

The European Commission's Cybersecurity Act 2 Proposal

An Impact Assessment of Title IV

About this study

In light of the European Commission's proposal for a revised Cybersecurity Act, Connect Europe asked Assembly to conduct an impact assessment of measures to restrict the use of so-called high-risk vendors (HRVs) in telecoms networks, including the implications of a mandated rip-and-replace process for operators.

Research correct as of July 2026.

About Assembly

Assembly produces custom and subscription-based research on regulatory, policy, and legislative developments in communications markets and the digital economy.

For more information visit assemblyresearch.co.uk

Disclaimer

This study was commissioned by Connect Europe on behalf of European telecoms operators (i.e. full members of the association only). The analysis, findings, conclusions, and opinions expressed are independently researched and authored by Assembly, and reflect the views of the authors alone. The client has not exercised any editorial control over the substance of the report, its conclusions, or recommendations. Assembly retains full independence in its research methodology, analysis, and editorial judgement.

Contents

Executive Summary	3
Background	9
Impact on Network Operations	13
Impact on Legal and Regulatory Certainty	16
Impact on Competition	25
Impact on Investment	31
Impact on Consumers (End Users)	36
Impact on Sustainability	41
Compensation Mechanisms	43
Assessment and Conclusions	47
Annex	49

List of figures and tables

Figure 1: Toolbox progress across Member States

Figure 2: Shares of the European telecoms equipment market

Figure 3: European telecoms capex

Figure 4: Europe's mobile investment gap

Figure 5: Monthly CPI for wireless telephone services

Figure 6: Comparing mobile network quality

Figure 7: Comparing 5G coverage

Table 1: Implementation of the Toolbox across Member States

Table 2: Impact assessment of the CSA2 proposal

Table 3: The UK's designated vendor requirements and timeframes

Executive Summary

The European Commission (EC) has published its plans to revise the EU's Cybersecurity Act (CSA). Under the guise of improving security, resilience and harmonisation across Member States, the 'CSA2' would significantly strengthen measures contained within the existing 5G Security Toolbox, transforming them into mandatory and costly obligations for Europe's operators to fulfil. Notwithstanding legal and constitutional questions regarding the EC's ability to implement the regulation, we find fault and concerns with various aspects of the proposal, including the potentially harmful competitive and investment implications for the region's telecoms industry, which would impact end users in the form of poorer network quality and delayed upgrades.



The CSA2 would single out the telecoms sector for specific and far-reaching treatment

By regulating telecoms in a sector-specific way, the proposal would create a marked imbalance with other sectors that are equally critical to European infrastructure but are otherwise addressed through more uniform, horizontal frameworks. This risks imposing disproportionate obligations on telecoms operators while departing from the technology- and sector-neutral approach reflected in other EU cybersecurity and critical infrastructure regulation.



The proposal would apply the most extreme measure uniformly across Member States

It replaces the current 5G Toolbox, which provided a graduated set of options, and defaults to a full rip and replace, the strictest measure. While the Toolbox was designed with national specificities in mind, the CSA2 proposal would move to the most extreme option at the EC's disposal, which would directly apply to all Member States uniformly. It also does not recognise the progress that has been made, with 18 Member States having taken some form of binding measure to implement the Toolbox, while many have already established risk management frameworks through transposition of the NIS2 Directive into national law. The proposal also goes beyond the scope of the Toolbox, which only applied to mobile networks, potentially extending vendor restrictions to fixed and satellite, despite the lack of dedicated risk assessments.



The EC's proposed timelines ignore reality

Disruptions to network operations would be unavoidable as operators face lengthy timeframes for receiving planning permissions (which can take up to two years) and acquiring the necessary qualified workforces for the rip-and-replace process. There is an "intense gap" for specialist telecoms engineers across the bloc. A rip-and-replace process would intensify the demand for such specialists, spreading them thinly throughout Member States, potentially leaving some operators without the necessary workforce for extended periods of time. Not only would these delays make it impossible to comply with the obligation to rip and replace network equipment, but they would leave end users either disconnected or with degraded services at different points throughout the process.



The CSA2 has not been developed in line with regulatory best practice

It does not sufficiently take into account the views of, and impacts on, the telecoms sector, representing a constant source of financial, technological and political risk for operators. With national security matters the explicit responsibility of Member States under the TEU, the CSA2 is built on questionable legal foundations, failing to adhere to vital principles of conferral, proportionality and subsidiarity, while the use of secondary legislation would centralise decision making powers away from Member States towards the EC. The CSA2 also conflicts both with the EC's simplification agenda by expanding the EU's cybersecurity rulebook and with the DNA's investment objectives through the costs a bloc-wide rip-and-replace mandate would impose.



The proposal contradicts its own stated principle and goal of a diverse supply chain

It references multi-vendor architecture as a risk-reduction strategy yet, by narrowing the mobile supplier base to effectively two (or one in parts of fixed), it undermines vendor diversity and paradoxically creates a new concentration dependency – increasing systemic risk rather than reducing it. Dramatically reducing the number of competitors in the supplier market risks weakening resilience through a more vulnerable supply chain and potential price increases, with remaining vendors facing lower competitive pressure. This would likely lead to higher costs for operators, which could leave no other choice than to rein in investment. Reduced supplier competition could have a negative impact on innovation too by slowing the pace and intensity of R&D.



In a heavily regulated and commercially challenging market, the CSA2 would harm the very players it seeks to protect

The proposal would impose significant costs that operators would largely have to absorb, impacting their collective investment capacity. Despite strong progress against the Digital Decade targets, operators will still need to make a significant capex commitment to deliver EU-wide coverage of 5GSA and fibre networks. The CSA2 would hamstring industry's ability to reach that goal, particularly if equipment prices rise. Rural and remote communities may be disproportionately affected given the business case for deployment is already less attractive, with resources focused on compliance and replacement activities rather than further network expansion.



An EU-wide rip-and-replace scheme would have significant environmental impacts

Site visits require both transportation and energy, which are already carbon intensive, and as multiple visits would be needed for each site, the carbon footprint of the process would quickly accumulate. Operators would also have to remove equipment from their networks that is still within its useful life and either discard it, which would generate substantial amounts of e-waste, or recycle it, which would require specialised recycling teams. Additionally, as the rip-and-replace process would be extremely cost intensive, funding would likely be directed away from sustainability initiatives or targets.



A rip and replace would leave consumers with degraded and disrupted services for an extended time

The UK's network coverage and quality have consistently scored below most, if not all, of its European peers following its rip and replace. This shows that in the wake of a rip and replace, consumers are left with worsened existing services and a delay to their access to services driven by newer technologies such as 5GSA, and in the future, 6G. Consumers would feel these impacts in urban and rural areas with delayed rollouts, as a result of labour shortages for qualified engineers, likely having knock-on effects for the adoption of 5G FWA and other advanced connectivity use cases.



Compensation is unlikely to come from the EC, meaning operators will be burdened with the full cost of a geopolitical policy decision

Although various operators have legally challenged rip-and-replace mandates in Europe, only one has resulted in the court recognising the right to compensation (TDC NET in Denmark). Therefore, if funding were to be made available, this would most likely have to come at a national level. Nevertheless, mandating extensive technology removals even with public funding would result in the imposition of unprecedented financial, operational and service level burdens on operators.

Assessment and conclusions

Our impact assessment shows that the telecoms industry would face several significant, horizontal impacts under the current CSA2 proposal. For each impact, we have assigned either a limited, material or substantial status, with most falling into the substantial category.

Network Operations	Substantial
Legal and Regulatory Certainty	Substantial
Competition	Substantial
Investment	Substantial
Consumers (End Users)	Material
Sustainability	Limited

The most extreme measure being applied uniformly across Member States leaves little room for national approaches to flex to their individual situations and should only be considered as a last resort. Countries with more HRV equipment are likely to require more time for replacement. The EC’s proposed timelines ignore reality, especially for mobile networks. In some Member States, such as Germany, acquiring the necessary planning permissions and site certifications can take up to two years alone, which would significantly delay any rip-and-replace process. These problems are only exacerbated by the bloc’s labour shortage of qualified telecoms engineers, the demand for whom would limit the speed at which operators can replace network equipment. These extended rip-and-replace processes would impact consumers too, leaving them with degraded and disrupted services. The UK’s rip-and-replace process has shown the impact of this degradation, with its network coverage and quality scores consistently falling below most, if not all, of its European peers.

The proposal contradicts its own stated goal of a diverse supply chain. By requiring operators to remove all HRV equipment, they will be left with little choice for their equipment suppliers. This would limit supply chain diversity in existing networks that are being replaced and in new deployments. The remaining options also may not be as sustainable, with the equipment that it would replace often particularly energy efficient. An EU-wide rip-and-replace scheme would likely have wider environmental impacts too. Site visits require transportation and energy, which are already carbon intensive, and with multiple visits needed, processes' carbon footprints will quickly accumulate.

The cost to operators would undoubtedly be one of the most significant impacts of the proposal, with future network investment likely to suffer as a result. Without that network investment, the wider economy would suffer too. European businesses are set to benefit from the adoption of a variety of innovative services and tools that can only be made possible by the high-speed connectivity that new network deployments can provide. Delaying these deployments would come at a significant productivity cost as businesses miss out on the opportunities that would be made available to them with better connectivity. Despite these problems, compensation from the EC is unlikely, meaning operators will have to shift their resources away from investing in necessary new very high capacity networks.

Background

Proposal for a Regulation and what it entails

On 20 January 2026, the EC set out a package of reforms on cybersecurity, including its proposal to revise the EU's Cybersecurity Act (CSA) to increase resilience and harmonisation among Member States.¹ The proposal would essentially shift the recommended but ultimately voluntary measures contained within the 5G Security Toolbox² into mandatory obligations, following the EC's complaints that implementation has been slow and fragmented. Operators would be obligated to 'rip and replace' network components from high-risk vendors (HRVs), likely to include Huawei and ZTE (although they are not named explicitly in the proposal, they were specified by the EC in a progress report on the Toolbox³), within 36 months of the revised CSA entering into force and the publication of the list of HRVs for mobile networks. The EC will also make risk assessments for the fixed and satellite sectors, which will determine the phase-out period for HRVs in these networks.

The existing 5G Security Toolbox and its implementation status by Member States

According to the EC's second progress report on implementing the Toolbox in 2023, only 10 countries had implemented actual restrictions on HRVs.⁴ Since then, according to our *Vendor Restrictions* benchmark, a total of 18 Member States have implemented some form of legislation to empower them to restrict high-risk vendors, with 13 requiring operators to either remove HRV equipment or blocking them for procuring it. Four more countries have adopted non-binding guidelines or declarations advising operators to avoid HRVs – see *Table 1*.⁵

Assembly

Table 1

Implementation of the Toolbox across Member States

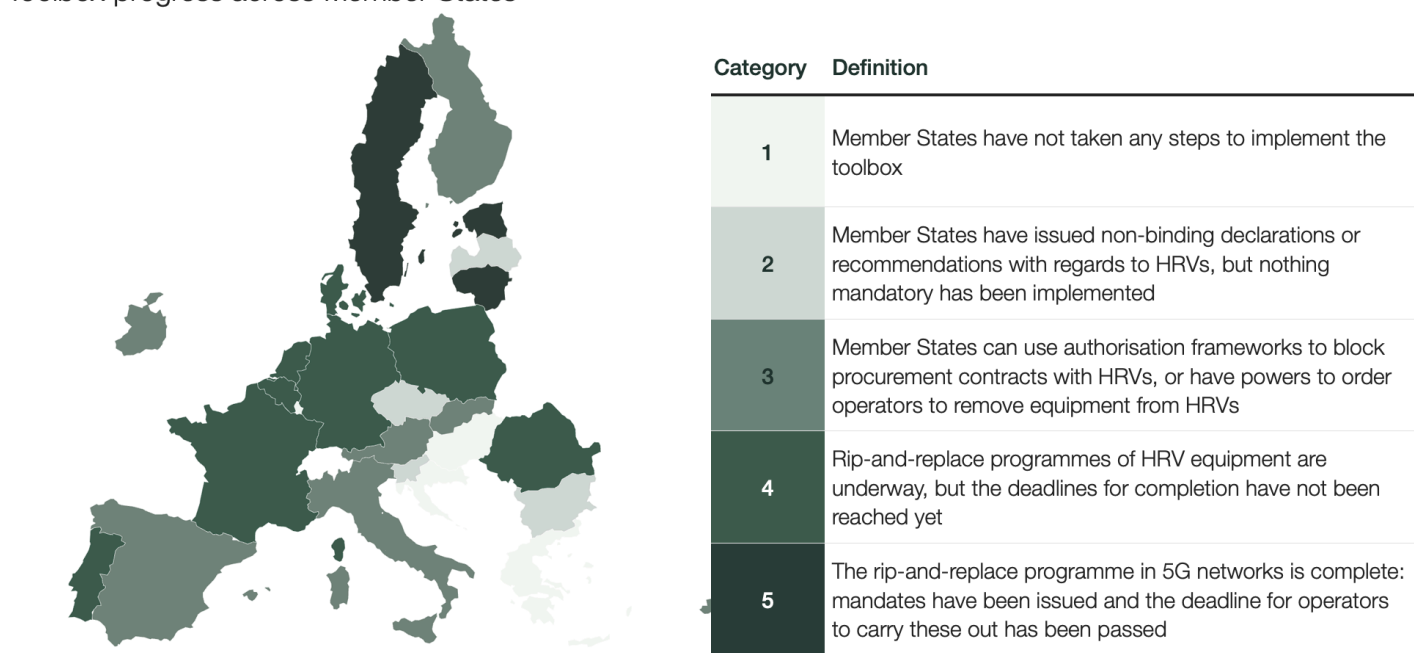
Country	Date introduced	Mandatory or non-binding	Vendor(s) affected	Part(s) of the 5G network in scope	Deadline(s) for removal
Sweden	October 2020	Mandatory	Huawei, ZTE	Core, access, transmission, service, maintenance	January 2025
Lithuania	May 2021	Mandatory	Any vendor	Whole network	December 2025
Estonia	November 2021	Mandatory	Any vendor	Whole network	2025 (5G networks) 2029 (4G networks)
Germany	July 2024	Mandatory	Huawei, ZTE	Core, management systems in access and transport networks	2026 (core) 2029 (access and transport)
Denmark	April 2023	Mandatory	Huawei	Transport	January 2027
Belgium	February 2022	Mandatory	Huawei, ZTE	Core, RAN, transport	2028 (core, RAN) 2031 (transport)
Romania	June 2021	Mandatory	Huawei	Whole network	2029 (core) 2031 (whole network)
France	August 2019	Mandatory	Any vendor	RAN	2028 (critical areas) 2032 (less sensitive areas)
Poland	April 2026	Mandatory*	Any vendor	Whole network	4 years (critical) 7 years (whole network)
Netherlands	March 2020	Mandatory	Any vendor	Core, critical (and adjacent) components, management environments, security elements	No deadline
Italy	March 2012	Mandatory	Any vendor	Critical infrastructure	No deadline
Finland	December 2020	Mandatory	Any vendor	Core, base stations	No deadline
Portugal	May 2023	Mandatory	Any vendor	Core, access, transport, management, interconnection	Not publicly available
Cyprus	August 2020	Mandatory	Any vendor	Critical infrastructure	No deadline
Austria	November 2021	Mandatory	Any vendor	RAN, core, management	No deadline
Ireland	March 2023	Mandatory	Any vendor	Critical infrastructure	No deadline
Spain	March 2022	Mandatory	Any vendor	Critical infrastructure	No deadline
Slovakia	January 2018	Mandatory	Any vendor	Critical infrastructure	Between 2-5 years*
Bulgaria	October 2020	Non-binding	Huawei, ZTE	Not specified	No deadline
Czechia	February 2022	Non-binding	Any vendor	Not specified	No deadline
Latvia	February 2020	Non-binding	Huawei, ZTE	Not specified	No deadline
Slovenia	August 2020	Non-binding	Huawei, ZTE	Not specified	No deadline

Notes: *Upon issuance of an administrative decision

Source: Assembly's Vendor Restrictions Benchmark (Cybersecurity Tracker)

See *Annex* for country level detail on HRV restrictions in Europe. Implementation of the Toolbox has not been consistent across Member States – see *Figure 1*. While some countries (Sweden, Estonia and Lithuania) have now completed a rip-and-replace process, other countries’ measures have been less strict, with Ireland and Italy relying on prior authorisation frameworks to block future procurement contracts with HRVs rather than requiring operators to remove this equipment. In other countries (Bulgaria, Czechia, Latvia and Slovenia), these measures have consisted of non-binding recommendations or declarations, but have not been meaningfully translated into mandatory regulations.

Figure 1
Toolbox progress across Member States



Source: Assembly

The CSA2 proposal does not account for national specificities

Since the Toolbox was launched in 2020, the majority of Member States have taken steps to implement it in a framework that aligns with their own national priorities and security risks. The EC’s proposal for the CSA2 does not recognise the progress that has been made. Instead, the EC moves to the most extreme option at its disposal, which would directly apply to all Member States uniformly. Further, the proposal significantly expands the scope of vendor restrictions beyond mobile networks to fixed and satellite infrastructure, despite there being no previous EU legislative basis for such measures and no sector-specific impact assessments demonstrating their necessity.

Assembly

Member States have not implemented the Toolbox in lockstep, and while countries have varying proportions of HRV equipment left in their networks, this is to be expected. The EC's argument for a stricter, blanket measure is that Member States have been too slow to remove HRVs themselves. However, at least 11 Member States have started the rip-and-replace process and three of these have completed it, making stricter regulation an overstep.

Ultimately, security is a key priority that Member States are committed to, demonstrated by the various measures taken to implement the Toolbox. However, this does not mean that all European countries need to conduct rip-and-replace schemes for all components of networks indistinctively, and the disruptive impacts of such a scheme would be lessened if it did not occur simultaneously across the region. Additionally, national security is not within the EC's competences, making this an overreach.

Impact on Network Operations

IMPACT ASSESSMENT

Limited	Material	Substantial
---------	----------	-------------

A rip-and-replace process would make service disruptions unavoidable, leaving end users either disconnected or with degraded services. Labour shortages and the complex array of planning permissions, site access permits and vendor selection procedures that operators would have to carry out before any physical works can start would make the EC’s proposed timeframe for a mobile rip and replace hard to meet.

Labour shortages

Equipment replacement would require qualified specialist engineering workforces across the EU, but labour shortages in this area present a challenge that would likely delay rip-and-replace processes, making the EC’s timeframes hard to meet. The European Centre for the Development of Vocational Training’s (Cedefop) TalentGap Index shows there is an “intense gap” for information and communications technicians and technology professionals, as well as science and engineering professionals.⁶ A mandated rip-and-replace process would increase demand for these specialists, which could lead to two problems:

- 1. Subcontractors may raise their prices due to the higher demand for their services, adding to the costs of the process for operators. These additional costs could limit operator investment into the deployment of new networks with the objective of expanding coverage, whether that be on the mobile or fixed side, and could result in upwards financial pressure on the telecoms sector at a time when it is already facing low earnings; and
- 2. The high demand for a small number of qualified subcontractors could intensify the existing labour shortage.

A further indirect impact is the risk of brain drain, particularly from certain parts of Europe. Specialists could be recruited away mid-programme by larger operators, potentially disproportionately impacting the speed and cost of rip-and-replace processes for smaller operators.

Even in the US, where the rip-and-replace process has been publicly funded, operators have still been delayed by labour shortages. According to the FCC, in the 2025/26 period, approximately 15% of funding recipients reported facing challenges with labour shortages, impacting their ability to complete the rip-and-replace process in their allotted, one-year timeframe.⁷ This highlights how the lack of qualified and local workforces could delay a similar process in the EU.

Planning permission and permits to access affected sites

Alongside the limited workforce available to carry out the replacement works, operators face delays in acquiring the necessary planning permissions and site access permits for these works. We expect that for the most impacted operators, the complete rip-and-replace process could take between 7-10 years and between 3-5 years for less impacted operators. In either situation, the EC's 36-month timeframe for a mobile rip and replace seems unachievable.

Planning permissions and permit requirements will differ between Member States, but are broadly similar across the EU. Site-level, local and landlord approvals can take anywhere between 6-12 months per site and potentially up to two years for sites in protected or dense urban areas. Antenna certifications can similarly take over a year, with some countries requiring in-person visits from relevant regulators before certain works can go ahead. In Germany, antenna replacements or modifications may require a new or amended site certification from the Federal Network Agency (BNetzA), depending on whether relevant technical parameters change.⁸ At its fastest, this process may only take three months. However, additional steps, such as physical site reviews, multi-user site alignment and regulator processing, can all significantly increase the length of the process. All operators, regardless of country, will need to go through their own vendor selection processes when deciding what to replace HRV equipment with. These processes must precede any replacements and our discussions with industry indicate these can take between 1-2 years on their own, further adding to delays.

The US' rip-and-replace process has seen similar disruption. The FCC has reported that approximately 11% of rip-and-replace funding recipients have challenges with permitting issues. The FCC's report details that in June 2026, six years on from the US Government's designations of Huawei and ZTE as national security threats, only 53 of the country's 126 priority rip-and-replace projects had been completed. This evidence further highlights that the EC's proposed 36-month timeframe for removing HRV equipment from mobile networks is unrealistic.

Possible disruption to end users' services and quality from a rip and replace

End users will be impacted by service disruptions and quality degradation such as reduced throughput, higher latency, dropped calls and weaker indoor coverage during replacement activities. Ofcom's Communications Market Reports highlights this, showing that customer satisfaction with mobile service signal strengths and reception has fallen from 85% in 2020 (when the UK Government introduced its HRV ban), to 80% in 2026.⁹ In the UK, the Government recognised that replacements in core and full fibre access networks could lead to service outages and disruptions for users.¹⁰ Although each time a network is replaced, the individual local service disruptions may be short, the cumulative impact of repeated interventions across thousands of sites over many years represents a material risk to end user experiences, especially in critical cases where hospitals or the emergency services' communications may be impacted.

Impact on Legal and Regulatory Certainty

IMPACT ASSESSMENT

Limited	Material	Substantial
---------	----------	-------------

While the EC’s proposal for a revision of the CSA was expected, its approach to the CSA2 has been anything but conventional. Developed with limited external input, the draft’s provisions on supply chain security for telecoms are stricter than expected, raising questions over alignment with the principles of proportionality, transparency and subsidiarity, as well as with existing EU-level policy and competences. The extensive use of secondary legislation makes for significant uncertainty, while moving decision making power from Member States to the EC.

Assessment of the proposal and the shift from the 5G Toolbox

The 5G Toolbox aims to encourage (while accounting for national circumstances) a concerted approach from Member States to protecting network, economic and societal security through the mitigation of risks and avoidance of supply chain dependencies. In line with this objective, operators seek to ensure security and resilience through comprehensive technical, operational and organisational measures, including the multi-vendor strategies recommended by the Toolbox itself. 18 of 27 Member States have now implemented some form of legislation to empower them to restrict HRVs, with 13 requiring operators to either remove HRV equipment or blocking them for procuring it, with visible progress made between the EC’s two progress reports. It is questionable therefore how the EC has arrived at the vendor restrictions proposed within the CSA2, with concerns as to their respect for principles of conferral, proportionality and subsidiarity.

The principle of conferral is enshrined in Article 5 of the Treaty on the European Union (TEU), which allocates powers between national and EU institutions, and limits EC competences to those granted to it by Member States under EU Treaties. Crucially, this does not include national security, which the TEU underlines “remains the sole responsibility of each Member State”. By potentially encroaching on an exclusively national competence, the CSA2 is positioned on precarious legal foundations, with it challenging to align the regulation and the EC’s ability to adopt and enforce it. The EC states that the proposed measures within the CSA2 are proportionate as they do not go beyond what is necessary to achieve its policy objectives, and that they do not impede any further national action on security. It also indicates that they comply with the principle of subsidiarity because it was accounted for when adopting the CSA, and because national solutions since have not achieved “market-wide trust and coordination”.

In this sense, the requirements to remove HRVs ignore steps already taken by governments to secure telecoms supply chains and would only respect the competence of Member States for national security matters should they go further than the baseline expectations imposed by the EC. While such a minimum harmonisation logic may be appropriate in areas of shared competence, it may be incompatible in a context where Member States retain the sole responsibility for their respective territory. More fundamental still is whether the EC can intervene at all. As things stand, the CSA2 would risk the EC attempting to go beyond the scope of its competences in order to limit Member States’ ability to administer their own national security.

BEREC’s view on the CSA2

The Body of European Regulators for Electronic Communications (BEREC) has found that the proposal raises concerns regarding “business impact and proportionality”.¹¹ For example, forcing the rapid replacement of still non-amortised equipment could impose a significant financial burden on operators and would not take into account national realities, such as the markets with less diversity of suppliers or a strong dependence on certain technology. BEREC considered that the CSA2 should remain “ambitious but achievable”, and would benefit from amendments to ensure that it is proportionate, reflects industrial realities and preserves resilience.

The EC also states that the framework for removing non-trusted suppliers foresees gathering evidence of what constitutes key assets and what measures would be proportionate and necessary to ensure de-risking of critical supply chains. That the proposed obligations for telecoms have not (yet) been grounded in sufficiently robust, up to date, evidence-based risk assessments (under Article 99) calls into question their validity ahead of those being completed. Associated economic impacts assessments (under Article 103) should account for the full range of costs of a given intervention, ensuring that it is only pursued where absolutely necessary to mitigate the effects of an identified security threat. As also highlighted by BEREC, the impacts of large-scale vendor replacement obligations remain uncertain and underestimating them carries risk, including for competition, investment capacity and even delays to achieving the Digital Decade connectivity targets.

Analysis of key Articles

Title IV, which spans Articles 98-117, of the CSA2, outlines the framework for identifying and addressing non-technical risks within “sectors of high criticality and other critical sectors”. The EC has been vocal that it may feel compelled to introduce regulation if it does not consider that Toolbox recommendations have been implemented sufficiently widely or fully. Henna Virkkunen (EVP for Technological Sovereignty, Security and Democracy, EC) has admitted to not being “satisfied at all” with the amount of network equipment still supplied by HRVs.¹² However, although the possibility of the EC introducing mandatory obligations has been signposted, Title IV is surprising on a number of counts, not least for its severity and complexity, the lack of transparency in how it has been developed and the degree of centralised power that it would give the EC.

It appears generally excessive and unusually rigid, and may therefore be out of step with the actions required to achieve the intended security objectives of the revised regulation. In atypical fashion, the draft text has also been developed without the meaningful and valuable collaboration of the stakeholders they would primarily affect.¹³ This approach does not align with the participation principle or consultation instrument of the EU’s better regulation guidelines,¹⁴ which would otherwise have helped craft proposals that would support security and resilience while being operationally workable and financially feasible. If approved as worded, Title IV would risk imposing unprecedented burdens on operators, overlooking a more proportionate assessment of risks and security as a Member State prerogative.¹⁵

Article 99

Under Article 99, the EC or at least three Member States may request that the Network and Information Systems (NIS) Cooperation Group – a forum established under the NIS Directive – conducts EU-level coordinated security assessments of key assets, including the main threat actors, risks and vulnerabilities that may affect them, as well as proposes measures (from the set described in Article 103) to address any issues identified. Although it is positive that EC-led assessments would be completed “taking into account the consultation of Member States”, an immediate challenge is that the draft text has been published before they have been undertaken. In October 2019, Member States completed (supported by the EC) a risk assessment for 5G network security, which was subsequently used to underpin the Toolbox. In July 2024, Member States then led the development of a risk assessment report on cyber resilience in the EU’s telecoms and electricity sectors.¹⁶ However, this report is not particularly comprehensive, failing to highlight the main threat actors, risks and vulnerabilities affecting specific assets, nor does it confirm or evolve the findings from 2019. The EC’s misordered sequencing therefore means that potential mitigation measures are not based on robust and up to date security assessments, with the proposal deviating from the risk-based approach of the 5G Toolbox.

Article 100

Under Article 100 of the CSA2, where – as a result of a risk assessment or “other sources” (e.g. such as a public statement made by the EU or a Member State) – it appears that a third country poses serious and structural non-technical risks to telecoms supply chains, the EC should verify the threat posed, taking into account five factors:

1. The existence of legislation requiring reporting on hardware or software vulnerabilities;
2. The existence of practices requiring reporting on hardware or software vulnerabilities;
3. The absence of effective judicial remedies, and independent and democratic control mechanisms;
4. Substantiated information about threat actors carrying out malicious cyber activities or campaigns; and
5. Relevant EU, Member State or international information on security risks.

Where the EC confirms a threat, it can – via implementing acts – prevent companies established in that country from supplying key assets for critical supply chains within the EU market. Basing the designation mechanism on non-technical criteria relating to the third-country governance rather than on proven risks or security failures is therefore concerning for both the firms affected and for European operators, while raising the possibility of trade policy retaliation from the third countries identified. It is essential to ensure that measures addressing non-technical issues do not inadvertently weaken capacity to invest nor to respond effectively to genuine technical and innovative challenges. Further, as implementing acts are binding but non-legislative, this determination process is demonstrably opaque, while potentially not adequately respecting the principle of subsidiarity by overriding Member State frameworks designed to safeguard service continuity and support investment within national contexts.

Article 103

Within Article 103, the draft provisions state that the EC is empowered to adopt implementing acts to prohibit the use of equipment supplied by HRVs. For telecoms supply chains specifically, the proposal would therefore represent a fundamental departure from the risk-based methodology enshrined in the current Toolbox, under which a graduated framework allows Member States to apply targeted mitigating measures to identified security issues. Under the CSA2, a binary HRV designation decision would automatically trigger a market-wide exclusion, with no requirement to demonstrate the harm posed by the supplier in question. Full prohibition and phase-out as the sole mitigation measure for a broad range (if not the entirety) of components in both mobile and fixed networks is clearly disproportionate, with the EC failing to explain that less intrusive alternatives, such as multi-vendor and diversification strategies, certification or access control to network operation, were duly considered and/or would not be comparably effective. Indeed, the EC makes no reference to such interventions within the three supply chain security options presented in its impact assessment, while stating that it discounted at an early stage widening the proposed rules for telecoms to other sectors as this could lead to “disproportionate restrictions with unknown impact”.

Article 104

Article 104 states that the EC should undertake a mapping exercise of equipment vendors, in turn establishing lists of high-risk suppliers based on the designations made under Article 100. Its initial assessments would again not be sufficiently transparent, involving the vendor under review and in some cases a “competent authority” – albeit without any guarantee. The EC’s preliminary findings on the establishment, control and ownership of the relevant supplier would be shared only with the supplier itself, ensuring a lack of broader visibility of, or involvement in, the process from affected stakeholders. The scope for the EC to regularly update the list of HRVs with a view to removing or adding companies makes for a potentially expansive intervention, which may be incompatible with the need for regulatory predictability and stability in long-term investment planning. In practice, operators are being asked to make commitments to vendors whose status could change, affecting the assumptions they can confidently rely upon for long-term technology roadmaps, supplier strategies and investment cycles.

Articles 110 and 111

Chapter II of Title IV, as well as Annex II of the CSA2 set out the scope and measures that would apply to telecoms. In effect, this would move the CSA from a horizontal framework to sector-specific legislation. The scope of the draft text is not appropriately targeted, failing to account for differences in threat landscapes or levels of network criticality. Not all types of equipment are equally sensitive, making a blanket, one-size-fits-all approach unnecessary and disproportionate. In the UK, advice to the Government from the National Cyber Security Centre (NCSC) identified the core as carrying the greatest cybersecurity risk, recommending that equipment from HRVs be removed from it while being limited elsewhere, including in the access network.¹⁷ This tiering of network elements is reflected in the NIS Cooperation Group’s 5G risk assessment from 2019, which only considered core network functions to be “critical” in sensitivity, whereas others were deemed “moderate” to “high”. The CSA2 proposal, however, groups all components as critical without justification as to why some should now move up to the most sensitive level. While this should be revisited, it is also vital that mitigating measures are not uniform by default but commensurate with the level of risk identified and properly justified.

The proposed 36-month phase-out period for HRVs from mobile infrastructure may also be a non-starter from a logistical perspective given operational realities and product lifecycles – as evidence from the US indicates.¹⁸ Further, the EC's suggested use of secondary legislation to determine phase-out deadlines for HRV equipment in fixed and satellite networks would limit relevant stakeholders from sharing their expertise with policymakers. Meanwhile, the future adoption of delegated acts to amend designated telecoms assets and timeframes leaves industry in a state of regulatory limbo without surety and control over its future operations.

Overlap and alignment

According to the EC, the CSA2 would deliver a harmonised regime that reduces the current fragmentation of approaches to telecoms supply chains across Member States, thereby representing a “substantial simplification and modernisation” of the EU's legal framework for cybersecurity. However, it appears that the proposal instead increases the already significant costs imposed by the bloc's digital rulebook (principally via numerous implementing and delegated acts), while introducing further complexity to it. For example, following transposition of the NIS2 Directive, as part of the national cybersecurity strategy, Member States are required to adopt policies addressing cybersecurity in the supply chain for telecoms products and services.¹⁹ In addition, the Cyber Resilience Act (CRA²⁰) is already considered to offer a useful approach to supply chain security (under Article 57), allowing authorities to address non-technical risks to products through targeted and proportionate measures made in consultation with Member States and “relevant economic operators”, rather than HRV designations.²¹ The addition of the CSA2 would therefore mean the EU would have three separate regulations providing for similar means and measures – an outcome that would hardly symbolise simplification.

Further, there is clear misalignment between the draft revisions to the CSA and the proposed Digital Networks Act (DNA).²² While seeing the initiatives as complementary and mutually reinforcing, the EC offers a limited indication of how and/or why this would be the case, other than stating that the trusted supply chain framework envisaged by the CSA2 would apply to mobile, fixed and satellite networks in line with the focus of the draft DNA. More worryingly, the DNA would tie its general authorisation regime (under Article 9) to compliance with cybersecurity rules contained within the CSA2. As the legislative processes for the two proposals are ongoing, it would be unwise to link them so explicitly given that they may both be subject to change. Even when finalised, the cross-reference only adds an unnecessary layer of regulation that serves no purpose.

The DNA also stresses the importance of a “modern and simplified legal framework” that incentivises the transition from legacy networks to fibre, 5G and 6G, and to cloud-based infrastructures. To help meet EU policy objectives, such as industrial competitiveness, security and resilience, the DNA therefore aims to encourage all market players to innovate and invest in advanced connectivity. On more than one occasion, Virkkunen has spoken publicly of the need for regulatory reform to stimulate investment, considering that introducing more rules would not necessarily be the right course of action.²³ The additional obligations and material costs that a mandated rip and replace of HRVs would cause once again underline the degree of misalignment between the two sets of proposals, which were launched just a day apart.

Risks for longer term uncertainty and decision making this precedent would set

Operators face structural legal uncertainty due to the approach taken by the EC, with questions arising as to whether its proposals are sound, or may be considered ultra vires – i.e. they go beyond the powers afforded to the EC under the Treaty on the Functioning of the European Union (TFEU). While the EC considers Article 114 TFEU (which provides for internal market harmonisation) the correct legal basis for the CSA2, the judgements and restrictions it would introduce effectively mirror sanctions, which are typically adopted under the Common Foreign and Security Policy (CFSP) approach through Title V of the TEU. The legal basis matters because Title V TEU gives Members State a veto power over EC-led determinations, whereas Article 114 TFEU would not.²⁴ The CSA2 may therefore be vulnerable from a legal perspective, affecting operators’ clarity as to how the file will progress and the suppliers they can use, while generating broader uncertainty on whether the EC is acting in a constitutional manner.

Secondly, industry faces considerable operational and financial uncertainty as a result of the CSA2. Although the text remains a draft, its drastic proposals (devised without adequate industry consultation) may have already affected business planning, prompting operators to reevaluate long-term investment decisions and adopt a wait-and-see approach to procurement until the final regulation is approved. Come that time, uncertainty would not diminish given the precedent the CSA2 would set. For a capital-intensive sector such as telecoms, with long investment cycles and payback periods, the implementation of a framework perceived as open-ended or subject to further expansion – for example, as a result of periodic reviews of HRV lists or key assets, or applications for exemptions from designations (under Article 105) – could increase cautiousness in the procurement of equipment, reduce investor confidence and complicate network transformation.

Thirdly, should the proposals become adopted in their current form, operators would be at risk of ongoing technological uncertainty. For instance, there are concerns that the wording of Article 98 of the CSA2 leaves the door open to future, incremental restrictions on equipment within the telecoms or adjacent, critical supply chains, as described in NIS2 annexes. This is notwithstanding the fact that while mobile network security has been debated and reflected in the adoption of the 5G Toolbox, the inclusion of fixed and satellite networks in the CSA2 is not based on any holistic prior risk or impact assessment. The scope of the proposals is already far-reaching; however, once a centralised framework is established, the criteria for extending restrictions (via implementing or delegated acts) to additional technologies, including cloud computing, data centres or customer premises equipment (CPE – as implemented in the US²⁶), becomes more unpredictable. Such additional rip-and-replace exercises would come with an entirely different set of challenges – as well as costs.

While the CSA2 conveys upon the EC extensive powers and opportunities to alter the rules of the game at its discretion (e.g. through unilateral risk assessments), it bestows on operators a permanent source of political and regulatory risk that is at odds with multi-year investment cycles and asset management timelines. Should the proposed designation mechanism be approved as worded, it would eliminate barriers in principle to extending restrictions to other vendors, including those currently considered trusted or safe. Such an extension would be effectively facilitated by the requirement under Article 103 for HRV determinations to be reviewed at least every 36 months, with Article 99 also enabling the EC or three or more Member States to initiate a coordinated security risk assessment at any given time.

There is a legitimate concern too regarding the impact that changes in the geopolitical context and/or future amendments to the suite of HRVs could have on perceptions of the predictability of Europe's regulatory landscape and on the rationality and attractiveness of its business environment. A range of foreign operators, private equity firms and sovereign wealth funds currently hold stakes in EU-based operators.²⁶ However, even if not the intention, the precedent set by the CSA2 could have a destabilising effect on these relationships and on the flow of capital into European telecoms infrastructure. This may affect confidence in the market's openness to investment, hampering the long-term benefits for connectivity, resilience and innovation it enables. Further, the nature of the proposed regulation runs the risk of retaliatory measures from countries restricted from the EU market, which, if effected, would affect the bloc's trade policy, economy and competitiveness on the global stage.

Impact on Competition

IMPACT ASSESSMENT

Limited	Material	Substantial
---------	----------	-------------

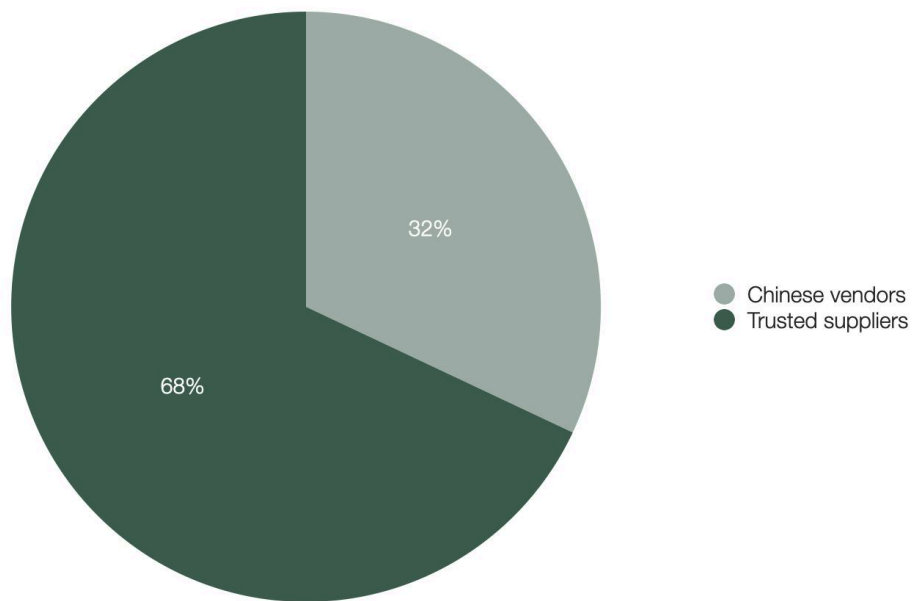
The CSA2 would have an obvious effect on competition in the supply chain by reducing the set of vendors able to access the EU market. While the largest remaining suppliers would be European in origin, structural change could impact security, innovation and equipment pricing – with an increase in the latter disproportionately felt by those operators unable to shoulder burden or currently using a high proportion of HRVs.

Impact on competition in the network equipment supply chain

While Europe is home to a diverse telecoms sector, with 44 mobile operators and 28 fixed operators having 500,000 subscribers or more,²⁷ the upstream network equipment market has long-been dominated by just a handful of vendors, i.e. Ericsson, Huawei, Nokia and ZTE. According to the EC’s impact assessment that accompanied its CSA2 proposal, Huawei and ZTE together account for 32% of the region’s telecoms equipment market (declining from around 40% a decade ago), with other, trusted suppliers (predominantly EU-based Ericsson and Nokia) accounting for the majority – see *Figure 2*.²⁸

Figure 2

Shares of the European telecoms equipment market
%, 2024



Source: Assembly, EC

These four vendors are integrated companies that supply a range of equipment, specialising in the RAN – e.g. antennas, base stations – and the core network markets. They account for the vast majority of the technology supplied to both markets, although other firms have a relatively small presence, including Samsung in the RAN market and Cisco in the core network market. The increasing cloudification and softwarisation of networks has supported (since the late 2010s) the emergence of the Open RAN movement, presenting opportunities for new entrants, including Altiosstar, Fujitsu, Mavenir and NEC – as well as for established suppliers. However, while the NIS Cooperation Group has stated that Open RAN could help mitigate risks in the 5G supply chain by allowing operators to reduce the potential for dependency on any single company,²⁹ the model will require more time and investment to gain further traction in Europe. In certain instances, operators have also opted to rescope their planned Open RAN deployments to consolidate existing vendor relationships.³⁰

Similarly, it appears that the EC is now seeking to readjust its position in respect of diversity of supply within the telecoms value chain, and in turn its approach towards ensuring network security and resilience by limiting operators' choice of vendors. Within the eight strategic measures contained within the Toolbox, the EC recommends that each operator has an appropriate multi-vendor strategy in place to avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile), and to avoid dependency on suppliers considered to be high risk.³¹ It further recommends that relevant authorities and industry collaborate to strengthen resilience at the national level, ensuring that there is an "adequate balance" of vendors in case of an incident. In contrast, the CSA2 would discount less intrusive options, such as multi-vendor strategies, taking the most extreme action with an all-out ban on HRVs.

Result of reliance on a reduced number of vendors, including on price, supply and resilience

The direct impact of the CSA2 proposal (if adopted in its current form) would be to reduce choice in the upstream infrastructure market, requiring industry to rely on a smaller pool of established suppliers – particularly for RAN, core and transport components. This would intensify an already highly concentrated oligopoly situation, if not create a de facto duopoly, with tangible security implications. As outlined by the UK's Telecoms Supply Chain Diversification Council, the connectivity delivered by telecoms networks underpins nearly all aspects of the economy; however, a reliance on a small number of equipment vendors makes the country's networks more vulnerable to supply chain disruption and cyberattacks, and increases the impact should they occur.³²

The EC identified 5G networks as "the future backbone of [Europe's] increasingly digitalised economies and societies".³³ In October 2019, the Member State-led risk assessment for 5G network security (which was supported by the EC) stated that a major dependency on a single supplier increases the exposure to a potential supply interruption, resulting for instance from trade sanctions or commercial failure, and its consequences. It also aggravates the potential impact of weaknesses or vulnerabilities, and of their possible exploitation by threat actors, in particular where the dependency concerns a supplier presenting a high degree of risk.³⁴ Under the EU's regulatory framework for telecoms, operators are required to take appropriate resilience and security measures to mitigate disruptions of their networks and/or services. However, by potentially narrowing the size of the accessible vendor ecosystem, the CSA2 could hinder their ability to deliver against their obligations easily and effectively, prolonging or exacerbating systemic risks associated with over-reliance – especially in the event of network-wide failure – that could lead to customer harm while hampering diversification efforts.

The draft revisions to the CSA could also have significant commercial implications for European operators, coming at a time when both their top and bottom lines are under pressure. By imposing constraints on industry's scope to source necessary network elements, the EC's proposal would place them in a worsened negotiating position with respect to those remaining suppliers. Reduced competition upstream could lead to weakened bargaining power downstream, likely feeding through to higher equipment prices and operator costs over time, as well as less advantageous delivery terms and R&D commitments. Limiting optionality in the procurement process, particularly with a forced, simultaneous replacement at the EU level, could cause demand for approved equipment to surge, potentially compounding the cost of removing certain technology and creating bottlenecks if remaining vendors are unable to supply a sufficient volume of substitute components. Though the EC's impact assessment includes a one-off replacement cost for mobile infrastructure of between €3.4-4.3bn over the suggested 36-month timeline, this estimate does not account for the long-term market effects described, includes proxies due to unavailable data, equates prices across trusted suppliers and HRVs, and makes a general assumption that costs imposed on operators would be "alleviated by new revenues created for trusted suppliers and more trustworthy offerings for citizens".

Ultimately, the economic reality of the EC's proposals is that replacement costs would need to be absorbed either by operators, consumers or reduced investment capacity. In some instances, the upstream impact may be passed on to consumers and businesses via increased retail prices, adding to the effects on reduced service quality during the migration phase. The EC envisages that a full transference of the CSA2's cost impact could amount to between €6.50-8.30 per mobile subscriber over three years. However, the competitive nature of telecoms markets in Europe and the different inputs relied upon by operators ensure that this outcome would not be universal. A sole operator using HRVs in a given Member State may be unlikely to be able to pass through increased equipment prices to end users when its competitors were not without risking a spike in churn rates. Naturally, any upstream price rises would be most keenly felt by those operators with a higher exposure to HRVs, who would have chosen a specific mix of suppliers based on the prevailing regulatory environment, potentially skewing the market by putting them at a disadvantage relative to their peers. As they would be forced to weather a materially larger share of the CSA2's overall cost impact, their competitors would be better placed to maintain focus on investment in network and service innovation.

The effects may also be exceptionally acute for smaller operators that may only operate in one or two Member States, or in smaller population or lower margin markets, that would therefore not benefit from the bargaining power or volume orders to negotiate more cost-effective deals that span the supply of infrastructure to multiple national businesses, or have the financial muscle to shoulder the simultaneous burdens of rip-and-replace programmes alongside higher infrastructure prices. That lack of scale could lead to them experiencing disproportionate harm, affecting the competitive constraint they impose on larger rivals.

A loss of innovation and features specific to Member States

Aside from increased economic dependencies, the EC's proposed CSA revisions could result in a heightened degree of reliance in terms of technology and innovation, disrupting the functioning of the market as it exists today. In the short term, a mandated rip and replace could prevent operators leveraging the capabilities of newly built 5G and fibre networks to develop and commercialise innovative services that create utility for end users. Meanwhile, operators would have a lower choice of vendors, with those that remain potentially not able to instantly replicate the network design for some Member States' planned deployments, leading to an effective stall on 5GSA rollouts while alternatives are developed and launched. In turn, weakened supplier competition could cause a slowdown in the pace and intensity of R&D, feature innovation and standards development that have contributed to global improvements in network quality over recent years, exposing and widening gaps between trusted firms and HRVs. Advanced RAN features such as beamforming, Massive MIMO and energy efficiency algorithms represent examples of the kind of solutions that may be at risk if operators are required to forego certain vendors.

Beyond the immediate impact of a reduction in available suppliers, there are questions about the prospect of alternatives stepping in to fill the void created and to restore competition in the vendor market. In the EU, the Open RAN market remains at a nascent stage, with most operators relying primarily on an end-to-end solution from a single vendor. In April 2021, in the UK, the independent Telecoms Diversification Taskforce recommended that the Government work toward a significant portion of equipment within mobile operators' networks being provided by new suppliers and/or through open architectures.³⁵ The Taskforce considered that 25% by the mid-2020s should be the initial aspiration for operators. While no mandate was handed down to industry, in December 2021, the Government and operators announced a joint ambition for 35% of the UK's mobile network traffic to be carried over Open RAN architectures by 2030³⁶ – a goal later restated within an MoU.³⁷

The delay to the diversification timeline in the UK speaks to the challenge in suitably replacing the presence of established vendors in the supply chain, not least through a technology ecosystem that has yet to fully enter the mainstream. Should the CSA2 leave the door open for restrictions to evolve or expand as/if geopolitical winds change, this could result in additional players from third countries being excluded, shrinking the supplier pool further. The knock-on effects for innovation in European networks could be profound in areas that have no EU-only equivalent at the required scale and maturity, while impacting broader AI and industrial digitisation agendas. It could also discourage operators from committing to the adoption of Open RAN solutions and/or hold back new operators entering the market on the basis of emerging network architectures in the future, preventing the realisation of the benefits that stem from market competition and a diverse vendor landscape.

Impact on Investment

IMPACT ASSESSMENT

Limited	Material	Substantial
---------	----------	-------------

Despite strong progress over recent years, operators will still need to make a significant capex commitment to deliver EU-wide coverage of 5GSA and fibre networks. The CSA2 would hamstring industry’s ability to reach that goal, particularly if equipment prices rise, with rural areas likely to be among the most affected. What is clear is that the EC’s proposal would not provide a boost to infrastructure investment.

Mapping planned and future investments in 5GSA and fibre

Telecoms operators in Europe have continued to spend heavily in terms of fibre and 5G network capex despite facing a tightly regulated, fragmented and flat-to-low revenue growth market environment. Total investment reached close to €65bn in 2024, a slight decrease on the previous year as many operators approach or move beyond the peak fibre capex cycle – see *Figure 3*. Overall investment per capita in the region also remains below global peers, at €118 per person in Europe, compared to €217 in the US, €173 in Japan and €151 in South Korea.³⁸

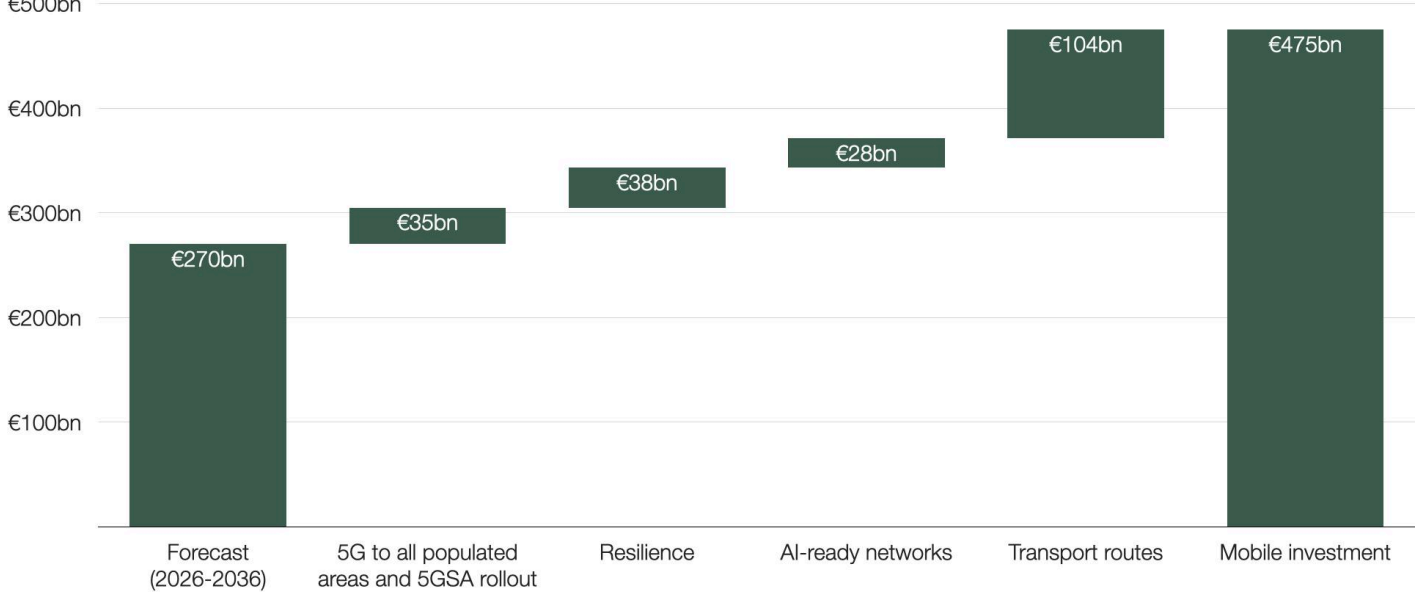
Figure 3
European telecoms capex
€bn, 2017-2024
€70bn



Source: Assembly, Connect Europe

In mobile specifically, operators have invested €141bn in capex since 2021, much of which has been directed to 5G networks. While the region has likely moved beyond the peak of the 5G investment phase, total capex out to 2030 is still projected to reach €106bn.³⁹ Further, operators are forecast to invest around €270bn to maintain the business-as-usual technology upgrade and replacement cycle in Europe over the 2026-2036 period, delivering network modernisation, as well as densification to improve quality, coverage and performance. That said, an incremental €200bn+ is expected to be required to (re)position the region as a “global mobile connectivity leader” – see Figure 4.⁴⁰

Figure 4
Europe’s mobile investment gap
€bn, 2026-2036
€500bn



Source: Assembly, GSMA

Estimates of such an “investment gap” build on the EC’s own research into the likely cost of achieving the Digital Decade targets, which aim to ensure that by 2030, all European households have access to gigabit-capable broadband, with all populated areas covered by a 5G network.⁴¹ In 2023, the EC stated that around €148bn of investment was needed to meet this ambition, with an additional €26-€79bn required to provide high-quality connectivity along the region’s main transport paths.⁴² However, while the EC has argued that full implementation of the Toolbox and the promotion of 5GSA networks are essential for mitigating security risks associated with mobile connectivity,⁴³ it has pointed to the “structural and policy hurdles” hampering Europe’s technological progression.⁴⁴

In its current wording, the CSA2 would therefore represent another regulatory hurdle for industry to tackle, coming at a time when the region is struggling to remain competitive with global superpowers, while running counter to public policy priorities to promote EU investment and growth. As Europe's dependence on connectivity continues to deepen and the risk landscape evolves, the security and resilience of telecoms networks is paramount. The proposals put forward by the EC could weaken the very sector they aim to safeguard, imposing regulatory costs that could materially and adversely impact network deployment, operational continuity and investment planning.⁴⁵ The substantial capex needed to deploy fibre and upgrade sites to 5GSA, and consequently reach more of the population, could suffer, risking Member States slipping down international rankings of network quality. In the UK, in 2020, the Government estimated that the removal of HRV technology would result in an annual net cost to business (predominantly operators) over the 2020-2027 period of £182.3m (€211.6m, in 2019 prices),⁴⁶ while BT⁴⁷ reportedly will have spent £500m (€579m) removing Huawei equipment from its network.⁴⁸ The UK Government has recognised the burden imposed on operators by the Telecommunications (Security) Act 2021,⁴⁹ with the country currently ranking just 57th in the world for mobile network performance and 42nd in terms of fixed.⁵⁰

Impact on rural and remote coverage

A reduction of upstream competition and the resultant unavailability of certain network equipment could be particularly impactful for how operators approach infrastructure rollouts in more rural and hard-to-reach (HTR) areas. Such locations are typically relatively expensive to connect and carry the prospect of inferior returns due to their lower population densities – and as such, often do not reflect the most attractive or pressing regions for deployment. While household coverage of 5G at the EU level stands at 97%, access drops to 89% for households in rural areas.⁵¹ Despite the assignment of coverage-oriented 700MHz spectrum across the vast majority of Member States, operators have nevertheless looked to leverage public funding (e.g. in Spain⁵²) or participate in network sharing agreements (e.g. in Denmark, Finland, Sweden⁵³) as cost-effective ways of expanding availability in remote or underserved regions.

The framework envisaged by the CSA2 could therefore disproportionately affect operators' incentives and capacity to invest in 5G in rural and HTR areas, eroding the viability of rolling out marginal sites in locations where the economics are already poor by comparison. Under a mandated removal of equipment, many resources would be focused on replacement activities and deadlines rather than further network expansion, especially where payback periods are long and the commercial opportunities are less significant or clearcut. The same concerns apply to fixed networks, where investment earmarked for FTTH expansion and transport network upgrades would instead be redirected towards compliance and equipment replacement, delaying connectivity improvements in rural and underserved areas. The business case in such locations could be reduced again by the costs operators would have to bear in effecting their obligations and by any price increases implemented as a result of changed market dynamics. Both would constrain the ability of operators, within the next three and a half years, to reach the >11%⁵⁴ of households that do not have access to 5G services, potentially shifting the burden on to national governments to plug holes in underfunded investment programmes. Alternatively, in light of spectrum licence or other regulatory obligations that require the fulfilment of minimum coverage targets in remote areas, operators could be forced to maintain investment programmes, potentially leaving certain urban and suburban locations behind.

Investment in a less competitive market where equipment is more expensive

All other things being equal, the revised Cybersecurity Act would place disproportionate demands on operators, creating significant financial (and operational) headwinds at a time when they should be provided the appropriate regulatory support to deliver the network investment needed to meet fast-approaching Digital Decade targets as well as underpin the bloc's broader technological and policy ambitions. For example, we anticipate that there could be a sizeable cost increase to operators in the event that prices for like-for-like configurations from trusted suppliers may, in certain tenders, already be higher than those offered by vendors likely to be designated as high-risk. Taken together with the prospect that equipment prices rise within a less competitive market, the economic impact on the telecoms sector could be even more damaging.

While operators share the EC's desire to mitigate network security risks and minimise supply chain dependencies, the draft CSA2 could therefore exacerbate existing challenges faced by industry, layering new regulatory burdens on top of replacement costs and potential price rises, with which bounded resources would struggle to cope without consequence or compromise. In the immediate term, debate over the revisions also creates a hold-up problem, with operators reluctant to advance procurement processes or sign contracts until the final text is agreed, causing uncertainty around future budgets and delaying investment well ahead of a potential contraction in operator capex should the EC's proposals become adopted as they are today.

Impact on Consumers (End Users)

IMPACT ASSESSMENT

Limited	Material	Substantial
---------	----------	-------------

Evidence from the UK shows that the rip-and-replace process can be most damaging to consumers through the poor quality of 5G services and lost productivity benefits. However, the EU’s competitive markets reduce the likelihood of any meaningful impact on consumer pricing.

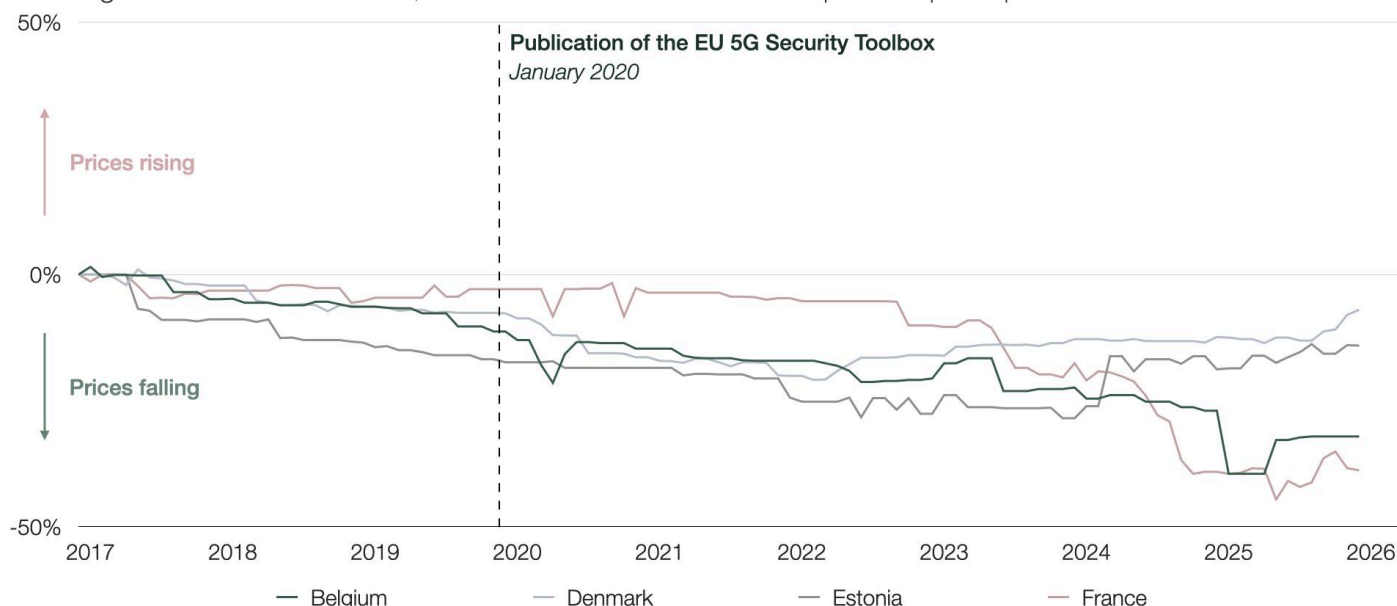
Pricing and consumer bills

The impact of HRV restrictions on consumer pricing would be low due to the highly competitive nature of much of Europe’s telecoms markets, which has tended to result in notable reductions in pricing long-term, as highlighted by CPI statistics from Eurostat for the prices of mobile services over the past 10 years (see *Figure 5*).

Figure 5

Monthly CPI for wireless telephone services

% change since December 2016, Member States with advanced rip-and-replace processes



Monthly CPIs are re-indexed to December 2016 = 0 and displayed as % changes; Sweden is not included due to its CPI data being unavailable

Source: Eurostat

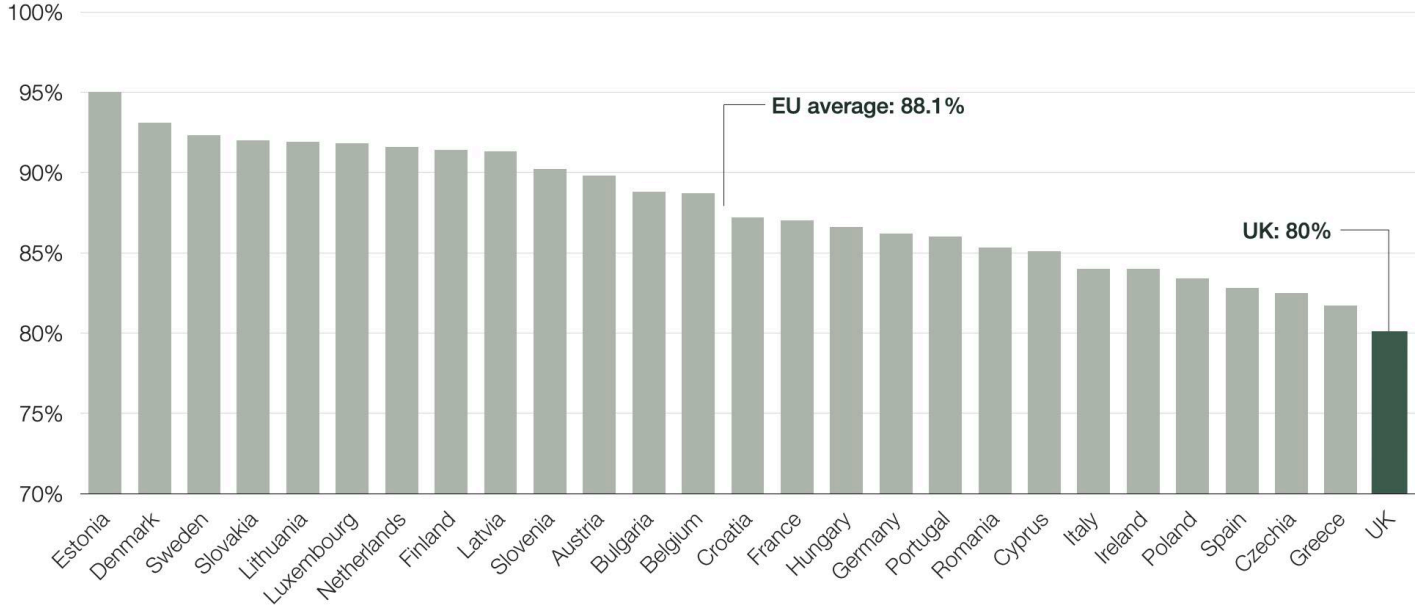
As Figure 5 shows, since the publication of the 5G Security Toolbox, prices have fallen in the studied countries with more advanced rip-and-replace processes. With more notable price falls happening after the implementation of each country's HRV ban, it seems unlikely that the rip-and-replace process would significantly impact consumer pricing.

In the UK, where a ban on Huawei and ZTE equipment was adopted in July 2020, pricing has been similarly unimpacted. According to Ofcom, the average prices of mobile services have been unaffected by the rip and replace. Before the ban, between 2015 and 2020, prices fell by around 22%, while between 2020 and 2025, the decrease was approximately 20%.⁵⁵ As each country example shows, the EU and UK's highly competitive markets have continued to reduce prices for consumers over the years and have remained relatively unaffected by the various vendor restrictions that have been imposed.

Impact on coverage and quality of experience

The impact of the CSA2's proposed rip-and-replace process on mobile network coverage and consumers' quality of experience would be notable. Rip-and-replace processes tend to have a negative impact on mobile network quality as operators are forced to reallocate their resources from network deployment, delaying the rollout of new technologies, most notably 5G. The UK is a prime example of this – it ranks last when compared with all 27 EU Member States for mobile network quality (see Figure 6). Although a number of these Member States have adopted their own HRV restrictions, few are comparable with the UK's.

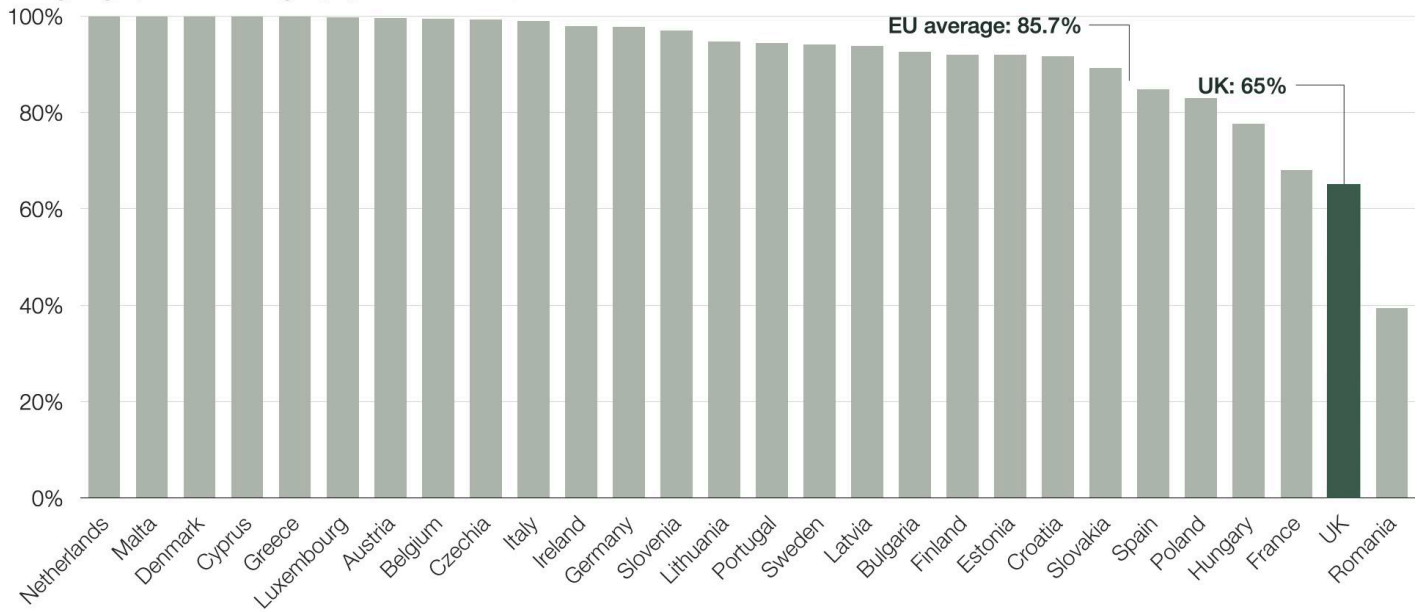
Figure 6
Comparing mobile network quality
Excellent consistent quality (%), EU27 + UK, Q1 2026



Source: Assembly, Opensignal

In the UK, mobile coverage has suffered too. 5G geographic coverage only reached 65% of the country in 2024, compared to an EU average of 85.7% (see [Figure 7](#)).⁵⁶

Figure 7
Comparing 5G coverage
5G geographic coverage (%), EU27 + UK, 2025



Source: EC, Ofcom

These figures show the disruptive impacts of mandated rip-and-replace processes on mobile network quality and 5G coverage. While this impact is clear, the UK is the only country that provides for a strong example. The UK was not as advanced in its 5G rollout when the Government's vendor restrictions were introduced in 2020, worsening the impact by slowing 5G network deployment before it had made any significant progress.⁵⁷

It would be unfair to say there would be a definite, high impact on consumers in every Member State. Rip-and-replace processes may have different impacts in other Member States depending on the characteristics of their mobile networks such as whether they already have wide-reaching 5G coverage and high network quality, or whether or not their networks, particularly in mobile RAN, rely heavily on HRV equipment. In Member States where operators do rely on a lot of this equipment, have lower- to mid-level network quality scores, or less 5G coverage, consumers are more likely to be impacted by a rip-and-replace process through degraded mobile services.

Delayed application and service availability

The potential for newer technologies, most notably 5GSA, to increase capacity means that a delay in its widespread availability is likely to harm EU consumers' and businesses' mobile service quality of experience. Consumers would miss out on the benefits that come from the ability to use extra capacity, especially in highly congested areas, such as stadiums or train stations.

This could significantly impact rural areas too, considering the potential of 5G FWA in providing gigabit-capable connectivity where fibre is not viable. Delaying the rollout of 5G by requiring operators to use their resources on replacing existing equipment rather than deploying new networks therefore risks leaving rural areas behind, potentially worsening the digital divide and hampering digital inclusion efforts.

The 5G rollout would likely be further delayed by the aforementioned labour shortages for qualified telecoms engineers capable of carrying out the rip and replace. Given the assumed impact this shortage will have on the replacement process itself, the impact on the deployment of new networks would likely be even worse. If the relevant engineering workforce is preoccupied with the rip and replace, work on new deployments may suffer. This would further delay the 5G rollout and could have a knock-on effect on the deployment of 6G networks in the future, limiting mobile coverage and network quality for consumers in the long-term.

While the precise timeframe for 5GSA's unique use cases becoming mainstream remains uncertain, a delay to its widespread availability would inevitably affect when consumers will be able to take advantage of the possibilities it brings about. In particular, high-quality remote learning and remote healthcare can be considered 'social equalisers' as they help address shortages of teachers and doctors in underserved areas. The increasing importance placed on remote working and learning further highlights the need for a fast 5GSA rollout. On the entertainment front, consumers would miss out on the newest experiences and ways to enjoy live shows and content, and on the new services on which these industries will focus their future investments.

Impact on Sustainability

IMPACT ASSESSMENT

Limited	Material	Substantial
---------	----------	-------------

HRV equipment will not necessarily be replaced with more energy efficient technology, meaning replacements may not be as sustainable. Additionally, while some of the replacement equipment will consume less energy in the long term, the short-term environmental impacts of wasting functional equipment and the high consumption of raw materials needed to replace it will likely counteract these benefits. Nevertheless, losses in energy efficiency will likely be limited as European vendors have recently been making progress in that regard.

Direct environmental impact of visiting affected sites

In-person visits would be required at potentially hundreds of thousands of sites across Europe, which would have a significant environmental impact. Further, sites would require multiple visits (e.g. surveys before work can begin, equipment delivery, removal and replacement of equipment and subsequent maintenance visits), with the environmental and monetary costs increasing with each visit. With operators conducting this process during the same period of time, there would likely be a spike in carbon emissions across Europe’s telecoms sector as a whole.

The main environmental impacts of site visits would be through transportation and power consumption. A high number of vans and trucks would be required to transport personnel and equipment, as well as heavy vehicles needed for large radio or antenna replacements. This impact would likely be greater in remote areas, with engineers and equipment having to travel further, or even having to use carbon-intensive air travel. Additionally, in rural areas, repeated visits can damage the soil and natural surroundings. Site visits are also energy intensive, with battery-powered tools and portable generators consuming significant amounts of energy. Overall, for a bloc-wide replacement, the cumulative fuel and energy consumption would be significant.

The cost of processing and recycling network equipment

Forcing all European operators to rip and replace perfectly functional equipment from their networks would generate substantial amounts of e-waste. It is also unlikely that there would be a second-hand market for this equipment, meaning a high proportion of hardware would have to be discarded or recycled before its natural end of life. The carbon embodied during the manufacturing, transportation and installation of the equipment would therefore be wasted. Specialised recycling teams would also be needed to process telecoms equipment as it contains hazardous materials; however, it is unlikely that there would be enough specialised teams to carry out this process across Europe within the proposed 36-month period.

Installing new equipment from other vendors would require additional energy and raw materials, which are scarce and finite. An EU-wide rip-and-replace scheme would therefore have a dual environmental impact – wasting these resources during the removal process while simultaneously creating a further surge in demand when equipment is replaced.

Equipment from some of the vendors that would be excluded is also well-known for being highly energy efficient, especially in comparison to equipment from other European vendors, although improvements have been made on this front over the past few years. Replacing equipment with less energy-efficient alternatives would increase the overall carbon footprint of operations in the long term. Equipment from some HRVs also tends to be smaller and lighter than other providers, meaning the entire infrastructure of a site would need changing to account for heavier equipment. This would be an additionally energy-intensive and costly procedure on top of the rip and replace of equipment.

A distraction from other sustainability initiatives

Operators' sustainability efforts may be derailed by a rip-and-replace process. Instead of investing in making networks more sustainable, capital would be diverted towards removing functional equipment still within its useful life. A number of European operators have pledged sustainability targets aiming to cut Scope 1, 2 and 3 emissions by 2030.

However, these targets may be heavily impacted by rip-and-replace measures. First of all, implementing the measures themselves would increase operators' carbon footprints. Secondly, the capital required to carry out this process would direct resources away from sustainability measures. There could also be knock-on effects, such as operators' reduced expenditure on innovation. This could result in a delay in the deployment of fibre networks, which are more sustainable and energy-efficient than copper. Therefore, the CSA2 does not align with European sustainability targets.

Compensation Mechanisms

Experience from countries where rip and replace has been implemented

The proposal as it stands does not mention any form of funding, compensation or redress to be offered to operators having to undergo a rip and replace. Operators will therefore face a significant financial burden, which will reduce the amount they can invest in expanding or improving their services. In addition, where foreseen, any compensation mechanism should be designed in a technologically and competitively neutral manner, and should not create undue advantages for operators that maintained HRV equipment for longer periods compared to operators that had already undertaken mitigation or replacement measures at their own expense.

The US remains the only country to provide compensation for rip-and-replace mandates. Following the FCC's 2020 designation of Huawei and ZTE as national security threats, it launched a \$1.9bn (€1.6bn) reimbursement programme in 2021 for operators with less than 10m customers. However, this was not enough, and the 2024 National Defense Authorization Act (NDAA) added \$3.1bn (€2.7bn) to support the removal of at least 24,000 pieces of Huawei and ZTE equipment, bringing total public funding to nearly \$5bn (€4.3bn).⁵⁸ Most recently, in June 2026, the FCC said that the funds raised from a spectrum auction will be mainly used to fund rip-and-replace processes.⁵⁹ The auction raised more than \$3.5bn (€3.1bn), with the FCC noting that up to \$3.3bn of this will be used to cover funds borrowed to support the programme.

Funding challenges have led to severe delays. By May 2025, only 34 of 126 recipients had completed the process, despite a deadline extension to May 2026.⁶⁰ The FCC's June 2026 progress report showed only 42% completion.⁶¹ With less than half of recipients managing to complete this process five years after funding was initially granted, the EC's proposed three-year timeline for European operators – who lack similar funding – seems highly unrealistic.

Other countries that have mandated rip-and-replace schemes without offering funding include the UK, Canada and Japan. Aside from the US, there is not a precedent to compensate operators for rip-and-replace mandates. In the EU, the EC left the question of compensation unanswered, leaving legislators and Member States to address the issue.

Ongoing legal cases

In various countries there are ongoing legal challenges to rip-and-replace measures. Only three lawsuits have been resolved thus far, with only one in which the court recognised the right to compensation in Denmark.

Denmark

In Denmark, TDC NET has been the only company ordered to remove Huawei equipment from its central transport network by the Centre for Cyber Security (CFCS) under the Telecommunications Security Act. In 2023, TDC NET stated that it would comply with the CFCS's decision but wanted a court to clarify whether it is entitled to compensation, requesting DKK195m (€26m). On 24 June 2026, the Eastern High Court recognised that while the CFCS's ban was not unlawful, it constituted expropriation, as TDC NET had been using Huawei equipment in good faith since 2011.⁶² Expropriation compensation was set at DKK80m (€10.1m). The High Court acknowledged that part of the reason that it granted expropriation compensation was because restrictions only targeted TDC NET. This case could be brought to the Supreme Court in Denmark, meaning that the High Court's decision may not be final, however it does recognise that operators should not bear the full cost of policy-driven equipment replacement measures.

Estonia

In Estonia, Elisa asked the CJEU in May 2024 to provide a ruling on a number of questions, including whether the country's Electronic Communications Act – and whether the vendor restrictions it introduces – is aligned with the EEC and other EU law. Elisa also argued that it should receive compensation for having to undertake a rip-and-replace process. The case is still pending, but in March 2026, Advocate General Tamara Cápeta published an opinion, stating that Member States may, on principle, exclude telecoms equipment on the basis of national security risk.⁶³ However, the AG also highlights that this decision must involve a specific risk assessment of the use of the intended equipment. The opinion also states that operators will not generally be entitled to compensation unless the national court finds that it entails a disproportionate burden. This is not binding, but the CJEU does often follow the opinions of AGs in its rulings.

France

In 2023, Bouygues Telecom and SFR launched legal action against the French Government over costs incurred in the removal of Huawei equipment from their networks. Huawei's radio equipment was not compatible with that of other vendors such as Ericsson and Nokia making replacements more costly and disruptive. The operators are more reliant on the vendor than competitors Free Mobile and Orange, and Bouygues Telecom claimed it would expect a cost burden of €82m with 3,000 antennas needing replacement.⁶⁴ In August 2023, the operators dropped their suit in exchange for the Government pushing back the deadline for removal in 'less sensitive' areas to 2032.⁶⁵

Netherlands

In 2023, Odido legally challenged the removal order and the Government's decision not to compensate operators. This was rejected by the Rotterdam District Court in October 2023. Odido then lodged an appeal before the Trade and Industry Appeals Tribunal (CBb), which confirmed the ruling in March 2026, also determining that Odido would not be eligible for compensation for damages because the extent of the damage falls below the applicable threshold.⁶⁶

Portugal

In April 2026, Portuguese operator MEO launched legal action against the Government's decision to effectively ban Chinese equipment from 5G networks. It is seeking €82m in damages, arguing that the restrictions required it to make substantial changes to its 5G network infrastructure, which led to significant unexpected costs and operational issues.⁶⁷ Huawei is also legally challenging the ban through the Lisbon Administrative Court.⁶⁸ There has been no outcome to either of these challenges.

Romania

Huawei legally contested the Government's decision to ban them from 5G networks in April 2024, stating that an objective assessment had not been carried out. In April 2026, Huawei obtained the referral of the Constitutional Court (CCR) regarding the possibility of the unconstitutionality of Law 163/2021.

What alternative support could look like

Apart from the US, governments have so far been reluctant to offer direct compensation or funding for operators undergoing rip and replace. However, there are other ways that support could be offered. To mitigate the impact on consumers and reduce business disruption, national governments could provide funding to go towards innovation rather than direct compensation rip-and-replace programmes.

In the UK, the Government invested £250m (€289m) in its Open Network R&D Fund, which aimed to accelerate the development of open interface architectures such as Open RAN.⁶⁹ The programme ran until March 2026, and was intended to support 5G network supply chain diversity after Huawei was banned from the networks. Member States could offer similar funding to promote the development of 5G networks without directly funding rip-and-replace schemes. This would also provide an opportunity to encourage vendor diversification, which the EC notes in its proposal as one way to reduce risk. However, multi-vendor approaches do not always reduce prices and improve efficiency, and it is often more cost effective for one vendor to supply equipment that matches an operator's specific requirements rather than using multiple vendors. Additionally, the diversity of European telecoms markets means that a multi-vendor approach will be more suitable in some regions than others. Therefore, this approach should be assessed on a case-by-case basis to avoid adverse effects.

Governments could also offer various financial incentives instead of direct funding. One such measure could include accelerated depreciation, which allows companies to write off the value of decommissioned equipment more quickly, thereby securing tax benefits and improving short-term cash flow. Another option would be to reduce spectrum fees, which would increase available capital for operators without requiring direct state compensation. This could be a workable solution as it would allow capital reallocation without the use of public funds. Although no country implementing these mandates has yet adopted such financial incentives, they represent potential strategies for the EC and Member States to explore.

Assessment and Conclusions

Impact assessment

European operators have publicly expressed support for the EC’s pursuit of security as the end goal of the CSA2.⁷⁰ However, there is considerable concern that the maximalist approach of the proposal on the table is not suitable to reach this goal. Our impact assessment shows that the telecoms industry would face several significant, horizontal impacts under the current CSA2 proposal. For each impact, we have assigned either a limited, material or substantial status, with most falling into the substantial category – see *Table 2*. As things stand, the EC’s proposals are therefore problematic for a number of reasons.

Table 2
Impact assessment of the CSA2 proposal

Horizontal issue	Impact
Network Operations	Substantial
Legal and Regulatory Certainty	Substantial
Competition	Substantial
Investment	Substantial
Consumers (End Users)	Material
Sustainability	Limited

Source: Assembly

The most extreme measure being applied uniformly across Member States leaves little room for national approaches to flex to their individual situations and should only be considered as a last resort. Countries with more HRV equipment are likely to require more time for replacement. The EC's proposed timelines ignore reality, especially for mobile networks. In some Member States, such as Germany, acquiring the necessary planning permissions and site certifications can take up to two years alone, which would significantly delay any rip-and-replace process. These problems are only exacerbated by the bloc's labour shortage of qualified telecoms engineers, the demand for whom would limit the speed at which operators can replace network equipment. These extended rip-and-replace processes would impact consumers too, leaving them with degraded and disrupted services. The UK's rip-and-replace process has shown the impact of this degradation, with its network coverage and quality scores consistently falling below most, if not all, of its European peers.

The proposal contradicts its own stated goal of a diverse supply chain. By requiring operators to remove all HRV equipment, they will be left with little choice for their equipment suppliers. This would limit supply chain diversity in existing networks that are being replaced and in new deployments. The remaining options also may not be as sustainable, with the equipment that it would replace often particularly energy efficient. An EU-wide rip-and-replace scheme would likely have wider environmental impacts too. Site visits require transportation and energy, which are already carbon intensive, and with multiple visits needed, processes' carbon footprints will quickly accumulate.

The cost to operators would undoubtedly be one of the most significant impacts of the proposal, with future network investment likely to suffer as a result. Without that network investment, the wider economy would suffer too. European businesses are set to benefit from the adoption of a variety of innovative services and tools that can only be made possible by the high-speed connectivity that new network deployments can provide. Delaying these deployments would come at a significant productivity cost as businesses miss out on the opportunities that would be made available to them with better connectivity. Despite these problems, compensation from the EC is unlikely, meaning operators will have to shift their resources away from investing in necessary new very high capacity networks.

Annex: Country-level detail on vendor restrictions in Europe

Austria

Under Article 45 of the Telecommunications Act 2021,^{[71](#)} the Federal Minister can formally designate a manufacturer as a “high-risk supplier” on the grounds of national security and exclude that vendor from supplying security-relevant components for networks. As of yet, no formal designation has been issued.

Belgium

Belgium has implemented the Toolbox through the law of 17 February 2022^{[72](#)} and the Royal Decree of 16 April 2023.^{[73](#)} The 2022 law amended the Electronic Communications Act to establish a security framework under which operators must obtain prior authorisation before using 5G network equipment. The 16 April 2023 Royal Decree sets deadlines for when operators would have to remove equipment from HRVs from their networks and not procure such equipment in future. The criteria for a supplier to be considered high risk seem to target Chinese vendors such as Huawei and ZTE in particular. By 1 January 2028, operators must cease using and remove high-risk equipment from the 5G core and RAN networks, and from the transport network by 1 January 2031.

Cyprus

Under the Security of Networks and Information Systems Law of 2020 (P.I. 408/2020),⁷⁴ Cyprus' Digital Security Authority can identify high-risk vendors and impose restrictions or exclusions concerning their participation in 5G networks. The Digital Security Authority has not yet designated any vendors as high risk.

Denmark

In April 2023, Denmark's Centre for Cyber Security (CFCS) ordered TDC NET to phase out Huawei equipment from its central transport network by 1 January 2027.⁷⁵ The CFCS has not demanded that any other operator should remove equipment from HRVs, primarily because they are not as reliant on Huawei equipment as TDC NET was. TDC NET is complying with the regulator's decision, although it has stated that CFCS has not pointed to any concrete threat or given any example of where the operator's security has been compromised. On 24 June 2026, the Eastern High Court recognised that although the CFCS's decision was not unlawful, it did constitute expropriation, and set expropriation compensation at DKK80m (€10.1m).⁷⁶

Estonia

On 24 November 2021, Estonia's Parliament approved a bill to transpose the European Electronic Communications Code (EECC), which aims to ensure the security of 5G networks.⁷⁷ On 1 February 2022, the act came into force, and requires high-risk technology to be removed from 5G networks by 2025 and from 4G networks by 2029. The regulation also uses a pre-authorisation system, meaning operators must submit requests before they deploy equipment. As a result of these restrictions, Elisa filed a lawsuit arguing that it should receive compensation for rip-and-replace processes. In March 2026, an AG published an opinion stating that while Member States may exclude telecoms equipment due to national security risks, operators may be entitled to compensation if they face disproportionate burdens.⁷⁸ This opinion is not binding, but the CJEU does often follow opinions issued by AGs in its rulings.

Finland

The Finnish Parliament has implemented measures of the Toolbox, including provisions that empower the national authority Traficom to require a removal of network equipment in critical parts of communications networks when it has “serious grounds” for suspecting that it endangers national security.⁷⁹ These restrictions initially covered the core network, but in January 2025, Traficom launched a project to update the technical specification of the critical parts of telecoms networks, which will enter into force on 19 December 2026. This new specification also applies to 5G base stations, which are considered a critical part of the network when they implement functionalities that essentially control or direct access to the network and traffic in the network. The regulation itself does not require removal of equipment or prohibit the use of any particular equipment manufacturer, but it specifies which parts of the network may be subject to the removal order referred to in the Act on Electronic Communications Services.⁸⁰ This does not entail a mandatory rip-and-replace scheme; instead, Traficom will make decisions on a case-by-case basis. The Act also provides a compensation mechanism in the case that operators are forced to remove network equipment.⁸¹ Additionally, on 18 June 2026, the Constitutional Committee of the Finnish Parliament published an opinion stating that it does not believe Finland should accept the CSA2 proposal in its current format.⁸² This is due to concerns over the protection of private property and strict rip-and-replace mandates potentially violating these rights. It also suggests that the proposal should include appropriate compensation provisions for expropriation. This is not a legally binding opinion but the Finnish Government will need to take it into account when reviewing its position on the proposal.

France

France adopted the '5G Law' in August 2019 (before the EC's Toolbox was announced), mandating operators to seek government approval for the hardware and software used in their networks "except fourth generation networks and previous generations".⁸³ Authorisations are granted for a maximum of eight years and can be renewed. While the French Government stated there was no intention to exclude any particular vendors from the market, operators were reportedly told that they could not renew licences for Huawei 5G equipment once they expire, effectively phasing the vendor out of the country's mobile networks by 2028. The Government chose to focus on removing Huawei equipment in strategically located areas, which included densely populated areas where Huawei equipment was prominent. In 2020, Bouygues Telecom stated that it would have to remove 3,000 Huawei-made mobile antennas as a result.⁸⁴ Subsequently, in 2023, Bouygues Telecom and SFR took legal action to receive compensation for having to remove Huawei equipment from their networks, as Huawei's radio equipment was not compatible with that of other vendors such as Ericsson and Nokia meaning replacements would be more costly. In exchange for the operators dropping their lawsuit in August 2023, the French Government decided to push back the deadline for removal in less sensitive areas to 2032.⁸⁵

Germany

The Federal Ministry of the Interior and Community (BMI) concluded individual legal contracts with Deutsche Telekom, Vodafone and Telefónica on the further use of critical components in 5G networks.⁸⁶ The contracts oblige the three operators to stop using all critical components made by Huawei and ZTE in their 5G core networks by the end of 2026. They must also replace the critical functions of Huawei and ZTE's 5G network management systems in the access and transport networks of their 5G networks by the end of 2029.

Ireland

In November 2021, the Irish Government agreed to a number of measures to enhance the security of telecoms networks, endorsing the Toolbox as the framework that would guide their implementation.⁸⁷ Under the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, the Minister of the Environment, Climate and Communications is able to assess the risk that vendors may be “subject to interference by a third country” and require that such suppliers are not used in or removed from telecoms networks in Ireland. No decision has been taken designating individual vendors as high-risk, meaning that operators have not yet had to undertake a rip-and-replace scheme.

Italy

Italy does not have a blanket ban on specific equipment vendors, but considers the issue on a case-by-case basis. Its implementation of the Toolbox has been largely based on its “Golden Power” decree, which allows it to veto contracts involving foreign investments that it deems threatening to national security. For example, in October 2020, the Government vetoed a 5G equipment deal between Fastweb and Huawei in the core network.⁸⁸ By using this regulatory framework, the Government has succeeded in removing equipment from HRVs from core mobile networks. With regards to the RAN, it has implemented a comprehensive risk mitigation strategy based on supplier diversification – limiting the presence of HRVs to below a defined threshold – complemented by risk mitigation measures such as annual VAPT assessments, 2FA and a robust policy for reviewing access privileges to equipment.

Lithuania

In May 2021, the Lithuanian Parliament voted to bar “unreliable” manufacturers and suppliers from the country’s telecoms networks, passing amendments to sectoral and national security legislation.⁸⁹ This is a comprehensive measure that applies across the whole network.⁹⁰ Operators using equipment and infrastructure that do not align with the amended laws had until the end of 2025 to replace it, otherwise they would not be eligible to apply for 5G spectrum licences.

Netherlands

In December 2019, the Dutch Government published the Telecommunications Security and Integrity Decree (Bvit).⁹¹ The Bvit amended the country's Telecommunications Act to create a legal basis for excluding suppliers. This was followed by the Telecommunications Security and Integrity Regulation (Rvit) in 2021, which contains five categories of security, 19 control measures and 60 implementation requirements for critical systems for all Dutch telecoms operators.⁹² The Dutch Authority for Digital Infrastructure (RDI) monitors the compliance of these laws and regulations. In 2021, the three major Dutch operators (KPN, Odido and Vodafone) were ordered to stop using Huawei equipment in the core of their 5G networks, although the exact terms of this agreement have not been disclosed. Odido legally challenged the removal order, with the District Court of Rotterdam dismissing the case in October 2023. After an appeal, the Dutch Trade and Appeals Tribunal (CBb) issued a final, unappealable judgement in March 2026, upholding the removal orders and denying the operator's requests for financial compensation.⁹³

Poland

Poland's adoption of the Toolbox has gone through various stages. The National Cybersecurity System Act was initially proposed in September 2020, and set out four risk categories for equipment vendors, with different restrictions for each one. The bill went through various debates and amendments, finally being passed in January 2026, and entering into force on 3 April 2026.⁹⁴ It provides for an individual administrative procedure for the designation of a high-risk supplier, and once a supplier has been designated as high risk, operators may no longer deploy their equipment and must phase out existing products. Operators will have up to four years to remove equipment used in critical functions and up to seven years for other equipment. At the time of publication, no such proceedings had been initiated, and no supplier had been designated. Earlier measures included partial implementation of the 5G Toolbox through telecommunications rules, multi-vendor requirements and 5G spectrum-reservation decisions.

Portugal

In 2023, Portugal's CSSC cybersecurity board banned equipment from vendors deemed "high risk", which would be those from countries that are not members of the EU, NATO or the OECD.⁹⁵ This effectively bans Chinese equipment from both 4G and 5G networks. In September 2024, Infrastructure Minister Miguel Pinto Luz confirmed the continuation of the restrictions imposed by the previous Government. In April 2026, Portuguese operator MEO launched legal action against the Government over this decision, seeking €82m in damages.⁹⁶

Romania

The Romanian Government has adopted a law to establish a mechanism for prior authorisation of equipment manufacturers, with particular regard to 5G.⁹⁷ The law does not target particular vendors; however, it restricts companies controlled by a foreign government, that do not have a transparent ownership structure, or are not subjected to an independent justice system in their home country. Once a supplier is designated as high-risk, operators would have five years to remove non-approved equipment from the core network and seven years to remove it from all 5G networks. Huawei applied for a licence to supply 5G equipment which was rejected in February 2024.⁹⁸ As a result, the deadline for removal of Huawei equipment in the core network is February 2029, and February 2031 for removal across the whole network. Huawei has since filed a legal challenge requesting the annulment of the government act issued in 2024.

Slovakia*

On 30 January 2018, Slovakia adopted Act No. 69/2018 Coll. on Cybersecurity,⁹⁹ which empowers the National Security Authority (NBU) to prohibit or restrict the use of a specific process, service or third party for the provision of an essential service where its use could jeopardise cybersecurity. This must be based on a risk assessment, and operators must be given a “reasonable time limit” to remove the vendor, which would be between two and five years. The act was amended by Act No. 366/2024 Coll.¹⁰⁰ to transpose the NIS2 Directive. However, as of yet, the NBU has not ordered any operators to remove high-risk vendors from their networks. The NBU’s Cybersecurity Risk Analysis Methodology (2025)¹⁰¹ also provides a sector-neutral framework for operators of essential services, including telecoms operators, to assess cybersecurity risks, and treats key suppliers as assets subject to risk assessment.

**An earlier version of the report only referenced Slovakia's 2020 non-binding agreement with the US. We've since clarified that the 2018 Act No.69/2018 Coll. on Cybersecurity gives Slovakia the ability to designate vendors as high risk.*

Spain

The Spanish Government has adopted Royal Decree-Law 7/2022 on the security of 5G networks and services, which states that the risk profile of the most important suppliers of 5G networks and service operators in Spain will be examined.¹⁰² As a result, suppliers designated as high risk may have to be removed from the network. However, to date, the Government has not designated any vendors as being high risk. Nevertheless, it did cancel a fibre service contract with Telefónica over the use of equipment made by Huawei.

Sweden

Sweden has perhaps taken the firmest stance. On 1 March 2020, the PTS introduced new rules for network security, which include stronger risk assessment requirements and the need to document operators' interaction with vendors and contractors for at least five years. On 20 October 2020, the agency went even further, ruling that operators would not be able to use Huawei or ZTE equipment to deploy 5G networks following the upcoming 2.3GHz and 3.5GHz spectrum auction (which took place in November of that year). By January 2025, operators had to have completely phased out Huawei and ZTE equipment from their networks.

Bulgaria, Latvia and Slovenia

Bulgaria,¹⁰³ Latvia,¹⁰⁴ and Slovenia¹⁰⁵ have each signed a “Joint Declaration on 5G Security” with the US that effectively aligns their development of 5G networks to that of the US, including avoiding the use of Chinese equipment vendors. The statements emphasise the importance of encouraging the participation of reliable and trustworthy network hardware and software suppliers in 5G markets, taking into account risk profile assessments, and promoting frameworks that effectively protect 5G networks from unauthorised access and interference. However, these declarations do not enforce bans on HRVs or require operators to complete a rip-and-replace process.

Czechia

The National Cyber and Information Security Agency (NÚKIB) made a non-binding recommendation for assessing the trustworthiness of technology suppliers of 5G networks in Czechia.¹⁰⁶ Operators are recommended to select vendors from EU or NATO countries for their 5G networks. This is not a mandatory requirement and operators are not forced to rip and replace HRVs from their networks. The recommendation is therefore likely to have a limited impact.

UK

While no longer an EU Member State, the UK's measures with regards to HRVs show that the EU's timeframe is largely unworkable, with UK operators having an additional two years to completely remove Huawei from their networks. On 14 July 2020, the UK Government announced that Huawei would be removed entirely from UK 5G networks by the end of 2027, with a ban on procuring new Huawei 5G equipment after 31 December 2020. This followed the May 2020 US amended Foreign-Produced Direct Product Rule, which expanded US controls to prohibit foreign companies from supplying Huawei with products that were produced or developed using US software, technology or manufacturing equipment. The UK Government's cut-off date of 31 December 2020 for procuring new equipment was in part to ensure that no Huawei equipment manufactured in line with the US sanctions could be used in UK 5G networks. In October 2022, following a consultation with affected operators, legal notices were sent to 35 UK operators, setting out legally binding requirements and deadlines and putting the Government's policy position on a legal footing – see *Table 3*.¹⁰⁷

Table 3

The UK's designated vendor requirements and timeframes

Network	Requirement	Deadline/timeframe
All networks	No use of Huawei managed services (specialist maintenance exempt)	From direction (October 2022) in force
All networks	No use of Huawei high data rate transmission equipment	After 31 December 2025
All networks (except fibre access)	No use of Huawei equipment affected by the altered US Foreign-Produced Direct Product (FPDP) Rule	From direction in force
Core (all networks)	No Huawei equipment or services in core network functions	31 December 2023 (extended from 28 January 2023)
Fixed (fibre access)	No installation of Huawei equipment affected by the altered US FPDP Rule	From direction in force
Fixed (FTTP/gigabit)	Cap Huawei at 35% of FTTP and gigabit-capable access networks	After 31 October 2023
Mobile	No Huawei in mobile access serving sites significant to national security	After 28 January 2023
Mobile (5G)	No use of Huawei 5G equipment procured after 31 December 2020	From direction in force
Mobile (5G)	No new installation of Huawei equipment in 5G (existing equipment and maintenance exempt)	From direction in force
Mobile (5G)	Cap Huawei at 35% of the 5G access network	After 31 July 2023
Mobile (5G)	No Huawei equipment or services in any part of any 5G network (full removal)	31 December 2027

Source: UK Government's designated vendor directions

The list of 35 operators includes fixed and mobile operators serving both consumer and business markets. Some of the providers contacted did not use Huawei at the time, but were considered large enough that they could present a threat to national security should they begin using Huawei goods and services. Some smaller providers were not issued with a legal notice, but the Government advised all providers to consider these restrictions when making decisions related to security. The operators affected by HRV restrictions under the CSA2 would be broadly similar, impacting fixed and mobile operators, however the EC goes further by also applying them to satellite providers.

The original deadline to remove Huawei equipment from the 5G core network was January 2023; however, this was extended to December 2023 following pushback from operators, who warned that the supply chain delays caused by the COVID-19 pandemic would make it difficult for them to replace equipment in time. In access networks, operators were obligated to have a share of Huawei equipment no higher than 35% after July 2023. Unlike the EU's CSA2 proposal, the UK Government's approach was done collaboratively with industry. Even though operators did not necessarily agree with a ban, the Government consulted with them and extended certain deadlines as a result. Additionally, the UK's restrictions are set within a longer timeline, with operators having just over five years to fully remove Huawei equipment in their 5G networks, with restrictions on procuring new equipment being effective for an additional year and a half. This starkly contrasts the EU's proposed three-year timeline for a complete rip and removal of HRV equipment across the region, and suggests that the EC should reconsider this timeline.

Norway

While not an EU Member State, the Norwegian Government's measures with regards to HRVs present a useful comparison. The Government allows operators to choose their equipment suppliers themselves, albeit within the framework of the country's Security Act.¹⁰⁸ Authorities do not exclude any suppliers from the market, but have required operators to choose more than one supplier if they choose 5G suppliers from countries with whom Norway does not have a security agreement (i.e. China). At least 50% of the base stations must be from suppliers from countries (e.g. EU Member States) with whom Norway does have a security agreement.

Endnotes

1. [Proposal for a Regulation for the EU Cybersecurity Act](#), EC, 2026
2. [The EU toolbox for 5G security](#), EC, 2020
3. [Commission announces next steps on cybersecurity of 5G networks in complement to latest progress report by Member States*](#), EC, 2023
4. [Second report on Member States' progress in implementing the EU toolbox on 5G Cybersecurity](#), EC, 2023
5. [Cybersecurity Tracker \(Vendor Restrictions Benchmark\)](#), Assembly Research
6. [Cedefop TalentGap Index](#), Cedefop, 2025
7. [Supply Chain Reimbursement Program Eighth Report](#), FCC, 2026
8. [Standortbescheinigung](#), BNetzA, 2017
9. [Communications Market Report](#), Ofcom, 2020-2026
10. [Huawei legal notices issued](#), DCMS, 2022
11. [BEREC's position on HRV phase-out under CSA2/DNA Framework](#), BEREC, 2026
12. [Confirmation hearings of European Commissioners-designate](#), Assembly Research, 2024
13. In the UK, the Government's decision to exclude HRVs from the country's networks followed extensive engagement with industry as part of the 2018/19 Telecoms Supply Chain Review, with the restrictions later finalised in conjunction with operators to ensure workable obligations and timelines. See [UK Telecoms Supply Chain Review Report](#), DCMS, 2019
14. [Better regulation guidelines](#), EC, 2021
15. [Telecom views on the Revised Cybersecurity Act](#), Connect Europe & GSMA, 2026
16. [Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors](#), EC, 2024
17. [NCSC advice on the use of equipment from high risk vendors in UK telecoms networks](#), NCSC, 2020
18. [Secure and Trusted Communications Networks Reimbursement Program](#), FCC, 2026
19. [NIS2 Directive](#), Official Journal of the EU, 2022
20. [Cyber Resilience Act](#), Official Journal of the EU, 2024
21. [EU cybersecurity rules: fixing certification, supply chains and critical entities](#), DigitalEurope, 2026
22. [Proposal for a Regulation for the Digital Networks Act \(DNA\)](#), EC, 2026
23. [Event debrief: FT/Connect Europe Forum](#), Assembly Research, 2025 and [Event debrief: BEREC's 14th Stakeholder Forum](#), Assembly Research, 2026
24. [Cybersecurity Act Revision \(CSA2\)](#), European Parliamentary Research Service, 2026
25. [FCC Updates Covered List to Include Foreign-Made Consumer Routers](#), FCC, 2026
26. [Ownership structures in European telecoms](#), Assembly Research, 2025
27. [State of Digital Communications 2026](#), Connect Europe, 2026
28. [Impact Assessment – Proposal for a Regulation for the EU Cybersecurity Act](#), EC, 2026
29. [Cybersecurity of Open Radio Access Networks](#), NIS Cooperation Group, 2022
30. [Samsung loses in UK 5G as Vodafone reverts to Ericsson and Nokia](#), Light Reading, 2025
31. [Secure 5G networks: Questions and Answers on the EU toolbox](#), EC, 2020
32. [Telecoms supply chain diversification: independent report and recommendations](#), Telecoms Supply Chain Diversification Council, 2024
33. [The EU toolbox for 5G security](#), EC, 2020
34. [Member States publish a report on EU coordinated risk assessment of 5G networks security](#), EC, 2019
35. [Independent report](#), Telecoms Diversification Taskforce, 2021
36. [A joint statement on the sunset of 2G and 3G networks and public ambition for Open RAN rollout as part of the Telecoms Supply Chain Diversification Strategy](#), DCMS, 2021
37. [UK and Mobile Network Operators' memorandum of understanding on Radio Access Network \(RAN\) solutions and Open RAN principles](#), DSIT, 2023
38. [State of Digital Communications 2026](#), Connect Europe, 2026
39. [The Mobile Economy Europe 2026](#), GSMA, 2026
40. [Mobile investment needs in Europe](#), GSMA, 2026
41. [2030 Digital Compass: the European way for the Digital Decade](#), EC, 2021
42. [Investment and funding needs for the Digital Decade connectivity targets](#), EC, 2023
43. [State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future](#), EC, 2025
44. [Annex 1 – State of EU digital transformation in 2025: progress and horizontal recommendations](#), EC, 2025
45. [Connect Europe Statement on the Cybersecurity Act](#), Connect Europe, 2026
46. [Impact Assessment – National security powers in relation to high risk vendors](#), DCMS, 2020
47. [Huawei swap-out in UK has become a costly and tortuous slog](#), Light Reading, 2024
48. Both estimates reflect one-off costs to operators and do not take into account potential ongoing impacts of the restrictions on industry as well as on the Government and Ofcom. They would also be expected to change if recalculated at a different point in time, reflecting developments in operators' 5G rollouts and usage of HRV equipment.
49. [Mobile Market Review: call for evidence](#), DSIT, 2026
50. [Speedtest Global Index \(April 2026\)](#), Ookla
51. [5G indicators: coverage](#), EC, 2026
52. [5G Coverage in Europe: Progress Toward Goals Amid Lingerin Disparities](#), GSMA, 2025
53. [The Envy of Europe: Nordics Lead in 5G Availability and Network Sunsets](#), GSMA 2025
54. [5G indicators: coverage](#), EC, 2026

Assembly

55. [Consumer pricing and engagement](#), Ofcom, 2026
56. [5G Observatory indicators data](#), EC, 2026 and [Connected Nations](#), Ofcom, 2025
57. [Huawei decision 'may delay 5G by three years and cost UK £7bn'](#), The Guardian, 2020
58. [Defend our networks: Congressional Record Vol. 169, No. 76](#), Congress, 2023
59. [US spectrum auction raises \\$3.5 billion](#), Reuters, 2026
60. [Supply Chain Reimbursement Program Sixth Report](#), FCC, 2025
61. [Supply Chain Reimbursement Program Eighth Report](#), FCC, 2026
62. [Verdict in the case regarding TDC NET's critical telecommunications infrastructure](#), Østre Landsret, 2026
63. [Opinion of Advocate General Cápeta delivered on 19 March 2026](#), EUR-Lex, 2026
64. [Bouygues Telecom and SFR sue government in pursuit of Huawei-ness](#), Mobile Europe, 2023
65. [Status of the dismantling of Huawei 5G antennas on national territory](#), National Assembly, 2025
66. [Business Appeals Tribunal](#), de Rechtspraak, 2026
67. [Meo sues the State to recover €82 million over Huawei's exclusion from 5G](#), Público, 2026
68. [Huawei files lawsuit against Portugal's 5G ban: Report](#), RCR Wireless News, 2023
69. [Open Networks Research and Development Fund](#), UK Government, 2022
70. The EU Cybersecurity Act 2, Assembly Research, 2026
71. [Telecommunications Act 2021](#), Federal Ministry Housing, Arts, Culture, Media, and Sport, 2021
72. [February 17 2022](#), Service Public Fédéral Justice, 2022
73. [16 April 2023](#), Service Public Fédéral Justice, 2023
74. [The Security of Networks and Information Systems Law of 2020](#), Digital Security Authority, 2020
75. [TDC NET phases out DWDM collaboration with Huawei](#), TDC NET, 2023
76. [Verdict in the case regarding TDC NET's critical telecommunications infrastructure](#), Østre Landsret, 2026
77. [Act on Amendments to the Electronic Communications Act](#), Riigikogu, 2021
78. [Opinion of Advocate General Cápeta delivered on 19 March 2026](#), EUR-Lex, 2026
79. [Reform of the Act on Electronic Communications Services](#), Valtioneuvosto, 2020
80. [Article 244 a, Act on Electronic Communications Services](#), Finlex, 2014
81. [Article 301 a, Act on Electronic Communications Services](#), Finlex, 2014
82. [Committee statement PeVL 21 /2026 vp](#), Eduskunta Riksdagen, 2026
83. [Law No. 2019-810 of 1 August 2019](#), Legifrance, 2019
84. [Bouygues to remove 3,000 Huawei mobile antennas in France by 2028](#), Reuters, 2020
85. [Status of the dismantling of Huawei 5G antennas on national territory](#), National Assembly, 2025
86. [Greater security and technological sovereignty for the German 5G mobile network](#), Federal Ministry of the Interior, 2024
87. [Communications Regulation and Digital Hub Development Agency \(Amendment\) Act](#), ISB, 2023
88. [Italy vetoes 5G deal between Fastweb and China's Huawei](#), Reuters, 2020
89. [Republic of Lithuania Law on the Protection of Objects Critical for National Security](#), Seimas, 2022
90. [List of equipment, devices and \(or\) software](#), National Defence of the Republic of Lithuania, 2021
91. [Telecommunications Security and Integrity Decree](#), Wetten Overheid, 2020
92. [Telecommunications Security and Integrity Regulation \(Rvit\)](#), Wetten Overheid, 2022
93. [Business Appeals Tribunal](#), de Rechtspraak, 2026
94. [The amendment to the Act on the National Cybersecurity System](#), Ministerstwo Cyfryzacji, 2026
95. [Safety Assessment Committee](#), GNS, 2022
96. [Meo sues the state to recover 82 million euros for excluding Huawei from 5G](#), Público, 2026
97. [Law No. 163 of June 11, 2021](#), Parlamentul României, 2021
98. [Decision No. 81 of February 29](#), 2024, Parlamentul României, 2024
99. [Section 27A of Act No. 69/2018](#), Ministerstvo Spravedlivosti Slovenskej Republiky, 2018
100. [Act No. 366/2024 Coll.](#), Ministerstvo Spravedlivosti Slovenskej Republiky, 2024
101. [Risk Analysis Methodology](#), National Security Authority (NBU), 2025
102. [Royal Decree-Law 7/2022](#), Boletín Oficial del Estado, 2022
103. [United States-Republic of Bulgaria Joint Declaration on 5G Security](#), US Department of State, 2020
104. [Joint Statement on United States-Latvia Joint Declaration on 5G Security](#), US Department of State, 2020
105. [Joint Statement on United States - Slovenia Joint Declaration on 5G Security](#), US Department of State, 2020
106. [The Recommendation for assessing the trustworthiness of technology suppliers of 5G networks in the Czech Republic](#), National Cyber and Information Security Agency, 2022
107. [Huawei legal notices issued](#), UK Government, 2022
108. [Important step for the digitalisation of Norway](#), Regjeringen, 2019

Important notice

By accepting this research, the recipient agrees to be bound by the following terms of use. This research has been prepared by Assembly Research Limited and published solely for guidance and general informational purposes. It may contain the personal opinions of analysts based on research undertaken. Assembly Research Limited gives no undertaking to provide the recipient with access to any additional information or to update or keep current any information or opinions contained herein. The information and any opinions contained herein are based on sources believed to be reliable but the information relied on has not been independently verified. Assembly Research Limited, its officers, employees and agents make no warranties or representations, express or implied, as to the accuracy or completeness of information and opinions contained herein and exclude all liability to the fullest extent permitted by law for any direct or indirect loss or damage or any other costs or expenses of any kind which may arise directly or indirectly out of the use of this research, including but not limited to anything caused by any viruses or any failures in computer transmission. The recipient hereby indemnifies Assembly Research Limited, its officers, employees and agents and any entity which directly or indirectly controls, is controlled by, or is under direct or indirect common control with Assembly Research Limited from time to time, against any direct or indirect loss or damage or any other costs or expenses of any kind which they may incur directly or indirectly as a result of the recipient's use of this research.

© 2026 Assembly Research Limited. All rights reserved. No part of this research may be reproduced or distributed in any manner including, but not limited to, via the internet, without the prior permission of Assembly Research Limited. If you have not received this research directly from Assembly Research Limited, your receipt is unauthorised.

Assembly

36 Spital Square
London
E1 6DY
United Kingdom

+44 20 3026 2700
info@assemblyresearch.co.uk