



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Policy-Making Dimensions for 5G Security

May 2026, Athens, Greece

Prepared by: Valentin Constantinescu - Advisor to the Director, The Romanian National Cyber Security Directorate

WHY 5G IS A POLICY CONCERN

From network technology to systemic dependency

Critical

5G now impacts healthcare, energy, transport, defence and public administration — the 'network of networks'.

Multi-vendor

Disaggregation (RAN/Core, virtualisation, O-RAN) widens the attack surface and shifts trust boundaries.

Cross-border

Roaming, slicing and supply chains make 5G risk a transnational problem — no Member State can secure it alone.



The implication for a National Cybersecurity Authority

5G security cannot be delegated to operators alone. It is a public-policy object that must be steered, supervised and continuously re-assessed by NCA.

Seven policy-making dimensions for an NCA

These dimensions map the levers a national cybersecurity authority can — and must — operate to discharge its mandate over 5G networks. They are interdependent: a gap in one weakens the others.



Strategic

Setting the national posture for 5G — sovereignty, resilience, EU alignment

What it covers

- Position 5G inside the National Cybersecurity Strategy as critical, cross-sector infrastructure.
- Translate the EU 5G Toolbox (TM01–TM11, SM01–SM07) into a national implementation roadmap.
- Define the posture on technological sovereignty — single-supplier dependency, open architectures, EU industrial base.
- Articulate how 5G security supports broader objectives: economic security, digital sovereignty, defence readiness.

NCA policy levers

- Issue / co-sign the National 5G Security Strategy
- Lead inter-ministerial coordination on 5G
- Publish national positions on Open RAN / O-RAN trust
- Define and review the high-risk-vendor framework

Anchor references

EU 5G Toolbox (NIS Cooperation Group, 01/2020) • Recommendation (EU) 2019/534 • National Cybersecurity Strategy • EU Critical Infrastructure protection regime

Regulatory

Translating strategy into binding obligations on operators and suppliers

What it covers

- Transposition and operationalisation of NIS2 (Directive (EU) 2022/2555) for the electronic-communications sector.
- Articulation with the European Electronic Communications Code (EECC, Art. 40–41) on security of networks and services.
- Set 5G-specific rules on architectural choices, vendor diversification, sensitive functions.
- Coherence with horizontal regulation — Cybersecurity Act, Cyber Resilience Act, GDPR, eIDAS2.
- Clear allocation of obligations across the value chain: MNOs, infrastructure providers, suppliers, MSPs.

NCA policy levers

- Draft and consult on secondary legislation
- Issue binding technical implementing acts
- Define security baselines (e.g. CyFun®-style)
- Coordinate with the NRA on telecom-specific rules

Anchor references

Directive (EU) 2022/2555 (NIS2) • Directive (EU) 2018/1972 (EECC) • Regulation (EU) 2019/881 (CSA) • Regulation (EU) 2024/2847 (CRA) • National transposition acts

Risk-based

Anchoring decisions in evidence — threats, vulnerabilities, supply-chain dependencies

What it covers

- National 5G risk assessment, kept current and aligned with the EU coordinated risk assessment.
- Sub-domain views: RAN, transport, core, MEC, OSS/BSS, network slicing, roaming.
- Supply-chain risk: country-of-origin profile, legal exposure of the supplier, lifecycle support, M&A risk.
- Concentration risk and resilience: dual sourcing, geographic distribution, exit strategies.
- Threat-led testing and red-teaming aligned with TIBER-EU principles where relevant.

NCA policy levers

- Maintain the national 5G risk methodology
- Designate / review high-risk vendors
- Mandate operator risk-management plans
- Trigger restrictions on sensitive functions

Anchor references

EU coordinated risk assessment of 5G networks (10/2019) • ENISA Threat Landscape for 5G • EU 5G Toolbox SM01–SM03 • Sector-specific risk methodologies (e.g. CyFun®)

Standards & Certification

Reducing trust costs through shared, verifiable assurance

What it covers

- 3GPP SCAS / SECAM is the technical foundation underpinning GSMA NESAS and the candidate EU5G NESAS-based scheme for 5G network products.
- EU 5G certification stack under construction by ENISA: a NESAS-based scheme for network products, EUCC (Common Criteria) for eUICCs and sensitive components.
- Radio Equipment Directive (RED Delegated Reg. 2022/30, EN 18031 series) sets cybersecurity essentials for 5G end-user devices from 1 Aug 2025 — superseded by the CRA on 11 Dec 2027.
- O-RAN-specific assurance gap: open interfaces (E2, A1, O1, O2), RIC, xApps and rApps are not yet fully covered by existing schemes — a key 5G-TACTIC contribution area.
- From paper to evidence: link certification outcomes to operational telemetry and repeatable testbed-based evaluation, the path the 5G-TACTIC Cybersecurity Toolbox operationalises.

NCA policy levers

- Position the NCA in ECCG and AHWG EU5G
- Recognise / mandate schemes via NIS2 acts
- Co-supervise RED 2022/30 with the NRA
- Fund national 5G evaluation labs (CABs)

Anchor references

Reg. (EU) 2019/881 (CSA) • EUCC scheme — Reg. (EU) 2024/482 • Candidate EU5G scheme (ENISA, under development) • RED 2014/53/EU + Delegated Reg. (EU) 2022/30 • EN 18031-1/-2/-3:2024 • Reg. (EU) 2024/2847 (CRA) • 3GPP TS 33.117/.216/.511–.527 (SCAS) • GSMA NESAS • O-RAN WG11

The EU 5G certification stack

Different layers of the 5G ecosystem are governed by different schemes. The NCA's job is to make this stack legible, recognised and supervised — and to drive uptake.

End-user devices • UE, CPE, IoT, gateways RED Delegated Reg. (EU) 2022/30 → EN 18031-1/-2/-3:2024 <i>Transitions to the Cyber Resilience Act (Reg. 2024/2847) on 11 Dec 2027.</i>	IN FORCE <i>since 1 Aug 2025</i>
Secure elements • eUICC / eSIM, smartcards, chips EUCC — Common Criteria-based scheme (Reg. (EU) 2024/482) <i>ENISA eUICC specifications under EUCC finalised in 2025 (no separate scheme).</i>	IN FORCE <i>operational</i>
5G network products • gNB, 5GC, MEC, OSS, transport Candidate EU5G scheme — NESAS-based, built on 3GPP SCAS + GSMA NESAS <i>Drafted by ENISA AHWG EU5G with ECCG, NCCAs and industry; not yet adopted.</i>	UNDER DEV. <i>in drafting</i>
Operator risk management • governance & supervision NIS2 (Dir. (EU) 2022/2555) + EECC Art. 41 + national lex specialis <i>Certification evidence feeds NIS2 supervisory practice — the policy bridge an NCA owns.</i>	IN FORCE <i>transposed</i>

 **Voluntary by default under the Cybersecurity Act** — Member States may make schemes binding via NIS2 implementing acts, sectoral regulation or supervisory practice.

Open RAN & virtualisation

Disaggregation, virtualisation and cloud-native operation widen the attack surface — and shift where assurance must be applied. Policy must follow the architecture.



O-RAN open interfaces

E2, A1, O1, O2 and Open Fronthaul become open trust boundaries. Multi-vendor integration disperses accountability and complicates root-cause analysis when something fails — assurance must be per-interface, not per-product.



RIC, xApps & rApps

Programmable RAN control with ML/AI introduces model poisoning, conflicting xApp policies, and a new supply chain of small specialised apps that the State has not previously had to vet.



Virtualised network functions

VNF/CNF lifecycle and image integrity, hypervisor and container hardening, SBOM and runtime attestation become first-class assurance concerns — not afterthoughts to a hardware certification.



Cloud platform & sovereignty

Telco cloud frequently runs on hyperscalers. Foreign control, data residency, network-slice isolation, MEC trust and OSS/BSS exposure raise policy questions that articulate with EUCS and EU sovereign-cloud work.



NCA implication — supervisory practice must follow the architecture: per-interface, per-VNF/CNF, per-slice. 5G-TACTIC WP3 (RAN/Core) and WP4 (supporting infrastructure & LCM) operationalise this.

Supervisory

Verifying that what is required is actually delivered — and acting when it is not

What it covers

- Risk-management measures: evidence-based supervision rather than self-attestation alone.
- Mandatory significant-incident notification (NIS2 timelines: 24h early warning, 72h, 1-month report).
- On-site and remote inspections, technical audits, security scans of operator infrastructure.
- Conformity assessments tied to certification outcomes and to the national high-risk-vendor framework.
- Graduated enforcement: binding instructions, administrative fines, and management-body accountability.

NCA policy levers

- Annual / multi-year supervisory programme
- Audit guidelines for the RAN/Core scopes
- Incident-handling SOPs with the national CSIRT
- Sanctioning powers and procedural safeguards

Anchor references

NIS2 Arts. 21, 23, 32–34, 36 • EECC Art. 41 • National sanctioning regime • ENISA technical guidelines on incident reporting

Cooperation

5G risk is transnational — so is the policy response

What it covers

- EU level: NIS Cooperation Group (5G work-stream), ENISA, CSIRTs Network, EU-CyCLONe.
- Operational cooperation: cross-border incident response, threat intelligence sharing, coordinated vulnerability disclosure.
- Industry dialogue: structured engagement with MNOs, vendors, integrators, hyperscalers, MSPs.
- Bilateral cooperation with peer NCAs and NRAs — especially on shared infrastructure (e.g. cross-border MORANs).
- Coordination with non-cyber authorities: NRA, data protection, defence, law enforcement, foreign-investment screening.

NCA policy levers

- Active mandate in NIS CG / CSIRTs Network
- MoUs with peer authorities
- Joint exercises (Cyber Europe, sector drills)
- Single national point of contact under NIS2

Anchor references

NIS2 Arts. 14–16 (NIS CG, CSIRTs Network, EU-CyCLONe) • ENISA mandate • Council Recommendation on coordinated response (Blueprint) • Bilateral / regional cooperation arrangements

Capacity Building & Innovation

Sustaining the policy over a decade — skills, ecosystem, and an industrial base

What it covers

- Build deep in-house RAN/Core expertise inside the NCA — not outsource technical judgement.
- Workforce pipeline: certifications, university partnerships, exchange programmes with operators and academia.
- Support the EU industrial base: O-RAN, open-source 5G stacks, EU SMEs, secure-by-design suppliers.
- Run national exercises and capacity-building activities for operators, suppliers and public-sector users.
- Bridge to research: feed pilot evidence (as in 5G-TACTIC) back into policy and supervisory practice.

NCA policy levers

- Sponsor / co-run training programmes
- Fund national 5G security testbeds
- Co-shape EU funding (DEP, Horizon, Chips Act)
- Engage in standards bodies on the State's behalf

Anchor references

5G-TACTIC WP6 (training) • EU Digital Europe Programme • Horizon Europe (Smart Networks & Services / 6G-IA) • EU Chips Act • National skills strategies

Three tensions every NCA must arbitrate

Good policy is not the absence of trade-offs — it is making them visible, deliberate and reviewable.

Security vs. Deployment speed Hard requirements protect citizens but can delay coverage, slice availability and 5G use cases. Phasing, transition periods and operator-specific roadmaps are the usual mediation.	Sovereignty vs. Openness Restricting suppliers narrows the attack surface but also the supplier base. Open architectures (O-RAN) widen choice but introduce new integration and assurance burdens.	Regulatory predictability vs. Adaptive supervision Operators need stable rules to invest. The threat landscape evolves faster than legislation. Risk-based, evidence-led supervision is how an NCA reconciles the two.
--	---	---

How 5G-TACTIC supports NCA policy work



Evidence base

SECAM-based evaluations of real 5G/O-RAN building blocks generate the technical evidence NCAs need to calibrate risk-management measures and supervisory expectations — beyond vendor self-attestation.



Methodologies & guidelines

Reusable evaluation methodologies, threat catalogues and mitigation playbooks for RAN, Core, MEC, slicing and orchestration — directly translatable into national audit guidelines and incident-response SOPs.



Capacity building

WP6 training is designed for European regulator and cybersecurity authorities. It builds the technical depth an NCA needs to keep pace with a multi-vendor, software-defined 5G stack.



Cross-authority cooperation

Six authorities from four Member States (DNSC, NASK, DSA, EETT, UKE, OCECPR) work side-by-side, building practical interoperability between cybersecurity and telecom regulators.

RECOMMENDATIONS

Five moves a National Cybersecurity Authority should make now

- 1** Treat 5G as a programme, not a project — assign a multi-year mandate inside the NCA with stable funding and a named senior owner.
- 2** Maintain a living national 5G risk picture — refreshed annually, sub-domain-specific (RAN / Core / supply chain), and tightly synced with the EU coordinated risk assessment.
- 3** Move from compliance to assurance — anchor supervision in the EU 5G certification stack (EU5G NESAS-based for network products, EUCC for secure elements, RED → CRA for devices), not just self-attestation.
- 4** Invest in technical sovereignty of the regulator — own RAN/Core expertise, run or co-run testbeds, engage directly in 3GPP/O-RAN/ENISA work.
- 5** Institutionalise cooperation — formal interfaces with the NRA, peer NCAs, ENISA, and operators; structured channels for cross-border issues (e.g. shared MORANs).

Thank you • Questions welcome