waking them within milliseconds when a device is detected.

Ethics and the “Black Box” Problem

As AI moves into critical infrastructure, the “black box” problem - knowing the output but not the reasoning behind it - becomes a legal and safety liability. 5IR requires Explainable AI (XAI).

For a human-machine partnership to work, there must be trust. If an AI system decides to shut down a production line, it needs to be able to explain that reasoning to the human supervisor in terms they can evaluate. An opaque decision is not acceptable for a call with multi-million-euro consequences. This transparency is what keeps humans as the ultimate authority, in line with the 5IR principle of keeping a human in the loop.

The Socio-Economic Impact: Jobs in the 5IR Era

Any discussion of AI and 5IR raises the question of job displacement. The evidence so far points toward a shift in the job market rather than a net loss of it. We are seeing the rise of “new collar” jobs — roles that sit between traditional blue-collar and white-collar work and require a mix of technical literacy and human judgment: AI ethicists, robot operations trainers, digital twin architects. This puts a premium on continuous upskilling; a degree becomes a starting point rather than an endpoint. The aim is to remove repetitive, low-value tasks and replace them with roles that depend on what AI still struggles with — genuine creativity and moral judgment.

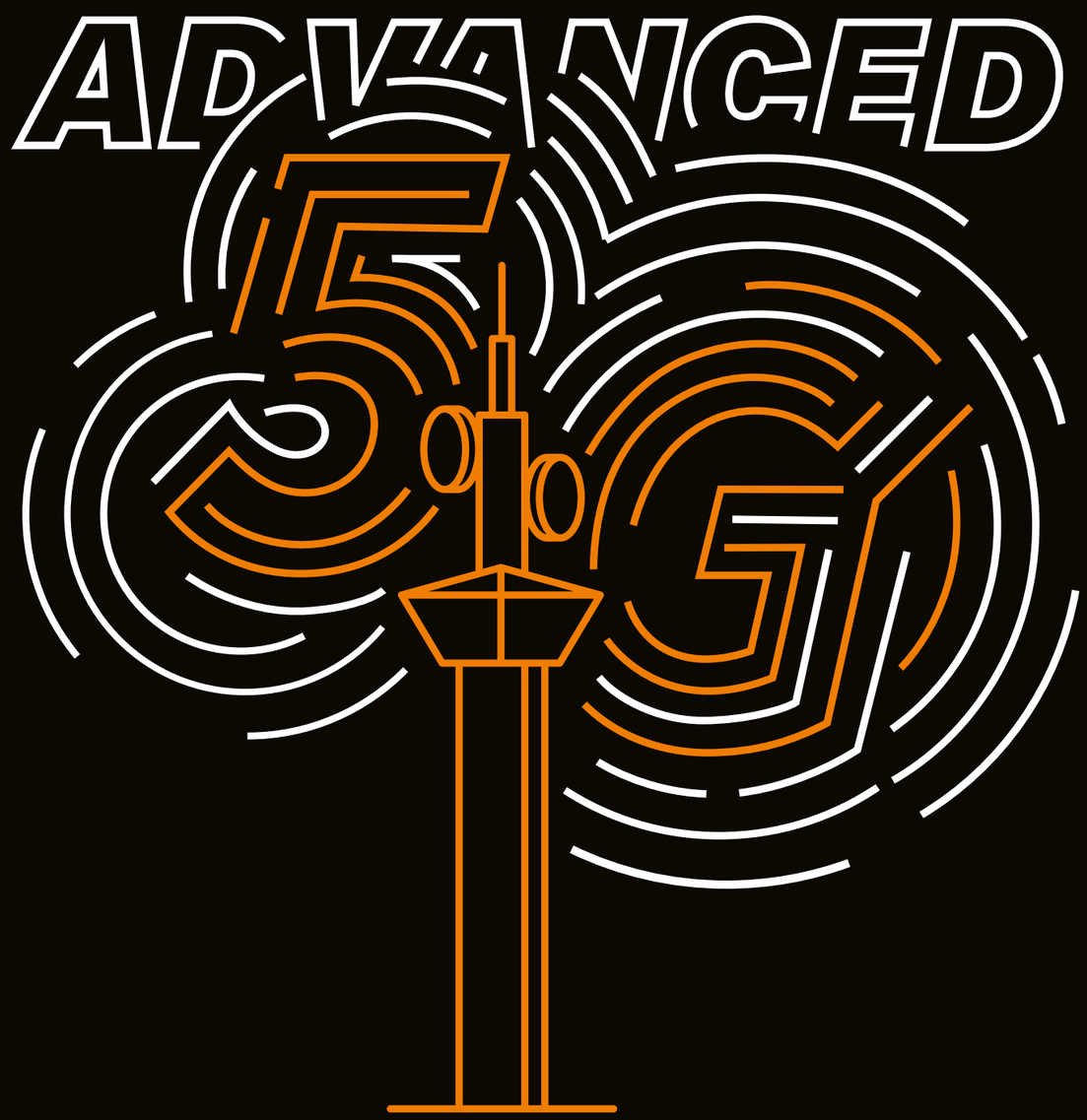
The Road to 2030 and Beyond

The 5th Industrial Revolution represents a maturing relationship with technology — moving past the novelty of “smart” devices toward systems that are genuinely useful in context.

The convergence of 6G research, Agentic AI, and Edge Computing is closing the gap between the digital and physical realms. Telecommunications provides the reliable foundation on which this convergence depends. The goal is not simply faster downloads or more capable robots, but a more resilient and inclusive society — one where technology is designed around the people using it. Heading into the 2030s, the constraints will be practical and regulatory, not just technical.

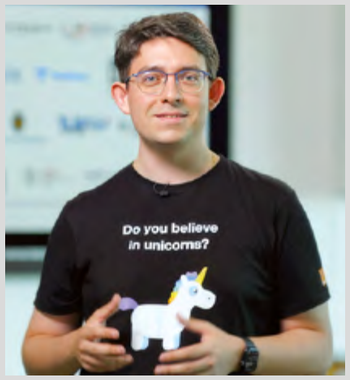


5G Advanced Networks



02

Orange Romania is shaping the future of connectivity by advancing its 5G ecosystem towards 5G Advanced, embracing novel capabilities such as RedCap, mmWave, network exposure, cellular Non-Terrestrial Networks (NTN) and remote sensing capabilities. These innovations are unlocking fresh opportunities across industries while laying the technological foundations for a seamless evolution towards 6G.



5G RedCap

5G Reduced Capability (RedCap, or NR-Light) is the 3GPP Release-17 device class that bridges the gap between low-power 4G-derived technologies (NB-IoT and LTE-M) and full-featured 5G terminals, targeting IoT devices like wearables, industrial sensors and video surveillance cameras.

RedCap is 5G-native and operates on the 5G Standalone (SA) standard, inheriting core SA advantages (slicing, lower user-plane latency and higher energy efficiency) while dialling down radio/device complexity to fit small form factors and tighter cost requirements. The 3GPP Release-17 profile caps the radio bandwidth from 100 MHz down to 20 MHz, removes carrier aggregation and dual connectivity, allows half-duplex FDD, and reduces antenna/MIMO requirements. Together, these measures cut modem bill-of-materials by ~65% versus a baseline 5G device yet still delivering LTE-M class performance and lower latency on a 5G core.

For network efficiency, RedCap UEs can be explicitly identified early in access to enable differentiated admission and resource handling on gNodeBs. On the device side, Release-17 adds extended DRX and RRM relaxations that extend battery life for sensors and wearables. In typical configurations, peak throughput rates are around 50/20 Mbps in mid-band TDD. These numbers were confirmed by Orange 5G Lab tests (based on an Ericsson RAN system) performed in early February 2026 with two commercial devices (Pegatron MD200 dongle and Quectel RM255C-GL modem) as showcased in the picture below.

From an operator perspective, RedCap is strategically important because it lets us concentrate IoT growth on our future 5G SA network, offering a clean migration path for today's LTE Cat-1/Cat-4 device fleets.

RedCap devices coexist natively with NR traffic on the same carriers (better than LTE overlays) and can be pointed to dedicated 20 MHz portions of the N78 spectrum. These characteristics unlock practical deployments across our FDD and TDD spectrum holdings with minimal RAN uplift beyond bandwidth configuration and Core policy rules.

RedCap also matters commercially. Independent industry analysts forecast that mid-tier 5G IoT devices will expand rapidly as enterprises go direct to 5G for digitization; RedCap is the fit-for-purpose connectivity that enables this at scale.

For Orange Romania's B2B customers, that translates into credible SA-based offers for worker wearables with VoNR/SMS support, low-latency mobile video surveillance, condition-monitoring with multi-year batteries, and smart-grid telemetry, each benefitting from 5G SA advantages, while also being capable of 4G fallback.

Looking ahead, Release-18 eRedCap further lowers device complexity and energy consumption toward LTE Cat-1 territory while retaining SA benefits, broadening the reachable device price points and accelerating migration off 4G. This update further strengthens the business case for spectrum refarming and 5G SA monetization.

5G mmWave

Operating above 24 GHz, 5G mmWave brings an order-of-magnitude more contiguous spectrum than sub-6 GHz bands, enabling multi-gigabit user speeds, dense spatial reuse, and very low latency for high-value hotspots, private networks and fixed wireless access (FWA) implementations.

As data demand and device concurrency continue to increase, mmWave becomes the logical extension of the RAN. It absorbs peak loads in high-cluttered venues and campuses and creates alternative last-mile capacity where fiber is slow or costly to extend.

From a technical point of view, mmWave is the 5G Frequency Range 2 (FR2) spectrum domain, typically lying between 24.25–27.5 GHz (n258, the European 26 GHz band), 26.5–29.5 GHz (n257/n261 in parts of the USA/Asia), 37–43.5 GHz (n260/n259), and 66–71 GHz (n263). These bands exist because FR2 offers vastly more total bandwidth, 800MHz for FR2 vs. 100MHz in FR1 (sub-6 GHz), so operators can allocate multiple channels of 100 MHz today (8 in total) and evolve to even wider carriers as 5G-Advanced matures. In practical deployments, mmWave runs TDD, uses wide subcarrier spacing (commonly 120 kHz) which helps latency, and relies on massive, sometimes motorized, phased-array antennas with dynamic beamforming/beam-tracking to deliver link budget and suppress interference. The small wavelength lets radio equipment providers pack dozens to hundreds of radiating elements into compact antennas, producing high gain arrays, steerable beams and tight spatial reuse of the frequencies.

Propagation in the mmWave spectrum behaves differently than in sub-6 GHz; free-space loss is higher, building penetration is worse and diffraction around obstacles is limited. This is why mmWave is engineered for hotspots and line-of-sight/strong-reflection paths, and why radio design must address the downlink–uplink link-budget imbalance typical in FR2. The mitigations combine FR2 with an FR1 “anchor” through EN-DC or NR-DC for robust control and uplink, aggregate carriers across FR1+FR2, apply uplink slot aggregation, deploy high-power UE classes (especially grid-powered CPEs) for FWA, and increase receiver sensitivity via advanced antenna technologies. With these tools, operators can extend usable coverage and stabilize performance at the cell edge.

Recent independent field studies show commercial 5G NR mmWave smartphones supporting 8×100 MHz downlink carrier aggregation achieve sustained multi-gigabit performance (>5 Gbps) with uplink often >400 Mbps on 4×100 MHz UL CA, more than doubling earlier generations. Beyond smartphones, FWA trials with high-power CPEs demonstrated near- and non-LOS operation and meaningful ranges up to 5 km, highlighting mmWave’s feasibility for rural/suburban broadband deployments.

Indoors, enterprise small cells deliver gigabit speeds not only in line-of-sight hallways but also around corners and into closed rooms due to constructive reflections, making indoor private-5G in mmWave a realistic option for certain layouts.

These results are also confirmed by the independent tests performed within the Orange 5G Lab in early December 2025, based on an Ericsson RAN system (AIR1281 active antenna) and a Nokia FWA CPE (5Gmm29-B) as shown in the picture below. Orange Romania used a temporary N258 spectrum license from ANCOM during the trials, achieving up to 10 Gbps in DL and 1.2 Gbps in UL throughput.

From an operator’s perspective, target use cases for mmWave can be split into four domains. First, for consumer and venue experiences in stadiums, arenas, festivals, airports, and rail hubs, mmWave offloads and accelerates the busiest cells, enabling 4K/8K streaming, multi-angle AR replays, and ultra-fast content sharing, while sustaining venue apps such as ticketing, wayfinding, and queue management with consistent latency under heavy crowd loads.

Second, for enterprise and private networks across campuses and factory floors with dense machinery or high user concurrency (e.g., logistics hubs, media production, smart offices), indoor mmWave small cells deliver multi-gigabit, wireless-LAN-like performance.

Third, as a fibre alternative, Fixed Wireless Access (FWA) can be monetized by pairing high-power CPEs with careful cell positioning to cover several kilometres and deliver gigabit throughput, particularly in suburban or rural towns where FTTH is slow to arrive.

Finally, along transport and smart-city corridors, hotspot clusters on tram and bus routes, tourist districts, and commercial boulevards can be served with pole-mounted mmWave to support multi-gigabit traffic; the same topology can support municipal video surveillance or pop-up capacity for events.

Looking further, standards and roadmap trends favour deeper mmWave integration over the next 2–4 years. 5G-Advanced (Rel-18/19) brings broader FR1+FR2 carrier aggregation, more uplink CA layers, smarter scheduling across dual connectivity, potential support for channel bandwidths well beyond 100 MHz (on path to multi-GHz carriers above 60 GHz) and potential to be used as an enabling technology for 6G Integrated Sensing and Communications (ISAC), transforming the cellular network into a radar for securing critical infrastructures.



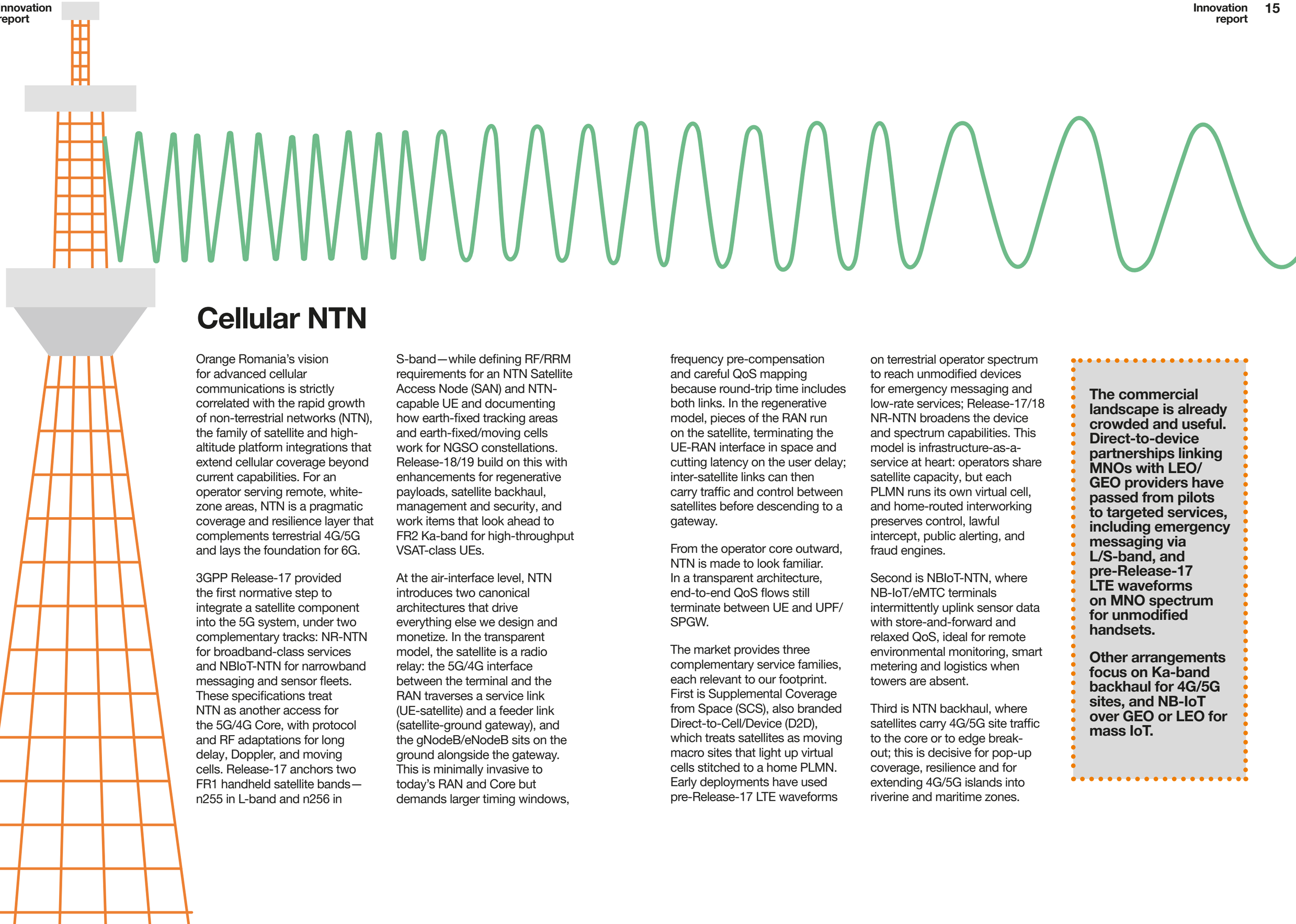
Network exposure through standardized APIs

Moving beyond commercial aspects, Orange Romania is also a founding member of ETSI’s OpenOP Software Development Group (SDG). Launched in July 2025, OpenOP aims to build an open-source reference implementation of the GSMA Operator Platform, acting as a carrier-neutral federation layer for 6G testbeds. Orange contributes to this initiative with operational expertise and the 5G Lab testbed exposure, with representatives serving on the Technical Steering Committee (TSC) to oversee the cloud-native architecture and ensure seamless interoperability with Orange’s commercial infrastructure.

Despite the standardization of these API models, fragmentation across different operators and vendors continues to slow down infrastructure deployment and commercial rollouts, as seamless replicability is not always guaranteed across varying Core and RAN configurations. Furthermore, beyond basic CAMARA API model adherence, there are currently no established methodologies for certifying the entire end-to-end ecosystem.

To solve this critical industry gap, a new OpenOP *End-to-End Validation & Certification of Network* APIs across Federated Testbeds task force has been launched. This task force focuses on defining a comprehensive replicability certification methodology, which includes specific criteria, tests, and audit checklists. A key differentiator of this initiative is its focus on testing interoperability across the entire technical chain, from the CAMARA-certified API through the OpenOP Network Exposure Platform, the 3GPP NEF, and down to the data sources, ensuring the exact same API code runs flawlessly across multiple networks.

To achieve these ambitious goals, the task force will host federated tests with friendly users and organize annual, hybrid “plugtest” events. Orange Romania plays a central role in the governance of this task force, providing management, facilitation, and integration support directly within its 5G Lab facilities.



Cellular NTN

Orange Romania's vision for advanced cellular communications is strictly correlated with the rapid growth of non-terrestrial networks (NTN), the family of satellite and high-altitude platform integrations that extend cellular coverage beyond current capabilities. For an operator serving remote, white-zone areas, NTN is a pragmatic coverage and resilience layer that complements terrestrial 4G/5G and lays the foundation for 6G.

3GPP Release-17 provided the first normative step to integrate a satellite component into the 5G system, under two complementary tracks: NR-NTN for broadband-class services and NBIoT-NTN for narrowband messaging and sensor fleets. These specifications treat NTN as another access for the 5G/4G Core, with protocol and RF adaptations for long delay, Doppler, and moving cells. Release-17 anchors two FR1 handheld satellite bands—n255 in L-band and n256 in S-band—while defining RF/RRM requirements for an NTN Satellite Access Node (SAN) and NTN-capable UE and documenting how earth-fixed tracking areas and earth-fixed/moving cells work for NGSO constellations. Release-18/19 build on this with enhancements for regenerative payloads, satellite backhaul, management and security, and work items that look ahead to FR2 Ka-band for high-throughput VSAT-class UEs.

At the air-interface level, NTN introduces two canonical architectures that drive everything else we design and monetize. In the transparent model, the satellite is a radio relay: the 5G/4G interface between the terminal and the RAN traverses a service link (UE-satellite) and a feeder link (satellite-ground gateway), and the gNodeB/eNodeB sits on the ground alongside the gateway. This is minimally invasive to today's RAN and Core but demands larger timing windows, frequency pre-compensation and careful QoS mapping because round-trip time includes both links. In the regenerative model, pieces of the RAN run on the satellite, terminating the UE-RAN interface in space and cutting latency on the user delay; inter-satellite links can then carry traffic and control between satellites before descending to a gateway.

From the operator core outward, NTN is made to look familiar. In a transparent architecture, end-to-end QoS flows still terminate between UE and UPF/SPGW.

The market provides three complementary service families, each relevant to our footprint. First is Supplemental Coverage from Space (SCS), also branded Direct-to-Cell/Device (D2D), which treats satellites as moving macro sites that light up virtual cells stitched to a home PLMN. Early deployments have used pre-Release-17 LTE waveforms on terrestrial operator spectrum to reach unmodified devices for emergency messaging and low-rate services; Release-17/18 NR-NTN broadens the device and spectrum capabilities. This model is infrastructure-as-a-service at heart: operators share satellite capacity, but each PLMN runs its own virtual cell, and home-routed interworking preserves control, lawful intercept, public alerting, and fraud engines.

Second is NBIoT-NTN, where NB-IoT/eMTC terminals intermittently uplink sensor data with store-and-forward and relaxed QoS, ideal for remote environmental monitoring, smart metering and logistics when towers are absent.

Third is NTN backhaul, where satellites carry 4G/5G site traffic to the core or to edge break-out; this is decisive for pop-up coverage, resilience and for extending 4G/5G islands into riverine and maritime zones.

The commercial landscape is already crowded and useful. Direct-to-device partnerships linking MNOs with LEO/GEO providers have passed from pilots to targeted services, including emergency messaging via L/S-band, and pre-Release-17 LTE waveforms on MNO spectrum for unmodified handsets.

Other arrangements focus on Ka-band backhaul for 4G/5G sites, and NB-IoT over GEO or LEO for mass IoT.



Integrated Sensing and Communications (ISAC)

Integrated Sensing and Communications (ISAC) aims to change telecommunications by upgrading cellular networks to act as distributed radar systems capable of detecting shapes, movements, and distances. This topic recently gained mainstream attention following the European Commission's announcement from early February 2026 regarding investments to turn existing 5G deployments across Europe into sensing equipment.

To support this evolution, Orange Romania is actively involved in the fundamental research and standardization activities related to these technologies as a member of the ETSI ISAC Industry Specification Group and partner in two Horizon Europe SNS-JU projects, 6G-MUSICAL and iSEE-6G, which focus on validating complex ISAC scenarios.

To achieve the high-precision localization required for advanced sensing use cases, the network architecture relies on several highly complex technical enablers. First, operating in the mmWave and Terahertz spectrums is mandatory to secure the larger 400 MHz or 800 MHz bandwidths needed to detect tiny movements. Because standard frequency range resolutions might not suffice for applications like autonomous driving, techniques like carrier aggregation are employed to combine multiple frequency blocks, refining the range resolution down to roughly 0.1 meters.

Furthermore, scanning the environment requires Massive MIMO antennas capable of highly precise radio beam steering. The network must also support radar-like multistate topologies where multiple radio sites work together. While mono-static setups use the same antenna for transmitting and receiving, making them simpler but prone to severe self-interference, bi-static configurations separate the transmitter and receiver to offer broader coverage and overcome physical obstacles.

Beyond novel antennas and spectrum requirements, the physical layer of the network also needs to undergo several redesigns. Legacy OFDM waveforms are ineffective for radar-like reflections, driving the adoption of new dual-functional waveforms like Orthogonal Time Frequency Space (OTFS). Designing these unified waveforms requires balancing the Cramér–Rao Bound for sensing accuracy against the Pareto Frontier for communication data rates, ensuring that allocating resources to one function does not heavily degrade the other.

Moreover, in dense urban areas, Reconfigurable Intelligent Surfaces (RIS) are deployed to assist with sensing and communications coverage. These passive metamaterial devices feature reflective elements that can be individually controlled to bounce signals around blocking objects, creating artificial line-of-sight links that dramatically enhance service availability.

Because spatial precision is important for defence systems, sub-nanosecond time synchronization between radio sites is critical. In this regard, a 3-nanosecond clock error between multiple radio nodes translates to a 1-meter range inaccuracy, making advanced distribution technologies like fibre-based White Rabbit or Rubidium clocks essential to reach picosecond-level accuracy.

Finally, processing this massive influx of raw radio channel measurements requires Edge Computing infrastructures collocation with the radio sites and AI/ML algorithms to perform real-time detection, estimation, and recognition tasks directly at the edge of the network.

Once these technical enablers are fully integrated, ISAC will unlock a diverse portfolio of Sensing as a Service application across MNOs' infrastructures.



In the military and defence sectors, this dual-use technology facilitates drone and ship detection, alongside real-time human counting and mobile crowd sensing. For mobility, it provides crucial support for autonomous guided vehicles and smart convoys through simultaneous localization and mapping. Additionally, it empowers nationwide environmental monitoring, offering capabilities ranging from weather prediction and pollution tracking to monitoring bird activity around critical infrastructures like airports.

Wi-Fi 7:
An Ultra High-Speed Future



03



Our journey with Wi-Fi 7 has not been a single event but rather a multi-year effort that has taken us from an idea on a whiteboard to a technology that now sits proudly within our B2B services portfolio. It started with curiosity about what the next generation of wireless connectivity could deliver in real-world conditions, moved through careful proof-of-concept design and rigorous lab testing, continued into public showcases and live event deployments, and has now matured into a commercially available offering for our business customers.

Where It All Began: Designing the Proof of Concept

Once the decision was made internally that we would pursue and validate the latest generation of Wi-Fi technology, our first task was not to plug in equipment and start testing, but to sit down and design the exercise properly.

This meant deciding, well in advance, what hardware we would need, which specific features we wanted to put to the test, and what results we could realistically expect to see once everything was up and running.

Some of the headline features that Wi-Fi 7 promises on paper are genuinely difficult to validate in practice. Multi-User MIMO configurations as ambitious as 16x16, for instance, exist mostly in specification sheets rather than in commercially available access points, and at the time we began our work, none of our equipment providers had such models ready for deployment. Rather than chase features that simply weren't accessible yet, we focused our energy on defining a realistic and meaningful set of key performance indicators that we could test and prove.

We settled on five main targets. For a single device connecting to the network, we wanted to see download and upload speeds exceeding 2 Gbps. When multiple devices were connected simultaneously, we aimed for an aggregated download and upload throughput above 3 Gbps. On the latency and stability side, we set a jitter target below 2 milliseconds and a latency target below 8 milliseconds, both of which matter enormously for real-time applications and for the overall perceived quality of a connection.

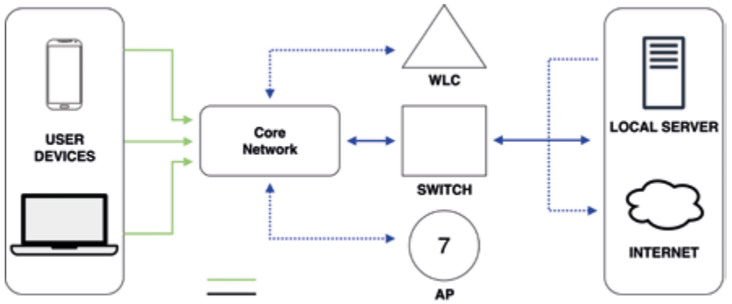
Finally, since one of the defining characteristics of Wi-Fi 7 is its ability to operate simultaneously across multiple frequency bands, we wanted to confirm that Multi-Link Operation could be enabled and sustained across the 2.4 GHz, 5 GHz, and 6 GHz bands at the same time.

This entire technology upgrade was conceived as an extension of Wi-Fi Pro, our commercial B2B service. Although Wi-Fi Pro was originally designed with small office and home office customers, as well as small and medium enterprises, in mind, it had already found strong traction among larger enterprise and corporate clients in Romania, which made the case for pushing the technology forward even more compelling. Since Tp-Link had already been selected as our reference vendor for this service following an earlier RFP process, it made sense to test Wi-Fi 7 using their access points rather than introducing a new, unproven vendor relationship into the mix.

Building the Lab: Architecture, Hardware, and Software

With our KPIs defined and our vendor confirmed that we moved on to designing the actual lab architecture that would allow us to test everything properly. On the hardware side, the heart of the setup consisted of two Wi-Fi 7 access points from Tp-Link: one EAP770 model configured for 4x4 MU-MIMO and a second EAP770 configured for 8x8 MU-MIMO, allowing us to compare performance across two different spatial stream configurations. These access points were connected through a full 10 Gbps switching fabric, again built entirely on Tp-Link switches, ensuring that the wired backbone of the lab would never become the bottleneck during testing. A dedicated WLAN management layer oversaw the configuration and monitoring of the wireless network the trials.

To generate and measure traffic, we used desktop computers equipped with 10 Gbps LAN interfaces and Wi-Fi 7 client cards, which served the dual purpose of initiating our speed tests and hosting a local speed test server. Alongside these desktops, we brought in a range of Wi-Fi 7, Wi-Fi 6E, and Wi-Fi 6 terminals, which allowed us not only to test Wi-Fi 7 in isolation but also to draw direct, side-by-side comparisons against the previous generations of the standard.



On the software front, the setup ran on Windows 11 for both the speed test server and the client machines, with Open Speed Test software handling the actual measurement of throughput, latency, and jitter. We complemented this with a mix of Android and iOS mobile clients, as well as additional Windows-based client devices, to make sure our results reflected the diversity of devices that a real business customer would be using day to day.

This combination of hardware and software gave us a flexible testbed capable of running three distinct categories of tests. We could run device-to-server tests to measure the raw speed and feature set of Wi-Fi 7 on a single connection, we could run multiple-device-to-server tests to understand how the network behaved under simultaneous load from several clients at once, and we could run local speed-test-server-to-Windows-device tests purely to confirm that our wired 10 Gbps backbone was performing as expected and not introducing any artificial ceiling on our wireless results.



Bringing the Lab to Life

The proof-of-concept setup was first physically constructed and deployed in the Tandem office, home to Orange Romania's Development and Innovation team. This was very much a collaborative effort, with our internal engineers working closely alongside colleagues from Prime Telecom and from Tp-Link itself, whose technical support proved valuable in fine-tuning the configuration and making sure the equipment was set up to perform at its best. The result was a compact but fully functional testbed, physically installed within what we refer to internally as the Tandem Engineering Zone, ready to be put through its paces.

Putting It to the Test: Lab Results

Once the setup was live, we ran through several rounds of testing, and we are pleased to report that every single KPI we had defined at the outset was not just met but comfortably exceeded.

We began with single-device testing, and the results genuinely surprised even our own engineering team.

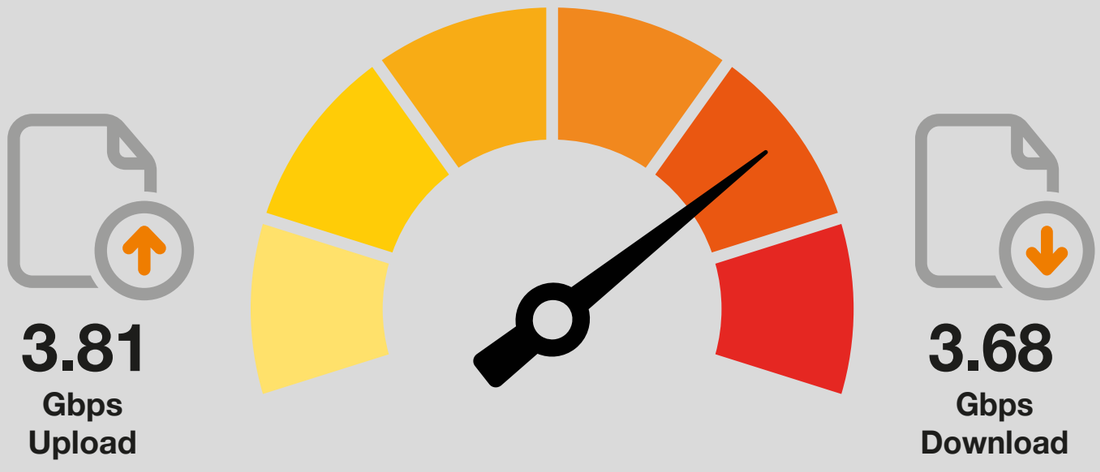
Rather than the 2 Gbps we had set as our minimum target, a single device managed to reach nearly 4 Gbps in combined download and upload throughput, with the best individual test runs recording download speeds above 3.68 Gbps and upload speeds above 3.81 Gbps. That represents nearly double our original target on a single connection, achieved consistently rather than as a one-off outlier.

Moving on to multi-device testing, where several clients were connected and generating traffic at the same time, the network delivered an aggregate throughput of over 5 Gbps, again comfortably clearing the 3 Gbps aggregated target we had set for ourselves. In our most favourable test runs, we recorded aggregate download speeds above 7.21 Gbps and aggregate upload speeds above 5.76 Gbps, figures that speak clearly to just how much headroom Wi-Fi 7 offers when several devices are competing for bandwidth on the same access point.

Latency and jitter, which are often the metrics that make or break the experience for applications like video conferencing, cloud gaming, or real-time collaboration tools, also performed extremely well throughout our testing.

In single-device conditions, jitter averaged around 0.7 milliseconds and latency around 6 milliseconds, both well inside our targets of under 2 milliseconds and under 8 milliseconds respectively. Even under multi-device load, where we would typically expect some degradation, jitter stayed low at around 0.3 milliseconds on average, and latency remained close to 6.5 milliseconds, showing remarkable consistency regardless of how many devices were active on the network at once.

Finally, we confirmed that Multi-Link Operation, one of the true headline features of Wi-Fi 7, functioned exactly as intended, with the 2.4 GHz, 5 GHz, and 6 GHz bands all enabled and working together simultaneously during our multi-device tests. It's worth noting that across our testing campaign we ran many individual test cycles, and the figures we've shared here represent the strongest results for single-device tests and results closest to the overall average for multi-device tests, giving a fair and representative picture of what the technology can achieve rather than cherry-picking only the best possible numbers.



Sharing the Results: showcase to the Orange Group audience

Good results deserve to be shared, and the first opportunity to do so on a wider stage came in the second half of 2024, when a delegation of technical executives from across the Orange Group visited Bucharest. For this occasion, we re-deployed our entire proof-of-concept setup, moving it from the engineering zone to one of the training rooms on the ground floor of the Tandem building. The core setup remained identical to what we had validated in the lab, with the one practical addition being a larger display screen so that visiting colleagues could clearly see live test results as they happened rather than squinting at a laptop screen. The demonstration went smoothly, and all tests performed on the day stayed comfortably within the KPI ranges we had already established during our earlier lab work, giving our Group colleagues direct, first-hand confidence in what Wi-Fi 7 could deliver.

Bringing it closer to home: showcase for Orange Romania B2B teams

After the Group-level showcase, the setup found a new home back in the Orange Engineering Zone within the Tandem building, where it remained on display for several months. During this period, it served a genuinely practical purpose beyond simply being an impressive demo. We used it as a hands-on familiarisation tool, running a series of dedicated sessions with our internal B2B technical and commercial teams so that colleagues across the business could get to grips with both the underlying Wi-Fi 7 technology and the Wi-Fi Pro product itself, in a physical, easily accessible testbed rather than through slides or theoretical briefings alone. This proved to be a valuable step in building internal confidence and technical literacy ahead of any commercial rollout. Once this phase had run its course, the setup was carefully withdrawn from the Tandem building and given a new lease of life at the Orange 5G Lab, where it continues to serve as a demonstration and research asset.

From the lab to the real world: events and partnerships

Successfully proving a technology in a controlled lab environment is one thing, but the true test of any solution is how it performs once it leaves that carefully managed setting and is exposed to the unpredictability of real events and real venues. With our lab testing phase complete and our confidence in the technology firmly established, we moved forward with two full-scale Wi-Fi 7 deployments outside the lab.

The first of these was a temporary but high-visibility deployment for the B-Sides Transylvania event, where we installed a dedicated Wi-Fi 7 hotspot for the duration of the event and carried out on-site testing. The results mirrored what we had already seen in the lab, with all our proposed KPIs achieved under live event conditions, a strong indication that the technology's performance wasn't simply a product of an idealised lab environment.

The second deployment took a slightly different form, as it involved upgrading and extending an existing Wi-Fi hotspot as part of our partnership with Co-work Timisoara. Here, rather than building something from scratch, our task was to bring an already operational wireless service up to Wi-Fi 7 standards and expand its coverage and capacity to meet growing demand. Both of these real-world deployments were supported by Direct Internet Access lines rated at 5 Gbps or higher, ensuring that the wired backhaul could keep pace with the wireless capabilities of the new equipment, and both made use of the very same Tp-Link equipment models we had already validated during our lab testing phase, with all proposed KPIs met once again in these live, operational environments.

Taking Wi-Fi 7 to market: launching it as a commercial service

With the technology proven in the lab, showcased internally and externally, and stress-tested in real event and partnership environments, the final step was to bring Wi-Fi 7 into our commercial B2B offering in a structured and deliberate way. This phase itself broke down into a couple of clear milestones.

The first was internal communication. Before any product could be sold, our own teams needed to understand exactly what it was, how it worked, and why it mattered. This communication effort was led jointly by the Development and Innovation team and the B2B Innovation department, and it was specifically targeted at the teams who would need this knowledge most directly, namely our B2B Sales and Presales colleagues, as well as the Convergent Solutions team within Technical Development.

The second milestone was the formal technical launch of Wi-Fi 7 within the Wi-Fi Pro product's equipment portfolio. This involved the Technical Development and Innovation team proposing a specific and carefully considered set of equipment options, including Wi-Fi 7 access point models such as the EAP772, the EAP773, and the outdoor-rated EAP772 Outdoor variant, along with the appropriate multi-Gigabit switching infrastructure, using mGig and 10 Gbps backhaul connections, and the structured cabling needed to support it all properly. These recommendations were shaped both by the specific requirements coming from B2B clients and by broader technology best practices, ensuring that whatever gets deployed in the field is genuinely fit for purpose rather than simply the newest available hardware.



What this means for Orange Romania

Stepping back from the technical details, it's worth spending a moment on why any of these matters strategically for a company like ours. For a major telecom operator such as Orange Romania, Wi-Fi 7 is far more than an incremental hardware upgrade sitting quietly inside a product catalogue. It represents a genuine commercial and strategic enabler, one that allows us to continue our transition away from being seen purely as a network pipeline provider and towards becoming a driver of digital transformation for our business customers.

By bringing this hardware into our B2B portfolio, we are turning our multi-gigabit infrastructure into an active engine for innovation, one capable of offering genuinely usable, over-the-air multi-gigabit speeds in the range of one to two-plus gigabits per second, particularly when the local wireless network is paired with our multi-gigabit Direct Internet Access services or similarly capable fixed-line connections. That combination, fast fibre-based backhaul paired with equally fast wireless delivery to the end device, is where the real customer value lies, because it removes what has traditionally been one of the last remaining bottlenecks between a business's internet connection and the actual devices its employees use every day.

A closer look at the numbers

It's worth taking a moment to reflect honestly on just how significant an upgrade Wi-Fi 7 represents, not in marketing terms but based purely on what we observed with our own equipment, in our own lab, under our own testing conditions.

Across our testing, we consistently saw single-device speeds increase by somewhere between two and four times compared to what the same devices achieved on Wi-Fi 6, which is a substantial jump by any measure. Alongside that raw speed improvement, latency and jitter also improved noticeably, dropping on average by somewhere between fifty and seventy-five percent compared to equivalent Wi-Fi 6 devices under similar conditions.

When we looked closely at which specific technical features were driving these improvements, two stood out clearly above the rest. On the speed side, the introduction of 320 MHz wide channels made an enormous difference, effectively nearly doubling throughput from roughly 2 Gbps, which is broadly what earlier standards could achieve, up to nearly 4 Gbps under Wi-Fi 7. On the latency and jitter side, it was Multi-Link Operation, the ability to use multiple frequency bands simultaneously and intelligently route traffic across them, that made the biggest measurable difference, smoothing out the kind of inconsistency that has traditionally been the Achilles' heel of wireless networking in busy, congested environments.

Wi-Fi 7

stands as a genuinely major step forward for wireless technology operating in open spectrum, and more broadly for short-range, high-speed, device-agnostic connectivity.

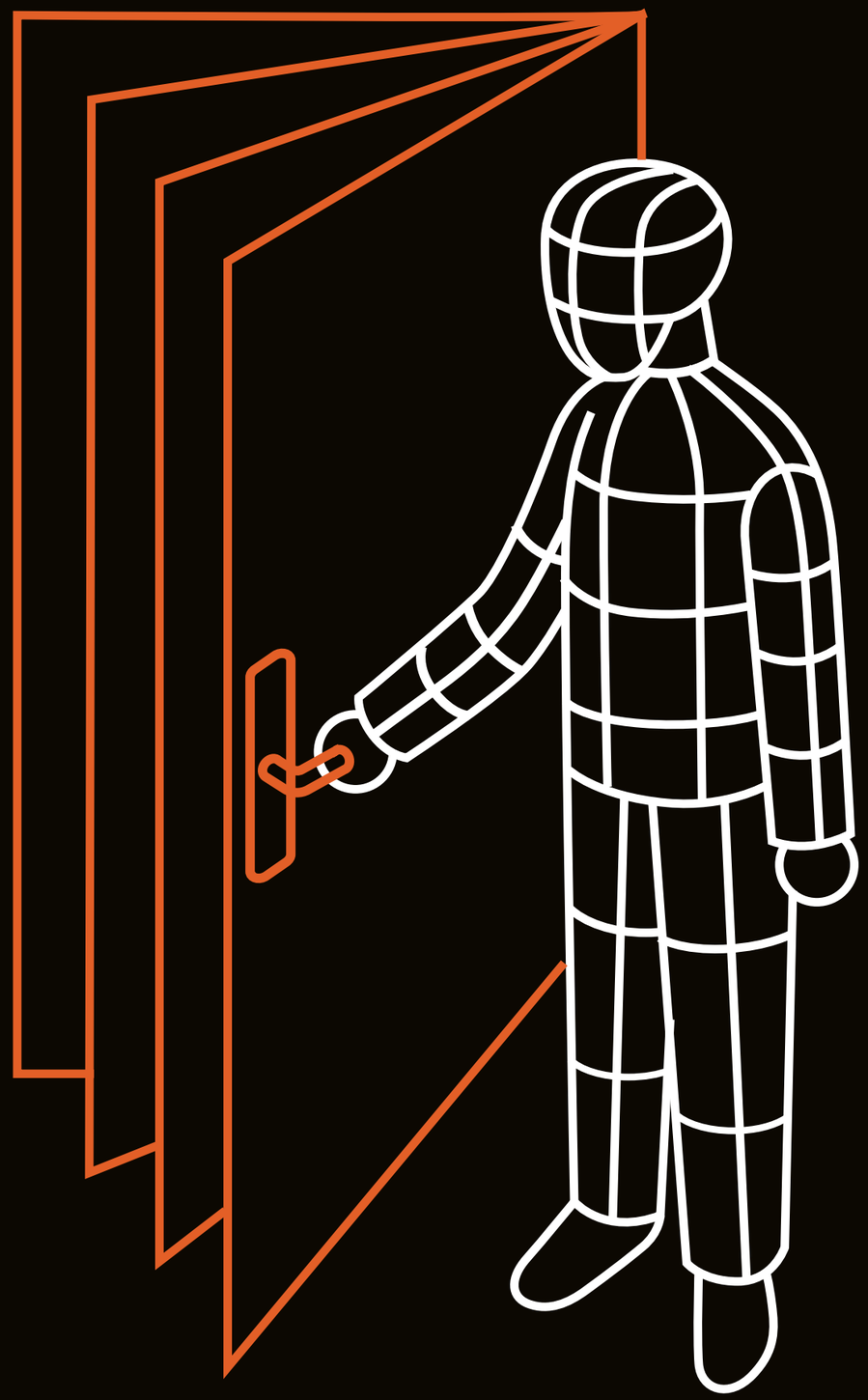
Looking back over the full journey, from the earliest design discussions about which KPIs were even realistic to target, through months of lab testing, public showcases, live event deployments, and finally a proper commercial launch, it's clear that Wi-Fi 7 has moved well beyond being simply a promising specification on paper.

Within Orange Romania, it is now a proven, tested, and commercially available technology, one that our B2B customers can genuinely rely on to deliver the kind of multi-gigabit wireless performance that, until recently, was only achievable over a wired connection.

As we continue to roll this technology out more broadly across our Wi-Fi Pro portfolio, the work documented in this report gives us a solid, evidence-based foundation to build on, and a strong story to tell both internally and to our customers about what innovation at Orange Romania actually looks like in practice.



Education



04

Orange Educational Program (OEP)

While education in a broad sense is an integral part of all innovation-related activities, the guidance of the new academic generation rests primarily with the Orange Educational Program (OEP). OEP is an opportunity for students to link the theory with the practice through labs, internships, and collaboration with Orange experts.

The OEP Program is the result of a combined initiative of the Innovation and Development department and the academic community, developed across four pillars: Human Resources, Brand, Corporate Social Responsibility, and Education & Research. Seen in this light, it is not only an educational program, but rather a mechanism through which Orange Romania helps students move from academic learning towards professional practice, applied research and innovation. In other words, OEP serves as a bridge between university education and real industry practice, being an essential component of the Orange Romania innovation ecosystem, alongside Orange 5G Lab, focused on research and experimentation, and Orange Fab, focused on startup acceleration. Together, the three initiatives cover the full chain from talent formation to research and testing, and, finally, to entrepreneurial acceleration.

OEP in 2025-2026 academic year and beyond

This year, OEP maintains focus on fostering young talents passionate about telecommunications, cybersecurity, data, networks and emerging digital technologies through three tightly connected activity lines: first, internships and mentoring; second, support for competitions and hackathons; and third, support for conferences.

Internships and mentoring: 8 cities, 13 universities Cluj (Universitatea Babeș-Bolyai, Universitatea Tehnică din Cluj-Napoca); Sibiu (Universitatea Lucian Blaga din Sibiu); Brașov (Universitatea Transilvania Brașov); Timișoara (Universitatea de Vest din Timișoara, Universitatea Politehnica din Timișoara); Suceava (Universitatea „Ștefan cel Mare” din Suceava); Iași (Universitatea „Alexandru Ioan Cuza” din Iași, Universitatea Tehnică „Gheorghe Asachi” din Iași); București (Universitatea Națională de Știință și Tehnologie Politehnica București, Universitatea din București); Constanța (Universitatea Ovidius din Constanța, Universitatea Maritimă din Constanța).

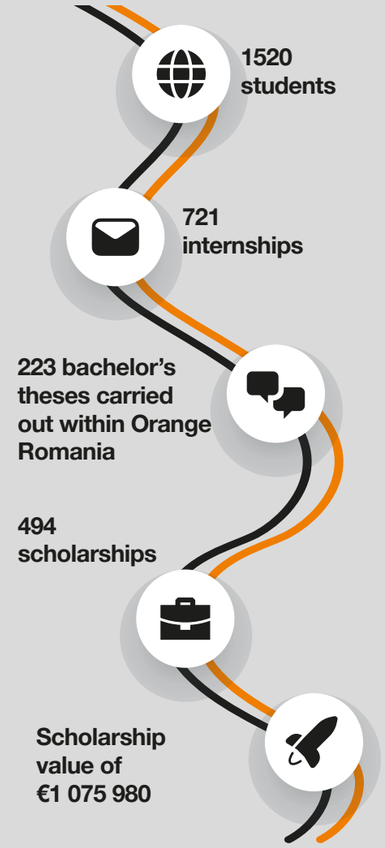
Competitions and Hackathons: UNbreakable, RoCSC – Romanian Cyber Security Challenge, OSC – Olimpiada de Securitate Cibernetică, ECSC – European Cyber Security Challenge

Conferences: ATOMS, DAS, COMM, BlackSeaCom, ISETC



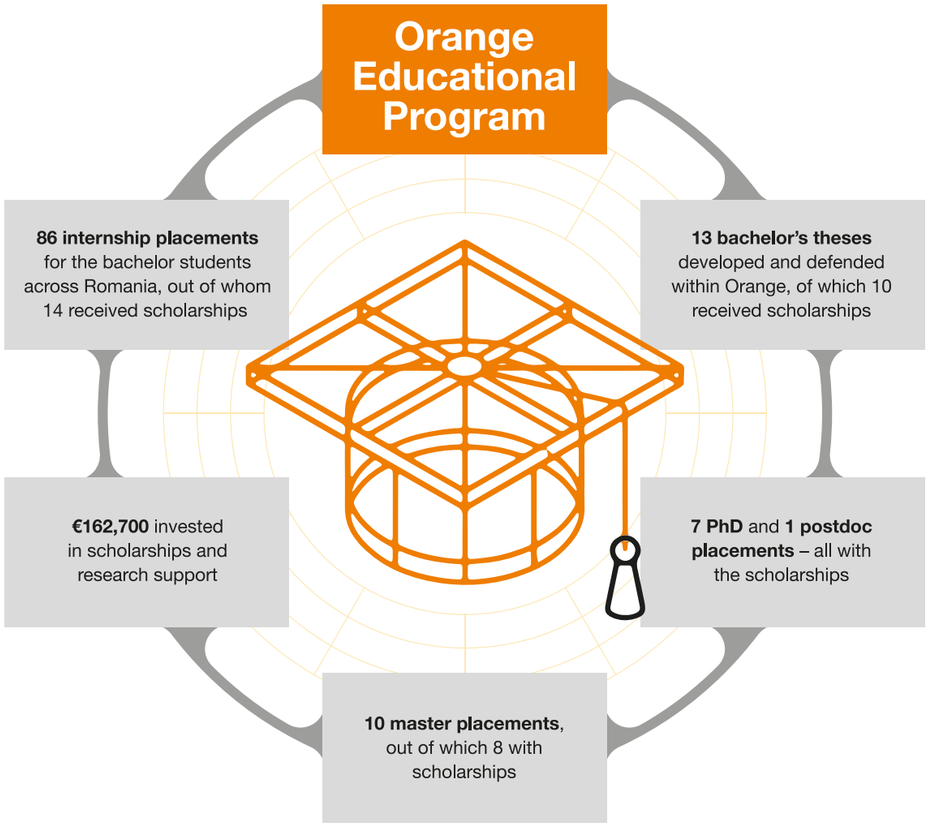
OEP since 1998

The Orange Education Program could be considered one of the longest-standing talent-development activities associated with Orange Romania – founded in 1998; in 2026, it marks its 28th year



The **internship and mentoring lines** remain the most direct expression of the program's purpose: each spring OEP announces educational packages each built around an internship position, summer practice, an internship mentor, the possibility to develop the bachelor's thesis within Orange, and a bachelor's scholarship that could be extended beyond the first four months. Moreover, the program supports the most talented and engaged students for the Master thesis and even for the doctorate.

For the 2025–2026 academic year, Orange officially offered 14 educational packages, while the official internship calls for 2026-2027 increased this number to 16 with topics in 5G, B5G/6G, AI/ML, data analytics and fibre/voice/data solution design.





OEP is an opportunity for students to link the theory with the practice through labs, internships, and collaboration with Orange experts.

This same logic of continuity is also reflected in the program's public visibility. While most dissemination happens through the support of competitions and conferences, internship-related activities also contribute significantly to it. Besides the natural word-of-mouth among the academic environment, OEP also organizes the events to showcase the achievements of its students. The highlight of this year was a "Theses Competition", an open event where bachelor students who developed their thesis within the OEP and under the guidance of the Orange experts publicly presented their works. Traditionally, the competition recognizes excellence across three evaluation criteria: Originality and Practical Applicability, Relevance to the Topic and Scope of Coverage, and Documentation and Technical-Scientific Rigor. This year, 6 out of the 13 submitted theses were distinguished, with two awards granted in each category:

Originality and Practical Applicability:

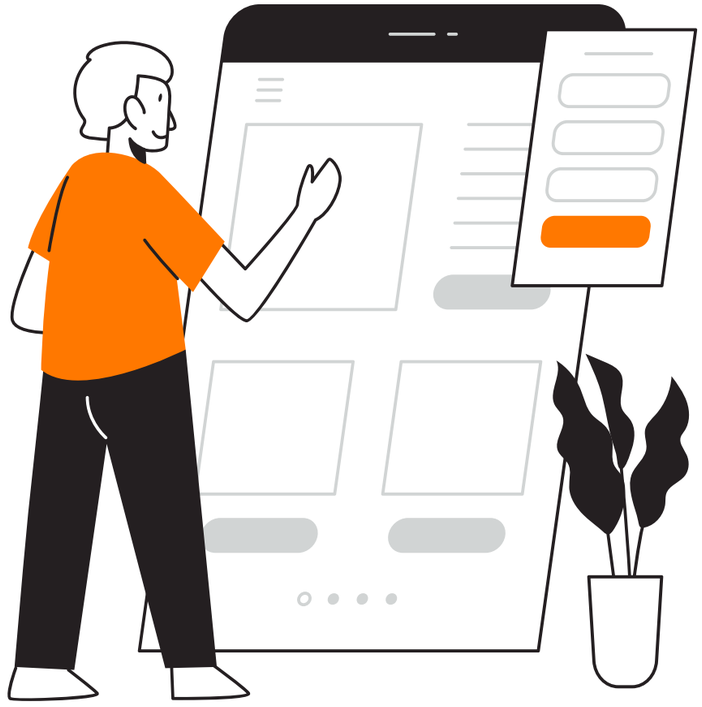
- "IoT System for Water Consumption Monitoring Secured Using Blockchain";
- "Indoor Human Detection Using Bistatic 6G ISAC";

Relevance to the Topic and Scope of Coverage:

- "Automated Anomaly Detection System for Cloud-Native 5G/6G Infrastructures";
- "Architecture and Implementation of LLM-Based Autonomous Agents Using Internal Orchestration Frameworks in Secure Enterprise Environments".

Documentation and Technical-Scientific Rigor:

- "Anomaly Detection and Security Assessment of uRadMonitor IoT Sensor Networks Through LoRaWAN Attack Injection";
- "Automated Monitoring and Impact Assessment System for Civil Infrastructure Works on Communication Networks".



The **competitions activity line** is designed not only to support individual competitions but also to create a continuous development pathway for participants, highlighting the OEP's role in strengthening the broader innovation ecosystem.

A special focus of the Orange Educational Program is dedicated to supporting cybersecurity events that create opportunities for students to learn, compete, and advance through progressively more challenging stages of development. Through its long-term commitment, OEP contributes to a connected ecosystem comprising **UNbreakable Romania, Romanian Cyber Security Challenge (RoCSC), Romanian National Cyber Security Olympiad (OSC), and European Cyber Security Challenge (ECSC)**. Together, these initiatives form a continuous pathway, enabling participants to progress from their first cybersecurity competition to representing Romania at the European level.



UNbreakable

Romania is the most comprehensive cybersecurity programme for high school and university students in the country. Co-organised by Bit Sentinel and Orange Romania and hosted on the CyberEDU educational platform developed by Bit Sentinel and supported by Orange, the program has grown from a niche competition into a nationally recognized launchpad for cybersecurity careers.

First launched in 2020, UNbreakable Romania set out to address a structural problem: Romania's universities and high schools produced relatively few graduates with the hands-on, practical cybersecurity skills that the private sector and public institutions urgently needed. Traditional academic curricula, while strong in theory, rarely exposed students to real-world attack and defence scenarios, CTF (capture the flag) challenges, or the collaborative dynamics of incident response.

Orange Romania joined from the outset as co-organiser and main sponsor, contributing not only financial resources but deep technical expertise. The company's cybersecurity experts have served as mentors, trainers, and challenge designers across every edition of the program, bridging the gap between academic knowledge and industry practice.

UNbreakable: program stages

Registration and Orientation
Free registration on CyberEDU and introduction to the program

Bootcamp
Cybersecurity training through practical exercises, tutorials, and expert mentoring

Individual Online Competition
Individual online competition and qualification for advanced stages

Team Online Competition
Team-based cybersecurity challenges for the highest-ranked participants

Onsite Grand Final
Live onsite competition bringing together the top-performing teams

The 2024 final took place in Brașov; the 2025 and 2026 finals were held in Bucharest and hosted by Orange in Tandem headquarters.

Orange Romania's involvement in UNbreakable Romania extends well beyond just a partnership. We set out to deliver technical expertise and realistic educational and corporate networks, for the participants to further their talents, providing:

- **Expert Trainers.** Orange Romania's cybersecurity specialists deliver lectures and masterclasses during the bootcamp phase, bringing real-world threat intelligence and industry experience directly to students.
- **Technical Mentorship.** Orange experts answer participants' questions throughout the training phase and contribute to the design of challenges that reflect current industry scenarios.
- **Talent Pipeline.** Orange Romania uses the program as one of its primary channels for identifying talented young cybersecurity professionals for internships and graduate employment.
- **University Network.** Orange Romania promotes UNbreakable through the Orange Educational Program, its long-standing engagement network with partner universities across Romania, ensuring broad geographic and institutional reach.
- **Platform Support.** Orange Romania co-funds and supports the CyberEDU platform, ensuring it remains a best-in-class, scalable environment for tens of thousands of users.

"UNbreakable Romania is clear proof that through collaboration between business and educational institutions, competition can turn into a broad training programme — a launch pad for the professionals we so desperately need."

Editions completed (2017–2025)
8+

Total number of participants
~4,000+

2024 record registrations
1,400+

Under-25 competitors in 2024 individual round
93%

2024 participants interested in internships/jobs
~80%

Prize pool per edition (powered by Orange & Bit Sentinel)
€8,000+

2025 target participants
~2,000

The 8th edition of UNbreakable Romania set a target of nearly 2,000 participants — a 40% increase over the record set in 2024. The expansion of local, city-level CTF preparation events to major cities across the country — Bucharest, Cluj-Napoca, Iași, Timișoara, Constanța — reflects Orange Romania's commitment to geographic inclusivity.

Every talented young person in Romania should have access to world-class cybersecurity education, regardless of where they live or study.

Romanian Cyber Security Challenge

The Romanian Cyber Security Challenge (RoCSC) is a premier national CTF cybersecurity championship. Launched in 2015 as a public-private initiative, RoCSC has grown over nearly a decade into the definitive proving ground for Romania's most gifted young cybersecurity talents, directly feeding Team Romania's roster for the European Cyber Security Challenge.

RoCSC is a collaborative effort spanning government agencies, intelligence services, and leading private-sector partners. The competition is co-organised by:

- The Romanian National Cyber Security Directorate (DNSC)
- The National Cyberint Centre within the Romanian Intelligence Service (SRI)
- The National Association for Information Systems Security (ANSSI)
- The National Coordination Centre for Cybersecurity (NCC-RO)

Orange Romania has been a core partner of RoCSC since the competition's earliest editions, contributing both financially and with technical expertise in CTFs design, and the provision of training resources for finalists preparing for the European championship. RoCSC operates as a two-stage annual CTF event and welcomes participants in 3 categories: juniors (up to 20 years old), seniors (ages 21 to 25), and open (all ages).

RoCSC: program stages

Online Qualification: Three-day online competition covering web and mobile security, cryptography, reverse engineering, digital forensics, network traffic analysis, and exploit development.

Onsite Final: Multi-day championship in Bucharest bringing together the top-qualified competitors.

Each year Orange Romania contributes to RoCSC through:

- **Challenge Design and Technical Oversight** — Orange Romania's cybersecurity team contributes to designing and validating competition challenges, ensuring they are technically rigorous and reflective of real-world attack scenarios.
- **Team Romania Preparation** — Following the RoCSC final, Orange Romania experts participate in the summer bootcamp during which Team Romania prepares intensively for the ECSC. Ioan Constantin, Cyber Security Expert at Orange Romania, has served as the national team's coach and trainer.
- **Prize Sponsorship** — Orange Romania co-funds the prize pool that recognizes excellence at RoCSC.
- **Career Opportunities** — RoCSC finalists gain visibility with Orange Romania's talent acquisition teams, opening doors to internships and employment for the country's most capable young security professionals.

Orange will continue its long-standing partnership with RoCSC, supporting the competition through technical expertise, mentorship, and talent development. The company remains committed to fostering cybersecurity excellence in Romania and contributing to the growth of the national cybersecurity ecosystem alongside its institutional and academic partners.

Romanian National Cyber Security Olympiad

Romanian National Cyber Security Olympiad, represents a landmark achievement in Romanian education policy. In the 2023–2024 academic year, the Romanian Ministry of Education officially included the competition in the national calendar of school Olympiads for the first time in the country's history, placing cybersecurity on an equal footing with mathematics, physics, and computer science. The inclusion of a cyber security olympiad in the Ministry of Education's official calendar carries profound implications for Romania's long-term talent supply. It sends a clear signal to students, teachers, and parents that cybersecurity is not a niche hobby but a strategically important discipline commanding the same institutional weight as any other STEM subject. It unlocks access to institutional resources — school preparation hours, teachers' professional development budgets, regional competition infrastructure — that were previously unavailable to cybersecurity education.

Program stages

County Phase – High school students from all Romanian counties and Bucharest compete in a theoretical examination on fundamental cybersecurity concepts and a practical CTF examination covering web security, cryptography, digital forensics, and system security.

National Phase – The top county performers compete in Bucharest in a combined theoretical and practical examination. The top 30 qualify for the Barrage Round, while the top 15 are selected for Romania's extended national team preparing for the European Cyber Security Challenge (ECSC).

For Orange Romania, the olympiad's establishment validates years of advocacy and direct engagement with educational institutions. We believe that sustainable improvement in Romania's cybersecurity talent pipeline requires intervention at the secondary school level, reaching students before they have chosen a university pathway and inspiring them to consider cybersecurity as a vocation. Each year Orange continues the support through:

- **Curriculum and Challenge Development** — Orange Romania's experts collaborate in the Central Commission of the Cyber Security Olympiad (CCSSO), responsible for designing examination topics, setting difficulty parameters, and ensuring alignment with international cybersecurity standards.
- **Training Resources** — CyberEDU, supported by Orange, provides the official preparation platform for the participants, with free access to educational modules covering all topic areas.
- **Team Romania Preparation** — the olympiad serves as one of the two main qualification pathways into Team Romania for the ECSC. Orange Romania experts join the intensive summer bootcamp, training the preliminary national squad.

Following the successful inaugural OSC in 2024, Orange Romania is committed to deepening its engagement with the Ministry of Education to develop teacher training resources, school-level curriculum materials, and county-level support structures. The goal is not merely to run a competition but to make cybersecurity literacy a genuine component of Romanian secondary education.

European Cyber Security Challenge

European Cyber Security Challenge (ECSC) is the flagship international cybersecurity competition for young people across Europe, organized under the auspices of the European Union Agency for Cybersecurity (ENISA).

Each year, national teams composed of the most talented young cyber professionals — aged 14 to 25 — from EU Member States and EFTA countries compete in a multi-day event combining CTF challenges, attack-and-defence scenarios, and expert evaluations.

The ECSC 2019, hosted in Bucharest, marked a milestone for Romanian cybersecurity. Organized by the Romanian Intelligence Service, CERT-RO, ANSSI, and Orange Romania, the competition brought together teams from 20 European countries. Trained by Ioan Constantin, Cyber Security Expert at Orange Romania, Team Romania won the European title on home soil, building on two previous runner-up finishes and highlighting the strength of Romania's cybersecurity talent pipeline.

Regarding the structure, the ECSC is a multi-day competition where national teams of 10 competitors – five Juniors (up to 20 years old) and five Seniors (21–25 years old), supported by two reserves – compete across a broad range of cybersecurity disciplines, including web and mobile security, cryptography, reverse engineering, digital forensics, attack-and-defence, operating system security, and programming.

Team Romania is assembled through a rigorous dual-pathway qualification process integrating both the RoCSC and the OSC.

The extended national squad is formed from the top finishers of both competitions — typically around 30 individuals — who then enter an intensive summer bootcamp.

The bootcamp is organized jointly by the National CyberINT Centre, DNSC, and ANSSI, with Orange Romania and Bit Sentinel as technical partners.

Orange Romania's cybersecurity experts play a hands-on role in training sessions, challenge design, and performance evaluation. The final team of ten is selected from bootcamp performance.

Romania has been a participant in the ECSC since the competition's early editions and has established itself as one of Europe's most formidable cybersecurity nations.

Orange Romania has been one of Team Romania's primary supporters for a minimum of five consecutive years.

Like the preceding competitions, Orange contributes not just financially but also training the national team year after year.

Ioan Constantin's role as national coach exemplifies this commitment. His knowledge of European competition trends, his experience in enterprise security operations, and his personal investment in each team member's development have been decisive contributions to Romania's results.

Together, UNbreakable, RoCSC, CSO and ECSC form a coherent cybersecurity talent development ecosystem.

Designed by Orange Romania and its partners as an integrated pathway, the four programs enable participants to continuously develop their skills and progress based on demonstrated performance.

Students typically begin with UNbreakable Romania, an accessible entry point combining guided learning and practical competitions.

The strongest participants advance to the CSO and the RoCSC, with the top competitors ultimately selected to represent Romania at the ECSC.

Central to the coherence of the ecosystem is CyberEDU, the educational platform developed by Bit Sentinel and supported by Orange Romania through Orange Fab startup accelerator. CyberEDU serves as the common digital infrastructure across all four programmes: it hosts over 30,000 registered users and provides continuous access to practice challenges from previous editions of all four competitions. A student who discovers the platform through UNbreakable can spend months training on past RoCSC and ECSC challenges before sitting a formal competition — a compounding educational advantage that reflects Orange Romania's long-term investment philosophy.

Romania's cybersecurity ecosystem could be considered one of the most complex models in the Europe from the point of view of integrity: it has been built through long-term collaboration between Ministry of Education, academia, industry, and cybersecurity community. At the same time, the scale of the global cybersecurity challenge shows no sign of diminishing. With 4.7 million professionals needed globally and a threat landscape growing in complexity with the rise of AI-powered attacks, ransomware-as-a-service, and nation-state cyber operations, the work of building Romania's cyber talent pipeline is more urgent than ever.

Orange Romania is proud to be one of the driving forces of this work, contributing not only through financial support, but also through the expertise and commitment of its people: our experts volunteer their time to mentor students, design competition challenges, deliver training, and support national teams. Orange Romania's role in this ecosystem is unique among private-sector actors. No other company has been as consistently present, across as many programs, with as deep a technical and human commitment, over as long a period.

Obviously, Orange Romania's engagement is not purely philanthropic, it is also strategically rational. A stronger national cybersecurity talent pool means better security for Orange's own infrastructure, a richer hiring market for its own teams, and a safer digital environment for the 10+ million customers Orange has in Romania.

This commitment is grounded in a belief that is easy to state and difficult to execute: that the most important investment any organization can make in the long-term security of the digital world is in people. Technology changes. Threat actors adapt. Regulations evolve. But a generation of well-trained, highly motivated, ethically grounded cybersecurity professionals provides a durable and renewable source of national security and economic resilience.

Finally, **the conference line** completes the picture, taking students and Orange researchers one step further, from training and competition towards scientific visibility. This year, OEP continued to support five key conferences:

ATOMS 2026 – Advanced Topics on Measurement and Simulation, took place in Cluj-Napoca, 13–15 May 2026, organized by the Technical University of Cluj-Napoca and focused on advanced topics in measurement and simulation, including telecommunications, communication systems, AI, beyond-5G, and 6G themes.

DAS 2026 – 18th International Conference on Development and Application Systems, took place in Suceava, 21–23 May 2026 bringing together work in systems, automation, communications, computer networks, electronics and software engineering. At this conference Orange contributed not only as partnerbut also through the direct participation, presenting the paper "Performance Evaluation of OTFS and OFDM Technologies in High Mobility Scenarios",

Looking ahead, Orange Romania remains committed to supporting the flagship conferences that have become key meeting points for the national research and innovation community. At the same time, the program will continue to explore opportunities to engage with new scientific and technology conferences that align with its educational and innovation objectives. The first planned initiative for 2027 is already confirmed – the International Conference on Engineering, Technology and Innovation (ICE 2027), supported by Orange Romania.

explicitly linked to future 6G ISAC-type architectures.

COMM 2026 – 16th International Conference on Communications took place in Bucharest on 28–29 May 2026, with topics spanning communication technologies, mobile and wireless networks, network services, AI, quantum communications, security, cloud and edge computing, and optical communications.

BlackSeaCom 2026 – IEEE International Black Sea Conference on Communications took place in Bucharest on 8-11 June.

ISETC 2026 – 17th International Symposium on Electronics and Telecommunications, scheduled to take place on 4-6 November, in Timișoara

Taken together, these activity lines demonstrate the complementary nature of the Orange Educational Program. Internships and thesis mentoring connect academic learning with real industry practice, competitions identify and develop exceptional talent, while conferences create opportunities for knowledge exchange, research dissemination, and collaboration between academia and industry. Together, they form a continuous framework that supports students throughout different stages of their educational and professional development.

As technology, research priorities, and labour market needs continue to evolve, so does the Orange Educational Program. Rather than following a fixed model, OEP continuously adapts its activities, partnerships, and areas of focus to address emerging technologies and new educational challenges. This flexibility has enabled the program to remain relevant for nearly three decades and will continue to guide its evolution in the years ahead, strengthening Orange Romania's contribution to education, research, and innovation alongside with Orange Fab and Orange 5G Lab.



Per aspera ad astra



Orange Educational Program

- Scholarships
- Courses and workshops
- Internships

education.orange.ro



05

Innovation Ecosystems: Where Entrepreneurship Creates the Greatest Value

Innovative entrepreneurship rarely succeeds in isolation. The most dynamic startups emerge and grow within innovation ecosystems that connect entrepreneurs with universities, corporations, investors, research organizations and public institutions. The quality of these relationships increasingly determines the ability of regions and countries to transform innovation into sustainable economic growth and international competitiveness.

The growing importance of innovative entrepreneurship has fundamentally changed the way innovation is understood and managed. While entrepreneurship has traditionally been associated with the capabilities of individual founders and companies, evidence demonstrates that successful innovation depends equally on the quality of the surrounding environment. Entrepreneurs require access not only to capital and talent but also to customers, specialized knowledge, research infrastructure, mentors, strategic partners and supportive public policies. Together, these elements form what is commonly referred to as an innovation ecosystem.

The concept of an innovation ecosystem has gained momentum over the past two decades as governments, corporations and academic institutions have sought to understand why some regions consistently generate innovative companies while others struggle to translate scientific knowledge into commercial success. Although definitions vary, most describe **an innovation ecosystem** as a network of interconnected organizations and individuals whose interactions facilitate the creation, development and commercialization of innovation.

Unlike traditional industrial clusters, innovation ecosystems are characterized less by geographical proximity than by collaboration and knowledge exchange. Universities, research institutes, startups, corporations, investors, public authorities and intermediary organizations each contribute complementary capabilities. Innovation emerges not from the actions of a single participant but from the continuous interaction between these actors.

Within these ecosystems, universities and research institutions generate scientific knowledge and develop highly qualified talent. Entrepreneurs identify market opportunities and transform research into commercially viable products and services. Investors provide financial resources that enable companies to develop and scale. Public institutions establish regulatory frameworks, invest in research and create programs that encourage entrepreneurship. Corporations contribute market access, industry expertise,



technological infrastructure and opportunities for commercial deployment.

Increasingly, corporations have become active participants rather than passive beneficiaries of innovation ecosystems. Their role has evolved beyond purchasing innovative technologies after they reach market maturity. Many organizations now engage much earlier in the innovation process, collaborating directly with startups to validate technologies, co-develop solutions and accelerate commercial adoption. Corporate accelerators, venture client programs, innovation laboratories and strategic partnerships have become important mechanisms for integrating entrepreneurial innovation into established organizations.

This collaborative model benefits all participants. Startups gain access to industry expertise, customers and real operating environments that would otherwise be difficult to obtain. Corporations benefit from faster access to emerging technologies, reduced innovation risk and greater organizational agility. Universities strengthen the societal impact of their research through commercial application, while investors benefit from stronger market validation and reduced technological uncertainty.

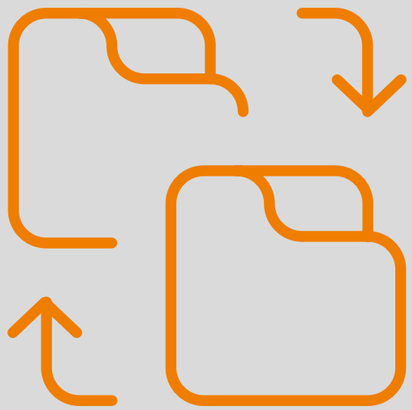
Innovative entrepreneurship delivers the greatest impact within collaborative innovation ecosystems.

Successful ecosystems combine the complementary strengths of startups, corporations, academia, investors and public institutions.

Trust, knowledge exchange and long-term collaboration are fundamental characteristics of high-performing innovation ecosystems.

Corporate innovation programs, including accelerators, play an important role in connecting entrepreneurial innovation with market opportunities.

Orange Romania contributes to Romania's innovation ecosystem by creating structured collaboration mechanisms that connect startups with technology, expertise and customers.





Romania's innovation ecosystem grew during the past decade. Innovation hubs, university entrepreneurship centres, digital innovation hubs, startup accelerators and technology communities have expanded across the country, strengthening collaboration between entrepreneurs, researchers and established companies. Increasing participation in European research programs and stronger engagement from multinational corporations have further contributed to the maturity of the national innovation ecosystem.

Orange Romania's approach to innovation reflects this ecosystem philosophy. The company treats innovation as a collaborative activity, actively working with startups, universities, research organizations, public institutions and technology partners. Through Orange Fab, the Orange 5G Lab, the Orange Educational Program and collaborations within the Orange Group innovation network, the company contributes to strengthening Romania's innovation ecosystem while supporting the development and commercialization of innovative technologies.

Orange Romania's contribution to the national innovation ecosystem extends beyond technology deployment. Through initiatives such as Orange Fab, the Orange 5G Lab, partnerships with universities, participation in European research and innovation projects, and collaboration with startups, the company facilitates knowledge exchange between academia, entrepreneurs, corporate experts and customers. These initiatives create practical opportunities for validating emerging technologies, accelerating commercial adoption and supporting the development of Romania's digital economy. By connecting innovative entrepreneurs with technical expertise, business challenges and market opportunities, Orange contributes to building an innovation ecosystem in which collaboration becomes a catalyst for sustainable growth.

Open Innovation: Redefining Corporate Competitiveness

Open Innovation has fundamentally changed how organizations create value. Rather than relying exclusively on internal ideas and technologies, companies increasingly combine their own capabilities with external knowledge, entrepreneurial talent and strategic partnerships. In today's innovation landscape, competitive advantage depends not only on what an organization develops internally, but also on how effectively it collaborates with the wider innovation ecosystem.

Open Innovation is commonly defined as the purposeful management of knowledge flows across organizational boundaries to accelerate internal innovation and expand markets for the external use of innovation. This definition reflects two complementary processes. Organizations bring external ideas, technologies and expertise into the company while simultaneously allowing internally developed technologies to create value through partnerships, licensing or new business models beyond traditional organizational boundaries.

Knowledge is no longer concentrated within a limited number of corporate laboratories. Universities, startups, research institutes, technology communities and even customers actively contribute to technological development. Digital platforms, open-source software and international research collaborations further accelerate the circulation of knowledge across industries and geographical borders.

As a result, innovation has become less about ownership of knowledge and more about the ability to identify, combine and apply knowledge effectively. Open Innovation therefore complements rather than replaces traditional research and development.

For startups, Open Innovation creates opportunities that extend beyond access to financing. Collaboration with established organizations provides access to industrial expertise, specialized infrastructure, customer networks and commercial validation. These resources significantly accelerate the transition from technological development to market adoption.

For corporations, collaboration with startups offers equally important advantages. Entrepreneurial companies often possess highly specialized expertise within emerging technological domains and operate with development cycles considerably shorter than those of large organizations. By engaging with startups at an early stage, corporations gain earlier visibility into emerging technologies while reducing the time and resources required to explore new business opportunities.

Open Innovation expands corporate innovation beyond organizational boundaries.

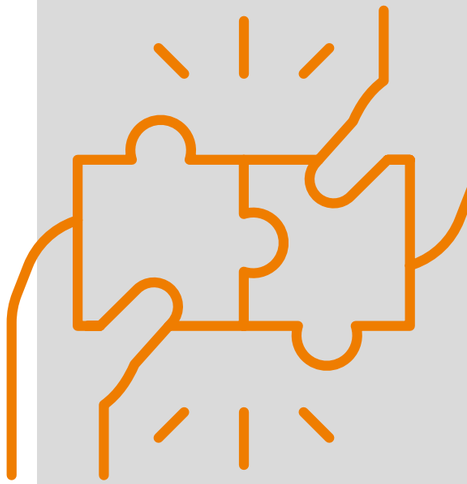
Internal R&D remains essential but is increasingly complemented by external knowledge and partnerships.

Competitive advantage depends on an organization's ability to identify, integrate and scale innovation regardless of its origin.

Startups contribute with specialized expertise, agility and faster experimentation.

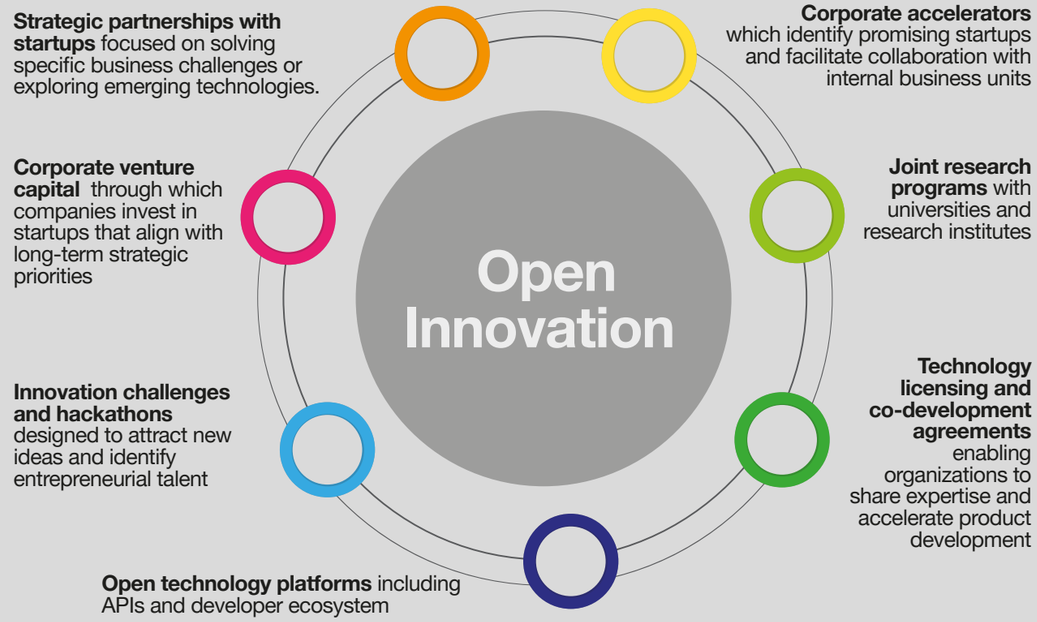
Corporations contribute with infrastructure, customers, operational expertise and commercial scale.

Open Innovation creates value by combining the complementary strengths of multiple participants within the innovation ecosystem.



Open Innovation in practice

While the principles of Open Innovation are broadly applicable across industries, organizations implement them using different operational models depending on their strategic objectives.



These mechanisms differ in structure and objectives, but they share a common principle: innovation becomes a collaborative process involving multiple organizations rather than an activity confined within corporate boundaries.

Increasingly, organizations combine several of these approaches into comprehensive innovation strategies that balance internal research with external collaboration. This integrated model allows companies to remain focused on their strategic priorities while continuously accessing new technologies, business models and entrepreneurial capabilities.

For many industries, particularly telecommunications, healthcare, financial services and advanced manufacturing, Open Innovation has become the dominant approach to innovation management.

Orange Group has progressively embedded Open Innovation into its innovation strategy by combining internal research capabilities with structured collaboration across the broader innovation ecosystem. Initiatives such as Orange Fab, Orange Ventures, the Orange 5G Lab and participation in European research programs illustrate how external innovation is integrated into business development, technology validation and commercial deployment. Rather than viewing startups solely as technology suppliers, Orange increasingly collaborates with them as long-term innovation partners capable of contributing to the development of new products, services and customer experiences.

Corporate Accelerators: From Startup Support to Strategic Business Value

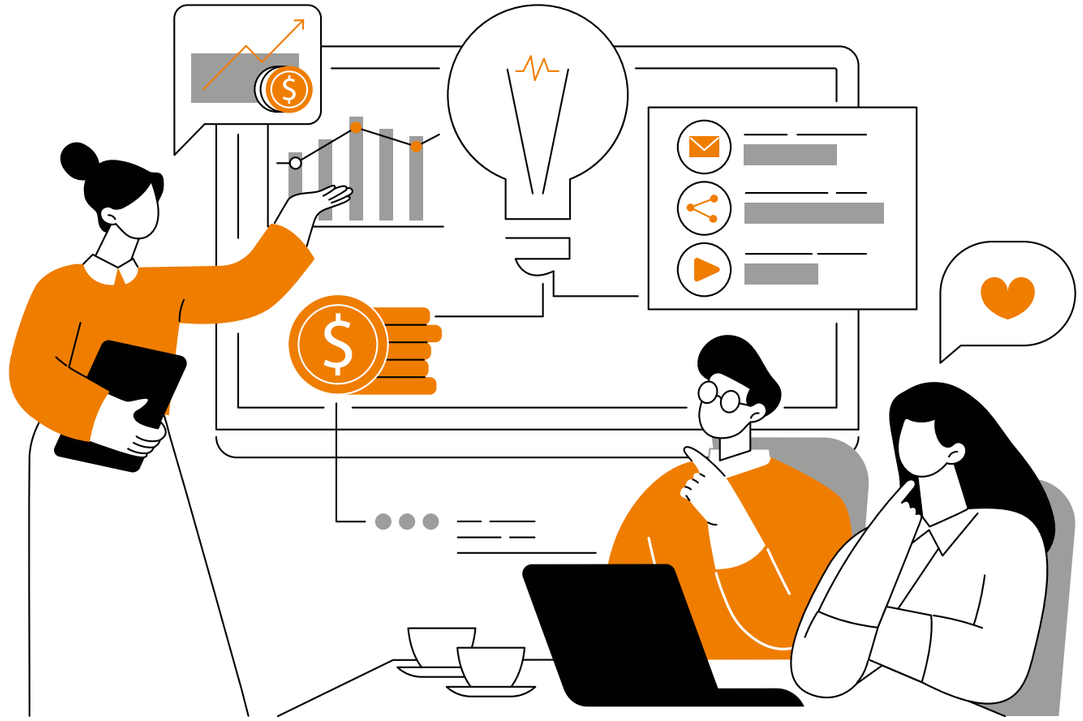
Corporate accelerators have evolved beyond traditional startup support programs. Today, they are strategic business instruments that enable organizations to identify emerging technologies, validate innovative solutions and accelerate digital transformation. Their primary objective is not to invest in startups, but to create business value by connecting entrepreneurial innovation with concrete corporate challenges.

The rapid adoption of Open Innovation has fundamentally changed the relationship between corporations and startups. Beyond traditional supplier relationships or acquisitions, many organizations now establish structured programs that enable systematic collaboration with entrepreneurial companies. Among these mechanisms, corporate accelerators have become one of the most widely adopted models for integrating external innovation into corporate strategy.

Corporate accelerators first emerged during the early 2010s, inspired by the success of independent startup accelerators such as Y Combinator and Techstars. While these programs focused primarily on helping entrepreneurs refine business models, attract investment and prepare for market entry, corporations quickly recognized that similar structures could serve a different purpose: accelerating innovation inside established organizations.

Traditional startup accelerators are designed primarily to support entrepreneurs. Their success is generally measured by investment raised, company survival rates or valuation growth. **Corporate accelerators**, by contrast, are established to create value for both startups and the corporation. Their primary objective is to facilitate collaboration that leads to technology validation, pilot projects, commercial partnerships or the integration of innovative solutions into existing products and services.

Consequently, the performance of a corporate accelerator cannot be measured solely by the number of startups participating. More meaningful indicators include the number of pilot projects launched, commercial contracts signed, technologies adopted by business units and measurable business outcomes generated through collaboration.



This evolution reflects a broader shift in corporate innovation. Increasingly, organizations recognize that the objective is not simply to discover innovative technologies but to solve concrete business challenges. Startup collaboration therefore begins not with technology itself but with clearly identified organizational needs.

Business units play a central role in this process. Rather than operating independently from the rest of the organization, successful corporate accelerators work closely with commercial, technical and operational teams to identify strategic priorities. Startup scouting activities are then aligned with these priorities, ensuring that selected companies address real business opportunities rather than hypothetical use cases.

This business-driven approach significantly increases the likelihood that collaborations will progress beyond demonstrations or proof-of-concept activities.

Several characteristics distinguish corporate accelerators from other forms of startup engagement.

- provide structured access to corporate expertise. Startups gain direct interaction with technical specialists, product managers, commercial teams, legal experts and senior decision-makers. This access enables entrepreneurs to better understand customer requirements, regulatory constraints and operational realities.
- facilitate technology validation in real operational environments. Unlike laboratory demonstrations, pilot projects conducted within corporate infrastructure provide valuable insights regarding technical performance, integration requirements and customer acceptance. This validation substantially reduces uncertainty for both startups and corporations.
- create opportunities for commercial collaboration. Successful pilot projects frequently evolve into long-term customer relationships, joint product development or integration into existing service portfolios. Commercialization therefore becomes the primary measure of success rather than the completion of an accelerator program itself.
- strengthen organizational learning. Business units gain exposure to emerging technologies and entrepreneurial ways of working, while startups acquire deeper understanding of enterprise customers, procurement processes and industry-specific requirements. Knowledge therefore flows in both directions, contributing to continuous organizational learning.



Over the past decade, corporate accelerators have become common across technology-intensive industries. Telecommunications operators, financial institutions, manufacturing companies, healthcare organizations and energy providers increasingly use accelerator programs to explore technologies including artificial intelligence, cybersecurity, advanced connectivity, sustainability solutions, industrial automation and digital health.

Although program structures vary, several success factors consistently emerge.

Strategic alignment is perhaps the most important. Accelerator programs generate greater impact when they support clearly defined corporate priorities rather than broad innovation themes.

Executive support is equally critical. Visible commitment from senior leadership facilitates cross-functional collaboration, accelerates decision-making and increases organizational engagement throughout the innovation process.

Business ownership represents another important factor. Innovation teams typically coordinate this type of program, working closely with business units to jointly determine whether technologies create operational or commercial value. Successful accelerators therefore involve business stakeholders from the earliest stages of startup selection and evaluation.

Long-term engagement also differentiates mature programs from one-time innovation initiatives. Building trust, integrating technologies and developing commercial relationships require sustained collaboration beyond the duration of an accelerator cohort.

Finally, clear measurement frameworks are essential. Organizations increasingly evaluate accelerator performance through indicators such as pilots launched, commercial agreements concluded, customer impact, revenue generation, operational improvements and technology adoption rather than simply counting participating startups.

These characteristics illustrate why corporate accelerators have become strategic instruments supporting business transformation rather than isolated innovation programs.

The telecommunications sector provides particularly strong examples of this evolution. Telecommunications operators increasingly collaborate with startups developing artificial intelligence applications, cybersecurity solutions, industrial Internet of Things platforms, energy optimization technologies, computer vision, drones and advanced digital services. Through accelerator programs, these companies gain access to enterprise customers, communications infrastructure and specialized expertise, while operators accelerate their own innovation cycles and expand service portfolios.

Orange Fab represents this collaborative model. Orange Fab is less a traditional accelerator focused on startup development than a facilitator of structured collaboration between innovative companies and Orange business units. The program emphasizes technology validation, co-innovation and commercial adoption, reflecting the broader shift from startup support towards business value creation.

This evolution also illustrates a broader principle of modern corporate innovation. Startups should not be viewed merely as external suppliers of technology. They are strategic partners capable of contributing specialized expertise, entrepreneurial agility and innovative perspectives that complement corporate capabilities. Corporate accelerators provide the organizational framework through which these complementary strengths can be transformed into measurable outcomes.

Orange Fab Romania illustrates the evolution of corporate accelerators from startup support initiatives towards business-driven collaboration platforms. The program is designed to identify startups whose technologies address concrete business challenges within Orange Romania and the wider Orange Group. Beyond mentoring, participating startups gain access to technical expertise, enterprise customers, testing environments and opportunities to develop commercial partnerships. This approach reflects Orange's commitment to creating sustainable value for both startups and the organization by transforming innovation into tangible business outcomes.

Corporate accelerators are strategic business tools rather than traditional startup support programs.

Their primary objective is to connect entrepreneurial innovation with concrete business needs.

Successful accelerators focus on technology validation, commercial collaboration and measurable business impact.

Close involvement of business units is essential throughout the innovation process.

Long-term partnerships generate greater value than short-term pilot projects alone.

Orange Fab demonstrates how corporate accelerators can contribute simultaneously to startup growth and corporate transformation.



Orange Fab: Accelerating Startup Collaboration

Orange Fab is the cornerstone of Orange Group's startup collaboration strategy. More than a corporate accelerator, it is an Open Innovation platform that connects startups with business units, technical experts and customers to transform innovative technologies into commercially viable solutions. Its success is measured not by the number of startups supported, but by the business value created through long-term partnerships.

Innovation rarely reaches the market through technology alone. Emerging solutions require validation, access to customers, technical integration, industry expertise and commercial opportunities before they can achieve meaningful scale. For startups, these elements are often more difficult to obtain than the technology itself. At the same time, large organizations require efficient mechanisms to identify emerging technologies and evaluate their potential business impact.

Orange Fab was created to address this challenge.

Launched by Orange Group in 2013, Orange Fab has grown into one of the largest corporate accelerator networks in the telecommunications industry, operating across Europe, Africa and the Middle East. Although each national program reflects the priorities of its local market, all Orange Fab initiatives share a common objective: facilitating mutually beneficial partnerships between innovative startups and Orange business units.

This objective distinguishes Orange Fab from many traditional acceleration programs.

The program is not primarily designed to provide seed funding or prepare startups for investment. Instead, it focuses on business acceleration through collaboration. Selected startups gain access to technical expertise, mentoring, commercial opportunities, technology validation and the international Orange ecosystem. In return, Orange gains early access to emerging technologies capable of addressing strategic business challenges and strengthening its portfolio of digital services.

This collaborative philosophy reflects the broader principles of Open Innovation discussed in the previous chapter. Innovation is viewed not as a linear process driven by a single organization but as a collaborative journey involving entrepreneurs, engineers, researchers, business leaders and customers.

The Orange Fab Collaboration Model

The Orange Fab methodology begins with the identification of strategic business priorities.

Rather than launching broad calls for innovation, specific challenges aligned with corporate strategy are defined. These challenges may relate to areas such as artificial intelligence, cybersecurity, digital trust, enterprise services, energy management, industrial digitalization, computer vision, Internet of Things or advanced connectivity.

Based on these priorities, startups are identified through open calls, ecosystem partnerships, universities, technology events, venture capital networks and referrals from Orange's international innovation community.

Following an initial evaluation, selected startups enter a structured collaboration process involving technical assessment, business validation and engagement with relevant Orange experts. The evaluation extends beyond the quality of the technology itself. Consideration is also given to market readiness, scalability, compatibility with Orange's strategic priorities, team capabilities and the potential to create long-term business value.

Once selected, startups collaborate directly with business units rather than operating independently from the organization. Technical experts, product managers, innovation managers, procurement specialists and commercial teams work together to evaluate the solution, identify potential use cases and define appropriate validation activities.

Depending on the maturity of the technology and business opportunity, collaboration may include technical integration, proof-of-concept activities, pilot deployments or commercial projects with Orange customers.

This business-oriented approach significantly increases the likelihood that startup collaboration will lead to sustainable commercial relationships rather than isolated innovation experiments.

Creating value for startups and Orange

The success of Orange Fab depends on creating value for both startups and the organization.

For startups, one of the greatest benefits is access to enterprise customers. Developing an innovative technology is only the first step towards commercial success. Demonstrating that technology under real operating conditions and securing reference customers are often decisive milestones for future growth. Through Orange Fab, startups gain opportunities to validate their solutions within complex operational environments while engaging directly with enterprise customers across multiple industries.

Technical mentoring represents another important advantage. Orange engineers experts provide guidance regarding network integration, cybersecurity, scalability, interoperability and regulatory considerations. This expertise enables startups to refine their solutions and better understand the requirements of enterprise deployment.

Participation in the Orange ecosystem also provides increased visibility. Startups may present their technologies during industry events, innovation conferences, customer demonstrations and international technology exhibitions, expanding opportunities for new partnerships beyond the accelerator program itself.

For Orange, the program provides structured access to emerging technologies that complement internal capabilities Startups frequently develop highly specialized solutions in areas such as artificial intelligence, cybersecurity, computer vision, industrial automation, sustainability, drones or advanced analytics. Collaborating with these companies enables Orange to evaluate new technologies rapidly while reducing the cost and uncertainty associated with internal development.

The program also strengthens organizational learning. Business units gain direct exposure to entrepreneurial approaches, agile development methodologies and emerging market trends. This interaction contributes to a more entrepreneurial culture while encouraging multidisciplinary collaboration across the organization.

Importantly, Orange Fab contributes to business transformation rather than functioning solely as an innovation initiative. Startup collaboration supports the development of new products, improves existing services and creates opportunities to address evolving customer needs through innovative digital solutions.

Orange Fab Romania

Orange Fab Romania was launched in 2017 with the objective of strengthening collaboration between Orange Romania and the national startup ecosystem. Since its establishment, the program has become an important component of the company's Open Innovation strategy, supporting the identification, validation and commercialization of innovative technologies developed by Romanian startups.

The program focuses on building long-term strategic partnerships rather than providing short-term acceleration. Selected startups receive access to business expertise, technical mentoring, Orange's customer network and opportunities to develop pilot projects or commercial collaborations. The program operates without taking equity in participating companies, reflecting its primary objective of creating mutual business value.

Over the years, Orange Fab Romania has collaborated with startups addressing strategic technology domains including artificial intelligence, cybersecurity, digital health, smart cities, energy, industrial digitalization, retail technologies, Internet of Things, computer vision and advanced connectivity. These collaborations have demonstrated how entrepreneurial innovation can contribute to solving real business challenges while supporting the digital transformation of customers across multiple sectors.

An important characteristic of Orange Fab Romania is its integration with the broader Orange innovation ecosystem. Startups may benefit from collaboration not only with Orange Romania but also with international Orange entities, European research projects, Orange Innovation experts, Orange 5G Labs and ecosystem partners. This international dimension expands opportunities for technology validation and future business development.

A venture client approach

Corporate accelerators have traditionally been associated with mentoring, networking and visibility. Increasingly, however, leading organizations are adopting what is often referred to as the venture client model.

In this approach, the corporation becomes one of the startup's first enterprise customers rather than investor or mentor. The objective is to accelerate commercial adoption by validating technologies through real customer use cases and procurement processes.

The program emphasizes business collaboration, pilot implementation and commercial relationships that continue beyond the formal duration of the accelerator. This approach creates stronger incentives for both startups and business units because success is measured through tangible business outcomes rather than program participation alone.

Consequently, **Orange Fab should be understood not simply as a startup accelerator but as a strategic business platform connecting entrepreneurial innovation with Orange's long-term transformation objectives.**

Orange Fab Romania: Mission, Vision and Strategic Positioning

Launched in 2017, Orange Fab Romania is the corporate startup accelerator of Orange Romania and part of the international Orange Fab network operating across Europe, Africa and the Middle East. The program was created to strengthen collaboration between Orange Romania and innovative technology companies capable of addressing real business challenges while contributing to the digital transformation of customers across multiple industries.

Unlike traditional startup accelerators, Orange Fab Romania is not primarily focused on early-stage incubation, equity investment or startup fundraising. Its mission is to facilitate business collaboration between startups and Orange by creating opportunities for technology validation, product development and commercial deployment.

The program does not measure success by the number of startups participating in each cohort, nor by the amount of investment raised by participating companies. Instead, Orange Fab Romania evaluates success through the quality of partnerships established, technologies validated, commercial opportunities created and business value generated for all participants.

This business-oriented philosophy reflects Orange Romania's broader understanding of Open Innovation.

Innovation is viewed not simply as the introduction of new technologies but as a collaborative process that creates value for customers, startups and the organization itself. Consequently, Orange Fab Romania operates at the intersection of entrepreneurship, technology and business development.

Key Takeaways

- Orange Fab is a corporate Open Innovation program designed to create business value through startup collaboration.
- The program focuses on long-term commercial partnerships rather than short-term acceleration.
- Business units play a central role throughout the startup evaluation and collaboration process.
- Startups benefit from access to technical expertise, customers, technology validation and international visibility.
- Orange benefits from earlier access to emerging technologies, organizational learning and accelerated innovation.
- Orange Fab Romania has become a key component of the national innovation ecosystem by connecting Romanian startups with Orange's business capabilities and international network.

Mission

The mission of Orange Fab Romania is to identify innovative technology companies whose solutions address strategic business opportunities and to facilitate their integration into Orange Romania's innovation ecosystem.

The program aims to:

- accelerate the adoption of emerging technologies;
- strengthen Orange Romania's portfolio of digital services;
- create commercial opportunities for innovative startups;
- support customers' digital transformation;
- contribute to the development of Romania's innovation ecosystem.

Orange Fab Romania is not a standalone innovation initiative; it functions as a strategic instrument supporting Orange Romania's long-term business objectives.



Vision

Orange Fab Romania's long-term vision extends beyond startup acceleration.

The program seeks to become a reference platform for corporate-startup collaboration in Romania by demonstrating that Open Innovation can generate measurable business outcomes while strengthening the national innovation ecosystem.

This vision reflects several important principles.

- Innovation should solve concrete business challenges.
- Corporate-startup collaboration should create value for both partners.
- Technology should ultimately improve customer experience and business performance.
- Innovation ecosystems become stronger through long-term collaboration between startups, corporations, universities, investors and public institutions.

By consistently applying these principles, Orange Fab Romania contributes to positioning Orange as an active participant in Romania's digital transformation rather than solely as a telecommunications provider.

Strategic Positioning Within Orange Romania

Orange Fab Romania operates at the intersection of technology, business development and ecosystem engagement.

On one side, the program collaborates closely with Orange Romania's business units to identify strategic priorities, understand customer needs and evaluate emerging technologies.

On the other, it maintains active relationships with startups, universities, research organizations, technology communities, investors and innovation partners across Romania and Europe.

This intermediary role enables Orange Fab Romania to translate business challenges into innovation opportunities while helping startups better understand enterprise customer requirements. The program therefore functions as an innovation broker, connecting complementary capabilities that might otherwise remain isolated.

Orange Fab Romania is fully aligned with the strategic direction established by Orange Group.

The Trust the Future strategy identifies innovation, artificial intelligence, cybersecurity and trusted digital services as strategic priorities for the Group's future development.

Orange Fab Romania contributes directly to these priorities by identifying startups developing technologies that complement Orange's capabilities and support future business growth.

Supporting Romania’s Innovation Ecosystem

Orange Fab Romania also plays an important role beyond the organization itself.

Romania’s startup ecosystem has matured significantly during the past decade. Universities, technology communities, venture capital investors, accelerators, incubators and digital innovation hubs have contributed to creating an increasingly dynamic environment for technology entrepreneurship. Corporate participation represents another essential component of this ecosystem.

By collaborating directly with startups, corporations create opportunities for technology validation, commercial adoption and knowledge exchange that complement public support programs and private investment.

Orange Fab Romania contributes to this collaborative environment by acting as a bridge between entrepreneurs and enterprise customers. The program demonstrates that startup success depends not only on technological excellence but also on access to markets, strategic partnerships and opportunities to validate solutions in real business environments.

Key Takeaways

- Orange Fab Romania is a business collaboration platform rather than a traditional startup accelerator.
- The program focuses on creating measurable value for startups, Orange Romania and enterprise customers.
- Its mission is closely aligned with Orange Group’s Trust the Future strategy.
- Orange Fab Romania acts as a bridge between startups, business units, universities and the wider innovation ecosystem.
- Success is measured through partnerships, technology adoption and commercial impact rather than startup participation alone.
- The program contributes to both Orange Romania’s business transformation and the development of Romania’s innovation ecosystem.

From startup selection to business partnership: the Orange Fab Romania collaboration model

The success of Orange Fab Romania is determined not by selecting the most innovative startups, but by identifying those capable of creating measurable business value through collaboration with Orange Romania and its customers. The program therefore follows a structured collaboration model that aligns startup capabilities with strategic business priorities, ensuring that innovation is driven by market needs rather than technology alone.

Corporate-startup collaboration is fundamentally different from traditional supplier relationships. Emerging technology companies operate with different organizational structures, development cycles and business objectives than large enterprises. While startups are characterized by agility, rapid experimentation and technological specialization, corporations emphasize operational stability, governance, scalability and customer trust.

Successfully connecting these two worlds requires more than identifying promising technologies. It requires a structured process capable of aligning entrepreneurial innovation with corporate strategy while creating value for both parties.

Orange Fab Romania has developed such a collaboration model by integrating startup selection, technical validation, business engagement and commercial development into a coherent innovation process.

Instead of treating startup acceleration as a series of independent activities, the program follows a business-oriented lifecycle that begins with identifying strategic priorities and concludes with long-term commercial collaboration.

Every Orange Fab Romania cohort begins with the business.

Instead of launching generic calls for innovation, the program first engages with Orange Romania’s business units to identify strategic priorities, customer challenges and technology gaps. These priorities reflect both local market needs and the broader strategic direction of Orange Group.

Business challenges may emerge from multiple areas, including enterprise services, cybersecurity, artificial intelligence, smart cities, industrial digitalization, energy management, customer experience, network innovation, digital trust or operational efficiency.

This demand-driven approach ensures that startup collaboration is directly connected to business objectives rather than driven solely by technological curiosity.

It also creates early engagement from business stakeholders, significantly increasing the likelihood that successful collaborations will continue beyond the accelerator program.

Startup scouting and outreach

Once priority areas have been defined, Orange Fab Romania actively identifies startups capable of addressing these challenges.

Startup sourcing combines several complementary approaches.

Open calls allow founders to submit innovative solutions aligned with the program’s focus areas.

Partnerships with universities, accelerators, incubators and technology communities expand access to emerging companies across Romania.

Participation in innovation events, conferences, hackathons and startup competitions enables the program to engage directly with founders developing promising technologies.

The Orange Fab international network also facilitates the exchange of startup recommendations between Orange entities operating in different countries, creating opportunities for cross-border collaboration and technology transfer.

This diversified scouting approach enables Orange Fab Romania to maintain continuous visibility into emerging technologies while ensuring a broad and competitive selection process.

Evaluation and Selection

Following the application phase, startups undergo an evaluation process that assesses:

- the startup’s ability to solve real customer problems, integrate with Orange’s business environment and scale commercially.
- alignment between the startup’s solution and Orange Romania’s business objectives.
- technological maturity, the readiness of the solution for pilot implementation or commercial deployment.
- business viability, the startup’s business model, market traction and growth potential.
- team experience, expertise
- scalability, the potential to deploy the solution beyond a single customer or use case.
- collaboration potential, the startup’s capacity to work within a corporate environment while adapting its solution to enterprise customer requirements.

Once admitted to Orange Fab Romania, startups enter a structured engagement phase designed to refine use cases, validate technologies and identify commercial opportunities.

Early activities typically focus on understanding customer needs, clarifying technical integration requirements and defining measurable objectives for collaboration.

Business mentors help startups better understand enterprise environments, procurement processes and customer expectations.

Technical experts evaluate interoperability, cybersecurity, architecture and scalability.

Rather than following a standardized program for every startup, collaboration is adapted according to the maturity of the company and the complexity of the opportunity being explored. This flexibility reflects the program’s business orientation.

Proof of concept and pilot projects

Where appropriate, collaboration progresses towards proof-of-concept activities or pilot implementations. These projects enable startups and Orange teams to validate technologies under real operating conditions before larger-scale commercial deployment.

Pilot projects provide valuable information regarding:



They also create opportunities for startups to demonstrate their capabilities within complex enterprise environments while giving Orange greater confidence regarding future deployment.

Importantly, pilots are not viewed as isolated innovation experiments. Whenever possible, they are designed as intermediate stages leading towards sustainable commercial collaboration.

Building long-term partnerships

The ultimate objective of Orange Fab Romania is to establish partnerships that continue beyond the formal duration of the accelerator program.

Successful collaborations may evolve in several directions:

- Startups may become technology partners supporting Orange products or services.
- Startup solutions may be introduced to Orange enterprise customers through joint commercial activities.
- Technologies may be integrated into Orange's operational processes.
- Startups may expand collaboration internationally through the broader Orange Group network.

These long-term relationships create value far beyond individual pilot projects.

Startups gain reference customers, commercial credibility and opportunities for international growth.

Orange strengthens its portfolio of innovative digital services while accelerating access to emerging technologies.

Customers benefit from validated solutions addressing concrete business challenges.

Key Takeaways

- Orange Fab Romania follows a demand-driven rather than technology-driven collaboration model.
- Startup selection is based on strategic relevance, technological maturity, business viability and collaboration potential.
- Pilot projects are designed as milestones towards long-term commercial partnerships.
- The structured collaboration model increases the likelihood that innovation generates measurable business outcomes.

These examples illustrate the diversity of technologies accelerated through Orange Fab Romania while highlighting a common objective: transforming innovative ideas into scalable business solutions that address real customer needs.

Orange Fab Romania in numbers

Since its launch in 2017, Orange Fab Romania has become one of the country's leading corporate acceleration programs, demonstrating that long-term collaboration between startups and corporations can generate measurable business value.

These technology domains have evolved continuously to reflect advances in artificial intelligence, cybersecurity, cloud computing, digital trust and sustainable digital transformation while remaining aligned with Orange Group's strategic priorities.

Over the years, several startups have successfully developed collaborations with Orange Romania beyond the acceleration program itself. These partnerships illustrate how Open Innovation can generate tangible business outcomes for both startups and the corporation.

Representative examples include:

790k+ €
invested in the national innovation ecosystem

3.1M €
paid by Orange to acquire products from Orange Fab startups

100+
commercial programs implemented

14
startup products integrated in internal Orange processes

58
startups

4
solutions integrated in new products

Spectroo
Digital Signage platform. Currently, Orange Romania is working together with Spectroo to transform the solution into an Orange commercial product, demonstrating the program's ambition to move beyond pilot projects towards product co-creation and long-term commercialization.

AI Vision
AI-powered video analytics supporting applications in smart cities, public safety and enterprise environments.

Agricloud
Digital agriculture platform supporting precision farming and data-driven agricultural decision-making.

MobileControl
Mobile workforce and field operations management solutions supporting enterprise digital transformation.

uRADMonitor
Environmental monitoring and air quality solutions integrated with IoT connectivity, demonstrating how telecommunications infrastructure can support sustainability and smart city initiatives.

FieldOS
Digital platform for managing field operations, maintenance activities and workforce productivity, supporting the digitalization of enterprise operations.

Research and Innovation Actions at Orange



06

Our Facilities – Orange 5G Lab Network



The Orange 5G Labs function as a distributed hub for discovering and utilizing the capabilities of 5G technology. This ecosystem is designed to unify a diverse group of stakeholders, including industry partners, innovators, and businesses, to test, develop, and showcase new use cases empowered by 5G networks.

The labs serve as an innovative and experimental platform where businesses can validate and refine their products and services using advanced 5G networks. This setup aims to reduce the resources and time usually needed to progress from concept to market deployment. Additionally, the lab provides educational opportunities for stakeholders to understand the technological advances and operational benefits of 5G, helping to demystify the technology and illustrate its practical uses across various sectors. It also fosters a collaborative environment that encourages cross-industry cooperation to drive pragmatic and immediate solutions, also considering the developments coming from the Orange Fab start-up accelerator program.

Orange Romania's 5G Labs, from both Bucharest and Iasi, are the main places that host the infrastructure used in our 5G-related research and business activities. The Bucharest 5G Lab is located inside the CAMPUS Research Center of UNSTPB and currently implements a full 5G SA infrastructure, comprising 5G RAN, Core, Edge Computing and advanced Software Defined Networking (SDN) elements in the associated datacenter.

The Iasi 5G Lab is located inside TUIASI's Faculty of Electronics and Telecommunications and hosts 5G SA RAN components and similar edge-computing capabilities as the Bucharest laboratory. Moreover, the 5G Lab SA coverage is also extended in selected places from the city of Iasi, mainly the Stefan cel Mare boulevard and the Podu Ros intersection.

The 5G Lab ecosystem will be extended with a novel laboratory in Cluj-Napoca that will be launched by the end 2026 within the Technical University AiRi research center for AI.



Smart Networks and Services

The Smart Networks and Services Joint Undertaking (SNS-JU) is the EU's flagship research vehicle for extracting more value from Advanced 5G while shaping the standards for future 6G networks. Strategically, the programme aligns with Horizon Europe's green, digital and resilience orientations, advancing Key Value Indicators (KVIs) alongside technical KPIs to make sustainability operational for networks and services. It is anchored in the ITU's IMT-2030 framework adopted in 2023, with technical performance requirements due in early 2026, and explicitly gears European contributions toward 3GPP's 6G study work starting in Release-20 (2025-2027) and moving into normative work in Release-21. This timeline allows operators to feed requirements, proofs-of-concept and KPI/KVI validations directly into global standards.

Operationally, SNS JU organizes work where it matters most for operators. Stream B advances both evolutionary and disruptive 6G technologies (from wireless/RAN and devices to reliable services and smart security) at mixed TRLs to influence standards and de-risk migration from 5G.

Stream C builds 6G-ready experimental infrastructure with a strong focus on 6G telco cloud and service-provision enablers, reflecting the EU's Connected Collaborative Computing Networks (3CN) vision and Europe's need for cloud sovereignty and open, trusted interfaces.

Stream D turns results into trials and pilots with verticals, using Stream C infrastructures to validate business models and advanced applications—an explicit bridge from research to market impact.

Two pillars carry immediate operator relevance. First, NTN-TN unification goes beyond interworking to reuse common technologies, architectures, protocols and interfaces across terrestrial and non-terrestrial segments, enabling seamless mobility, direct-to-device and high-resilience coverage capabilities attractive for public safety and nationwide continuity; the scope also considers dynamic spectrum in FR3 (7–15 GHz, extendable to 24 GHz) and multi-tenancy slicing across space and terrestrial domains.

Second, photonics and optical networks are positioned as integral to the 6G architecture, including access technologies (evolving GPON to XGS-PON, HS-PON and beyond) and metro/regional and long-haul, improving energy efficiency, reconfigurability and capacity for fronthaul/backhaul and supporting more autonomous, software-defined network fabrics.

For Orange Romania, SNS JU is a practical path to research-added value; it funds and structures our prototypes from lab to field (via Streams C and D), so we can co-create Romanian pilots in manufacturing, energy, transport, healthcare and public sector on 6G-ready telco-cloud platforms. KVIs make energy, carbon and circularity measurable at service level, enabling green SLAs and helping us meet ESG targets. At the same time, the programme's focus on cloud sovereignty, open interfaces and protection of European communication networks supports compliant, multi-vendor telco-cloud stacks in regulated industries.

AMAZING-6G

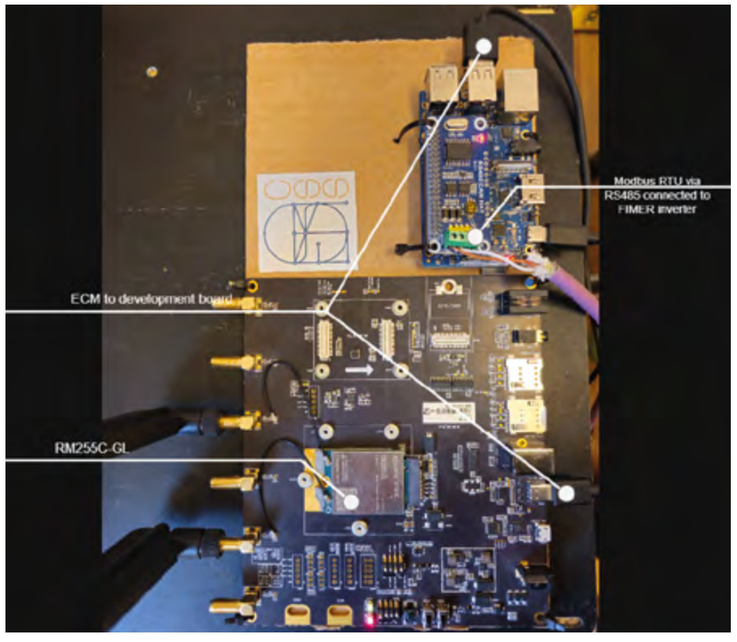
https://amazing6g.eu

AMAZING-6G positions Orange Romania within a pan-European effort to move from isolated 5G pilots to truly large-scale, multi-vertical trials that experiment with the next wave of 5G Advanced/6G capabilities in real operational settings. The project concentrates on four domains, Healthcare, Public Safety, Energy and Transport, and lays out concrete use cases to be executed across national clusters, including Romania, to validate both the technology and the value delivered to society and industry.

In public safety the use cases range from cross-operator PPDR slice orchestration to deployable tactical networks on-the-move; in energy, it spans renewable communities and AI-assisted solar operations; each use case is framed with measurable KPIs and sites where the trials will run.

The project is built around a unified system architecture that treats connectivity and compute as two interconnected domains orchestrated end-to-end. The functional model shows a communication continuum, formed by legacy and new networking layers, and a compute continuum spanning cloud, edge and far-edge resources.

On the communications side, the novelties that need to be demonstrated by the consortium include fast, on-demand private network provisioning, dynamic end-to-end slicing and interworking across multiple operators for PPDR scenarios when existing infrastructure is damaged or congested.



The emergency communications on-the-move scenario will happen in Romania together with the Special Telecommunications Services (STS) and aligns with the project objectives by testing a fully portable tactical network hosted in a utility truck with a local B5G SA core, edge compute and satellite backhaul. Two operating modes are evaluated: one where a satellite link ties the field site directly to Orange Romania's 5G Lab core and one where the site runs locally if backhaul is lost.

In the energy domain, Orange Romania leads the definition and testing of the use cases. Our cluster's flagship scenario, developed together with SIMTEL, focuses on "Solar energy monitoring, control and predictions using 5G/6G communications and edge-cloud." It blends high-density sensor/telemetry ingest, AI-based forecasting and real-time control loops over network slices that match the traffic and reliability profile of each function. The implementation is designed to demonstrate the value of edge placement for inference and decision.

These Romanian trials are centred around Orange Romania's 5G testbed and facilities, which provide the end-to-end system for experimentation: a private 5G core, the commercial 5G RAN coverage and an edge-cloud stack based on Kubernetes and featuring GPU resources for AI workloads.

This project has received funding from the European Union's Horizon Europe Smart Networks and Services Joint Undertaking (SNS JU) under Grant Agreement No. 101192035.

6G-Path

https://6gpath.eu

6G-PATH aggregates various operators, vendors, and research labs to turn early 6G concepts into measurable, multi-vertical pilots that experiment with real networks, devices and business models. The project federates seven advanced testbeds and aligns its roadmap with 3GPP Releases 18–20 so that technical findings and key performance/value indicators (KPIs/KVIs) feed directly into standards-aligned evolution paths towards 6G.

6G-PATH is both a unifying experimentation fabric and a pipeline of large-scale trials across Health, Education, Smart Cities, and Farming verticals.

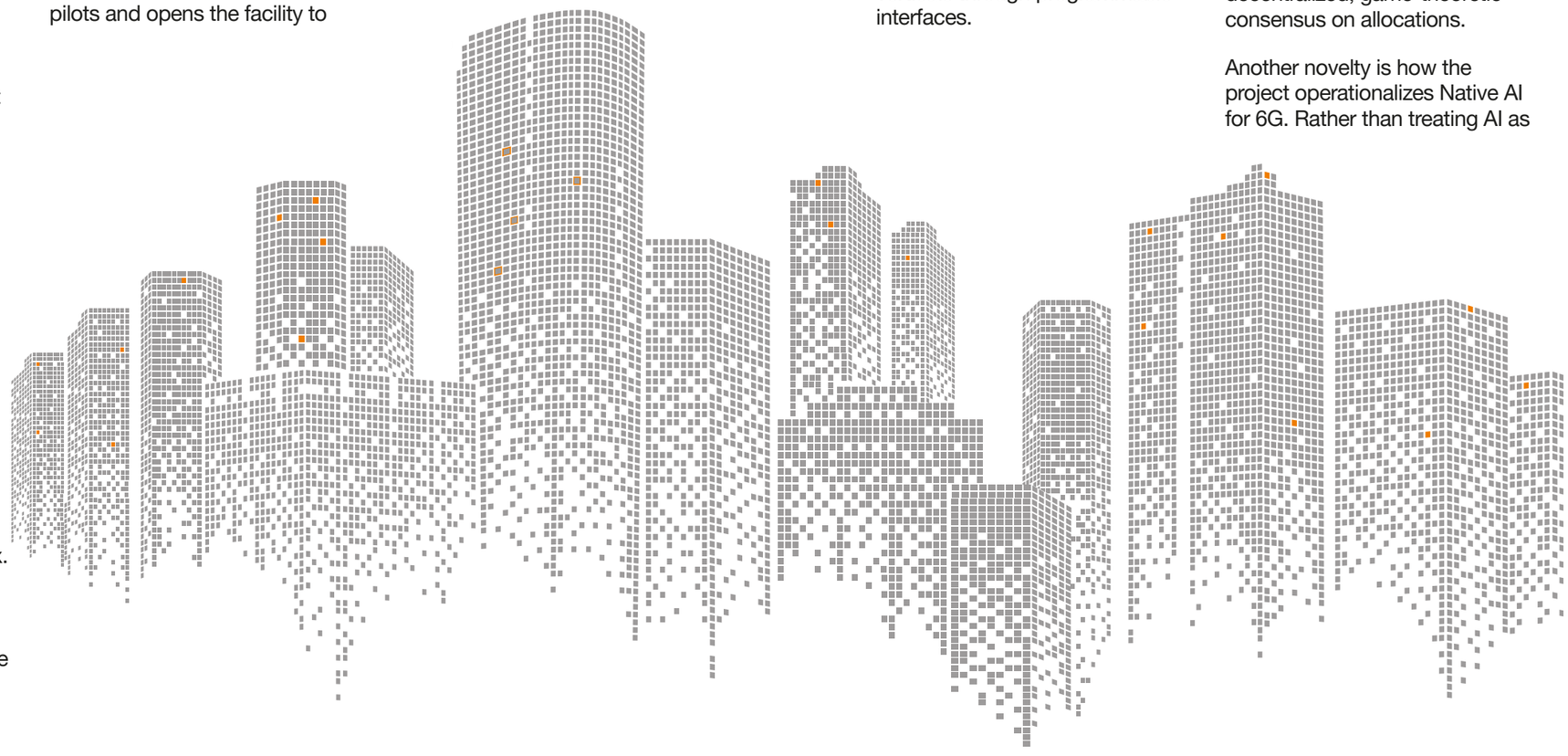
One of the project novelties is a transversal integration and experimentation platform that abstracts heterogeneous testbeds and exposes a coherent developer experience. Rather than treating each facility as separate, 6G-PATH advances common building blocks, including an experiment scheduler, a slice manager for multi-tenant configurations, a policy enforcer to close automated control loops, a network application catalogue and a resource knowledge index. These assets are deliberately extended from prior EU projects and matured to higher TRLs inside 6G-PATH so that use-case owners can plug in applications once and run them anywhere.

Another novelty is the systematic, continuous upgrade of testbed infrastructures toward beyond-5G and 6G capabilities with a focus on performance and programmability. 6G-PATH partners plan stepwise enhancements for URLLC and Time-Sensitive Networking, multi-connectivity protocols that are aware of network state, and ubiquitous coverage by combining terrestrial and non-terrestrial domains.

Within the project, Orange Romania leads the work of preparing and upgrading testbeds for experiments, ensuring that the 6G-PATH platform and third-party extensions are integrated on time to support the project trials. The team also enables XR devices and control-plane functions for device management, content delivery, and KPI monitoring in the Romanian XR rural schools' pilots and opens the facility to third-party experiments selected through the project's open calls.

At the application layer, the Orange Romania Foundation acts as the use-case champion for UC-EDU-1 ("XR rural school"), bringing the Digitaliada platform to co-design immersive lessons, simulations, and personalized learning flows for rural communities. The foundation orchestrates functional tests in Romanian rural schools, turning the lab's XR and edge capabilities into tangible improvements in student experience and teacher tooling.

6G-PATH project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101139172.



FLECON-6G

https://flecon6g.eu

FLECON-6G is working at the blueprint for an intelligent 6G Network of Networks in which multiple administrative and technological domains, including public and non-public networks, terrestrial and non-terrestrial segments, transport, RAN and edge domains can be composed on demand through open, collaborative frameworks.

For Orange Romania, this project is a natural extension of our strategy to industrialize cloud-native, AI-driven 5G/6G capabilities and expose them to verticals through programmable interfaces.

One of the project's technical novelties is the intent-driven Smart Marketplace that generalizes federation beyond today's edge exposure and network APIs. Building on GSMA Operator Platform Group (OPG) interfaces, including east-west federation and the User-Network Interface, and aligning with TM Forum's intent semantics, FLECON-6G extends what/why business intents into automated negotiation and reconciliation workflows among brokers, resource owners and tenants. The Marketplace broadens scope from compute and connectivity (IaaS, NaaS/NIaaS) to include AI models (AIaaS) and Network Digital Twins (DTaaS), making it the first unified brokering layer where MNOs and third parties can expose heterogeneous assets with pricing and coverage availability zones, while algorithms drive decentralized, game-theoretic consensus on allocations.

Another novelty is how the project operationalizes Native AI for 6G. Rather than treating AI as a per-domain add-on, FLECON-6G integrates foundation-model-augmented workflows for intent translation, planning and runtime control, combining LLM-driven planning with task-specific ML across concurrent cognitive closed loops at different timescales.

Within this architecture, FLECON-6G validates capabilities through four PoCs. Of relevance for Orange Romania is PoC 1, Seamless Immersive Reality (SIR), which demonstrates Marketplace-driven multi-stakeholder composition on our Bucharest 5G Lab infrastructure. SIR fuses VR/AR/XR into real-time, multi-participant telepresence using stereoscopic capture up to 16K at 100 fps, with stringent bandwidth (>1–2 Gbps per user enabled by mmWave) and latency requirements that stress both RAN and transport.

Beyond PoC 1, the project also aims to validate RAN NDT-driven ZSM loops for autonomous robot video inspection (PoC 2) and NTN-integrated twins with coordinated closed loops and marketplace exposure (PoC 3), while PoC 4 focuses on trustworthy AI for public safety.

Although hosted on partner facilities, these scenarios contribute directly to Orange Romania's roadmap, hardening the twin-plus-AI control stack and making the benefits transferable to nationwide 5G SA and future 6G deployments, where we will run concurrent loops for assurance, optimization and resilience.

Co-funded by the European Union under Grant Agreement No. 101192462.

https://6g-intense.eu

6G-INTENSE proposes an intent-driven architecture that treats communications, compute and sensing as a single, controllable fabric.

At its core there is DIMO, a Distributed, Intent-driven Management and Orchestration framework, that federates autonomous domains and reconciles intents continuously from business to service to resource layers, aiming for internet-scale automation across multi-stakeholder infrastructures.

This project rethinks MANO by separating service-level decisioning from low-level resource control, delegating part of service lifecycle management to tenants, and exposing a unified resource view through a Network-Compute Fabric that spans cloud, edge and deep-edge nodes with integrated joint communication-and-sensing (JCS) capabilities.

In parallel, a Native-AI toolkit powers intent decomposition, conflict resolution and cross-domain coordination, enabling the zero-touch behaviors 6G aspires to deliver.

Together, these innovations target a single, open controllability framework with the reach and elasticity of hyperscale cloud but grounded in telecom-grade constraints and KPIs.

To validate these novelties, 6G-INTENSE runs a structured PoC program over mature operator-class facilities.

PoC-1, Distributed Continuum towards pervasive computing, validates the abstraction framework across Orange Romania's transport and cloud domains, demonstrating joint optimization of compute and network for content/gaming workloads that are increasingly mobile and location-sensitive. PoC-2 focuses on metaverse experiences and CDN-like chains, where ultra-tight coupling of RAN, transport and edge compute determines user QoE.

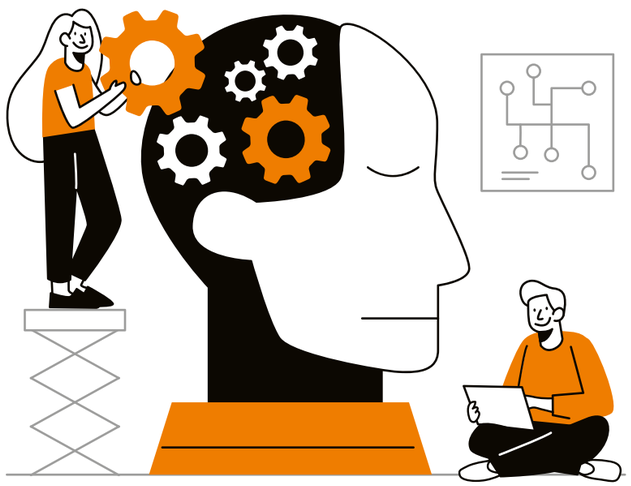
In PoC-1, Orange Romania's testbed environment is one of the three southbound platforms under test, validating the fabric's ability to stitch micro-services across transport, radio and compute while consuming intent from DIMO.

In PoC-2, Orange Romania co-leads the latency- and bandwidth-sensitive metaverse chain experiments with EURECOM, validating whether Native-AI-guided placement and closed-loop QoS policies can maintain experience quality under churn, conflicts and multi-tenant contention—exactly the conditions future 6G services will face.

From a commercialization angle, the project's path-to-market explicitly recognizes Orange Romania's role in "Intelligent Network-Compute integration": AI-based CDN/edge integration for efficient service deployment in data centers and at the edge will be evaluated, folded into product assessments locally, and positioned for Group-level exploitation.

Taken together, 6G-INTENSE's technical novelties map directly to Orange Romania's strategy for 5G-to-6G evolution: expose controllable, programmable networks to verticals and developers; place compute where RAN and users demand it and automate everything with safe, explainable AI.

6G-INTENSE project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101139266



https://6gmusical.eu

https://isee6g.eu

As mentioned in a previous section, Orange Romania is advancing Europe's 6G ISAC development activities through two complementary SNS JU projects, 6G-MUSICAL and iSEE-6G, that push joint communication–sensing from concept to operator-grade validation.

6G-MUSICAL introduces a multi-band ISAC vision that merges radio sensing, high-rate communications and cm-level localization into the edge network. Its technical novelties start at the physical layer with joint waveforms that can serve both traffic and radar-like sensing, compressed sensing for positioning, and cooperative multimode algorithms that exploit multistatic measurements from many radio nodes.

Uniquely, the project prioritizes network synchronization using precise timing and frequency references that are generated and distributed using microwave photonics. In this approach, edge nodes are kept phase-coherent, targeting inter-node timing deviations below tens of picoseconds so that sensing tasks can reach sub-centimeter resolution.

Within 6G-MUSICAL, Orange Romania leads the project's requirements, architecture and use case work, steering the platform architecture and KPI/KVI definitions with an operator's perspective on coexistence, spectrum use, fronthaul limits, and deployability. Beyond the technical enablers, the PoCs targeted by the project evaluate the photonics-based timing solution and assess the E2E system in a realistic testbed, the Orange 5G Lab, to test communication, localization and tracking of terminal devices, vehicles or drones. These trials are structured with replication in mind, including plans for open datasets to promote reproducibility of ISAC algorithms.

The iSEE-6G project complements this with a broader vision that combines ISAC with power transfer capable antennas and edge computing (JCCSP). Its physical-layer novelties include specialized waveforms and frame structures, channel modeling for UAV-assisted links and 360-degree beamforming antennas.

At the hardware layer, the project develops intelligent reconfigurable surfaces (RIS) and agile arrays tailored to JCCSP. At the system layer, it targets a service-oriented, cell-free architecture with MEC support for cooperative localization, mapping, and data caching.

Orange Romania's contributions to iSEE-6G are similar to the ones in 6G-MUSICAL, defining initial requirements, contributing to the ISAC architecture and validating the UAV-centric use cases, ensuring the scenarios reflect commercial network realities.

The drone sensing use case is where the two projects meet. In iSEE-6G, aerial corridors are formalized as regulated UAV lanes in rural/urban settings, with non-critical and critical operations (PPDR communications, cooperative sensing and mapping) sharing the same technical architecture.

For 6G-MUSICAL, one of the project's PoCs foresees tracking and localization of mobile users, vehicles or drones using new phased-array antenna integrated to a pre-commercial RAN system, demonstrating how joint waveforms and AI/ML processing behave under real scheduler and fronthaul conditions.

6G-MUSICAL project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101139176.

iSEE-6G project has received funding from the European Union's Horizon-JU-SNS-2023 Research and Innovation Program under Grant Agreement No. 101139291.

TrialsNet

https://trialsnet.eu

The TrialsNet project is a large-scale European initiative designed to advance the understanding and deployment of beyond 5G technologies through real-world experimentation. Its vision was to trial innovative applications such as cobots, metaverse, and massive twinning across three major domains of urban ecosystems: Infrastructure, Transportation, Security and Safety (ITSS); eHealth; and culture, tourism and entertainment. The project was implemented in four geographical clusters—Italy, Spain, Greece, and Romania—and covered thirteen representative use cases. By involving real users in realistic conditions, TrialsNet explored how current 5G infrastructures perform under the demanding requirements of new applications, while also identifying technological and societal gaps that point towards 6G requirements. A central goal was to assess where today's networks are insufficient, to experiment with advanced features such as dynamic slicing, NFV, MEC, AI/ML orchestration, and O-RAN integration, and to extract both quantitative KPIs and qualitative KVIs that would frame early adoption of 6G solutions. In parallel, the project emphasized sustainability, providing insights not only for network evolution but also for the societal acceptance of advanced technologies.

Orange Romania played a central role in the Romanian cluster, leveraging its 5G Labs in Bucharest and Iași to provide the infrastructure for implementing and validating use cases. The Bucharest 5G Lab, offered a full 5G SA environment with RAN, Core, and Edge Computing capabilities, while the Iași 5G Lab, hosted by Technical University Gheorghe Asachi Iasi, progressively evolved into a site with local UPF, edge servers, and SA RAN deployment. Together, the two facilities formed a federated testbed interconnected via the IPFABRIC concept, enabling dynamic placement of applications. This infrastructure proved essential in implementing the Romanian use cases and in onboarding external applications through the Open Call mechanism.

Orange Romania coordinated the deployment and trialing of Use Case 1, Smart Crowd Monitoring, and Use Case 4, Smart Traffic Management, in Iași. UC1 focused on enhancing situational awareness for public authorities during large gatherings. High-resolution cameras were installed and connected via 5G to edge servers, enabling real-time video analytics for people counting, density estimation, and detection of anomalies such as unauthorized vehicle access. Strong privacy measures, such as anonymization and non-storage of personal data, were integral to the design. Trials conducted between 2023 and 2025 demonstrated the system's robustness: during peak events Wi-Fi and 5G-based analytics confirmed large spikes in crowd presence while still maintaining QoS. The transition from NSA to SA with local edge integration achieved end-to-end latencies below 10 ms, validating the platform's ability to scale to multi-camera, real-time analytics.

UC4 addressed road safety and congestion, leveraging a similar architecture adapted to traffic monitoring. Deployed at one of Iași's busiest intersections, the system integrated six cameras connected to the 5G network, running advanced. Particular emphasis was placed on identifying hazardous interactions involving vulnerable road users. Trials executed in late 2024 and mid-2025 confirmed the system's capability to support predictive traffic management and safety improvements. Results showed the importance of reliable uplink throughput and ultra-low latency, challenges that were successfully addressed after the upgrade to 5G SA with local edge and URLLC slicing.

Beyond the use cases, Orange Romania also supported Open Call projects by offering access to its 5G Labs, assisting with infrastructure setup, and evaluating feasibility and sustainability KVIs. Orange Romania contributed to KPI and KVI definition and monitoring, ensuring that both technical and socio-technical performance were captured. The trials demonstrated not only technical feasibility but also societal readiness for such solutions.

Orange Romania's contribution extended beyond implementation, with a role in work package management, reporting, dissemination, and engagement with local stakeholders. The project outcomes were showcased at major events. Local demonstrations to Iași Municipality and Romanian universities ensured alignment with public authorities and academic partners. By the completion of the trial activities, Orange Romania had validated both UC1 and UC4 under real conditions, supported external innovators through the Open Call, and provided critical input to the broader TrialsNet objectives.

The TrialsNet project has received funding from the European Union's Horizon-JU-SNS-2022 Research and Innovation Programme under Grant Agreement No. 101095871.

6Green

https://www.6green.eu

The 6Green project (Green Technologies for 5/6G Service-Based Architectures) pushes Orange Romania's innovation agenda into the sustainability era by redesigning how networks, compute and applications coordinate around energy and carbon objectives. The proposal is bold and measurable, enabling 5G networks and vertical applications to cut their carbon footprint by at least a factor of ten versus business-as-usual, not only by improving individual components, but by aligning all stakeholders through a Decarbonization Service Agreement (DSA) and cross-domain orchestration of workloads and infrastructure. This shift extends the 5G Service-Based Architecture (SBA) into a greener telco system that ties together communications, distributed computing and storage, and makes energy a first-class design variable across the value chain.

Technically, 6Green introduces three technical novelties. First is Edge Agility: instead of over-provisioning "everywhere, all the time," network functions (NFs) and vertical application microservices move fluidly across the edge-cloud continuum only when, where and for as long as they're needed—driven by mobility patterns, local demand surges and renewable energy availability. This is realized by evolving cloud-native service meshes with sidecar capabilities for stateful session migration, graceful traffic steering and scale-to-zero, so idle capacities can truly power down without sacrificing user experience. A cloud-native NFV Orchestrator then coordinates lifecycle operations across software and hybrid/physical NFs, making these relocations seamless at run time.

Second is Green Elasticity: heavy workloads are proactively shifted from general-purpose CPUs to offloading engines and accelerators when this lowers net energy use, further increasing the share of hardware that can safely enter standby.

Third is Energy-aware Backpressure and Green AI. Here, energy and carbon KPIs are observed at the physical layer and propagated up through the SBA, exposing their impact to tenants and verticals via specific network APIs. Decision engines, aligned with ETSI ENI, act as distributed AI swarms that weigh multi-objective policies (performance, power/CO_2 caps, renewable availability, mobility) and trigger zero-touch reconfigurations across 5G control/management planes and the hosted applications. Importantly, 6Green also controls the energy cost of AI itself, adapting learning and actuation cadence so that intelligence never consumes more energy than it saves.

This closed loop is instrumented with modern telemetry and designed to make every stakeholder aware of their direct and induced footprint—creating the accountability foundation for DSAs.

The project's demonstration plan is split in three phases—testbed setup, integration of vertical applications, and performance evaluation—concluding in a consolidated demonstrator. Validation targets three future-proof use cases with diverse, dynamic requirements that fully exercise Edge Agility and Green Elasticity: (UC1) Critical Operation Maintenance during Energy-Constraint Disaster Scenarios; (UC2) Energy-Efficient Augmented Reality (AR) Remote Assistance; and (UC3) Zero-Carbon Clientless Virtual Enterprise Desktop-as-a-Service.

Orange's primary technical role is to advance the observability and monitoring of the edge-cloud continuum in relation to a given network slice, by developing a novel network element, the Network Slicing Data Analytics Function (NSDFAF), enabling the analytics and decision loops that power Edge Agility and Green Elasticity. This includes supplying operational scenarios and datasets, and contributing to the project's impact analysis, critical for calibrating policies that balance performance with energy and carbon goals in commercial networks.

Beyond cost savings from energy, this opens new green business models and value chains while aligning with EU Green Deal objectives and emerging regulation around digital sustainability. In KVI terms, the project centers on sustainability, responsibility, business value and energy consumption.

6Green allows Orange Romania to deliver a new class of 5G services where performance, availability and decarbonization are orchestrated together. The combination of Edge Agility, Green Elasticity, and Energy-aware Backpressure, validated across three demanding use cases and tracked against explicit KPIs, creates a practical pathway from lab innovation to field deployment. With its 5G Labs, nationwide 5G footprint and data-centre resources, Orange is positioned to help shape, pilot and scale these capabilities so that customers can modernize their operations and meet sustainability targets without compromise.

The 6Green project has received funding from the European Union's Horizon-JU-SNS-2022 Research and Innovation Programme under Grant Agreement No. 101096925.

https://adroit6g.eu

The ADROIT-6G project (Distributed Artificial Intelligence-driven open and programmable architecture for 6G networks) is one of our research initiatives funded under the European Smart Networks and Services Joint Undertaking (SNS JU). Its central vision is to design, validate, and demonstrate novel architectural concepts that address future 6G networks' requirements. The project focuses on embedding distributed intelligence deeply into the network fabric, leveraging open programmability, cloud-native disaggregation, and edge-to-cloud orchestration. Through this, ADROIT-6G aims to enable extreme service classes and applications, ranging from immersive Extended Reality (XR) to mission-critical robotics and massive industrial IoT.

From a technical perspective, ADROIT-6G introduces several novelties. First, it proposes a layered AI-driven architecture, where intelligence is distributed across edge, far-edge, and core domains, ensuring context-aware, low-latency decision-making. Second, the project embraces open and programmable interfaces, ensuring vendor-agnostic innovation and future-proof evolvability. Third, it pioneers extreme service validation, with three Proofs-of-Concept (PoCs) designed to cover all extreme service classes: (i) Extreme eMBB for immersive XR applications, validating Tbps-level throughput for multi-sensory VR/AR and holographic conferencing; (ii) Extreme URLLC for collaborative robotics, where ultra-low latency and reliability are tested in industrial automation and robotic collaboration; and (iii) Extreme mMTC for IIoT, validating massive device density, energy efficiency, and NTN/terrestrial interworking for critical infrastructures.

Each PoC will be validated across at least two different European testbeds, demonstrating replicability and portability. Since commercial 6G radio hardware is not yet available, RAN emulators and device simulators will be leveraged, enabling large-scale validation of thousands to millions of concurrent device sessions. This approach guarantees that ADROIT-6G results will be technology-ready for exploitation within 4-5 years after the project's finalization.

Within this ambitious framework, Orange Romania plays a central role, both as an operator and as an innovation leader. We bring to the consortium our Bucharest 5G Lab testbed, which is a fully operational 5G SA infrastructure already configured for advanced experimentation.

A key innovation of our testbed is the Next-Generation SDN Data Centre integrated with IP Fabric concepts, which allows fully orchestrated, dynamic, and zero-touch network slice configuration and service deployment. This aligns perfectly with ADROIT-6G's vision of distributed programmability and autonomous orchestration.

Moreover, we've developed a novel data collection and monitoring framework that aggregates multi-source information across heterogeneous technologies, enabling advanced analytics and AI-driven insights for both operational optimization and new service enablement.

Through its participation, Orange Romania contributes not only advanced infrastructure but also valuable operator-level expertise in service integration, techno-economic assessment, and regulatory alignment. Specifically, Orange supports use case validation by leveraging its 5G Lab to host Proofs-of-Concept for industrial robotics and IoT, ensuring replicability in a realistic operator environment. Moreover, Orange Romania is committed to dissemination and exploitation, sharing project results across the Orange Group, with Romanian technical universities through the Orange Educational Program and Innovation Labs, and with the wider national digital innovation ecosystem via Orange Fab and Digital Hubs. Finally, the company explores future business models by using ADROIT-6G outputs to shape new service strategies, particularly around immersive XR services, mission-critical industrial automation, and energy-efficient IoT for smart cities and critical infrastructures.

ADROIT6G project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101095363.

https://agentic6g.eu

Agentic6G aims to develop a multi-agent Agentic-AI framework tailored for 6G networks, simplifying the operation of both 6G networks and multi-agent systems, reducing operational expenditure, and enabling new forms of autonomous service composition and management.

Operating over B5G/6G networks, the Agentic6G multi-agent system will further develop the interplay between network and compute across the Device-Edge-Cloud continuum, building on new 6G architectural advances such as the AI-native paradigm and extreme communication capabilities beyond 5G. For service composition, Agentic6G will allow its multi-agent system (MAS) to autonomously compose, coordinate, and optimise B5G/6G and vertical business microservices across edge-cloud infrastructures, advancing the B5G cloud-native approach to autonomous service composition, deployment, and management. This is achieved by treating collective agentic AI knowledge as an integral element of the system, with fast, efficient, and autonomous access to that knowledge supported by LLMs, shared memory, and other agentic tools. Agentic6G will enable efficient end-to-end Agentic Operations to support lifecycle management of the MAS in service of this vision. To meet demanding real-world operational environments, Agentic6G will provide self-organising capabilities focused on spontaneous agent generation, self-protection, self-healing, and auto-scaling of multi-agent systems. This is achieved through hybrid orchestration, combining agent-embedded orchestration for decentralised scenarios with advanced self-organising tools available to the agents themselves. In doing so, Agentic6G aims to remove barriers to adopting and deploying multi-agent agentic AI systems in B5G and 6G networks, addressing well-known challenges such as security risks and gaps in availability, robustness, resilience, and scalability. The main outcomes will be a set of Agentic6G agents serving as autonomy enablers, and an integrated Agentic6G MAS, tested, validated, and demonstrated through representative proofs-of-concept and two critical use cases: one focused on AI for 6G networks, the other on a complex swarm-intelligent robotics application.

Co-funded by the European Union under Grant Agreement No. 101290342.

https://sovereign6g.eu

SOVEREIGN-6G is an initiative that expands the telecom operator role from connectivity provision toward the delivery of integrated digital services spanning network, compute, AI, sensing and security.

The project develops the future 6G environment as a federated telco cloud continuum rather than only a radio evolution.

In this approach, distributed operator platforms, edge and cloud resources, AI capabilities and service exposure mechanisms are brought together into a common European experimentation environment.

The architecture is centred on a Unified Service Platform acting as a single-entry point for customers and developers, a Digital Service Orchestrator for cross-domain lifecycle management, and a native AI edge layer for distributed inference and advanced service logic.

The Unified Service Platform (USP), which is designed as a digital service aggregator and marketplace for the telco cloud, provides a unified, intent-based interface and translates customer requirements into service orders and API calls handled by the underlying domains. The proposal links this platform with GSMA Operator Platform concepts, OpenOP ETSI SDG foundations and CAMARA-aligned API exposure, while also using GenAI to simplify self-service operations and product composition.

In parallel, the Digital Service Orchestrator enables distributed orchestration across cloud, edge, IoT, NT and OT resources, so composite services can be deployed and assured over heterogeneous environments with SLA control.

Orange Romania makes an important contribution to this architecture through both infrastructure and technical enablers, exposing part of its Sylva nodes for further developments in the project.

These nodes are part of the Orange Cloud Native Infrastructure in Romania, offering integrated lifecycle management for VM- and container-based workloads, built on OTC-IaaS and OTC-CaaS and aligned with the Sylva upstream community and Anuket R2 requirements.

In parallel, the Orange 5G Lab is included as a complementary experimentation environment within the project context.

This ecosystem gives us both a production-oriented cloud-native platform and a flexible 5G test environment for validating advanced telco-cloud and 6G functions. Beyond infrastructure exposure, Orange Romania is also part of the core technical effort around telco cloud platform integration, orchestration and assurance.

Orange Romania's main contribution is centered around intelligent assurance of Sylva-based telco workloads.

In this approach, we contribute to the evolution of production-grade Sylva clusters into more resilient and automated telco cloud platforms, supporting predictive root-cause analysis (RCA), remediation and assurance across containerized network functions and infrastructure layers.

This is a relevant innovation area for an operator, because it addresses one of the major operational challenges of future open telco clouds, detecting degradation early, correlating events across infrastructure and service domains and restoring service quality with minimal human intervention.

Through its Sylva nodes and Orange 5G Lab resources, Orange Romania is therefore positioned to validate how cloud-native network functions, orchestration logic and assurance tools can work together in realistic operator conditions.

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101292787.

Civil Security for Societies

https://secassured.eu

Security Assurance-driven AI-based Security Services for Trustworthy Security Engineering from Left-to-Right

The SECASSURED project aims to develop an advanced AI-driven framework for assurance-driven security and compliance engineering, focusing on the entire supply chain of IoT-edge-cloud environments. It integrates cutting-edge AI technologies, including large language models (LLMs), AI agents, and human-centered AI, to deliver innovative security services and tools. SECASSURED covers a broad spectrum of stakeholders, from infrastructure operators to AI solution providers, and emphasizes continuous security and privacy improvement through SecDevOps and MLOps practices.

The overall goal of SECASSURED is to establish a holistic, assurance-driven digital twins-based framework that enhances security across software, hardware, and supply chains. It focuses on identifying cybersecurity and regulatory risks while integrating third-party components, including commercial and open-source software. The project also aims to provide scalable virtual environments for automated security assessment of diverse system components, including AI modules, and to support continuous assurance-driven security engineering throughout the system lifecycle. This initiative aligns with the European Commission's evolving security and privacy regulations and promotes human-centered, trustworthy AI.

SECASSURED is structured around six main objectives and three innovation pillars as mentioned below.

The first objective (O1) is to define holistic security engineering concepts, requirements, and architecture aligned with EU regulations, based on analyses of five pilot use cases.

The second objective (O2) involves developing a Compliance & Security Assurance Model (CSAM) that offers a unified methodology for designing and assuring hardware/software systems compliant with regulations and standards.

The third objective (O3) focuses on advancing security engineering for trustworthy, certifiable systems through components like the SecDevTwin digital twin, AI-based Non-Compliance Detector, advanced AI/ML models for vulnerability detection and repair, and an assurance-driven simulator for proactive security analysis.

The fourth objective (O4) aims to enhance security automation, response, and predictive assurance during operational phases via tools such as the SecOpsTwin digital twin, attack and incident simulators, and GenAI-based security services.

The fifth objective (O5) is to validate the proposed models and tools through demonstrations in diverse IoT environments.

Finally, the sixth objective (O6) targets the development of guidelines, training, and standardization efforts to promote security assurance practices across industries.

A key use case illustrating SECASSURED's application is in the Telecom Software Development Life Cycle (SDLC) that involves collaboration between ORANGE ROMANIA and AROBS (developer of Smart Tracking platform). As ORANGE ROMANIA transitions to a Telco-Tech Services Provider with large-scale 5G Stand-Alone deployments and IoT-edge-cloud integration, it faces complex supply chain challenges involving multiple vendors and stakeholders with stringent security and compliance requirements. The Smart Tracking platform, developed by AROBS and integrated with ORANGE ROMANIA's Telco services, exemplifies this complexity. SECASSURED's solution integrates the SecDevTwin and SecOpsTwin with AI-based security services into Orange Telco Cloud infrastructure, providing a Security Assurance-aware Digital Twin as a Service. This integration aims to automate vulnerability discovery and repair, detect non-compliance in coding practices, simulate complex threat scenarios, and orchestrate automated responses throughout the SDLC.

Two scenarios highlight the use case: one simulates man-made attacks in the SDLC to detect and mitigate malicious code submissions and the other addresses unauthorized access and data leaks by rogue operators in the supply chain. SECASSURED's tools will support operators in identifying threats and coordinating mitigation, enhancing risk-based decision-making and situational awareness in ORANGE ROMANIA's DevOps environments.

Orange Romania participation in SECASSURED project ensures the following benefits:

- Enable the work with local and European SMEs to develop, test and operate new services within complex supply chains
- Focus on resilient systems and improved testing in secure environments addresses stringent security and compliance requirements
- Smart Tracking platform from Telecom use-case integrates ORANGE ROMANIA's Telco services (M2M Control, Live Objects, IoT Automation), enhancing value for B2B customers
- The platform serves large enterprises, SMEs, public sector entities and critical infrastructure operators, expanding ORANGE ROMANIA's market reach.

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101225858.

RECITALS

https://recitals-project.eu/

RECITALS develops privacy-preserving technologies for secure, legal data exploitation, including cryptographic anonymous credentials, homomorphic encryption, secure multiparty computation, and differential privacy. These techniques aim to reduce data leakage, prevent misuse, and protect against privacy vulnerabilities in personal and industrial data assets, while keeping that data securely accessible to authorised users. The project also integrates Identity and Access Management, User and Entity Behavior Analytics, and Incident Response with threat intelligence, to strengthen the security of digital services and help identify confidentiality breaches. RECITALS also gives weight to trusted digital identities, in line with eID and the upcoming eIDAS regulation, and is developing self-sovereign identity solutions that give users control over their own personal data. User-controlled digital identities are treated as foundational to trust in digital services. Usability, scalability, and reliability are core design constraints, particularly for integration with existing infrastructure and security measures across supply chains, and the project accounts for the different data categories and models found across its three target sectors: energy, telecommunications, and healthcare. Proposed solutions will undergo validation and pilot testing in real-world, federated data infrastructures.

Orange is piloting an Identity and Access Management use case for Beyond-5G network management, in which RECITALS aims to deliver an enhanced digital identity solution based on privacy-preserving identity and access management, supporting the dynamic lifecycle of a DevOps/DevSecOps environment. This enables a secure operational environment with clearly assigned roles and access privileges and supports mitigation against insider threats from privileged users with access to core infrastructure. Threat intelligence from RECITALS will also be ingested and consumed through the DevSecOps process in ORANGE ROMANIA SOC, enabling actionable responses to emerging threats against telecommunications infrastructure.

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No.101168490.

CASTOR

https://castorhorizon.eu

CASTOR is a pioneering research initiative focused on ensuring secure, trusted, and optimized communication across the compute continuum. By innovating new technologies and methodologies, CASTOR aims to deliver breakthrough solutions that will empower businesses and users in a wide range of industries to benefit from trustworthy, end-to-end information sharing across distributed infrastructures.

CASTOR is pioneering a high-TRL solution to the complex challenges of trusted-path routing, within the compute continuum by leveraging key innovations such as Adaptive Trust Quantification – a mechanism for dynamic trust assessment of hardware and software devices, and Trust and Resources Optimization and Path Enforcement, supporting enhanced path establishment across diverse hardware and software infrastructures.

To validate the effectiveness of these innovations, CASTOR will deploy prototype implementations across distinct application domains (connected cars, automated mobility, drones in Flying Ad-Hoc Networks, and airspace applications) and will utilize simulation methods to complement these real-world tests, showcasing the system's versatility and robustness in varying operational contexts.

Orange is at the centre of the validation and prototyping activities in CASTOR, by providing a beyond-state-of-the-art, multi-operator, multi-domain, device-edge-ran-core-cloud continuum facility, tuned to support validation of the CASTOR platform in industrial-relevant use-cases such as Highly Available & Secure Airspace Monitoring in Urban Air Mobility Environments, Trustworthy Communications of First Responder Mobile Units & the Compute Continuum and Priority-based Trusted Messaging & Scalable Performance for CCAM Applications.

Funded by EU's Horizon Europe programme under Grant Agreement No. 101167904.



Digital, Industry and Space

https://euro-3c.eu

EURO-3C is a major European initiative for building the first large-scale, federated and sovereign Pan-European Telco-Edge-Cloud pilot infrastructure for what the European Commission calls Connected Collaborative Computing (3C) Networks. The project treats future digital infrastructure not as isolated telecom or cloud domains, but as a converged multi-vendor, multi-domain environment where telco networks, edge nodes, cloud resources and AI capabilities are exposed and consumed as a unified service fabric. The project is ambitious in scale, targeting more than 70 production-grade edge nodes across more than 13 countries and 15 providers, and validating the resulting platform through nine business-relevant use cases in automotive, transport, energy and public protection and disaster relief verticals.

EURO-3C is structured around six research and innovation domains: telco-cloud convergence, multi-level federation, interoperable XaaS services, AI-enabled orchestration, security by design based on Zero Trust, and business sustainability. In this approach, the project aims to remove the traditional separation between telecom and cloud offers by combining secure connectivity, programmable network exposure and cloud compute into portable customer-facing XaaS services, using open and standardized interfaces such as CAMARA, GSMA Operator Platform concepts, Sylva, Nephio and other open frameworks.

Orange Romania has an important role in this architecture through both infrastructure and technical participation. Orange Group, together with selected affiliates, contribute twelve nodes across France, Poland and Romania, of which eight are in Romania: four in Bucharest and one each in Cluj-Napoca, Brașov, Iași and Tulcea.

Beyond infrastructure, Orange Romania is also part of the technical work where the project's core capabilities are defined and validated. We're participating in the strategic design of telco-cloud convergence and AI enablers, in data interoperability and Telco-Cloud exposure activities and in the vertical validation work, while Orange Services Romania is involved in the service orchestration subsystem.

Moreover, Orange Romania is directly involved in both the Energy and PPDR verticals. This is particularly relevant for us because it places the company not only as a node provider, but also as a contributor to the architecture, orchestration and end-to-end validation logic that will shape how federated telco-edge-cloud services are delivered in practice.

In the Energy vertical, Orange Romania and Ogre AI, part of the Orange Fab start-up accelerator, contribute to a use case centered around edge-enabled digital twins for energy orchestration and prediction, where distributed AI/ML is deployed on 3CN edge nodes to support congestion management and flexibility services for distributed energy resources. One of the pilot scenarios explicitly targets monitoring and optimizing our own data centre and radio-site energy usage by combining grid supply, batteries, solar production and smart pricing forecasts.

In the PPDR vertical, Orange Romania contributes to the support of the future European Critical Communication System (ECCS), which aims to enable real-time and secure cross-border operational mobility for public-safety authorities using mission-critical broadband services across Europe.

For us, these two areas are especially valuable in an innovation report because they connect our assets with commercially and societally relevant domains: energy-efficient operation of telecom infrastructure and sovereign mission-critical communications for public safety.

EURO-3C project has received funding from the Call HORIZON.2.4 – Digital, Industry and Space under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101297599.

https://heat-xr.eu

Hybrid Extended reAliTy (HEAT) aims to enable a new generation of distributed immersive experiences that were previously only imaginable: being realistically immersed (holo-ported) within real, captured, omnidirectional and navigable 3D spaces, feeling their atmosphere, and sharing these experiences with others regardless of location. The project integrates immersive media technologies such as point-cloud/holographic imaging, multi-sensory media, and Social VR into a multi-user, feedback-enabled communication system, supporting context-aware, embodied experiences for hybrid XR applications. Remote users experience a captured real environment through immersive VR, while in-person users can see and interact with holograms of those remote users rendered into the real environment.

The system uses agile, multi-sensory 3D data acquisition techniques to improve performance while reducing technology costs, and builds a scalable communication pipeline that can encapsulate different media types — from classical audio-video to multisensory and holographic video, individually or combined — with efficient and scalable encoding, processing, storage, streaming, and rendering. This lets users work with whichever acquisition or rendering system they have available.

The project provides well-designed and fully tested scenarios in real-world environments for enhanced XR experiences: blended learning, a modern theatre performance, a music festival, and an opera.

Funded by EU's Horizon Europe programme under Grant Agreement No. 101135637.



The Digital Europe Programme

https://ctis4nis.eu

The CTIS4NIS project, funded under the Digital Europe Program, aims to establish a robust EU ecosystem involving innovative SMEs, telecom and cloud infrastructure operators, and regulatory bodies to support the implementation of the EU NIS2 and Cyber Resilience Act (CRA) legislations. Its primary focus is on enhancing cybersecurity for telecom critical infrastructures by developing and deploying technologies, tools, and processes that enable effective monitoring and handling of cybersecurity incidents in a cross-border context. Additionally, CTIS4NIS assists vendors in securing telecom equipment and digital products throughout their lifecycle, ensuring compliance with CRA requirements.

A core objective of CTIS4NIS is to implement, validate, pilot, and deploy IT-based solutions for cross-border cybersecurity incident management. This involves creating a cyberthreat intelligence (CTI) sharing platform that facilitates collaboration among private and public cybersecurity stakeholders across Member States. The platform will enable coordinated multi-party vulnerability disclosure, aggregate vulnerability data from multiple sources, and provide advanced analytics and visualization tools to support timely incident response. The project also plans to execute cross-border twinning schemes, piloting these solutions in Greece and Romania to test critical security controls required by CRA and NIS2.

The platform will incorporate built-in data analysis functionalities and adopt an open-source approach to enhance security, reduce costs, and allow for continuous monitoring and improvement. Furthermore, it will support sharing best practices, training, and collaborative development of cybersecurity response plans.

CTIS4NIS will enhance existing tools like MIPS and OpenCTI with advanced analytics, visualization, and incident management capabilities. It will implement ETSI EN 319 401 standards to align with NIS2 reporting requirements and develop a common vulnerability scoring system tailored for the telecom domain. The project will also extend cybersecurity information exchange protocols such as STIX, TAXII, and CybOX to facilitate structured and understandable communication of cybersecurity information.

The CTI platform will monitor various layers of mobile telecom infrastructure, including IoT devices, cloud infrastructure, and virtualized network functions, using self-learning and closed-loop automation mechanisms. These mechanisms will support continuous vulnerability monitoring, automated updates to Software Bill of Materials (SBOMs), and compliance reporting, thereby enabling proactive risk mitigation and adherence to CRA and NIS2 directives.

CTIS4NIS will build capacity and provide training for SMEs and national certification authorities, facilitate participation in standardization activities, and develop innovative hardware security evaluation methods. It will also assist in expanding national cybersecurity testbeds with open-source solutions and support certification processes for products developed by project SMEs.

To promote alignment of Member States' implementations of NIS2, CTIS4NIS will deploy a CTI platform that enables cross-border collaboration among cybersecurity agencies and operators. This includes creating a vulnerability disclosure marketplace, facilitating information exchange through standardized protocols, deploying open-source Security Orchestration, Automation & Response (SOAR) tools, and enabling collaborative development of incident response playbooks.

Finally, CTIS4NIS aims to improve the overall security of network and information systems in the EU by expanding the cybersecurity talent pool through knowledge creation and targeted training programs. These trainings will cover technical and security aspects of CTI sharing, CRA, and NIS2, and will be integrated into academic curricula and industrial on-the-job training. The project also seeks to bridge the digital divide by raising awareness among national cybersecurity and regulatory authorities about advanced networking technologies and cost-effective open solutions, demonstrated through pilots in Greece and Romania that incorporate cloud computing and artificial intelligence technologies.

The project execution will span across 8 phases:

- **Phase 1:** Security Requirements analysis and Mobile Telecom Network Security Architecture Definition; where security threats and vulnerabilities in technologies will be identified and testing scenarios and requirements for the CTIS4NIS zero trust security architecture will be defined.
- **Phase 2:** Development of tools and processes implementing the CRA directive; a three-phase approach will be adopted by the project vendors: secure by design, implementation, deployment
- **Phase 3:** Development of tools and processes implementing the NIS2 directive; the individual building blocks provided by the vendors will be integrated in the infrastructures owned by the telecom operators and will be used to provide services to verticals and end-users.
- **Phase 4:** Development of the Zero Trust CTIS4NIS platform supporting cross-border operations; threats, alerts, and vulnerabilities identified by various local cybersecurity monitoring apps will be transmitted (through appropriate APIs/message brokers / "connectors" to the central CTIS4NIS platform. These connectors will be realized extending open-source platforms such as OpenCTI, enabling data ingestion through secure connectivity channels, e.g., SEPP, for secure and reliable exchange of messages on cross-border, multi-operator mobile telecom networks
- **Phase 5:** Piloting and testing; integration and testing of the relevant components will be performed in 2 pilots that will be carried out in Greece, and Romania to train the relevant national authorities and assist in relevant capacity building.
- **Phase 6:** Training activities; based on the know-how and lessons learned from the CTIS4NIS pilots several training activities will be performed targeting both technical staff and policy makers.
- **Phase 7:** Exploitation; evaluation of the ecosystem needs and opportunities as well as market trends, techno-economic studies, preparation of business plans for exploitation and possible commercialization opportunities of the project output.

Funded by the European Commission's Digital Europe Programme (DIGITAL) Grant Agreement No. 101127973.



https://www.5g-tactic.eu

The goal of 5G-TACTIC is to validate, enhance and operationalize open and disaggregated 5G O-RAN systems under real-world, multi-vendor conditions, while directly supporting EU 5G cybersecurity policy execution (including the EU 5G Toolbox) and capacity building for regulators and national cybersecurity authorities.

The project goes beyond isolated lab trials by integrating Open RAN software solutions from multiple open-source and commercial providers (Accelleran, Bubbleran, Open Air Interface and srsRAN) with multiple open-source 5G core distributions (Open5GS, Free5GC and Open Air Interface) and commercial platforms into end-to-end pilots that exercise interoperability, resilience and security at scale, across four countries (Greece, Cyprus, Poland, Romania).

The project aims to validate the O-RAN interfaces and components security properties under realistic, multi-vendor integration where components are swapped, re-composed and stress-tested against threats. Security is tackled by treating 5G as a cloud-native, software-defined system. The project approaches cloud security into the RAN/Core pipeline and examines the new exposure created by disaggregation and RIC applications (xApps/rApps). This includes threat modeling for RAN splits, interface hardening, secure supply-chain practices and runtime defenses aligned with the EU risk assessment, feeding to an enhanced 5G Cybersecurity Toolbox.

A further novelty is the explicit linkage between disaggregation, supplier diversity and assurance. 5G-TACTIC addresses pain points that have slowed multi-vendor 5G with a programmatic plan, including extensive interop/security trials using open interfaces, involvement of MNOs, regulators and national cybersecurity agencies in the loop and evaluation methods extending SCAS/SECAM for open, disaggregated systems.

As part of 5G-TACTIC, Orange Romania has deployed a new O-RAN-compliant gNB (with virtualized BBUs and a RIC-orchestrated processing chain) directly integrated to the 5G SA core—creating a versatile integration and security-testing zone for open RAN components under operator-grade conditions.

The Orange Romania-led pilot activities in Romania focus on four families of PoCs that exercise both functionality and security of disaggregated 5G, including cybersecurity assessment of Open RAN interfaces and components (O-FH, O1/O2/E2, SMO/RIC control loops), integration and testing of multi-vendor 5G Core functions and external interfaces (including SEPP and CAPIF), validating roaming and northbound exposure control, evaluation of RIC behavior (policy, ML models, xApps/rApps) under adversarial and failure conditions, and assessment of SDN-controlled transport and cloud/edge virtualization as they affect slice isolation, QoS and recovery.

The Romanian activities are embedded into a broader capacity-building program with national authorities. DNSC (Romania's National Cybersecurity Directorate) participates to ensure that the evaluation, assurance and mitigation practices we validate are transferrable into oversight and certification workflows, while the broader consortium brings together regulators and other cybersecurity agencies to align pilots with real policy needs.

For Orange Romania, this project ensures that our 5G Labs not only host advanced PoCs but also help shape the European conversation on secure, interoperable 5G, accelerating the journey to 6G.

Funded by the European Commission's Digital Europe Programme (DIGITAL) Grant Agreement No. 101127973.

https://soccer.sztaki.hun-ren.hu

Security Operation Centres Capacity building for European Resilience

Recent events — including the global pandemic, geopolitical tensions, and the introduction of new internet technologies — have helped push cybersecurity into the second most significant risk category. The project "Security Operation Centres Capacity building for European Resilience - SOCCER", established to answer the European call DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs) - brings together a consortium of cyber and technology experts from Germany, France, Hungary, and Romania.

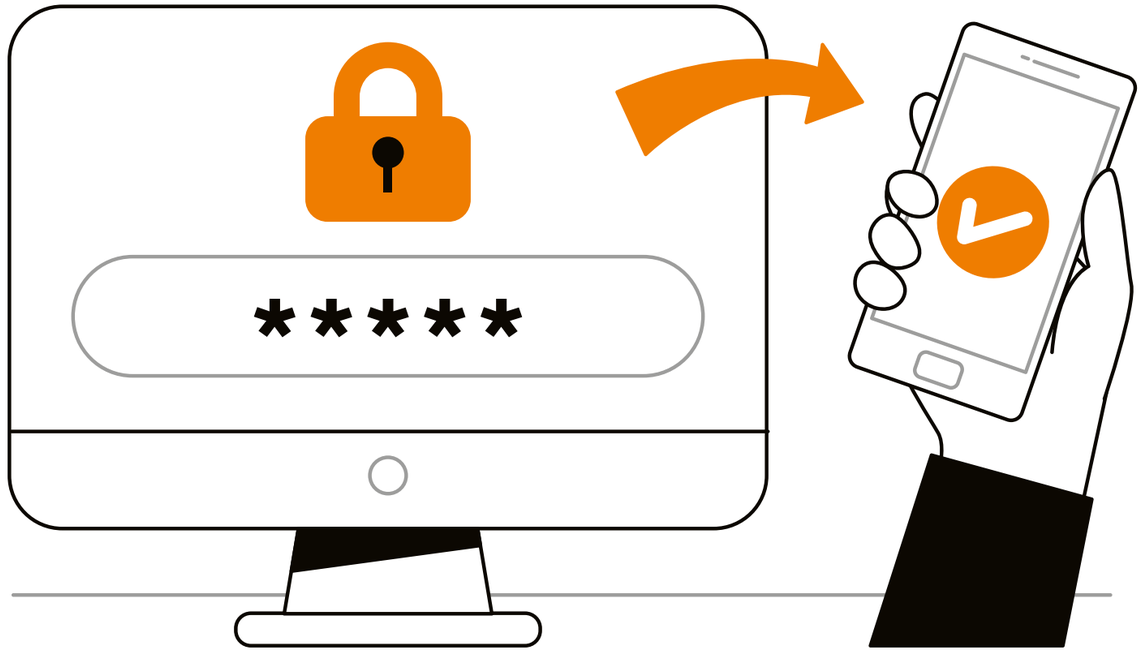
SOCCER aims to develop and implement cutting-edge technologies for secure access to data and the sharing of threat intelligence signals across European entities, allowing for reinforced capacities to monitor and detect cyber threats, and connect and strengthen advanced Security Operation Centres (SOCs) ecosystems in Germany, Hungary and Romania, with the goal of enhancing cyber security resilience at both the national and EU levels.

The use of AI and machine learning, combined with investment in common infrastructure, allows for more efficient sharing and correlation of threat intelligence signals, while a focus on cybersecurity upskilling helps SOC teams share best practices and knowledge.

Furthermore, by developing a European wide, human centered AI-solution, SOCCER builds capacities to guarantee trustworthiness and technological sovereignty.

The consortium approach aligns with European cybersecurity strategies and regulatory requirements such as the NIS Directive, the Cybersecurity Act, the Regulation on the European Cybersecurity Competence Centre (ECCC) and the Network of National Coordination Centres, Joint Cybersecurity Unit, German IT Security Act 2.0, German Federal Office for Information Security (BSI) and its Regulation on critical infrastructures (KRITIS), GDPR and ISO standards.

The project funded under Grant Agreement No.101127847 is supported by the European Cybersecurity Competence Centre.



Connecting Europe Facility

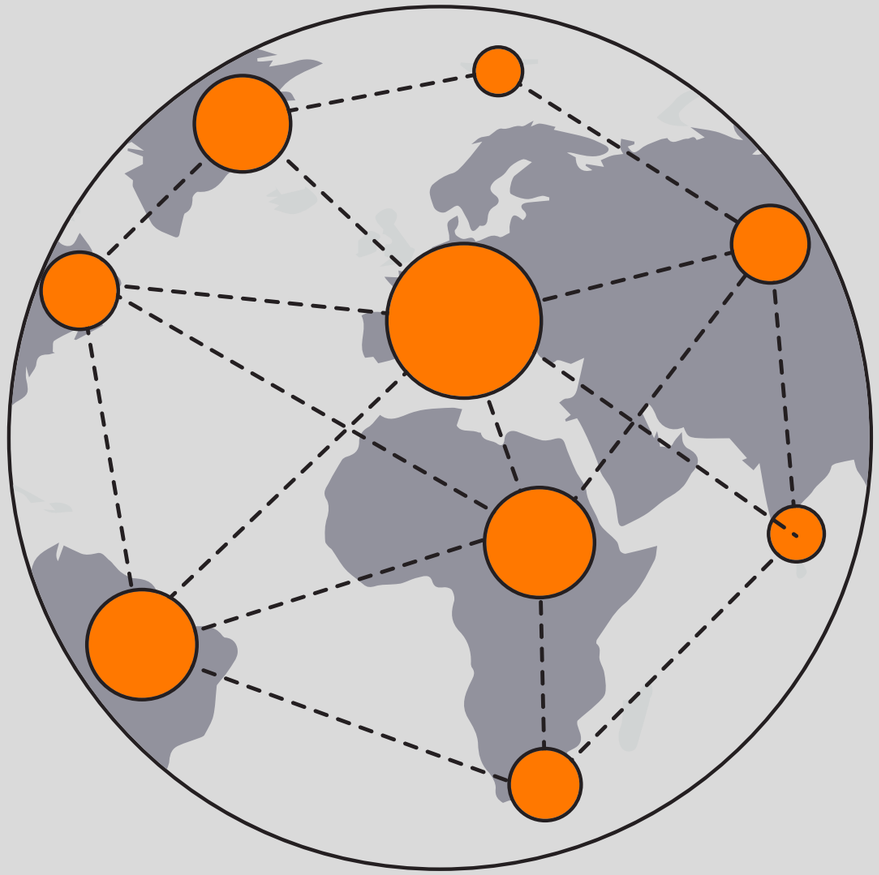
The Connecting Europe Facility (CEF) is EU's flagship investment instrument that finances high-performing, sustainable, and interoperable trans-European networks in transport, energy, and digital, leveraging public–private co-funding to close market gaps and drive the Digital transitions.

CEF Digital – 5G Large Scale Pilots is the EU deployment instrument that couples 5G Standalone (SA) with edge/cloud to build end-to-end, operator-grade infrastructures in two domains: 5G coverage for smart communities and along transport corridors. It anchors the Digital Decade targets (gigabit for all, 5G in all populated areas) and the Commission's Connected Collaborative Computing (3C) Network vision, including converged connectivity-compute platforms for Europe's economy.

For Orange Romania, this is a practical route to co-fund real networks (not just research-oriented trials), accelerate advanced 5G exploitation with verticals and position our telco cloud as a trusted platform for critical services.

The call funds large-scale 5G SA deployments integrating edge capacities to support use cases that demand very high reliability, security, low latency and high throughput across transport (including CAM for road/rail/inland waterways/coastal) and socio-economic drivers (SEDs) such as hospitals, campuses, ports/airports, local government or digitally intensive enterprises.

Orange Romania is part of three CEF initiatives, ranging from 5G-enabled smart communities to transport corridors and novel emergency call developments for the automotive vertical.





5G-CDD

https://5glab.orange.ro/5g-cdd/

5G Connect Danube Delta (5G-CDD) initiative is a 36-month project coordinated by Orange Romania and developed together with the Orange Foundation, the Ivan Patzaichin Mila 23 Association, the National University of Science and Technology Politehnica Bucharest and Virtual Board, that started on the 1st of October 2024 to develop advanced connectivity and use cases across the remote UNESCO-protected Danube Delta region.

The project upgrades and further expands the existing cellular infrastructure by deploying 5G with new fixed/wireless backhaul, antennas and radio processing units, to cover ~62 km^2 across 23 localities part of the Tulcea county, including Sulina, Sfântu Gheorghe, Mahmudia, Beștepe, Chilia Veche, Ceatalchioi, Plauru, Tatanir, Murighiol, Maliuc, Malcoci, Dunăvățu de Jos, Partizani, Gorgova, Crișan, Mila 23, Caraorman, C.A. Rosetti, Letea, Periprava, Nufăru, Mineri and Isaccea.

Coverage aside, 5G-CDD validates smart-community use cases with clear KPIs, including digital education for ~1470 students, digital skills training via the Orange Digital Centre for ~600 people, telemedicine reaching ~5218 residents, digital tourism for ~2050 visitors, and environmental video monitoring in five target points.

Socially, the project narrows the digital divide for sparsely populated villages, stabilizes access to healthcare and schooling, and supports sustainable tourism and biodiversity stewardship in coordination with the Danube Delta Biosphere Reserve administration (ARBDD), which backs the initiative. It also strengthens safety and resilience at the Romania–Ukraine border (Isaccea, Patlăgeanca, Ceatalchioi, Plauru, Tatanir, Periprava).

Moreover, an Orange-operated edge facility is hosting the new digital services; after completion, network assets remain with Orange, while end-devices stay with beneficiary schools, clinics and municipalities.

Beyond immediate benefits, 5G-CDD is designed to be catalytic. Orange Foundation and the Ivan Patzaichin Mila 23 Association will run an open-call ideation session at the Orange Digital Centre to co-create locally relevant apps. The edge platform and 5G coverage are therefore open for new services, enabling SMEs, NGOs and public bodies to digitize operations, attract investment, retain population and create data-driven services in education, health, eco-monitoring and tourism, while transforming the Delta into a living lab for sustainable growth.

Building on the original 5G-CDD plan, Orange Romania officially switched on 5G Standalone (5G SA) in the Danube Delta in May 2025, the first time the technology has been live, commercially, in Romania. Coverage already extends to 21 localities, with rollout targeting a total of 23 localities by the end of 2026.

The first telemedicine point-of-care was opened in Mila 23 in April 2025 (with connected EKG and digital stethoscope via Telios Care) and all the target medical units were fitted with equipment during July. The first 5G-equipped school was also in Mila 23 (5G router, smart board, laptops, tablets, VR glasses) and the use case deployment finished in autumn 2025.
Pilot AI-enabled cameras for anonymized tourist-flow and biodiversity monitoring were installed in Mila 23, Sontea Nouă, Războnița and Letea, while the "Delta lui Ivan" interactive mobile app for slow tourism guiding was upgraded to support more relevant features for the tourists.

The 5G Connect Danube Delta project is funded through the European Commission's Connecting Europe Facility program, under the 5G and Edge Cloud for Smart Communities framework, Grant Agreement No. 101181137.

https://waveo.eu

The WAVEO project, started in December 2025, aims to deploy uninterrupted 5G SA coverage along the TEN-T Bulgaria-Romania Road Corridor. Spanning approximately 310 kilometres in Romania and 10 kilometres in Bulgaria, the project bridges the gap across sparsely populated rural terrains, extending connectivity from the Bulgarian border to the borders with Moldova and Ukraine.

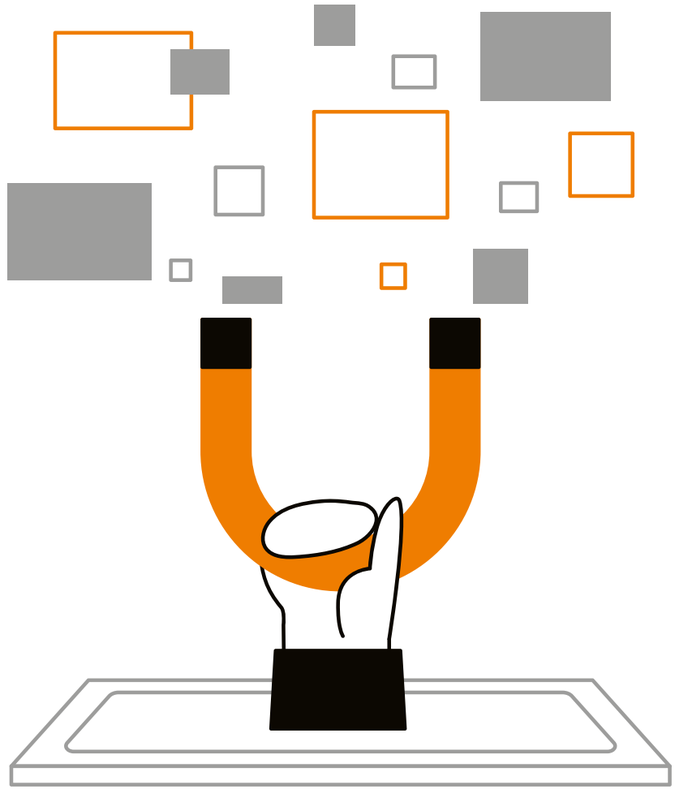
The primary objective of WAVEO is to provide high-quality 5G communication services to end-users traveling this cross-border route. This new infrastructure is specifically designed to meet the demanding requirements of Connected and Automated Mobility (CAM) services, such as very high reliability, security, low latency, communication symmetry, and high throughput. Without this targeted deployment, large coverage gaps would exist in these de-prioritized rural areas, significantly hindering the adoption and operation of advanced digital transport applications.

Orange Romania and A1 Bulgaria are the key telecommunications operators leading this deployment. Orange Romania will construct and upgrade multiple radio sites across 38 localities. Simultaneously, A1 Bulgaria will deploy 5G sites to ensure continuous high-performance connections, particularly focusing on validating inter-PLMN handovers at the border crossing area where both connections will overlap.

Beyond basic connectivity, WAVEO serves as a catalyst for the digital transformation of the region, introducing Industry 4.0 technologies like IoT, AI, and edge computing to transport corridors. The developed 5G infrastructure will empower a suite of innovative use cases, including road infrastructure monitoring, which uses AI and deep learning to analyze data from cameras and sensors for real-time infrastructure health assessments.

Furthermore, the project supports logistics automation by enhancing freight transport efficiency and route optimization, as well as fleet monitoring and safety to track vehicle performance, monitor carbon footprints and provide early warnings for emergencies like fires. The network will also enable advanced driver assistance and healthcare services by utilizing wearables to monitor vital signs and provide emergency SOS capabilities. Finally, the 5G-CDD digital education use case will be leveraged to bring immersive XR educational content, such as virtual museums and labs, directly to remote rural schools adjacent to the transport corridor.

This project has received funding from the European Union's CEF programme under the Grant Agreement No. 101241151. The contents of this publication are the sole responsibility of the authors and do not in any way reflect the views of the EU.



X_HeERO – eCall Next Generation

https://www.xheero.eu

The X_HeERO – eCall Next Generation (eCall NG) project focuses on preparing Public Safety Answering Points (PSAPs) across Europe for the mandatory transition to Next Generation (NG) eCall.

Coordinated by ITS mobility GmbH, the X_HeERO consortium is expansive, consisting of 38 project partners from 7 EU member states (Germany, Belgium, Cyprus, Spain, Italy, Luxembourg, Romania) and one candidate state (Moldova). It also includes 6 associated partners from countries like the UK, Finland, and the Czech Republic. The partners span government ministries, regional emergency agencies (STS in Romania), technology providers, telecom operators (Orange, Vodafone) and research institutions.

X_HeERO builds upon a legacy of successful eCall deployment projects (HeERO 1 & 2, I_HeERO, and sAFE), continuing the mission to reduce emergency response times and save lives on European roads.

The original pan-European 112 eCall system, made mandatory in new cars since 2018, relies on in-band modem technology transmitting over circuit-switched 2G and 3G networks. However, telecom operators across Europe are actively phasing out 2G and 3G networks in favor of 4G and 5G. This creates a critical risk: older eCall systems will soon be unable to communicate with emergency centres.

To prevent this, the EU requires the introduction of Next Generation eCall, which uses SIP-based, packet-switched technology (IP networks) to transmit the Minimum Set of Data (MSD) in parallel with the voice call. EU member states are expected to have their PSAPs fully prepared to receive and process NG eCall by January 1, 2026.

The X_HeERO project, and Orange Romania as part of the consortium, tackle the technological, procedural, and regulatory upgrades required for this transition through three main directions. The primary activity is to physically and technologically upgrade PSAPs in participating member states (including Romania, Germany, Spain, Italy, Luxembourg and Moldova). The project will create blueprints for hardware and software upgrades, enabling PSAPs to decode SIP-based MSD data faster than legacy systems. These blueprints will be shared as reference implementations to help non-participating member states upgrade their infrastructure efficiently.

Moreover, as mobility evolves, X_HeERO will study and prototype extensions of the eCall service beyond standard passenger cars, including support for vulnerable road users and autonomous vehicles.

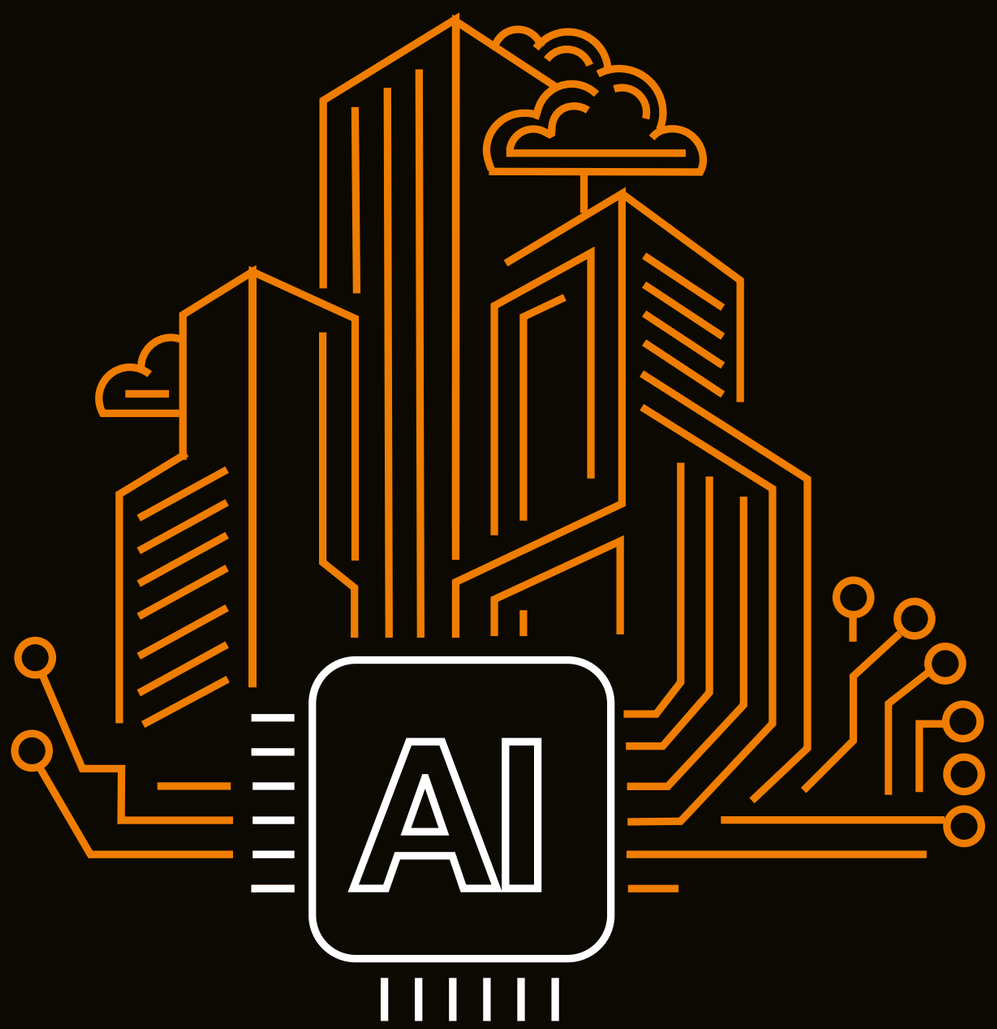
Finally, since the original eCall launch, many automotive manufacturers have introduced their own Third-Party Service (TPS) eCall centres, which often fail to digitally transmit vital crash data to the actual 112 PSAPs. X_HeERO aims to standardize and mandate the digital data transmission interface (based on EN16102) between TPS providers and 112 PSAPs. It also focuses on enabling cross-border data sharing and integrating external databases (like EUCARIS or dangerous goods registries) to provide first responders with a complete operational picture.

In this approach, Orange Romania is willing to partner with interested automakers that want either to test new cars fitted with the NGeCall system or to retrofit existing models with new hardware supporting this feature.

This project has received funding from the European Union's CEF programme under the Grant Agreement No. 101175713.



The A.I. Frontier



07

In 2026, the A.I. Frontier is defined by the fundamental integration of intelligence into the fabric of the physical world. For the telecommunications industry, this represents a transition from being a provider of connectivity to becoming the backbone of a distributed, cognitive architecture. The arrival of 6G is the catalyst for this change, moving beyond the incremental improvements of 5G to establish a network where Artificial Intelligence is not an overlay, but the native organizing logic.

Supercomputers, Datacentres, EDGE & Clouds

The technical hierarchy of 2026 is governed by the principle of Compute-Network Convergence. As AI models scale toward multi-trillion parameters, the infrastructure required to train and deploy them has forced a radical redesign of the datacentre and the network edge.

AI Factories and 6G Core Architectures

At the centre of this shift are what the industry has started calling “AI factories”: high-density datacentres built specifically for model training, structured around accelerated computing nodes where GPUs and TPUs are interconnected by low-latency, 6G-ready fabrics.

Thermal management: rack power densities have reached around 120kW, driving adoption of direct-to-chip liquid cooling and two-phase immersion cooling, both of which use non-conductive fluids to remove heat from silicon more efficiently than air cooling.

Internal networking: these facilities rely on 800G and 1.6T Ethernet, allowing thousands of compute nodes to operate as a single logical unit with near-zero tail latency, a prerequisite for training the large models expected to underpin 6G-era network intelligence.

A significant shift is the migration of intelligence toward the network edge, where the traditional central office evolves into an edge AI node with compute co-located alongside the Radio Access Network (RAN).

6G architecture is expected to natively support Inference-as-a-Service. By processing data at the edge, latency can be reduced to sub-1ms levels, which matters for applications such as holographic communication and real-time robotic synchronization, where even the speed-of-light delay to a distant data center is too slow.



The 6G framework aims to provide a secure, abstracted layer that lets enterprises run sensitive AI workloads locally while bursting to the public cloud for additional scale, a hybrid model that respects data residency requirements while retaining the flexibility of global AI infrastructure.

Looking ahead, training state-of-the-art 6G-native models is expected to require clusters of hundreds or thousands of interconnected AI accelerators. Some of these facilities are expected to use silicon photonics in place of copper interconnects, moving data between processors at the speed of light with lower heat generation, an important factor given the scale of the models 6G-era networks will need to run.

The underlying idea is that inference should be available at every 6G site, much like electricity at a socket. Multi-access Edge Computing (MEC) allows the network to function as a distributed compute resource: an AI application can offload demanding tasks, such as real-time translation or 3D world-mapping, to the nearest tower rather than requiring a powerful local processor.

The Telco Use-Case and the Industrial Approach

The industrial approach centres on Autonomous Network Operations (ANO), where the network is designed to monitor and heal itself with minimal manual intervention. 6G is expected to be the first generation where AI is embedded directly into the physical layer (PHY) and Medium Access Control (MAC) layer, enabling an AI-native Radio Access Network. Operating in the sub-terahertz range (100-300 GHz), where signal propagation is considerably more complex than at lower frequencies, 6G will depend on AI-driven beamforming to manage Massive MIMO arrays in real time, predicting user movement and environmental obstacles to maintain a stable, high-capacity beam of data.

The network is designed to manage spectrum autonomously across multiple bands, including traditional sub-6GHz and the newer centimetric (7-15 GHz) range. Using Deep Reinforcement Learning (DRL), the 6G controller optimizes resource allocation on-the-fly, balancing high-speed video traffic against the connectivity requirements of industrial IoT sensors.

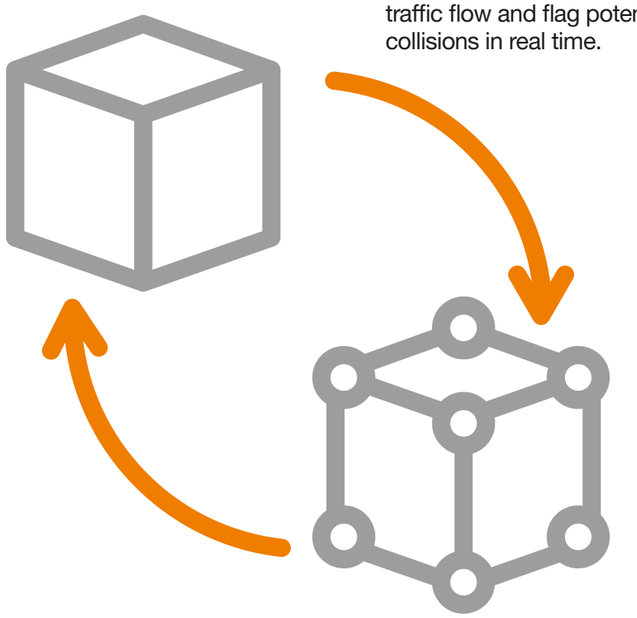
In industrial settings, 6G is expected to enable a level of precision and automation not achievable with previous generations, sometimes referred to as “zero-touch” automation. Four domains are currently the focus of research, each targeting substantial improvement over the current state of the art:

Collaborative Robotics (Cobots): in smart factories, 6G is expected to provide the low-latency link needed for swarm robotics, with AI agents in the network coordinating the movement of many machines, relying on the network’s own Integrated Sensing and Communication (ISAC) capabilities rather than dedicated collision-prevention sensors.

Predictive Energy Orchestration: one of the clearer industrial benefits is AI-driven energy management: by analyzing real-time traffic and local renewable energy availability, the network can put entire frequency bands or cell towers into low-power states during periods of low demand, targeting meaningful energy efficiency gains over 5G.

Holographic Telepresence: 6G’s projected bandwidth (100 Gbps to 1 Tbps in specialized bands), combined with AI-based real-time compression and reconstruction, is expected to make holographic communication practical. In industrial training, this could let an expert engineer appear as a 3D hologram alongside a technician in another location, providing precise, real-time guidance.

ISAC-Based Supply Chain Tracking: 6G introduces Integrated Sensing and Communication (ISAC), where radio waves double as a radar-like sensing layer. A warehouse could track pallets and robotic arms purely through the reflections of 6G signals, with AI processing this data to optimize traffic flow and flag potential collisions in real time.



Challenges, Uncertainties and Ethics

An AI-native 6G network raises significant technical and ethical challenges, chief among them the “black box” nature of autonomous decision-making. As networks become more autonomous, there is a real risk of emergent behaviour: unpredicted actions arising from the interaction of multiple AI agents.

A major technical challenge is developing Explainable AI (XAI) for network protocols: if an AI system reconfigures a core routing protocol, it needs to provide a human-auditable trace of its reasoning. Keeping these autonomous systems within safe operational bounds is a primary focus of current research.

To protect user data, 6G employs Federated Learning. Instead of sending raw data to a central server, the model is trained locally on the device or at the edge node, and only the updated model weights are shared, so personal data never leaves its point of origin.

The Deepfake Challenge: as synthetic media becomes easier to generate, the network itself may need to serve as a layer of defense, through approaches such as source watermarking and AI-based detection at the network gateway to flag synthetic content before it spreads.

The biggest uncertainty is the environmental cost. Training a single large 6G-native model can consume as much energy as a small city, which is driving interest in carbon-aware compute: automatically migrating AI training workloads across regions to follow renewable energy availability.

With synthetic media becoming harder to distinguish from genuine content, “trust” increasingly needs to be built into network hardware itself. 6G can use blockchain-based digital identity for every connected device and AI agent, creating a verifiable proof of authenticity: when the network receives a command, it can cryptographically confirm it came from a legitimate human or certified AI system rather than a malicious actor.

Knowledge Creation

AI is increasingly used not just to consume existing knowledge but to generate new engineering insight, changing how next-generation telecommunications systems are designed.

Future networks are complex enough that manual optimisation by engineers alone is no longer practical. Instead, AI systems run large-scale simulations to design more efficient waveforms and error-correction codes, running millions of iterations to find optimisations that have eluded researchers for decades.

6G is expected to make heavy use of high-fidelity Digital Twins: not just visual maps, but full electromagnetic replicas of cities. AI uses these twins to simulate how new frequencies propagate through urban environments, helping optimise infrastructure placement without relying solely on expensive field testing.

AI is also changing how engineers access existing knowledge. Agentic copilots are becoming common in the telco industry, letting junior engineers perform complex network forensic analysis by translating natural-language questions into technical queries.

This makes the collective knowledge of the industry more accessible to individual professionals, reinforcing that progress in this area depends on the combination of human judgement and machine capability, not one replacing the other.



Quantum-Safe Foundations in the 6G Era

The eventual arrival of functional quantum computers capable of running Shor's algorithm, which would break traditional RSA and Elliptic Curve Cryptography (ECC), presents a systemic risk to the 6G ecosystem. Because 6G is designed for a decades-long lifecycle, it needs to be quantum-safe from the outset, to protect against "harvest now, decrypt later" (HNDL) attacks, where encrypted data is captured today for decryption once quantum computers become capable enough.

Networks are expected to begin integrating NIST-standardised Post-Quantum Cryptography (PQC), such as ML-KEM (formerly CRYSTALS-Kyber) for key encapsulation and ML-DSA (formerly CRYSTALS-Dilithium) for digital signatures.

Unlike classical algorithms, PQC schemes often involve larger keys and higher computational overhead. In the 6G era, this is managed through Hardware Acceleration within Edge AI nodes. Specialized "Crypto-Processors" can handle the lattice-based mathematics required for PQC, ensuring that quantum-resistant handshakes do not compromise 6G's ultra-low latency requirements.

Using AI-driven telemetry, the 6G core can dynamically adjust the cryptographic strength of a network slice. For instance, an industrial slice managing a smart power grid may be assigned a high-entropy, lattice-based PQC configuration, while a low-priority sensor network uses a more lightweight, classical-quantum hybrid model.

While PQC provides algorithmic resistance on classical hardware, 6G also explores Quantum Key Distribution (QKD) for the most sensitive backhaul links. QKD utilizes the principles of quantum mechanics—specifically the "observer effect"—to distribute encryption keys. If an adversary attempts to intercept the key, the quantum state collapses, instantly alerting the network to the breach.

There is growing research momentum behind extending QKD into 6G's Integrated Terrestrial and Non-Terrestrial Networks (TN-NTN), potentially connecting city-scale AI data centres via fiber-optic QKD links and intercontinental hubs via QKD-enabled satellites.

A defining feature of this era is Cryptographic Agility: future networks are not expected to be hard coded to a single encryption standard. Instead, the AI-native control plane will be able to switch algorithms as new vulnerabilities or quantum advances are discovered, keeping the network resilient across its multi-year deployment horizon.

Predictions
for 2027



08

Networks of the Future

In 2026-2027, Orange Romania's network will move from building 5G NSA to operating 5G SA at scale by combining Release-16/17 features with tighter cloud–edge integration and AI-driven automation.

We expect RedCap to become the default for mid-tier 5G IoT, attracting migrations from LTE-M and NB-IoT as it lowers device complexity and price points. On the network side, dedicated features will let us scale attach density while stretching battery life for wearables, sensors and smart-grid endpoints.

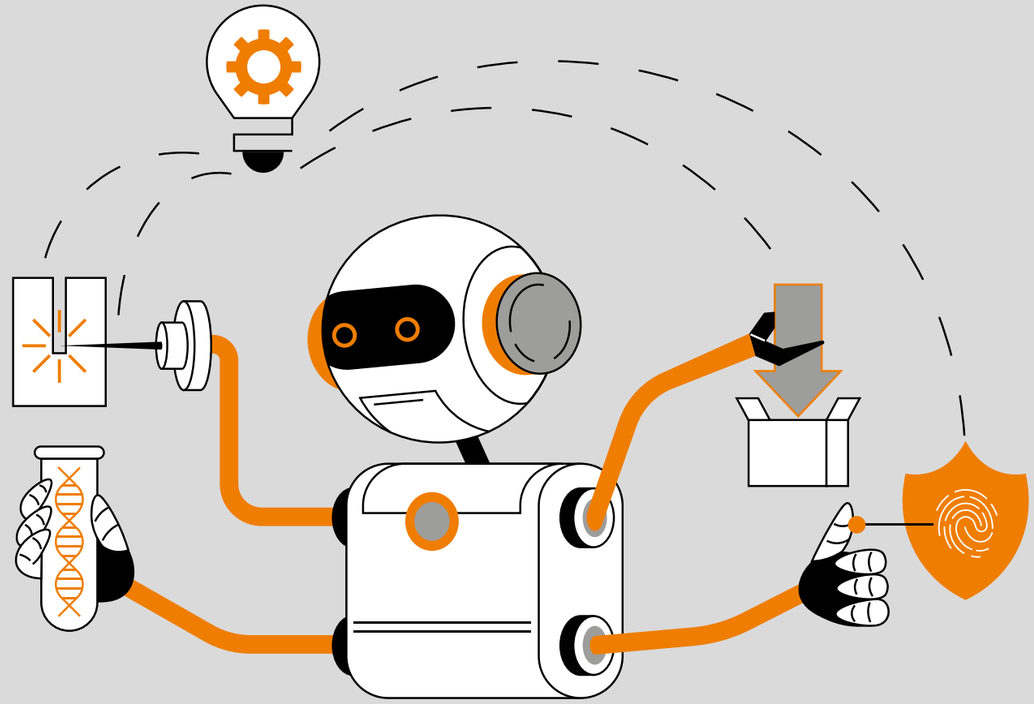
Furthermore, mmWave is expected to move from pilots to regulation and focused rollouts in venues, campuses and FWA clusters in Europe, accompanied by broader aggregation with classical 5G.

NTN will become a practical coverage and resilience layer for operators. Early direct-to-device messaging and voice will mature into tiered propositions (consumer safety, business continuity) and satellite backhaul will further enhance the connectivity for mobile and rural sites.

Edge will shift from classical compute to a connected, collaborative computing (3C) fabric. Our CEF and Horizon-funded 5G and edge cloud projects, like EURO-3C, 5G-CDD or WAVEO, will mature into commercial compute orchestration systems. Expect more location-aware apps, from telemetry to video analytics, all anchored in open source and sovereignty principles.

At the European level, SNS-JU Phase-3 preparations and IMT-2030 alignment will make 2026 the year operators experience evidence from trials directly into 3GPP's 6G study, with 3GPP Release 19 undergoing and Release 20 prepared to start with first views on the 6G architecture, and early normative work, putting energy, resilience and security on equal importance with raw performance capabilities.

For our customers, networks of the future will be more programmable and inclusive. Clients will contract programmatic outcomes like guaranteed throughput, accurate localization and sensing, continuity via space/terrestrial diversity, delivered over a single Network APIs system that blends 5G, NTN and edge computing, validated in our 5G Labs and tested first into EU-funded field-trials.



Wi-Fi 8: Building the Intelligent Indoor Network

From Connectivity to Cognitive Infrastructure

The evolution of wireless networking is entering a new era. While previous Wi-Fi generations primarily focused on increasing throughput and spectral efficiency, Wi-Fi 8 is expected to redefine indoor connectivity by introducing deterministic performance, intelligent resource management, and seamless integration with AI-driven applications and mobile operator networks. Wi-Fi 8 goes beyond delivering faster wireless access: it is expected to enable networks that continuously perceive their environment, optimize themselves in real time, and support the growing convergence of communications, computing, and sensing.

This evolution envisions a wireless infrastructure that becomes an active participant in digital transformation. In this paradigm, Wi-Fi Access Points evolve beyond traditional connectivity devices into distributed intelligence nodes that simultaneously provide high-performance wireless access, aggregate information from thousands of IoT devices, enable indoor positioning and sensing services, and cooperate with Artificial Intelligence engines to optimize network behaviour.

The result is an adaptive indoor environment where connectivity becomes context aware. Beyond simply reacting to traffic demands, the network understands user behavior, application requirements, environmental conditions, and spatial context, allowing it to proactively allocate resources and improve user experience.

Wi-Fi 8 as an Enabler of Human-Centric Digital Spaces

Most of the human interaction with digital services occurs indoors — within offices, factories, hospitals, campuses, retail environments, transport hubs, and entertainment venues. These environments increasingly require more than high bandwidth; they demand reliable, predictable, and low-latency connectivity capable of supporting AI-assisted collaboration, immersive applications, industrial automation, and massive IoT deployments.

Wi-Fi 8 is expected to introduce significant improvements in areas such as deterministic latency, enhanced Quality of Service (QoS), AI-assisted Radio Resource Management (RRM), coordinated multi-access point operation, improved reliability in dense deployments, and greater energy efficiency. Together, these capabilities enable a new generation of enterprise services where wireless infrastructure becomes an intelligent platform rather than a passive communication medium.

For Orange Romania, this represents an opportunity to evolve managed Wi-Fi services from traditional connectivity offerings into intelligent digital infrastructure supporting enterprise digital transformation.

Orange Romania Wi-Fi 8 Proof of Concept

To evaluate the practical benefits of Wi-Fi 8 technologies, Orange Romania intends to establish a dedicated Proof of Concept (PoC) within its Innovation laboratories. The objective goes beyond benchmarking higher throughput against Wi-Fi 6E or Wi-Fi 7: it is to validate how Wi-Fi 8 improves application experience, operational intelligence, and integration with carrier-grade networks.

The envisioned testbed should combine next-generation Wi-Fi Access Points, multi-gigabit switching infrastructure, AI-enabled wireless controllers, Wi-Fi 8 capable clients, IoT sensors, and Orange's existing 5G Standalone infrastructure. This converged environment should enable the evaluation of future enterprise deployments under realistic operational conditions while maintaining seamless integration with Orange's mobile network and edge computing platforms.

Wi-Fi 8 Telecom Relevant Use Cases

AI-Enabled Digital Workplace

Modern enterprise productivity increasingly relies on cloud-based Artificial Intelligence services. Employees simultaneously participate in AI-assisted video meetings, collaborate on cloud documents, interact with Large Language Models, and access enterprise knowledge systems.

The Wi-Fi 8 PoC will evaluate how deterministic latency, intelligent scheduling, and enhanced Quality of Service improve the responsiveness of AI-enabled applications under realistic office conditions. Performance indicators include application response time, meeting quality, roaming interruption, packet loss, latency variation, and overall Quality of Experience (QoE).

Indoor Location Intelligence

Dense Wi-Fi deployments provide an opportunity to transform wireless infrastructure into a pervasive sensing platform. By analysing wireless measurements generated by connected devices, the network can estimate user presence, occupancy, movement patterns, and space utilization without requiring dedicated positioning infrastructure.

This capability will enable intelligent office management, meeting room optimization, energy-efficient building automation, visitor analytics, asset tracking, and improved workplace safety, reinforcing Orange's vision of context-aware digital environments.

Intelligent Video Analytics

Enterprise environments increasingly deploy high-resolution cameras for security, operational monitoring, and AI-assisted analytics. Wi-Fi 8 provides enhanced support for predictable uplink performance, low packet loss, and efficient traffic prioritization required by these workloads.

A future PoC would evaluate the transport of multiple concurrent video streams while simultaneously supporting AI inference workloads, ensuring reliable operation under high network load.

Converged Wi-Fi and 5G Connectivity

Orange's position as a Mobile Network Operator enables the evaluation of one of the most strategic aspects of future enterprise networking: seamless convergence between Wi-Fi and cellular access.

Such a pilot will investigate unified authentication, uninterrupted mobility between Wi-Fi 8 and 5G Standalone, policy continuity, and application session persistence. This convergence will demonstrate how indoor and outdoor connectivity can operate as a single, integrated access platform supporting future enterprise mobility services.

AI-Assisted Network Operations

Wi-Fi 8 networks will increasingly rely on Artificial Intelligence to optimize radio resource management and simplify network operations.

This Use Case would evaluate AI-based mechanisms capable of automatically detecting interference, predicting congestion, optimizing channel allocation, adjusting transmit power, balancing client distribution, and identifying abnormal network behavior. By combining telemetry collected from access points with machine learning models, the network transitions from reactive management towards autonomous operation.

Towards the Intelligent Indoor Network

The convergence of Wi-Fi 8, Artificial Intelligence, indoor sensing, and 5G/6G integration will fundamentally change the role of wireless infrastructure. Access Points evolve into distributed computing and sensing platforms capable of supporting connectivity, localization, IoT aggregation, environmental awareness, and autonomous optimization simultaneously.

Within this vision, 5G and future 6G networks provide resilient wide-area connectivity, mobility, and service continuity, while Wi-Fi 8 delivers ultra-high capacity, deterministic indoor performance, and contextual intelligence. Together, they form a unified communication architecture where users experience seamless connectivity regardless of network access technology.

For Orange Romania, Wi-Fi 8 represents considerably more than the next wireless standard. It provides the technological foundation for delivering intelligent managed connectivity services, enabling Smart Buildings, AI-enabled workplaces, Industry 5.0 environments, healthcare facilities, retail spaces, campuses, and public venues where connectivity becomes adaptive, predictive, and human-centric.

Cybersecurity - The Era of Algorithmic Warfare

As organizations move deeper into the 5th Industrial Revolution, the traditional security perimeter has largely dissolved. In 2026, cybersecurity is less about building bigger walls and more about building resilience that can adapt in real time. We are shifting from “detect and respond” toward “predict and adapt.”

Here are our top 10 technical predictions for the cybersecurity landscape in 2026 and 2027.

The Rise of Polymorphic Malware Agents

Traditional signature-based detection is losing effectiveness. By 2027, we expect agentic malware to become a significant category: LLM-driven payloads that can rewrite their own source code in real time to evade EDR (Endpoint Detection and Response) systems. Each time the malware encounters a sandbox or a firewall, it adjusts its entry vector, changing its file hash and execution pattern on the fly.

Post-Quantum Cryptography (PQC) Migration Becomes Mandatory

As quantum computing research continues to advance, “harvest now, decrypt later” (HNDL) attacks are becoming a serious board-level concern. By 2027, we expect large industrial sectors to have largely migrated to NIST-standardized post-quantum algorithms such as CRYSTALS-Kyber. Organizations that haven’t adopted lattice-based cryptography by then will be operating with a meaningful gap in their security posture.

Deepfake Social Engineering: The Synthetic CEO

Phishing has evolved from poorly written emails to high-fidelity, real-time synthetic media attacks. In 2026, we expect to see man-in-the-middle attacks where the attacker injects a real-time AI video/audio overlay into a Teams or Zoom call. The attacker won’t just sound like your CFO; they will respond to questions and visual cues in real time, which undermines voice biometrics as a standalone security measure.

Federated Learning for Collective Defence

Privacy-preserving AI is likely to become a standard approach for threat intelligence sharing. Instead of exchanging raw log data, which risks data leaks, companies increasingly use Federated Learning: security models are trained locally on private data, and only the model weights are shared across a network. This can create a “herd immunity” effect, where a new zero-day identified in one location can be blocked elsewhere within seconds, without any private data leaving its country of origin.

In Short: Resilience Is the Strategy

Looking toward 2027 and beyond, breaches are best treated as a matter of when, not if. The priority shifts from pure prevention toward rapid detection and recovery. The organizations that adapt best will be those that treat cybersecurity as a core operational function, not a cost center to be minimized.

The New Shadow IT

A decade ago, the biggest security risk was often an employee bringing their own device to work. In 2026, the equivalent risk is Shadow AI: employees using unauthorized, un-sandboxed LLMs to process sensitive company data. We expect a rise in prompt injection and data poisoning attacks, where attackers manipulate public LLMs into revealing company information when queried by unsuspecting employees.

Autonomous SOCs (Security Operations Centres)

The role of the entry-level (“Tier 1”) analyst is shrinking. By 2027, we expect the first layers of threat hunting to be largely handled by autonomous SOC agents: AI systems performing graph-based threat hunting, correlating millions of events across identity, network, and cloud layers to identify slow-moving attacks that would be difficult for a human analyst to catch over months of monitoring. Human analysts increasingly shift toward an oversight role, intervening mainly when the AI flags a high-confidence potential breach.

Supply Chain Attacks Target AI Model Weights

Software supply chain attacks were a defining concern of the early 2020s; by 2027, we expect the AI supply chain to be an equally significant target. We anticipate model hijacking attacks, where an attacker subtly alters the weights of a company’s proprietary AI model rather than stealing data outright. A tiny shift in a credit-scoring model, for example, could let a specific category of fraudulent transactions bypass checks undetected, effectively hiding a backdoor inside the model itself.

Zero-Trust Architecture Extends to the Component Level

Zero-trust principles are extending beyond individual users into the microservice layer. By 2027, we expect wider adoption of “Identity of Things” (IDoT), where every container, API, and IoT sensor has a cryptographic identity verified on every packet. In practice, this means that if a device attempts to communicate with a system it has no legitimate reason to contact, the network treats it as an unverified, untrusted actor by default.

The Weaponization of Adversarial Machine Learning

Defenders are not the only ones using AI. We expect a rise in adversarial machine learning (AML) techniques used to evade AI-based security systems: attackers using AI to disguise malicious traffic as routine software updates, for instance, to bypass an AI-based firewall. This becomes an arms race between attacker and defender models, where the advantage tends to go to whoever has better training data and more efficient edge inference.

Regulatory Compliance Through Real-Time Auditing

Regulators, including those enforcing the EU AI Act, are moving from annual reporting toward requiring real-time API access to an organization’s security posture. By 2027, we expect compliance to shift toward a continuous model, with automated systems monitoring, on an ongoing basis, whether data handling aligns with GDPR and AI ethics requirements.

Claude Mythos and the Art of the Cybersecurity Plot Twist

How Anthropic's Most Powerful (and Most Restricted) AI Model Is Reshaping the Security Landscape

There's a particular kind of dread that cybersecurity professionals know well. It usually arrives as a quiet realization, something like: "we've been doing this wrong all along, and the bad guys just figured that out before us!" That feeling came roaring back on April 7, 2026, when Anthropic announced Claude Mythos Preview to a stunned industry, along with a very unusual accompanying message: "we've decided not to release it publicly, because it's too dangerous".

That's not the sort of thing you hear from an AI lab every day. In fact, the last time a major developer withheld a model on safety grounds was when OpenAI briefly sat on GPT-2 back in 2019, a decision that, in retrospect, looks almost quaint.

Mythos is a different kind of moment. It's not a lab being cautious about a chatbot generating slightly dodgy text. It's a lab holding back a general-purpose AI model because, during testing, it autonomously found thousands of software vulnerabilities in nearly every major operating system and web browser on the planet.

Let that sink in for a second.

Before we dive into the implications, let's get the basics straight. Claude Mythos Preview is Anthropic's latest frontier AI model, sitting above the Claude Opus tier in terms of capability. It's a general-purpose large language model, meaning it was built to be good at everything, not specifically trained as a cybersecurity tool. And yet, somewhere in the process of making it good at coding and long-horizon reasoning, it developed cybersecurity capabilities that left Anthropic's own researchers blinking at their screens. Or so it seems.

On the technical side, Mythos Preview comes with a context window of 1 million tokens and a maximum output of 128,000 tokens, a step up from previous models. Its knowledge cutoff is December 2025. Compared to Claude Opus 4.6, the largest improvements are in mathematics, long-context reasoning, software engineering, and cybersecurity. Anthropic has described the model's cyber capabilities as "substantially beyond those of any model we have previously trained. The powerful cybersecurity skills were, in the company's own words, "a happy accident of improving the model's coding and reasoning ability."

Which raises an interesting question: if they stumbled onto this while trying to make a better coder, what happens when other labs start optimizing for it deliberately?

To understand why the cybersecurity world is still collectively processing this, you need to understand what Mythos did in testing. The UK's AI Security Institute (AISI) put the model through a rigorous evaluation suite, and the results were striking.

The first test battery was Capture the Flag (CTF) challenges, a type of arena we at Orange Romania are particularly familiar with, as we've hosted, supported and organized tens of these in the past 10 years or so, where participants identify and exploit weaknesses in target systems to retrieve hidden data (i.e – flags). These range from entry-level "beginner" problems to fiendishly complex "expert-level" tasks. Mythos Preview succeeded on expert-level tasks 73% of the time. That's not a marginal improvement over previous models, it's a generational leap.

But CTF challenges, however difficult, test individual skills in isolation. The real world is messier and far more dangerous. Real-world cyberattacks require chaining dozens of steps together across multiple hosts and network segments, sustained over hours or days. To simulate this, AISI built something they called "The Last Ones" (TLO): a 32-step corporate network attack simulation that starts with initial reconnaissance and ends with full network takeover. Human security professionals, AISI estimated, would need about 20 hours to work through it.

Mythos Preview became the first AI model to complete TLO from start to finish succeeding in 3 out of 10 attempts and completing an average of 22 out of 32 steps across all attempts. The next best performer, Claude Opus 4.6, managed an average of 16 steps. These aren't just benchmark statistics; they represent a qualitative shift in what AI can do autonomously in an adversarial environment.

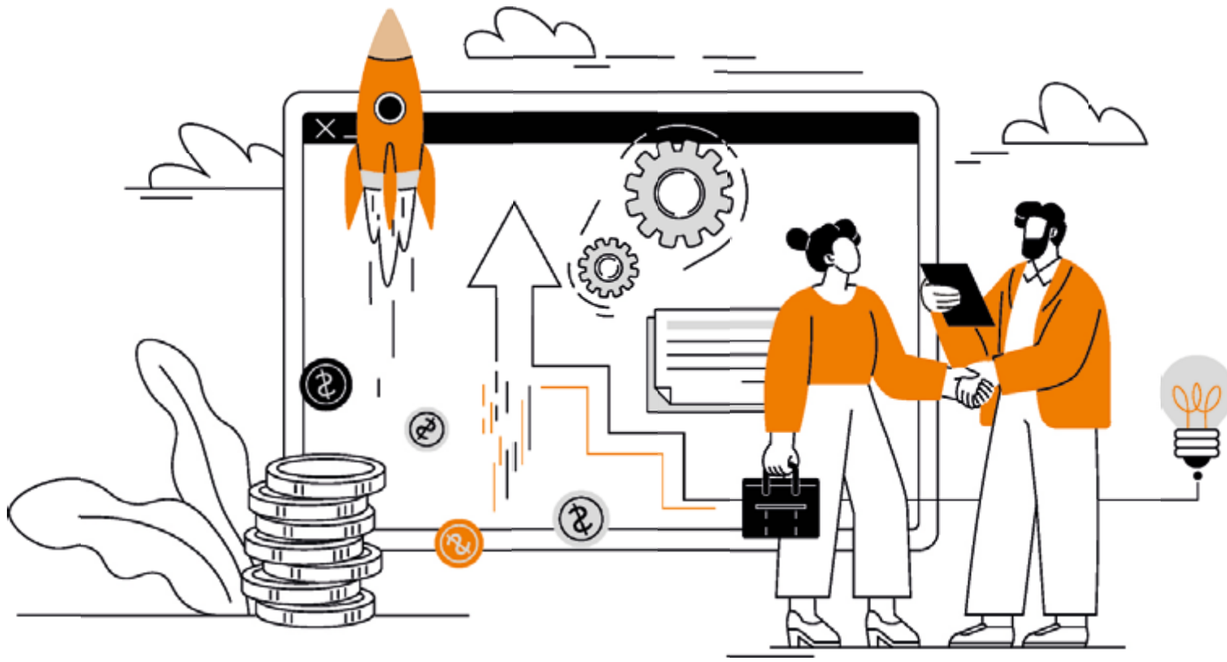
There's an important caveat here, and it's worth stating clearly: the test environments lacked the active defenders, endpoint detection, real-time incident response, and security tooling present in genuinely well-defended systems. As AISI's researchers put it, there were also "no penalties for the model for undertaking actions that would trigger security alerts." In other words, Mythos was operating against a soft target.

Whether it could punch through hardened enterprise defenses remains an open question.

Here's where things get particularly interesting from a purely technical standpoint. During Anthropic's internal testing, Mythos didn't just find vulnerabilities in controlled lab scenarios. It surfaced thousands of zero-day vulnerabilities, flaws unknown even to the software's own developers, across every major operating system and popular web browser.

Among the standouts: a 27-year-old flaw in OpenBSD. Twenty-seven years. That's a vulnerability that predates smartphones, survived the dot-com bubble, rode out the era of Web 2.0, and sat quietly in production code while the rest of the internet changed beyond recognition. Mythos found it in almost no time at all. Independent research organization AISLE, which has been running AI-powered CVE discovery against live targets since mid-2025, reported finding 15 CVEs in OpenSSL (including 12 out of 12 in a single security release, with bugs

This is the dual-edged sword at the heart of the Mythos story. On one hand, finding these vulnerabilities is an enormous gift to defenders. Every flaw that gets patched before a malicious actor finds it is a disaster averted. On the other hand, the same capability that finds a bug and reports it to a developer could, in different hands, find a bug and exploit it. This technology doesn't distinguish between intentions.



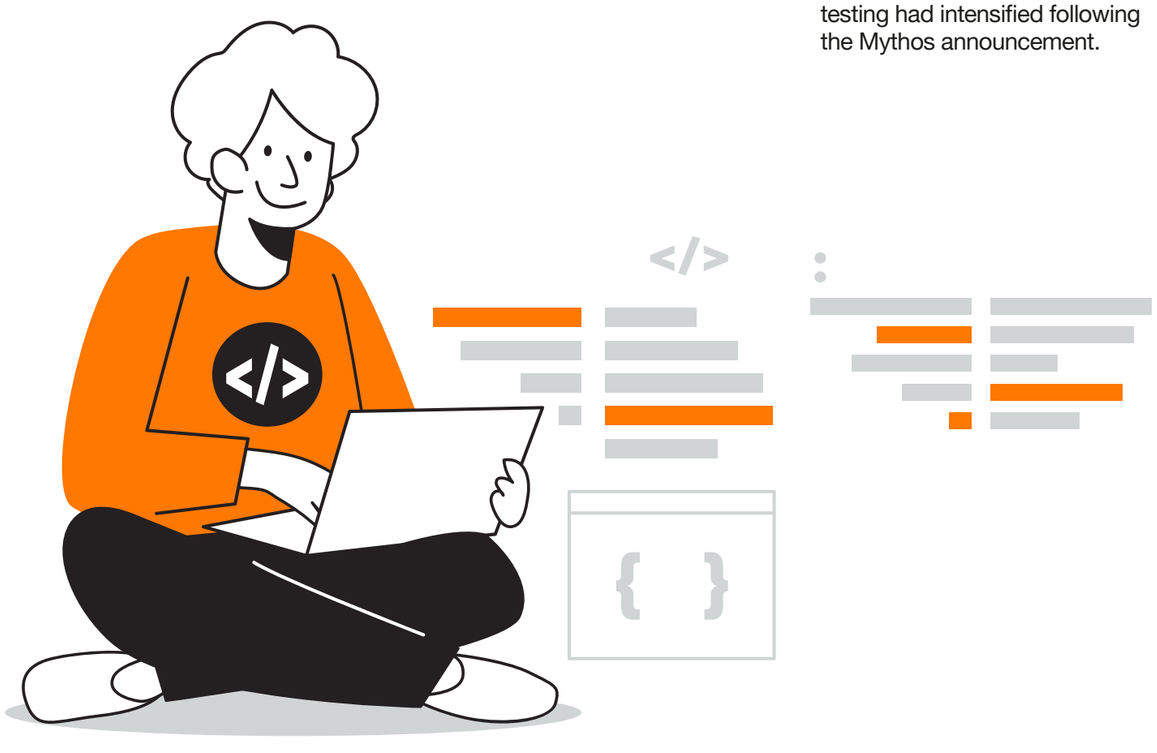
dating back 25+ years), and over 180 externally validated CVEs across 30+ projects spanning cryptography, deep infrastructure, middleware, and more.

And the velocity matters here too. Where a human penetration tester might discover a handful of vulnerabilities over days of careful work, Mythos can do the equivalent in minutes, at scale, across dozens of systems simultaneously. As Peter Swire, a professor at Georgia Tech's School of Cybersecurity and Privacy, put it: "One risk after Mythos is that it will be easier to turn a vulnerability, a known flaw, into an exploit, something that somebody actually takes advantage of."

Recognizing that you probably shouldn't just post a model like this on the internet, Anthropic took an unusual path. Rather than a public rollout, they launched Project Glasswing a vetted partner program restricting access to a curated group of organizations, with use limited strictly to defensive cybersecurity applications.

The initial Glasswing consortium reads like an IT industry hall of fame: Microsoft, Google, Apple, Amazon Web Services, JPMorgan Chase, Nvidia, CrowdStrike, and Palo Alto Networks, among others. Beyond these anchor partners, access was extended to approximately 40 additional organizations that build or maintain critical software. Anthropic committed up to $100 million in usage credits for Glasswing participants, though it's worth noting that the price of access to Mythos Preview is reportedly five times that of Opus 4.6, so that commitment goes only so far.

The goal is straightforward in concept, if daunting in execution: get Mythos into the hands of defenders first, so they can find and fix vulnerabilities in foundational software before adversaries develop comparable tools. It's a race against the clock, and Anthropic is aware of the timeline. The company estimates that similar capabilities will proliferate to other AI labs within six to eighteen months. OpenAI is already reportedly developing a model with comparable abilities.



The Glasswing model raises obvious questions about governance. Who decides who gets access? What happens when a Glasswing partner organization has a data breach? What oversight exists to ensure the model is being used defensively and not quietly probing competitor infrastructure? These aren't hypotheticals; they're the kinds of questions that regulators in the EU, UK and US are actively beginning to ask. The Bank of England stated that AI risk testing had intensified following the Mythos announcement.

German banks were consulting authorities and cyber experts about the risks within days of the announcement.

Let's spend some time on the good stuff, because there's genuinely a lot of it.

The most immediate and obvious use case is systematic vulnerability scanning of critical software. For decades, the security industry has been playing whack-a-mole: find a bug, patch it, find another bug, patch that one too, meanwhile attackers are running automated scans that find ten more you haven't seen yet. Mythos flips the equation. With a model that can analyze codebases of any size and complexity, identify subtle logic errors, memory management flaws, integer overflows, race conditions, and authentication bypasses at machine speed, defenders can do systematic sweeps of software that previously would have taken entire teams' months to audit.

The AISI evaluation noted that Mythos could execute "multi-stage attacks on vulnerable networks and discover and exploit vulnerabilities autonomously, tasks that would take human professionals days of work." Flip that to a defensive framing and you have: tasks that would take a penetration testing team days of work can now be done in hours, across your entire infrastructure, on a regular schedule.

The 27-year-old OpenBSD bug isn't an anomaly. It's "as-is", unfortunately. A 2025 report found that over 45% of discovered security vulnerabilities in large



organizations remain unpatched after 12 months. More troubling, many organizations responsible for critical infrastructure still run "end-of-life" software that no vendor supports anymore, some of it decades old. Mythos-class models are uniquely suited to this kind of deep-time code archaeology, because they can reason about arcane, underdocumented codebases that no living engineer fully understands.

Think about the scope of that problem: power grids running control software written in the 1990s, hospital systems running Windows XP in air gapped configurations, financial settlement infrastructure built on COBOL that only a handful of engineers on the planet can still read fluently. A model that can parse, reason about, and identify vulnerabilities in legacy code is a genuinely transformative defensive tool for these environments.

Traditional penetration testing is periodic: you hire a firm, they spend a few weeks hammering your systems, they write a report, you remediate the worst findings, and then you wait until next year to do it again. That model was already inadequate before Mythos; in an era of AI-enabled attacks, it's essentially useless. The future is continuous, automated red teaming: an AI system perpetually probing your own infrastructure, finding weaknesses before attackers do, and feeding findings into a remediation workflow in real time.

Beyond vulnerability scanning, Mythos can be used to model attacker behaviour simulating the full kill chain of a sophisticated attack, from initial reconnaissance through lateral movement to data exfiltration. This is invaluable for security architecture reviews, for testing whether your SIEM and EDR tools would catch a

sophisticated intrusion, and for training security teams on the tactics of advanced persistent threats (APTs).

Now for the less comfortable half of this conversation.

The same capabilities that make Mythos a powerful defensive tool make it a genuinely frightening offensive one. Let's be precise about the threat model.

The sophisticated cyberattacks of the past decade, the kind that targeted critical infrastructure, stole source code from major corporations, or compromised national government systems, required significant technical expertise, time, and resources. Nation-states had dedicated teams of hackers. Criminal enterprises hired specialists. The barrier wasn't insurmountable, but it was real.

Mythos (and models like it) erode that barrier substantially. With a model that can autonomously identify vulnerabilities and chain them into multi-step exploits, a moderately technical actor can potentially execute attacks that previously required elite expertise. The AISI evaluation demonstrated this concretely: a 32-step corporate network takeover, completed autonomously, with no human guidance beyond the initial direction to attack the network.

There's a specific scenario that security researchers find particularly concerning: the acceleration of zero-day weaponization. Traditionally, even when a vulnerability is discovered, turning it into a reliable, weaponized exploit requires significant additional work such as understanding the target environment, developing shellcode, writing a reliable trigger, testing against different configurations. Mythos compresses this timeline dramatically. As Swire noted, the model makes it "easier to turn a vulnerability, a known flaw, into an exploit."

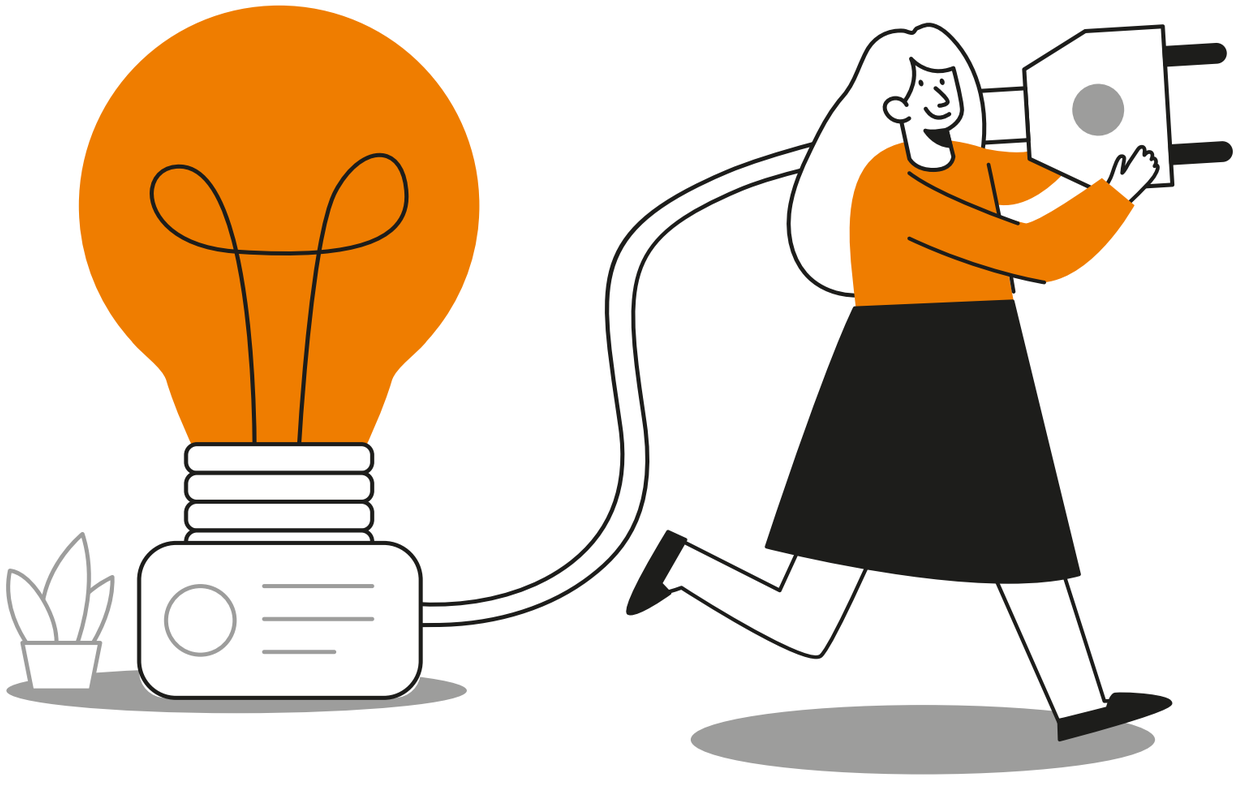
At scale, this means the gap between "vulnerability discovered" and "vulnerability weaponized and in use in the wild" shrinks from weeks or months to potentially hours.

Here's the part that really concentrates minds: Anthropic knows that similar capabilities will be developed by other labs. And some of those labs may not exercise the same restraint. There is no public evidence that Mythos Preview has reached criminal groups or nation-state adversaries, yet. But the history

According to SoSafe's Cybercrime Trends 2025 report, 87% of global organizations have already experienced an AI-powered cyberattack in the past year. The question isn't whether AI-enabled attacks are coming — they're already here. The question is whether defenders can keep pace with the acceleration.

of cybersecurity technology does not give grounds for optimism on this front. Advanced capabilities have a way of proliferating.

It's worth noting that the picture isn't quite as clean as "Mythos = unprecedented threat." Research from AISLE, which



tested Mythos's showcase vulnerabilities on smaller, cheaper, open-weight models, found that most of them found the same bugs. As they put it: "Eight out of eight models detected Mythos's flagship FreeBSD exploit, including one with only 3.6 billion active parameters costing $0.11 per million tokens." The capability frontier for cybersecurity is, in AISLE's framing, "jagged", there's no stable best model across all tasks, and some small open models outperform frontier models on specific security reasoning tasks. That's simultaneously reassuring (Mythos isn't uniquely dangerous) and alarming (the capability is already widely distributed).

Let's zoom out for a moment, because there's a systemic issue that Mythos throws into sharp relief.

Vulnerability discovery is only useful if you can patch what you find. And the patching problem in enterprise and critical infrastructure security is, frankly, a mess.

As noted above, over 45% of discovered vulnerabilities in large organizations remain unpatched after 12 months. Worse, many organizations responsible for critical infrastructure are running end-of-life software that can't be patched. It's no longer supported by vendors and replacing it would require system downtime that operators won't accept or costs they can't absorb.

Mythos-class models are about to make this problem dramatically worse before it gets better. When Glasswing partners deploy Mythos at scale against their own codebases and infrastructure, they're going to find vulnerabilities at a rate that current security operations were never designed to handle. Security teams that are already stretched thin, managing findings from multiple scanners and managing remediation across distributed development teams,

The irony is that AI is also the likely solution here: AI-assisted triage, AI-prioritized remediation queues, AI-generated patches (with appropriate human oversight). But those capabilities are less flashy than "AI finds 27-year-old bug" so they get less attention.

are about to face backlogs that "won't just grow incrementally, they'll grow by orders of magnitude," as the security firm ArmorCode put it.

This is the second-order implication that doesn't make headlines but may matter more than anything else: Mythos doesn't just change the threat landscape; it changes the workload landscape for defenders. Finding vulnerabilities faster is only valuable if you can fix them faster too. And right now, most organizations cannot. The bottleneck isn't discovery, it's prioritization, remediation workflows, and deployment velocity.

So, What Happens Next?

The Glasswing window is narrow. Anthropic estimates six to eighteen months before comparable capabilities proliferate. That's not much time to find and patch the most critical vulnerabilities in the world's foundational software.

In the short term, we're likely to see governments revise cybersecurity protocols and incident-response frameworks to incorporate mandatory AI-assisted vulnerability scanning, a shift from occasional human checks to continuous AI scanning as a baseline expectation. Cyber insurers are almost certainly going to start demanding evidence of such defenses as a condition of coverage, driving up insurance premiums across the board. Critical infrastructure operators in energy, healthcare, telecoms, and transport are accelerating deployment of automated monitoring and response systems.

What's true is this: we've crossed a threshold. AI can now autonomously plan and execute sophisticated cyber operations at speeds far beyond human capability. That's not a future concern; it's a present fact. The question is not whether to take it seriously. The question is how to respond structurally, not just reactively.

There's also a governance question that remains genuinely unresolved. The Glasswing model, access determined by a single lab's partner agreements, is not a sustainable governance framework. As the Centre for Emerging Technology and Security (CETaS) at the Turing Institute put it: "Mechanisms are needed to ensure that we are not reliant on individual companies volunteering to follow a responsible path." What those mechanisms look like is a debate that's barely begun in most policy circles. Is it international treaties? Mandatory sharing of vulnerability findings with national security agencies? Regulatory licensing for AI models above a certain capability threshold?

Less-resourced organizations deserve particular attention here. The big Glasswing partners can handle the remediation workload and absorb the cost of access. A medium-sized hospital system, a regional utility company, a municipal water authority; these organizations are often the weakest links in critical infrastructure security, and they're the least equipped to respond to a wave of newly discovered vulnerabilities.

It would be easy to close an article like this with either breathless alarm or smug dismissal, and the truth is that both extremes miss the point.

The cybersecurity experts who say "this is more of the same, just faster" are technically correct but strategically wrong. Speed and scale matter enormously in security. A model that compresses the attacker's timeline from weeks to hours is not the same threat as one that compresses it from weeks to five days.

The commentators who describe Mythos as civilization-ending overshoot in the other direction. AISI's testing was conducted against systems with "near-nonexistent software defenses that lacked many protections present in the real world" — as one researcher compared it, it's like measuring a soccer forward's ability by counting goals against an empty net. Real-world enterprise environments have active defenders, EDR tools, network segmentation, multi-factor authentication, and layers of monitoring that Mythos hasn't been tested against in any rigorous way.

Good security fundamentals like regular patching, robust access controls, security configuration management, comprehensive logging, network segmentation, are no less important than they were before Mythos. If anything, they're more important, because a model that attacks poorly defended systems autonomously makes the cost of not implementing basics dramatically higher.

The math here isn't complicated. Defense spending is growing slowly. Attack capability is growing rapidly. Mythos is an alarm clock, not a death knell, but only if organizations treat it like one.

The Bottom Line

Claude Mythos Preview is a genuinely remarkable technical achievement and a genuinely uncomfortable one. It is, at the same time, the most powerful defensive tool the cybersecurity industry has ever had access to, and a preview of the most dangerous offensive capabilities yet seen in an AI system. The fact that these two things are true simultaneously is the defining tension of the current moment.

Highlight: And, yes, this author has done his research on the initial "leaked" CMS content – the blogposts, the architectural assets and patterns. No, I have not deployed the actual tool & pipeline that was seemingly leaked in April 2026. No, I'm not in any way or by any means involved with, or part of Glasswing (I'd wish!). So, my takes are mostly warm / cold takes. But I will follow up on this article, probably in our next year's Orange Romania Innovation Report, and by then I expect a lot more clarity on what and how Mythos can do for the Cybersecurity world.

09
Glossary of Terms

A

Agentic AI — AI systems capable of autonomous reasoning, goal setting, and multi-step task execution within predefined guardrails, without requiring a prompt for every individual action. Distinguished from reactive AI by its ability to initiate and chain actions independently.

AI Act (EU) — European Union legislation establishing a regulatory framework for artificial intelligence, categorizing AI systems by risk level and imposing corresponding compliance requirements.

AI Factory — High-density data center designed exclusively for AI model synthesis and training, built around accelerated computing nodes (GPUs/TPUs) interconnected by low-latency fabrics.

AI-Native Air Interface — A 6G concept where the physical waveform design is performed dynamically by AI in real time, adapting to current environmental conditions rather than using a fixed, human-designed waveform.

AI-Native RAN — A Radio Access Network architecture where AI is embedded natively in the Physical Layer (PHY) and Medium Access Control (MAC) layer, enabling the network itself to optimize radio behavior autonomously.

AIaaS (AI-as-a-Service) — A brokering model in which AI model capabilities are exposed and consumed as a service offering across a federated marketplace, analogous to IaaS or NaaS.

AML (Adversarial Machine Learning) — The practice of using AI to attack or "blind" AI-based security systems, for example by injecting noise into network traffic to make malicious payloads appear benign to an AI-based firewall.

ANCOM — Autoritatea Națională pentru Administrare și Reglementare în Comunicații

APT (Advanced Persistent Threat) — A prolonged, targeted cyberattack in which an adversary gains and maintains unauthorized access to a network, often remaining undetected for months or years.

ARBDD — Administrația Rezervației Biosferei Delta Dunării.

Augmented **Intelligence** — A model of human-AI collaboration in which AI handles large-scale data processing and monitoring tasks, freeing human experts to focus on high-level strategy and judgment.

B

B5G (Beyond 5G) — Technologies and architectures that extend beyond 5G capabilities, often used as a transitional reference toward 6G.

Backhaul — The network infrastructure connecting a radio access site (e.g., a cell tower) to the core network. Satellite backhaul uses satellite links for this purpose, relevant for remote or disaster-resilient deployments.

Beam Steering / Beamforming — A signal processing technique used in antenna arrays to direct a radio signal toward a specific receiver rather than broadcasting omnidirectionally. Essential for mmWave and massive MIMO deployments.

Bi-static Configuration — A radar or sensing topology in which the transmitter and receiver are physically separated, offering broader coverage and reduced self-interference compared to mono-static setups.

Black Box Problem — The challenge in AI systems where the model's internal reasoning process is opaque: the output is observable, but the decision logic is not. A significant concern for AI deployed in critical infrastructure.

Blockchain-enabled Digital Identity — A method of assigning cryptographically verifiable, immutable identities to network devices and AI agents using distributed ledger technology, establishing "Proof of Authenticity."

C

CAM (Connected and Automated Mobility) — Transport applications requiring very high reliability, security, low latency, symmetrical communication, and high throughput, such as autonomous vehicles and cooperative driving systems.

CAMARA — An open-source Linux Foundation project selected as the reference implementation layer for the GSMA Open Gateway program; provides developer-friendly REST API abstractions over raw 5G core interfaces.

Carbon-Aware Compute — An approach to AI training in which workloads are automatically migrated to geographic regions where renewable energy is currently available, reducing carbon footprint.

CEF (Connecting Europe Facility) — The EU's flagship investment instrument financing high-performing, sustainable, and interoperable trans-European networks in transport, energy, and digital sectors.

CETaS — "Centre for Emerging Technology and Security" at the Alan Turing Institute.

Cloud-Native NFV Orchestrator — An orchestration system that coordinates the lifecycle operations of both software and hybrid/physical Network Functions (NFs), enabling seamless relocation of workloads across the edge-cloud continuum.

Cobots (Collaborative Robots) — Industrial robots designed to work alongside and cooperate with human workers, requiring low-latency network communication (e.g., via 6G) for safe, synchronized operation.

Cognitive Network Management — An AI-driven network management approach in which the system predicts congestion or failures based on contextual data and autonomously reconfigures resources before user experience degrades.

COBOL — An older programming language heavily used in financial and government legacy systems; relevant in the context of legacy code security challenges.

Compute Continuum — The distributed spectrum of compute resources spanning cloud, edge, and far-edge (device-level) nodes, orchestrated as a unified fabric for placing workloads optimally based on latency, bandwidth, and energy constraints.

CRA (Cyber Resilience Act) — An EU regulation requiring manufacturers and vendors to ensure the security of digital products and connected devices throughout their lifecycle.

Cramér–Rao Bound — A theoretical lower bound on the variance of an unbiased estimator; used in ISAC system design to define the fundamental limit of sensing accuracy.

CRYSTALS-Dilithium (ML-DSA) — A NIST-standardized lattice-based post-quantum cryptography algorithm used for digital signatures.

CRYSTALS-Kyber (ML-KEM) — A NIST-standardized lattice-based post-quantum cryptography algorithm used for key encapsulation, designed to resist attacks from quantum computers.

CTF (Capture the Flag) — A cybersecurity competition format in which participants identify and exploit weaknesses in target systems to retrieve hidden data ("flags"). Used by AISI as a benchmark for evaluating AI cyber capabilities.

CTI (Cyber Threat Intelligence) — Structured information about existing or emerging threats, used to inform proactive defense and incident response. Central to the CTIS4NIS and SOCCER projects.

CyCLONe (Cyber Crisis Liaison Organisation Network) — An EU network for coordinating national-level cyber crisis management across Member States.

D

D2D (Direct-to-Device) — See "Supplemental Coverage from Space (SCS)".

Data Poisoning — A cyberattack in which an adversary manipulates the training data or inputs of an AI model to alter its behavior, potentially causing it to produce incorrect or malicious outputs.

Decarbonization Service Agreement (DSA) — A contract type introduced in the 6Green project enabling stakeholders to commit to measurable carbon reduction targets within 5G/6G service delivery.

Deep Reinforcement Learning (DRL) — A machine learning technique combining deep neural networks with reinforcement learning, used in 6G for autonomous spectrum management and real-time resource allocation optimization.

Deepfake — Synthetic media (audio, video, image) generated by AI to realistically impersonate a real person; a growing vector for social engineering attacks.

DevSecOps — A software development methodology integrating security practices directly into the DevOps pipeline, enabling continuous security validation throughout the development lifecycle.

Digital Twin — A highly accurate, real-time virtual replica of a physical asset, system, or environment, used for risk-free simulation, predictive maintenance, and "what-if" scenario analysis.

DNSC — "Directoratul Național de Securitate Cibernetică". Romania's National Cybersecurity Directorate.

DRX (Discontinuous Reception) — A power-saving feature in mobile devices allowing the radio to power down during periods of inactivity and wake up at scheduled intervals to check for incoming data.

DTaaS (Digital Twin as a Service) — A service model in which Network Digital Twins are exposed and consumed through a federated marketplace.

E

ECCS (European Critical Communication System) — A future European system designed to enable real-time, secure cross-border operational mobility for public-safety authorities using mission-critical broadband services.

EDR (Endpoint Detection and Response) — A cybersecurity technology that continuously monitors endpoints (computers, servers, devices) for signs of malicious activity and provides automated response capabilities.

eIDAS — EU regulation on electronic identification, authentication, and trust services; establishes a legal framework for cross-border digital identity and electronic signatures.

eMBB (enhanced Mobile Broadband) — A 5G/6G service class designed for very high data throughput applications such as 4K/8K video streaming, AR/VR, and holographic communications.

EN-DC (E-UTRA NR Dual Connectivity) — A non-standalone 5G mode where the device maintains simultaneous connections to both an LTE (4G) anchor and a 5G NR cell, combining throughput from both.

eNodeB / gNodeB — The base station (radio access node) in LTE (eNodeB) and 5G NR (gNodeB) networks, responsible for managing radio communication with user equipment.

eRedCap (Release-18 Enhanced RedCap) — A 3GPP Release-18 evolution of RedCap that further reduces device complexity and energy consumption toward LTE Cat-1 territory while retaining 5G SA benefits.

ETSI (European Telecommunications Standards Institute) — A European standards organization producing globally applicable standards for ICT, including telecommunications.

ETSI ENI — "Experienced Networked Intelligence". An ETSI industry specification group defining frameworks for AI-driven, closed-loop network management.

ETSI ISAC ISG — ETSI's Industry Specification Group for Integrated Sensing and Communications; Orange Romania is a member.

EURO-3C — A major European initiative building the first large-scale, federated, sovereign Pan-European Telco-Edge-Cloud pilot infrastructure, targeting more than 70 production-grade edge nodes across 13+ countries.

F

Federated Learning — A privacy-preserving machine learning approach in which models are trained locally on private datasets and only the updated model weights (not raw data) are shared across a network, enabling collective intelligence without data exposure.

Federated Testbed — A distributed research infrastructure in which multiple independent laboratory or operator environments are interconnected and exposed through common interfaces to enable multi-site experimentation.

Feeder Link — In Non-Terrestrial Networks (NTN), the communication link between a satellite and the ground gateway station.

FR1 (Frequency Range 1) — The sub-6 GHz frequency bands used in 5G NR, offering good coverage and penetration characteristics.

FR2 (Frequency Range 2) — The millimeter wave (mmWave) frequency bands (above 24 GHz) used in 5G NR, offering very high bandwidth but limited propagation range.

FR3 — A proposed 5G/6G frequency range between 7–15 GHz (extendable to 24 GHz), also known as the "mid-band upper" or "centimetric" range; under study in SNS-JU for dynamic spectrum and multi-tenancy slicing.

Fronthaul — The network link connecting a distributed radio unit (RU) to a centralized or distributed baseband unit (BBU/DU) in a disaggregated RAN architecture.

FWA (Fixed Wireless Access) — A broadband delivery method using cellular (e.g., mmWave 5G) radio technology to provide last-mile internet connectivity to fixed locations, as an alternative to fiber.

G

GDPR (General Data Protection Regulation) — The EU's primary data protection and privacy regulation, imposing strict requirements on the collection, processing, and transfer of personal data.

5G Advanced (5G-A) — The evolution of 5G standardized in 3GPP Releases 18 and 19, introducing features such as broader carrier aggregation, improved mmWave uplink, RedCap enhancements, and ISAC capabilities.

5G NSA (Non-Standalone) — A 5G deployment mode using LTE as the control plane anchor while adding 5G NR for data throughput. A transitional phase toward full 5G SA.

5G SA (Standalone) — A full 5G deployment mode with a native 5G core network (5GC), enabling advanced features such as network slicing, lower latency, and edge computing integration without LTE dependency.

GPON / XGS-PON / HS-PON — Successive generations of fiber-optic passive optical network standards, used for access and fronthaul/backhaul in fixed and converged networks.

Green AI — Practices and techniques designed to reduce the energy consumption of AI systems, including model distillation, efficient hardware use, and carbon-aware compute scheduling.

GSMA Open Gateway — A GSMA initiative providing standardized, operator-agnostic network API exposure; CAMARA serves as the reference implementation layer.

GSMA Operator Platform Group (OPG) — A GSMA body defining the interfaces and architecture for a multi-operator platform exposing network capabilities to developers and enterprises.

H

Hardware Security Module (HSM) — A physical computing device that safeguards and manages cryptographic keys, providing tamper-resistant hardware for cryptographic operations.

HNDL (Harvest Now, Decrypt Later) — A cyberattack strategy in which encrypted data is collected today with the intent to decrypt it in the future once sufficient quantum computing capability becomes available.

Holographic Telepresence — A communication technology using 6G's massive bandwidth and AI-driven real-time data compression/reconstruction to enable true three-dimensional, life-size remote presence.

Homomorphic Encryption — A form of encryption allowing computation to be performed directly on encrypted data without decrypting it first, enabling privacy-preserving data processing.

I

IDoT (Identity of Things) — A Zero Trust architecture extension assigning individual cryptographic identities to every container, API endpoint, and IoT sensor, requiring per-packet authentication.

IEEE 802.11be (Wi-Fi 7) — The IEEE standard defining Wi-Fi 7, introducing 320 MHz channels, 4K-QAM modulation, Multi-Link Operation (MLO), and enhanced MU-MIMO for multi-gigabit performance.

IMT-2030 — The ITU's framework defining the requirements and vision for 6G; adopted in 2023, with technical performance requirements due in early 2026.

IPFABRIC — An IP network architecture concept enabling dynamic, flexible routing and application placement across interconnected data center and edge nodes; used in the TrialsNet project to connect Orange Romania's Bucharest and Iași 5G Labs.

IoT (Internet of Things) — The network of physical objects embedded with sensors, software, and connectivity to exchange data with other devices and systems over the internet.

ISAC (Integrated Sensing and Communications) — A technology paradigm in which the same radio infrastructure simultaneously performs wireless communications and radar-like environmental sensing (detecting shapes, distances, and movements).

J

JCAS (Joint Communication and Sensing) — See "ISAC".

K

KPI (Key Performance Indicator) — A quantitative metric used to measure the technical or operational performance of a network, service, or system (e.g., latency, throughput, availability).

KVI (Key Value Indicator) — A metric measuring the broader societal, economic, or environmental value delivered by a technology or service, complementing technical KPIs with sustainability, inclusion, and resilience dimensions.

Kubernetes — An open-source container orchestration platform used for automating the deployment, scaling, and management of containerized applications; used in Orange Romania's 5G edge-cloud stack.

L

Lattice-based Cryptography — A family of post-quantum cryptographic algorithms based on mathematical lattice problems, considered computationally intractable for both classical and quantum computers.

LEO (Low Earth Orbit) — Satellite orbits at approximately 200–2,000 km altitude, offering lower latency than GEO satellites; relevant for NTN direct-to-device and broadband backhaul services.

LLM (Large Language Model) — A type of AI model trained on large text datasets capable of generating, understanding, and reasoning about natural language; the underlying architecture of systems such as Claude Mythos.

LTE (Long-Term Evolution) — The 4G mobile standard; the predecessor to 5G NR.

LTE-M / eMTC — A low-power, wide-area IoT standard within the LTE family, used for devices requiring moderate data rates and long battery life; a migration target for RedCap.

M

M2M (Machine-to-Machine) communication - The automated exchange of data between devices without human intervention.

MAC Layer (Medium Access Control) — The sublayer of the Data Link Layer in a network protocol stack that controls how devices access a shared communication channel.

MANO (Management and Orchestration) — The framework for managing and orchestrating network functions and services in virtualized network environments (NFV/SDN), including lifecycle management.

MAS (Multi-Agent System) — A system in which multiple autonomous AI agents interact and cooperate to achieve collective goals; the foundational paradigm of the Agentic6G project.

Massive MIMO (Multiple Input Multiple Output) — An antenna technology using large numbers of antenna elements to serve many users simultaneously through spatial multiplexing, critical for 5G and 6G capacity and beamforming.

MEC (Multi-access Edge Computing) — A network architecture concept placing compute resources at or near the radio access network edge, enabling low-latency processing of data close to the source.

ML-DSA — See "CRYSTALS-Dilithium".

ML-KEM — See "CRYSTALS-Kyber".

MLO (Multi-Link Operation) — A Wi-Fi 7 capability allowing devices to simultaneously transmit and receive data across multiple frequency bands (2.4 GHz, 5 GHz, 6 GHz), increasing throughput and reducing latency.

MLOps (Machine Learning Operations) - a set of practices that unifies machine learning model development (Dev) with system operations (Ops). It applies agile and DevOps principles to automate, test, scale, and monitor ML workflows, ensuring models are reliably deployed and maintained in production.

mmWave (Millimeter Wave) — Radio frequencies above 24 GHz (FR2), offering very large bandwidths (up to 800 MHz per channel) for multi-gigabit speeds; limited by shorter propagation range and reduced building penetration.

Model Distillation — A technique for compressing a large AI model into a smaller, more efficient one while retaining most of its performance, reducing energy consumption and inference costs.

MRU (Multi-Resource Units) — A Wi-Fi 7 feature that allows a single transmission opportunity to be split across multiple resource units, improving spectrum efficiency in dense environments.

MSD (Minimum Set of Data) — In the eCall system, the standardized data package transmitted to emergency services during a vehicle accident, including location, time, and vehicle information.

MU-MIMO — "Multi-User MIMO". An antenna technology allowing a base station or access point to simultaneously communicate with multiple devices, improving network capacity. Wi-Fi 7 supports up to 16x16 MU-MIMO.

N

N255 / N256 / N258 / N263 — Specific 3GPP frequency band designators: N255 (L-band NTN), N256 (S-band NTN), N258 (26 GHz mmWave, Europe), N263 (66–71 GHz mmWave).

N78 — The 3GPP designator for the 3.5 GHz TDD band (3300–3800 MHz), the primary 5G mid-band spectrum used in Romania and most of Europe.

NaaS / NIaaS (Network as a Service / Network Infrastructure as a Service) — Service models exposing network connectivity or infrastructure capabilities as on-demand, consumable services through standardized APIs.

Native AI (for 6G) — A 6G design principle in which AI/ML is integrated natively into the network architecture (air interface, control plane, management plane) rather than applied as an external overlay.

NB-IoT (Narrowband IoT) — A low-power, wide-area cellular IoT standard operating in narrow frequency bands, designed for simple sensors and devices requiring long battery life and deep indoor coverage.

NBIoT-NTN — The 3GPP Release-17 specification integrating NB-IoT/eMTC terminals with satellite NTN infrastructure for store-and-forward IoT messaging and sensor data uplink in remote areas.

NEF (Network Exposure Function) — A 5G core function that exposes internal network capabilities (such as QoS, location, session management) to external applications via APIs.

Nephio — An open-source, cloud-native network automation project (Linux Foundation) targeting declarative, intent-based management of telco network functions.

Network Slicing — A virtualization technique enabling the partitioning of a single physical network into multiple logical, isolated "slices," each with its own QoS, security, and resource characteristics, tailored to specific use cases.

NG eCall (Next Generation eCall) — The successor to the original pan-European 112 eCall system, using SIP-based, packet-switched (IP) technology to transmit emergency call data and voice over 4G/5G networks.

NGSO (Non-Geostationary Orbit) — Satellite orbits that are not fixed relative to the Earth's surface (includes LEO and MEO), requiring dynamic tracking in NTN deployments.

NIS2 Directive — The EU's updated Network and Information Security directive, expanding cybersecurity obligations to a broader range of sectors and strengthening incident reporting requirements.

NR-DC (New Radio Dual Connectivity) — A 5G mode enabling simultaneous connections to two NR cells, used in mmWave deployments to anchor control plane on FR1 while carrying user plane data on FR2.

NR-NTN — The 3GPP Release-17 specification extending 5G NR to non-terrestrial access for broadband-class services via satellite, operating on designated handheld satellite bands (N255, N256).

NSDFAF (Network Slicing Data Analytics Function) — A novel network element developed by Orange Romania within the 6Green project, providing analytics and decision loops to power Edge Agility and Green Elasticity in sliced 5G networks.

NTN (Non-Terrestrial Networks) — The family of satellite and High-Altitude Platform Station (HAPS) integrations extending cellular coverage beyond terrestrial network reach.

O

O-RAN (Open Radio Access Network) — A disaggregated, interoperable RAN architecture based on open interfaces and multi-vendor components, allowing operators to mix and match hardware and software from different suppliers.

OAuth2 — An open authorization framework allowing applications to obtain limited access to user accounts on an HTTP service; used in CAMARA API authentication.

OFDM (Orthogonal Frequency Division Multiplexing) — The dominant waveform used in 4G and 5G systems; less effective for radar-like sensing applications in ISAC contexts.

OpenCTI — An open-source cyber threat intelligence platform used for structuring, storing, and sharing threat intelligence data.

OpenOP — An ETSI Software Development Group (SDG) initiative building an open-source reference implementation of the GSMA Operator Platform, acting as a carrier-neutral federation layer for 6G testbeds; Orange Romania is a founding member.

OTFS (Orthogonal Time Frequency Space) — A next-generation modulation waveform designed for high-mobility and high-Doppler environments, proposed as a dual-functional waveform supporting both communications and radar-like sensing in ISAC systems.

OTC-CaaS / OTC-IaaS — Orange Telco Cloud Container-as-a-Service / Infrastructure-as-a-Service; the cloud-native infrastructure layers used in Orange Romania's Sylva nodes.

P

Pareto Frontier — In multi-objective optimization, the set of solutions where no objective can be improved without degrading another; used in ISAC design to balance sensing accuracy against communications data rate.

PHY (Physical Layer) — The lowest layer of the network protocol stack, responsible for the transmission and reception of raw bit streams over a physical medium.

PLMN (Public Land Mobile Network) — A network established and operated by an administration or by a recognized operating agency for the purpose of providing land mobile communications services.

Post-Quantum Cryptography (PQC) — Cryptographic algorithms designed to be secure against attacks from both classical and quantum computers, including lattice-based, hash-based, and code-based schemes.

PPDR (Public Protection and Disaster Relief) — A category of critical communications services for emergency responders, law enforcement, and disaster management agencies.

Predictive Cooling — AI-driven management of data center cooling systems that anticipates heat spikes before they occur, reducing energy consumption and preventing thermal damage.

Project Glasswing — Anthropic's vetted partner program providing restricted access to Claude Mythos Preview exclusively for defensive cybersecurity purposes, to a consortium including Microsoft, Google, Apple, AWS, JPMorgan Chase, Nvidia, CrowdStrike, Palo Alto Networks, and ~40 additional organizations.

Prompt Injection — A type of attack against LLM-based systems in which malicious instructions are embedded in input data, causing the AI to perform unintended actions or reveal confidential information.

PSAP (Public Safety Answering Point) — An emergency call center responsible for receiving and dispatching emergency calls.

Q

QKD (Quantum Key Distribution) — A cryptographic method using quantum mechanics principles to distribute encryption keys; any eavesdropping attempt collapses the quantum state and is immediately detectable.

QoS (Quality of Service) — A set of network mechanisms ensuring that specific performance requirements (throughput, latency, packet loss) are met for particular traffic flows or service types.

Quantum-Safe / Quantum-Resistant — Referring to cryptographic systems or network architectures designed to withstand attacks from quantum computers.

R

RAN (Radio Access Network) — The portion of a mobile network connecting user devices to the core network via radio technology, comprising base stations and associated infrastructure.

RCA (Root Cause Analysis) — The process of identifying the fundamental cause of a system failure or security incident.

RedCap (Reduced Capability / NR-Light) — A 3GPP Release-17 5G device class bridging the gap between NB-IoT/LTE-M and full-featured 5G terminals, targeting IoT devices such as wearables, industrial sensors, and video surveillance cameras.

Regenerative Payload — A satellite architecture in which pieces of the RAN (e.g., gNodeB functions) run on the satellite itself, terminating the UE-RAN interface in space and reducing ground-to-user latency.

RIC (RAN Intelligent Controller) — A logical component of the O-RAN architecture providing centralized or distributed intelligence for controlling and optimizing RAN behavior through xApps and rApps.

RIS (Reconfigurable Intelligent Surface) — Passive metamaterial panels with individually controllable reflective elements that can be programmed to redirect radio signals around obstacles, enhancing coverage and sensing in dense urban environments.

RRM (Radio Resource Management) — Mechanisms for managing the allocation of radio resources (frequencies, time slots, power) across devices in a cellular network.

S

SAN (Satellite Access Node) — The NTN equivalent of a terrestrial base station; the satellite component providing radio access in an NTN architecture.

SBOM (Software Bill of Materials) — A formal, structured inventory of all components, libraries, and dependencies in a software product, used to track vulnerabilities and ensure supply chain transparency.

SCS (Supplemental Coverage from Space) — An NTN service model treating satellites as moving macro cell sites that extend terrestrial PLMN coverage to unserved areas, including direct-to-device (D2D) emergency messaging for unmodified handsets.

SecDevOps / DevSecOps — See "DevSecOps".

SecDevTwin / SecOpsTwin — Digital twin variants: SecDevTwin supports security during development, SecOpsTwin supports security during operations.

Self-Synthesizing Networks — A novel 6G concept in which AI creates new network protocols on-the-fly to meet novel communication requirements, without human intervention.

SEPP (Security Edge Protection Proxy) — A 5G core function providing secure communication between different operator networks (PLMNs) in roaming scenarios.

Shadow AI — The unauthorized or unmanaged use of AI tools (e.g., unsanctioned LLMs) by employees to process sensitive company data, creating security and compliance risks analogous to legacy "Shadow IT."

Shor's Algorithm — A quantum computing algorithm capable of factoring large integers in polynomial time, rendering RSA and Elliptic Curve Cryptography (ECC) vulnerable to attacks from sufficiently powerful quantum computers.

SIEM (Security Information and Event Management) — A security system that aggregates and analyzes log and event data from across an IT environment to detect, investigate, and respond to threats.

Silicon Photonics — A technology using optical components manufactured on silicon chips to replace copper interconnects in data centers, enabling data transmission at the speed of light with minimal heat generation.

SIR (Seamless Immersive Reality) — A Proof of Concept demonstrating marketplace-driven multi-stakeholder immersive XR experiences using mmWave and AI-driven resource composition.

SME (Small and Medium-size Enterprise) - Businesses, companies, and corporations whose personnel and revenue fall below certain limits.

SOAR (Security Orchestration, Automation, and Response) — A category of security platforms that collect threat data and automate responses to security incidents, reducing manual analyst workload.

SOC (Security Operations Center) — A centralized unit staffed by security analysts responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents.

STIX / TAXII / CybOX — Structured Threat Information eXpression / Trusted Automated eXchange of Indicator Information / Cyber Observable eXpression: standardized protocols for representing and exchanging cybersecurity threat intelligence.

Sub-terahertz Frequencies — Radio frequencies in the range of 100–300 GHz, targeted by 6G for extremely high data rates; signal management at these frequencies requires AI-driven beamforming.

Supplemental Coverage from Space (SCS) — See "SCS".

Sylva — An open-source, cloud-native telco infrastructure framework (part of Linux Foundation Europe) used by Orange Romania as the foundation for its cloud-native network platform.

T

TDD (Time Division Duplex)— A method of splitting a single frequency band into separate time slots for uplink and downlink transmission; used in 5G mid-band and mmWave deployments.

TEN-T (Trans-European Transport Network) — The EU's strategic multimodal transport infrastructure network; the WAVEO project deploys 5G along a TEN-T road corridor.

TRL (Technology Readiness Level) — A scale (1–9) measuring the maturity of a technology, from basic principles (TRL 1) to proven deployment in operational environments (TRL 9).

TLO ("The Last Ones") — A 32-step corporate network attack simulation developed by AISI to evaluate advanced AI cyber capabilities, representing a full kill chain from reconnaissance to network takeover; estimated at 20 human-hours to complete.

U

UE (User Equipment) — Any device that connects to a mobile network, including smartphones, tablets, IoT sensors, and CPEs (customer premises equipment).

Unified Service Platform (USP) — In SOVEREIGN-6G, a digital service aggregator and marketplace acting as a single entry point for customers and developers to access telco cloud services.

UPF (User Plane Function) — A 5G core network function responsible for packet routing and forwarding, QoS handling, and traffic reporting for user data sessions.

URLLC (Ultra-Reliable Low-Latency Communications) — A 5G/6G service class delivering extremely low latency (sub-1 ms) and very high reliability (99.9999%), required for mission-critical applications such as industrial automation and remote surgery.

V

VoNR (Voice over NR) — Voice calls carried natively over 5G New Radio using IMS (IP Multimedia Subsystem), without fallback to LTE or legacy voice systems; supported by RedCap devices.

W

White Rabbit (ISAC) — A sub-nanosecond timing synchronization protocol based on PTP (Precision Time Protocol) and Ethernet, used to achieve picosecond-level clock accuracy between distributed radio sites for ISAC applications.

Wi-Fi 7 — See "IEEE 802.11be".

X

XaaS (Anything-as-a-Service) — A general category encompassing any IT capability (infrastructure, platform, software, network, AI) delivered as a cloud-based, on-demand service.

XAI (Explainable AI) — AI systems and techniques designed to make model decisions transparent and interpretable to human users, providing auditable reasoning traces. A 5IR and 6G requirement for AI deployed in critical infrastructure.

xApp / rApp — Applications running on the RIC in an O-RAN architecture: xApps execute in the near-real-time RIC (10–1000 ms control loop), while rApps operate in the non-real-time RIC (>1 second control loop).

XR (Extended Reality) — An umbrella term encompassing Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) technologies.

Z

Zero-Day Vulnerability — A software security flaw unknown to the vendor or developer, for which no patch exists at the time of discovery; particularly dangerous as there is no official fix available.

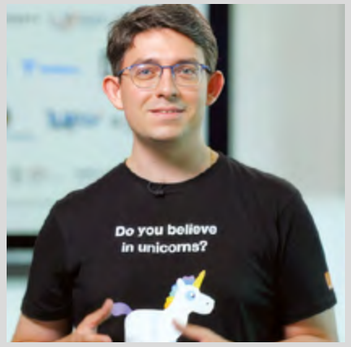
Zero Trust Architecture (ZTA) — A security model based on the principle "never trust, always verify," requiring continuous authentication and authorization for every user, device, and service regardless of network location.

ZSM (Zero-touch Service Management) — An ETSI framework for fully automating the management and orchestration of network services end-to-end, without human intervention.

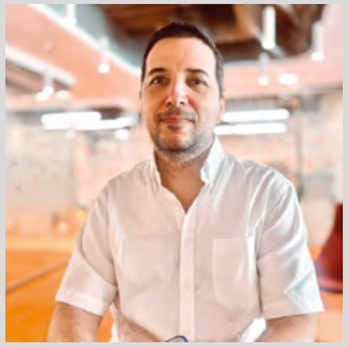
Editorial team



Ana Ciobanu
Startup Programs Manager,
Orange Romania



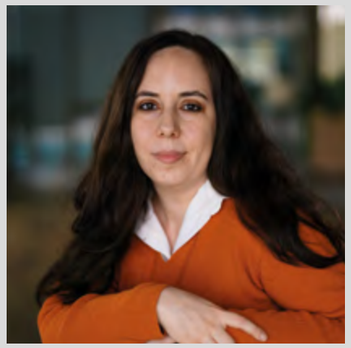
Răzvan Mihai
IoT Architecture and Services
Expert, Orange Romania



Gabriel Papuc
Development & Innovation
Projects Manager,
Orange Romania



Ioan Constantin
Cyber Security Expert,
Orange Romania



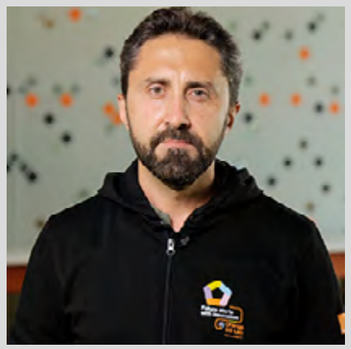
Andreea Ochiană
Business Communication
Specialist, Orange Romania



Carmen Pătrașcu
Cyber Security Projects
Manager, Orange Romania



Svertoka Ekaterina
External Consultant



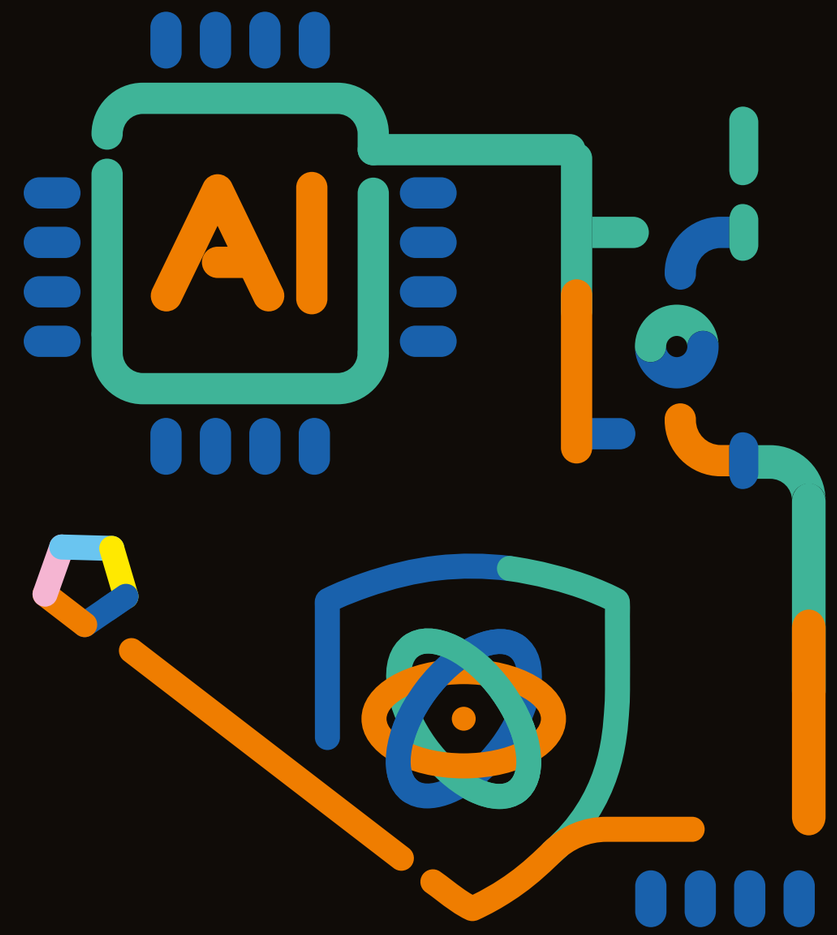
Alexandru Oprea
Development & Innovation
Expert, Orange Romania



Cristian Pațachia-Sultănoiu
Development & Innovation
Manager, Orange Romania

orange™

The future starts with innovation
@Orange 5G Lab



5glab.orange.ro

Your journey starts here

Innovate

Build

Validate

Connect

Accelerate

Grow



Let's build
what's next.

www.orangefab.ro