A Huge Cost of “Guardrails”: Security or Blockade?

Economic Impact Assessment of EU CSA2 Proposal and the CCCEU Position Paper

Editorial Team

Editor-in-Chief
Liu Jiandong

Deputy Editor-in-Chief
Fang Dongkui

Managing Editors
Liang Linlin，Cao Qian

Editorial Board
Ji Yu

With contributions from KPMG and the CCCEU Digital Economy Working Group, and with support from CCCEU member companies and relevant research institutions.

Contents

07 / Chamber Position and Core Recommendations: Safeguarding Bilateral Mutual Trust and Returning to Technological Neutrality

Conclusion: Safeguarding Openness with Mutual Trust, and Advancing Prosperity Through Rationality

Foreword I

The digital economy has moved to the center of the global governance agenda. Maintaining a balanced relationship between security and openness requires strict adherence to the principle of proportionality. This remains an important shared challenge for policymakers worldwide.

China and the European Union (EU) are key trade and investment partners, with their economies deeply embedded in an increasingly interconnected digital ecosystem. The EU continues to play a leading role in regulatory developments and foundational research, while Chinese enterprises contribute substantial engineering capabilities, manufacturing strength, and large-scale deployment experience. Together, they play an important role in shaping Europe's ongoing digital transformation.

At the regulatory level, recent developments related to the proposed revision of the EU Cybersecurity Act (hereinafter "CSA2") have raised growing concerns among industry stakeholders and market participants. While the objective of strengthening cybersecurity across the Single Market is both legitimate and necessary, certain provisions in the proposal appear to place disproportionate emphasis on the geopolitical origin of suppliers, thereby shifting the regulatory focus away from verifiable technical standards.

A regulatory logic based on origin-based classification risks introducing structural distortions into the internal market. It would weaken the principle of technology neutrality and is likely to result in fragmentation of certification and procurement frameworks across Member States. Over time, this would increase compliance complexity, raise implementation costs, and reduce efficiency in the deployment of digital infrastructure.

Ultimately, such developments may undermine interoperability across Europe's digital ecosystem and weaken the coherence, efficiency, and long-term resilience of the Single Market's technological foundation.

To contribute to the constructive discussion on the CSA2 proposal, the China Chamber of Commerce to the EU (CCCEU), in collaboration with KPMG, conducted a structured economic impact assessment based on defined regulatory and deployment scenarios. The findings indicate that CSA2 could result in cumulative economic impacts of around €370 billion over the next five years.

These estimated impacts are primarily associated with accelerated replacement cycles of existing digital infrastructure, increased compliance and certification costs, and potential delays in the rollout of digital transformation projects. Taken together, these factors may generate cascading effects across the broader digital ecosystem, amplifying adjustment pressures over time.

Liu Jiandong
Chairman of the China Chamber of Commerce to the EU (CCCEU)

Given the highly interconnected nature of Europe's digital value chains, such impacts would extend beyond the ICT sector and affect key industries including energy, telecommunications, and industrial manufacturing, all of which increasingly depend on secure, interoperable, and continuously upgraded digital systems. The resulting cost pressures would be borne across the economy, with small and medium-sized enterprises and end users likely to experience higher sensitivity.

The CCCEU maintains that effective cybersecurity governance must be grounded in technical transparency and verifiable standards. True resilience is best achieved through technical excellence and system robustness, while diversity within the technological ecosystem can further enhance innovation capacity and operational reliability.

Adherence to technological neutrality is essential to fostering an open, competitive, and interconnected digital future. A strong foundation of mutual trust underpins long-term stability and predictability for all stakeholders.

Against this backdrop, the CCCEU encourages EU institutions to further advance a governance paradigm based on capability verification rather than origin-based classification. Transparent, standards-based audits, supported by clear and consistent technical requirements, can effectively ensure security while preserving the integrity and coherence of the EU Single Market.

The Chinese business community will continue to engage with European partners on a pragmatic and forward-looking basis. In an increasingly interconnected digital economy, sustaining open and balanced technological exchange is not merely a shared objective, but a practical necessity to avoid fragmentation, contain costs, and support long-term innovation. At a time of growing global uncertainty, this also constitutes a shared responsibility and a common strategic imperative.

Foreword II

The global economy is currently at a critical juncture marked by shifting growth drivers and the reshaping of rules. Sluggish growth, elevated inflation, and geopolitical conflict are compounding one another, making the maintenance of stable industrial and supply chains an urgent shared priority for all countries. Against this backdrop, the pattern of interaction between China and the EU, as the world's two major economies, concerns not only bilateral interests but also the broader trajectory of the global economy.

Looking back, China–EU economic and trade cooperation has developed over half a century into a structure characterized by deep interdependence and strong complementarity. In trade, China and the EU are each other's second-largest trading partners, with bilateral trade reaching USD 828.1 billion in 2025, up 5.4% year on year. In investment, two-way accumulated investment exceeded USD 280 billion by the end of 2025. Meanwhile, the China–Europe Railway Express—an essential supply-chain artery linking the Eurasian continent—surpassed 20,000 train trips for the first time in 2025 and now reaches more than 200 European cities, serving as a key channel for safeguarding Eurasian supply-chain resilience.

Cooperation between the two sides has now evolved beyond traditional trade in goods into a deeply symbiotic model encompassing R&D collaboration, industrial-chain integration, and standards coordination. High-tech products and green, low-carbon development have become defining features of China–EU trade cooperation. This partnership reflects not only the EU's strong foundations in basic research, original innovation, and international standards systems, but also China's complete industrial chains and strong engineering capabilities. China's pronounced strengths in applied technology R&D, rapid iteration, and industrial-scale integration are making it an important driver of global technological innovation and the large-scale deployment of green technologies. Together, China and the EU, through a cooperation model grounded in complementary advantages and market-oriented priorities, constitute a key force driving the global green and digital transition.

In recent years, however, within the EU's three-pronged approach of China, the roles of "economic competitor" and "systemic rival" have become increasingly prominent, while that of "partner for cooperation and negotiation" has gradually weakened. "De-risking" has increasingly become a central theme of the EU's economic and trade policy toward China. The excessive politicization and instrumentalization of security issues are causing governance tools originally intended to enhance economic resilience to deviate from their purpose and turn into instruments of market segmentation shaped by geopolitical considerations.

To establish a unified security framework for the information and communications technology supply chain, systematically identify and address the risks posed by so-called “high-risk suppliers,” enhance cybersecurity resilience, and safeguard strategic autonomy, the EU formally proposed amendments to the Cybersecurity Act (CSA2) in January 2026. However, the proposal relies excessively on geopolitical labels rather than risk assessment based on objective technical factors, and it does not adequately consider the broad economic costs and social implications that would result from the mandatory replacement of already deployed equipment.

In order to assess comprehensively and objectively the real impact of the mandatory replacement provisions proposed under CSA2, this report considers multiple dimensions, selects core indicators, and ensures rigor through cross-validation using authoritative multi-source data, first-hand industry research, and expert views. The analysis shows that the EU’s recent cybersecurity policy has drifted away from a technology-neutral approach and may give rise to three major economic concerns. First, discriminatory screening based on “place of origin” rather than technical factors undermines market fairness and suppresses technological progress. Second, aggressive mandatory replacement would impose losses amounting to hundreds of billions of euros on the EU over five years, with the costs being transmitted through key sectors such as energy and telecommunications to society as a whole, thereby raising production and living costs and fuelling inflation. Third, “one-size-fits-all” regulation would intensify developmental imbalances among member states and further strain already tight fiscal space.

Past practice has shown that openness and cooperation are the fundamental path to addressing challenges and enhancing industrial resilience. We call on the EU to return to a technology-neutral and evidence-based regulatory approach and to strike a prudent balance between safeguarding security and preserving openness.

The camel bells of the ancient Silk Road bore witness to mutual learning among civilizations; today, as the great vessel of China–EU relations sails forward, even greater solidarity is required. China–EU relations today should rise above short-term political noise and, with a long-term strategic vision, jointly write a new chapter of openness, cooperation, and mutual benefit. This concerns not only the wellbeing of the peoples on both sides, but also a shared responsibility for upholding multilateralism and global prosperity and stability.

01

Executive Summary

A Strategic Choice Between Non-Technical Cybersecurity Criteria and Rational Standards

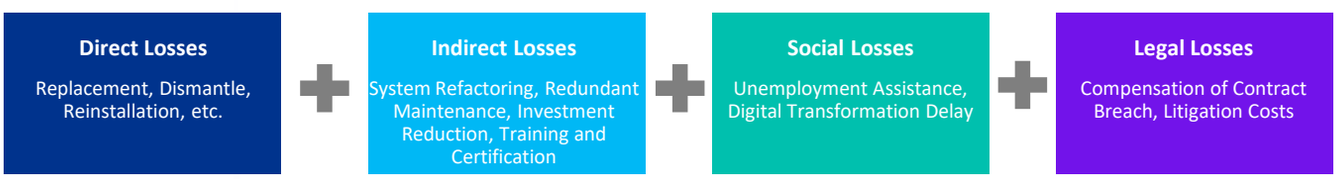
At a time when economic globalization and digital transformation are becoming increasingly intertwined, China and the EU, as two of the world's key economic forces, have developed a deeply integrated and mutually beneficial industrial relationship across areas such as green and low-carbon development, digital infrastructure, and intelligent manufacturing. Experience over recent decades has shown that Chinese enterprises are not only active participants in the EU's green and digital twin transition, but also long-term, highly reliable, and full compliant co-builders of its digital ecosystem. With advanced technological solutions and strong compliance record, Chinese enterprises have continued to create value in Europe's twin-transition process and have significantly improved overall quality and efficiency. However, as the proposed amendments to the EU Cybersecurity Act ("CSA2") advance, this foundation of cooperation built on mutual trust is facing serious challenges.

Current policy developments indicate that EU cybersecurity governance is increasingly tending toward an expanded notion of national security and, in turn, toward geopolitically motivated protectionism. The core risk of the CSA2 proposal lies in using non-technical factors based on the origin of supply as a market-access criterion. Such an approach departs from the fundamental principles of technological neutrality and fairness and poses a potential challenge to international economic and trade rules. This restrictive policy, which exceeds the principles of conferral and proportionality, is unlikely to deliver meaningful security reinforcement. Instead, it may create regulatory islands by fragmenting global industrial chains, seriously weakening Europe's ability to absorb advanced technologies and undermining its long-term innovation ecosystem.

The resulting knock-on effects would translate into a systemic economic loss. According to a joint assessment by the CCCEU and KPMG, mandatory supplier exclusion under the CSA2 framework could result in economic losses of up to EUR 367.8 billion across EU Member States over the first five years[1] across 18 sectors[2], with impacts continuing to evolve thereafter.

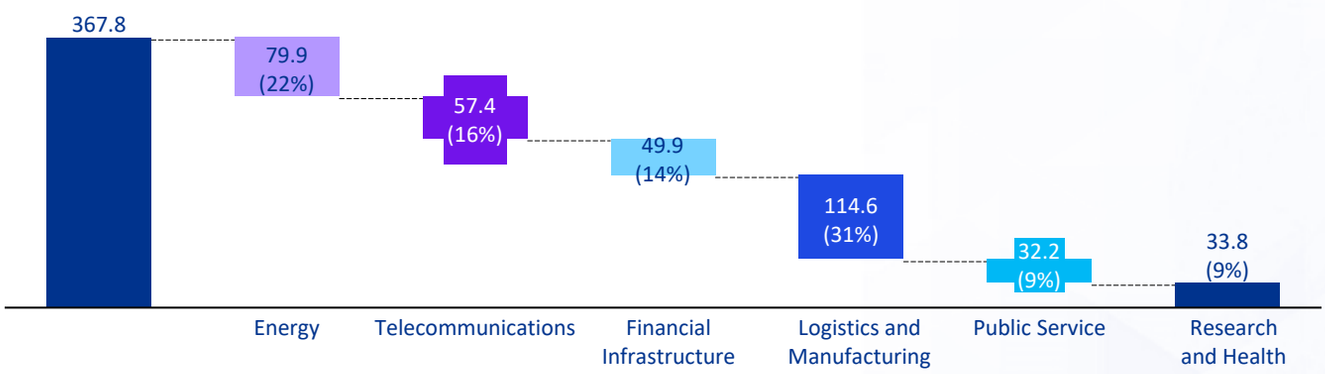
- The losses comprise four components: direct losses, indirect losses, social losses, and legal losses. Direct losses arising solely from hardware replacement, dismantling, and reinstallation account for 40% (approximately EUR 146.2 billion); indirect costs generated through system reconstruction and resource reallocation account for 22% (approximately EUR 81.5 billion); social losses associated with service disruption and employment adjustment account for 28% (approximately EUR 102.1 billion); and legal risks related to dispute resolution, recertification, and compliance account for 10% (approximately EUR 38.1 billion)[3].

Figure 1: Four-Tier Loss Structure Used in This Assessment



- Sectoral impact: As the foundational pillars of twin transitions, the energy and telecommunications sectors would bear nearly 40% (38%) of the total economic loss, Logistics and Manufacturing also bear 31% of the total economic shock[3]. This "compliance premium" would not only erode corporate innovation budgets, but would ultimately be passed on as inflationary pressure to European consumers and taxpayers.

Figure 2: Losses by Sector[3] (EUR billion, %)



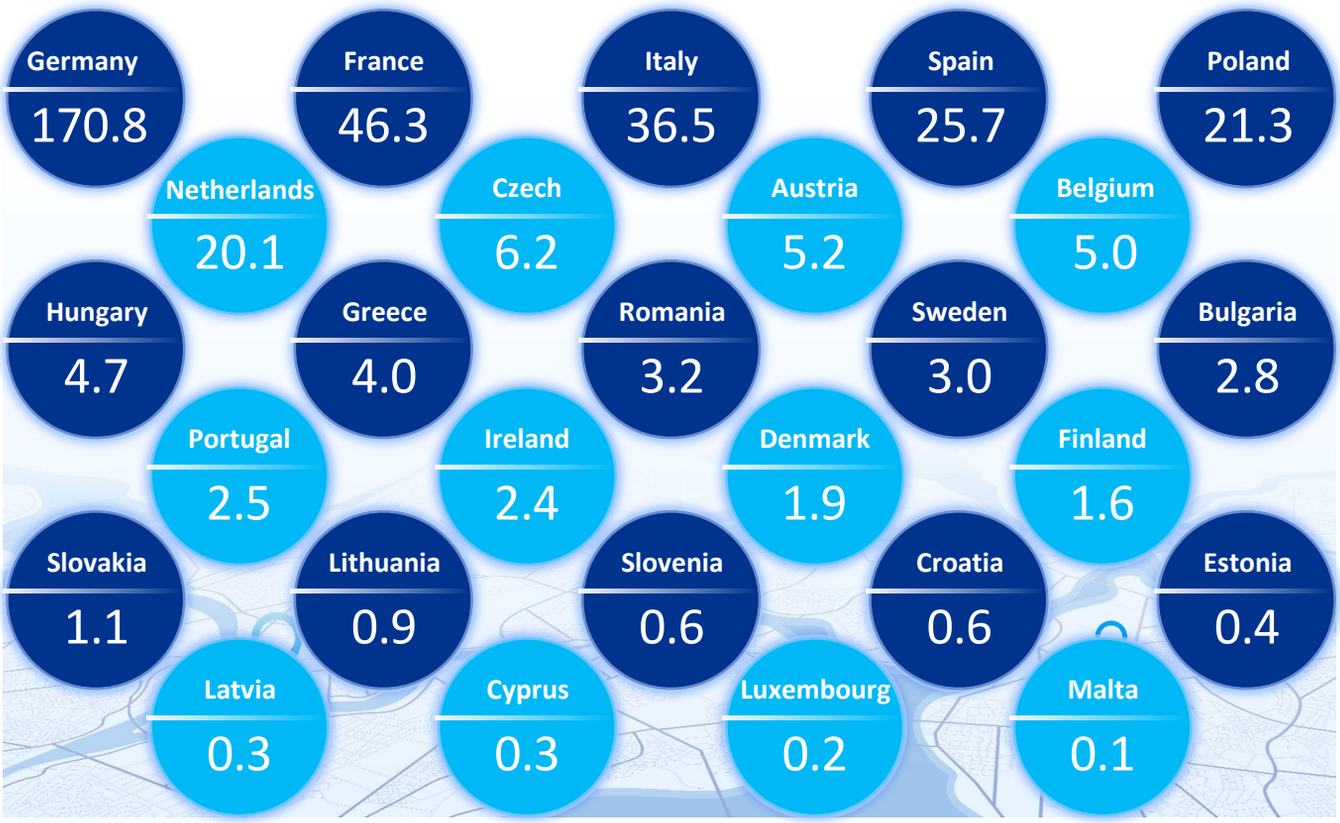
1. The proposal stipulates that mandatory replacement of mobile-network equipment must be completed within 36 months, but does not specify mandatory replacement deadlines for other sectors and related equipment. To facilitate this assessment, the observation period is set at 2026–2030, assuming that the relevant replacement work would be substantially completed within five years. This assumption is based on the view that completing replacement within 36 months would be operationally difficult in practice. Given that CSA2 remains at the proposal stage, only some downstream customers, operators, and project entities are expected to begin supplier-substitution assessments in 2026–2027 and make precautionary adjustments to procurement, certification, and supply-chain arrangements. Should the proposal later be formally adopted and enter into force, the more concentrated effects of mandatory replacement requirements are expected to begin to materialize progressively from 2028 onward.

2. The NIS2 Directive covers 18 major sectors, including energy, transport, banking, financial market infrastructures, healthcare, drinking water, wastewater, digital infrastructure, ICT service management, public administration, space, postal and courier services, waste management, the production, manufacture and distribution of chemicals, food production, processing and distribution, manufacturing, digital services, and research.

3. Compiled and estimated by KPMG and the China Chamber of Commerce to the EU on the basis of authoritative public sources, including Eurostat and the Ministry of Commerce of China, as well as publicly available corporate financial statements and interviews with industry experts. For detailed methodology and data, please refer to Chapters 4 to 6 of this report. KPMG's contribution to this report is primarily limited to providing assistance with economic modeling and quantitative assessments. All policy positions, viewpoints, and recommendations contained herein are independently formulated and issued by the China Chamber of Commerce to the EU.

- Asymmetric Economic Imbalances: A deeper crisis lies in the fact that such regulatory policies may trigger asymmetric economic imbalances within the EU itself. The one-size-fits-all logic of CSA2 disregards the profound heterogeneity among member states in industrial structure, fiscal buffering capacity, and the pace of digital transformation. Industrial powers such as Germany, France, and Italy would face fiscal pressures amounting to tens or even hundreds of billions of euros, while relatively fiscally fragile countries could fall into a trap of "slowed digital development" due to the high costs of replacement, thereby undermining the overall competitiveness of the EU single market. This screening mechanism, grounded in geopolitical discrimination rather than empirical risk evidence, not only raises legal risks under the Charter of Fundamental Rights of the European Union and WTO rules, but also challenges the legal competence of member states in matters of national security.

Figure 3: Distribution of Overall Economic Losses Across EU Member States, 2026–2030[3] (Unit: EUR Billion)



Accordingly, a return to technological neutrality and economic rationality is essential to achieving mutual benefits between China and the EU. The CCCEU calls on EU institutions to halt discriminatory policies based on non-technical, country-of-origin criteria and to recognize that de-risking should not become a government-led tool of systemic decoupling. The EU should return to a regulatory path that is evidence-based and consistent with international trade and economic rules. Europe can best safeguard its supply-chain resilience, industrial competitiveness, and citizens' long-term wellbeing by shifting away from unilateral approaches and building an inclusive cybersecurity framework that balances security and openness. Otherwise, the current approach risks blockade over security—creating a huge cost of "Guardrails".

---

1. The proposal stipulates that mandatory replacement of mobile-network equipment must be completed within 36 months, but does not specify mandatory replacement deadlines for other sectors and related equipment. To facilitate this assessment, the observation period is set at 2026–2030, assuming that the relevant replacement work would be substantially completed within five years. This assumption is based on the view that completing replacement within 36 months would be operationally difficult in practice. Given that CSA2 remains at the proposal stage, only some downstream customers, operators, and project entities are expected to begin supplier-substitution assessments in 2026–2027 and make precautionary adjustments to procurement, certification, and supply-chain arrangements. Should the proposal later be formally adopted and enter into force, the more concentrated effects of mandatory replacement requirements are expected to begin to materialize progressively from 2028 onward.

2. The NIS2 Directive covers 18 major sectors, including energy, transport, banking, financial market infrastructures, healthcare, drinking water, wastewater, digital infrastructure, ICT service management, public administration, space, postal and courier services, waste management, the production, manufacture and distribution of chemicals, food production, processing and distribution, manufacturing, digital services, and research.

3. Compiled and estimated by KPMG and the China Chamber of Commerce to the EU on the basis of authoritative public sources, including Eurostat and the Ministry of Commerce of China, as well as publicly available corporate financial statements and interviews with industry experts. For detailed methodology and data, please refer to Chapters 4 to 6 of this report.

4. Based on this assessment, the EU's total economic loss is estimated at approximately EUR 367.8 billion. Minor differences between the sum of annual figures and the total loss are due to rounding.

1.1 Key Finding One: Chinese Enterprises Remain Important Participants in the EU's Economic Development and have Maintained a Strong Compliance Record

Over the past decades, China and the EU have developed extensive industrial linkages in key areas such as green and low-carbon transition, digital infrastructure, intelligent manufacturing, and energy efficiency. These linkages have contributed to the EU's objectives of economic competitiveness, digital transformation, and the green transition. Chinese enterprises are not only stable providers of advanced technologies and solutions, but also long-term co-builders and enablers of the EU's digital and green ecosystem. Through integrated solutions combining cost-effectiveness, reliability, and energy efficiency, Chinese enterprises have helped improved investment and operating efficiency for a wide range of European market participants, significantly improved the speed and quality of digital-infrastructure deployment, and supported Europe's leap forward in the digital age. In sectors such as telecommunications, energy, and industry across multiple countries, established end-to-end Chinese technology solutions and localized services have supported the construction of critical infrastructure and the modernisation of public services in the EU, contributing to regional industrial upgrading, SME digital transformation, and the achievement of green and low-carbon objectives.

Throughout this long period of close cooperation, Chinese enterprises have consistently regarded compliance as the lifeline of their presence in Europe, adhering to applicable to EU and Member State legal frameworks and cybersecurity standards. There is no substantiated evidence to date of a "technical backdoor" or regulatory violation. This combination of technological capability and compliance-oriented operations has not only created tens of thousands of local jobs, but has also generated sustained innovation spillovers for Europe's domestic supply chains through industrial linkages, delivering a genuine win-win outcome across the global value chain.

1.2 Key Finding Two: Geopolitical Protectionist Policies are Unlikely to Deliver Effective Security for the EU

We fully understand the EU's strategic concern over "supply-chain security" in the current geopolitical context. It must be stated, however, that the ongoing spread of unilateral protectionism and interventionism is steering this security governance agenda in the wrong direction. Restrictive regulatory policies represented by CSA2 rely excessively on discriminatory screening based on country of origin rather than technical factors. They are extremely difficult to implement, of very low practical feasibility, and are, in essence, risk decisions detached from industrial realities.

The exclusion and replacement measures targeting high-risk suppliers under CSA2 entail prominent legal risks. The mechanism emphasizes non-technical criteria linked to the supplier's country of origin and uses country of origin as a substitute for concrete technical risk in imposing mandatory controls. This violates the principles of proportionality and non-discrimination; procedurally, it reverses the burden of proof and provides insufficient rights of defense, casting doubt on its legality. The measures may violate bilateral investment treaties (BITs) between China and most EU member states, potentially triggering large compensation claims in arbitration as well as multi-level administrative, civil, and constitutional litigation within the EU and its member states. At the same time, the proposal may breach WTO rules and the EU's commitments under the WTO, including principles and rules under GATT 1994, GATS, the SCM Agreement, the TBT Agreement, and the TRIPS Agreement, thereby further intensifying international economic and trade frictions. These systemic legal risks could increase the fiscal burden on the EU and its member states while undermining regulatory stability and market confidence, and therefore require a balanced response grounded in clear risk standards and respect for the rule of law.

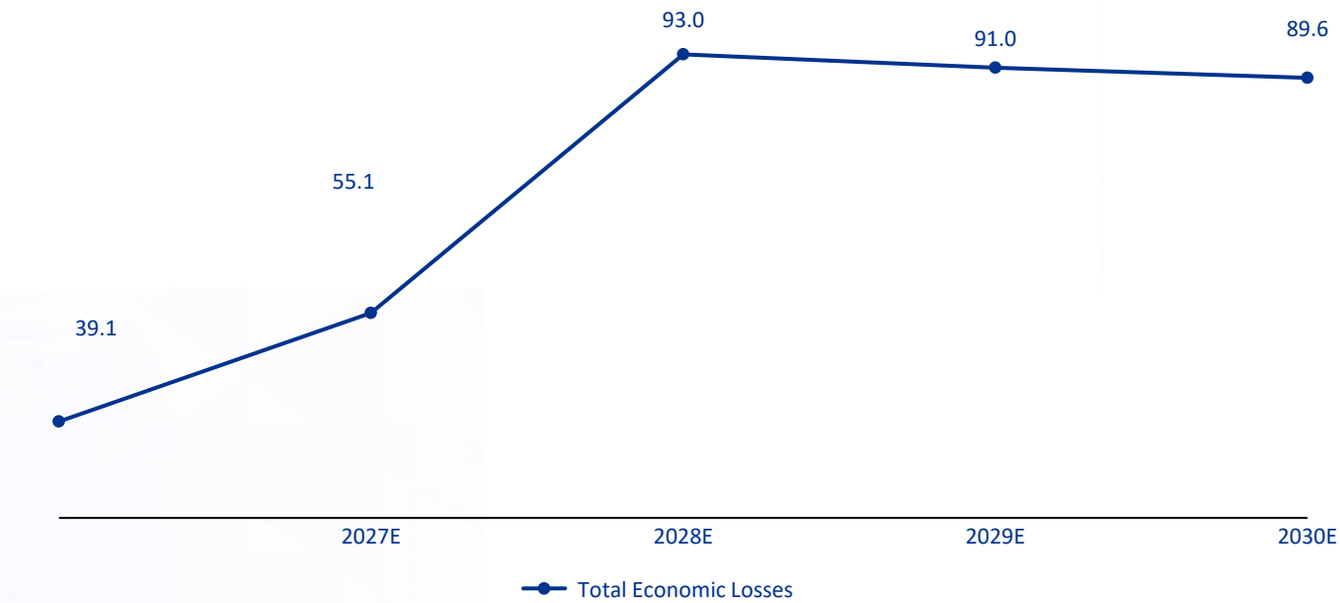
The current mandatory replacement plan is not only unlikely to achieve substantive security hardening; it would instead generate systemic negative effects. The premium created by restricting supplier origin would crowd out corporate innovation budgets, increase the fiscal burden on member states, and erode the disposable income and social welfare of EU citizens. Using enormous economic sacrifice and technological regression to relieve unproven "security pressure" is pushing the EU into a governance paradox in which slower development is traded for security, ultimately weakening Europe's long-term competitiveness and international reputation.

1.3 Key Finding Three: Unilateral and Disproportionate Regulation Departing from the Principles of Conferral and Proportionality Would Result in Hundreds of Billions of Euros in Economic Losses and Undermine Stable Industrial Revenues in the EU

If CSA2 were to complete[1] mandatory replacement across[2]18 major sectors over the next five years, the EU and its member states would incur losses of nearly EUR 367.8 billion from supplier replacement alone during 2026–2030. Direct[3] losses from equipment replacement, dismantling, and installation services alone would amount to approximately EUR 146.2 billion.

Over time, the EU's annual total loss is projected to rise from approximately EUR 39.1 billion in 2026 to about EUR 89.6 billion in 2030. Direct losses alone would increase from EUR 6.7 billion in 2026 to EUR 38.8 billion in 2030. This pattern reflects the assumption that in 2026–2027 the policy would still be in the proposal and refinement stage, with only some EU operators and project owners initiating supplier replacement each year. As the proposal is gradually legislated and enters large-scale implementation, the related economic losses would become more pronounced in 2028–2030.

Figure 4: Total Economic Losses from Mandatory Supplier Replacement[4] in the EU, 2026–2030 (EUR billion)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

1. The proposal stipulates that mandatory replacement of mobile-network equipment must be completed within 36 months, but does not specify mandatory replacement deadlines for other sectors and related equipment. To facilitate this assessment, the observation period is set at 2026–2030, assuming that the relevant replacement work would be substantially completed within five years. This assumption is based on the view that completing replacement within 36 months would be operationally difficult in practice. Given that CSA2 remains at the proposal stage, only some downstream customers, operators, and project entities are expected to begin supplier-substitution assessments in 2026–2027 and make precautionary adjustments to procurement, certification, and supply-chain arrangements. Should the proposal later be formally adopted and enter into force, the more concentrated effects of mandatory replacement requirements are expected to begin to materialize progressively from 2028 onward.

2. The NIS2 Directive covers 18 major sectors, including energy, transport, banking, financial market infrastructures, healthcare, drinking water, wastewater, digital infrastructure, ICT service management, public administration, space, postal and courier services, waste management, the production, manufacture and distribution of chemicals, food production, processing and distribution, manufacturing, digital services, and research.

3. Compiled and estimated by KPMG and the China Chamber of Commerce to the EU on the basis of authoritative public sources, including Eurostat and the Ministry of Commerce of China, as well as publicly available corporate financial statements and interviews with industry experts. For detailed methodology and data, please refer to Chapters 4 to 6 of this report.

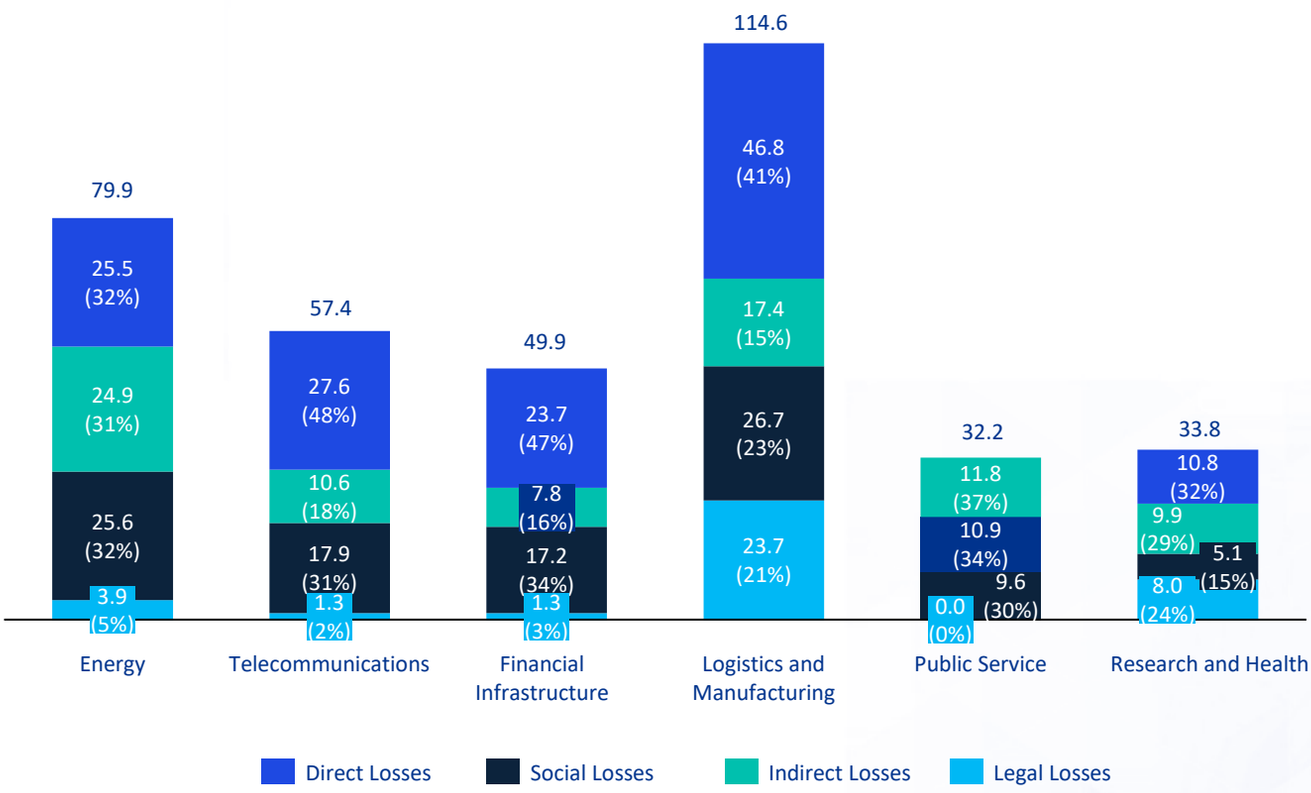
4. Based on this assessment, the EU's total economic loss is estimated at approximately EUR 367.8 billion. Minor differences between the sum of annual figures and the total loss are due to rounding.

The assessment divides the indicators into four layers: direct losses, indirect losses, legal breach-related losses, and social losses. Direct losses include replacement of existing hardware, dismantling and reinstallation, and impairment from early retirement of assets. Indirect losses mainly include system reconstruction, parallel maintenance, capital transfer losses, and training and certification. Legal losses include state compensation and litigation-related costs. Social losses mainly include pass-through effects on end-user prices and unemployment assistance for labor. Under this assessment, direct losses account for the highest share at approximately 40%, followed by indirect losses, social losses, and legal losses at 22%, 28%, and 10%, respectively.

For the purposes of this assessment, the 18 affected sectors are grouped—based on sectoral characteristics[5] and equipment types—into six segments: energy, telecommunications, financial infrastructure, logistics and manufacturing, public services, and health and research. Losses vary markedly across these segments, as set out below:

The logistics and manufacturing sectors will be severely impacted by the CSA2 proposal, with total mandatory replacement losses reaching EUR 114.6 billion, accounting for 31% of total losses. Direct losses in this segment alone would amount to EUR 46.8 billion. It is followed by the energy and telecommunications segments, with total mandatory replacement losses of EUR 79.9 billion and EUR 57.4 billion, respectively. Direct losses would amount to EUR 25.5 billion in energy and EUR 27.6 billion in telecommunications.

Figure 5: Total Losses by Sector Under EU Mandatory Replacement, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

3. Compiled and estimated by KPMG and the China Chamber of Commerce to the EU on the basis of authoritative public sources, including Eurostat and the Ministry of Commerce of China, as well as publicly available corporate financial statements and interviews with industry experts. For detailed methodology and data, please refer to Chapters 4 to 6 of this report.

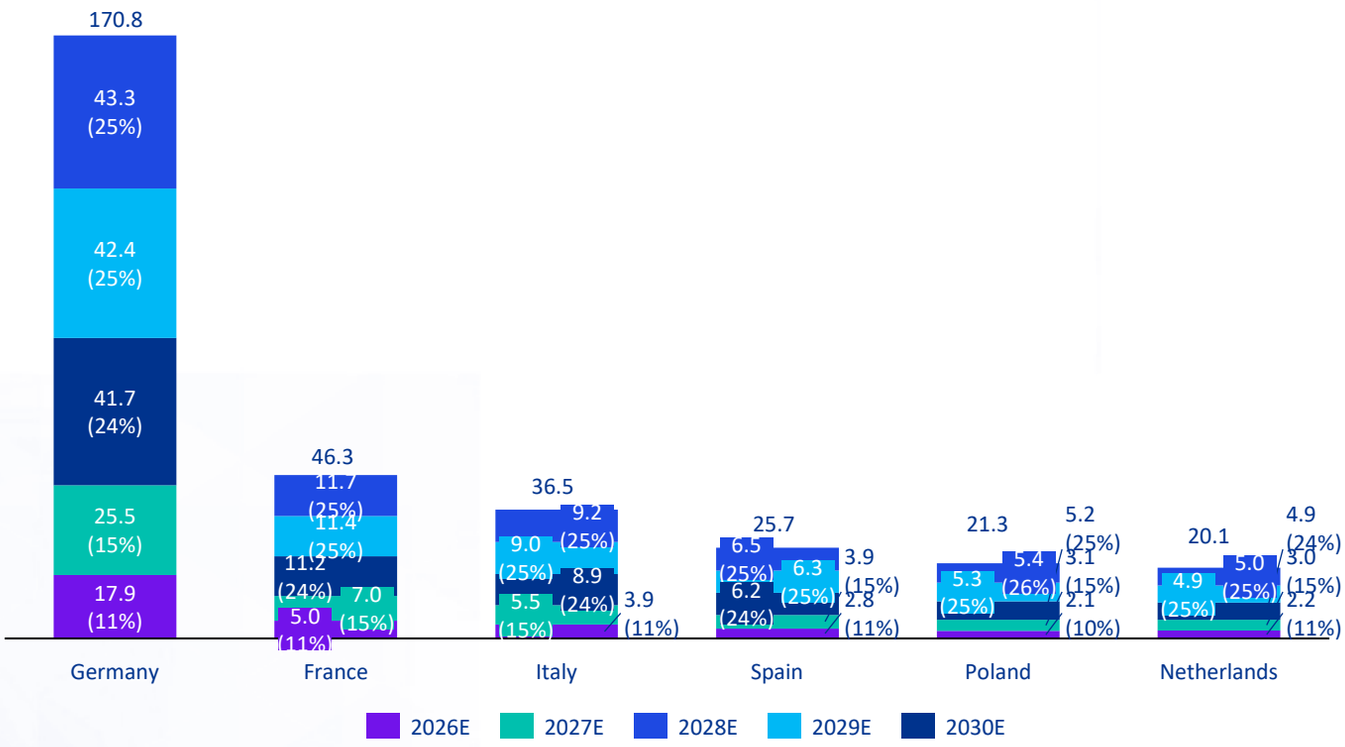
5. The first segment is energy, covering sectors such as solar PV, wind power, and energy storage. The second segment is telecommunications, covering both wireless and fixed networks. The third segment is financial infrastructure, mainly including banking, financial market infrastructures, and digital providers; losses in this segment are related to system availability, disaster-recovery arrangements, data processing, and continuity of digital services. The fourth segment is logistics and manufacturing, mainly including manufacturing, chemical production and distribution, transport, and food production, processing and distribution; impacts in this segment are largely reflected in equipment and system adjustments across production lines, dispatching, warehousing, and delivery systems. The fifth segment is public services, mainly including water systems (drinking water and wastewater treatment) and public administration; industries in this segment are more closely tied to public-budget arrangements and the continuity of public services. The sixth segment is health and research, mainly including healthcare and scientific research, and is characterized more by high-value, high-reliability equipment and specialized analytical requirements.

1.4 Key Finding Four: “One-Size-Fits-All” Regulation Intensifies Economic Divergence Among Member States, Triggering Asymmetric Developmental Imbalances and Fiscal Pressures

The mandatory replacement provisions under CSA2 take no account whatsoever of the substantial heterogeneity among EU member states in industrial structure, fiscal buffering capacity, and the pace of digital transformation. Not only would they be difficult to implement in practice, they would also create severe asymmetric economic pain within the Union.

Member states differ markedly in the development stage of the 18 sectors concerned and in the lifecycle of the equipment deployed, resulting in very different orders of magnitude in the compliance premium they would[6] bear. Estimated losses across the main stress tiers are as follows.

Figure 6: Estimated Total Losses for the High-Pressure Tier of Countries Under EU Mandatory Replacement (EUR billion, %)



3. Compiled and estimated by KPMG and the China Chamber of Commerce to the EU on the basis of authoritative public sources, including Eurostat and the Ministry of Commerce of China, as well as publicly available corporate financial statements and interviews with industry experts. For detailed methodology and data, please refer to Chapters 4 to 6 of this report.

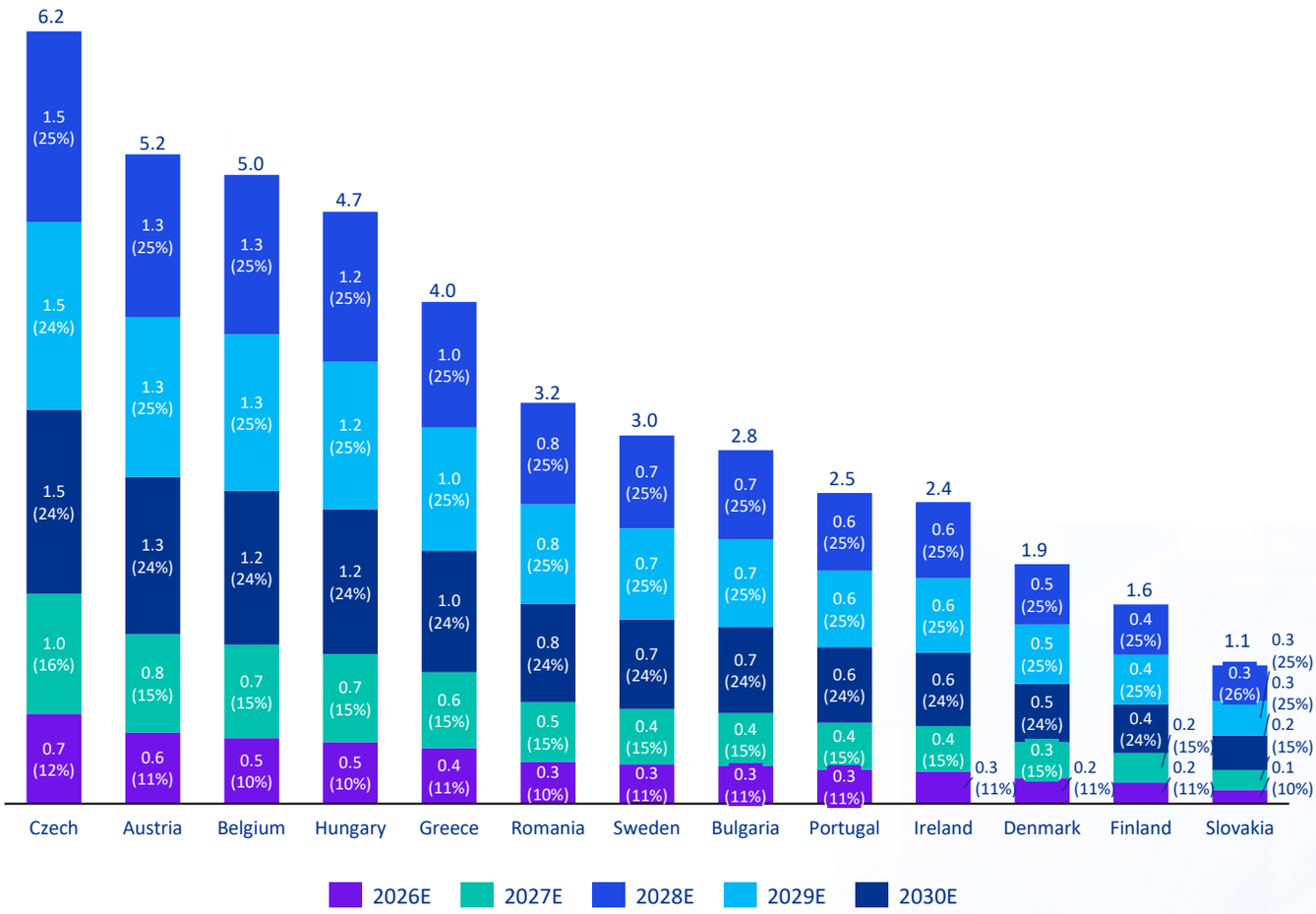
5. The first segment is energy, covering sectors such as solar PV, wind power, and energy storage. The second segment is telecommunications, covering both wireless and fixed networks. The third segment is financial infrastructure, mainly including banking, financial market infrastructures, and digital providers; losses in this segment are related to system availability, disaster-recovery arrangements, data processing, and continuity of digital services. The fourth segment is logistics and manufacturing, mainly including manufacturing, chemical production and distribution, transport, and food production, processing and distribution; impacts in this segment are largely reflected in equipment and system adjustments across production lines, dispatching, warehousing, and delivery systems. The fifth segment is public services, mainly including water systems (drinking water and wastewater treatment) and public administration; industries in this segment are more closely tied to public-budget arrangements and the continuity of public services. The sixth segment is health and research, mainly including healthcare and scientific research, and is characterized more by high-value, high-reliability equipment and specialized analytical requirements.

6. Based on the size of economic losses by member state, this assessment classifies countries with losses above EUR 10 billion as the high-pressure tier, mainly including Germany, France, Italy, Spain, Poland, and the Netherlands. Countries with losses above EUR 1 billion but below EUR 10 billion are classified as the medium-pressure tier, mainly including Austria, the Czech Republic, Hungary, Belgium, Greece, Bulgaria, Romania, Sweden, Portugal, Ireland, Denmark, and Finland. Countries with losses below EUR 1 billion are classified as the general-pressure tier, mainly including Slovakia, Lithuania, Slovenia, Croatia, Estonia, Cyprus, Latvia, Luxembourg, and Malta.

Among the countries in the high-pressure tier, Germany is expected to face the highest total losses, at approximately EUR 170.8 billion, largely reflecting its strong industrial digitalization capabilities and leading green transition. France, Italy, Spain, Poland, and the Netherlands are also projected to incur losses of EUR 46.3 billion, EUR 36.5 billion, EUR 25.7 billion, EUR 21.3 billion, and EUR 20.1 billion, respectively.

Beyond the highest-pressure countries, other member states would also face total losses ranging from hundreds of millions to several billions of euros. These large fiscal gaps would directly worsen public debt positions and force member states into painful resource misallocations between EU compliance obligations and public welfare. Such asymmetric economic burdens would not only intensify political fragmentation within the EU, but could also push some fiscally fragile countries into a trap in which the high cost of digitalization reverses developmental gains, thereby undermining the overall competitiveness of the EU single market.

Figure 7: Estimated Total Losses for the Medium-Pressure Tier of Countries Under EU Mandatory Replacement [3,5](EUR billion, %)

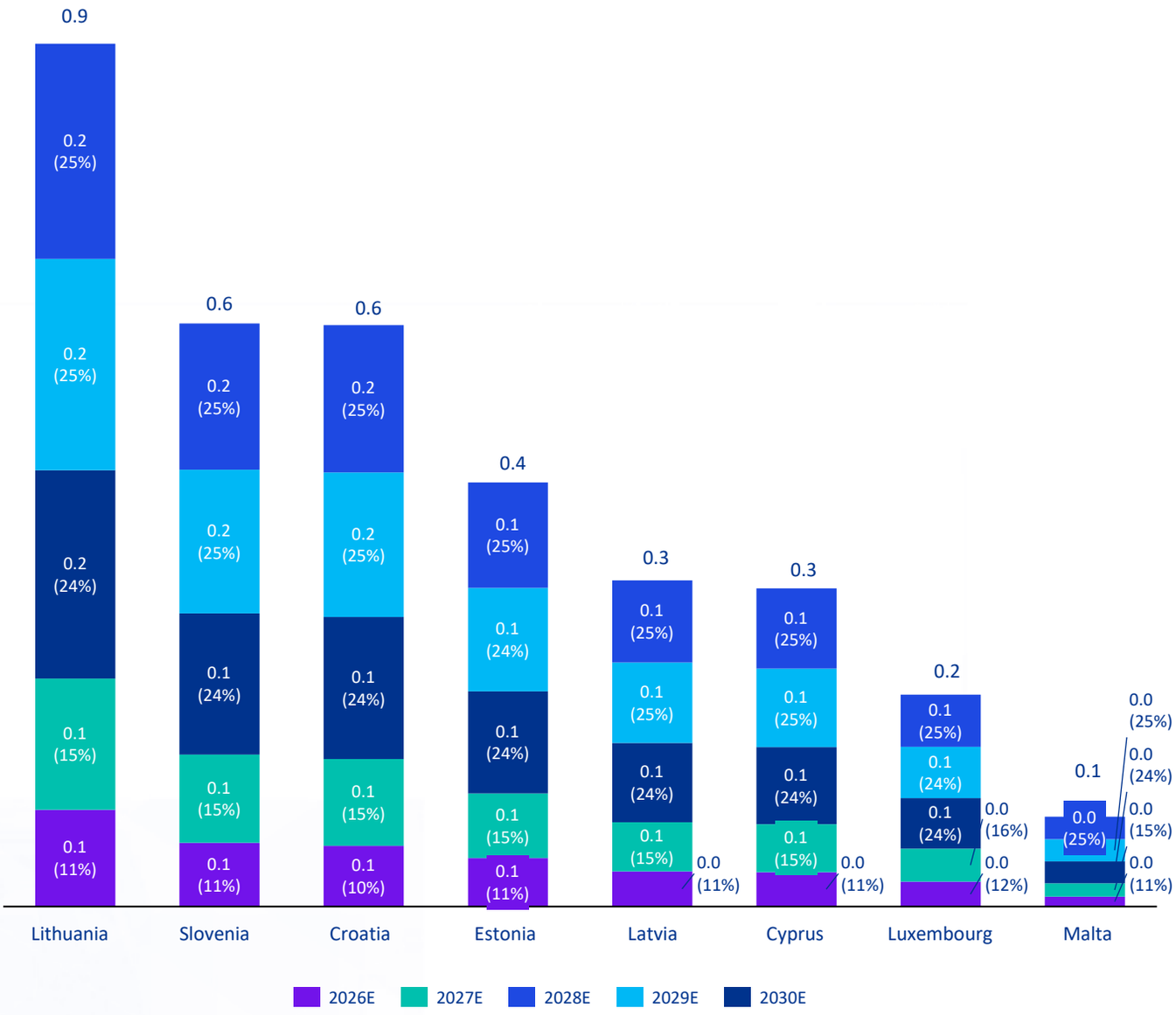


Source: Estimates by the CCCEU and KPMG; authoritative public data; industry and association expert interviews

3. Compiled and estimated by KPMG and the China Chamber of Commerce to the EU on the basis of authoritative public sources, including Eurostat and the Ministry of Commerce of China, as well as publicly available corporate financial statements and interviews with industry experts. For detailed methodology and data, please refer to Chapters 4 to 6 of this report.

5. The first segment is energy, covering sectors such as solar PV, wind power, and energy storage. The second segment is telecommunications, covering both wireless and fixed networks. The third segment is financial infrastructure, mainly including banking, financial market infrastructures, and digital providers; losses in this segment are related to system availability, disaster-recovery arrangements, data processing, and continuity of digital services. The fourth segment is logistics and manufacturing, mainly including manufacturing, chemical production and distribution, transport, and food production, processing and distribution; impacts in this segment are largely reflected in equipment and system adjustments across production lines, dispatching, warehousing, and delivery systems. The fifth segment is public services, mainly including water systems (drinking water and wastewater treatment) and public administration; industries in this segment are more closely tied to public-budget arrangements and the continuity of public services. The sixth segment is health and research, mainly including healthcare and scientific research, and is characterized more by high-value, high-reliability equipment and specialized analytical requirements.

Figure 8: Estimated Total Losses for the General-Pressure Tier of Countries Under EU Mandatory Replacement (EUR billion, %)



Source: Estimates by the CCCEU and KPMG; authoritative public data; industry and association expert interviews

3. Compiled and estimated by KPMG and the China Chamber of Commerce to the EU on the basis of authoritative public sources, including Eurostat and the Ministry of Commerce of China, as well as publicly available corporate financial statements and interviews with industry experts. For detailed methodology and data, please refer to Chapters 4 to 6 of this report.

5. The first segment is energy, covering sectors such as solar PV, wind power, and energy storage. The second segment is telecommunications, covering both wireless and fixed networks. The third segment is financial infrastructure, mainly including banking, financial market infrastructures, and digital providers; losses in this segment are related to system availability, disaster-recovery arrangements, data processing, and continuity of digital services. The fourth segment is logistics and manufacturing, mainly including manufacturing, chemical production and distribution, transport, and food production, processing and distribution; impacts in this segment are largely reflected in equipment and system adjustments across production lines, dispatching, warehousing, and delivery systems. The fifth segment is public services, mainly including water systems (drinking water and wastewater treatment) and public administration; industries in this segment are more closely tied to public-budget arrangements and the continuity of public services. The sixth segment is health and research, mainly including healthcare and scientific research, and is characterized more by high-value, high-reliability equipment and specialized analytical requirements.

1.5 Key Finding Five: Returning to Technological Neutrality and Rejecting Geopolitical Discrimination Is the Rational Choice for Achieving Mutually Beneficial China–EU Cooperation

We strongly recommend that CSA2 return to technological neutrality and economic rationality and avoid sacrificing the EU's supply-chain resilience, competitiveness, industrial innovation, and public interest in the name of security. From the perspective of economic development and governance practice, technological neutrality is a rational choice that balances security, efficiency, and fairness. Its rationality and feasibility have been fully tested in global digital-governance practice. It helps foster a stable and predictable institutional environment and is the most prudent and practical path for ensuring the healthy and orderly development of industry.

The CCCEU expresses grave concern over, and firm opposition to, the proposed mandatory, universal, and time-bound supplier exclusion policy targeting key sectors under CSA2. The proposal's assessment mechanism for "third countries posing cybersecurity concerns" is, in essence, a political screening mechanism rather than an objective security framework, and it seriously lacks evidence-based risk substantiation. By linking trustworthiness to country of origin and other non-technical factors, this discriminatory approach not only violates the principles of equality, non-discrimination, and effective judicial protection established under the Charter of Fundamental Rights of the European Union, but also challenges the legal boundary under the EU Treaties that national security remains a competence of the member states, thereby creating a potential misuse of the legal basis for internal-market coordination.

From the perspective of economic and industrial development, such one-size-fits-all exclusion measures would have far-reaching negative implications for Europe's twin digital and green transition and for the stability of global supply chains. Forcing out existing suppliers—especially requiring the replacement of mobile-network equipment within 36 months in the telecommunications sector—not only departs from the realities of industrial investment cycles, but also leads to high compliance costs and weakens Europe's innovation capacity and market competitiveness. The Chamber stresses that security should not become a tool of protectionism, and de-risking should not evolve into government-led systemic decoupling. It therefore calls on EU institutions to stop pursuing mandatory exclusion, return to a regulatory path that is technologically neutral, evidence-based, and WTO-consistent, and build through inclusive dialogue a cybersecurity framework that balances security with openness.

02

Policy Background and Current Context: China and the EU Have Long Shared a Mutually Beneficial Relationship, Underpinned by Deeply Interwoven Industrial Ties

China and the EU have long been among each other's most important economic, trade, and investment partners, with mutual benefit at the core of the relationship. China's long-term and stable investment in Europe, together with the capital, technology, and market-driven innovation vitality of Chinese enterprises, has supported Europe's economic recovery and shared development, created substantial local employment, promoted technological upgrading and economic growth, and become an important pillar of Europe's economic and social development.

2.1 Key Points of Focus

Over decades of intensive engagement, China–EU cooperation has evolved beyond trade into a highly interconnected economic and industrial relationship characterised by mutual benefit.

China's sustained and stable investment in Europe, together with technological collaboration, has not only injected capital vitality into European markets, created a large number of jobs, and generated considerable tax revenue, but has also provided critical support in areas such as infrastructure upgrading, green transition, and digital-industry development, making it an important external force for Europe's stable economic growth and enhanced industrial competitiveness.

Chinese enterprises have complied with relevant EU regulatory requirements and have cooperated with stringent EU oversight and security reviews, while building a strong foundation of professional trust with European clients through measures such as source-code audits, compliance certification, and local governance arrangements. Existing cooperation reflects not short-term price considerations, but of long-term market competition and institutional adaptation.

If supply chains are unilaterally stripped apart and existing ecosystems of cooperation are artificially severed, this would not only weaken investment and growth momentum in relevant European industries, increase corporate costs, and slow transformation, but also erode the mutual-trust foundation and win-win pattern of cooperation built over the long term, ultimately having a negative impact on Europe's own economic interests and development capacity.

2.2 The Foundations of China–EU Mutual Benefit Are Deep and Enduring, and China Has Become a Stable and Sustainable Support for EU Industrial and Economic Development

Since the formal establishment of diplomatic relations between China and the European Community in 1975, China–EU relations have taken a historic step forward. In 1998, the two sides established a constructive partnership and institutionalized high-level dialogue, accelerating cooperation across the board. In 2003, China and the EU formally established a comprehensive strategic partnership, ushering bilateral cooperation into a golden period marked by breadth, depth, and wide-ranging engagement.

Over the decades, China and the EU have consistently remained among each other's most important economic, trade, and investment partners. Their cooperation has long surpassed simple trade in goods and has evolved into a community of shared interests deeply integrating capital, industry, and technology. China's sustained and stable investment in Europe has injected strong momentum into European economic growth, employment expansion, and industrial transformation, while the two sides have continually deepened mutual trust and coordination through mutually beneficial cooperation, jointly building a stable and resilient bilateral partnership. Through tangible capital investment, industrial deployment, and technological collaboration, China has provided solid support for Europe's growth, job creation, and industrial transformation, and the two sides have continuously strengthened the foundations of cooperation, forging a close partnership defined by mutual trust, mutual support, and shared development.

Bilateral trade and investment between China and the EU have continued to grow rapidly in both scale and quality. When diplomatic relations were first established in 1975, trade in goods between the two sides amounted to only USD 2.4 billion. By the end of 2025, total bilateral trade in goods had reached USD 828.1 billion,[7] making China and the EU each other's second-largest trading partners. In 2025, China's non-financial direct investment in Europe increased by 20.9% year on year[8]. We believe that China–EU investment cooperation remains highly resilient and will continue to offer substantial opportunities in the future.

Manufacturing has occupied an important place in China's investment in Europe. In recent years, the focus of Chinese investment in Europe has further shifted from mergers and acquisitions toward greenfield investment, with greater concentration in automobiles, batteries, energy equipment, and related manufacturing activities. Chinese investment in Europe rebounded to approximately EUR 10 billion in 2024,[9] up 47% from the previous year, with electric vehicles, batteries, and related manufacturing projects remaining key drivers of that investment. The recovery in China's completed outbound investment in 2024 was mainly driven by capital-intensive greenfield projects, while the automotive sector became an important contributor.[10]

Figure 9: Stock of China's Direct Investment in EU Member States[11] (USD 10,000)

Country/Region	2022	2023	2024
Ireland	167,618	203,857	315,537
Estonia	518	169	161
Austria	52,392	57,297	81,259
Bulgaria	14,214	15,525	12,870
Belgium	41,415	35,365	39,416
Poland	64,510	78,942	102,308
Denmark	31,908	32,126	31,944
Germany	1,855,056	1,706,352	1,801,368
France	481,426	462,281	361,493
Finland	72,141	46,278	21,171
Netherlands	2,830,170	3,189,027	3,842,228

7. General Administration of Customs, 2025 annual import and export performance, http://www.scio.gov.cn/live/2026/37809/tw/

8. Ministry of Commerce of the People's Republic of China, 'China's Outbound Investment and Cooperation in 2025,' January 2026, https://www.mofcom.gov.cn/article/ae/ai/202601/20260103530821.shtml

9. MERICS and Rhodium Group, 2024 annual update.

10. Rhodium Group global investment report: https://merics.org/en/report/chinese-investment-rebounds-despite-growing-frictions-chinese-fdi-europe-2024-update

11. Ministry of Commerce of the People's Republic of China, Statistical Bulletin of China's Outward Direct Investment, b62b8a78eadd4f92898d27286fd5209b.pdf

Figure 9: Stock of China's Direct Investment in EU Member States, 2022–2024 (USD 10,000)

Country/Region	2022	2023	2024
Czech Republic	31,917	69,518	76,094
Croatia	24,248	37,009	18,056
Latvia	2,064	2,273	1,242
Lithuania	923	2,675	2,135
Luxembourg	2,055,460	2,286,848	2,515,362
Romania	22,022	23,469	28,459
Malta	3,140	3,454	2,936
Portugal	2,503	5,331	8,208
Sweden	1,867,481	1,345,773	1,751,383
Cyprus	13,546	13,911	15,506
Slovakia	433	354	564
Slovenia	47,349	54,562	52,057
Spain	118,581	169,386	174,255
Greece	12,522	12,907	9,450
Hungary	58,066	108,674	152,314
Italy	247,626	278,876	267,627
Total	10,119,250	10,242,241	11,685,402

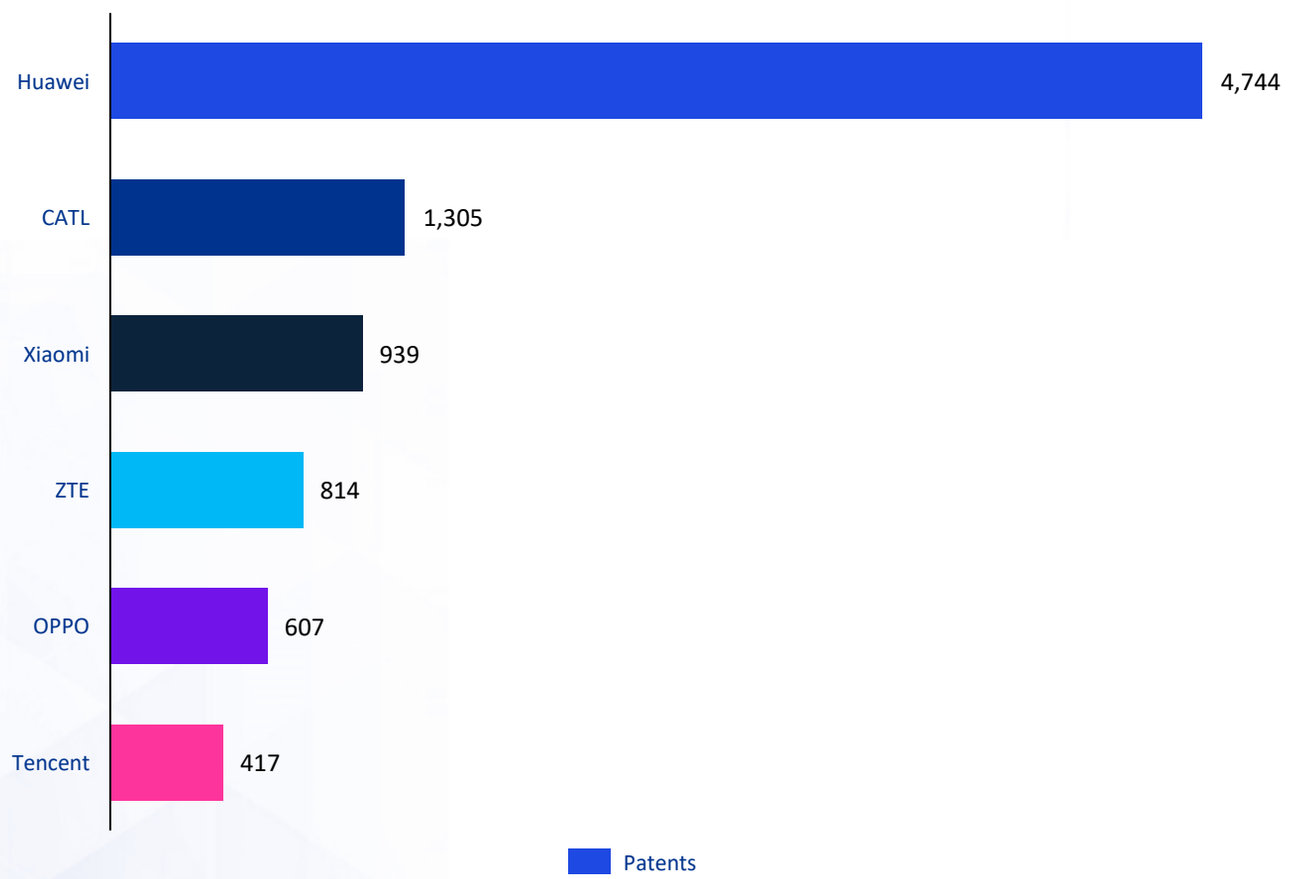
Chinese investment has brought competitive vitality and supplier diversity to the EU market. During the recovery from the financial crisis and the post-pandemic period, Chinese capital provided long-term and steady support. Through close cooperation with European companies, the two sides achieved mutual benefit in areas such as jointly developing third-party markets and jointly developing standards, thereby effectively maintaining the stability of global supply chains.

2.3 Chinese Enterprises Contribute to Industrial Upgrading in Europe Through Technology and Have Become an Important Participant in the EU's Economic Development

Chinese companies' investment in Europe is not merely a capital injection; it has also promoted local industrial upgrading through upstream and downstream supply-chain collaboration and other mechanisms.

From the perspective of innovation contribution, Chinese enterprises are already deeply integrated into Europe's patent and standards systems. With 4,744 European patent applications, Huawei ranked second among EPO applicants in 2025, while CATL, Xiaomi and ZTE also entered the top 20 with 1,305 and 939, and 814 European patent applications, respectively[12]. In terms of standardization, Chinese enterprises have long participated in the work of European standard-setting bodies such as ETSI and have remained highly active in 5G standard-essential patents and proposals for international standards. These facts show that the contribution of Chinese enterprises to Europe extends beyond investment and employment to include patents, technical standards, and innovation ecosystem building. An open and predictable market environment is an essential foundation for Europe to continue attracting global R&D resources, sustaining its influence over standards, and enhancing industrial.[13]

Figure 10: Number of European Patents Filed by Chinese Enterprises (units)



12. EPO《Patent Index 2025》

13. Patent Index 2025 - Statistics at a glance，https://link.epo.org/web/about-us/statistics/en-patent-index-2025-at-a-glance.pdf

Chinese enterprises are deeply embedded in Europe's innovation ecosystem and have broadly established joint R&D centers, joint laboratories, and innovation centers with European universities, research institutions, and companies across digital technology, new energy, automobiles, biomedicine, and advanced manufacturing, making them an important platform for China–EU technological collaboration.

Chinese enterprises have also become deeply embedded in Europe's local supply chains and are an important source of revenue for local European SME suppliers. Nearly half of Chinese enterprises operating in Europe have achieved deep supply-chain localization. As of last year, about 47% of Chinese enterprises in Europe sourced more than 50% of their total procurement from[14] within Europe, providing strong support for local EU industrial chains and employment.

Chinese enterprises have deepened ongoing investment in green sectors such as solar-plus-storage and power batteries, as well as in digital infrastructure fields such as 5G networks, contributing through pragmatic cooperation to the EU's timely achievement of its low-carbon and Digital Decade strategic goals while continuously generating substantial tax revenues in support of social welfare and infrastructure development.

Case

In Germany's 5G networks, Chinese suppliers have used leading Massive MIMO technology to help German telecom operators achieve high-speed network coverage from dense urban areas to remote rural regions. Compared with relying on high-premium single-source equipment, this diversified supply directly advanced Germany's timetable for large-scale commercial 5G deployment by at least 12–18 months. By entering into public-law contracts with operators, the German government calibrated security requirements and compliance obligations to the risk profile of different components, thereby avoiding the disproportionate costs and inefficiencies associated with a one-size-fits-all regulatory approach.

If Chinese suppliers' equipment were subject to mandatory replacement, European telecom operators would struggle to meet delivery schedules and government coverage obligations on time. This would directly affect operators' financial performance, expose them to punitive fines, and indirectly hinder national progress toward digitalization targets. Telecom operators are also pursuing multi-vendor strategies and network-architecture optimization to diversify risk and keep security risks manageable.

> We should keep all doors open, learn from the best, wherever they come from, and not becoming dependent on anyone. In network architecture, DT introduces external RAN equipment through a multi-vendor strategy while pursuing in-house development at the critical control layer, thereby balancing an open ecosystem with technological [15]
>
> ——Tim Höttges, CEO of Deutsche Telekom, March 2026

14. China Chamber of Commerce to the EU and Roland Berger, Report on the Development of Chinese Enterprises in the EU 2025/2026, based on a survey of 205 enterprises.

15. https://www.mwcbarcelona.com/agenda/sessions/6091-keynote-4-what-does-strategic-tech-sovereignty-mean-for-europe. The above comments are summarized based on the original text in the official video.

Case

High-efficiency antennas and low-power 5G macro base stations supplied by Chinese enterprises to Spanish telecom operators consume 15% less energy than equipment from European vendors while delivering roughly 30% higher energy[16] efficiency. Against a backdrop of highly volatile energy prices, this represents not only technological leadership but also direct support for Spanish operators in preserving their profit margins, thereby allowing more budget to be devoted to cutting-edge 6G pre-research.

At a critical stage in the evolution of 5G, Chinese suppliers, through efficient R&D conversion and engineering delivery, have significantly lowered the capital expenditure threshold for European operators while also stimulating market competition in the EU through a "a salutary competitive effect." Despite turbulence in the global geopolitical environment, the stock of assets and localized contribution of Chinese enterprises in Europe has continued to demonstrate strong strategic resilience.

2.4 Compliance and Transparency: Chinese Management Systems Have Stood Up to Long-Term Professional Scrutiny

Cybersecurity and supply-chain governance can be advanced on the basis of technical review, transparent compliance, and continuous verification.

Chinese enterprises were among the first in the world to pass the GSMA Network Equipment Security Assurance Scheme (NESAS) assessment and ICCC security certification, and they have established multiple source-code audit centers in Europe, including in Bonn, Germany. This posture of "opening the door to scrutiny" demonstrates that security is something to be verified, not merely presumed.

Chinese enterprises' compliance practices within European and international security assessment systems have already produced a number of verifiable cases. First, at the level of the international mobile communications industry, GSMA announced in 2020 that major network equipment suppliers such as Huawei and ZTE had completed assessments under NESAS covering product development and lifecycle management processes. NESAS, jointly defined by GSMA and 3GPP, is intended to provide a unified industry security assurance framework for network equipment.

The case demonstrates that supplier security can be verified through unified standards, independent assessment, and lifecycle management processes, rather than judged solely on the basis of origin [17].

17. https://www.mobileworldlive.com/zte-updates-2019-20/zte-obtains-the-cc-eal3-certificate-for-its-otn-products/

With respect to transparent local review mechanisms in Europe, Chinese enterprises established cybersecurity laboratories in Brussels and elsewhere in 2019. These laboratories are open to customers, regulators, and other stakeholders, and support independent security assessment of products, services, and processes, including source-code review, document review, black-box testing, and penetration testing. This practice shows that security governance can be built on open review, verifiable processes, and sustained regulatory engagement, without relying entirely on one-off judgments based on country-of-origin labels. [18]

BYD is a representative case of a Chinese new-energy vehicle company implementing data and cybersecurity compliance in Europe. As its business has continued to expand across markets such as Germany, France, the Netherlands, and Spain, BYD has had to comply with the EU General Data Protection Regulation (GDPR) and related member-state regulatory requirements in the operation of intelligent connected vehicles, establishing localized compliance mechanisms covering in-vehicle data collection, user authorization management, remote services, cross-border data transfer, and information security. At the same time, NEV products entering the European market must comply with UNECE Regulation R155 on vehicle cybersecurity and Regulation R156 on software update management, and satisfy EU whole-vehicle type-approval requirements. BYD's continued expansion into multiple European member states and its localization investments in places such as Hungary indicate that it already possesses the integrated capability needed to meet European-market requirements in product safety, data governance, and digital compliance. This case shows that compliance by Chinese automakers has extended from manufacturing into higher-standard domains such as data governance, software management, and cybersecurity governance. [19]

Over many years, Chinese enterprises have strictly complied with EU laws and regulations and established mature and transparent compliance-governance systems. Under more than a decade of stringent scrutiny by regulators across Europe, such as Germany's BSI and the UK's NCSC, mainstream Chinese equipment suppliers have never been found to have any technical backdoors or data-breach violations. This clean record of zero violations is itself long-term proof of their compliance. Through more than a decade of full-spectrum transparent governance, Chinese enterprises have built records that are transparent and capable of withstanding audit.

The facts demonstrate that compliance is not determined by country of origin, but by whether regulatory rules are clear and whether processes and code are transparent. Through long-term compliance practices, Chinese enterprises have already established de facto professional trust. If the EU selectively disregards this time-tested and reproducible security evidence and instead adopts discriminatory country-of-origin labels, the damage would extend not only to the interests of Chinese enterprises, but also to the consistency, fairness, and authority of the EU legal system as a whole.

Chapter Summary: Strong Foundations for China–EU Cooperation; Partnership and Development Remain the Right Path

Since the establishment of diplomatic relations, China and the EU have maintained close and pragmatic cooperation over the long term, forming a stable pattern of deep interdependence and mutual benefit.

China has continued to expand investment in Europe and maintained steady input across many fields, including new energy, digital infrastructure, and advanced manufacturing. This has not only provided strong support for EU economic growth, job creation, and industrial transformation, but has also helped the EU realize its carbon and digital strategy goals through technological innovation and green solutions.

Over the long term, Chinese enterprises have adhered to compliant operations and transparent management. Their operating systems are fully recorded, traceable, and auditable, and can withstand both professional scrutiny and the test of time.

Chinese enterprises have always been an important positive force for EU economic stability and industrial upgrading, while China–EU industrial and supply chains remain complementary and deeply intertwined in interests. Only by adhering to mutual respect, professional compliance, and open cooperation, rejecting the tendency to over-securitize, and returning to technology and markets themselves can the two sides truly realize complementary advantages and win-win development, and promote the steady and sustained advancement of the China–EU comprehensive strategic partnership.

18. https://www.reuters.com/article/us-zte-cyber-brussels/chinas-zte-follows-huawei-with-brussels-cybersecurity-lab-idUSKCN1U51FW/

19. https://www.byd.com/eu/privacy

03

Assessment of Expected Policy Effects: The Overextension of Geopolitical Considerations Undermines Multilateral Order and Heightens Development Risks

In recent years, EU policy toward China has increasingly framed the country as a “systemic rival” and “competitor,” while placing less emphasis on “cooperation” and “partnership.” In the economic and trade sphere, the EU has actively pursued an “economic security” strategy and sought to reduce dependence on China, leading to a growing politicization of economic and trade issues. This approach is unlikely to achieve genuine security objectives; instead, it risks undermining the rules-based multilateral trading system and introducing greater uncertainties for the economic and industrial development of both China and the EU.

3.1 Key Points of Focus

The identification of “high-risk suppliers” is shifting from technical review toward origin-based judgment. The vague and overly broad definitions in CSA2 have already triggered doubts and opposition within the EU. The exclusion and replacement measures targeting high-risk suppliers carry significant legal risks, violating the principles of proportionality and non-discrimination while reversing the burden of proof and providing insufficient rights of defense. Their legality is therefore doubtful. Rather than truly strengthening EU cybersecurity, they are more likely to trigger large compensation claims and international trade frictions, creating substantive obstacles to EU industrial development.

From the perspective of Europe’s overall strategy, the proposal would further slow the EU’s already significantly delayed Digital Decade agenda and create a two-sided squeeze on the green transition, thereby undermining Europe’s strategic layout in digital infrastructure and energy decarbonization. From the market and corporate perspective, the mandatory replacement mechanism would impose huge and irreversible cost burdens on EU operators and related enterprises, crowding out key investment in 5G, fiber, AI, and green energy, and leading to weaker innovation capacity and diminished industrial leadership. At the same time, the proposal would gradually erode public wellbeing and the public interest through higher prices for public services and changes in network coverage and quality, thereby increasing the burden on livelihoods. This increase in political intervention “in the name of security” would significantly damage the EU’s global investment reputation, international influence, and long-term growth momentum.

Both internal EU cases and examples from elsewhere in the world show that such measures are not only inefficient to implement and highly wasteful of resources, but are also unlikely to achieve long-term and stable industrial and security objectives. At the same time, they can inflict irreparable damage on global investor confidence and on the EU’s reputation.

3.2 The Black Box of the High-Risk Supplier Definition: The Shift from Rational Technical Regulation to Geopolitical Discrimination

Under the EU’s current cybersecurity framework, including the Cybersecurity Act and the 5G Toolbox, the criteria for identifying “high-risk suppliers” remain highly subjective and arbitrary.

CSA2 still does not provide quantified and auditable technical security indicators. Instead, it assigns core weight to non-technical dimensions such as a “supplier’s links with the government of a third country” and “the legal environment of that country.” In practice, this grants regulators extremely broad administrative discretion and shifts security review away from examining code vulnerabilities toward examining corporate headquarters coordinates.

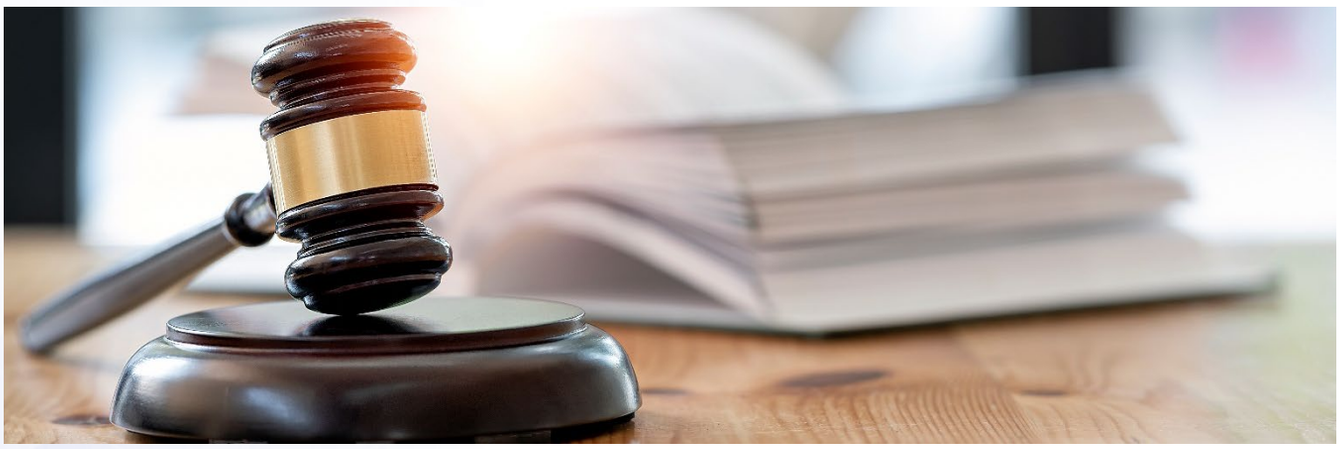
> “CSA2 adopts an extremely broad definition of control, based on the capacity to exert decisive influence directly or indirectly. This vague and overly expansive definition means that even a company with a high degree of operational independence may still be included within the scope of a high-risk supplier if it has shareholding links, management arrangements, or control relationships with a country under scrutiny. Under such a framework, joint ventures, affiliated companies, contract manufacturers, and even relatively independent subsidiaries all face the legal risk of being implicated by association.”
>
> ——A leading EU law firm

Since its release, the provisions in CSA2 concerning the definition of high-risk suppliers and mandatory replacement have triggered widespread controversy and strong opposition within Europe. Multiple industry associations and political groups have openly voiced clear objections, arguing that the definitions are overly broad, rely excessively on non-technical criteria, impose very high replacement costs, and offer insufficient security benefits, while broadly calling for a prudent regulatory approach grounded in empirical risk evidence.

> DIGITALEUROPE supports efforts to make the EU cybersecurity certification framework more effective, and predictable. Strong industry involvement and a clear focus on usability will be critical to ensuring that certification enhances trust without distorting competition.[20]
>
> ——DIGITALEUROPE, January 2026

In April 2026, the European Telecommunications Standards Institute (ETSI) formally responded to the CSA2 proposal and expressed concern that restrictions on "high-risk suppliers" and the expanded role of ENISA could affect the integrity of Europe's standardization system. As one of the three European standardization organizations recognized by the EU, ETSI stressed that the European standardization system should continue to uphold the principles of openness, fairness, and non-discrimination, and should avoid turning the standards-setting process into a political process driven by non-technical considerations. ETSI also noted that industry-led harmonized standards are more conducive to global uniformity and broad adoption, and that ENISA's role should focus more on interpreting the legal framework, conducting risk assessment, and providing technical guidance, rather than replacing standards bodies and industry experts in the standards-setting function. These views indicate that preserving the openness and professionalism of Europe's standardization system is itself an important condition for strengthening Europe's cybersecurity governance capacity and international influence[21] .

There is no doubt that the regulatory design of CSA2 around high-risk suppliers has already generated dissatisfaction and skepticism within the EU. The controversy does not lie in whether the security objective is legitimate, but in what standards, procedures, and boundaries should govern the way that objective enters market governance. Member states such as Germany, Spain, Finland, and Austria have required operators under relevant legislation to conduct supply-chain risk assessments or formulate replacement plans, yet none of them has designated any specific high-risk country or high-risk supplier. Unless the relevant provisions are adjusted on the basis of technical risk, cost-effectiveness, and fair competition, they may become geopolitical tools rather than genuine cybersecurity measures, thereby creating real obstacles to EU industrial development.



20. https://www.digitaleurope.org/news/cybersecurity-act-review-certification-can-boost-security-and-competitiveness-if-europe-gets-it-right/

21. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14578-The-EU-Cybersecurity-Act/F33393088_en

3.3 Legal and Procedural Risks: The High-Risk Supplier Exclusion Mechanism Conceals Multiple Systemic Legal and Trade Risks

Under the framework of the CSA2 Proposal, the measures including exclusion and replacement targeting **High-Risk Supplier (HRS)** manifest conspicuous deficiencies in **legal basis, proportionality principle, and procedural safeguards**. These measures raise serious doubts as to their legality and further trigger controversies over legality, and further give rise to investor-State arbitration under BIT, **Administrative litigation, Constitutional litigation and multi-tiered legal challenges.**

From the perspective of substantive law, the measures carry a high risk of illegality, centering on the tension between proportionality and non-discrimination. EU law requires that public intervention satisfy suitability, necessity, and strict proportionality. However, the CSA2 Proposal's **Blanket Exclusion** rests not on concrete product or technology risks, but on supplier's country of origin or abstract security assessments. This is hard to justify as the least restrictive means of achieving cybersecurity, especially where alternative tools—**certification, risk assessment, tiered management**—already exist, making it prone to being found excessive. If the measures in practice target specific countries or firms, they may breach the non-discrimination and fair competition principles of EU **Internal Market law**. Should the measures mandate removal of installed equipment, they may constitute an undue restriction on property rights, or even amount to a **de facto expropriation** resulting in compensation.

Procedural flaws further heighten the risk of illegality, most notably through **burden-shifting** and deficient **hearing rights**. Under the CSA2 Proposal, the risk-assessment framework effectively requires suppliers to prove they pose no risk, rather than regulators demonstrating a concrete threat. This shift **undermines the legitimacy of administrative decisions**. While the right to be heard exists formally, suppliers often lack access to sufficient material for an effective defense due to restricted disclosure—whether on national security or sensitivity grounds. This violates the EU principles of **good administration and effective remedy**, exposing decisions to **annulment in Administrative Litigation**. In short, even a legitimate security objective **cannot cure procedural defects that renders the measures unlawful.**

For international and investment law, the measures may expose Member States to international investment disputes and substantial damages. All EU members except Ireland have Bilateral Investment Protection Agreements (BIPAs)with China. Where affected enterprises are Chinese investors, their investments in these countries—telecommunications equipment, infrastructure—enjoy treaty protection. **Mandatory replacement or exclusion gives rise to claims of indirect expropriation or breach of fair and equitable treatment (FET) under BIPAs**. Lack of transparency, unpredictability, or discriminatory implementation may also violate members' obligations under BIPAs. Chinese investors may initiate international investment arbitration in accordance with suspected breaches. Awards in such cases are routinely enormous. Critically, even where the legislation originates at EU level, the financial liability falls on Member States, creating a spillover of fiscal pressure and policy risk.

At both EU and Member State levels, these measures face equally significant challenges from administrative litigation and Constitutional litigation, creating a multi-tiered litigation landscape. Affected suppliers and operators are entitled to challenge specific administrative decisions, implementing measures, or the legislative basis itself through judicial review before the CJEU or national courts. Such review typically examines proportionality, procedural defects, fundamental rights infringement, and ultra vires issues. **Findings of incompatibility with EU law may not only annul the decision at hand but also force regulators to recast the overall policy framework**. Beyond this, enterprises may bring civil claims for breach of contract—damages for forced termination of long-term service agreements, for instance. This interplay of administrative, civil, and international arbitration proceedings will materially increase legal uncertainty and prolong the dispute resolution cycle.

Furthermore, the CSA2 Proposal is suspected of violating multiple WTO rules and EU WTO commitments, including several principles and rules of the General Agreement on Tariffs and Trade 1994 (GATT 1994); principles and rules of the General Agreement on Trade in Services (GATS), thus breaching EU WTO commitments; the Agreement on Subsidies and Countervailing Measures (SCM Agreement), constituting prohibited subsidies; the Agreement on Technical Barriers to Trade (TBT Agreement); and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). WTO challenges by affected states risk acute international economic friction amid sharpening geopolitical tensions, with collateral damage to multilateral trade order and cross-border economic cooperation.

In sum, the CSA2 Proposal carries systemic, spillover risks that can escalate from a discrete regulatory issue into sweeping legal and economic disruption. The layering of illegality disputes, BIT arbitration, and multi-tiered litigation will inflate Member States' fiscal exposure while eroding the stability and predictability of the EU legal order. More fundamentally, this uncertainty will corrode market confidence in the regulatory environment, distorting long-term investment and supply chain decisions. Institutional refinement should therefore prioritize: clear risk criteria, robust procedural safeguards, strict proportionality, and targeted, verifiable tools, to strike a durable balance between security and the rule of law.

3.4 EU-Wide Strategic Delay: Dual Obstacles to the "Digital Decade" and the Green Transition

By implementing mandatory exclusion through politicized definitions, CSA2 would undoubtedly strike directly at the EU's two core strategic objectives—the Digital Decade and the Green Transition—thereby creating a form of strategic self-obstruction.

Through a supplier-exclusion mechanism that is neither technical nor risk-based, the proposal would artificially fragment the deeply integrated global ICT ecosystem. A one-size-fits-all 36-month replacement requirement for mobile-network equipment would force large amounts of engineering resources to be diverted toward stock replacement rather than new deployment. The EU's Digital Decade agenda is already significantly behind schedule, with key targets repeatedly delayed[22]; this round of mandatory replacement would further raise infrastructure costs, crowd out resources for 5G/6G and fiber deployment, and slow the uptake of AI and cloud technologies, making the Digital Decade targets even harder to achieve and potentially delaying them once again.

A February 2024 report by network-quality testing agency MedUX indicated that London—where Huawei had been excluded from 5G construction—was among the European cities with the weakest network experience. MedUX stated that, given that the Huawei ban was imposed after the UK had already begun deploying 5G, the measure likely affected overall 5G coverage, availability, and user experiences. [23]

> UP KRITIS want to give feedback to the 4 main topics in the revision of the Cyber Security Act (CSA2) in the attached position paper 1. Expanded ENISA Mandate 2. EU wide ICT supply chain security framework 3. Reform of the EU cybersecurity certification framework 4. Closer Alignment with existing EU cyber security regulation. [24]
>
> ——UP KRITIS, April 2026

> If these obligations are not grounded in robust, evidence-based risk assessments and supported by mitigating measures such as cost reimbursement mechanisms, they will materially and adversely impact network deployment, operational continuity and investment planning.[25]
>
> ——Connect Europe, January 2026

22. European Commission, 2025 State of the Digital Decade Report (2025-06-16).
23. MedUX report: https://medux.com/blog/all-5g-networks-are-not-created-equal-unveiling-true-qoe-5g-europe-ii
24. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14578-The-EU-Cybersecurity-Act/F33387335_en
25. https://connecteurope.org/news/connect-europe-statement-cybersecurity-act

At the same time, reduced supply-chain diversity and constrained technology choice would significantly lower the efficiency of EU green-infrastructure construction, forcing delays in the upgrading of critical infrastructure and causing costs to soar. The financial feasibility of the EU's green transition objectives would face a severe blow. The issue is not merely one of financial burden, but also one of Europe's political credibility in fulfilling its climate commitments.

3.5 Market and Corporate Pressure: Innovation Crowding-Out and a Downward Spiral in Economic Efficiency

CSA2 would trigger a dual vicious cycle of innovation crowding-out and spiraling declines in economic efficiency.

Non-market access restrictions weaken competition, reduce supplier choice, and increase procurement and maintenance costs, leading to supply concentration, price increases, and declining service quality in key fields. As compliance costs continue to accumulate, investment payback periods lengthen, and market uncertainty intensifies, the global competitiveness of European enterprises would gradually weaken and willingness to invest from abroad would decline. The result would be a downward spiral of "rising costs—slower innovation—declining competitiveness—shrinking investment," seriously damaging the vitality of the EU single market and its long-term growth potential.

26.GSMA Europe: https://www.gsma.com/about-us/regions/europe/news/gsma-statement-on-cybersecurity-act-proposals-on-behalf-of-european-mobile-operators/

27. https://www.businesseurope.eu/wp-content/uploads/2026/01/2026-01-22-BusinessEurope-Omnibook-to-reduce-regulatory-burden.pdf

28. https://techpost.bsa.org/2026/04/22/bsa-survey-europeans-value-openness-security-and-quality-in-choosing-tech-services/

EU enterprises would also face a systemic drain on innovation momentum. Firms would be forced to divert substantial capital, human resources, and R&D resources into supplier replacement, compliance review, system reconstruction, and repetitive certification, directly crowding out spending on frontier technology R&D, product innovation, and digital transformation—creating an "innovation squeeze" driven by security compliance. In addition, the audit fees, consulting fees, and litigation costs generated by these potential non-technical reviews amount to a costly "regulatory burden tax." This would not only lower the return on capital for European companies and weaken their endogenous growth momentum, but also saddle them with heavy additional costs in competition with major Chinese and US technology firms.

> Industry is already navigating overlapping cyber obligations under NIS2, the Cyber Resilience Act and sectoral rules. Any new supply chain security measures must therefore be proportionate, justified by clear risk assessments and designed to align with existing frameworks. [29]
>
> ——Digital Europe, January 2026

3.6 Social Premiums Paid: The Gradual Erosion of Social Interests and Public Wellbeing

The broad securitization embodied in CSA2 would gradually erode public wellbeing and the broader public interest in an indirect and incremental way. This would be reflected not only in household bills, but also in the hidden deterioration of the quality of social services.

The supply-chain restructuring and rising costs triggered by the proposal would ultimately be passed through to end users in many forms, including public-service prices, telecommunications charges, energy bills, and the quality of digital public services. The costs of mandatory replacement in key sectors such as telecommunications, energy, transport, and healthcare would ultimately be borne jointly by governments and consumers, thereby increasing living costs and public fiscal pressure.

Reduced supplier diversity and constrained technology choice would lead to poorer network coverage, slower service upgrades, and delayed diffusion of digital services, widening urban-rural and regional digital divides and passively shrinking social fairness in the name of regulatory security. At the same time, a regulatory orientation driven by politics rather than technological neutrality would gradually erode the social foundations of market fairness, open innovation, and consumer choice, producing a welfare squeeze carried out in the name of geopolitics.

Although the UK is no longer part of the EU, the price pass-through mechanism in its telecommunications sector remains instructive for Europe. In 2024, operators including BT, Vodafone, and Three continued to implement inflation-linked pricing clauses in customer contracts, with BT customers seeing tariffs rise by 7.9% from April and Vodafone and Three confirming the same 7.9% increase. Vodafone's own website also illustrated that, under a CPI + 3.9% mechanism, a customer paying GBP 22 per month would pay GBP 1.61 more per month, while a customer paying GBP 40 per month would pay GBP 2.92 more. This case shows that investment, inflation, and cost pressures in communications networks can often be passed through to end users relatively quickly via contractual mechanisms[30] .

29. https://www.digitaleurope.org/news/cybersecurity-act-review-certification-can-boost-security-and-competitiveness-if-europe-gets-it-right/

30. https://www.theguardian.com/money/2024/jan/17/uk-mobile-broadband-price-inflation-rises-vodafone

Over the longer term, such unnecessary regulatory intervention would reduce overall social welfare, widen inequality, and undermine the EU's citizen-centered digital and social development goals.

> A truly competitive and innovation-friendly Digital Single Market requires harmonised rules, coherent enforcement, proportionate risk-based obligations, and practical compliance mechanisms.[31]
>
> ——EuroISPA, March 2026

3.7 A Warning from the EU's Own History: The Practical Costs of Reversing Infrastructure Policy

In the operation of long-cycle infrastructure, the EU has previously faced governance difficulties arising from abrupt policy shifts. The costs created by such policy reversals are typically not realized all at once when the policy is announced, but continue to unfold over a long period and ultimately impose a heavy fiscal burden on governments.

Case

Following the Fukushima accident in 2011, Germany decided to accelerate the phase-out of nuclear power, thereby shortening the operating life and investment recovery period of existing nuclear assets. In 2016, the German Federal Constitutional Court ruled that the relevant legislation had, in certain respects, infringed the operators' property rights and required lawmakers to establish reasonable compensation arrangements through supplementary legislation. This led to a legal battle lasting a full decade, during which the Court repeatedly ruled that the government had infringed lawful property rights. The matter was ultimately[32] settled with compensation of EUR 2.428 billion. In addition, approximately EUR 21.7 million in legal, expert, and litigation expenses was incurred in relation to claims by the Swedish state-owned energy[33] company Vattenfall.

31. https://www.euroispa.org/wp-content/uploads/2026/03/2026-Digital-Omnibus-EuroISPA.pdf

32.Joint statement of the German Federal Government (5 March 2021): https://www.bundesregierung.de/breg-en/service/archive/compensation-for-nuclear-phaseout-1881422

33. German Bundestag reply to a parliamentary question from The Left Party (1 October 2020): https://www.bundestag.de/webarchiv/presse/hib/2020_10/795774-795774

Case

In the 2000s, Spain used relatively generous subsidies to attract renewable-energy investment; between 2012 and 2014, however, it substantially adjusted the original subsidy mechanism due to fiscal and electricity-tariff deficits. After this policy reversal, foreign investors initiated multiple arbitration proceedings under the Energy Charter Treaty and related investment agreements. By 2025, Spain had lost more than 30 cases in international arbitration forums such as ICSID and had been ordered to pay more than EUR 1.5 billion in compensation to investors including NextEra, Antin, and Eurus, thereby damaging[34] its sovereign credibility and attractiveness to foreign investment. At the same time, Spain continues to face unresolved claims totaling approximately[35] EUR 10.6 billion, plus related interest costs.

The two cases reveal several common features. First, a shift in policy objectives does not automatically translate into low-friction implementation, especially in infrastructure sectors characterized by high capital intensity, long investment cycles, and strong continuity dependence, where existing assets and contractual arrangements are often already embedded in financing, return, and operational systems. Second, policy costs are not limited to equipment and systems themselves, but progressively extend to compensation obligations, dispute resolution, and capital-market pricing. Third, these effects exhibit clear temporal persistence: judicial disputes and the restoration of investor confidence are typically measured in years, and the ultimate burden is borne by public finance and ordinary citizens.

3.8 Reflections from Global Parallels: The High Cost and Low Effectiveness of Supply-Chain Removal and Replacement Policies in the US and UK

Over-politicizing supply-chain issues can easily lead to a severe disconnect between policy design and practical implementation, ultimately resulting in governance dilemmas that are costly, inefficient, and difficult to execute. Outside the EU, both the United States and the United Kingdom have introduced restrictions involving supply-chain adjustments in the single telecommunications sector. Such policies are often introduced rapidly in the name of national security, yet in implementation they have commonly revealed serious underestimation of costs, engineering complexity far beyond expectations, widening funding gaps, and repeated schedule delays. In the end, they have not achieved their stated goals on time, but have instead caused major fiscal and industrial losses while also delaying domestic digital-infrastructure construction.

Case

The communications equipment removal-and-replacement program promoted by the US Federal Communications Commission (FCC) is another typical example of the politicization of supply-chain policy. In 2021, the US Congress passed the Consolidated Appropriations Act, 2021, amending the Secure and Trusted Communications Networks Act of 2019 and appropriating USD 1.9 billion to the FCC to reimburse eligible operators for the costs of removing and replacing communications equipment and services associated with Huawei and ZTE. At the initial design stage, this appropriation was regarded as the core safeguard for advancing supply-chain adjustment, but implementation soon exposed a clear mismatch between the budget and actual demand. In 2022, FCC Chair Jessica Rosenworcel stated that reimbursement applications first submitted by small and rural network operators had already reached USD 5.6 billion, far above the original appropriation of USD 1.9 billion. In May 2024, the FCC further informed Congress that total funding needs would reach approximately USD 4.98 billion in order to cover all approved applications with “reasonable and supported cost estimates.” In December of the same year, the Fiscal Year 2025 National Defense Authorization Act was signed into law, authorizing the FCC to borrow up to USD 3.08 billion from the US Treasury. At that point, the total federal funding requirement rose to USD 4.98 billion.

34. Reuters, 2025: https://www.reuters.com/sustainability/climate-energy/eu-commission-tells-spain-not-pay-up-long-running-renewable-subsidies-case-2025-03-24/

35. El País and The Economist: https://elpais.com/economia/2025-03-24/la-comision-europea-concluye-que-espana-no-tiene-que-pagar-al-fondo-antin-por-las-renovables.html

Case

The UK's experience with 5G supply-chain adjustment is a typical example of the practical constraints facing policies of forced infrastructure replacement. In 2020, the UK government announced that purchases of new Huawei 5G equipment would be prohibited from the end of that year and that related equipment must be removed from UK 5G networks by 2027. The government also made clear that this decision would delay the UK's overall 5G deployment by two to three years and increase total costs by as much as GBP 2 billion. For policymakers, this decision reflected a choice about security and supply chains; for operators, however, it meant that the existing pace of network construction was forcibly interrupted, and resources originally intended for expansion and upgrades had to be diverted to dismantling, replacing, and reconstructing existing equipment.

Disclosures from operators further confirm the heavy cost of implementation. BT publicly stated that, in order to meet the equipment-removal and market-share cap requirements, its own related spending would amount to approximately GBP 500 million, equivalent to 2.4% of its FY2022 operating revenue. Vodafone also noted that if large-scale equipment replacement had to be completed within a short cycle, the cost would run to the billions of pounds and could significantly affect customer service quality and network stability. These costs are not simply equipment procurement expenses; rather, they reflect the comprehensive price of a mismatch between policy timing and engineering realities such as live-network migration, technology cutover, and substitute supply, thereby placing simultaneous pressure on project costs, implementation schedules, and service quality.

The increase in required funding from USD 1.9 billion to USD 4.98 billion—roughly 2.6 times higher—shows that the initial policy design significantly underestimated engineering implementation costs. The case demonstrates that forced replacement in practice tends to drive up fiscal pressure, extend implementation timelines, and increase service risks at the same time. More importantly, the USD 4.98 billion figure mainly covers directly reimbursable costs; it does not include indirect losses, opportunity costs, or revenue losses from service interruptions that operators may bear, nor does it include potential losses to broader social and economic development. The FCC has repeatedly warned that if funding remains insufficient over the long term, some operators may be forced to shut down networks, leaving certain areas without their only communications provider. In infrastructure sectors, forced replacement does not become low-friction implementation simply because compensation mechanisms exist, and recovery is difficult to achieve quickly in the short term; the effects typically last five to ten years.

Taken together, the experiences of the FCC's equipment-replacement program in the United States and the UK's 5G supply-chain adjustment confirm that supply-chain restructuring driven by political motives is often incapable of producing sustainable and implementable policy outcomes. Both countries experienced severe initial budget shortfalls, substantial overruns in actual input, repeated delays in dismantling and replacement, and overall goals that proved difficult to complete on time. The result was that enterprises and taxpayers bore massive economic costs, while network construction lagged and digital competitiveness weakened. If even the losses associated with replacing specific suppliers in a single sector in two of the world's major economies were so large, then the CSA2 proposal—driven by geopolitical intent and imposing mandatory time-limited adjustments on an open-ended range of so-called "high-risk suppliers" across 18 sectors in 27 EU member states—would be even less capable of achieving security and compliance objectives, and would instead suffer from low efficiency, severe resource waste, and an inability to attain long-term and stable industrial and security outcomes.

Chapter Summary: The Tension Between Geopolitical Impulses and Economic Rationality

In pursuing “geopolitical de-risking” and “supply-chain resilience,” the EU is falling into a governance paradox: security review, which should belong to the technical domain, is being transformed into access discrimination based on political labels such as identity and origin.

The EU should acknowledge that “security” and “economic efficiency” are not a zero-sum game. In practice, coercive supply-chain disengagement centered on the notion of the “high-risk supplier” is materially reshaping the underlying fairness of the European market.

This policy orientation will not build a genuine security barrier. Instead, by using non-technical criteria it is artificially creating major trade barriers and has already given rise to allegations of systemic illegality. The result is that the EU would trade away economic efficiency and erode public interests in exchange for a form of “de-risking” that simultaneously means “de-opportunity.” Unless this closed logic is broken, the EU will inevitably fall into a structural trap in which excessive restriction leads to technological lag.

True security comes from sustained technological leadership and the diversified resilience of ecosystems. If the pursuit of a false sense of security based on excluding particular countries or enterprises causes European firms to lose their capacity for innovation because costs become too high, then a less competitive Europe will become more vulnerable to external technological sanctions and market shocks, and will also lose its leading position in the age of digital civilization.

04

Overall Economic Impact Analysis for the EU

The impact of the CSA2 proposal on the overall EU economy goes far beyond visible engineering costs such as equipment reconstruction, dismantling, and reinstallation. It would generate full-chain, systemic economic burdens across corporate operations, member-state finances, and public wellbeing.

At the corporate level, the proposal's compulsory divestment and replacement requirements would force resources away from frontier R&D and production expansion toward redundant deployment and network reconstruction. At the member-state level, governments would have to bear additional high costs including compensation for breaches of bilateral agreements, legal dispute expenses, and unemployment assistance. For EU citizens, the consequences would include declining quality and coverage of public services, longer waiting times for medical treatment, and rising energy and telecommunications bills.

More seriously, the CSA2 proposal would turn cybersecurity certification from a voluntary mechanism into a mandatory market-access threshold. This form of "front-loaded regulation" would not only lengthen certification cycles, but also impose a systemic drag on the EU's long-term economic efficiency through a massive compliance premium.

The EU is therefore urged to fully recognize the multi-dimensional costs, long transmission chains, very broad scope of impact, and hundreds of billions of euros in economic losses that the relevant provisions of the proposal could trigger, and to approach them with a high degree of caution and prudent assessment.

4.1 Key Points of Focus

The EU's current economic impact assessment of CSA2 suffers from clear limitations: it does not cover all member states, all affected sectors, or full-chain systemic losses. It also overlooks the multi-year chain reactions that would follow once the proposal is implemented.

To assess comprehensively and objectively the real impact of the proposal's mandatory replacement provisions, this assessment considers multiple dimensions, selects core indicators, and ensures rigor through cross-validation using authoritative multi-source data, first-hand industry research, and expert views. In addition, the assessment divides indicators into four layers—direct losses, indirect losses, legal breach-related losses, and social losses—and evaluates them one by one. Direct losses reflect the cost of asset exit and replacement itself; indirect losses reflect the subsequent operational, investment, and systemic effects. Social and legal losses reflect the spillover impact of implementation on the public, governments, and other stakeholders.

According to this assessment, if CSA2 were mandatorily enforced, the EU and its member states would bear cumulative losses of EUR 367.8 billion between 2026 and 2030. Of this, visible direct losses alone—including hardware replacement and dismantling and installation services—would reach EUR 146.2 billion, or roughly 40% of the total.

Beyond the quantifiable economic losses captured in this assessment, CSA2 would also, over the long term, raise service prices in key EU sectors, increase burdens on households and businesses, weaken global investors' confidence in the EU market, and slow its digital and green transition. At the same time, this unilateral regulatory rule would intensify the fragmentation of global digital and industrial standards and split global industrial and supply chains, further damaging the EU's reputation for international cooperation and its long-term development competitiveness.

4.2 Regulatory Spillovers Across the Value Chain Could Create a Systemic Deficit, with Total EU Losses Expected to Around EUR 370 Billion

The EU's existing CSA2 economic impact assessment framework is significantly limited. It focuses only on visible procurement substitution costs, while seriously overlooking chain reactions across 18 critical sectors and 27 member states over the full industrial chain and full lifecycle. Through multi-dimensional modeling, this assessment reconstructs more comprehensively the systemic deficit that would arise if the proposal were implemented.

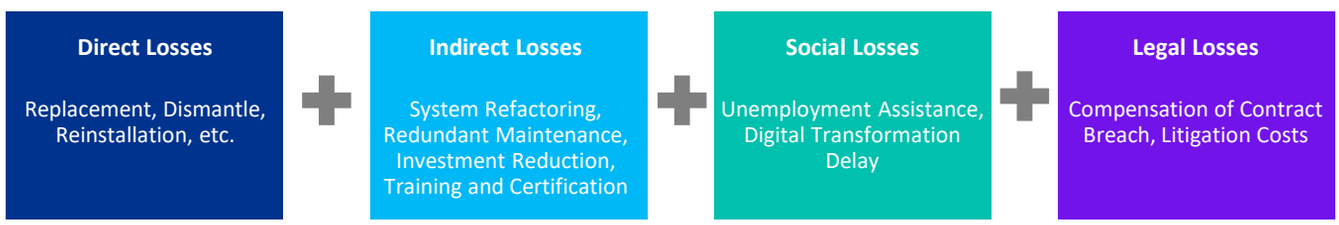
First, from the perspective of affected entities and duration, this assessment incorporates the likely losses that would be borne by upstream and downstream supply-chain enterprises, member-state governments, and the EU public, as well as the minimum duration for which the chain economic effects triggered by the proposal would persist, so as to ensure analytical rigor.

Second, in selecting loss indicators, this assessment comprehensively considers multiple dimensions, including equipment repurchase, dismantling and installation services, redundant maintenance, network reconstruction, residual value and depreciation, liquidated damages, capital crowding-out, and broader social transmission effects. From these, it selects a set of core indicators that are significant in impact, large in economic magnitude, and quantifiable in loss terms, thereby ensuring comprehensive coverage.

Third, regarding the logic of loss estimation and data sources, the assessment draws on authoritative public secondary data including Eurostat macroeconomic and industry operating data, European Commission industry reports, UN global trade data, and China Ministry of Commerce data on China–EU trade; it also uses first-hand measured data from executives, technical experts, and compliance specialists from leading companies in the 18 affected sectors. In addition, it incorporates expert input from industry associations, leading global think tanks, and partners at top-tier law firms. Through multi-source comparison and cross-validation, it verifies the estimation logic and the coverage, granularity, and credibility of the data, thereby ensuring objectivity and authenticity.

Finally, the assessment divides the indicators into four major layers: direct losses, indirect losses, legal breach-related losses, and social losses. Direct losses mainly include the timing mismatch impairment arising from hardware replacement, dismantling and reinstallation, and premature retirement; indirect losses include spillover costs such as system reconstruction, parallel maintenance, capital transfer losses, and training and certification; legal losses include state compensation and litigation-related costs; and social losses mainly include pass-through effects on end-user prices and unemployment assistance. In this way, each layer of indicators is systematically decomposed and estimated one by one.

Figure 11: Four-Tier Loss Structure Used in This Assessment



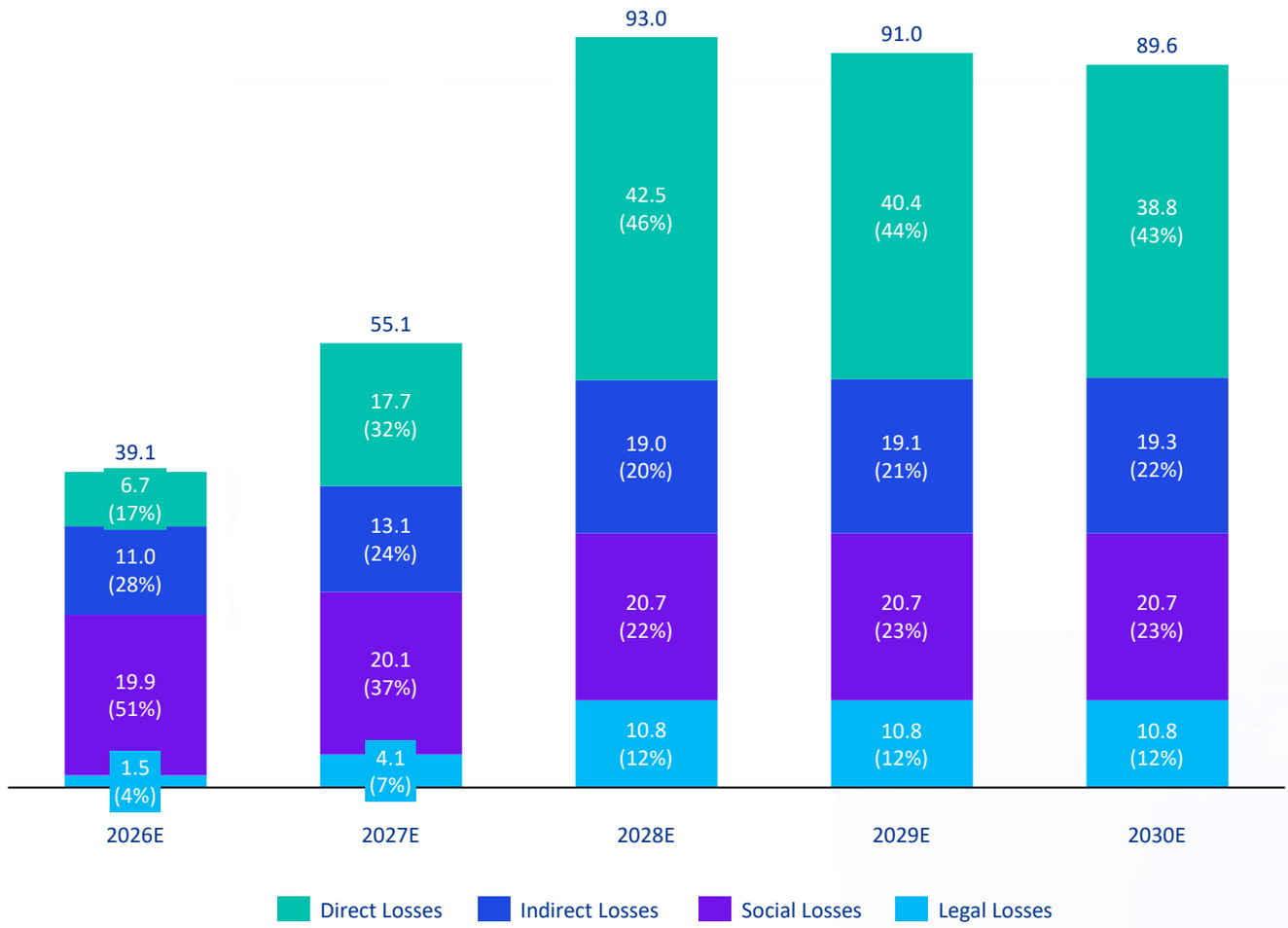
Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

This assessment considers a 36-month wireless-equipment replacement cycle to be practically infeasible. Assuming that the EU nonetheless completes mandatory replacement across 18 major sectors within a minimum five-year period, the EU and its member states would incur nearly EUR 367.8 billion in losses from supplier replacement alone during 2026–2030.

Among these, direct losses from equipment replacement and dismantling and installation services alone would amount to approximately EUR 146.2 billion, constituting the primary compliance pressure visible on corporate financial statements. In addition, indirect losses, social losses, and legal breach-related costs would reach EUR 81.5 billion, EUR 102.1 billion, and EUR 38.1 billion, respectively. Through system adaptation and the reordering of investment, these costs would materially crowd out R&D budgets originally intended for 6G, AI, and green infrastructure, turning the regulatory premium into a long-term opportunity cost for Europe.

From the perspective of annual trends, total losses would rise in a stepwise pattern. As the policy moves from legislative discussion into large-scale implementation, annual EU losses are projected to increase from approximately EUR 39.1 billion in 2026 to about EUR 89.6 billion in 2030. Direct losses alone would rise from EUR 6.7 billion in 2026 to EUR 38.8 billion in 2030. This reflects the assumption that in 2026–2027 the policy would still be in the proposal and refinement stage, with most EU operators and project owners remaining in a wait-and-see mode and only a limited number of enterprises initiating supplier replacement. As legislation is completed and implementation expands, the related economic losses would become more pronounced during 2028–2030.

Figure 12: Total Losses by Category from EU Mandatory Replacement, 2026–2030 (EUR billion, %)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

4.3 EU Economic Losses Are Multi-Dimensional, Extending from Visible Asset Expenditure to Systemic Risk

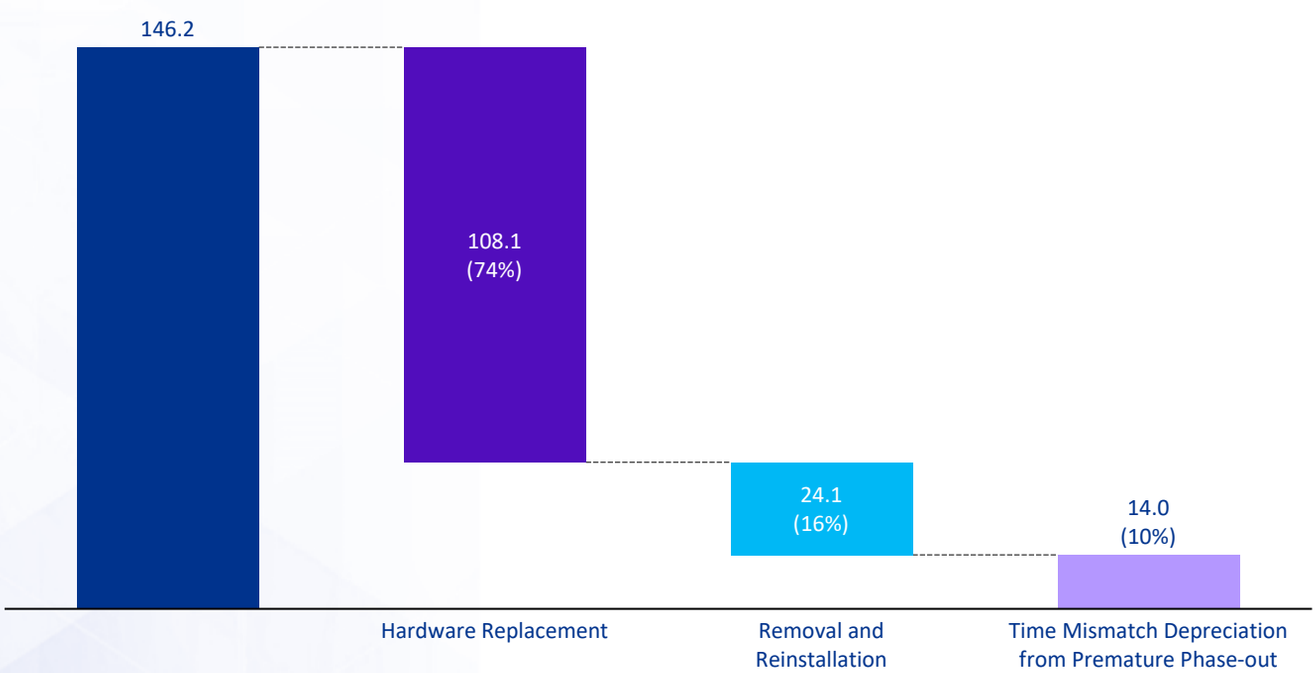
4.3.1 Direct Losses Exceed EUR 100 Billion: Forced Asset Replacement Severely Damages Corporate Financial Resilience

Direct losses are the visible expenditures directly borne by enterprises under mandatory replacement arrangements. Specifically, they consist of three parts: first, hardware replacement costs; second, dismantling and reinstallation costs; and third, timing-mismatch impairment caused by the premature exit of equipment before completion of its natural lifecycle.

Among these, hardware replacement costs constitute the main component of direct losses and generally depend on the existing scale of installed equipment, the procurement price of replacement equipment, and the pace of replacement. Dismantling and reinstallation costs are the engineering-service expenditures associated with implementation, such as on-site removal, transport and disposal, and reinstallation. Timing-mismatch impairment refers to the value loss arising when assets that could otherwise have been depreciated and replaced gradually over their normal service life are instead forced to exit prematurely within a much shorter timeframe, leaving residual value unapportioned and use abruptly terminated.

Total direct losses in the EU during 2026–2030 are estimated at approximately EUR 146.2 billion. Of this, hardware replacement costs amount to roughly EUR 108.1 billion, accounting for 74% of direct losses and constituting their principal component; dismantling and reinstallation costs amount to about EUR 24.1 billion, or 16%; and timing-mismatch impairment from premature retirement amounts to roughly EUR 14.0 billion, or 10%. This structure shows that direct losses manifest first as capital expenditure on new equipment procurement, second as engineering-service costs incurred during implementation, and third as value loss arising from the forced early retirement of assets that had not yet completed normal depreciation.

Figure 13: Direct Losses from EU Mandatory Replacement, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Hardware replacement costs dominate because they directly correspond to the asset renewal process of “old equipment exit—new equipment purchase.” In critical infrastructure sectors, once existing equipment is required to exit within a specified period, project owners must first bear the procurement costs of substitute equipment. These costs are typically driven by three factors: the scale of the installed base, the procurement price of substitute equipment, and the pace of replacement. Given the large installed base of critical equipment and high unit values, hardware replacement naturally becomes the largest component of direct losses.

Dismantling and reinstallation costs correspond to engineering-service expenditures incurred during implementation, including on-site dismantling, transport and disposal, reinstallation, access integration, and commissioning. Compared with hardware procurement, these costs do not directly increase asset scale, but they are nonetheless unavoidable in infrastructure sectors. In particular, where continuity requirements are high, equipment is geographically dispersed, and construction organization is complex, dismantling and reinstallation often require additional engineering windows, labor input, and on-site coordination, thereby forming the second-largest direct cost item. Structurally, a 16% share shows that direct losses are not merely about equipment prices, but also include substantial implementation costs.

Although timing-mismatch impairment accounts for only 10% of direct losses, the issue it reflects has deeper institutional significance. This component is not new procurement or engineering expenditure; rather, it is the residual value loss created when assets that could otherwise have been depreciated and replaced gradually over their normal service life are instead required to exit prematurely within a shorter period. In other words, this loss arises because the “policy clock moves faster than the asset-life clock.” For equipment with long service lives and stable depreciation schedules, premature exit means that asset value not yet normally amortized is forcibly cut short, essentially reflecting an administrative disruption of the original capital-recovery rhythm.

The core pain point of direct losses lies in two aspects. First, a large volume of assets that have not yet completed their natural depreciation lifecycle would be forced out early, and the resulting timing-mismatch impairment amounts in substance to an administrative deprivation of asset value. Second, this would directly affect firms’ market choices. At the same time, such visible expenditures would directly worsen corporate balance sheets and substantially weaken the cash-flow stability of capital-intensive industries.

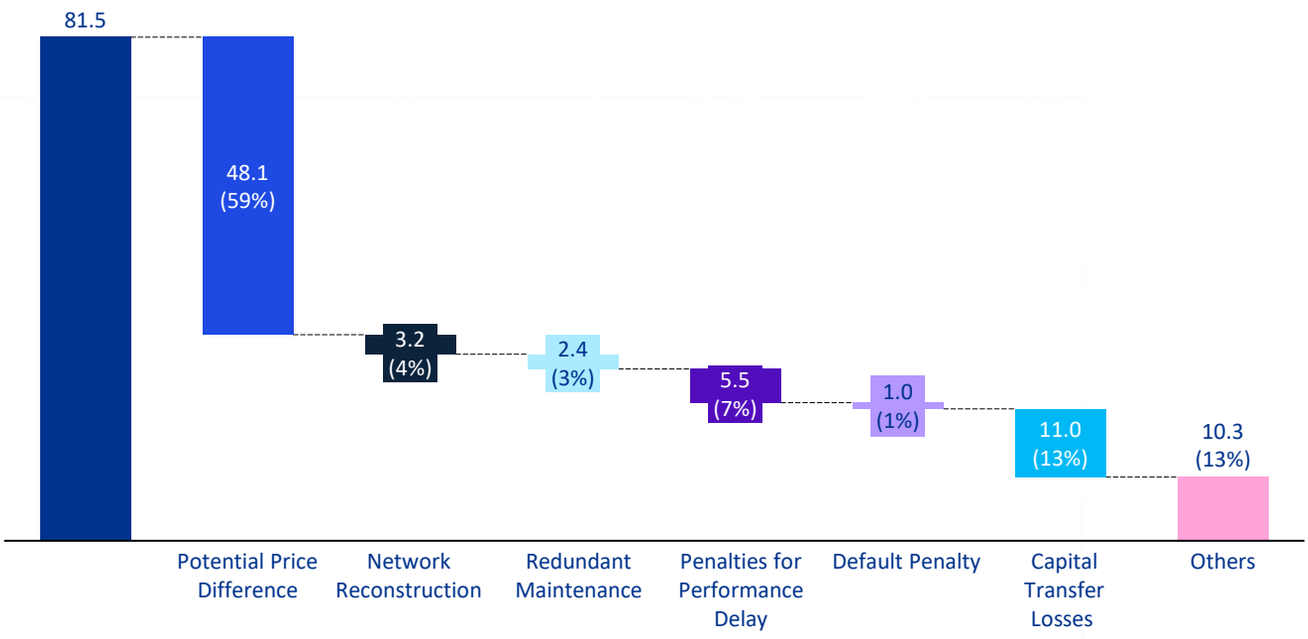
4.3.2 Indirect Losses Reach EUR 80 Billion: System Reconstruction and Innovation Crowding-Out Add to Industrial Burdens

Indirect losses are likewise borne by enterprises and refer to the additional economic burden imposed on normal business operations beyond visible expenditures. Unlike direct losses, they do not take the form of hardware procurement, dismantling and reinstallation, or premature-retirement impairment; instead, they reflect the disruptions that replacement arrangements cause to project timing, capital allocation, operational efficiency, and service continuity. Under this study's approach, indirect losses mainly include potential price differentials, network reconstruction, redundant maintenance, performance-delay penalties, SLA liquidated damages, capital transfer losses, and other related expenditures.

System reconstruction costs mainly consist of integration, development, and commissioning expenses. In enterprise operations, equipment rarely functions in isolation; rather, it is embedded in existing dispatch, monitoring, control, network-management, billing, and maintenance systems. Even after new equipment has been procured and installed, restoring operations still requires corresponding adjustments to interfaces, protocols, software environments, and related systems. Parallel operation refers to the redundant resource inputs and maintenance expenditures incurred during the forced transition period when enterprises, unable to achieve seamless and stable integration between old and new systems, must keep both in operation simultaneously to maintain service continuity. Capital transfer losses primarily reflect the gap between the return that forced replacement generates and the return that the same funds could have generated had they been used for normal productive activities such as innovation, R&D, or capacity expansion. Other related costs borne by enterprises—such as future procurement price differentials, SLA liquidated damages, performance-delay penalties, additional certification fees, and training expenses arising from replacement—also fall within the scope of indirect losses.

Overall, cumulative indirect losses from EU mandatory replacement during 2026–2030 are estimated at approximately EUR 81.5 billion. Of this, potential price differentials amount to about EUR 48.1 billion, representing 59% of indirect losses and constituting their main component; capital transfer losses amount to about EUR 11.0 billion, or 13%; other costs amount to about EUR 10.3 billion, or 13%; performance-delay penalties amount to about EUR 5.5 billion, or 7%; and the remaining portion includes network reconstruction at EUR 3.2 billion (4%), redundant maintenance at EUR 2.4 billion (3%), and liquidated damages at EUR 1.0 billion (1%). Indirect losses thus reflect broad operating costs arising from substitute procurement, the reordering of capital, and disrupted project timing.

Figure 14: Indirect Losses from EU Mandatory Replacement, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Among the various components, potential price differentials account for the largest share and are the core source of indirect losses. Their significance goes beyond the current procurement price itself; they refer to the ongoing cost differential that enterprises may have to bear in future equipment procurement, upgrades, and related investments after being forced to alter their original supplier and equipment pathways. In other words, this loss reflects the gap between "what would originally have been the more efficient market-based choice" and "the cost structure that enterprises are forced to accept under an alternative path." A 59% share indicates that the most important indirect consequence of mandatory replacement is not one-off system debugging, but the persistent price disadvantage firms would face in subsequent procurement and configuration.

Capital transfer losses are the second category of indirect cost requiring particular attention. Their core lies in the fact that enterprises are forced to divert funds that could otherwise have been used for R&D innovation, capacity expansion, digital upgrading, or next-generation infrastructure deployment into stock replacement and related expenditures. What results is not a conventional accounting loss, but the gap between the return on normal productive investment and the return on forced replacement. For the EU, this process—where capital shifts from incremental investment toward the impairment of existing stock—means that corporate investment priorities are being administratively reordered, and that funds which could have generated medium- to long-term competitiveness are being prematurely consumed.

Other costs and performance-delay penalties together make up the third layer of indirect losses. Other costs mainly include additional certification fees, training costs, adaptation expenditures, and other ancillary costs that are difficult to isolate individually but are incurred in reality. Performance-delay penalties reflect revenue losses or contractual penalties caused during the replacement process by declining performance, extended commissioning cycles, or slower system recovery. Together, these two categories account for more than 20% of indirect losses, indicating that beyond the equipment itself, replacement arrangements continue to amplify operational pressure on enterprises through project execution quality, operating efficiency, and ancillary expenditures.

By comparison, network reconstruction, redundant maintenance, and liquidated damages account for a relatively small share of the total, but they remain significant in specific sectors and scenarios. Network reconstruction mainly corresponds to integration development, interface adjustments, protocol adaptation, and commissioning expenses required to restore operations after new equipment is connected to existing systems. Redundant maintenance arises during transition periods when both the old and the new systems must be kept in operation in parallel to ensure service continuity, thereby generating additional resource input and maintenance expenditures. Liquidated damages mainly correspond to liability costs arising when replacement prevents performance under existing contracts, service-level agreements, or delivery schedules. Although these three items together account for less than one-tenth of the total, their presence shows that the impact of mandatory replacement on enterprises extends beyond price levels into the spheres of system operations and contractual execution.

Beyond the quantified indicators included in this assessment, the EU should also pay attention to other management difficulties not incorporated into the model but still capable of creating significant adverse effects on enterprises and even entire industries. From the perspective of corporate organization and governance, forced replacement would also indirectly increase management complexity and reduce operational efficiency. Corporate legal, procurement, engineering, finance, operations, and compliance teams would often need to coordinate more frequently around replacement arrangements. This would require not only internal changes to decision-making processes, but also adjustments in external supply-chain systems. Such organizational costs are usually difficult to list separately, but their effects on management efficiency and project progress are very real. In settings involving multiple parallel projects, cross-regional operations, and cross-member-state deployment, the cost impact associated with increased organizational complexity should not be underestimated.

In addition, once project delays and shutdown-window arrangements arise, the scale of indirect losses would be further amplified. Replacement in infrastructure sectors typically must be carried out within tightly controlled time windows, balancing service continuity with construction organization and operational stability. If equipment replacement overlaps with existing expansion plans, upgrade schedules, or commissioning plans, original project timelines are more likely to be delayed. The resulting losses are not limited to the delay of a single project, but also manifest in postponed revenue recognition, slower capital turnover, and involuntary rescheduling of subsequent projects.

Even more important, the forced reordering of capital originally intended for capacity expansion, technological upgrading, next-generation infrastructure deployment, and innovation R&D has implications for the EU that extend well beyond the cost of a single year, and may instead be reflected in future years' potential growth and competitiveness. If investment originally earmarked for 6G, artificial intelligence, smart grids, and green energy is delayed or compressed because funds must be diverted to replacing existing stock, the proposal ceases to be merely a compliance-cost issue and becomes an opportunity-cost issue as well. This shift from incremental investment to the impairment of existing stock would turn regulatory burdens into a long-term erosion of the EU's strategic competitiveness.

4.3.3 Legal Liabilities Increase Cross-Level Litigation Risks, While Massive Compensation for Breach Aggravates Public Fiscal Burdens

Fully separate from direct and indirect losses, losses arising from legal liability would primarily be borne by member states. Once related legal disputes enter judicial proceedings before EU courts and international arbitration, the EU and its member states would also face high adjudication costs, legal representation fees, expert-witness fees, and other dispute-resolution expenses. Ongoing multi-level litigation and arbitration would not only significantly increase public-fiscal expenditure, but would also—through lengthy procedures and high costs of legal defense—further aggravate the economic burden and uncertainty surrounding regulatory implementation.

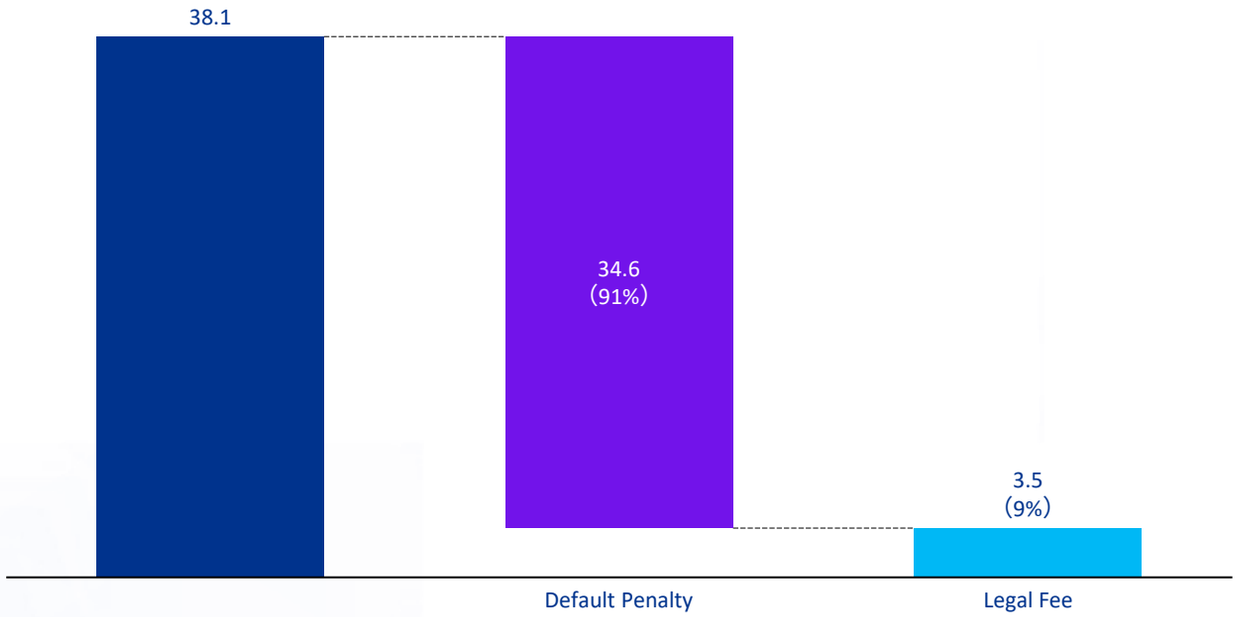
Losses arising from legal liability include, but are not limited to, claim-related losses and litigation-cost losses. With respect to claims, the 2025 World Investment Report published by UNCTAD shows that, in investor–state dispute settlement (ISDS) cases based on bilateral investment treaties (BITs) between 2015 and 2024, the average amount claimed by investors was USD 981.8 million, with a median of USD 162.4 million, while the average final compensation awarded by arbitral tribunals was USD 233.9 million, with a median of USD 40 million. These data show the continued rise in claim amounts in international investment arbitration. Litigation-cost losses mainly include ongoing[36] adjudication and legal fees associated with multi-level judicial and arbitral confrontation, which would further increase the fiscal burden on member states and heighten both the economic cost and legal uncertainty of regulatory enforcement.

36. UNCTAD, World Investment Report 2025: Investment Policy Trends, Chapter II, p. 122, March 2025, https://unctad.org/system/files/official-document/wir2025_ch02_en.pdf.

Mandatory exclusion policies are highly likely to trigger investor arbitration under BITs, administrative litigation, and civil lawsuits for contractual breach. The EUR 38.1 billion in losses attributable to legal liability are projected to rise from EUR 1.5 billion in 2026 to EUR 10.8 billion in 2030 as the proposal is implemented. Protracted multi-level legal contestation would not only increase legal-representation and expert-witness costs, but would also significantly reduce the predictability of the regulatory environment due to lengthy procedures, thereby intensifying market anxiety over compliance. At the same time, large-scale claims would place member states under enormous fiscal compensation pressure.

The EU's high legal losses from mandatory replacement are the unavoidable price of unlawful measures. Compensation for breach accounts for approximately 91% of legal losses and constitutes the overwhelming main component, while legal fees account for 9%. This structure shows that legal losses do not arise primarily from routine procedural communication or scattered compliance costs, but are instead highly concentrated in compensation liabilities resulting from interrupted contracts and altered service obligations, together with the legal spending required to respond to those disputes.

Figure 15: Legal Losses from EU Mandatory Replacement, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Of the two components, compensation for breach is the core source of legal losses. It mainly corresponds to compensation liabilities that enterprises, operators, project sponsors, and public-sector bodies may bear once policy-driven equipment replacement, service termination, project rescheduling, and the inability to continue fulfilling existing commitments occur. Such liabilities may arise from procurement contracts and equipment service agreements, but also from service-level agreements, project delivery commitments, and long-term operations and maintenance arrangements. Once an existing supply relationship is interrupted by policy requirements, the basis for performance under the original contract is affected, and the resulting compensation liabilities can quickly become the largest item within legal losses.

Legal fees account for 9% of the total. Although significantly lower than compensation for breach, their importance is far from marginal. This portion mainly reflects legal-service expenditures incurred by enterprises, operators, and other relevant parties in responding to contract disputes, claim negotiations, administrative procedures, litigation preparation, and arbitration matters. It covers not only representation fees after formal proceedings begin before courts or arbitral tribunals, but also professional service costs incurred at earlier stages, including legal review, liability identification, contract renegotiation, negotiation support, and risk response. In other words, although legal fees are smaller in scale, they are an important accompanying cost of the continuing accumulation of compensation liabilities and the expansion of dispute procedures.

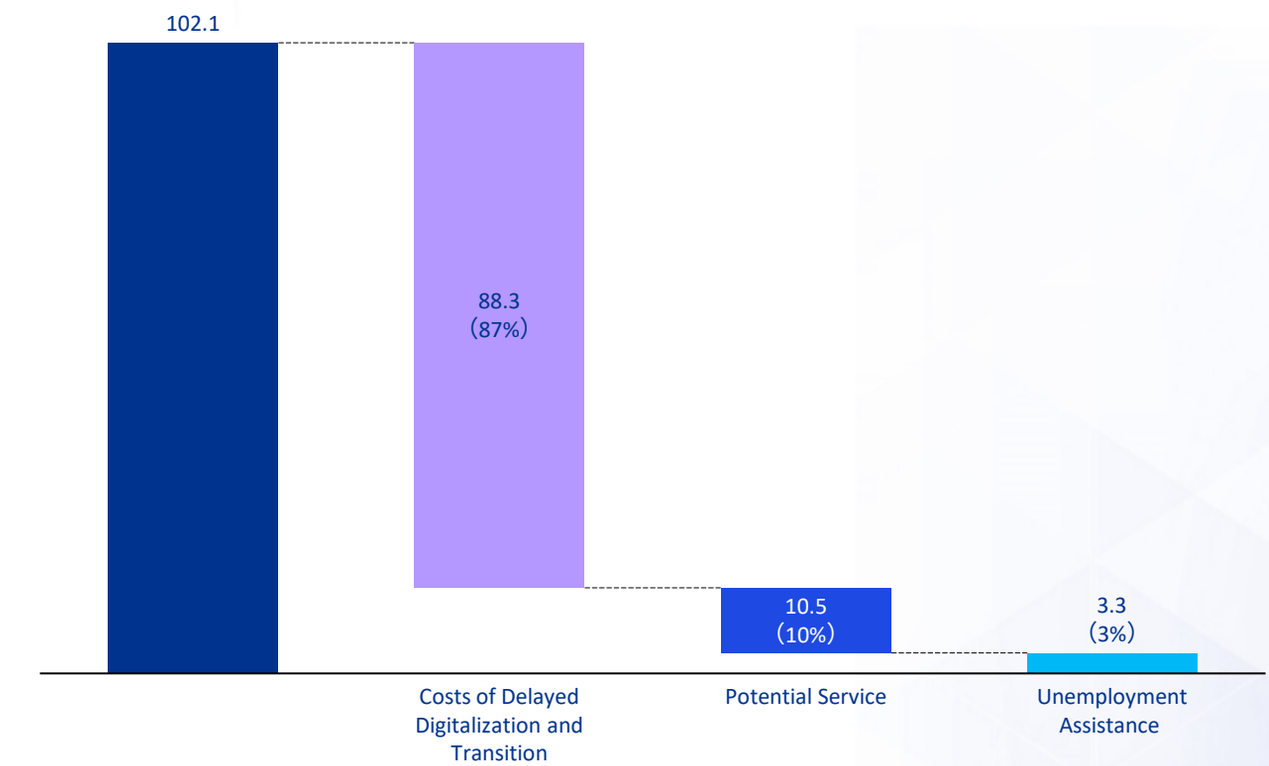
4.3.4 Broad Social Impact: Price Pass-Through and Other Effects Erode Public Welfare and Intensify Cross-Regional Development Imbalances

If the proposal enters the implementation stage, it will generate significant social impacts in addition to direct losses, indirect losses, and legal-liability losses. Unlike the first three categories of loss, social losses would be borne more by member states and the wider EU public, and would mainly include unemployment assistance for EU workers resulting from the forced market exit of relevant enterprises, as well as the costs of delayed digital transformation. These are not direct cash payments; rather, they reflect the loss of end-user welfare whereby consumers could otherwise have enjoyed higher-quality services, but service-coverage density and service timeliness decline because resources are diverted. Unlike the principal amounts reflected in enterprises' direct losses, this represents the incremental economic value that the industry could otherwise have generated. Such effects typically do not appear in full at the beginning of policy implementation, but gradually spread across a broader social spectrum as implementation progresses, prices are adjusted, and budgets are reordered.

In assessing social impacts, this study adopts a conservative approach and includes only those relatively quantifiable social-loss items not already captured in the first three categories of loss, such as unemployment assistance and delayed digital transformation resulting from the forced exclusion of suppliers. Taking only the energy and telecommunications sectors as examples, the costs of equipment replacement and network reconstruction would gradually be transmitted through projects, enterprises, and industries to governments, public services, and households. These massive reconstruction costs would be passed through via electricity-pricing mechanisms and telecommunications tariffs, directly increasing the daily expenditure burden of residents and enterprises.

Cumulative social losses from EU mandatory replacement during 2026–2030 are estimated at approximately EUR 102.1 billion. Of this total, the cost of delayed digitalization and transition amounts to about EUR 88.3 billion, accounting for 87% and constituting the main component of social losses; potential service losses amount to about EUR 10.5 billion, accounting for 10%; and unemployment assistance for labor amounts to about EUR 3.3 billion, accounting for 3%. This structure shows that social losses do not primarily arise from short-term subsidies or price changes, but first and foremost from the forced slowing of digital, networked, and green transitions, followed by more concrete costs in service capacity and public support.

Figure 16: Social Losses from EU Mandatory Replacement, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Among the three components, the cost of delayed digitalization and transition accounts for the largest share and is the core source of social losses. What it reflects is not simple project delay, but the comprehensive social cost arising because the EU's and member states' original digital and green transition processes are forced backward due to supplier replacement, equipment reconstruction, repeated certification, and the crowding-out of implementation resources. For the EU, this type of cost has stronger spillover characteristics because it means not just that individual projects come online later, but that the overall progress of digital infrastructure, smart grids, energy transition, and public-platform upgrading is affected. A 86% share indicates that, at the social level, the greatest cost is not the immediately visible change in bills, but the overall slowing of transition processes that could otherwise have generated broader public benefits.

Potential service losses constitute the second component of social losses. They mainly take the form of reduced service continuity, slower coverage rollout, delayed launch of public and commercial services, and the gradual pass-through of related costs to end users via electricity prices, telecom tariffs, and enterprise service charges. Energy and telecommunications are the most typical channels of transmission: the costs arising from equipment replacement and network reconstruction are often gradually passed through to households and enterprises through electricity-pricing mechanisms, network charges, and telecom tariffs. At the same time, the replacement of digital systems in finance, industry, public services, and research platforms may also create social losses that are difficult to perceive immediately yet persist over time, through reduced service accessibility, delayed delivery, and rising usage costs. A 10% share indicates that, although the service dimension is not the dominant component, it is the layer most directly felt by the public.

Unemployment assistance accounts for 3% of the total, and although relatively small in scale, it carries strong policy significance. This component mainly corresponds to the employment-placement and unemployment-support pressures that member-state governments may need to bear after the exit of Chinese suppliers, project adjustments, or restructuring of related industrial chains. In some regions, the effect may not take the form of large-scale unemployment, but instead show up as interruption of specific projects, downsizing of localized service teams, loss of technical posts, and rising related public-support costs. Although smaller in monetary terms than the costs of delayed digitalization and transition and potential service losses, its impact on local labor markets and policy stability should not be underestimated.

In addition, the EU should further consider broader social effects not covered in this assessment. From the perspective of public-resource allocation, social impact is also reflected in changes to budget arrangements and spending priorities. In responding to compliance-driven replacement, member-state governments may be forced to make defensive adjustments to existing budgets, causing delays in other public-service projects or deterioration in service quality. Peripheral and rural regions with tighter budget constraints may also suffer passive delay in service coverage and the diffusion of digital dividends because of the long engineering cycle and limited replacement options, thereby aggravating internal EU development imbalances.

Chapter Summary: Regulatory Premiums Severely Damage Long-Term Economic Efficiency

The mandatory supplier-replacement provisions of the EU CSA2 proposal are, in essence, weakening global investors' confidence in the EU market and exposing Europe to long-term threats of standards fragmentation and industrial-chain dislocation in global digital governance.

At the market-price level, the enormous costs created by implementation—equipment replacement, compliance certification, and redundant maintenance—would gradually be transmitted to downstream end markets, directly driving up prices for services in key sectors such as telecommunications and energy, and ultimately increasing household expenditure and operating costs for businesses, thereby causing structural changes in the EU-wide price level.

At the level of international investment, the proposal's high compliance costs, uncertain regulatory risks, and market-access restrictions would substantially weaken corporate willingness to invest, disrupt existing investment layouts and pacing, and cause imbalances in the investment structure of the EU's digital infrastructure and high-tech sectors, resulting in long-term erosion of investment confidence.

At the level of digital and green transition, large sums of capital would be crowded out toward compliance rectification and equipment reconstruction rather than incremental innovation, directly delaying the upgrading of EU digital infrastructure, digital-technology innovation, and green-energy transition, causing the EU to deviate from the pace required by its digitalization strategy and carbon-neutrality goals, and slowing coordinated regional industrial digitalization and greening by 3 to 5 years.

In the area of public budgets and public services, the proposal would, on the one hand, increase public-fiscal expenditure by the EU and its member states on regulation, subsidies, and related items, thereby intensifying budgetary pressure; on the other hand, lagging infrastructure iteration and rising service costs would reduce the quality and efficiency of essential public services such as public communications and energy supply, undermining service inclusiveness.

In labor markets, cost pressure on affected sectors would lead to business contraction and reduced R&D investment, causing fluctuations in related jobs. At the same time, the slowing of transition processes would also suppress job creation in emerging digital sectors, thereby producing a dual negative impact on the overall scale and structure of employment in the EU.

At the level of international standards and industrial cooperation, the EU's use of non-technical country-of-origin-based assessments to govern supply chains, and its exclusion of particular suppliers from standards cooperation, would intensify the fragmentation of global cybersecurity and digital-technology standards, split global industrial and supply-chain cooperation systems, obstruct cross-border cooperation between the EU and third countries in the digital economy and energy industries, and further increase the risk of fragmentation in global digital governance and industrial coordination.

05

Breakdown of Economic Losses Across 18 Sectors

The 18 critical sectors covered by the proposal differ in their degree of technological dependence, supply-chain structure, and level of digitalization, and would therefore face differentiated compliance costs and operational disruption. These effects would then be transmitted into investment, employment, and even long-term competitiveness, generating systemic economic impacts.

5.1 Key Points of Focus

If implemented, the CSA2 proposal would directly impose a systemic economic shock on the short-term operating costs, medium-term investment returns, and long-term market structure and international competitiveness of the 18 affected sectors in the EU. Economic losses vary significantly across sectors because of their differing industry characteristics.

The logistics and manufacturing segment would be the most severely affected, accounting for 31% of total losses. This segment encompasses several large-scale production- and dispatch-intensive subsectors, including automobile manufacturing, chemical production and distribution, transport, and food production, processing, and distribution. It is the segment most deeply coupled with physical production and supply-chain delivery, making it more susceptible to costs arising from line stoppages, commissioning, and delivery delays during the replacement process.

This is followed by the energy and telecommunications sectors, which together account for 37% of total losses. The energy segment, due to its broad scope of retrofitting and high investment intensity, is projected to incur total losses of EUR 79.9 billion; the telecommunications segment, owing to migration complexity and high continuity requirements, is projected to incur losses of about EUR 57.4 billion. Beyond these sectors, the negative effects of regulation would also spread to multiple fields through system replacement and interface adjustment. The financial infrastructure segment would face severe production-continuity challenges and high-availability validation costs, with estimated total losses of EUR 49.9 billion. In addition, health and research segment and the public services segment would bear compliance costs of EUR 33.8 billion and EUR 32.2 billion, respectively.

Once the proposal enters the implementation stage, compliance pressure would no longer be limited to equipment procurement expenditure, but would penetrate deeply into production rhythms, service continuity, and long-term investment scheduling across sectors, thereby exerting systemic pressure on the overall operating efficiency of EU industry.

5.2 Energy Segment: Asset Replacement and Grid-Connection Complexity Drive Up Economic Losses, While Forced Exclusion Delays the EU's Green Transition

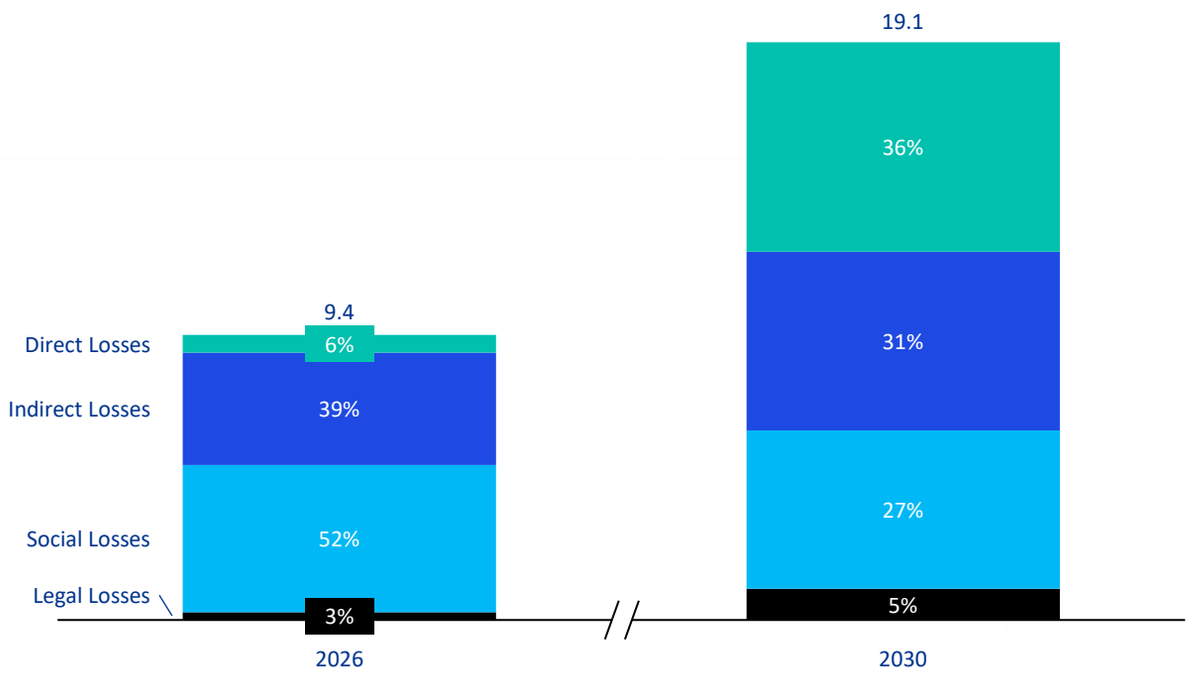
CSA2's controls over the energy sector cover the full chain of equipment, software, hardware, and services across generation, grids, distribution, and end-use systems, including solar PV, wind power, energy storage, transmission and distribution, smart grids, distribution automation, and end-point metering and dispatch systems. These systems are tightly linked to critical ICT equipment and control systems, and adjustments to one set of equipment can affect communication interfaces, dispatch logic, operational arrangements, and project schedules across the whole system.

This assessment considers only the replacement of core hardware in the three principal green-electricity areas prioritized by the EU's green transition—solar PV, wind power, and energy storage. Taking into account practical replacement difficulty and feasibility, it excludes items such as replacement of existing residential-storage installations in the EU from the loss calculation. Assuming that forced removal is completed within five years, total losses in the energy sector would reach as high as EUR 79.9 billion, making it one of the most severely affected sectors in this assessment. Annual losses in the sector are projected to rise from EUR 9.4 billion in 2026 to EUR 19.1 billion in 2030.

This category of energy equipment is deeply coupled with grid-dispatch logic. Forced replacement would not only generate enormous hardware expenditure, but would also involve highly complex supporting work such as interface re-adaptation, grid-connection safety verification, and cross-level joint commissioning. The impact would extend beyond the equipment itself to the overall system connection process, operational validation, and project scheduling.

If one further includes more granular dimensions such as smart grids and demand-side systems, the energy sector alone would generate economic losses of an even higher order of magnitude. These massive compliance expenditures are producing a clear crowding-out effect, directly driving up levelized cost of electricity. They could easily worsen the financial models of newly installed projects and force enterprises to divert R&D budgets toward compliance impairment, thereby seriously delaying the EU's established timetable for achieving the Digital Decade and the green transition.

Figure 17: Energy Sector: Four-Tier Distribution of Losses, 2026–2030 (EUR billion,%)

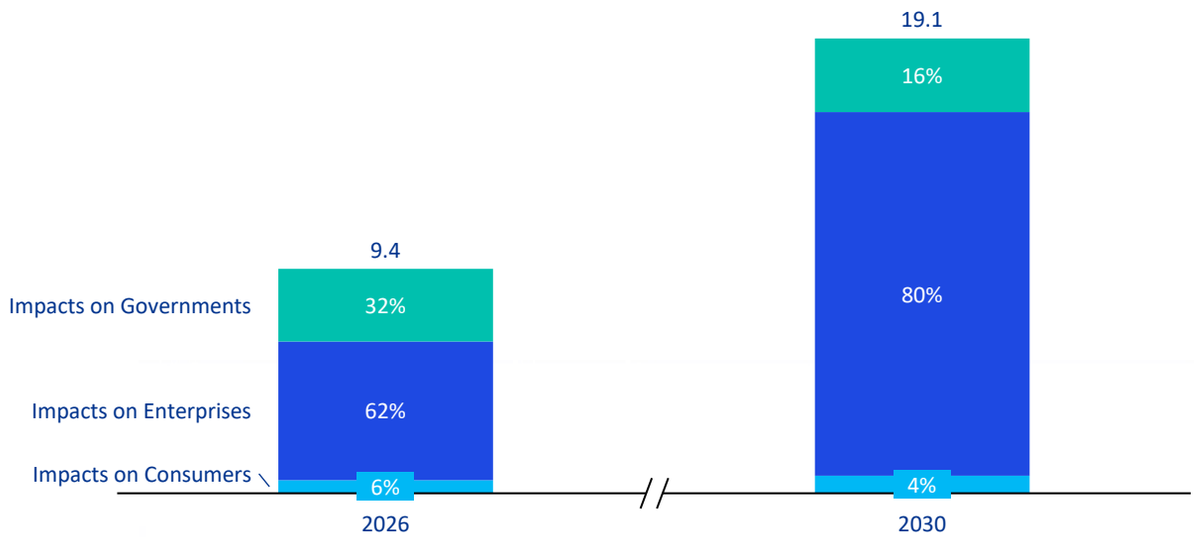


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of loss structure, the share of direct losses in the energy sector shows an upward trend. Assuming that in the first of the next five years most companies are still waiting on the sidelines and only a small number of aggressive projects proceed with replacement—yielding a replacement rate of 2%—which then rises to 10% in year two and to 29% in years three through five as the draft is fully implemented, direct losses in the sector would rise from EUR 0.6 billion in 2026 to EUR 6.9 billion in 2030, with hardware repurchase constituting the largest component.

Although the shares of indirect and social losses show a slight decline due to changes in the weighting of other categories, the amounts involved still rise from EUR 3.7 billion and EUR 4.9 billion in 2026 to EUR 5.9 billion and EUR 5.2 billion in 2030, respectively.

Figure 18: Energy Sector: Distribution of Impacts on Stakeholders[37], 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of the scope of losses in the short to medium term, cost pressure in the energy sector is highly concentrated on industrial operating entities, with enterprises bearing around 80% of operating losses, mainly from equipment replacement, project investment, and performance-related breach risks. Governments bear a relatively limited share in the form of supporting governance costs related to regional energy coordination and grid-connection control, while pass-through effects on end-use electricity consumers are not yet prominent. Over the longer term, however, the related costs would ultimately be borne mainly by member-state governments and the public.

37. Source note: the categories of economic loss shown in Figures 15, 17, 19, and 21 are classified according to the actual short- to medium-term bearer of the losses. Portions paid directly by enterprises, such as direct losses and indirect losses, are attributed to enterprise impacts; items borne directly by governments, such as contractual compensation and unemployment assistance, are attributed to government impacts; and items borne directly by consumers, such as initially visible price premiums for products and services, are attributed to consumer impacts.

38. https://www.eurelectric.org/publications/open-strategic-autonomy-considerations-from-the-power-sector-on-made-in-europe/

39. https://www.solarpowereurope.org/press-releases/statement-european-commission-publish-draft-revision-of-the-cybersecurity-act

5.3 Telecommunications Segment: The Complexity of Live-Network Migration Raises Replacement Costs, and Aggressive Decoupling Threatens the Continuity of Digital Infrastructure

CSA2 would have extremely deep reach into the telecommunications sector, covering the full chain of equipment from access networks to transport networks and core networks, as well as software-defined networking and operations-and-maintenance services. This includes 4G/5G base stations, optical transmission equipment, routers, gateways, carrier-grade servers, and the operating systems and management platforms that support this hardware. As part of the digital nervous system of modern states, these systems are so interconnected that equipment adjustments can directly affect signaling interactions, capacity configurations, roaming protocols, and complex cutover plans across the entire network, thereby affecting the smooth flow of network communications.

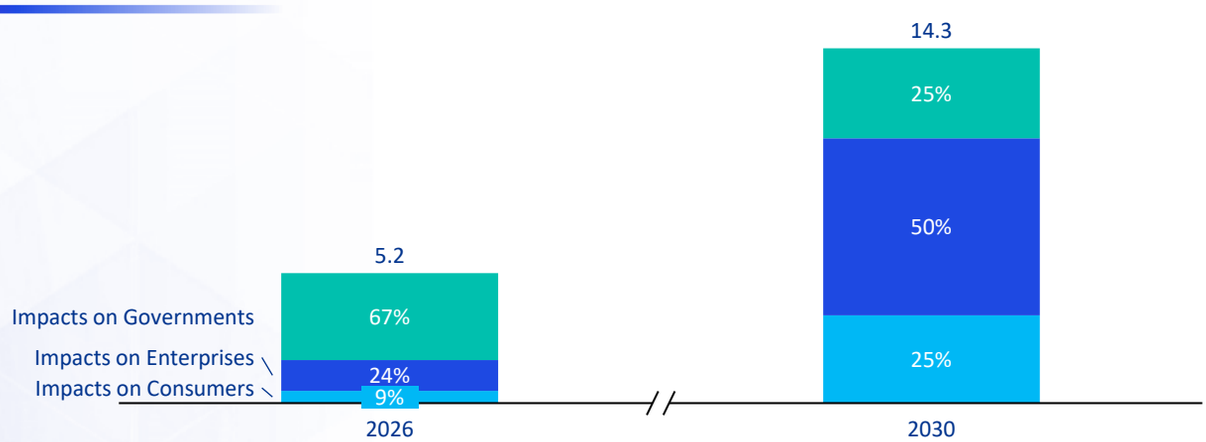
This assessment focuses on existing live-network equipment of Chinese suppliers in wireless access networks, optical transport backbone networks, fixed-network ONTs, and fixed-network OLTs, while also taking into account the topological feature of communications networks in which a change in one place can affect the system as a whole.

The replacement and upgrading of communications network equipment depends heavily on the live-network operating environment, and the interdependence of technical adaptation across levels is extremely strong. Updating access-layer equipment requires simultaneous compatibility with transmission and core-network protocols; changes in backbone networks are transmitted into service dispatch, data forwarding, and billing-control links; and upgrades to back-end support systems affect the full process of O&M monitoring and customer service. The impact of rectification thus runs through the entire network operating system.

At the same time, the core requirement in telecom network transformation is to ensure uninterrupted communications for users. The transition therefore typically adopts stable migration models such as parallel dual-network operation, zoned cutovers, and shadow running throughout the process. The replacement of base stations, transmission, and core-network systems all requires repeated coverage testing, traffic switchover, and route-stability verification, while cloud-network nodes and OSS/BSS support systems also need full-process business continuity testing. As a result, cutover cycles are long, commissioning steps are numerous, and the complexity of delivering network migration is exceptionally high.

Within the overall structure of EU economic losses, the telecommunications sector is smaller than energy but still substantial. Assuming forced replacement is completed within five years, total losses in telecommunications would reach EUR 57.4 billion, with annual losses rising from EUR 5.2 billion in 2026 to EUR 14.3 billion in 2030. Losses in the telecom sector are reflected in network migration, system switchover, testing and validation, and service-continuity arrangements, and more directly illustrate how supply-chain governance intrudes into live-network operations and customer-service systems.

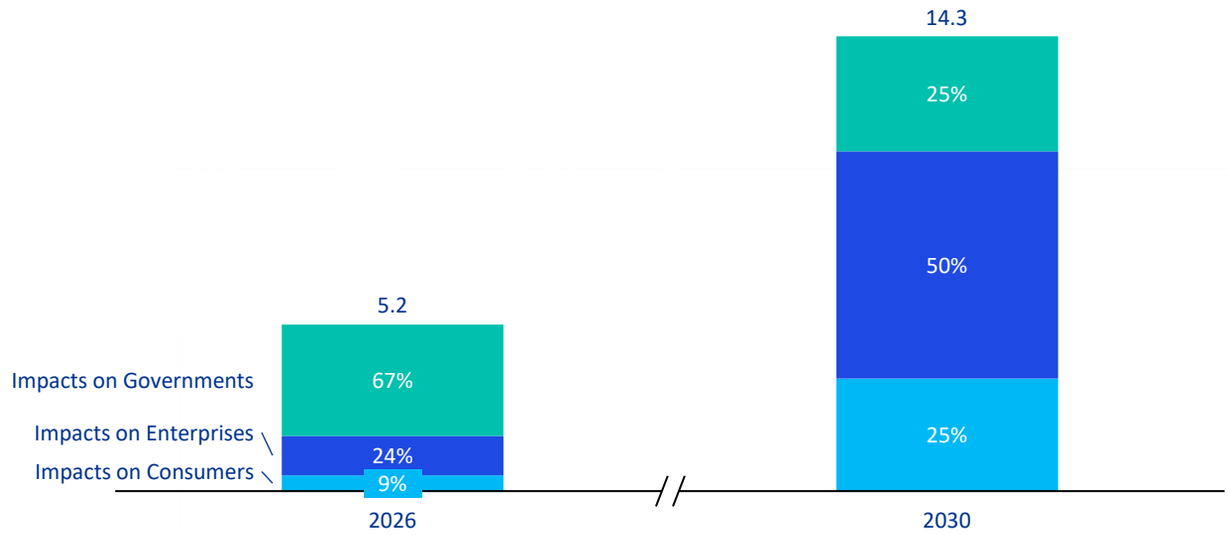
Figure 19: Telecommunications Sector: Four-Tier Distribution of Losses, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of loss structure, the share of direct losses in telecommunications rises continuously, increasing from 12% in 2026 to 53% in 2030. If mandatory removal and replacement were implemented over the next five years according to the assumed pace—2% in year one, 10% in year two, and 29% in years three through five—then, based on current equipment cost estimates, direct losses in the sector would rise from EUR 0.62 billion in 2026 to EUR 7.6 billion in 2030, with hardware repurchase constituting the largest component. Indirect losses would also rise from EUR 0.85 billion in 2026 to EUR 2.8 billion in 2030.

Figure 20: Telecommunications Sector: Distribution of Impacts on Stakeholders, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of impact scope, losses in telecommunications would be distributed across the full chain of government, enterprises, and consumers. Enterprises would face the heaviest pressure, with costs concentrated in equipment replacement and O&M transformation. Governments would bear supporting expenditures for compliance oversight and public communications assurance, while consumers would simultaneously share in small additional operating costs through communications services.

From an operational perspective, the telecommunications sector places greater emphasis on network continuity and service stability. Network services are closely linked to household communications, business operations, and public services, and system adjustments generally cannot be completed through one-off shutdowns, but instead must be advanced in phases while systems continue operating. This means that the associated costs arise not only from equipment procurement and system integration, but also from longer periods of parallel operation, denser testing arrangements, and more complex cutover organization.

> Ensure supply chain security measures strictly follow a risk-based approach, while respecting the competence of Member States for national security matters. Measures need to be proportionate, taking into account the need for predictability when rolling out network infrastructure with modernisation cycles of at least ten years – and risk assessments need to be up-to-date, carefully considering the impact on investment, resilience and service continuity.[40]
>
> ——Connect Europe, January 2026

40. https://connecteurope.org/news/connect-europe-statement-cybersecurity-act

5.4 Financial Infrastructure Segment: High-Availability Validation Drives Replacement Costs, While Reconstruction of Critical Systems Intensifies Operational and Compliance Risks

The various service scenarios within the financial infrastructure segment differ in emphasis, but most perform functions such as payment clearing, transaction processing, data storage, identity management, and support for critical business operations. The impacts they face are therefore closely tied to system availability, disaster-recovery arrangements, data processing, and the continuity of digital services.

CSA2's reach into the financial infrastructure segment extends across the full process of data centers, payment settlement, computing hubs, and risk-control systems used by financial institutions. It covers core routing and switching equipment, high-performance servers, distributed storage systems, firewalls, and critical business-logic software. These ICT devices form the bedrock of the modern financial system; minor latency issues or protocol mismatches can affect real-time transaction settlement, clearing instructions, disaster-recovery logic, and the compliance arrangements governing cross-border payments.

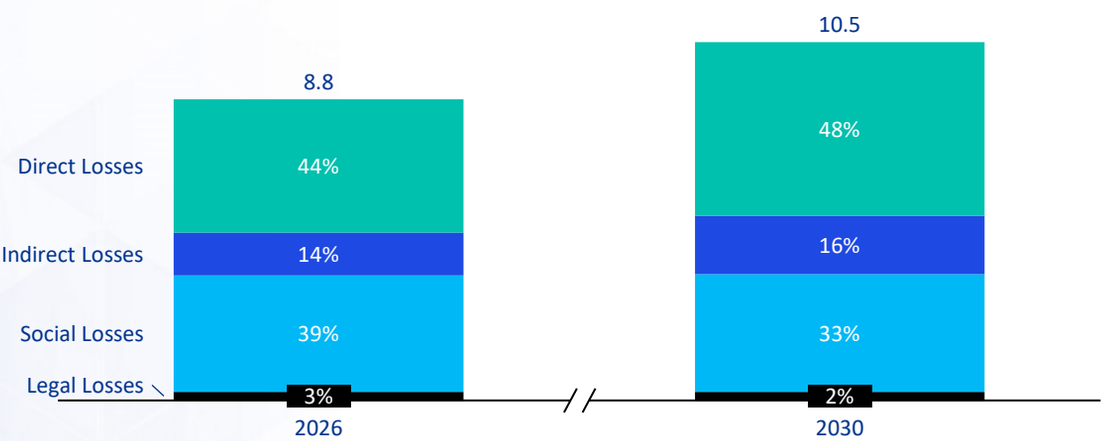
At the equipment and system level, the key affected carriers include full-network data-center equipment, computing server clusters, professional storage-control systems, financial key-encryption verification systems, dedicated interbank payment-switching devices, transaction platforms supporting the full range of securities and fund products, full-scope disaster-recovery and protection switchover systems, and compliant cloud-virtualization infrastructure. This assessment focuses on the compliant replacement costs of equipment at core computing nodes and data-storage endpoints, excluding scattered losses in some non-core business systems.

Such equipment is particularly vulnerable because it serves continuously operating critical digital businesses. For example, switching equipment, identity-management systems, and transaction-platform support systems within banking payment systems are directly tied to clearing, settlement, and risk-control processes.

The core operating logic of this sector differs from that of ordinary industries: all equipment iteration, system optimization, and architectural adjustment must be carried out on the premise of high availability and high reliability. In practice, equipment and platform replacement is usually accompanied by parallel main/backup operation, main/backup switchover testing, disaster-recovery validation, and extended observation periods.

Within the overall structure of EU economic losses, the financial infrastructure segment is smaller than energy and telecommunications. Assuming forced replacement is completed within five years, total losses in the segment would amount to EUR 49.9 billion, with annual losses rising from EUR 8.8 billion in 2026 to EUR 10.5 billion in 2030. The changes are mainly reflected in the implementation costs and operational adjustments associated with maintaining stability, auditability, and continuous operation while critical systems are being replaced, migrated, and adjusted.

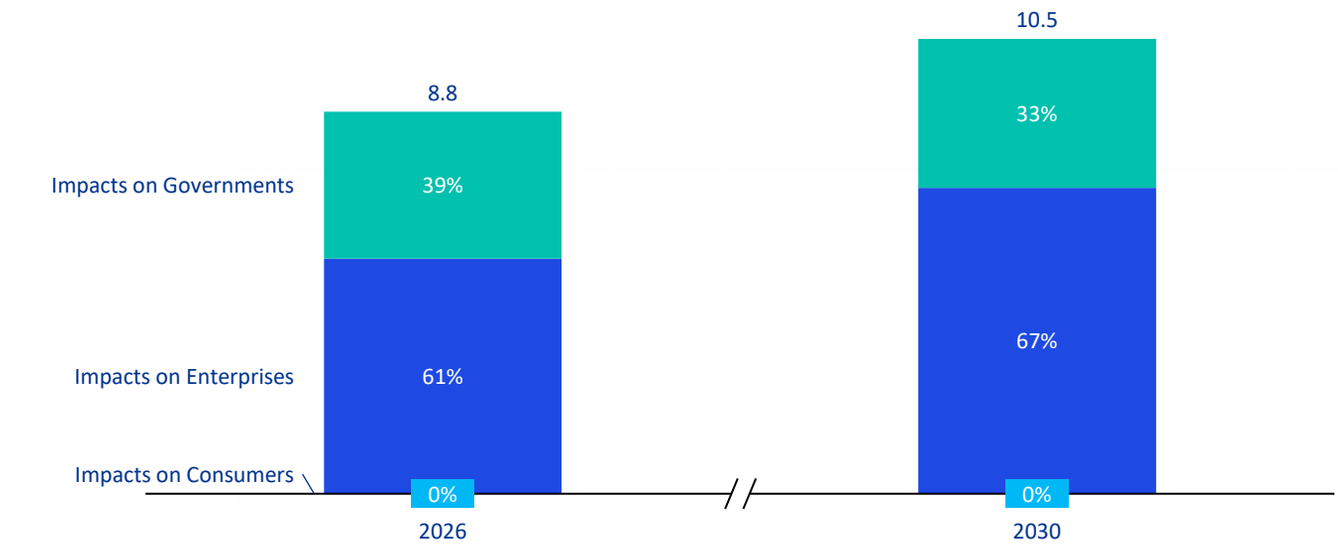
Figure 21: Financial Infrastructure Segment: Four-Tier Distribution of Losses, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of loss structure, direct losses dominate the financial infrastructure segment, consistently accounting for more than 40% and remaining stable over the five-year period. If mandatory removal and replacement were implemented over the next five years according to the assumed pace—2% in year one, 10% in year two, and 29% in years three through five—hardware replacement costs would amount to EUR 3.87 billion in 2026 and rise to EUR 4.72 billion in 2030. Indirect losses would account for approximately 15%.

Figure 22: Financial Infrastructure Segment: Distribution of Impacts on Stakeholders, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Compliance costs in the financial infrastructure segment would largely be absorbed within a closed loop by major banks and financial institutions, which would face severe compliance premiums and operational-stability challenges. Governments and regulators would mainly bear the costs of reshaping supervisory frameworks and monitoring market stability.

> This may give rise to concerns regarding transitional arrangements and the mitigation of claims for wrongful termination, notably in agreements procuring ICT assets and services concluded at the group level on behalf and to the benefit of entities across the EU or even the globe.[41]
>
> Due to the overlap with DORA, the Commission should have proposed a sectoral exemption for financial services from the Cyber Resilience Act. This is a missed opportunity for bold simplification. We urge the European Parliament and Council to challenge this decision not to exempt financial services, as has been done with industries such as aviation and automotives.[42]
>
> ——European Banking Federation, February 2026

41. https://www.nautadutilh.com/en/insights/new-eu-cybersecurity-package--digital-sovereignty-without-saying-it/

42. https://www.afme.eu/media/303hv0vt/digital-omnibus_-op-res-cyber.pdf

5.5 High Replacement Costs Would Hit Real-Economy Production Directly, while Supply-Chain Separation Would Disrupt Delivery Timelines Across the EU

The logistics and manufacturing segment includes industrial control systems, advanced manufacturing and semiconductor-related production, chemicals and specialty materials, food production and supply systems, port systems, and logistics systems. Although these industries differ from one another, the impacts they face are mainly reflected in equipment and system adjustments in production-line control, warehouse management, logistics dispatch, and delivery systems.

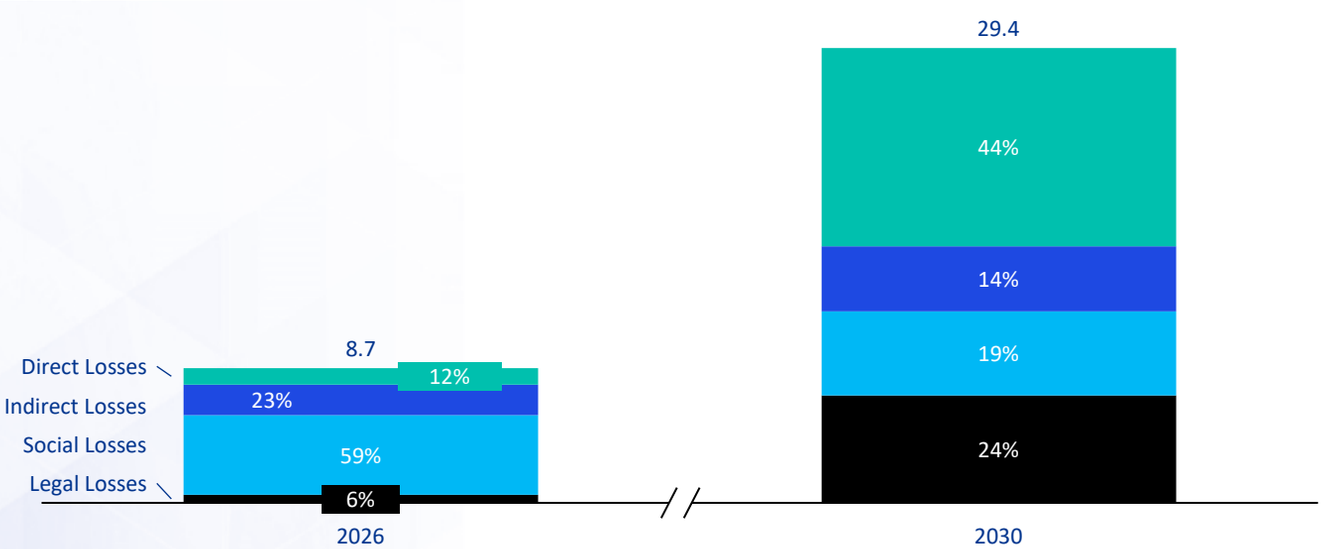
Once equipment and systems enter an adjustment period, the effects extend to production rhythms, dispatch logic, and delivery organization. The key affected carriers include industrial switches, warehouse automation systems, transport-dispatch platforms, and supply-chain visibility platforms, all of which perform critical functions in production control, data monitoring, and logistics connectivity. This assessment focuses on the replacement of key production automation and supply-chain management products such as general-purpose precision machine tools, automated execution equipment, and intelligent sensing devices.

Such equipment is particularly vulnerable because it is closely tied to continuous production and just-in-time delivery. Equipment in industrial control systems is typically directly related to process flows, quality management, and equipment maintenance; automated-control systems, transport-dispatch systems, and supply-chain visibility platforms in warehousing and logistics are likewise closely connected to inventory organization, vehicle coordination, and regional distribution.

Replacement in this sector must proceed in line with existing production and transport rhythms and cannot be carried out independently of the production line. Implementation therefore requires partial line stoppages, interface adaptation, on-site commissioning, and phased switching.

Total losses in the logistics and manufacturing segment amount to EUR 114.6 billion, making it the most severely affected segment in the EU's overall economic-loss profile. Assuming forced replacement is completed within five years, annual losses would rise from EUR 8.7 billion in 2026 to EUR 29.4 billion in 2030. These changes are mainly reflected in implementation costs, changes in operational organization, and project-timing adjustments during the replacement, migration, and interface adjustment of production, warehousing, transport, and dispatch systems.

Figure 23: Logistics and Manufacturing Segment: Four-Tier Distribution of Losses, 2026–2030 (EUR billion,%)

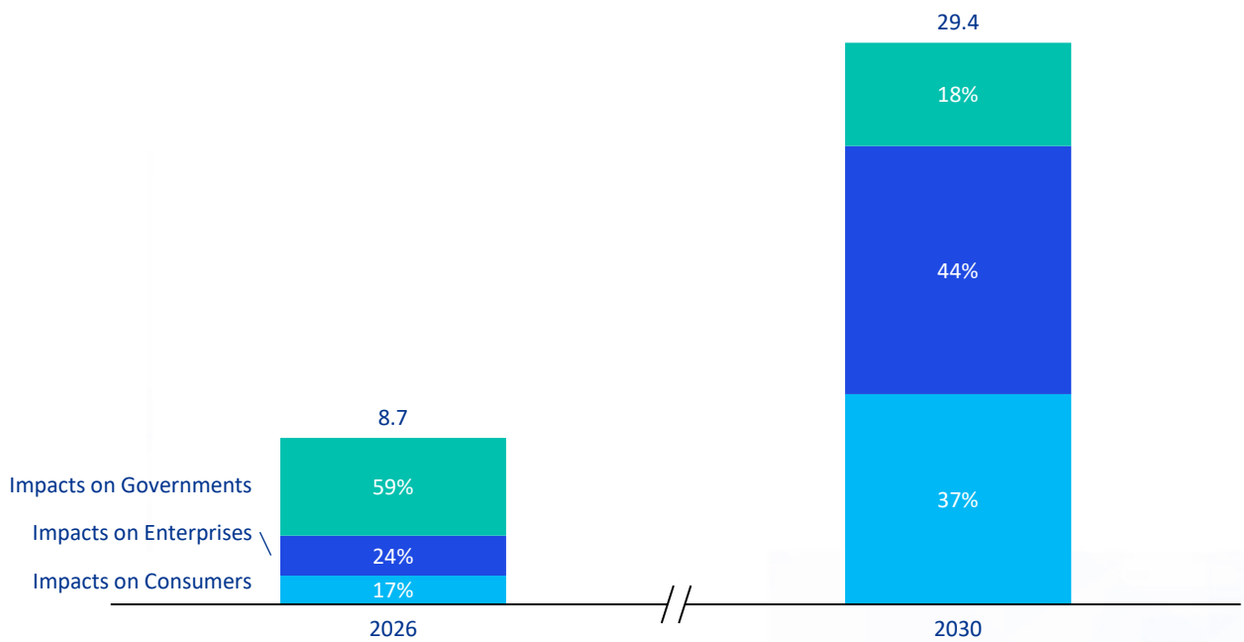


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of loss structure, the share of direct losses in the logistics and manufacturing segment would rise from 12% in 2026 to a high of 44% in 2030. The Direct losses in the sector would rise from EUR 1.08 billion in 2026 to EUR 12.8 billion in 2030, with hardware repurchase constituting the largest component. Indirect and social losses involved still rise from EUR 1.97 billion and EUR 5.16 billion in 2026 to EUR 4.2 billion and EUR 5.5 billion in 2030, respectively.

If one further considers dimensions such as digital twins and smart warehousing in the evolution of Industry 4.0, the systemic loss generated by industry alone would reach an even higher order of magnitude. The resulting crowding-out effect would force enterprises to reduce R&D budgets for advanced manufacturing processes, directly worsening financial models and substantially weakening the cost competitiveness of EU manufacturing in the global value chain.

Figure 24: Logistics and Manufacturing Segment: Distribution of Impacts on Stakeholders, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of the scope of impact, cost pressure in logistics and manufacturing would remain highly concentrated on manufacturing entities in the short to medium term. Over the longer term, however, governments would face employment fluctuations and output losses stemming from declining corporate competitiveness, while the impact on end consumers would gradually increase as higher production costs and lower efficiency are transmitted through the industrial chain, ultimately showing up in greater price volatility for finished consumer goods, longer delivery cycles, and declining stability of market supply, thereby creating increasingly tangible effects for consumers.

Case

The Risks and Costs of Replacing Security Screening Equipment:

Taking security screening equipment as an example, such devices play an important role at the borders of member states. If mature technology products that have operated stably for many years no severe security incidents on record were forcibly replaced on a large scale, this would likely, on the one hand, lead directly to a marked decline in security inspection and protection capabilities, thereby creating border-control risks; and on the other hand, generate a series of additional economic costs such as equipment replacement, system commissioning, and site shutdowns. Moreover, during replacement and commissioning, gaps in security inspection could easily arise, potentially allowing drugs, smuggled goods, and other prohibited items to enter the European market, thereby creating potential security hazards, economic losses, and broader social-security impacts for the EU.

> Companies operating in sectors of high criticality and other critical sectors may face disruption in their ICT supply chain and increased costs if suppliers are listed as high-risk and/or the sourcing countries are designated, particularly where alternative ICT components are limited. In some cases, product or service redesign may be required.[43]
>
> ——ACQUIS, February 2026

> But if CSA2 now comes in through the side entrance and starts imposing supply-chain measures tied to the same vehicle-related systems and assets, then the neat boundary the EU itself drew begins to look rather decorative. It is difficult to argue with a straight face that vehicles should stay out of one horizontal cyber regime because sector-specific regulation exists, while also trying to pull them into another horizontal regime built around the same technical reality.[44]
>
> ——SMARTNUTS, March 2026

43. https://www.acquislp.eu/your-guide-to-the-proposal-for-the-cybersecurity-act-2-security-of-ict-supply-chains-16-february-2026

44. https://smartnuts.com/2026/03/20/the-commissions-latest-regulatory-land-grab-why-csa-2-should-stay-out-of-automotive/

5.6 Public Services Segment: Compliance Expenditure Crowds Out Public Finance, While Service Continuity May Be Constrained by Local Budget Bottlenecks During Implementation

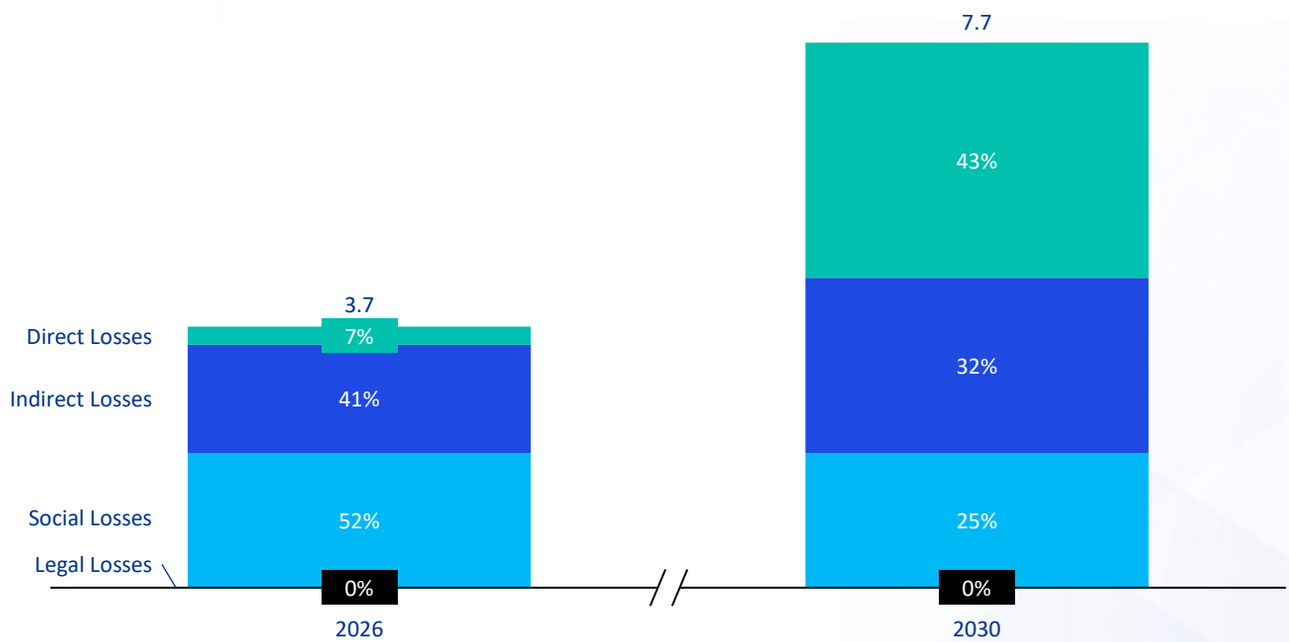
The public services segment mainly includes water systems and public administration. The affected industries in this segment are more closely tied to public budget arrangements and the continuity of public services.

Core facilities in the public-services field that are vulnerable to disruption mainly include intelligent pump-station dispatch systems, industrial PLC controllers, communications management and control platforms, core databases, and public-service software. These facilities are widely deployed in water services and public administration and perform key functions in data collection, intelligent dispatch, process control, and support for public livelihood services. This assessment focuses on the replacement of public-administration servers and water-related control equipment.

Such equipment is located at critical nodes of public operations and is weakly resilient to disruption. Monitoring systems and pump-station equipment in water utilities are directly linked to the stability of water supply and drainage, while public-management databases and servers support livelihood services and local administration. The associated costs include not only equipment procurement and installation, but also O&M assurance, off-peak construction, and organizational coordination.

The public-services segment is relatively smaller within the EU's overall economic loss structure, with total projected losses of EUR 32.2 billion. Assuming forced replacement is completed within five years, annual losses would rise from EUR 3.7 billion in 2026 to EUR 7.7 billion in 2030. These changes mainly reflect implementation arrangements, budget organization, and service-assurance requirements during the replacement, migration, and adjustment of public operating systems.

Figure 25: Public Services Segment: Four-Tier Distribution of Losses, 2026–2030 (EUR billion,%)

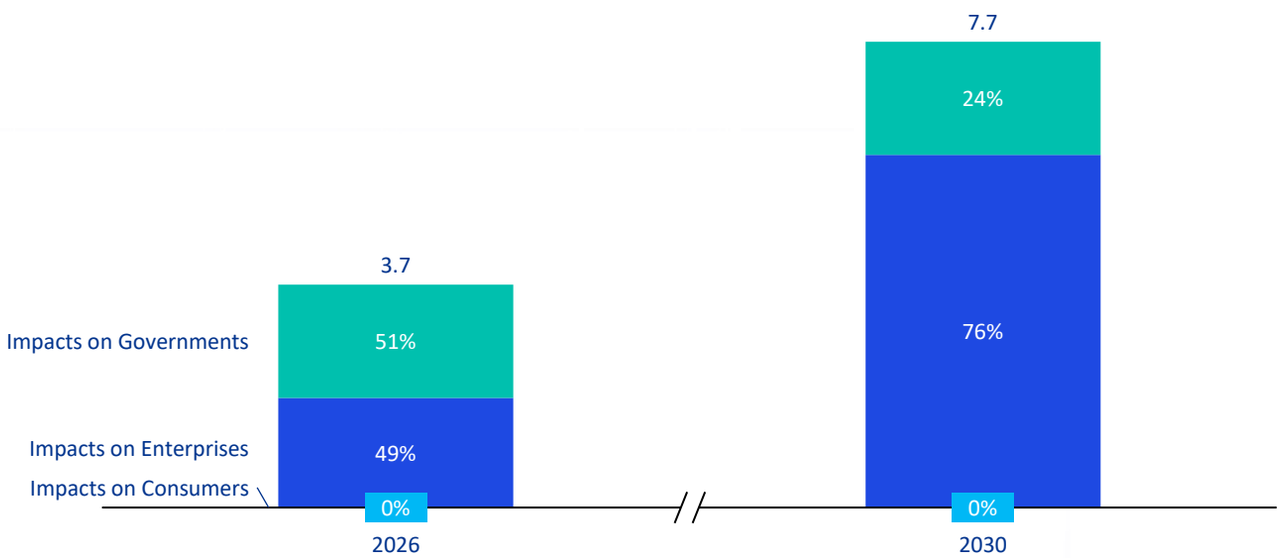


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of loss structure, as the proportion of forced replacement continues to rise, the amount of direct losses in the public-services sector would increase from EUR 0.26 billion in 2026 to EUR 3.3 billion in 2030. By contrast, the share of indirect losses and social losses would decline, although the absolute amount would arise.

Figure 26: Public Services Segment: Distribution of Impacts on Stakeholders, 2026–2030 (EUR billion,%)

Direct losses in the sector would rise from EUR 1.08 billion in 2026 to EUR 12.8 billion in 2030, with hardware repurchase constituting the largest component. Indirect and social losses involved still rise from EUR 1.97 billion and EUR 5.16 billion in 2026 to EUR 4.2 billion and EUR 5.5 billion in 2030, respectively.



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of the scope of impact, cost pressure in the public-services field would be borne almost entirely by governments. Although enterprises acting as contractors would bear part of the operational pressure, they would ultimately pass it on to local public finance through renegotiated government contract prices. End users would not directly bear fiscal costs, but would face the risk of deteriorating public-service quality.

45. https://table.media/assets/europe/com2026_11_tdurgvaqaicqrywwhhz78q00k_123727.pdf

5.7 Health and Research Segment: Forced Replacement Delays Medical Efficiency, While Data-Interruption Risks Severely Drag on Innovation and R&D Progress

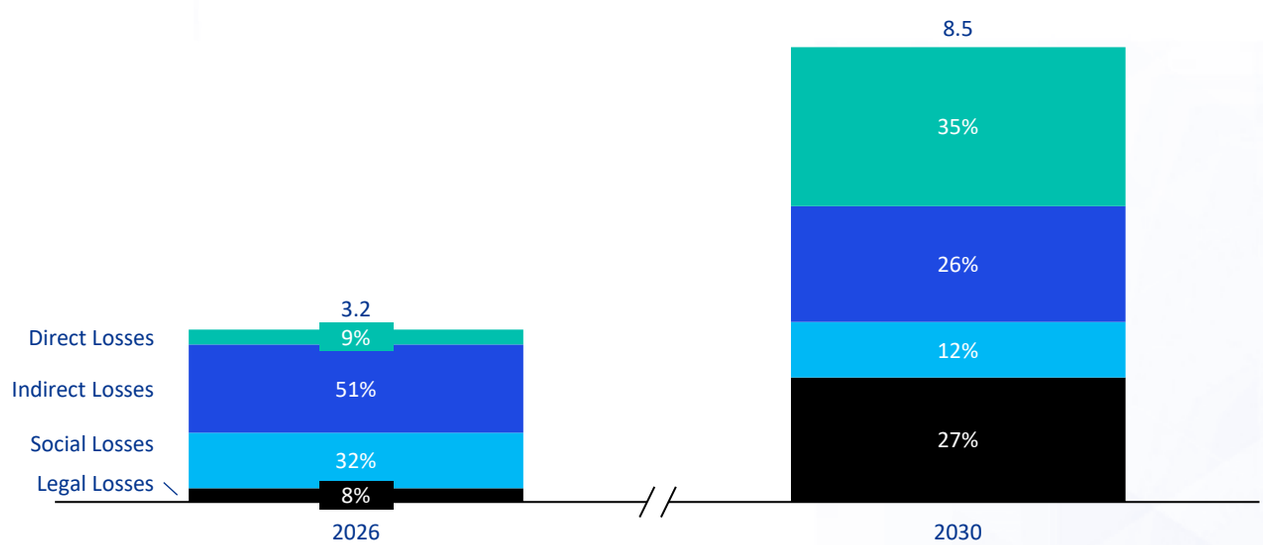
The health and research segment mainly includes medical equipment, smart healthcare, and research platforms, and is characterized more by high-reliability equipment and professional workflows.

The specific core components affected include hospital network equipment, core medical imaging equipment, laboratory information management systems, research computing and storage platforms, and research network infrastructure. Imaging and clinical platforms in healthcare systems are tied to hospital networks and clinical workflows, while computing and storage equipment on research platforms supports research tasks and long-term projects. This assessment focuses mainly on the replacement of key medical-impact equipment, high-performance computing equipment, and laboratory automation equipment.

Such equipment is particularly vulnerable for two reasons: first, it requires extremely high levels of stability, accuracy, and continuity; second, it is deeply embedded in professional workflows, data processing, and long-term project arrangements. During replacement, the impact runs through the full process of platform operation, data management, and professional services, rather than being confined to hardware replacement alone.

Total losses in the health and research segment amount to EUR 33.8 billion, which is comparatively small within the overall structure of EU economic losses. Assuming forced replacement is completed within five years, annual losses are projected to rise from EUR 3.2 billion in 2026 to EUR 8.5 billion in 2030. These changes mainly reflect operating arrangements, validation requirements, and project-timing changes during the replacement, migration, and adjustment of medical-service and scientific-research platforms.

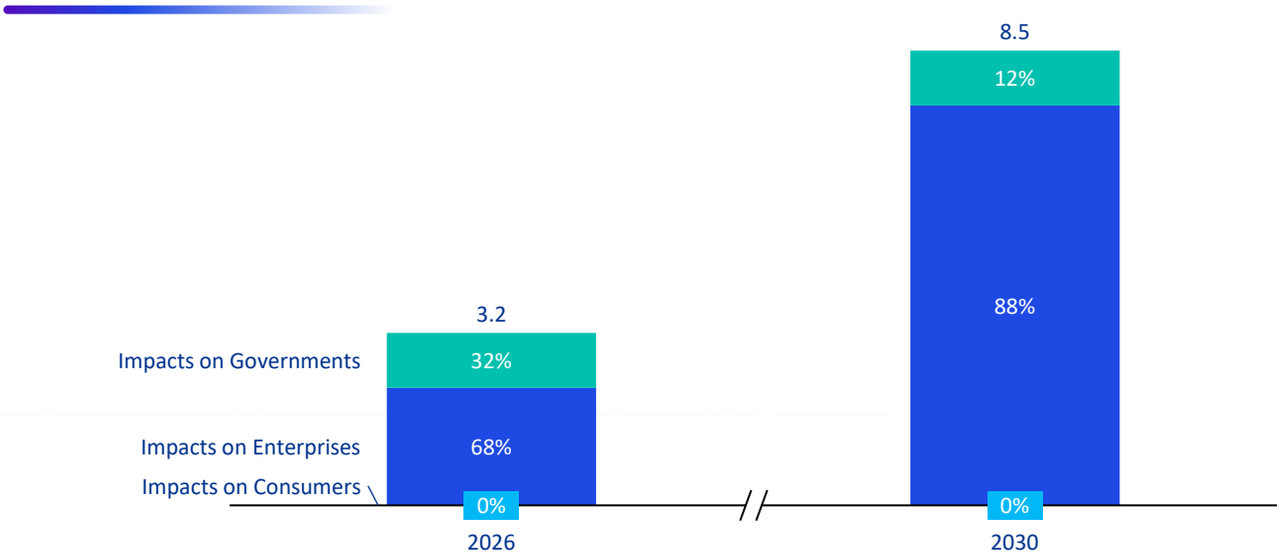
Figure 27: Health and Research Segment: Four-Tier Distribution of Losses, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of loss structure, the amount of direct losses in the health and research segment would rise from EUR 0.27 billion in 2026 to EUR 3.0 billion in 2030; meanwhile its indirect losses and social losses would not decline.

Figure 28: Health and Research Segment: Distribution of Impacts on Stakeholders, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

From the perspective of the scope of impact, compliance pressure in the health and research segment would be highly concentrated in the short to medium term on hospitals and major research institutions, with enterprises and institutions bearing more than 85% of direct losses. At the same time, governments would face challenges to the efficiency of public-health expenditure. Although ordinary patients may not feel direct costs in the short term, delayed R&D progress and the replacement of medically significant equipment would directly lengthen diagnosis and treatment cycles. Over the long term, negative social consequences would undoubtedly increase.

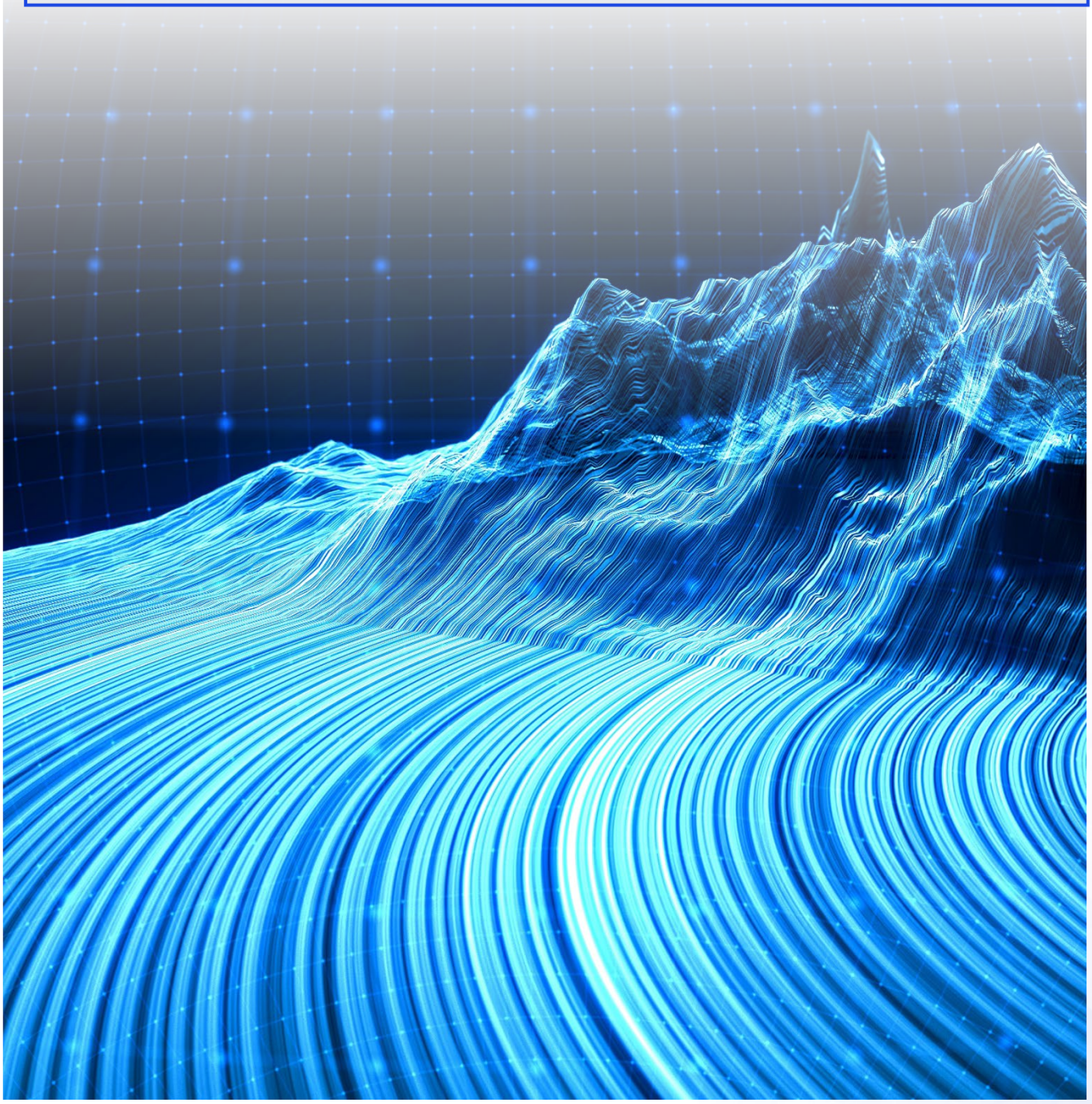
> This proposed shift risks forcing sectors – including health, energy, and finance – to remove deeply integrated ICT components that have supported business operations for decades.[46]
>
> ——IBEC, April 2026

> IBEC, the group that represents Irish business, has warned that proposed changes to the EU Cybersecurity Act (known as 'CSA2') could threaten the stability of 18 critical industries. IBEC highlights that the European Commission's proposal introduces "high-risk supplier" designations based on geopolitical origin rather than technical security flaws, overriding national security competencies.[47]
>
> ——IBEC, April 2026

46. https://www.ibec.ie/connect-and-learn/media/2026/04/15/eu-cybersecurity-act-review-presents-concerns-for-irish-business-new-ibec-report
47. https://www.ibec.ie/connect-and-learn/media/2026/04/15/eu-cybersecurity-act-review-presents-concerns-for-irish-business-new-ibec-report

Chapter Summary: Anchor Sectors Face Deep Pressure, and the System of Industrial Collaboration Faces Structural Erosion

CSA2 is triggering a systemic shock that reaches into the industrial foundations of the EU. The energy sector ranks first in total losses because of the scale of equipment replacement and the extremely high investment intensity involved; telecommunications ranks second because of migration complexity and continuity requirements. Financial infrastructure, logistics and manufacturing, public services, and research and health follow behind. This comprehensive penetration—from core infrastructure to specialized service platforms—means that the impact of the proposal is no longer confined to the replacement of a small number of suppliers, but has become a systemic erosion of the overall operating efficiency of EU industry. Enterprises would be forced into painful resource misallocations between compliance costs and innovation momentum, which would not only weaken global competitiveness across sectors, but could also undermine the foundations of the EU's Digital Decade and green transition goals.



06

Assessment of Economic Losses Across the 27 EU Member States

Once a uniform EU-level rule enters the implementation stage across 27 sovereign states, originally balanced policy expectations are transformed into highly differentiated national burdens, producing clear asymmetric economic consequences.

6.1 Key Points of Focus

There is clear divergence in the pressure borne by member states. Because countries differ greatly in industrial structure, fiscal space, energy systems, and digital-transformation progress, the economic outcomes generated by the CSA2 proposal vary sharply across member states. Governments would be forced into extremely painful resource misallocations between bearing high asset-replacement costs and maintaining social welfare. This imbalance in compliance burdens would severely affect the overall stability of the EU single market.

The burden at the member-state level displays pronounced tiering, and the scale of loss is not simply proportional to economic size; rather, it is closely tied to factors such as the complexity of national industrial systems and the degree of coupling between energy and digital systems. According to the assessment, Germany (projected losses of EUR 170.8 billion), together with France (EUR 46.3 billion), Italy (EUR 36.5 billion), Spain (EUR 25.7 billion), Poland (EUR 21.3 billion), and the Netherlands (EUR 20.1 billion), forms the high-pressure tier, while other countries would also face average losses ranging from several billions to tens of billions[48] of euros. These losses are not merely about equipment replacement expenditure, but involve systemic challenges relating to service continuity, corporate cash flow, public cost premiums, fiscal pressure on governments, and the pace of industrial digitalization.

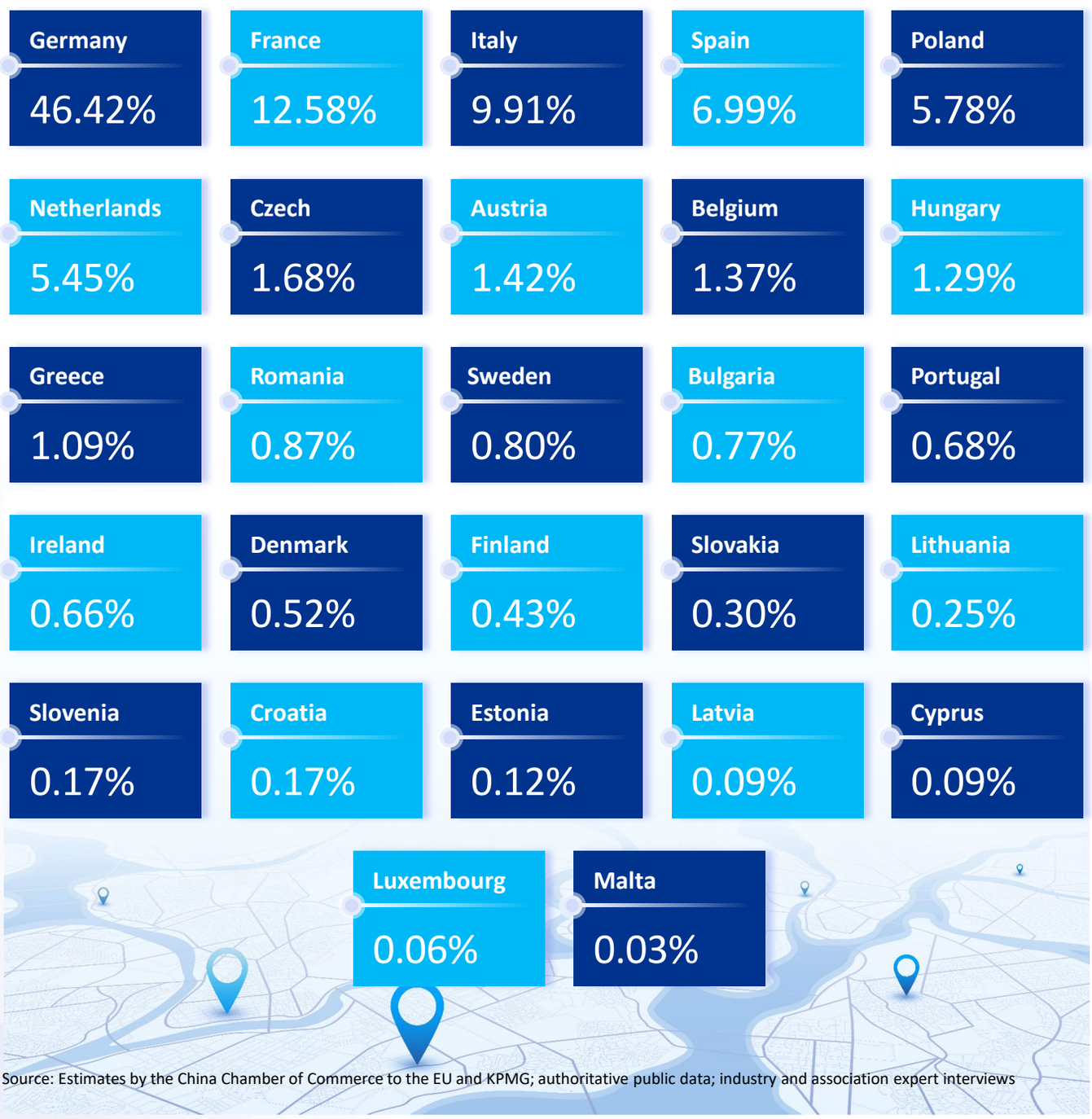
The complex constraints that policy objectives encounter in real-world implementation differ sharply from country to country because of economic and geographic diversity. In Germany and Italy, pressure is concentrated more on the interaction between industrial energy costs and distribution-network retrofitting, while Spain is more affected by delayed energy-transition progress, grid-connection delays for projects, and rising household bills. Countries with more limited fiscal space or that remain in a catch-up phase of digitalization are even more likely to fall into a trap in which mandatory replacement becomes so expensive that it reverses development gains; the resulting disruption to budget scheduling could lower the quality of public services and create a direct conflict between the policy's intended security objectives and the real growth drivers of member states.

48. Compiled and estimated by KPMG and the China Chamber of Commerce to the EU on the basis of authoritative public sources, including Eurostat and the Ministry of Commerce of China, as well as publicly available corporate financial statements and interviews with industry experts.

6.2 Distribution of Overall Economic Losses Across the 27 EU Member States: High-Pressure Countries and Tiered Characteristics

When the CSA2 proposal is applied across member states, it is unlikely to generate homogeneous security gains. Instead, given the major heterogeneity in national industrial structures, it would evolve into an asymmetric economic shock. The cumulative losses triggered by the proposal would be distributed very unevenly across member states and would display clear tiered characteristics.

Figure 29: Distribution of Overall Economic Losses Across EU Member States, 2026–2030 (%)

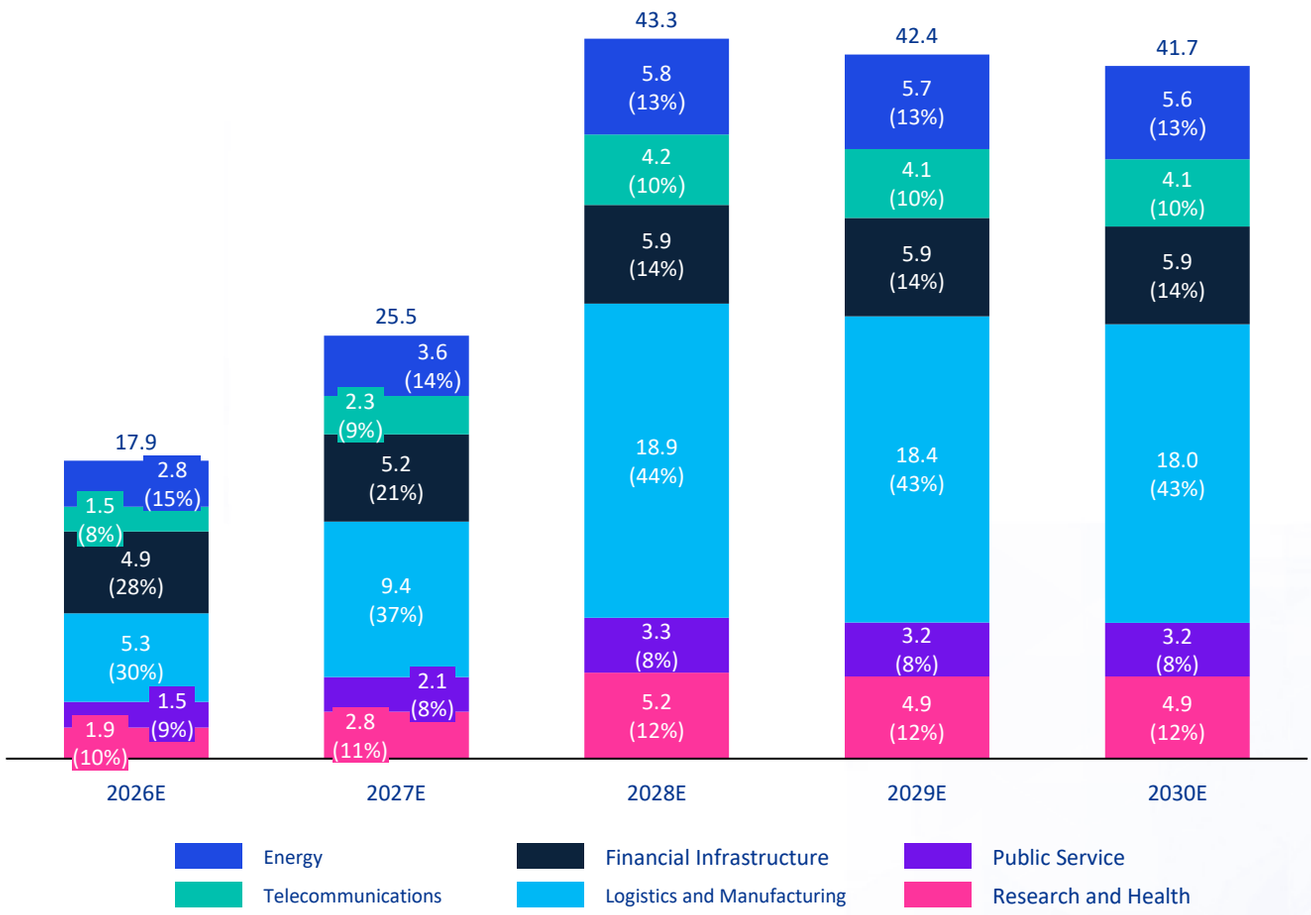


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

In this wave of regulatory disruption, the EU's economic engines and industrial powers would be at the forefront of pressure. The distribution of losses is not only a matter of size, but also reflects the cumulative effect of multiple factors including industrial structure, energy systems, digital-infrastructure maturity, and fiscal capacity to absorb shocks. At the same time, economic losses in all countries display an accelerating upward trend as the proposal advances.

Germany stands at the top of the high-pressure tier, with projected total losses of EUR 170.8 billion. If the proposal begins to be implemented rapidly and then deepens gradually, Germany's annual economic losses during 2026–2030 would rise continuously from EUR 17.9 billion to EUR 41.7 billion. In terms of the composition of total losses, the logistics and manufacturing segment accounts for the highest share at around 44%, followed by the financial infrastructure segment and the energy segment. This is closely related to Germany's strong industrial digitalization capabilities and the achievements it has already made in green transition.

Figure 30: Germany: Distribution of Overall Economic Losses, 2026–2030 (EUR billion,%)

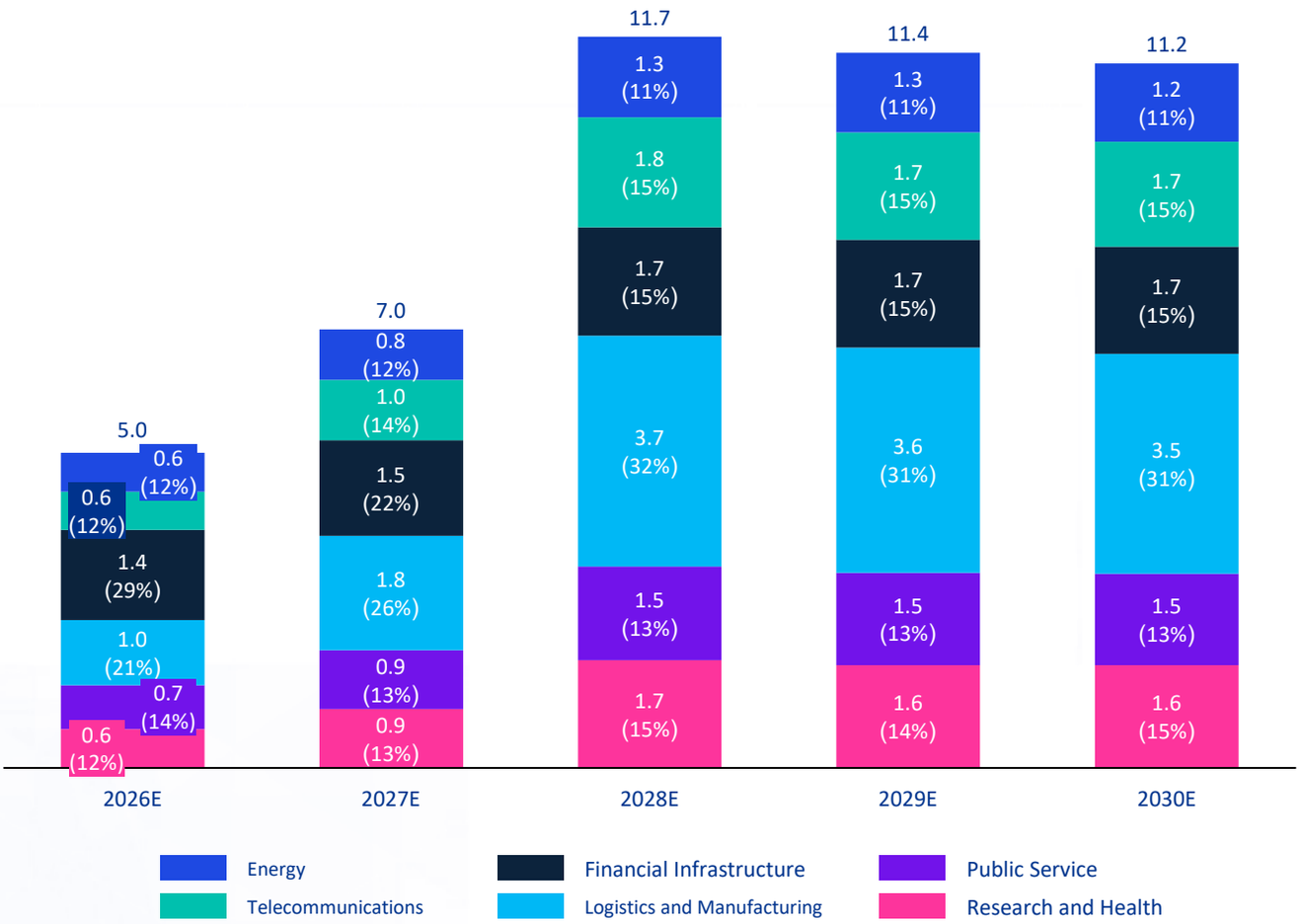


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Germany's deep manufacturing base, broad application of industrial control systems, and strong coupling of energy and digital infrastructure with the wider economy make the policy's effects more likely to manifest through industrial costs, investment rhythms, and production organization. For Germany, the losses would not simply take the form of spending changes at the equipment and system level, but would also affect Industry 4.0 progress, SME cash flow, and the green transition.

France is projected to suffer total losses of EUR 46.3 billion. If the proposal is implemented gradually, annual losses would rise from EUR 5.0 billion in 2026 to EUR 11.2 billion in 2030. The logistics and manufacturing segment would face the highest compliance pressure, accounting for about 30% of losses, followed by telecommunications, financial infrastructure, and energy; compared with Germany, France's burden is more evenly distributed across sectors. However, the shares of public services and research and health are significantly higher in France than in the other countries, implying a heavier burden on government fiscal expenditure.

Figure 31: France: Distribution of Overall Economic Losses, 2026–2030 (EUR billion)

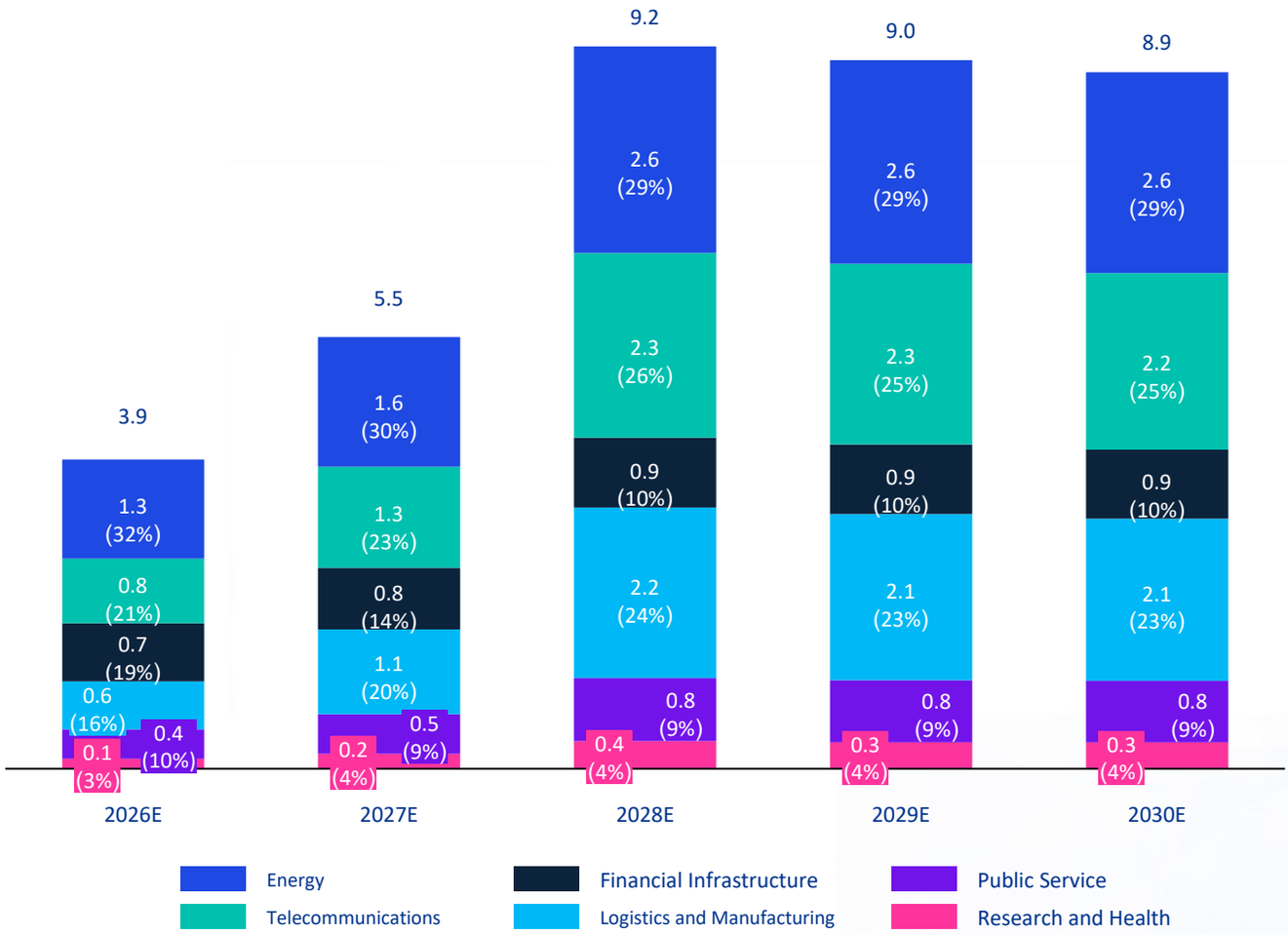


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Among EU member states, France has one of the most comprehensive supply-chain covers and one of the highest-value and most complex industrial structures. In this round, it would have to balance critical infrastructure, public-service systems, and the open innovation ecosystem. As resources flow toward security and compliance expenditure, France would still need to sustain continued investment in public-service coverage, critical infrastructure, and digital upgrading themselves.

Italy's total economic losses are projected to reach EUR 36.5 billion. As implementation deepens, losses are projected to rise from EUR 3.9 billion in 2026 to EUR 8.9 billion in 2030, albeit with some fluctuation. By sector, the energy segment would be hardest hit, accounting for nearly 30% of losses, followed by telecommunications at 25%. The shares of logistics and manufacturing, financial infrastructure, and other segments are significantly lower than in Germany and France, making the burden distribution across sectors notably differentiated.

Figure 32: Italy: Distribution of Overall Economic Losses, 2026–2030 (EUR billion,%)

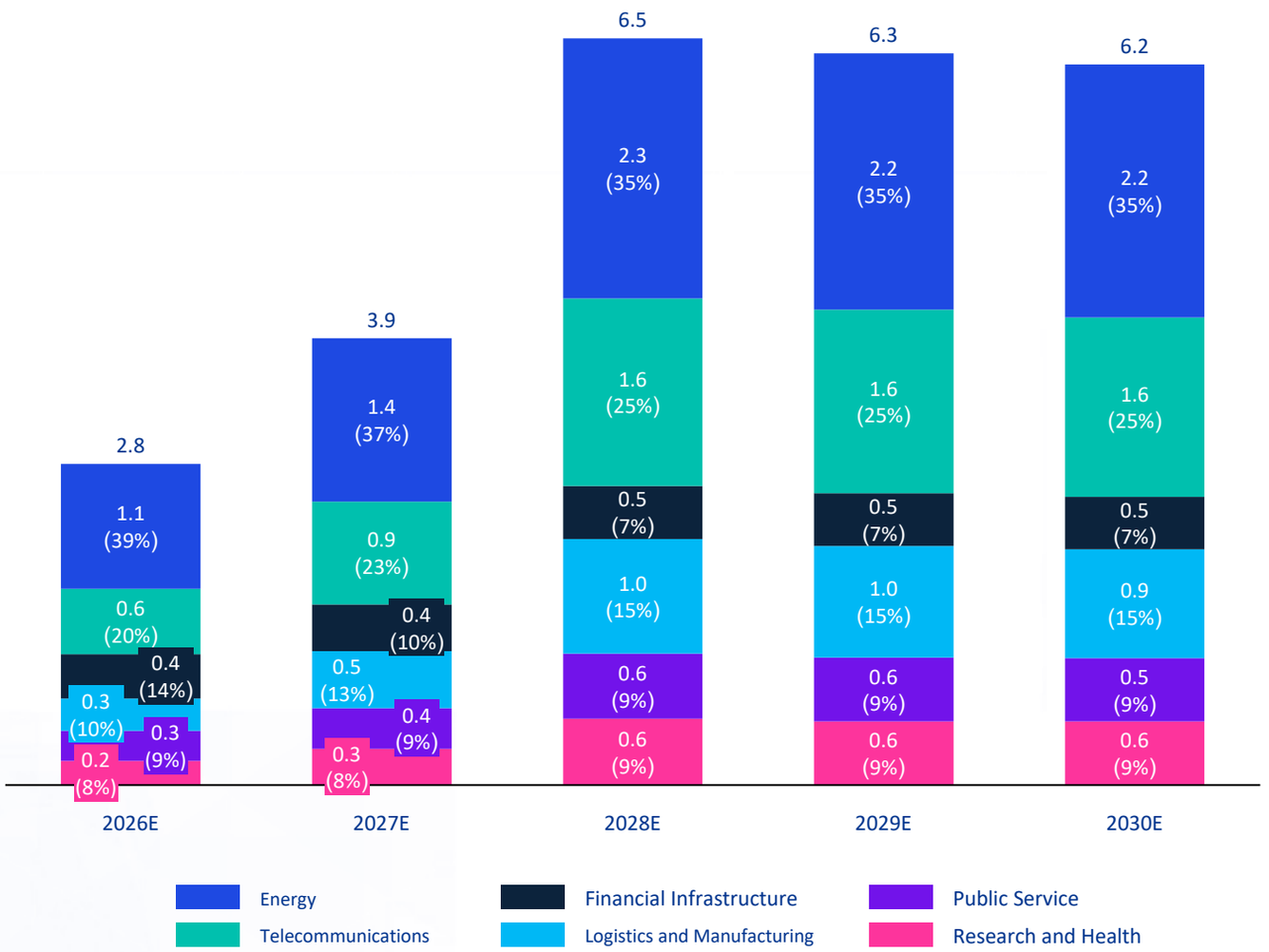


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Italy has high renewable-energy installed capacity, a highly digitalized grid, and high 5G coverage. Yet telecommunications and energy are among the sectors most heavily regulated under CSA2, meaning that the relevant policy would impose high compliance costs on Italy while further increasing fiscal pressure. It would also significantly slow Italy's green transition and digitalization process.

Spain is projected to incur total economic losses of about EUR 25.7 billion, with annual losses rising from EUR 2.8 billion in 2026 to EUR 6.2 billion in 2030. The energy segment accounts for the largest share among the high-pressure countries at about 35%, followed by telecommunications at 25%. The shares for financial infrastructure, logistics and manufacturing, and other segments are relatively smaller. This is closely related to Spain's high installed capacity in green energy and the depth of its digital economy.

Figure 33: Spain: Distribution of Overall Economic Losses, 2026–2030 (EUR billion,%)

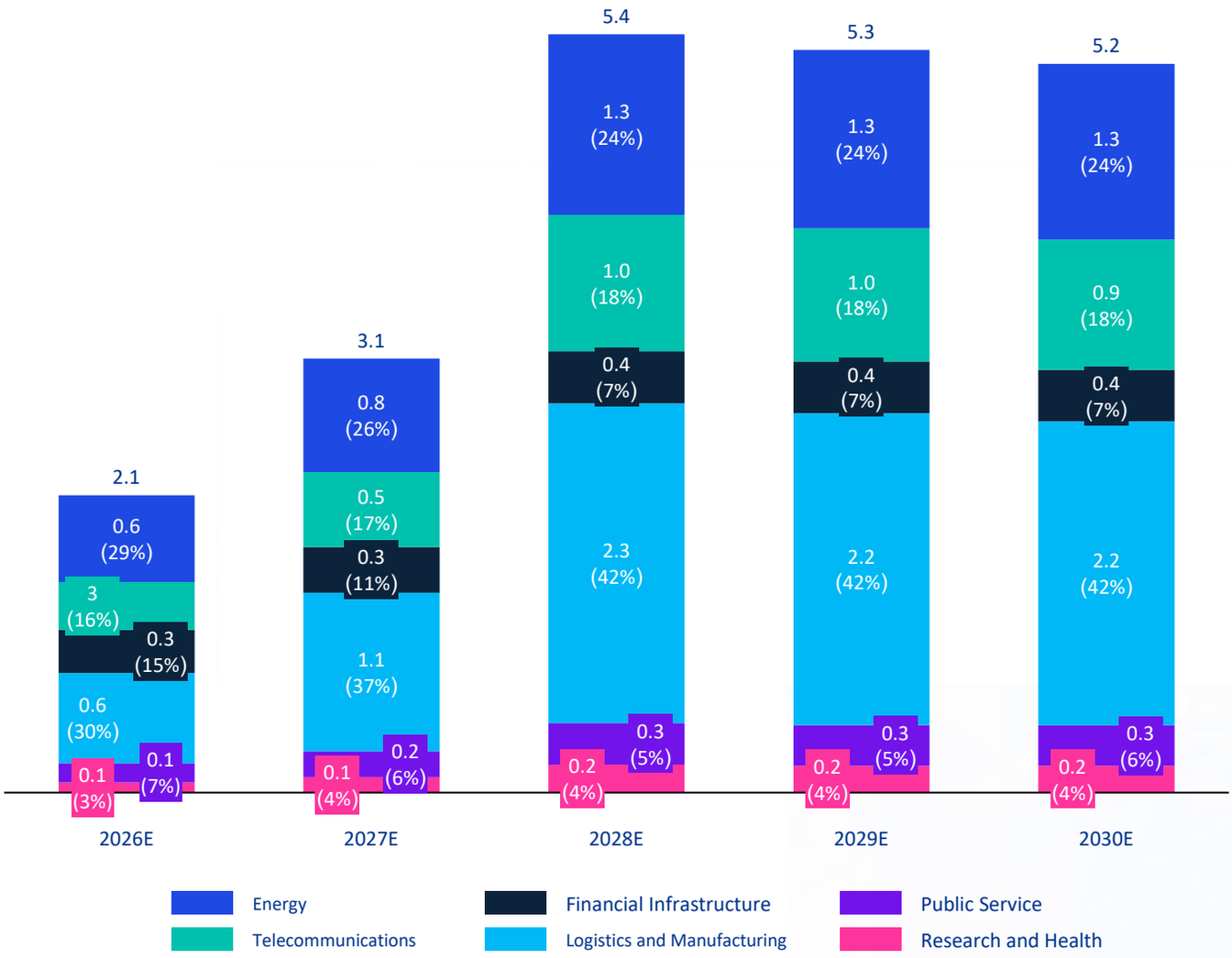


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Spain ranks among the leading EU countries in renewable-energy installations, with mature wind, solar, and geothermal generation technologies. Broadband and 5G deployment are also at a leading level. As one of the member states moving relatively quickly in the energy transition and hosting a high density of projects, Spain's large economic losses would not only take the form of transformation costs for energy systems and digital infrastructure, but would also directly affect service coverage, service quality, and the disposable income of businesses and residents. These effects would undoubtedly weigh on Spain's currently strong economic growth and employment performance.

Poland is projected to incur total economic losses of about EUR 21.3 billion, with annual losses rising from EUR 2.1 billion in 2026 to EUR 5.2 billion in 2030. The logistics and manufacturing segment accounts for the highest share at approximately 42%, followed by energy and telecommunications. The shares of other segments are relatively smaller, mainly because of Poland's strong industrial base, high share of renewable energy, and comparatively strong software capabilities.

Figure 34: Poland: Distribution of Overall Economic Losses, 2026–2030 (EUR billion,%)

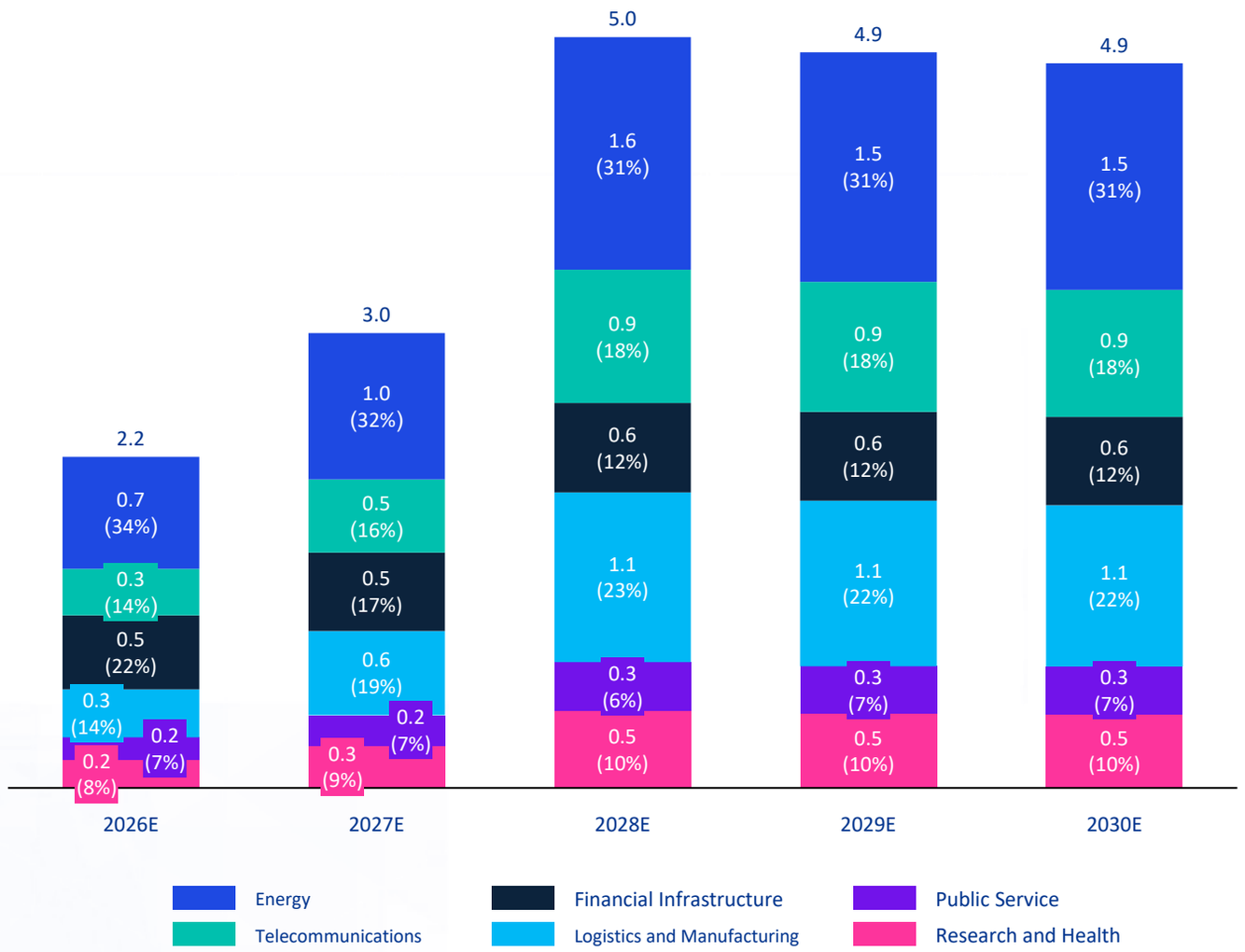


Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

Although Poland's energy structure is still centered on traditional coal-fired generation, solar and wind power have grown rapidly in recent years, renewable-energy installations now account for roughly half of capacity, and the share of renewable generation is also rising steadily, making green transition a prominent trend. At the same time, as a major industrial and logistics center in Central and Eastern Europe, Poland performs strongly in automotive, home appliances, and IT, while 5G coverage is in the middle-to-upper range. If the proposal were implemented, the multi-year forced replacement process would not only potentially create major shocks to grid stability, but would also affect public welfare, widen urban-rural gaps in telecom coverage, and drag on public finances.

The Netherlands is projected to incur total economic losses of about EUR 20.1 billion, with annual losses rising from EUR 2.2 billion in 2026 to EUR 4.7 billion in 2030. The energy segment accounts for the largest share at about 32%, followed by logistics and manufacturing at 23%. This is closely related to the Netherlands' very high level of energy digitalization and smart-grid development, as well as its world-class industrial infrastructure.

Figure 35: Netherlands: Distribution of Overall Economic Losses, 2026–2030 (EUR billion,%)



Source: Estimates by the China Chamber of Commerce to the EU and KPMG; authoritative public data; industry and association expert interviews

The Netherlands is the EU's leading offshore wind power country and is at the forefront in hydrogen, carbon capture, and the circular economy, with extremely high levels of energy digitalization and smart-grid development. At the same time, it is one of Europe's major hubs for broadband, 5G, and data centers, and its digital infrastructure is among the most advanced in the EU, while AI application also firmly places it in the first tier. Although the Dutch government has long run surpluses and enjoys ample fiscal space, the proposal would still create unnecessary financial losses. It would also seriously affect the Netherlands' model reputation as an open economy and damage its international reputation and related investment.

Beyond the high-pressure tier, the impacts on other member states are reflected more in two categories: medium pressure and general pressure.

The medium-pressure group mainly includes Austria, the Czech Republic, Hungary, Belgium, Greece, Bulgaria, Romania, Sweden, Portugal, Ireland, Denmark, and Finland. These countries generally have relatively solid and stable industrial and infrastructure bases, while also having somewhat greater fiscal buffering capacity. The effects of the proposal are therefore more likely to manifest in project timing and internal industry adjustments. Even so, they would still face substantial economic losses ranging from more than EUR 1 billion to several billions of euros.

The general-pressure group mainly includes Slovakia, Lithuania, Slovenia, Croatia, Estonia, Cyprus, Latvia, Luxembourg, and Malta. These countries are smaller in economic size and the scale of affected sectors is relatively limited. Although the impact on this group may amount only to several hundred million euros, this does not mean it can be ignored; relative to the size of their economies, it would still represent a substantial expenditure.

6.3 The Basis of Country-Level Differences: Interpreting the Disconnect Between Regulatory Rules and Economic Reality

The proposal gives rise to significant differences among member states in both total economic loss and sectoral composition, mainly for the following reasons.

First, heterogeneity in industrial structure cannot be ignored.

Differences in the scale of national losses stem from objective differences in economic foundations. Member states with a higher share of manufacturing and more complete industrial systems typically have more complex industrial control systems, broader application scenarios for energy and digital infrastructure, and longer operating chains for equipment and systems. As a result, under mandatory replacement they must bear capital expenditures many times larger than those in service-oriented economies. The impact of the proposal is therefore more likely to be reflected in production costs, investment timing, and industrial digitalization. Germany's massive losses, for example, are mainly due to the rigid dependence of its highly automated production lines on real-time data security and low-latency networks; forced removal of equipment implies direct risks to production continuity.

By contrast, economies with a higher share of services and relatively limited application of industrial control systems would still be affected, but their burden would more often be expressed through changes in public-service costs, the operation of digital platforms, and the pace of infrastructure transformation. Differences in industrial structure thus constitute the first layer underlying the variation in pressure across member states.

Second, differences in energy systems and digital-infrastructure foundations also affect implementation constraints across member states.

Countries with higher shares of renewable energy, more complex live-network structures, and more difficult grid-connection and dispatch systems are more likely to experience pressure in areas such as energy project scheduling, system access, end-user price pass-through, and service assurance. Spain, for example, as a "front-runner" in digital transformation and green energy, faces a particularly heavy compliance burden precisely because it has the highest density of installed live-network assets and the most complex replacement tasks.

The proposal disrupts existing investment schedules, forcing such countries to bear high additional administrative replacement costs on top of the costs required to achieve their original green-transition objectives. In substance, this amounts to penalizing the countries that have moved ahead in transition and weakens Europe's overall dual-transition momentum.

For member states that are still in the stage of infrastructure expansion and catch-up, the proposal would further affect construction rhythms, budget constraints, and the pace of service coverage. Differences in infrastructure foundations therefore produce differing sectoral-loss patterns and implementation difficulties across member states, but in all cases the proposal would disrupt existing trajectories.

Differences in transition progress further amplify divergence in the burdens borne by countries. For member states with faster green transition, stronger digital foundations, and larger project pipelines, the impacts are more likely to be reflected in changes to project timing, levelized electricity costs, installation rhythms, and the investment priority order for digitalization. For member states with weaker transition foundations and more limited original investment capacity, the impacts are more likely to appear as project delays, tighter budget constraints, and a slower pace of service expansion. The former face the problem of having their existing transition paths reset; the latter face further constraints on their starting point and capacity to advance transition. The real pressures on the two groups are not identical, but both demonstrate that uniform rules do not automatically produce uniform outcomes at the national level.

Third, fiscal space, engineering implementation costs, and local substitution conditions are also important factors behind differences among member states.

For member states with stronger fiscal capacity and relatively greater elasticity in public spending, additional expenditures caused by equipment replacement, system reconstruction, and service assurance may still be absorbed through budget adjustment, subsidy arrangements, or phased implementation, although this would also affect the original allocation of public resources. For member states under tighter fiscal constraints and heavier public-debt pressure, however, such changes are more likely to translate into budget reshuffling, project delays, and slower improvement in public services.

System replacement, interface adaptation, testing and validation, and parallel-operation arrangements all require corresponding engineering resources, professional teams, and local service capacity. Member states with stronger engineering capabilities and more mature supporting services may be able to absorb these pressures through project management and construction organization, though at the cost of low-value resource consumption; for member states with more limited professional implementation resources, smaller market capacity, or insufficient replacement conditions, equipment and system adjustments are more likely to translate into construction congestion, certification queues, and rising implementation costs.

Accordingly, differences at the member-state level are reflected not only in the size of losses, but also in industrial structure, infrastructure, fiscal space, engineering implementation costs, and many other factors. The one-size-fits-all approach embodied in CSA2 plainly fails to take these differences sufficiently into account.

6.4 Implementation Constraints and Burden-Bearing Capacity: Assessing the Real Obstacles to Policy Execution

The mandatory implementation timetable set out in CSA2 is, to a large extent, detached from the practical realities facing EU member states. It fails to adequately consider the objective constraints each country faces in fiscal absorption capacity, engineering implementation cycles, and supply-chain resilience.

The 36-month compulsory replacement cycle required by the proposal is in natural conflict with the modernization cycle of more than ten years typical of core infrastructure such as telecommunications. For operators, such an intense concentration of tendering, testing, and replacement work would lead to severe engineering congestion. In the absence of sufficient engineering manpower and substitute resources, such an aggressive timetable would directly cause project delays and deterioration in service quality.

The fiscal space available to member states to absorb cost shocks is extremely uneven. For countries under greater debt pressure, massive equipment replacement expenditure cannot easily be absorbed through government subsidies and would inevitably be passed through to end-use businesses and households via higher energy and communications bills. This hidden form of "regulatory taxation" would directly reduce household purchasing power, raise industrial energy costs, and sharply weaken public acceptance.

Mandatory supplier exclusion is not only a matter of financial loss; it also concerns the risk-bearing capacity of supply chains. Because some member states are highly deficient in local substitute solutions and service resources, forced replacement would expose them to serious supplier lock-in risks. Once the range of available vendors is drastically compressed, the remaining suppliers would gain very strong pricing power. This would not only further raise construction costs, but would also reduce the overall resilience of Europe's critical infrastructure in the face of unknown cyber threats because of the loss of technological diversity.

Chapter Summary: Heterogeneous Pressure Highlights the Compliance Gap, While Asymmetric Costs Undermine the Stability of the Single Market

The current mandatory replacement provisions of CSA2 completely disregard the major heterogeneity among member states in industrial structure, fiscal flexibility, and the pace of digital and green transition. This asymmetric economic burden would not only fail to achieve the intended security objectives, but would instead create severe economic pain within member states, intensify political fragmentation, and ultimately weaken the overall competitiveness of the EU single market.

07

CCCEU Position and Core Recommendations: Safeguarding Bilateral Mutual Trust and Returning to Technological Neutrality

Based on our systematic assessment of 18 sectors and 27 EU member states, we have quantified the enormous economic losses that implementation of the CSA2 proposal could trigger. This is not only a matter of financial cost, but also a matter of legal principle. The exclusion policy contemplated by the proposal departs from the principles of proportionality, non-discrimination, and lawful protection of property rights, creating a severe imbalance between the socioeconomic sacrifice it would impose and the unproven “security gains” it purports to deliver.

7.1 Key Points of Focus

The mandatory exclusion policy in the CSA2 proposal is a politicized, non-objective, and discriminatory measure that turns security into protectionism and seriously undermines the stability of European industry and supply chains. The CCCEU firmly opposes such excessive intervention and calls for a return to a technology-neutral and evidence-based regulatory path, using dialogue to build a governance framework that values both security and development.

The enduring way to sustain economic and trade exchanges lies in cherishing bilateral mutual trust and honoring the original commitment to cooperation. Only by upholding the essence of technological neutrality and rejecting interference from non-technical factors such as geopolitics can the foundations for healthy economic development be strengthened.

7.2 The CCCEU Position on the Proposed Amendments to the EU Cybersecurity Act (CSA2)

7.2.1 The CCCEU Recognizes the Importance of EU Cybersecurity and the Protection of Critical Infrastructure. However, It Expresses Grave Concern and Firm Opposition to the CSA2 Proposal''s Introduction of Non-Technical Criteria, as Well as Mandatory, Universal, and Time-Bound Exclusion Measures for Enterprises.

This one-size-fits-all approach would not only disrupt normal market order and significantly raise corporate compliance costs, but would also have profound negative implications for Europe's dual digital and green transition, industrial competitiveness, and China–EU economic and trade relations.

Security is not the opposite of efficiency. By establishing unified security standards that are auditable, verifiable, and broadly applicable, the EU can not only preserve its fiscal buffer space and guide orderly industrial and technological development, but also protect society and the public interest. Only by returning to rational governance and upholding technological neutrality, fairness, and openness can the EU safeguard stability and sustainable development and preserve its strategic position in global competition.

7.2.2 The CCCEU Is Deeply Concerned About the Assessment Mechanism in CSA2 for Third Countries Posing Cybersecurity Concerns: In Practice, This Mechanism Displays the Characteristics of Political Screening Rather Than a Framework Based Entirely on Security Considerations

CSA2 authorizes the European Commission, on the basis of cybersecurity risk assessment, to designate any third country as a third country posing cybersecurity risks. Article 100 of CSA2 sets out the criteria for identifying such countries by relying on vague non-technical factors such as the third country's legal system, governance model, and political environment, as well as unspecified "conclusive information regarding threat actors," without providing clear standards or empirical evidence of actual risks to the EU ICT supply chain.

In the absence of objective technical grounds, linking "trustworthiness" to country of origin and other non-technical factors is inherently discriminatory and violates the principles of equality and non-discrimination established in Articles 20 and 21 of the Charter of Fundamental Rights of the European Union. A non-technical assessment mechanism also leaves space for politicized decision-making and makes judgments vulnerable to external pressure or subjective interpretation. The CCCEU believes that cybersecurity should not be instrumentalized as a tool of trade protectionism, and that "de-risking" should not lead to "forced decoupling." The result of forced decoupling would be to damage the openness and competitiveness of the European market.

7.2.3 The CCCEU Opposes the Introduction of Mandatory and Time-Bound High-Risk Supplier Exclusion Measures Across Multiple Critical Sectors

Although presented in the name of "supply-chain de-risking," CSA2 carries the practical risk of institutionalizing and normalizing selective decoupling procedures targeted at non-EU suppliers, especially those from countries deemed to present "structural non-technical risks."

This mechanism is political in nature and broad in scope. Any supplier established in, or controlled by an entity from, a country designated as raising cybersecurity concerns may be classified as a "high-risk supplier" and face exclusion from the EU ICT supply chain, regardless of whether the technical security of its products has been verified. The designation applies horizontally across all sectors covered by the NIS2 Directive and does not set differentiated thresholds based on company size, turnover, or other objective criteria.

Although Article 105 of CSA2 establishes a theoretical exemption mechanism, its conditions reverse the burden of proof and are, in legal practice, almost impossible to satisfy—for example, by requiring proof that "no possible improper interference by any third-country state exists." This renders the right to be heard under Article 41(2) and the right to effective judicial protection under Article 47 of the Charter of Fundamental Rights largely formalistic, leaving suppliers without a substantive opportunity to defend themselves.

The final regulatory measures will be determined through implementing acts of the European Commission, which not only centralizes decision-making power to a high degree but also leaves substantial room for political discretion. This gives rise to concern that regulation may deviate from an objective and risk-based path and instead be influenced by broader geopolitical factors, while member states would have only limited influence over such decisions.

Moreover, the impact of CSA2's high-risk supplier measures would go beyond market access. Under Article 100(4), suppliers designated as high-risk would be excluded from European standardization processes, prohibited from obtaining EU cybersecurity certification, and stripped of eligibility to participate in public procurement and EU-funded programs. In the telecommunications field, such designation would also automatically prohibit the supplier from providing all relevant mobile and fixed-network telecom equipment, and already installed equipment would have to be phased out within the prescribed exit period.

In other words, these measures could evolve into de facto decoupling of the ICT supply chain and lead to fragmentation of industrial standards between the EU and major global partners such as China. The risk of fragmented industrial standards would increase costs for European enterprises, constrain their ability to access global innovation and R&D resources, and ultimately weaken Europe's level of digital development and industrial competitiveness.

The Chamber stresses that mandatory exclusion should not be conflated with "de-risking," because the former is, in essence, a government-led systemic exclusion carried out in the name of security. The CSA2 proposal infringes the fundamental EU rights enjoyed by suppliers designated as high-risk. These rights include the freedom to conduct a business (Article 16 of the Charter), the right to property (Article 17(1)), and the principles of equality and non-discrimination (Articles 20–21).

In addition, under Article 5(4) of the Treaty on European Union and Article 52(1) of the Charter of Fundamental Rights, any exclusionary measure must pass strict proportionality review, meaning that the security risk concerned must be shown to be real, present, and sufficiently serious, and that the relevant equipment and associated risks must be assessed concretely. Generalized determinations based only on suspicion or shaped by political factors, while disregarding technical reliability and evidence-based risk assessment, are unlikely to survive such proportionality review and may raise serious concerns regarding legality and fundamental rights. Security pursued at the cost of restricting technological choice and narrowing market openness is neither sustainable nor credible. Europe's competitiveness has long depended on open markets, fair competition, and deep integration into global value chains.

7.2.4 The CCCEU Reiterates That Cybersecurity Is, by Its Nature, a Competence Reserved to Member States Rather Than a Uniform EU-Level Power

National security is a competence reserved to the member states. Article 4(2) of the Treaty on European Union makes clear that national security remains the sole responsibility[49] of each member state.

CSA2 invokes Article 114 of the Treaty on the Functioning of the European Union (TFEU)—that is, "internal market harmonization"—as its legal basis. However, recourse to that provision is lawful only where differences in member-state rules create substantial obstacles to the internal market or lead to clear distortions of competition. In the present context, the different supply-chain measures adopted by member states reflect legitimate differences in their national security assessments and risk exposure and should not be treated as market fragmentation.

CSA2 blurs the boundary between market regulation and foreign policy. Its actual effect is to restrict the participation of suppliers from certain third countries in the EU market on security grounds. Traditionally, this falls within the EU's external trade and economic security policy, governed by Article 207 TFEU, rather than the internal-market coordination matters under Article 114 TFEU. The former[50] area of EU competence is subject to specific institutional safeguards, including member-state control and unanimity requirements.

7.2.5 By Introducing a "Country Designation Mechanism" into Internal-Market Legislation, CSA2 Risks Circumventing the "Constitutional Safeguards" Governing EU Foreign Policy and External Economic Measures. This May Constitute a Potential Misuse of Article 114 TFEU to Pursue Geopolitical Objectives Unrelated to Internal-Market Harmonization. The CCCEU Is Deeply Concerned About the Major Economic Impact and Systemic Trade Consequences of Such Exclusion Measures

In the fields of ICT and digital infrastructure, China–EU trade and industrial interdependence involves capital measured in the hundreds of billions. Forcibly excluding suppliers with whom cooperation has already been established would raise operating costs, reduce supplier diversity, delay network upgrades, and weaken Europe's innovation capacity and global competitiveness. The implementation of mandatory exclusion would inflict self-harming damage on Europe's digital and industrial foundations.

The telecommunications sector, including operators and industry associations, has already expressed serious concern about the proposed three-year time-limited exclusion policy for mobile-network equipment.

Operators[51] note that requiring tendering and replacement within 36 months for equipment supplied by vendors designated as "high-risk" is extremely aggressive. For a sector whose investment cycle typically extends to ten years and that lacks a sufficient European cost-compensation mechanism, such a requirement is detached from reality. According to telecom operators' estimates, the relevant replacement costs could reach EUR 60 billion. [52]

49. Bird & Bird, 'The CSA2's ICT Supply Chain Framework: Necessary Reform or Legal Overreach?'

50. EURACTIV, 'Cybersecurity revamp risks legal overreach and market fallout.'

51. EURACTIV / ANSA: https://www.ansa.it/europa/notizie/rubriche/altrenews/2026/02/04/ferraiuolo-con-cybersecurity-act-rischio-incertezza-per-investimenti_e7add232-4397-425a-b023-f934bf364413.html

52. Expansión, 'Banning Huawei in Europe: The Easier Decision to Make' - https://www.expansion.com/economia-digital/2026/02/19/6996d69ce5fdea7a148b45ab.html#google_vignette

Connect Europe has stated that the relevant measures must follow[53] the principle of proportionality and fully consider the need for predictability in network-infrastructure construction, whose modernization cycle is at least ten years. In addition, risk assessment should remain timely and should carefully weigh effects on investment, resilience, and service continuity. GSMA has similarly argued[54] that legislative measures concerning supply-chain security should be targeted, remain risk-based, and provide long-term predictability to affected industries on the basis of comprehensive impact assessment, thereby taking current operational realities into account while fully respecting the principle that matters of national security remain within the competence of EU member states.

In light of the major economic and operational pressure facing the telecommunications sector, the Chamber further emphasizes that the shift toward mandatory cross-sector exclusion policies has raised serious questions regarding proportionality, non-discrimination, and consistency with[55] World Trade Organization rules. Excessively broad application of "security exception" clauses, or exclusionary measures based on supplier "nationality" or "country of origin," risks undermining multilateral trade norms, splitting global supply chains, and provoking trade disputes.

7.2.6 The CCCEU Calls on EU Institutions to Stop Advancing Mandatory Exclusion Measures and Instead Uphold an Evidence-Based, Proportionate, and WTO-Consistent Cybersecurity Framework So as to Safeguard Europe's Competitiveness and Promote Inclusive Industry Dialogue

The CCCEU calls on the European Commission, the European Parliament, and EU member states to:

- Halt the promotion of mandatory exclusion measures;
- Maintain a technology-neutral, evidence-based, and proportionate regulatory approach in cybersecurity;
- Safeguard Europe's long-term competitiveness, innovation capacity, and digital leadership;
- Recognize and respect the exclusive competences of EU member states in the field of national security;
- Ensure full compliance with WTO rules and international trade commitments;
- Engage in meaningful and constructive dialogue with industry stakeholders, including both EU and non-EU enterprises.

We call on both China and the EU to carry out constructive dialogue on cybersecurity, industrial cooperation, and related issues; to properly manage differences in respective concerns; and, while effectively safeguarding cybersecurity, to uphold open cooperation, technological neutrality, and fair competition, thereby jointly maintaining the stability of global industrial and supply chains.

The CCCEU remains committed to constructive engagement and is willing to work closely with EU institutions to build a cybersecurity framework that safeguards cybersecurity without damaging competitiveness, openness, or Europe's position in the global digital economy.

53. Connect Europe, statement on the Cybersecurity Act - https://connecteurope.org/news/connect-europe-statement-cybersecurity-act

54. GSMA, statement on behalf of European mobile operators on the Cybersecurity Act proposal - https://www.gsma.com/about-us/regions/europe/news/gsma-statement-on-cybersecurity-act-proposals-on-behalf-of-european-mobile-operators/

55. EURACTIV, 'Brussels' proposed cybersecurity overhaul risks constitutional red flags

7.2.7 The CCCEU Calls on EU Institutions to Bring ICT Supply-Chain Security Governance Back to International Standards and Industry Best Practices

In the era of Globalization 2.0, supply-chain security governance should not become a “political filter,” but should instead adopt international standards and industry best practices. At its core, the system is evolving from the earlier free-market division of labor centered on “efficiency and cost optimization” toward a cooperative division of labor that balances security, resilience, and diversification. Supply-chain security governance therefore requires “shared responsibility” among all stakeholders, with each link in the chain requiring risk management and mitigation measures. It covers multiple dimensions, including risk management, information security, business continuity, quality control, and compliance, and involves international standards such as: (1) risk management: the ISO 31000 series; (2) supply-chain security management systems: the ISO 28000 series; (3) information security: the ISO 27001 series; (4) business continuity: the ISO 22301 series; (5) quality control: ISO 9001; and (6) supplier relationship management: the ISO/IEC 27036 series, among others.

For example,

- BMW Group’s all-electric BMW iX3 is manufactured at the company's production base in Shenyang, China, and exported to overseas markets including Europe. According to BMW Group, the iX3 was its first model produced in a Chinese plant for export to global markets. Subsequent updated versions have continued this "made in China, delivered globally” arrangement and entered the EU market in the autumn of 2021. China's role in the current global automotive supply chain has long gone beyond that of a single local manufacturing base; it has become an integral part of how multinational companies coordinate R&D, manufacturing, and market delivery. For such highly integrated supply chain networks, any source based simplification restrictions could spill over to the production organization, cost control and market responsiveness of European companies themselves. [56]

- A Tesla Model 3 contains approximately 10,000 individual parts, ranging from the smallest screws and washers to major battery packs, body panels, motors, and electronic control components. Its supply chain spans multiple regions around the world. In such a system, supply-chain security does not depend on control within a single geography, but on a model of “shared responsibility” and the effective joint management of supply-chain security by all stakeholders under international ISO standards. Supported by globally accepted standards and the company’s own governance mechanisms, Tesla coordinates a highly complex global supply chain through its global Gigafactory system. For example, Tesla’s Shanghai Gigafactory produced its three-millionth vehicle in October 2024 and exported its one-millionth vehicle in September 2024, while its China supply-chain localization rate reached 95% .

- The latest Apple smartphones contain approximately 2,700 components. Based on a “shared responsibility” model, international ISO standards, and Apple’s Supplier Code of Conduct, Apple works with all stakeholders to manage supply-chain security effectively. Apple relies on global supply-chain management, with design in California and components manufactured around the world. Globally, 86% of its iPhone assembly is done in China, where 157 supplier of core components have factories. [58]

Accordingly, in the era of Globalization 2.0, supply-chain security governance should not become a “political filter.” Instead, true security should be achieved through joint action, shared responsibility, international standards, and industry best practices.

56.https://www.press.bmwgroup.com/global/article/detail/T0310696EN/the-first-ever-bmw-ix3?language=en

57. https://digitalassets.tesla.com/tesla-contents/image/upload/IR/TSLA-Q3-2024-Update.pdf https://www.iisd.org/system/files/2024-11/electric-vehicle-battery-production-india.pdf

58. https://www.apple.com/sg/supply-chain/ Apple Supplier Code of Conduct https://s203.q4cdn.com/367071867/files/doc_downloads/2024/04/Supplier-Code-of-Conduct-and-Supplier-Responsibility-Standards.pdf

Chapter Summary: Technological Neutrality Is the Key to Breaking the Deadlock; Mutual Trust and Cooperation Should Replace Discriminatory Exclusion

The core appeal of the CCCEU is that the relevant provisions of the CSA2 proposal must not become instruments of geopolitical rivalry or trade barriers, and that technological neutrality is the key principle for resolving the current impasse in cooperation.

The EU is urged to return to a governance paradigm centered on “capability verification.” Through multi-party audits, source-code escrow, and performance monitoring, a solid security defense should be built. Technology should be allowed to return to its original value: improving productivity, driving innovation, and enhancing social welfare. Only such an open approach to governance can enable Europe to safeguard its security baseline without sacrificing efficiency.

Only by recognizing industry concerns, adhering to the technological essence, and strengthening the foundation of mutual trust can barriers to cooperation be removed and bilateral technological and economic cooperation return to a healthy path of development. This is both an urgent need for industry and a necessary requirement for the steady and sustained development of bilateral relations.

Conclusion:

Safeguarding Openness with Mutual Trust, and Advancing Prosperity Through Rationality

China–EU economic and trade cooperation concerns not only the growth momentum of both sides, but is also an important pillar for maintaining the stability of global industrial and supply chains, promoting the broad-based diffusion of technology, and building an open world economy. Over the long term, the deep cooperation between the two sides in economic, trade, and technological fields has gone beyond simple commercial exchange and has become one of the core driving forces sustaining stable investment relations and promoting regional and global economic development.

Against the backdrop of intertwined digitalization and globalization, genuine security should not stem from physical isolation, but from sound governance systems and unified technical standards. If the EU insists on sacrificing economic efficiency in pursuit of a static and exclusive sense of security, the result may be a closed system that is costly, slow to iterate, and lacking in vitality. Unilateral restrictive measures will inevitably trigger market responses, in turn causing digital contraction. Such isolation would not only fail to guarantee security, but might instead induce systemic risk through declining economic competitiveness.

As stated in the Executive Summary of this report, cybersecurity should be built on technical evidence and scientific governance, not on isolation based on geopolitical attributes. If the CSA2 proposal continues to use “source of supply” as a market-access criterion, Europe may face substantial economic costs and delayed transformation:

Mandatory supplier replacement is projected to generate economic losses of EUR 367.8 billion. These costs would be transformed into inflationary pressure and fiscal burdens ultimately borne by European consumers and taxpayers. Sacrificing efficiency in pursuit of merely formal compliance may leave Europe's digital ecosystem isolated and weaken its global competitiveness.

From industrial logic to the broader public interest, the essential value of technology lies in openness, sharing, and inclusive development. Politicizing technical issues or artificially severing bilateral ties of cooperation violates market principles and does not contribute to the long-term development of any party.

The CCCEU calls on EU institutions to address the real concerns of industry, resolve regulatory differences through pragmatic action, and build through inclusive dialogue a cybersecurity framework that balances security and openness.

The Chamber calls for a return to a governance paradigm centered on “capability verification,” establishing an objective and transparent security defense system through multi-party audits, source-code escrow, and real-time performance monitoring.

Only by returning to the original value of technology—improving efficiency and driving innovation—and by adopting an open view of governance can Europe effectively safeguard its security baseline without sacrificing efficiency.

Only by respecting the objective laws of the market, adhering to technological neutrality, and strengthening the foundation of mutual trust can barriers to cooperation be removed and China–EU economic, trade, and technological cooperation return to a healthy track.

The CCCEU stands ready stands ready to work with all stakeholders to promote the steady and sustained development of China–EU economic and trade relations.