93% of Europe's Internet Traffic Flows Through Routers – Yet No One Is Paying Attention: Study Demands Action on Digital Sovereignty

Wednesday 24 June, 2026

Berlin, 24 June 2026
– The Sovereignty Alliance for European Network Technology (SAFENet), together with the Innovate Europe Foundation (IE.F) and Berlin-based consultancy iconomy, publishes a new foundational study revealing that 93% of European internet traffic flows through routers and yet the EU has no sovereignty framework for this key component of the digital ecosystem. Meanwhile, Chinese manufacturers already control 37% of the market.

While Europe debates sovereignty in AI, cloud, or chips, a central element of digital infrastructure remains largely overlooked: the router. Whether in the family living room or on the network of a small or medium-sized enterprise, 93% of internet traffic in Europe flows through it. By comparison, mobile connectivity accounts for only around 7%. Yet routers receive no comparable political attention.

A newly published study shows: routers represent one of the greatest untapped levers for Europe's digital sovereignty and activating it is among the most impactful and easiest-to-implement measures of the current legislative term.

Concentrated Dependency with Security Risks

According to the IE.F study, Chinese manufacturers such as ZTE, Huawei, TP-Link, Xiaomi, and Tenda already control around 37% of home networking devices in the EU, giving them theoretical access to an estimated 95 million European households. Overall, more than half of all router and repeater installations in Europe come from vendors based outside the EU.

This dependency is not merely a question of market structure, it is a matter of security. Since the router sits upstream of every device on the network, a single compromised router opens a window into the entire digital activity of a household or business. The study identifies three core risks:

- **Data interception at the firmware level** – potentially affecting even encrypted communications,
- **Weaponisation for cyberattacks** – compromised routers are the building blocks of botnets, with market concentration amplifying vulnerability,
- **Legal exposure** – particularly due to the obligations China's National Intelligence Law imposes on manufacturers.

Inconsistency in the Sovereignty Debate

What stands out most: Europe is already acting against high-risk vendors in other critical hardware sectors, yet when it comes to routers, it remains inactive. "With the 5G Toolbox, a proven operational playbook exists. The institutional frameworks, the legislative instruments, and the coordination mechanisms are in place," the study states. "What is missing is the political will directed at the specific question of router security."

Clark Parsons, Managing Director IE.F: *"Europe has the tools, the precedent and the political moment. The question is whether it will act before the dependency becomes irreversible."*

Jan Oetjen, SAFENet Chair and CEO of FRITZ!: *"Independent and secure network technology is the foundation for Europe's digital sovereignty. Only together can we ensure that Europe retains control over European networks and shapes its own digital future."*

Consumers Trust Europe – Without Knowing It

That political will would find public support. A YouGov survey of more than 16,000 people across the EU shows: 58% of Europeans trust European routers, while 51% of respondents distrust routers from Chinese manufacturers and 63% distrust routers from Russian manufacturers. The problem: most Europeans do not even know where their router comes from. Those who receive a device from their provider overwhelmingly assume it is European – very often incorrectly, as many provider-supplied routers still come from non-European manufacturers.

Media:

SAFENet
SOVEREIGNTY ALLIANCE FOR EUROPEAN NETWORK TECHNOLOGY

Related Sectors:

Computing & Telecoms :: Government ::

Related Keywords:

Europe :: Network :: Technology :: Sovereignty :: Study ::

Scan Me:

The study concludes: transparency alone would ignite the political momentum for further-reaching measures.

SAFENet Calls For Europe To Act Now

"The analytical evidence is not disputed by anyone who seriously examines the market data, the threat landscape, and the legal exposure," says SAFENet. "Router security and sovereignty has been – and continues to be – crowded out of the European debate and regulation by larger, more visible challenges. It is time to close this gap."

From Knowledge to Action: Four Levers for Europe's Router Sovereignty

The good news: Europe does not need to create new institutions or start from scratch. The regulatory tools are already in place, it is a matter of deploying them in a targeted way. SAFENet consolidates them into a four-pillar framework:

- **Transparency and awareness**, including mandatory, standardised labelling of country of origin and legal jurisdiction for network devices,
- **Public procurement reform**,
- **Supply chain governance**,
- **Strengthening European industrial capacity**, so that trusted European and allied manufacturers can compete in a market shaped by asymmetric state subsidies.

About SAFENet

The Sovereignty Alliance for European Network Technology (SAFENet) is a strategic alliance of leading European network technology companies. Its goal: A digital Europe that is self-determined, resilient and future-proof.

Learn more at safe-net.tech.

About the IE.F

Independent Berlin-based think tank for Europe's place in the global digital economy.

Learn more at ie.foundation.

Press contact:

Kira Terstappen-Richter · SAFENet · media@safe-net.tech

Clark Parsons · IE.F · c.parsons@ie.foundation

Study:

https://www.ie.foundation/content/4-publications/ief_router-risk_260615_final.pdf

Company Contact:

_

news aktuell

E. desk@newsaktuell.de
W. https://www.newsaktuell.de/

View Online

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:
https://www.newsaktuell.pressat.co.uk