The Hidden Backbone of Digital Sovereignty: Why Europe Must Care About Internet Routers

IEF

SAFENet
SOVEREIGNTY ALLIANCE FOR EUROPEAN NETWORK TECHNOLOGY

iconomy

Contents

Foreword

AS A CHURCH ALTAR BOY in my boyhood, I was given an unforgettable bit of advice regarding my role as the priest's little helper at the altar: no one notices an altar boy unless or until they make a mistake. As we set out to produce this paper, that idea kept running through my head, because the topic at hand, routers, are like the unseen acolytes of our daily lives on the Internet. They are everywhere, but in many respects invisible and unexamined. We usually only encounter them unless we are having trouble with our Internet connections.

Normally this would not be a problem, but recent political realities have brought geopolitics into all layers of the technology realm. Europe and the United States, for instance, have gone to great effort to debate or even remove Chinese hardware from critical 5G networks. Many still debate if the threat matches the actions, but the public and lawmakers have grown increasingly willing to stand up for Europe's interest. Until now, that vigilance has strangely not extended all the way to the user's end point device. This paper hopes to change that.

The Innovate Europe Foundation has long championed more sovereignty through development of a European tech and digital ecosystem. Like many, we often focused on platforms and the digital services built atop them, until we began turning our attention more to the infrastructure layers below. Our cloud computing paper from 2018 already pointed to the risk of critical dependencies in cloud infrastructure.

Now, as Europe's ambitions for more tech sovereignty have become widespread, we humbly suggest that there is still another tech layer that has too often been ignored: the routers and repeaters that comprise basic infrastructure in most homes and businesses. Until now, few are aware of a) the predominantly non-European origin of this equipment and b) the level of risk that potentially entails. Fortunately, a new European coalition, SAFENet, is being formed to help raise awareness about this vulnerability.

So together with our friends from SAFENet and iconomy, the IE.F has produced what we hope will be an eye-opening background paper on one of the last unexamined areas of our common technology stacks. We hope that this paper makes a valuable contribution to the public discourse around this topic, and we especially are excited to see the new SAFENet coalition establish itself as a unified voice for this important part of the European hardware ecosystem.

Clark Parsons
Managing Director
Innovate Europe
Foundation

Executive Summary

CRITICAL DIGITAL INFRASTRUCTURE has become the front line on which the most defining geopolitical and economic conflicts of our time are being fought. Governments in the United States, China, and across the globe have concluded that the hardware and software powering critical systems can no longer be treated as ordinary commercial goods. These technology supply chains are now understood as instruments of geopolitical competition and national security, driving import controls, market restrictions, and security designations once considered unthinkable measures. The rise in state-sponsored cyberattacks on critical infrastructure has reinforced this shift, turning the security of digital systems into a matter of national defense and sovereignty.

Yet the European Union has failed to adapt to this new strategic reality. Its markets remain open to hardware and software imports that create strategic dependencies and security vulnerabilities across critical infrastructure while undermining Europe's own digital supply chains. Most troubling, some of the most fundamental layers of Europe's digital infrastructure remain largely outside the scope of meaningful sovereignty and supply-chain security policy.

Over the past decade, the European Union has built one of the most ambitious digital regulation and cybersecurity frameworks in the world. The General Data Protection Regulation, the Data Act, the Radio Equipment Directive, the AI Act, the NIS2 Directive, the Cyber Resilience Act, and the 5G Cybersecurity Toolbox each address distinct aspects of how digital products, services, and infrastructure are governed in the single market. Collectively, these instruments reflect a **hard-won political consensus that critical digital systems require active governance**.

Within this architecture, however, the supply-chain dimension of one critical layer of infrastructure remains poorly addressed. The **routers and home gateway devices** installed in hundreds of millions of European homes, small and medium-sized enterprises, public administrations, schools, and healthcare premises, the physical hardware through which

approximately **93% of European internet traffic flows**, operate largely outside the EU's broader sovereignty and supply-chain security framework. While Europe legislated for cloud sovereignty and semiconductor supply chains, the literal first and last hardware hop of European digital activity became a critical supply chain blind spot. Installed in hundreds of millions of European homes and businesses and supplied directly by ISPs with no consumer choice over the manufacturer, these devices sit unscrutinized at the heart of Europe's digital infrastructure. Trusted by default and invisible in practice, they are a potential Trojan horse that no coordinated supply chain security framework currently addresses.

This paper sets out the case that customer network devices, covering routers, home gateways, and wi-fi mesh and repeater devices, represents the **single most glaring gap in the EU's digital sovereignty architecture**, and that closing it is among the lowest-friction, highest-leverage policy moves available to the Commission and Member States in the current legislative cycle.

The issue at hand rests on four pillars: the scale and centrality of routers, which handle the vast majority of European internet traffic; a concentrated market in which Chinese manufacturers hold 37% of the home network equipment in the European Union; documented cybersecurity risks arising from botnets, firmware backdoors, and the obligations imposed by China's National Intelligence Law; and a growing regulatory inconsistency, given Europe's readiness to act against high-risk suppliers in other critical hardware sectors.

In order to address this gap, the European Union does not lack regulatory capacity or analytical tools. A robust architecture around digital infrastructure security already exists. Existing and upcoming instruments address cybersecurity baselines, supply-chain risk, procurement preferences, and critical infrastructure resilience across a range of sectors and technologies. As this paper sets out in detail, that architecture has so far insufficiently addressed the strategic and supply chain risks associated

with home and SME network equipment. Europe has proven, most clearly through the 5G Cybersecurity Toolbox, that it knows how to approach this problem. The question is why it has not yet done so.

The regulatory case for action is reinforced further by public sentiment. Recent survey data across EU member states shows a sharp shift in public opinion against the influence of foreign technology providers on European digital infrastructure. The same citizens who express that skepticism are largely unaware that the router installed in their home by their Internet Service Provider (ISP) may be manufactured by the very companies they distrust. Once that gap is closed, through the transparency measures recommended below, the political logic for further action becomes very difficult to ignore. Public opinion is already ahead of the regulatory framework.

The issues identified in this paper point to four areas where European institutions and Member State governments can act, each reflecting a different lever, a different actor, and a different positive outcome for the European Union.

- **Transparency** is the lowest-cost entry point and the one most immediately achievable through instruments already in force. Mandating disclosure of hardware origin, firmware jurisdiction, and update-channel responsibility for all network devices placed on the EU market, including ISP-supplied and white-label devices, creates the information baseline without which procurement reform and supply chain governance cannot function. ISPs should be required to communicate provenance clearly to subscribers, and a coordinated public awareness initiative through ENISA should close the gap between what citizens say they distrust and what they unknowingly have installed in their homes.

- **Procurement reform** is the most direct demand-side lever available today. Applying Buy Trusted requirements to public authorities, critical infrastructure operators, and publicly funded institutions, backed by

a supply-chain-aware certification baseline for ISP-supplied routers under the European Cybersecurity Certification Framework, would reshape market incentives without waiting for a new horizontal legislative instrument. Structured replacement incentives, modeled on those used for the 5G Huawei phase-out, should support priority sectors in transitioning away from high-risk hardware.

- **Supply chain governance** is the structurally significant option, and the institutional conditions for action already exist. First, the upcoming Cybersecurity Act (CSA2) trilogue presents a concrete opportunity to bring home networking equipment into the supply chain risk conversation. In parallel, the NIS Cooperation Group has the mandate under NIS2 to prioritize a coordinated risk assessment of the routers supply chain, and the 5G Cybersecurity Toolbox already provides the operational model for what that assessment should produce: a common risk methodology and a high-risk supplier designation mechanism applicable across Member States.

- **Industrial capacity** is the long-horizon condition. Investment through InvestEU and IPCEI frameworks, combined with the harmonization of router freedom across the single market, would deepen European manufacturing capacity and expand the market segments in which European manufacturers already compete successfully.

1
THE UNFINISHED SOVEREIGNTY AGENDA

EUROPE HAS MADE SIGNIFICANT PROGRESS on digital sovereignty over the past decade. The AI Act, the Data Act, the Digital Markets Act, the NIS2 Directive, the Cyber Resilience Act, the proposed Industrial Accelerator Act and Tech Sovereignty Package, and the 5G Cybersecurity Toolbox each address discrete aspects of how digital systems are governed in the single market. The EuroStack concept, namely the layered set of European digital capabilities from connectivity at the foundation to applications at the top, has structured the most recent strategic analyses on the subject.

Taken together, these instruments reveal that digital sovereignty is not a single concept but a layered one operating across four distinct but mutually reinforcing dimensions. **Supply chain sovereignty** asks who manufactures the hardware and which states can legally compel manufacturer cooperation. **Know-how and intellectual property sovereignty** asks whether European firms retain the design and software capabilities that determine long-term competitive independence. **Security sovereignty** asks whether Europe can defend its systems against cyberattacks, vulnerabilities, and criminal exploitation from outside. **Infrastructure sovereignty** asks whether systems already installed inside Europe can be turned against it from within, as an instrument of foreign state espionage, sabotage, or coercion. Each dimension reinforces the others, and weakness in any one ripples through the rest. A credible sovereignty agenda must therefore address all four and must do so at every layer of the digital stack.

Most of the digital sovereignty conversation, however, has focused on Europe's dependency on United States hyperscaler software at the upper layers of the digital tech stack. Cloud services, AI systems, and online platforms have attracted intense attention from Brussels and Member State capitals. Hardware infrastructure at the base layer, particularly the consumer and SME network equipment through which European digital activity actually transits, has fallen through the cracks of the public debate.

The most influential strategic studies on the EU, such as the Draghi report on the future of European competitiveness, the European Parliament's report on European Technological Sovereignty and Digital Infrastructure,[1] and the European Commission's Competitiveness Compass[2] each identify growing concerns around technological dependency, asymmetric industrial competition, and the erosion of European digital sovereignty.

More recently, emerging evidence of a "second China shock"[3] has reinforced these concerns and demonstrated that their impact on Europe's industrial and technology sectors is becoming increasingly severe. A recent analysis by the Centre for European Reform estimated that Germany alone may already have lost more than 400,000 jobs linked to collapsing exports to China, while warning that Chinese industrial overcapacity and export growth are increasingly disrupting strategic sectors across Europe[4]. Despite the growing emphasis on digital sovereignty and industrial resilience, little regulatory attention has been turned toward the network access layer and customer network devices supply chain.

A sovereign European cloud and data ecosystem remains exposed when the hardware gateways connecting to it are vulnerable to supply chain attacks, data interception, or disruption executed via software controlled by non-EU actors.

The consequences of this oversight are significant. Home and SME routers are mass-market, long-lived infrastructure installed across more

1 The Future of European Competitiveness, European Commission, Available at: https://commission.europa.eu/topics/competitiveness/draghi-report_en; Report on European Technological Sovereignty and Digital Infrastructure, European Parliament, available at: https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

2 Competitiveness Compass, European Commission, available at: https://commission.europa.eu/topics/competitiveness/competitiveness-compass_en

3 Deutschland ist das Epizentrum des zweiten China-Schocks, by Handelsblatt, available on: https://www.handelsblatt.com/politik/deutschland/china-deutschland-ist-das-epizentrum-des-zweiten-china-schocks-01/100226122.html

4 China shock 2.0 The cost of Germany's complacency, Centre for European Reform, available at: https://www.cer.eu/sites/default/files/pb_BS_ST_china_shock_2.0_18.5.26.pdf

than 100 million European households and tens of millions of small and medium-sized enterprises. They are also the most exposed layer of the telecommunications supply chain to which no coordinated EU framework currently applies. The 5G core, although still imperfectly secured in implementation terms, has at least been subject since 2019 to a common risk-classification approach and to political accountability at EU and national level.

The network devices layer occupies an unusual position in the regulatory landscape. It is simultaneously a consumer product and a piece of critical digital infrastructure, sold through fragmented retail and ISP channels where commercial cost considerations have historically taken precedence over supply chain security. Unlike professional network equipment, it sits in the hands of end users who have a legitimate interest in choosing their own devices, and any regulatory response should expand that freedom rather than restrict it. At the same time, the scale of deployment and the absence of any coordinated EU framework mean that millions of devices manufactured by entities subject to foreign state jurisdiction are installed across European homes and businesses with no mechanism to assess or mitigate the risk they represent.

This paper navigates the complexities and current vulnerabilities of the network devices layer, examining why routers matter as security-critical infrastructure, how the current market is shaped, what the threat landscape looks like, and what regulatory momentum already exists that can be extended to close the gap. It draws on the legislative precedent of the 5G Toolbox and on a pattern of action visible across multiple other sectors to argue that routers represent the next logical and necessary step in Europe's sovereignty agenda.

The political conditions for action are unusually favourable. The Commission's May 2026 decision to halt EU funding for projects using solar

inverters from high-risk jurisdictions[5], citing the explicit risk of coordinated remote firmware manipulation causing grid-scale blackout, establishes both the legal-political precedent and the institutional appetite for extending equivalent logic to network infrastructure. The proposed Cybersecurity Act 2[6] and the Industry Accelerator Act point in the same direction at the legislative level: the former by introducing a horizontal ICT supply chain security framework that creates a direct case for bringing network equipment within scope, the latter by addressing the economic disadvantages European manufacturers face against state-subsidised competitors. Both policy files represent a concrete opportunity to ensure that home network equipment is explicitly recognised as a priority sector. The conditions for action on routers will not be more favourable than they are now.

This momentum finds its clearest example in the Tech Sovereignty Package[7], which brings cloud, AI, semiconductors, and data centres under a single sovereignty framework. It is a landmark initiative and one this paper welcomes. But it is also, once again, a framework that stops short of home network equipment. Sovereign semiconductors require protected transport pathways. Sovereign cloud infrastructures depend on resilient access points. Sovereign AI scales only on reliable infrastructure. The network layer that connects all of it remains unaddressed, and that is precisely the gap this paper was created to address.

5 Commission blocks EU funding for Huawei solar tech, reported by Politico, available at: https://www.politico.eu/article/commission-blocks-eu-funding-for-huawei-solar-tech
6 Proposal for a Regulation for the EU Cybersecurity Act, available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act
7 Strengthening Europe's Tech Sovereignty, European Commission, available at: https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty

SAFENet, (the Sovereignty Alliance for European Network Technology), a strategic alliance of leading European network technology companies, calls on EU institutions and member state governments to treat home and SME routers as critical infrastructure, apply the same risk-based supply chain logic already proven in 5G, and act before the dependency window closes.

2
WHY ROUTERS MATTER AS THE HIDDEN GATEWAY

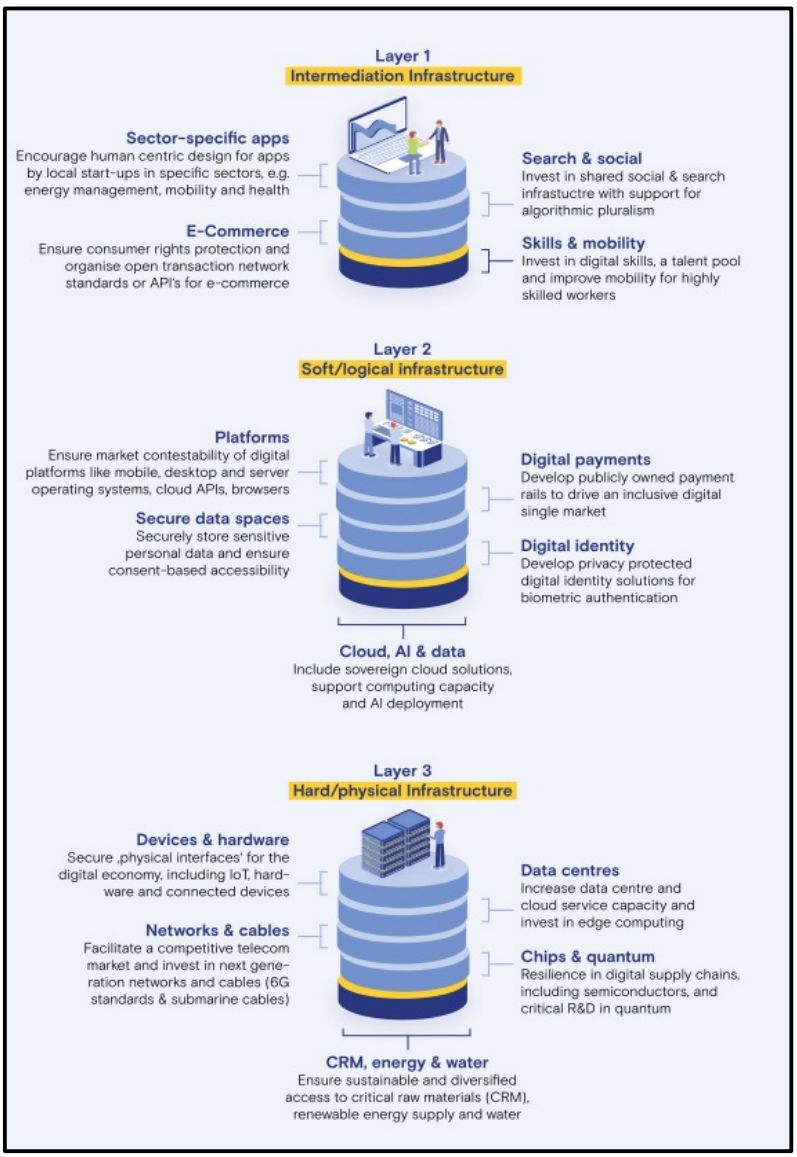
2.1 The Architecture of European Internet Traffic

Discussion of digital infrastructure in Europe is dominated by visible, high-profile assets. These include data centres, submarine cables, 5G base stations, and satellites. The router, a small, network device sitting in a hallway, a basement, or behind a television, attracts almost no comparable attention. And yet the router is, in practical terms, one of the most consequential single pieces of hardware in the entire European digital ecosystem. The image below helps illustrate why.

Europe's digital infrastructure operates as a layered stack, from applications and platforms at the top, through cloud services and operational infrastructure in the middle, down to the hard physical layer at the base. Every layer above depends on the layer below. And at the very bottom of that stack, before any data reaches a cloud service, a platform, or an application, it passes through a router. Every bank transfer, every medical record, every private message, every government login, every home office video call, every smart home device, everything a household or business sends or receives on the internet, flows through this one device. Beyond the data, all local communication within the Wifi or LAN that is managed by the router, such as printing out a letter from PC to printer, sending photos from Smart Phone to a TV, controlling heat thermostats via an App, among many other examples.

It is the mandatory gateway through which all traffic must pass, in both directions, for every user and every device. A compromised data centre affects the users of that data centre. A compromised router affects every device, every service, and every communication of everyone connected to it, silently, persistently, and without the user ever knowing.

Image 1: The Three Layers and Three Foundations of the Digital ecosystem[8]



8 The "European Way" – A Blueprint for Reclaiming our Digital Future, page 17, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5251254&download=yes
Based on 'The Technology Stack' by Gautam Kamath ECDPM, 2025

Based on data compiled from the Bundesnetzagentur, ASSIA's State of Wi-Fi reporting, and GSMA analysis,[9] routers and home gateway devices process approximately 93% of all European internet data traffic. Mobile networks, the subject of intense regulatory attention and significant public investment, account for the remaining 7%.

Routers carry 93% of European internet traffic. The regulatory attention devoted to them is nowhere near proportionate to their role in the digital economy.

2.2 What Routers Actually Do

A modern home router or home gateway does far more than route packets and sensitive information. It is the nerve centre of household and SME digital activity, managing Wi-Fi networks, coordinating smart home devices, handling voice-over-IP telephony, applying parental controls and network filtering, and, in an increasing number of cases, processing traffic associated with remote working, telemedicine, and digital government services. It is, in functional terms, a small server permanently exposed to the public internet and permanently connected to the user's most sensitive digital life.

Critically, the router operates continuously, with persistent access to all data transiting the network. A browser application can be audited, updated, or replaced in minutes. By contrast, router software is typically updated infrequently, often not at all, and the device itself may remain in service for five to ten years. Unlike a smartphone, which most users replace every two to three years, a router is rarely a considered purchase. It arrives with an ISP contract and stays until it breaks.

9 Calculation based on the following Sources: Bundesnetzagentur; ASSIA: 'State of Wi-Fi Reporting', 8 June 2021, available at: https://dynamicspectrumalliance.org/wp-content/uploads/2021/06/ASSIA-DSA-Summit-Presentation-v7.8.pdf; GSMA: 'The Importance of 6 GHz to Mobile Evolution', September 2024, available at: https://www.gsma.com/connectivity-for-good/spectrum/wp-content/uploads/2024/09/GSMA_Mobile-Evolution-in-6-GHz.pdf

For the purposes of this paper, it is important to understand routers not as a single device but as three distinct layers, each with its own origin, its own owner, and its own exposure to foreign jurisdiction.

1. **The physical hardware** is the device itself, assembled in a manufacturing facility in a particular country.
2. **The firmware and operating system** is the software embedded in that hardware, typically developed by the brand manufacturer or by an upstream original design manufacturer, and where most security risk concentrates.
3. **The management channel** is the remote pipeline through which the manufacturer pushes changes to the device after installation, and which represents effective ongoing control over the device for its entire service life.

A compromise of any single layer is sufficient to compromise the whole. This also means that sovereignty over a router cannot be achieved by addressing only one of these layers. A device assembled in Europe but running firmware developed under a foreign jurisdiction, and receiving updates through servers controlled abroad, remains fundamentally exposed. With this architecture in mind, we can now examine the three categories of risk that any serious regulatory response will need to address.

2.3 Three Core Risks

The three-layer architecture described above, hardware, firmware, and update channel, creates three distinct categories of risk that any serious regulatory response will need to address.

- **Data interception (firmware layer).** Traffic passing through a compromised router can be inspected, copied, and redirected. This applies to unencrypted traffic directly and, through more sophisticated firmware-level attacks, can potentially affect encrypted communications as

well.[10] Because the router sits upstream of every device on the network, a single compromise gives an attacker visibility into the entirety of a household or business's digital activity.

- **Weaponisation for cyberattacks (hardware and firmware layer).** Compromised routers are the primary building block of botnets, large networks of hijacked devices used to launch Distributed Denial of Service attacks, distribute malware, and conduct large-scale credential theft. Because a single firmware vulnerability can affect every device from the same manufacturer simultaneously, market concentration directly amplifies this risk.

- **Kill switch and infrastructure disruption (update channel layer).** The update channel layer is where this risk becomes most acute. A manufacturer subject to foreign state jurisdiction retains, through the update channel, effective ongoing control over every device it has ever shipped. A state actor with legal authority over that ISP and/or manufacturer can, in principle, instruct it to push a firmware update or activate an already built in pre-installed function that disables, disrupts, or weaponises millions of routers simultaneously.

Precisely because these risks are structural rather than incidental, the question of who manufactures and supplies European routers is not a market question. It is a security question. Understanding the current state of the European Network Devices market is therefore the necessary starting point for any serious policy response.

10 ENISA Threat Landscape 2024, European Union Agency for Cybersecurity, October 2024, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. ENISA Threat Landscape 2023, European Union Agency for Cybersecurity, October 2023, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

3
WHO DOMINATES EUROPE'S NETWORKS

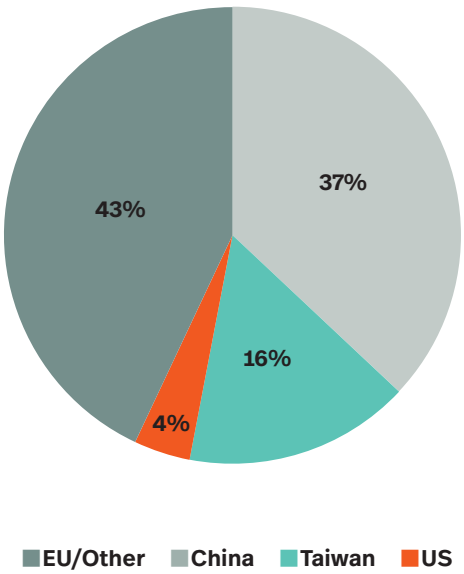
3.1 Router Market Structure

Understanding the risk posed by home and SME routers requires a clear picture of the current European market. Data compiled by the YouGov Consumer Survey 2025 and supplemented by GfK Point-of-Sale panel data[11] provides the most comprehensive available snapshot.

The findings reveal a market in which manufacturers headquartered in the People's Republic of China hold a substantial share alongside European and Taiwanese vendors. EU and other manufacturers account for approximately 43% of combined router and repeater devices across European households, with companies ranging from those operating at scale in the ISP channel, such as Sagemcom and Vantiva, to brands competing directly in retail and specialist segments, including FRITZ!, Devolo, Lancom, Icotera, MikroTik, and Teltonika. Chinese manufacturers, among them ZTE, Huawei, TP-Link, Xiaomi, and Tenda, account for approximately 37% of devices, representing an installed base across an estimated 95 million European households. Taiwanese vendors, including Sercomm, Arcadyan, ASUS, D-Link, and Zyxel, hold a further 16%, with a small United States presence at 4% concentrated in the retail segment. Taken together, non-EU vendors account for more than half of all router and repeater installations across Europe.

11 Compilation based on YouGov Consumer Survey 2025 (DE, AT, CH, NL, IT, UK); FRITZ! internal ISP CPE database; GfK Point-of-Sale Panel data 2025; Context POS Panel data for ES, FR, BE, DK, NO, SE, FI (07/2023–06/2024). Fixed assumption applied to remaining European Member States. Figures are directional.

Router and Repeater in EU by Region of Manufacturer



Source: YouGov Survey 2025 in DE, AT, CH, NL, IT, UK – For ISP routers, the country of manufacture split was determined using an internal knowledge database on ISP CPEs. Additional Countries (FR, PL, ES, GR, CZ, SE, NO, DK, FI) – For ISP routers, the country of manufacture split was determined using an internal knowledge database on ISP CPEs. GFK Data on Repeater Market Shares

Manufacturer origin	Most Manufacturers
European	Sagemcom and Vantiva at scale in the ISP channel; FRITZ!, Devolo, Lancom, Icotera, MikroTik, Teltonika and additional national manufacturers in retail and specialist segments
People's Republic of China	ZTE, Xiaomi, Huawei, TP-Link, Tenda, Reyee white labelled for ISPs and as consumer brands in Retail
Taiwan	Sercomm, Arcadyan, Compal, ASUS, D-Link, Zyxel often white-labelled for ISPs and some also as consumer brands
United States	Primarily Netgear, eero (Amazon) concentrated in the retail segment. Cisco, Linksys, Ubiquiti, Belkin, Google und Starlink are also providers.

Behind those market share figures lies a distribution dynamic that most European consumers never see. How a router reaches a home determines, in large part, whose router it will be.

3.2 How Routers Reach European Consumers

Home and SME network equipment reaches European users through two distinct distribution channels, and the difference between them shapes both the security profile of the installed base and the policy levers available to address it.

The first channel is via **Internet Service Provider supply**. In most European markets, the majority of households receive their primary router as part of their broadband subscription. The device is selected by the ISP through commercial procurement, installed at activation, and typically remains in place for the duration of the contract, often for years. The consumer plays no role in selecting the equipment, and in many cases is not aware of who manufactured the device installed in their home.

The second is **retail purchase**. Consumers and small businesses buy routers, mesh systems, and repeaters directly from electronics retailers, online marketplaces, and specialist vendors. While information about supply chain provenance and manufacturer jurisdiction is not systematically available even in this channel, the consumer is at least a party to the decision, tends to engage with it more actively, and retains a direct relationship with the device and its manufacturer.

These two channels produce systematically different market outcomes. Where consumer choice is more present, most notably in markets that have enacted dedicated router freedom legislation, consumers report higher satisfaction with their network equipment and disproportionately choose European-headquartered manufacturers.

European law already recognises the principle that consumers should be able to choose their own terminal equipment. Article 3(1) of the Regulation

on users' rights to electronic communication services[12] establishes the right of end-users to use terminal equipment of their choice when connecting to an electronic communications network. Member States have implemented this principle with varying degrees of force. Germany's Free Choice of Telecommunications Terminal Equipment Act of 2016, known as *Freie Routerwahl*[13], established the strongest national implementation, requiring ISPs to allow customers to use their own router and to provide the access credentials needed to do so. Italy adopted comparable provisions in 2018[14], and similar rules apply with varying scope across other Member States. Other European markets, including the United Kingdom, have not implemented equivalent protections.

A pattern becomes clear when brand-level data is examined alongside market structure. As the chart below illustrates, brands chosen by consumers in markets with effective router freedom consistently record positive Net Promoter Scores, while ISP-supplied and Chinese-manufactured devices cluster in negative NPS territory regardless of their awareness levels. The brands that consumers actively select when given the choice are not only more trusted, they are also predominantly European-headquartered. Where the procurement decision belongs to the consumer, satisfaction and European manufacturer preference move together.

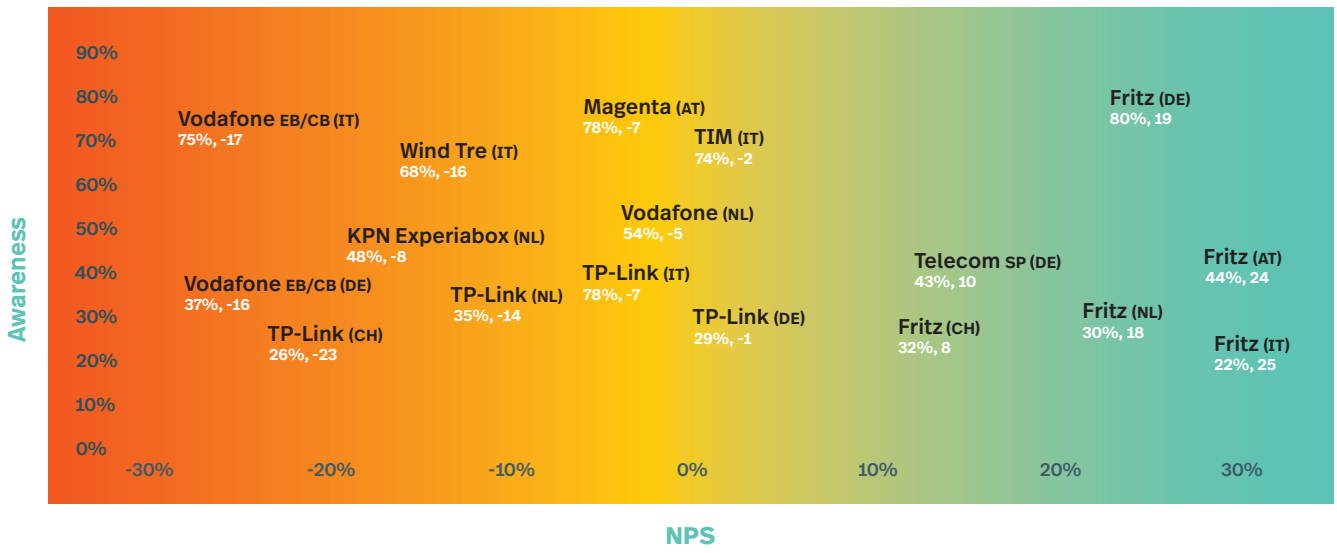
The data points to something the market structure figures alone do not capture, namely a resilient and consumer-validated European industry that competes effectively **where the conditions allow it to**. When given genuine choice and adequate information, European consumers gravitate toward European products. ISPs are not acting against the law. They are making rational procurement decisions within a framework that does not require them to weigh manufacturer jurisdiction, firmware prove-

12 Regulation (EU) 2015/2120, available at: https://eur-lex.europa.eu/eli/reg/2015/2120/oj/eng

13 Freie Routerwahl, Bundesministerium für Wirtschaft und Energie der Bundesrepublik Deutschland, available at https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Artikel/Digitale-Welt/freie-routerwahl.html

14 Delibera 348/18/CONS, Autorità Per Le Garanzie Nelle Comunicazioni, available at https://www.agcom.it/provvedimenti/delibera-348-18-cons

Image 2: Brand Awareness vs. Net Promoter Score by Router Manufacturer



Sources: Awareness: Survey by M&R, 2024, NPS: Survey by YouGov 2025

nance, or supply chain risk. The recommendations set out in this paper are designed to ensure that consumers, ISPs, and public institutions all operate with the same information about the devices entering European homes, and that European and third-country manufacturers compete on a genuinely transparent playing field. Where that information exists and consumers can act on it, the market has already shown which way they lean.

Yet the resilience of European manufacturers in the segments where they compete today should not be mistaken for structural security. Current market trends, driven by the pricing dynamics and industrial support examined in the following section, are actively eroding the conditions that make that competition possible. If those trends continue unchecked,

the window in which European alternatives remain viable will narrow, and with it the consumer choice Europeans value.

3.3 A Market in Motion

The market shares described above are not a static picture. They reflect a market that is actively shifting toward greater concentration in the hands of manufacturers headquartered in the People's Republic of China, and the dynamics driving that shift are accelerating.

Chinese network device manufacturers are investigated for benefiting from Chinese government-subsidised prices that have unfairly influenced the marketplace against Western communications equipment manufacturers. The US Department of Justice has opened a criminal antitrust investigation into whether TP-Link engaged in predatory pricing by selling routers below cost[15], a pricing practice that, if confirmed, would reflect the kind of structural state support that privately funded European and Taiwanese manufacturers cannot absorb or match. If confirmed, the result is a gradual displacement of European and trusted non-European manufacturers from a segment that sits at the foundation of the digital economy.

That displacement is now being compounded by external pressure. Following the US Federal Communications Commission's March 2026 decision to ban all foreign-manufactured consumer routers on national security grounds, Chinese manufacturers excluded from the US market represent significant industrial capacity that now has nowhere to go except towards other open markets. High US tariffs on imports from China have already led to a measurable increase in Chinese exports to the EU, with European markets absorbing redirected capacity across a range of

15 Bloomberg, Router Maker TP-Link Faces US Criminal Antitrust Investigation, 24 April 2025, available at https://www.bloomberg.com/news/articles/2025-04-24/router-maker-tp-link-faces-us-criminal-antitrust-investigation

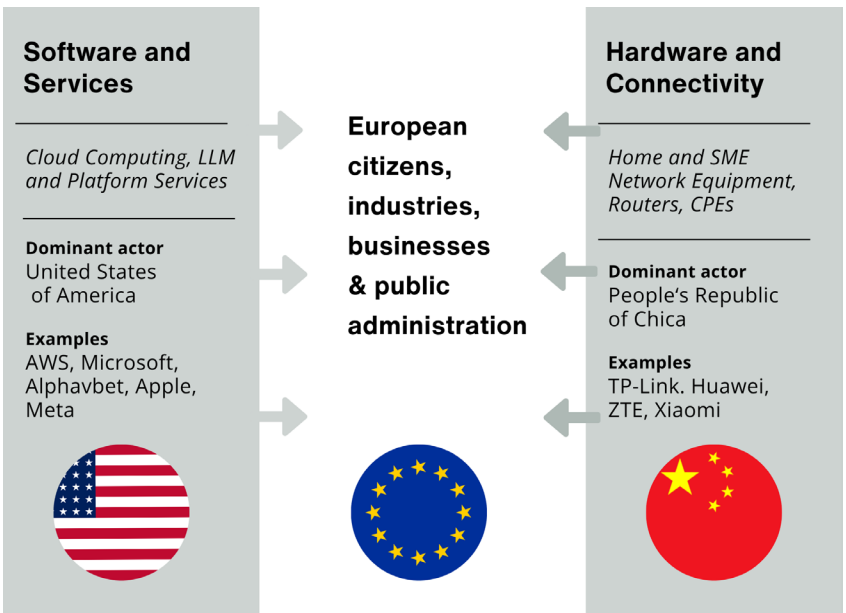
product categories.[16] If Europe does not come to terms with its exposure and take action, it will become the natural destination for a flood of Chinese routers that even the United States has deemed too great a security risk to allow on its own networks. The question is what that exposure actually means for European security, which is the subject of the next section.

16 CEPR VoxEU, Tariffs to Trade Flows, Diversion Effects and China's Exports to the EU, February 2026, available at cepr.org/voxeu/columns/tariffs-trade-flows-diversion-effects-and-chinas-exports-eu

4
THE THREAT LANDSCAPE

AS PREVIOUSLY DISCUSSED, Europe finds itself in a structurally exposed position on the digital infrastructure stack. At the upper layers, cloud computing, AI infrastructure, and platform services are dominated by United States companies, a dependency that has driven a decade of regulatory and industrial policy responses. At the hardware base layer, the manufacturing of consumer network equipment is increasingly dominated by companies headquartered in the People's Republic of China. European citizens and institutions sit between these two non-European technology poles, dependent on one for their software and on the other for the hardware through which all of it flows.

The European Dual Dependency on American Software and Chinese Hardware



The sections that follow examine what the market concentration of Chinese-headquartered hardware manufacturers documented in the previous section means for European security and sovereignty across three distinct but interconnected dimensions, covering conventional cybersecurity threats, geopolitical and state-level risks, and structural risks to European industrial sovereignty.

4.1 IT Security. Botnets, Vulnerabilities and Criminal Exploitation

Routers manufactured by any vendor can and do contain vulnerabilities. ENISA has consistently identified routers, network devices, and other internet-connected network infrastructure as significant attack surfaces within Europe's cyber threat landscape[17]. Public vulnerability databases, including the MITRE CVE[18] Program and the U.S. National Vulnerability Database (NVD)[19], further document a persistent stream of disclosed vulnerabilities affecting routers and embedded networking equipment across vendors.

An upcoming study by the Gesellschaft für Informatik (GI), Germany's leading professional body for computer science, provides the most granular vendor-level vulnerability assessment to date for the German market. Analysing the NVD for the period 2020–2025, the study identified 2,190 unique Common Vulnerabilities and Exposures (CVEs) affecting the router products of the leading vendors in Germany: Netgear (US), D-Link (Taiwan), TP-Link (China), and AVM FRITZ! (Germany). The distribution is striking. Netgear accounts for 1,016 CVEs (46%) and D-Link for 955 (44%), with TP-Link at 218 (10%). FRITZ!, the German manufacturer, records a single CVE across the entire six-year period. The divergence becomes more pronounced when severity is examined. Of the CVEs classified as critical – those with a Common Vulnerability Scoring System (CVSS) score

17 Internet Infrastructure ENISA Threat Landscape, available at: https://www.enisa.europa.eu/sites/default/files/all_files/Detailed%20Mind%20Map%20for%20Internet%20Infrastructure%20Assets.pdf
18 Available at: https://www.cvedetails.com
19 National Vulnerability Database, Available at: https://nvd.nist.gov

of 9.0 or above, indicating unauthenticated remote access, full system takeover, or arbitrary code execution – D-Link accounts for 280 (29% of its total), TP-Link for 60 (28% of its total), and Netgear for 149 (15% of its total). Nearly one in three vulnerabilities disclosed for D-Link reaches the highest severity classification. The study notes that TP-Link, despite a lower absolute CVE count, carries nearly double the relative proportion of critical vulnerabilities compared to Netgear, suggesting structural weaknesses in fundamental security mechanisms such as authentication and input validation rather than incidental or peripheral flaws.

The specific risk associated with high-market-share vendors is one of concentration. When a single manufacturer's firmware architecture contains a vulnerability, whether introduced negligently or deliberately, the scale of exposure is proportional to market share. A vulnerability in a vendor controlling 20 to 50% of European router installations provides a potential attack surface spanning tens of millions of connected devices simultaneously. The VPNFilter malware campaign, attributed by US and UK authorities to Russian state actors, demonstrated precisely this dynamic through a single coordinated operation compromising routers across multiple vendor platforms and affecting hundreds of thousands of devices across 54 countries[20]. The 2016 attack on Deutsche Telekom's router infrastructure, in which a vulnerability in the remote management function caused approximately 900,000 devices to crash and knocked nearly one million customer connections offline[21], offers a comparable illustration at national scale.

The scale of router-based cybercrime is significant. Botnets built on compromised routers have been responsible for some of the largest DDoS attacks on record, including sustained attacks on critical national infra-

20 US-CERT Alert TA16-288A, Heightened DDoS Threat Posed by Mirai and Other Botnets, America Cyber Defence Agency, available at https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

21 Global Internet Attack, reported by Deutsche Welle, available at: https://www.dw.com/en/deutsche-telekom-hack-part-of-global-internet-attack/a-36574934

structure, financial services, and healthcare systems. The Mirai botnet, which in 2016 briefly disrupted large portions of internet infrastructure in the United States and Europe, was built primarily on compromised connected devices, with routers representing a significant component[22,23]. Subsequent botnet families including Meris, Mantis, and their successors have demonstrated the same vulnerability architecture at even greater scale.

Beyond large-scale attacks, individual router take over enables persistent, targeted surveillance. A compromised router sitting in the home or office of a high-value target, such as a government official, a journalist, a lawyer, or a business executive, provides an adversary with durable, low-visibility access to all network activity. Unlike endpoint malware, firmware-level router vulnerabilities are extremely difficult to detect and may survive routine device restarts.

The threat landscape is also evolving. As artificial intelligence tools become increasingly accessible, the capacity to exploit compromised infrastructure at scale increases correspondingly. A botnet of millions of compromised routers, coordinated through AI-assisted command and control, represents a qualitatively different threat than the same botnet operated through conventional means. AI capabilities are also being applied for vulnerability discovery, with the practical effect that the time between a router firmware vulnerability becoming known and being exploited at scale is shrinking. The security calculus that applies today will intensify as AI capabilities proliferate, which strengthens the case for action while market share concentration remains addressable through ordinary policy tools.

22 Official alert on Mira, CISA, available ati: https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets
23 What Is the Meris Botnet?, Akamai's Meris explainer, available at: https://www.akamai.com/glossary/what-is-the-meris-botnet

4.2 Geopolitical and State-Level Risks. The Legal Architecture of Dependency

The cybersecurity risks described above apply, to varying degrees, to any manufacturer with weak security practices. The concern attached specifically to manufacturers headquartered in the People's Republic of China arises from a structural source. The legal and political environment in which those companies operate creates obligations that no amount of corporate goodwill or contractual arrangement can override. The previously cited GI study, drawing on its expert interviews, notes that attribution in this domain is structurally complicated by the fact that the same actor groups frequently operate simultaneously as criminal entities and as state-directed operators, which complicates the binary distinction between commercial cybercrime and geopolitical risk.

The PRC's National Intelligence Law (2017) and Counter-Espionage Law (2023)[24] impose legally binding obligations on all PRC individuals and organisations to support, assist, and cooperate with PRC state intelligence activities. These obligations apply to PRC companies regardless of where they operate. A PRC-headquartered router manufacturer with a 20 to 25% share of the European market is, under PRC law, a potential instrument of PRC state intelligence, and this status reflects a legal obligation that cannot be contracted away.

The Huawei case established this concern in the context of 5G infrastructure with sufficient clarity to drive coordinated policy action across the European Union and its major allies. Huawei is itself a manufacturer of home and SME routers present across European retail and ISP channels. The legal analysis that supported restrictions on Huawei in core network equipment applies with equal logic to Chinese manufacturers of home and SME routers. The relevant question concerns whether the legal framework governing a manufacturer creates a structural condition of potential

24 Law of the People's Republic of China on National Intelligence (2017), Articles 7 and 14; Counter-Espionage Law of the People's Republic of China (revised 2023), available at: https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017

compellability that is incompatible with the security requirements of critical infrastructure.

The "kill switch" scenario represents the most extreme expression of this risk and is not a hypothetical concern. As previously cited, Chinese manufacturers collectively account for approximately 37% of the combined European router and repeater market, meaning a coordinated firmware instruction pushed across that installed base could simultaneously disrupt internet connectivity for tens of millions of European households and SMEs. A PRC-headquartered manufacturer with that level of market presence, subject to PRC state authority and operating devices with remote firmware update capability, represents a potential vector for coordinated infrastructure disruption at national or European scale. The Commission's May 2026 decision to halt funding for projects using Chinese solar inverters, explicitly citing the risk of coordinated remote manipulation causing grid instability, demonstrates that European policymakers already recognise this threat vector as real and actionable.

State-sponsored cyber operations exploiting router infrastructure have been documented repeatedly. The 2023 joint advisory by the US NSA, CISA, FBI, and Five Eyes partners attributed a sustained campaign of router exploitation to PRC state-linked actors. The Volt Typhoon campaign of 2024 was found to have pre-positioned malicious code within United States critical infrastructure through compromised network edge devices.[25] In 2025, the Czech foreign ministry publicly attributed a sustained cyberattack to PRC state actors. In the same year, US authorities confirmed that the "Salt Typhoon" campaign attributed to PRC state hackers had compromised telecommunications infrastructure across at least 80 countries.[26]

25 Joint Cybersecurity Advisory – People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices. NSA, CISA, FBI, and partners, available at: CISA – PRC State-Sponsored Cyber Actors Exploit Network Providers and Devices (AA22–158A)
26 US-Behörden: Chinesische Telekom-Hacker in 80 Ländern aktiv, Deutschlandfunk, available at: https://www.deutschlandfunk.de/us-behoerden-chinesische-telekom-hacker-in-80-laendern-aktiv-102.html

A short note on Taiwan is warranted given that Taiwanese manufacturers hold a comparable market share. Taiwan operates under a democratic constitutional order and an independent judiciary, with no equivalent of the PRC's National Intelligence Law of 2017 obliging private companies to cooperate covertly with state intelligence operations. Across the EU's de-risking and economic security framework, Taiwan is treated as a partner rather than a systemic rival. Taiwan's geopolitical exposure to the PRC and the prevalence of PRC-sourced firmware in Taiwanese-branded products remain live considerations, which is why the recommendations in Section 7 cover firmware provenance and update-channel control alongside hardware assembly origin.

4.3 Strategic Sovereignty and the Competitiveness Dimension

The third dimension of the threat landscape is less immediate but no less consequential. Who manufactures the physical hardware determines not only who captures the economic value of the network devices market, but who controls the foundation on which the firmware and update channel layers depend. Losing the hardware layer means losing the ability to govern the layers above it.

European router manufacturers compete in an open market against vendors whose cost structures reflect sustained state support rather than market competition alone. The Rhodium Group's May 2025 assessment concluded that China's strategy has been to systematically extend dominance across advanced manufacturing sectors through a combination of state subsidies, preferential market access, and the exclusion of foreign competitors from the domestic market.[27] The consequence for European network device manufacturers is a gradual displacement from a market that is both economically significant and strategically critical.

27 Was Made in China 2025 Successful, prepared for the US Chamber of Commerce, available at rhg.com/wp-content/uploads/2025/05/Was-MIC25-Successful.pdf

The divergence between US and European approaches compounds this dynamic. Chinese manufacturers excluded from the US market have intensified their focus on the European market, accelerating the very concentration dynamic that creates security risk. European infrastructure is becoming the global exception, the only major developed economy maintaining open door for vendors excluded elsewhere on security grounds. Europe still has a meaningful manufacturing presence in the router market. That window will not remain open indefinitely.

The GI study's market analysis of the German router segment provides an illustrative counterpoint. In Germany, where the 2016 abolition of router compulsion gave consumers the legal right to choose their own router, European manufacturers compete successfully on the merits of their products. Companies such as Devolo, FRITZ! and Lancom maintain strong positions in the retail and specialist segments, while the largest broadband provider, Deutsche Telekom, holds only 19% of the router market despite controlling more than 40% of broadband connections. The asymmetry illustrates that, where consumer choice operates, European manufacturers can hold and defend significant market share against vendors competing on cost alone. Conversely, in segments and jurisdictions where consumer choice does not operate, the structural advantages of state-subsidised competitors translate more directly into market displacement.

The three dimensions of risk described in this section, taken together, constitute a profile that European policymakers have encountered before and have already shown they can address. The legal compellability of foreign manufacturers, the concentration of market share in the hands of vendors from a single non-allied jurisdiction, and the structural difficulty of unwinding dependency once it has deepened were precisely the conditions that shaped the debate over 5G network infrastructure between 2018 and 2020. Europe addressed that challenge through a coordinated, risk-based framework that proved both workable and effective. The sections that follow examine how that framework was built, how it has since been

extended to other sectors, and why the same approach applied to routers leads to the same conclusion.

5
THE 5G ANALOGY AND A PATTERN OF ACTION

5.1 How the EU Addressed 5G Supply Chain Security

The European Union's approach to 5G supply-chain security stands as the most relevant precedent for the action this paper recommends. It also constitutes a concrete demonstration that coordinated, risk-based regulatory action on network infrastructure can succeed.

The 5G Cybersecurity Toolbox, adopted by the NIS Cooperation Group in January 2020 and endorsed by the European Commission's Communication on Secure 5G, established a framework built on three mutually reinforcing elements. First, a common risk assessment methodology that Member States were required to apply to their 5G supply chains. Second, a set of strategic measures including the identification of high-risk suppliers and the capacity to restrict or exclude such suppliers from core and sensitive parts of the network. Third, a coordinated Member State implementation process, supported by Commission guidance, that resulted in the de facto exclusion of Huawei and ZTE from core 5G network infrastructure across the large majority of EU Member States. Both companies are also present as manufacturers of home and SME network devices, with significant combined market share across European retail and ISP channels.

The key lesson of the 5G Toolbox is that it did not require the EU to prove that a specific breach had occurred. A risk-based assessment of whether the legal, technical, and geopolitical conditions surrounding a particular vendor created unacceptable risk exposure for critical infrastructure was sufficient. On that basis, action was taken and markets were effectively reshaped. The combination of security classification, procurement rules, and market signalling worked together to deliver an outcome that no single instrument could have produced alone.

The 5G Toolbox did not wait for a breach. A risk-based framework was deployed to prevent one. The same framework applied to routers leads to the same conclusion and the same imperative to act.

The same analytical framework, applied to home and SME routers, leads to the same conclusion. The legal conditions applying to PRC-headquartered router manufacturers are identical to those applying to PRC-headquartered 5G equipment vendors. The risk vectors, including data interception, kill switch capability, and state compellability, are structurally analogous. The market concentration is documented. The window of opportunity to act before dependency becomes irreversible exists now, as it did for 5G in 2019 and 2020.

5.2 A Consistent Pattern of Action Across Sectors

The 5G case is far from isolated. Examined across sectors, European and Member State policy reveals a coherent and increasingly applied logic. Where Chinese manufacturers hold significant market share in hardware with remote access capability and critical infrastructure implications, Europe has moved to restrict, regulate, or de-risk. The case of routers stands as the conspicuous exception.

The table below maps documented EU and member state actions across sectors where Chinese supply chain risk has prompted regulatory response.

Table 3. Cross-sector comparison of EU and partner action on high-risk-jurisdiction supplier presence in critical hardware categories, 2020 to 2026.

Sector	Rationale	EU action	Non-EU equivalents
Solar inverters	Risk of coordinated remote firmware manipulation causing grid-scale disruption. Majority of EU-installed inverters are manufactured in China.[28]	Commission decision of April–May 2026 to halt EU funding under cohesion and recovery instruments for projects using inverters manufactured in high-risk jurisdictions, including the PRC, Russia, Iran, and North Korea; communicated to financial institutions from 1 May 2026 and formalised in Commission guidance of 13 May 2026.[29]	**China:** domestic manufacturers such as Huawei, Sungrow, and Ginlong have achieved dominant positions in the global inverter market, supported by Made in China 2025 industrial policy, SOE-driven procurement, and structural scale advantages[30] that have significantly constrained the competitive position of European suppliers in the Chinese market. **US:** Over 54 House Republicans formally requested import restrictions on Chinese inverters in November 2025, citing critical grid security risks, including the discovery of unauthorised communication devices in Chinese-manufactured inverters capable of enabling remote access to grid infrastructure.[31] **Japan:** METI and ANRE have increased attention to supply-chain and cybersecurity risks in the power sector, publishing guidance on supply-chain security for power control systems in June 2025. Under the 2022 Economic Security Promotion Act , designated critical-infrastructure operators in sectors including energy are subject to prior-notification requirements and government screening before installing specified critical facilities, a framework that can encompass equipment used in electricity systems, including inverter deployments.[32]

CONTINUED ▶

28 Commission Blocks EU Funding for Huawei, Politico, available at: https://www.politico.eu/article/commission-blocks-eu-funding-for-huawei-solar-tech

29 Euronews report on high risk inverters, available at: https://www.euronews.com/my-europe/2026/05/04/eu-moves-to-ban-high-risk-inverters-from-china-over-cybersecurity-threats

30 China's Solar Industry upheaval will be global, available at: https://www.csis.org/analysis/chinas-solar-industry-upheaval-effects-will-be-global

31 US Republicans press Trump to block Chinese inverter imports, available at: https://rsc-pfluger.house.gov/media/press-releases/rsc-calls-out-chinese-solar-inverters-security-risk-us-energy-infrastructure

32 Guide to Supply Chain Security Measures for Power Control Systems Published, meti, available at: https://www.meti.go.jp/english/press/2025/0603_007

Sector	Rationale	EU action	Non-EU equivalents
5G core network	Legal compellability of manufacturers under Chinese state law, remote firmware update capability, concentrated supplier risk.	5G Toolbox 2020. Member State restriction of high-risk suppliers, de facto Huawei and ZTE exclusion in majority of MS[33]	**China:** Following the 2022 revision to China's Cybersecurity Review Measures[34], extending CAC oversight to procurement by critical information infrastructure operators, Nokia and Ericsson contracts were subjected to national security reviews with undisclosed criteria. The combined market share of both vendors in China's mobile networks fell from approximately 12% in 2020 to around 3% by 2025. Nokia's Greater China revenues declined by 58% between 2019 and 2025, from approximately €2.2 billion to €913 million[35]. **US:** Secure and Trusted Communications Networks Act 2019 and FCC Covered List designating Huawei and ZTE; Secure Equipment Act 2021 prohibiting further FCC authorisations for listed equipment.[36] **UK:** Ban on new Huawei equipment in 5G from 2021, full removal by end of 2027. **Australia:** Huawei and ZTE excluded since 2018. **Canada:** Huawei and ZTE prohibited from 5G and 4G from May 2022, removal by 2027.

▶

33 EU 5G Toolbox and Commission Communication on Huawei and ZTE: https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

34 China Issued New Measures for Cybersecurity Review in 2022, available at: https://www.whitecase.com/insight-alert/china-issued-new-measures-cybersecurity-review-2022

35 Ericsson and Nokia see their sales in China fall off a cliff, available at: https://www.lightreading.com/5g/ericsson-and-nokia-see-their-sales-in-china-fall-off-a-cliff

36 Secure and Trusted Communications Networks Act of 2019m available at https://www.congress.gov/bill/116th-congress/house-bill/4998
FCC Covered List (Huawei and ZTE designations) available at: https://www.fcc.gov/supplychain/coveredlist
Secure Equipment Act of 2021, available at: https://www.congress.gov/bill/117th-congress/house-bill/3919

Sector	Rationale	EU action	Non-EU equivalents
EVs near critical sites	Remote telemetry, persistent geolocation, on-board sensor data collection, and potential for remote disablement or interference; compellability of PRC-headquartered manufacturers under PRC state law.	Poland (lead), other MS developing restrictions on PRC-manufactured EVs near sensitive infrastructure[37]	**China:** From 2021, Chinese authorities banned Tesla vehicles from military bases, government buildings, airports, and a growing range of state-affiliated venues, citing data security concerns over the vehicle's sensors and connectivity. Tesla remained excluded from most government procurement lists and was not permitted to transfer vehicle data outside China without regulatory approval[38]. **US:** Department of Commerce final rule of January 2025 under the Information and Communications Technology and Services authority, prohibiting the import and sale of connected vehicles incorporating PRC- or Russia-linked vehicle connectivity systems (hardware and software) and automated driving systems software, phased in from model year 2027 (software) and model year 2030 (VCS hardware).[39] **UK:** Government review under way following January 2023 reports of PRC-manufactured tracking devices found embedded in government vehicles.[40]

37 Poland bans Chinese cars from military sites: https://www.fdd.org/analysis/2026/02/20/poland-bans-chinese-cars-from-military-sites-over-spying-fears

38 Tesla cars face more entry bans in China as 'security concerns' accelerate, available at: https://asia.nikkei.com/spotlight/supply-chain/tesla-cars-face-more-entry-bans-in-china-as-security-concerns-accelerate

39 US Federal Registry, available at: https://www.federalregister.gov/documents/2025/01/16/2025-00592/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles

40 Hidden Chinese tracking device 'found in UK Government car' sparks national security fears, available at: https://inews.co.uk/news/hidden-chinese-tracking-device-government-car-national-security-2070152

Network Devices (Routers for consumer and SME)	**Identical risk vectors to the sectors above:** legal compellability of PRC-headquartered manufacturers, remote firmware update capability, comparable or greater market concentration than 5G core networks at the time of EU action, and substantially greater installed base.	**No coordinated EU framework comparable to the 5G Toolbox applies to consumer and SME network equipment.** Horizontal instruments including the Cyber Resilience Act and the Radio Equipment Directive Delegated Act apply to consumer routers, but neither provides a supply-chain risk-classification mechanism. The proposed Cybersecurity Act 2 introduces such a mechanism for critical ICT supply chains but does not, as currently drafted, extend to consumer and SME network equipment.	**China:** In 2014, following the Snowden disclosures on NSA surveillance of equipment sold overseas, China's Central Government Procurement Center removed Cisco, Apple, Intel, McAfee, and Citrix from its approved supplier list[41]. **US:** FCC decision[42] on March 23, 2026 adding all foreign-manufactured consumer-grade routers to the FCC Covered List, prohibiting authorisation of new models; existing devices are grandfathered, with a software update waiver for manufacturers running until 1 March 2027. US Department of Justice criminal antitrust investigation into TP-Link opened in late 2024.[43] **UK, Canada, and Australia** have each issued advisory guidance or operational restrictions on high-risk network equipment; formal regulatory frameworks addressing routers are under development in each jurisdiction.

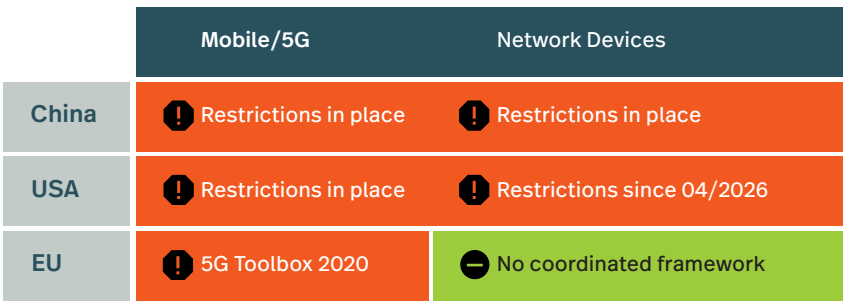
41 China 'drops US tech giants' from approved list, available at: https://www.bbc.com/news/technology-31640539

42 FCC Updates Covered List to Include Foreign-Made Consumer Routers, Prohibiting Approval of New Models, available at: https://docs.fcc.gov/public/attachments/DOC-420034A1.pdf

43 US conducting criminal antitrust investigation into TP-Link, available at: https://www.reuters.com/technology/tp-link-faces-us-criminal-antitrust-investigation-bloomberg-news-reports-2025-04-25

The cross-jurisdictional picture is striking. In every sector listed above, the European Union has acted in line with its major democratic partners, with one exception: In network devices, Europe stands alone among major developed economies in maintaining open market access for vendors that have been restricted elsewhere on identical security grounds, especially when it comes to securing networks. This is not a neutral position. Applying the 5G Toolbox risk logic to mobile networks while leaving network devices ungoverned is an inconsistency that no allied jurisdiction has chosen to maintain, and one that becomes harder to justify with each passing month.

Image 3: An Outlier Among Peers: The EU Has No Framework for Home Network Device Security



The EU applied supply chain security logic to 5G in 2020. It has not applied the same logic to fixed-line broadband Home Network Devices. Every comparable jurisdiction is ahead of Europe or moving in that direction.

The structural contradiction is also difficult to defend publicly. Europe restricts the use of Chinese solar inverters to protect the electricity grid, restricts Chinese equipment in 5G networks to protect communications infrastructure, and considers restrictions on Chinese vehicles near sensitive sites, but permits unrestricted deployment of Chinese routers that manage the internet connectivity of every European home and business.

6
WHAT IS ALREADY IN MOTION

THE CASE FOR ACTION on network security does not require building from a blank regulatory slate. A substantial body of EU legislation already exists that addresses elements of the problem, creates relevant obligations, and, in several cases, points toward the gap that a dedicated router security instrument would fill. Understanding what is already in motion is as important as identifying what is missing.

Table 4. EU instruments touching on Network Devices supply-chain security. Contribution and gap analysis.

Instrument	Relevance	Contribution and gap
Cybersecurity Act 2 (proposal, COM(2026) 11)	Very high	Currently in the early state of the Ordinary Legislative Procedure. Establishes a trusted ICT supply-chain framework with high-risk supplier designation and prohibition powers. The legislative vehicle through which the long-term recommendation in this paper can be operationalised.
Industrial Accelerator Act (proposal)[44]	High	Commission proposal published March 2026 under the Clean Industrial Deal / Competitiveness Compass implementation. Carries forward "Made in EU" procurement preferences, but scope is limited to energy-intensive industries (steel, cement, aluminium), electric vehicles, and net-zero technologies. Routers and ICT equipment are not currently within scope; alignment with network devices requires a specific political decision.
Public Procurement Directives revision[45]	High	Revision of Directive 2014/24/EU under preparation. Provides the principal legal vehicle for sector-neutral procurement preferences and national-security-justified exclusions, including for network devices.

44 ???
45 ???

Tech Sovereignty Package[46]	Medium	Commission communication and accompanying measures, 2026. Sets the strategic framing for cross-cutting digital sovereignty action across the Commission's mandate. Network devices not currently named as a priority workstream.
Cyber Resilience Act	Very High	Mandatory baseline cybersecurity requirements for connected products including Routers. Origin-agnostic. Addresses whether a device behaves securely, and does not address whether the manufacturer can be compelled to make it behave otherwise.
NIS2 Directive	Medium	Obliges telecoms operators to manage supply-chain risk. Obligations should not stop at the network termination point and therefore do not reach the network devices procurement decision.
RED Delegated Act and Open Internet Regulation	Medium	RED Delegated Regulation requires wireless devices to protect user data and network operation, mandatory from August 2025. Article 3(1) of the Open Internet Regulation establishes the user's right to choose terminal equipment. Provides the legal anchor for transparency obligations on ISP-supplied routers.
SAFE Regulation and STEP	Medium	Procurement preferences for EU-manufactured critical technology and investment mechanisms for strategic technologies. Extension to mass-market routers requires a specific political decision.
5G Cybersecurity Toolbox	High (by analogy)	The definitional precedent, comprising risk-based high-risk supplier classification, Member State implementation, and market-restriction authority. Directly applicable as a model.

6.1 Why the Cyber Resilience Act Alone Is Not Sufficient

The most predictable institutional objection to the recommendations in this paper is that the Cyber Resilience Act,[47] which entered into force in December 2024 and applies from December 2027, already mandates baseline cybersecurity requirements for connected products including routers and home gateways. If a router device complies with the CRA, the argument runs, why is anything further required?

46 ???

47 Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).

The objection conflates two categorically different risk surfaces. The CRA addresses whether a device behaves securely under normal operation. It mandates secure-by-design principles, vulnerability handling, software bill of materials documentation, and conformity assessment. These are necessary and welcome obligations. Supply-chain governance addresses whether the manufacturer can be lawfully directed by a foreign state to make the device behave otherwise. It asks about the legal framework governing the actor that controls the device's firmware over its service life, rather than about the device's default behaviour.

A network device manufactured by a company subject to the PRC's National Intelligence Law can comply fully with every CRA technical requirement and remain, in legal terms, a potential instrument of PRC state intelligence. CRA conformity assessment is performed against the device's observable behaviour at a point in time. By design, it cannot assess the legal compellability of the entity that controls the device's update channel. The CRA is a technology-neutral product safety instrument, deliberately origin-agnostic. The 5G Cybersecurity Toolbox was adopted in 2020 precisely because conformity assessment alone could not capture non-technical risk. The Cybersecurity Act 2 proposal of January 2026 reflects the same insight, establishing a horizontal supply-chain governance framework above and alongside the existing product-security architecture.

The existing EU framework asks whether a device is secure. A supply-chain governance instrument modelled on the 5G Toolbox is needed to address whether the manufacturer can be directed to make it insecure.

6.2 The Cumulative Gap and the Political Momentum

The case for supply chain governance does not rest on legal analysis alone. Public sentiment has moved in the same direction as the legislative architecture, and in some respects has moved ahead of it. Reviewing the existing regulatory architecture reveals a consistent pattern. Each instrument addresses important elements of device security, market access, or

network resilience. None, however, addresses the specific combination of factors that may render PRC-jurisdiction network devices a strategic risk: **the intersection of high market concentration, remote access capability, and the potential compellability of manufacturers under Chinese national security and intelligence legislation.** Beyond the formal regulatory architecture, the broader political environment within the European Union has become increasingly favourable to measures aimed at reducing strategic dependencies in critical sectors.

This shift is reflected in the Joint Communication on the European Economic Security Strategy[48], which identifies economic security, supply-chain resilience, and the protection of critical infrastructure as core strategic priorities for the Union. The strategy's emphasis on de-risking, technological resilience, and safeguarding sensitive infrastructure provides a broader policy rationale for heightened scrutiny of foreign-manufactured network equipment in strategically significant communications environments.

The political conditions are further reinforced by public sentiment. According to a POLITICO European Pulse survey of 6,698 Europeans conducted in March 2026, around 84% of respondents say they do not trust U.S. technology companies with their personal data, while 93% express the same view regarding Chinese firms. In Germany, distrust is among the highest in the sample[49]. A Bertelsmann Stiftung eupinions study published[50] in May this year finds that 61% of Europeans view China's global influence negatively. The same study reports that 67% of respondents believe their country is economically dependent on China. Among those who perceive such dependence, 77% support reducing it even if

48 JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL ON "EUROPEAN ECONOMIC SECURITY STRATEGY", available at https://op.europa.eu/en/publication-detail/-/publication/3948446b-101c-11ee-b12e-01aa75ed71a1

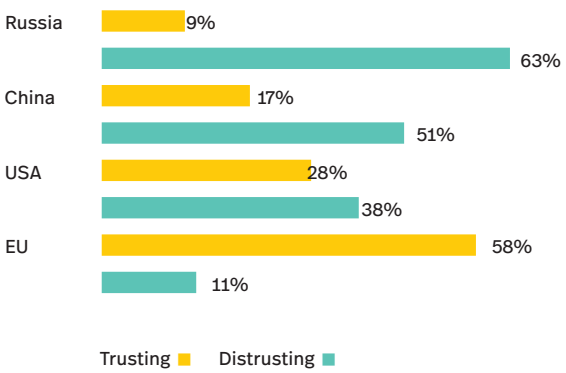
49 POLITICO 8 in 10 European don't trust US, Chinese firms with Data, available at: https://www.politico.eu/article/8-in-10-europeans-dont-trust-us-chinese-firms-with-data

50 Europe's Call for Greater Independence study, available at: https://bst-europe.eu/europe-in-the-world/europes-call-for-greater-independence

this comes at economic cost. These findings indicate both widespread concern about China's global role and strong public support for policies aimed at reducing strategic and economic dependency.

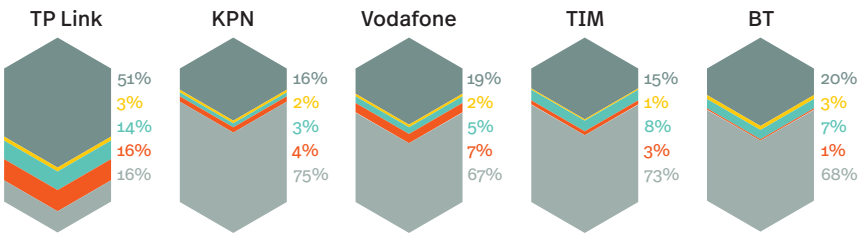
Public distrust of foreign technology companies extends directly to the devices managing European home networks. A 2025 YouGov survey of over 16,000 respondents across EU Member States found that a clear majority expressed distrust toward Chinese and Russian router manufacturers specifically, rating them as the least trusted sources of home network equipment among all manufacturer origins presented.

Trust and Distrust among Router Manufacturers (weighted)

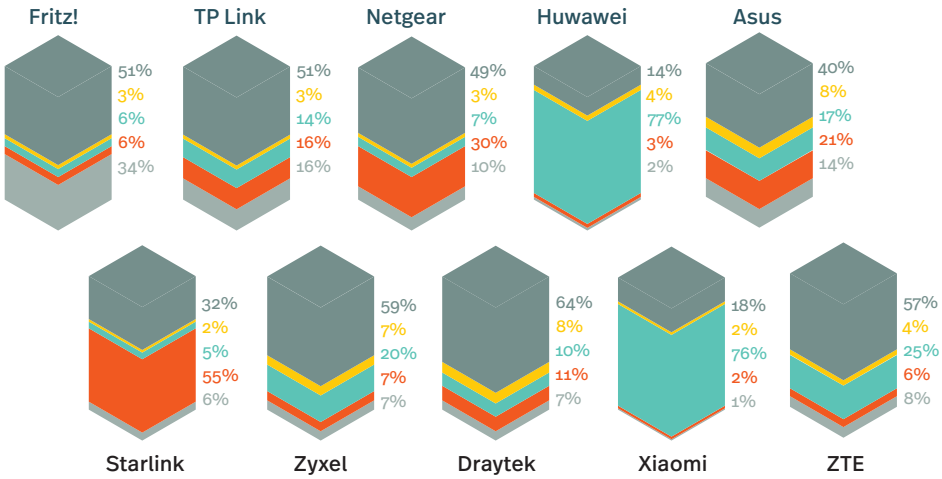


Perhaps unsurprisingly, when asked about the origin of their ISP-supplied router, most European consumers assume the device in their home is European. The same citizens who express strong scepticism toward Chinese technology are largely unaware that their router may have been manufactured by the very companies they distrust. Once that gap is closed, through the transparency measures recommended in this paper, the political logic for further action becomes very difficult to resist. On this question, public opinion is already ahead of the regulatory framework.

Which Country or Region Do You Think the Router Manufactures for the Following Internet Service Providers come from?



Which Country or Region do you think the following Router Manufacturers are from?



7
RECOMMEN-DATIONS

THE SAFENET COALITION presents a four-part action framework covering the full range of levers available to European institutions and Member State governments to address the router sovereignty gap. The four areas of **transparency, procurement reform, supply chain governance, and industrial capacity**, when taken together and fully pursued will ensure that home and SME network equipment is brought within Europe's digital sovereignty architecture, and that the 93% of European internet traffic transiting through network devices is no longer an unaddressed gap.

7.1 Transparency and Awareness

European citizens, businesses, and public authorities cannot make informed decisions about network equipment they cannot identify, and regulators cannot govern markets they cannot see. We recommend the following actions:

Mandatory Country-of-Origin and Jurisdiction Labelling for Network Devices

Manufacturers and distributors of home and SME routers and network devices should be required to disclose, clearly and in a standardised format, the country of manufacture of the device hardware, the country of jurisdiction over the firmware developer, and the country of jurisdiction over the update-channel operator. This labelling should apply at point of sale, in ISP contractual terms, and in device packaging.

ISP Disclosure Requirements on Hardware and Firmware Provenance

Internet Service Providers supplying network devices to residential and SME customers as part of broadband contracts should be required to disclose, in plain language accessible to consumers, the manufacturer origin of the device, the jurisdiction governing the manufacturer, and the firmware supply chain. This requirement should extend to the firmware and operating system layer, where provenance is often opaque even to ISPs themselves, and not merely to the physical hardware.

Mandatory Software Bill of Materials for Network Devices Firmware

Network device manufacturers placing devices on the EU market should be required to provide a Software Bill of Materials (SBOM) for all firmware covering the full transitive dependency graph rather than only top-level dependencies addressing supply chain risks not fully addressed by current requirements in Annex I, Part II(1) of the Cyber Resilience Act, and to make that SBOM accessible to ISPs and large institutional purchasers in addition to market surveillance authorities. This requirement complements the hardware provenance disclosure obligation and addresses the firmware layer, where the operational risk of remote manipulation is most acute.

Consumer Awareness Initiative on Routers Security

The Commission and Member State communications agencies should support a targeted public awareness campaign, coordinated with ENISA and national cybersecurity authorities, on the security implications of home router provenance. The campaign should address the gap between consumer concern about Chinese technology and consumer awareness of the actual provenance of their ISP-supplied devices. Awareness campaigns have been demonstrated, in the context of GDPR and cybersecurity hygiene, to create meaningful shifts in consumer behaviour.

7.2 Procurement Reform

Transparency measures create visibility, procurement reform creates the commercial incentives needed to shift market structure. The EU is the largest single purchaser of network equipment in the European market when public administration, healthcare, education, and critical infrastructure procurement are taken together, and the conditions it attaches to that procurement directly shape vendor incentives.

Buy Trusted Requirements for Public Sector and Critical Infrastructure Procurement

Public authorities, regulated critical infrastructure operators, and publicly funded institutions should be required to procure network devices from manufacturers not subject to the legal compellability conditions identified as disqualifying in the 5G Toolbox context. Pending the establishment of a formal high-risk supplier classification mechanism under the Supply Chain Governance recommenadtion at 7.3, contracting authorities can apply the 5G Toolbox risk criteria by analogy. The requirement should be implemented through the upcoming Public Procurement Act and specific NIS2 implementing guidance on supply chain risk for network devices. The principle should be Buy Trusted in the first instance, with a Buy European preference where trusted European supply meets functional and commercial requirements. These criteria can acquire binding effect for routers once the CSA2 framework enters into force.

European Cybersecurity Certification Baseline for Network Devices

ENISA, working with the Commission and national cybersecurity authorities, should develop a dedicated European cybersecurity certification scheme for routers under the European Cybersecurity Certification Framework, building on the security requirements established by the Cyber Resilience Act and complementing the essential requirements applicable to radio equipment under the Radio Equipment Directive, but extending to include supply chain provenance and high-risk supplier classification criteria.

Structured replacement incentives for high-risk hardware in priority contexts

Structured financial incentives, analogous to those used to facilitate the phase-out of Huawei equipment from 5G networks, should be made available to support the replacement of high-risk network devices in priority sectors including public administration, healthcare, education, and critical infrastructure operators. The instrument can be delivered through

the STEP mechanism, through national recovery and resilience plans, or through targeted Connecting Europe Facility allocations.

7.3 Supply Chain Governance

Transparency and procurement are necessary but not sufficient. A supply chain governance framework comparable to the one the EU built for 5G between 2019 and 2020 is the appropriate vehicle for addressing the underlying compellability of manufacturers, the structural concentration of the routers market, and the cross-Member-State coordination problem that arises when each national procurement environment makes decisions in isolation.

Bringing Home and SME Network Equipment into the Cybersecurity Act 2 Legislative Debate

As the Cybersecurity Act 2 advances through the legislative process, Parliament and Council should consider ways to address risks in the router supply chain. The CPE segment presents compellability questions of the same character as those the 5G Toolbox was designed to address, and the CSA2 framework's emerging architecture provides a natural vehicle through which those questions can be examined. The legislative process represents an opportunity to ensure that the supply chain dimensions of home and SME network equipment do not remain outside the scope of the EU's horizontal ICT security framework by default.

A Commission Recommendation on Routers Supply Chain Risk Assessment

The Commission can issue a recommendation under Article 292 TFEU directing Member States to apply the 5G Toolbox risk assessment logic to routers supply chains without waiting for the legislative process to conclude. In parallel, ENISA can be tasked through its annual work programme under the Cybersecurity Act to produce a dedicated threat landscape assessment for network devices supply chain risk, creating the analytical foundation for Cooperation Group action on its own timeline.

A Router Security Toolbox

The EU should develop a Router Security Toolbox modelled explicitly on the 5G Cybersecurity Toolbox. The Toolbox should establish a common risk assessment methodology for network devices supply chains, a mechanism for the designation of high-risk suppliers and the restriction of their products from security-sensitive deployments, and a coordinated Member State implementation process. The CSA2 framework, once adopted, provides the legal architecture through which the Toolbox measures can be operationalised as binding implementing acts under Articles 101 to 104. Unlike the 5G Toolbox, which applied primarily to professional network operators, the Router Security Toolbox must address the mass-market, consumer-facing dimension of the router market.

High-risk supplier classification mechanism

Building on CSA2 recognition and the Router Security Toolbox, the EU should establish a high-risk supplier classification mechanism for the router supply chain. The mechanism should apply the risk-based supplier assessment approach of the 5G Toolbox to the network devices context, creating a legal basis for differentiated certification and procurement requirements that factor in manufacturer jurisdiction.

7.4 Industrial Capacity Transformation

Regulatory demand-side measures must be accompanied by supply-side investment and by the expansion of the market segments in which European manufacturers already compete successfully. The goal is not European autarky in network devices, but ensuring that trusted European and allied manufacturers can compete effectively in a market currently shaped by asymmetric state support.

Near-Term: Demand Activation Through Router Freedom Harmonisation

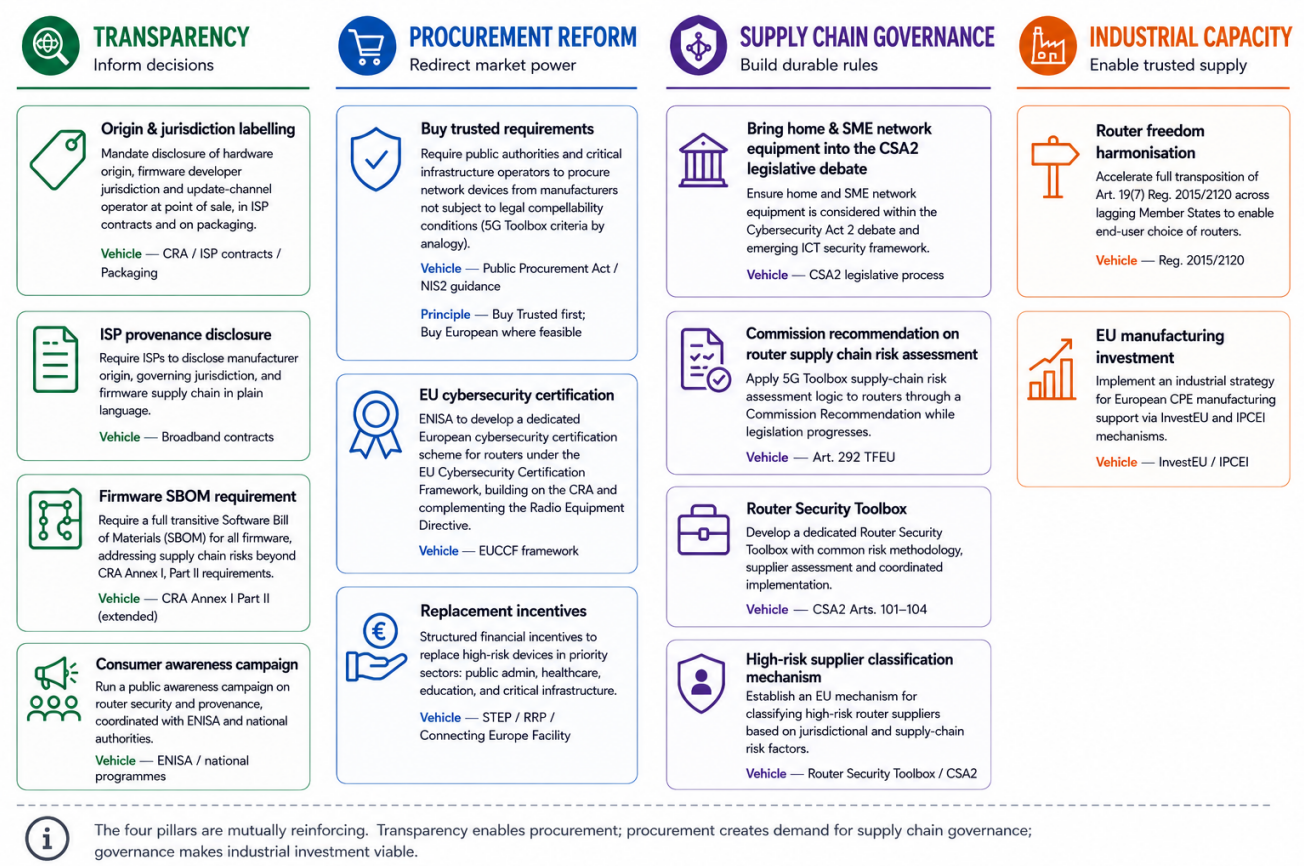
The most immediately available supply-side lever requires no new spending. Harmonising router freedom across all Member States to the standard established by Germany's Freie Routerwahl and Italy's 2018 provisions

would expand the market segments in which European manufacturers already outperform Chinese competitors on consumer preference. Where the procurement decision belongs to the consumer, European manufacturers hold their ground. Accelerating full transposition of Article 3(1) of Regulation 2015/2120 across lagging Member States is therefore both the lowest-cost and the fastest-acting supply-side measure available.

EU Investment in European Routers Manufacturing Capacity

Regulatory demand-side measures must be accompanied by supply-side investment to ensure that trusted European alternatives can meet market demand. The Commission and Member States should develop an industrial strategy for European router manufacturing, including targeted support through the InvestEU, Important Projects of Common European Interest (IPCEI) mechanisms, and public-private partnership frameworks. European manufacturers such as FRITZ!, Sagemcom, Vantiva, and Lancom demonstrate that a competitive industrial base already exists and is worth defending. The goal is not European autarky in network devices but ensuring that trusted European and allied manufacturers can compete effectively in a market currently shaped by asymmetric state support.

A Four Pillar Framework for Securing Europe's Home and SME Network Equipment



8
CONCLUSION – FROM AWARENESS TO ACTION

EUROPE HAS TO ACT NOW. Security risks, technical sovereignty, and the economic rationale of supporting European technology industries require immediate action. Europe has built the institutional frameworks, the legislative instruments, the coordination mechanisms, and, in the 5G Toolbox, the proven operational playbook. The analytical case that home and SME routers represent a critical infrastructure gap in Europe's digital sovereignty architecture is not contested by anyone who examines the evidence, the market data, the threat documentation, the legal exposure, and the glaring inconsistency with actions already taken in other sectors.

What needs to happen is political will focused on the specific question of router security. That question has been crowded out, in successive Commission Work Programmes, in NIS2 implementation debates, and in Cyber Resilience Act negotiations, by larger, more visible, and in some respects less tractable digital sovereignty challenges. Even though AI governance and cloud dependency rightly command significant attention, the critical components of the underlying network infrastructure through which all digital value flows cannot be allowed to remain an afterthought. Routers sit, literally, at the entry point to every European home and business. They are the hardware gateway through which the entire digital sovereignty architecture is accessed, and the one layer of that architecture that no coordinated European framework currently addresses.

The costs of inaction are extremely high. Every year that passes without a router security framework is a year in which Chinese manufacturers consolidate their market position, in which ISP procurement decisions lock in high-risk hardware for another decade of service life, and in which the concentration dynamic driven by US market closure amplifies European exposure. The window for cost-effective, pre-emptive action, the window that existed for 5G in 2019, is open now. It will not remain open indefinitely.

Europe has the tools, the precedent, and the political moment. The question is whether it will act before the dependency becomes irreversible.

The SAFENet Coalition calls on EU institutions and Member State governments to treat home and SME routers as the critical point in the digital services supply chain they are, to apply the same coherent logic of security and sovereignty that has already been applied everywhere else, and to act before the window closes. The European manufacturers, cybersecurity organizations, and digital rights advocates represented in the SAFENet Coalition share a single objective: advocates represented in the Coalition share a single objective. A Europe in which the fundamental infrastructure of digital life is governed with the seriousness and foresight that its role demands.

9
ABOUT THIS PAPER

About the SAFENet Coalition

The Sovereignty Alliance for European Network Technology (SAFENet) is a strategic alliance of leading European network technology companies. SAFENet understands network technology as the backbone of the digital ecosystem. The alliance represents the interests of European manufacturers in political and regulatory processes, thereby contributing to digital sovereignty and the long-term security of Europe's own digital infrastructure. Its goal is a digital Europe that is self-determined, resilient and future-proof.

About the Innovate Europe Foundation (IE.F)

The IE.F is an independent think tank driven by a circle of leading figures from the European tech world who have come together to fight for Europe's place in the global economy. As a Berlin-based forum-giver and dialogue partner, it promotes the interests of the European digital and tech economies.

About iconomy

iconomy is a Berlin-based consultancy and venture builder working at the intersection of European industrial policy and digital regulation. Deeply embedded in the European startup and scaleup ecosystem and sitting at the crossing of venture building and digital regulation, iconomy advises clients and backs builders in critical stages across Europe's most strategically important technology markets.

Copyright and citation

 This paper may be cited as IE.F and SAFENet Coalition, Who Controls Europe's Internet? | Home Routers, Supply Chain Risk and the Case for European Action (IE.F, May 2026).

Publisher

Innovate Europe Foundation (IE.F)
Schonhauser Allee 43a
10435 Berlin
www.ie.foundation

Authors

Clark Parsons
IE.F

Gustav Robrahn
iconomy

Kira Terstappen-Richter
SAFENet

Contact

Clark Parsons
Innovate Europe Foundation (IE.F)
c.parsons@ie.foundation

Publication
June 2026