

Securing European 5G Networks

A Vertical Perspective of Regulation

Dr. Aggeliki Pragiati

Regulatory Expert | EETT Innovation Dpt.

- The Strategic Importance of 5G Security in the EU Policy Context
- Core EU Legal and Policy Instruments
- Holistic EU Regulatory Framework of Trust: The pillars
- Practical Implications for National Regulators
- Future directions
- Concluding remarks and key takeaways

5G networks underpin Europe's digital and green transformation across critical sectors from energy to public health.

Key challenges include:

- Virtualisation, SDN, network slicing
- Increased attack surface via IoT
- Resilience of critical infrastructures

EU identifies 5G cybersecurity as a strategic priority



This calls for a collaborative approach to security across the entire 5G ecosystem

Vertical Stack Vulnerabilities

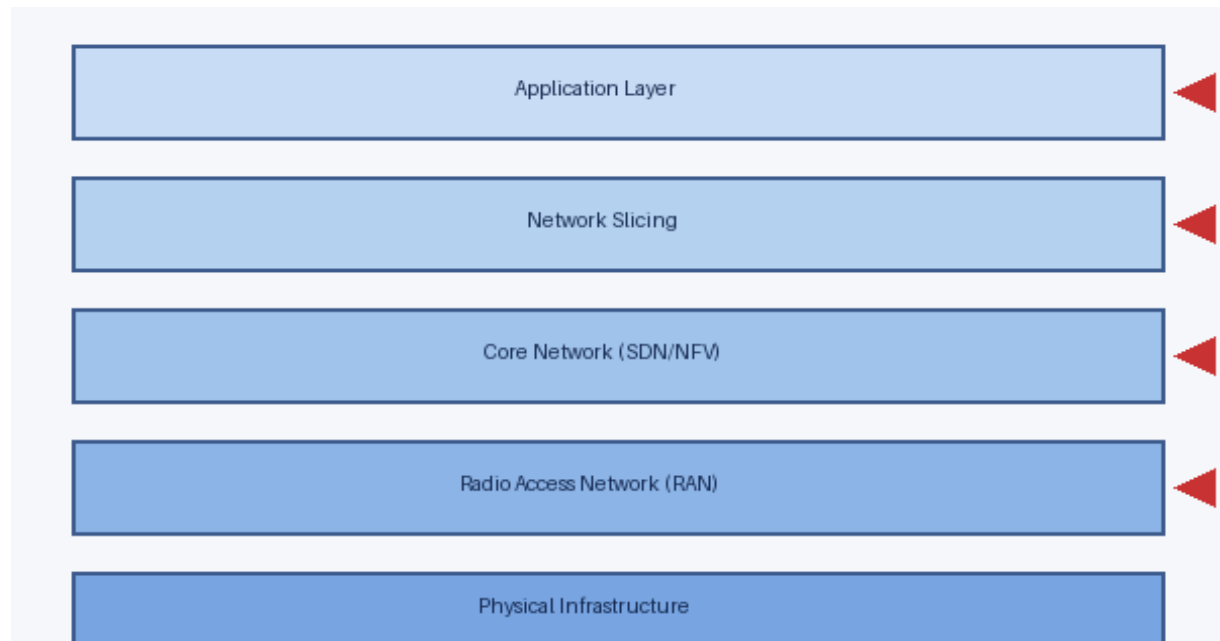
Physical: Submarine cable tapping, tampering of nodes, physical synchronization attacks.

Open interfaces: (i.e. O-RAN) exposed to third-party code.

Infrastructure: interoperability challenges for security mechanisms.

5G/6G Edge: Massive IoT expansion and AI-driven automated attacks.

Cloud Convergence: SDN makes the entire vertical stack a potential unified target.



"Vertical" Policy pillars

- Resilience of Critical Infrastructure: Ensuring that a failure in the physical network doesn't collapse the energy or transport sectors (NIS2 focus).
- Digital Sovereignty: Promoting European-made solutions for the 6G stack to avoid vendor lock-in.
- The Connectivity Gap: Ensuring that high security requirements don't prevent the rollout of 5G/6G in rural or underserved "vertical" industries.

Policymakers' considerations

- Provide legal certainty and ensure a level playing field for businesses.
- Deliver consistent and reliable privacy experiences for users.
- Support technological and data-driven innovation that unlocks economic and social benefits while meeting public policy objectives.

Moving beyond isolated fixes to a comprehensive ecosystem of trust

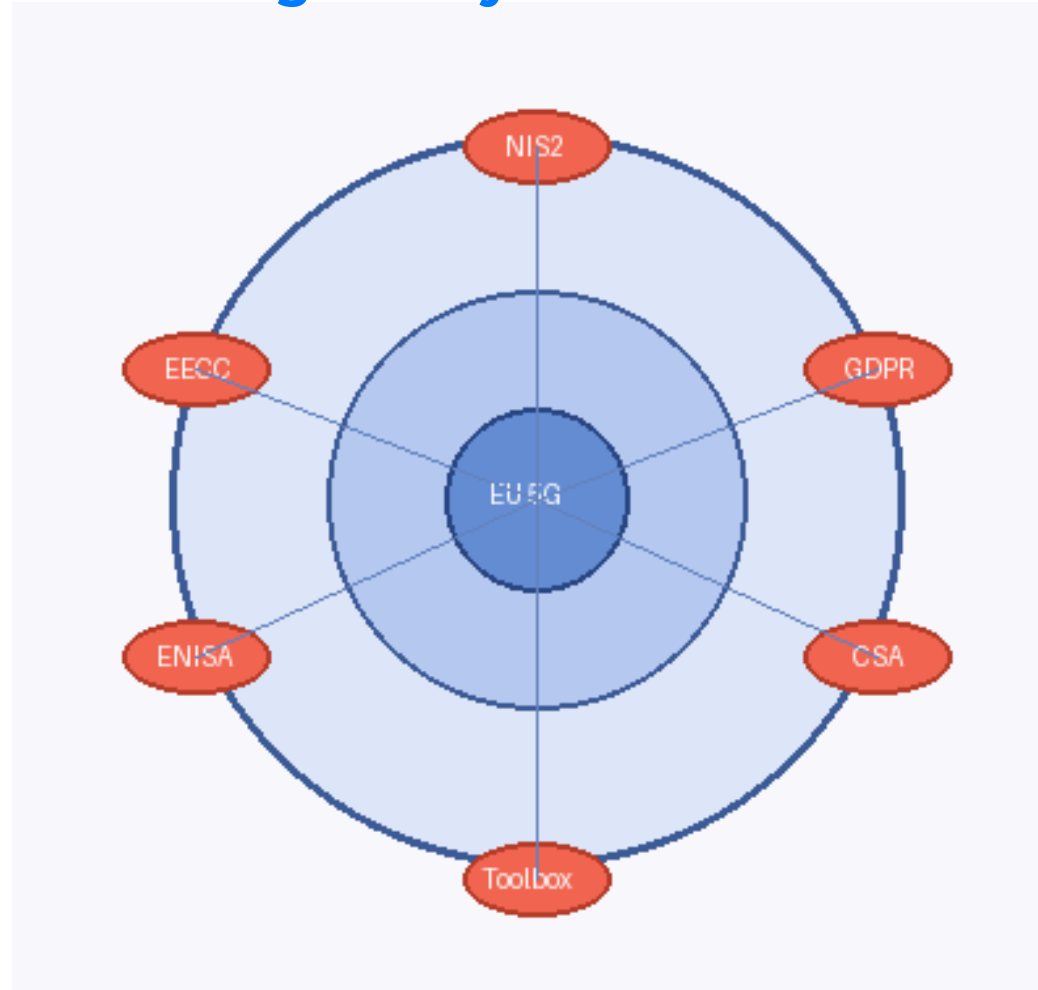
Regulation Network and Information Security (NIS2) Directive

Certification CyberResilience Act (CRA): Regulation (EU)2019/881

Risk Assessment The EU 5G Cybersecurity Toolbox

Coordinated Governance ENISA 5G Security Controls Matrix

EU has formed a Holistic Regulatory Framework



Holistic EU Regulatory Framework of Trust

EECC

Incident reporting
Operator licensing
Security obligations
NRA supervisory powers

Supply chain &
NRA oversight

Telecom Operators
Security Obligations

5G Network Security

NIS2

Network-wide risk mngt
National authorities powers
NIS Cooperation Group

Incident mngmt &
Vulnerability disclosure

EU 5G Cybersecurity Toolbox

Supplier risk assessment
Supply chain diversity
High-risk vendor rules
Strategic/technical measures

Product Assurance
for 5G Components

Cyber Resilience Act (CRA)

"Security by Design"
Vulnerability disclosure
CE marking for ICT products
Essential requirements

Directive (EU) 2022/2555, since 18/10/2024 a legal requirement

- Replaces the original NIS Directive, ensures a high common level of cybersecurity across EU.
- Applicable to electronic communications networks, digital infrastructure, and critical sectors.
- Key obligations for operators:
 - Implementation of tech and organisational measures to manage cybersecurity risks.
 - Incident notification to competent authorities.
 - Supervisory and enforcement powers granted to national regulators.

Detection

24 Hours

72 Hours

1 Month



Incident Identified

Early Warning

Official Notification

Final Report

*Stringent timelines ensures rapid EU-wide coordination
and mitigation of systemic cascading failures*

CRA: Securing the Supply Chain

Entered into force on 10/12/2024 - Main obligations from 11/12/2027



CRA Mandates

Certification of ICT products and Software Bill of Materials (SBOM) for operators.



Risk Profiles

Identifying high-risk vendors and ensuring strategic autonomy in network core functions.



ENISA Schemes

Standardizing product assurance: The upcoming EU5G certification scheme creates a common assurance baseline across all Member States.

Focuses on assurance, transparency, and trust in ICT products, services, and processes

Oversight Repository

Mapped to **EECC Art. 40**, this matrix supports NRAs in supervising providers under NIS2.

8 Security Domains

29 Objectives

140+ Technical measures

Mapping of threats to specific network assets



Governance



Risk Mgmt



Supply Chain



Network Sec



Incident Resp



Physical Sec



Continuity



Audit

Aligns with ISO 27002/27005 and NIST cybersecurity framework.

Used to structure compliance audits of operators.



STRATEGIC MEASURES

- Reinforced assessment of supplier risk profiles.
- Diversity of supply chains to avoid vendor lock-in.
- Enhanced regulatory powers of scrutiny over procurement.



TECHNICAL MEASURES

- Securing core network functions & authentication.
- Hardening network slicing & virtualization.
- End-to-end security monitoring & incident response.



SUPPORTING ACTIONS

- Enhancing cybersecurity capabilities of authorities.
- Strengthening EU-wide info sharing (NIS Group).
- Promoting common risk assessment methodologies.

Designed to mitigate systemic risks through a coordinated, risk-based approach across all Member States.

Practical Implications for National Regulators

NRAs act as National Competent Authorities under NIS2 and EECC



Ex-Ante Supervision

Shift from reactive to proactive supervision via risk assessments and pre-deployment audits.



Sanctions

Legally mandated corrective measures and fines for non-compliance with security objectives.



Cross-Border Cooperation

Participation in the NIS Cooperation Group, uniform enforcement to avoid Single Market fragmentation.



Cross-sector coordination

Vertical regulation supervising SW security, HW supply chains and physical infrastructure resilience.

NRAs can promote “Security by Design” practice



Adoption of Standards

Encouraging the adoption of standards i.e. NIST control frameworks.



Liaison with operators

To understand the security review processes and then potentially baselining best practices.



Support Innovation

Holding workshops to foster an environment where competing operators can work together on good security by design practices.

The EU Cybersecurity Certification Scheme for 5G (EU5G), when adopted, will standardise product and process assurance across Europe.

National regulators will play a pivotal role in the implementation, recognition, and supervision of certified products.

Continuous policy evolution expected in alignment with AI, IoT, and edge computing regulatory frameworks.

The EU's approach to 5G cybersecurity is holistic, combining regulation, certification, risk assessment, and coordinated governance.

National regulators are the cornerstone of enforcement and trust assurance.

The integration of the EU 5G Toolbox, ENISA 5G Controls Matrix, and NIS2 supervisory practices forms a coherent framework to safeguard the integrity, availability, and confidentiality of 5G networks.

Resilience is an Investment

Secure 5G networks are not just a technical requirement but the bedrock of public trust.

Vertical Alignment

Security must be addressed holistically, addressing the whole vertical stack.

Proactive Supervision

The shift from reactive "ex-post" to proactive "ex-ante" regulation is essential for maintaining trust.

Collaborative Governance

Regulators, operators, and researchers must bridge the gap between innovation and legislation to ensure European technological sovereignty.

Thank You!



✉ 5gtactic_eett@eett.gr

🌐 5g-tactic.eu
eett.gr
ctis4nis.eu