BEREC
Body of European Regulators for Electronic Communications

BoR (26) 88_19

BEREC's position on HRV Phase-Out Under CSA2 / DNA Framework

2 June 2026

On 21 January 2026, the European Commission (EC) published the proposal for a Digital Networks Act[1] (DNA) (hereinafter: "the proposal"), The proposal aims at updating the objectives and relevant regulatory tools of the EU framework for electronic communications, with a new focus on competitiveness, network resilience and security, sustainability and enhancing the Single Market for electronic communications networks and services (ECN/S).

Following the publication of the proposal, BEREC has undertaken an in-depth analysis of the text in parallel with the DNA, the Commission's proposed a cybersecurity package—most notably the forthcoming revision of the Cybersecurity Act (often referred to as CSA2) which introduces horizontal measures addressing ICT supply chain risks and resilience requirements across sectors. Given the increasing interdependence between cybersecurity and electronic communications infrastructure, these initiatives are closely interconnected, as also recognised in the DNA proposal itself, which highlights the need for more coordinated EU action to addressing persistent dependencies and security risks in digital networks. As a result, the cybersecurity proposals have direct implications for the regulatory framework governing ECN/S, including aspects related to network deployment, vendor choice and operational resilience.

This creates a clear nexus between the DNA and CSA2, and consequently calls for a structured and high-level response from BEREC in its capacity as the EU body representing national regulatory authorities in the electronic communications sector.

BEREC will further work on analysing relevant aspects as the debate may evolve and stands ready to support the co-legislators with its regulatory expertise and to collaborate on targeted improvements, including alternatives, to the legislative text.

Objective of the CSA 2 proposal

BEREC supports the objective of addressing geopolitical risks within supply chains.

HRV phase-out under CSA2[2]

From a BEREC perspective, the objective of strengthening security and resilience of electronic communications networks is fully supported. Secure, reliable and resilient connectivity is a cornerstone of Europe's digital transformation, competitiveness and societal functioning. Measures such as the mandatory phase-out of High-Risk Vendors (HRVs) must be carefully assessed having regard to costs, timeframe, proportionality and the broader market impact. In addition, market access restrictions, if not backed by a credible industrial policy, may result in reduced competition, incentivize rent-seeking, increase costs, and raise the risk of technological decline.

Feasibility

The proposal raises concerns regarding business impact and proportionality:

[1] COM(2026) 16 final, Proposal for a Regulation of the European Parliament and of the Council on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU (Digital Networks Act)

[2] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

- The electronic communications sector is characterised by long investment cycles and high capital intensity. Forcing rapid replacement of still non-amortised equipment could impose significant financial burden on operators and does not take in account national realities, such as the markets with less diversity of suppliers or a strong dependence on certain equipment.
- This could divert investment away from future, new infrastructure (e.g. fibre and advanced 5G) towards replacing existing assets, slowing down the transition to next-generation networks.
- The proposed deadline may be inconsistent with national decisions taken and could create additional implementation challenges.

In this context, BEREC underlines that the policy objectives should remain ambitious but achievable, taking into account the actual effort required from both public and private stakeholders.

Economic and societal impact

While the Commission has undertaken broad impact assessments for the Digital Networks Act, the specific impacts of large-scale vendor replacement obligations remain uncertain and may be underestimated.

Key potential effects include:

- Asymmetric impact on operators: those more reliant on HRVs could be disproportionately affected, leading to distortions in competition.
- Reduced investment capacity: resources could shift from innovation and network expansion to forced replacement.
- Potential delays in achieving the Digital Decade connectivity targets, including gigabit and 5G coverage.

Given that connectivity is a fundamental enabler of economic growth, innovation and essential public services, any measure that risks slowing down its deployment must be carefully justified.

Potential impact on the market, availability and suitability of alternative vendors

In the scenario where major suppliers are designated as HRVs, important challenges arise with regard to the availability and suitability of alternative vendors for some parts of the networks. The number of viable suppliers in some key network functions is limited, which would reduce competition in the equipment market.

At the same time, alternative vendors may face constraints in manufacturing capacity, skilled personnel and support services, potentially leading to longer delivery times and supply bottlenecks. While no significant economic impact has been observed in the member states that have implemented restrictions against HRVs, reduced competitive pressure may result in higher prices, while differences in technological maturity, performance or interoperability could further complicate the transition. This could ultimately be passed on to end-users, and may also reduce incentives for innovation and quality improvements or even lead to quality degradation at vendor and operator level. On the other hand, Open RAN standardisation and virtualisation trends may

enable greater vendor diversity and competition, creating opportunities for innovation and improved service quality if adequately supported by regulatory harmonisation.

Moreover, supply chain dependencies remain a structural issue, as acknowledged in the broader policy framework, which highlights persistent dependencies affecting electronic communications networks and critical infrastructure.

Impact on strategic EU objectives

The mandatory phase-out of HRVs may be in conflict with broader EU strategic objectives. In particular, it could delay the deployment of fibre, high-quality 5G and future 6G networks, thereby affecting the achievement of connectivity targets. The transition itself could introduce short-term disruptions that affect network resilience, should operators be unable to switch to reliable and likely more costly vendors.

Enforcement challenges

Under the current design, non-compliance with CSA2 supply-chain requirements, including the removal of HRVs, may lead to the withdrawal of General Authorisation or spectrum rights. This effectively turns cybersecurity obligations into a market access condition, with potentially disproportionate consequences and limited scope for NRA assessment of proportionality or market impact. Such a decision should therefore be in the responsibility of the NRA. The authority overseeing the CSA2 should therefore be mandated to contact the NRA in case there is a breach.

The mandatory replacement of HRVs could affect the pre-existing conditions set for the frequency spectrum licences. These may lead to legal actions and compensation claims from the licence holders.

Conclusion

BEREC supports the objective of enhancing the security and resilience of electronic communications networks and is fully committed to support the co-legislators with its expertise.

However, the current proposal would benefit from further adjustments to be proportionate, based on a risk assessment, to reflect industrial realities (including lifecycle management, the availability of alternatives and production capacity), and to preserve resilience by avoiding dependencies on a limited number of suppliers.

A more balanced approach would require flexibility in timelines and procedures, with a thorough national level assessment of impacts and appropriate safeguards to preserve competition and investment capacity, in line with the overarching objectives of the EU regulatory framework.

BEREC has observed that both the DNA and the CSA2 requirements are lacking the detail required to give of full understanding of the implementation of the regulations. Noting that the Commission has indicated that the necessary detail will be provided in implementing acts, BEREC would advise to consider the following recommendations for such.

BEREC recommends:

- Lifecycle alignment: Ensure that compliance obligations and any vendor restrictions are taking into account the network lifecycle planning (procurement, rollout, operations, upgrades, and end-of-life).
- Phased implementation: Introduce clear, risk-based transition phases (milestones and deadlines) that allow replacements to occur at natural renewal cycles, unless an immediate, substantiated security risk requires earlier action.
- Continuity of service: Require transition plans that preserve service continuity, operational stability, existing alternatives production capacity and maintenance capacity (spare parts, software support, and skilled workforce).
- Avoid stranded costs: Include mechanisms to minimize unnecessary premature replacement and “stranded assets,” notably where the affected equipment does not materially increase risk.
- Case-by-case assessment: Condition accelerated timelines on component-level risk assessments and verified availability of adequate alternatives (quality, quantity, and industrial capacity).
- Monitoring and adjustment: Provide for periodic review of transition timelines based on market capacity, deployment constraints, and evolving threat assessments.
- Focus on the most important entities, identified under CER and not the NIS 2 entities.