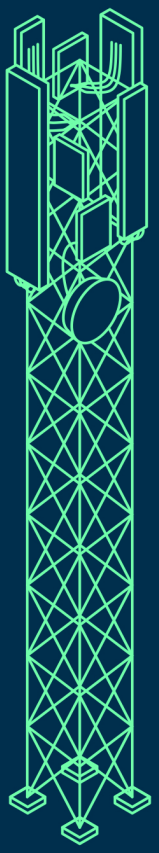
Policy Brief

10 July 2026



Digital Infrastructure Sovereignty

To Secure 5G Hardware, Europe Needs a Transparent Sovereignty-First Procurement Policy

By Orla Harris

Series 1, Brief No. 9
Editor: **Giulia Convertini**
Unit Head: **Francesco Bernabeu Fornara**

European Strategic Policy | EP

China creates, the US innovates, and the EU regulates; the infamous motto which has instilled Europeans in a 'catch up' race in global tech. What if this did not have to be the case? How do we begin remedying our strategic dependencies in tech?

Executive Summary

The European Union (EU) is racing to have the hardware and software necessary to create a fully integrated European Stack (EuroStack). In doing so, Europeans are catching up on a nearly 40-year-old Stack model developed by ISO whilst adapting it to emerging technological needs.

One area of relevance in this Stack is the *network layer,* where the *communications sector* lies. More specifically, this brief focuses on 5G networks. To harmonise legislation in this area, the European Commission is proposing the Digital Networks Act (DNA), which would make investment and manufacturing more attractive within the EU. In addition, the Cybersecurity Act would play a key role in safeguarding mobile, fixed, and satellite networks against high-risk suppliers. Thanks to these efforts, European businesses will see favourable conditions to secure their footing in this Stack layer, thereby enabling the creation of potential pathways towards European digital sovereignty and resilience.

Overall, this Brief will shed light on *why* and *how* the EU should achieve a sufficient level of sovereignty in this layer.

By Orla Harris

Digital Infrastructure Sovereignty Analyst,
European Strategic Policy Unit (ESP)
Visit Author's Page

Contact: *contact@europrospects.eu*

Key Recommendations

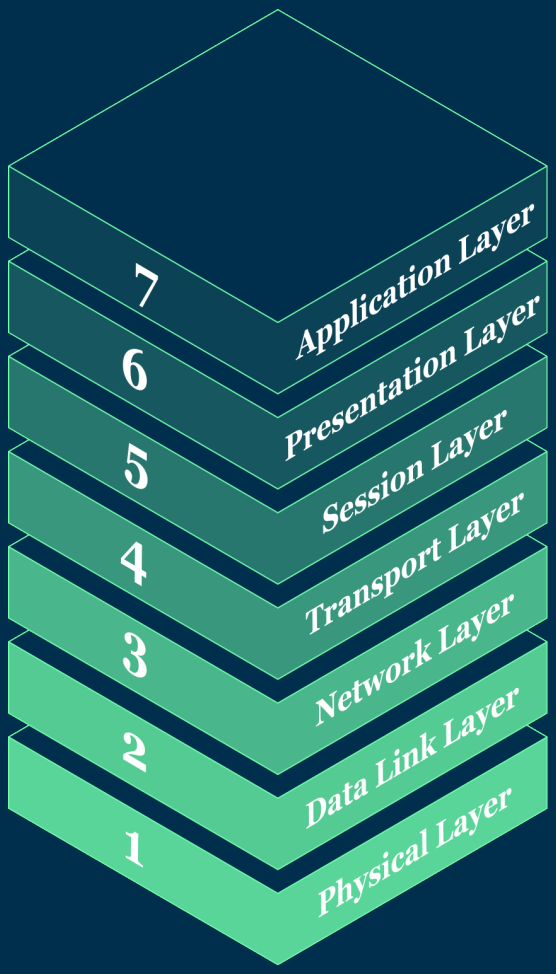
1. **Rethinking Foreign Public Procurement** by strategically redirecting national public partnerships away from foreign-influenced companies and towards EU businesses in the 5G network sector.

2. **Preemptively Account for Simplification** by carving strategic pathways for targeted amendments in sovereign-enabling legislation whilst ensuring afforded protections to mitigate Omnibus debates.

3. **Supply-side Transparency Measures** by adding a sub-paragraph to the DNA, creating an EU-wide transparency registry for suppliers to register their business and services with strategic BEREC oversight and certification scheme.

These recommendations are to be taken on the EU level and supported by Member States. Further elaboration is found in Section ***IV, Recommendations on Future Steps***.

The EuroStack (based on the ISO OSI model):



Network Types and Their Policy Grounds

The most up-to-date legislation relevant to 5G networks is the EU's Digital Networks Act (DNA). As a draft act, its aims are to harmonise and boost connectivity networks whilst making sure that resilience and sustainability are not amiss. It is a piece of a larger picture on technological infrastructure, providing a much-needed examination of the EU's current level of communications network and overall digital infrastructure, also known as its '*level of digital architecture.*'

One of the most important communications networks in the EU, and the focus of this brief, is 5G networks. 5G is a cellular standard developed from 3G and 4G technology that operates on different frequencies (low/mid/high band), with that spectrum being licensed, shared, or unlicensed via mobile network operators (eg., Orange, Tango, T-Mobile). 3G enabled mobile data, 4G/LTE scaled it for smartphones and streaming, and 5G builds on 4G's existing architecture while multiplying speed, reducing latency, and connecting far more devices simultaneously.

Important to this conversation is the hardware that enables and maintains this network. Unfortunately, no central EU body or group has released a comprehensive overview encompassing 5G network hardware components. Rather, this leaves for a fragmented understanding which must be pieced together:

- Modem (the chipset enabling connection from mobile/IoT to network);
- Base station (radio units, power supply systems for interface between users and the networks);
- Small cells (DAS, picocells to help manage dense urban coverage);
- Core (central component for managing data traffic and network services);
- Antenna array (antenna configuration to enhance signal strength); and
- Ran (interface between user devices and the 5G core network).

"Collectively, this is most of the hardware that enables our 5G network."

Operating this hardware is no small feat. To which, there are two problematic associated costs that legislation has attempted to remedy: permit granting and licence terms.

The former costs are mainly imposed by local authorities that relate to digging and installation rights for towers, masts, and other network infrastructure hardware. The 2014 Broadband Cost Reduction directive (BCR) was supposed to be key in remedying this burdensome cost. Yet, as the BCR faced significant inconsistent transposition across MS, that translated into less reduction of uptake costs. To remedy this, the Gigabit Infrastructure Act (GIA) was introduced in 2024, nearly 10 years after the BCR, and it was supposed to support faster and more cost-effective deployment of very-high-capacity networks. However, in a key provision, public-private partnerships

were weakened by the exclusion of municipalities from their scope. Leaving this policy area weakened and unfinished.

The latter costs are associated with licenses for the use of radio network spectrum by mobile operator networks. These licenses were given for 15-20 years, which posed reliability issues for these network operators. Operators could not confidently invest millions when their license might expire before they recovered the costs. Similar to the BCR, the EU introduced legislation to remedy this problem, the DNA. The DNA resolves this problem by imposing indefinite licenses with a 40-year minimum limit (with exceptions and safeguards to prevent abuse). Under the DNA, EU mobile operating networks would have the financial certainty they need for long-term investments. This allows for both incumbents and new entrants to plan long-term capital expenditure without fear of license expiration or regulatory uncertainty.

The Call for Sovereignty

In an increasingly digital world, networks form an integral part of our day-to-day lives. At both extremes, from emergency preparedness to ensuring day-to-day business activities, communication and its networks are vital to advanced economies. Any destabilisation in our communications would essentially paralyse society and economic activity.

The cost of using non-sovereign solutions is apparent in various digital sectors. From technological policing due to geopolitical tension (Microsoft revoking ICC judges' software access) to cases of foreign election interference (Cambridge Analytica scandal and, more recently, TikTok's indirect involvement in the 2024 Romanian elections). The push for EU sovereign solutions has gained substantial momentum in recent years. From civil society to academics, industry, and even ordinary people in the Union, sovereignty is at the forefront of technological development.

Thereby, the rationale is at least two-pronged: *control and independence*. Europe must have control over its technology, as technological sovereignty = controlled independence.

Hardware Origins & Potential Challenges

I: Europe's Hardware Suppliers:

Europe has typically preferred to purchase communications hardware from non-EU companies due to their ready availability, low cost, and overarching relationship-building advantages with foreign suppliers.

In Europe, mobile network operators have often outsourced parts of their costs, such as expensive tower operations, with private equity buyers readily willing to take on the costs. Most of these companies are long-term European-based businesses, but some are also US-based (3i is US-based, and Apax is UK, Paris, and US-based, but with long-term near billion investments in Israeli technologies).

Huawei and ZTE are two of Europe's biggest foreign companies supplying the EU with 5G network hardware, both being China's flagship tech firms. Together, these companies provide hardware components for some of the EU's most critical and sensitive 5G network infrastructure in Europe. As recently as 2024, countries' 5G RAN hardware has been supplied by Chinese companies, particularly in Cyprus, Austria, and the Czech Republic.

Such unhindered prosperity in the European market, however, would be short-lived. By 2023, growing skepticism over embedded Chinese surveillance technologies and legislative crackdowns would begin constraining the Chinese telecommunications industry. The Cybersecurity Act would empower European authorities to phase out "countries posing cybersecurity concerns" such as China.

"EU network operators are at the forefront of the development and transformation of the digital infrastructure that supports our digital economy and society."

II: Dependencies & Supply Challenges:

Setting aside the competitive argument that limited suppliers limit competition, having key hardware components manufactured outside of the EU's reach creates a deeply insecure supply chain reliance.

Reliance on Chinese companies is not inherently bad if it were not for their national intelligence laws mandating that every organisation and citizen "support, assist, and cooperate [...] in national intelligence work," even in times of peace. In cases of increasing geopolitical tensions, the People's Republic of China could leverage its laws to require Huawei and ZTE to destabilise European networks.

While a full-blown deterioration of EU-China relations might be backstopped by the nearly 900 billion EUR trade of goods between the two actors, tensions are already creeping in as the EU pushes to exclude Chinese companies from 5G network contracts. The EU is mandating the phase-out of high-risk suppliers of ICT components in electronic communication networks. As a result of this sovereign-enabling legislation, we are seeing heightened lobbying by Beijing to remove such provisions.

This is why the EU must advance in its goals to lead, support, and develop sovereign solutions.

Recommendations on Future Steps

I: Rethinking national public procurement

One of the larger claims in the sovereignty debate lies in leveraging public procurement to enable the development and uptake of sovereign applications. One of the leading voices on this topic is Cecelia Reik. In a key paper on the topic, Reik's research sheds light on '*offer[ing] a democratic, public-led digital stack*' and '*end contracts with BigTech*'. A fine line would nonetheless have to be drawn in order not to disproportionately exclude foreign companies from being able to operate within the EU market. Implemented radically, such policies may interfere with the single market's

principles of competition and lead to tech decoupling and isolation.

Concretely, one suggestion is to borrow this public procurement idea and apply it to 5G network ecosystems built in the EU. In practice, the EU's steps would look like;

1. Reevaluate 5G network public procurement deals (tenders and aid) on the national and EU levels.
2. Not renew public 5G network procurement deals with companies that have deep non-EU government ties.
3. Buying European: implementing new public tenders and creating mechanisms for financial aid that support EU businesses in the 5G network ecosystem.
4. Create a centralised platform that provides open-source 5G network solutions that EU businesses can reliably use.

This first recommendation is similar to already-researched public procurement arguments and similar to legislative initiatives already on the table (cybersecurity ICT supplier phase-outs), making it an achievable goal. However, in order to effectuate it, safeguards need to be implemented. For instance, mechanisms to prevent 'EU washing' whereby companies subscribe to the 'Made in EU' model already in use in manufacturing.

Preemptively Account for Simplification

Alongside researching solutions and releasing press briefs about EU sovereignty needs, we need to find ways to take this topic from a *European desire* and turn it into *actionable measures*. To which, the EU has already begun proposing initiatives to 'achieve technological sovereignty [...] that are interconnected and mutually reinforcing'. These are all welcome initiatives with one major caveat: potential 'simplification'. Given the recent digital omnibus turmoil, one can only question whether today's good sovereignty-legislative intentions, such as the DNA, Cybersecurity Act and Technology Sovereignty Package, may be simplified with less protection down the line once the political will to keep on pushing for European-based solutions expires.

Instead of entrenching the law and making it un-amendable, the following preemptive policy recommendation is suggested:

Concretely, creating timelines and pathways for laws to be amended where additional protection is afforded in the DNA, Tech Sovereignty Package, Cybersecurity Act, and other sovereignty-enabling legislation.

The second point on *additional protection* is just as important as the first *amendment*. Without concrete scope for amendment, protections can be withdrawn, as claimed in the GDPR Digital Omnibus debate. Having this intention would guide amendments to prevent

potential regulatory capture from occurring. This recommendation is similar to the already existing 'fitness check' of laws, with the addition of this *guiding* element. Allowing for this amendment would preemptively remedy instances of regulatory stagnation.

"We need sovereignty solutions to be more than a political trend; we need them to materialise and stay."

Supply-side Transparency Measures

As of writing this brief, there is no centralised information point on where EU 5G network hardware comes from. The only source with an EU overview is a 2020 report by Strand Consult that only covers Chinese operators and is available only upon request. Therefore, the only publicly available information on this is out of date and not accessible. By knowing what hardware is European and which is not, this transparency would allow for smoother compliance with the Gigabit Act and the Cybersecurity Act's phase-out of high-risk suppliers from European 5G networks.

Concretely, this requires adding a subparagraph to Article 6 of the DNA allowing for the creation of an EU transparency registry of 5G network hardware suppliers.

This would make the Body of European Regulators for Electronic Communication (BEREC) in Article 6 of the DNA go further than just collecting information about the "architecture, capabilities and usage of network segments."

To do so, BEREC would create a centralised transparency registry for this purpose and work with national telecommunication bodies to require businesses to verify whether their 5G hardware component suppliers have registered in this registry. Placing the burden on the suppliers of 5G components removes unnecessary compliance burdens from businesses building these networks. Businesses on the receiving end of the hardware would be required to verify compliance with said registration through an official document generated once supplier registration is approved in the EU registry. This would provide a publicly available and holistic understanding of where our 5G network hardware comes from.

Future Research

The topic of digital sovereignty is a well-studied field with ever-growing considerations. This policy brief sheds light on one important strategic sector, that of communications and specifically 5G networks. Yet, it cannot take into consideration all developments related to EU initiatives, as they are theoretical as of writing this brief.

Future research should map these theoretical (or soon-to-be practical) initiatives, such as the 'Made in Europe' tag, and see exactly to what this label is applied (most recently found in the proposed Industrial Accelerator Act regulation applicable to low-carbon emissions). Future research should also factor in the proposed re-

view of the EU's 2014 public procurement framework.

About the Author

Orla Harris LL.M is a policy analyst at Euro Prospects with a keen interest in leveraging sovereignty technology to fortify European digital values. With an LL.B in International and European law (data protection focus) from the Hague University and an LL.M in Technology law (tracking technology focus) from Utrecht University, Orla is well versed in how technology and the law co-exist in the European Union. With both consultancy and published research experience, Orla looks forward to working on meaningful policy reporting at Euro Prospects.

About Euro Prospects

Euro Prospects is an independent platform for in-depth analysis of European political affairs. We publish articles on the issues shaping Europe today, from the EU–Mercosur trade agreement and Europe's semiconductor supply chains to the European Union's strategic shift on Syria and Serbia's global arms trade, to name a few.

But informing readers is only part of our Mission. Euro Prospects was founded to help cultivate a European public sphere — a transnational space of political curiosity and civic engagement among Europe's citizens. A healthy EU democracy depends on citizens who are interested in and engage with EU debates shaping their future, regardless of their political convictions.

To this end, Euro Prospects offers a platform for reflection and debate on Europe's politics, policies, and prospects, bringing together a diverse team of students and young professionals from across the continent.

Visit Euro Prospects

Partnerships

Are you an organisation interested in partnering with Euro Prospects? ESP is actively building relationships with researchers, institutions, and publications working on European policy. If you'd like to discuss this brief or explore ways to work together, reach out.

Contact Us

About ESP

The European Strategic Policy Unit (ESP) is Euro Prospects' dedicated think tank department. We produce forward-facing, policy-actionable analysis on European strategic sovereignty across defence, technology, trade, energy, industry, and digital infrastructure.

ESP Members

Francesco Bernabeu Fornara
Head of Unit; Editor-in-Chief, EP

Giulia Convertini
Digital Systems Sovereignty

Finn Sands Robinson
Trade & Industrial Strategy

Rimsha Arif
Energy Market Resilience

Matilde Minetti
EU-China Strategic Competition

Orla Harris
Digital Infrastructure Sovereignty

Jerfi Wigley
Supply Chain Resilience

Annika Gerbig
Defence Industrial Autonomy

Trinabh Banerjee
Strategic Digital Security

Luka Okropirashvili
Eastern Neighbourhood

Juan Carlos Leunissen
Transport & Energy Connectivity

Erik Giuliano Würthner
ESP Outreach & Partnerships Coordinator

European Strategic Policy

EP