KINSTELLAR

THE EUROPEAN CYBERSECURITY REFORM

(CSA2)

OVERVIEW AND CRITICAL ANALYSIS

EXECUTIVE SUMMARY

The European Cybersecurity Reform (CSA2)

What it is and why it matters?

Will the increase of central cybersecurity resilience result in conflicts with national laws?

The European Commission's proposal for a Cybersecurity Act 2.0 ("**CSA2**") represents one of the most consequential regulatory restructurings of the EU's digital governance framework since the adoption of the original Cybersecurity Act (Regulation (EU) 2019/881). Presented as a response to accelerated geopolitical tensions, industrial-scale cybercrime, and systemic vulnerabilities in global ICT supply chains, the CSA2 Proposal seeks to centralise critical cybersecurity competences at the EU level, expand ENISA's mandate, and introduce a harmonised framework for assessing "non-technical risks" associated with third-country suppliers.

While the stated objective is to reinforce the EU's digital resilience and reduce fragmentation, CSA2, in its current form, constitutes a structural shift far beyond technical harmonisation. By embedding security-driven supplier exclusion mechanisms into an internal-market instrument relying on Article 114 TFEU, the Proposal effectively reassigns core national-security prerogatives – traditionally protected under Article 4(2) TEU – to the European Commission. This creates a constitutional, regulatory, and institutional tension at the heart of the EU's legal order, raising serious questions regarding respect for Member States' sovereignty, proportionality, the rule of law, and the adequacy of legislative safeguards for intrusive security measures.

At the regulatory level, the CSA2 Proposal introduces a framework for identifying "third countries posing serious and structural non-technical risks" and designating associated manufacturers as high-risk vendors (HRVs). Once listed, such vendors would be automatically excluded from EU funding, EU cybersecurity certification schemes, and public procurement procedures, and would be subject to mandatory phase-out obligations – most notably the 36-month "rip-and-replace" mandate for 5G and other critical ICT network components. These measures are legally and economically impactful, fundamentally altering competitive conditions in the Digital Single Market.

The Commission's Impact Assessment estimates that the mandatory removal and replacement of HRV-linked infrastructure could impose €3.4- €4.3 billion annually in costs on mobile network operators, diverting capital from innovation and the deployment of 5G Advanced and 6G networks. This raises broader concerns about Europe's global competitiveness, supplier concentration, and the risks of technological oligopolies forming around a limited pool of politically endorsed manufacturers.

Furthermore, CSA2 risks creating de facto sanctions without the procedural and substantive safeguards prescribed by the Common Foreign and Security Policy (CFSP) framework under Articles 24 and 29 TEU, and without the unanimity requirement that protects Member States' sovereign discretion. The use of implementing acts to adopt HRV lists bypasses these safeguards and may be challenged as incompatible with the treaties' allocation of competences.

EXECUTIVE SUMMARY

Additionally, by requiring Member States to share sensitive, potentially classified information on supply-chain dependencies and vendor assessments with EU institutions, the Proposal may conflict with national secrecy laws and intelligence-handling protocols – especially in Member States with strict protection regimes.

CSA2 further raises significant concerns under the principles of legal certainty, legitimate expectations, and protection of property, given that operators may be compelled to dismantle infrastructure lawfully acquired and deployed under previous regulatory regimes, without a clear compensation mechanism. The pending CJEU case C-354/24 (*Elisa Eesti*) underscores that even non-expropriatory limitations may require "reasonable compensation" when they impose exceptionally heavy burdens – a threshold easily met by the structural financial impacts anticipated under CSA2.

For Member States such as Croatia and Hungary, the Proposal presents additional constitutional and economic risks. In both countries CSA2 may conflict with core constitutional guarantees concerning national security sovereignty, the rule of law, property rights, and freedom of entrepreneurship. In addition, CSA2 threatens to marginalise specialised national authorities, disrupt sector-specific certification regimes, conflict with public pxrocurement law, and undermine constitutional protections for property and proportionality under Member States' constitutions.

Overall, while the objective of enhancing Europe's cybersecurity resilience is both legitimate and urgent, CSA2 – in its current form – appears to exceed what may be justified under an internal-market legal basis and risks eroding fundamental constitutional safeguards and economic freedoms. In its current draft form, the Proposal requires substantial amendment to ensure compliance with EU acquis communautaire, respect for the balance of competences, and adherence to essential rule-of-law principles.

Tímea Bana
Partner, Head of the local Technology service line

+36 1 428 4411
timea.bana@kinstellar.com

Kinstellar at a glance

Kinstellar is a leading independent law firm in Central and Southeastern Europe, and Central Asia.

Operating as a single fully integrated firm, Kinstellar delivers consistently high quality services across all jurisdictions in an integrated and seamless style. We are particularly well suited to servicing complex transactions and advisory requirements spanning several jurisdictions.

17 years

300+ lawyers

200+ rankings

13 offices

11,000+ clients

∞ solutions

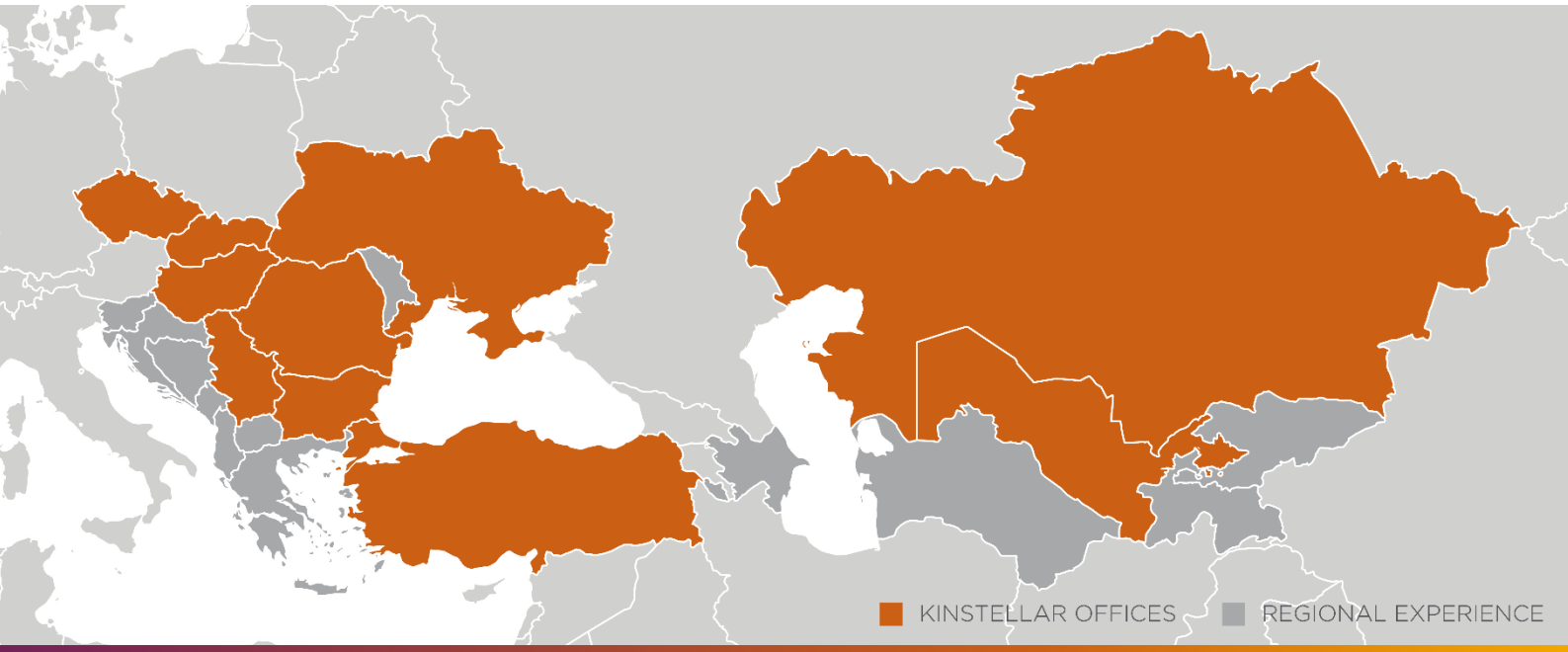


Table of contents

PART I.

The legacy of the 2019 Cybersecurity Act and the drivers of reform

The Cybersecurity Act (**Regulation (EU) 2019/881**) established the foundational architecture for cybersecurity governance within the European Union. It provided **ENISA** with a permanent mandate and created the European Cybersecurity Certification Framework (**ECCF**). At the time, the Act reflected a balanced compromise between strengthening the internal market and respecting Member State competences – particularly in areas touching upon national security.

However, the landscape in which the EU now operates has changed fundamentally. A series of geopolitical disruptions, rapid escalation in state-sponsored cyber operations, the industrialisation of cybercrime, and heightened exposure to global supply-chain vulnerabilities have collectively reshaped the contours of cybersecurity policymaking. The emergence of concentrated chokepoints in ICT supply chains and the increasing strategic importance of digital infrastructure have contributed to renewed pressure on the EU to create a more interventionist, centrally coordinated framework.

Against this backdrop, the Commission introduced the Cybersecurity Act 2.0 ("**CSA2**"), framing it as a necessary evolution of the 2019 regime. While the overarching narrative emphasises resilience and harmonisation, the CSA2 Proposal marks a paradigm shift: it expands the EU's role from regulator of the internal market to a quasi-security authority capable of excluding suppliers based on "non-technical risks" associated with their jurisdiction of origin.

This transition raises fundamental questions about its compatibility with the constitutional balance of competences under the Treaties, the primacy of Member State discretion in national security, and the proportionality of EU-level interventions.

Why this white paper now?

The EU has reached a critical inflection point in its digital transformation. The Commission's pursuit of a more centralised "Cybersecurity Shield" appears to be motivated by legitimate concerns relating to cybersecurity preparedness, but it also risks creating a model that over-extends the internal-market legal basis (Article 114 TFEU) to regulate matters that are, in substance, national-security decisions.

The Proposal purports to deliver economic efficiencies by reducing fragmentation and streamlining certification, promising administrative cost savings and greater legal coherence. Yet these anticipated benefits must be weighed against the significant economic dislocation that could result from Europe's technological decoupling from certain global suppliers, diminished competition, and forced replacement of existing infrastructure.

In this context, this white paper aims to:

- provide a detailed, critical assessment of the CSA2 Proposal,
- identify legal risks, and
- contribute to an informed debate regarding the proportionality, legality, and sustainability of the proposed reforms.

Shifting geopolitical realities and the rise of hybrid threats

The Proposal is framed as a response to an era in which cyber operations increasingly intersect with geopolitical confrontation. The Commission cites intensified hybrid threats, cross-border espionage, and strategic manipulation of ICT supply chains as justification for more intrusive oversight mechanisms.

While these concerns are legitimate, CSA2 signals a shift away from technical risk assessments – which have traditionally formed the basis of cybersecurity certification – towards potentially politicised determinations grounded in a supplier's country of establishment, its legal environment, perceived alignment with international norms, and the behaviour of its home state in cyberspace.

This recalibration may create regulatory uncertainty for operators and investors, as the criteria are inherently subjective and could evolve with shifting geopolitical dynamics. For European enterprises dependent on long-term planning and stable risk frameworks, the introduction of such uncertainties poses material commercial and legal risks.

The architecture of the reform: four operational pillars

The CSA2 Proposal rests upon four operational pillars that together reconfigure the EU's cybersecurity governance model:

1. Strengthening ENISA's operational mandate

ENISA would evolve from an advisory body into an EU-level centre of operational expertise, with significant additional resources and responsibilities. This includes the management of a Cybersecurity Reserve, creation of a European vulnerability database, and development of technical specifications where market standards are lacking.

2. Simplification and expansion of the ECCF

The Proposal aims to streamline the existing certification regime by shifting towards entity-level assessments of "cyber posture", offering a presumption of conformity with NIS2 requirements. While this is intended to reduce bureaucracy, centralisation may introduce bottlenecks if new certification schemes cannot keep pace with rapid technological innovation.

3. Reduction of administrative burden and reporting fragmentation

Through initiatives such as the Single Reporting Platform and the Digital Omnibus, operators would be relieved of duplicative reporting obligations. Amendments to NIS2 would also exclude certain small providers (e.g. micro and small DNS entities) from its scope.

4. Creation of a trusted ICT supply chain security framework

The Proposal introduces a contentious pillar: a framework that enables the Commission to classify third countries as posing "serious and structural non-technical cybersecurity risks" and to designate specific companies as high-risk vendors. This mechanism carries immediate and far-reaching consequences for procurement, certification, funding eligibility, and ongoing infrastructure deployments.

The coherence, proportionality, and constitutional legitimacy of this fourth pillar form a central focus of this white paper.

Transformation of ENISA and the certification framework

ENISA's reinforced mandate

Under CSA2, ENISA's mandate would expand dramatically. The agency would receive substantial new funding and staff, effectively doubling its capacity. It would gain responsibilities such as:

- managing the EU Cybersecurity Reserve;
- maintaining a EU-wide vulnerability database;
- operating the Single Reporting Platform; and
- issuing technical specifications in the absence of adequate market standards.

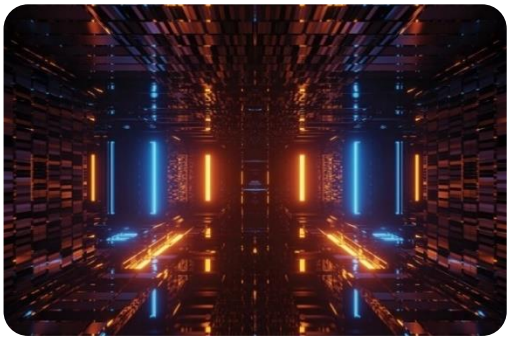
These powers would elevate ENISA from a supporting actor to a regulatory authority with quasi-executive functions – an evolution that raises complex questions concerning delegation of powers, democratic accountability, and institutional balance.

Entity-level certification and "cyber posture"

The ECCF would no longer limit itself to product or service certifications. Instead, it would incorporate holistic, organisation-level certification schemes assessing continuous compliance with EU law. Entities holding such certificates would benefit from a presumption of conformity with NIS2 obligations.

Although this ambition aligns with the goal of harmonisation, it also risks creating administrative congestion if ENISA becomes a centralised bottleneck for certifying large numbers of organisations across the EU.

While the addition of 118 FTE positions is intended to increase efficiency, it raises the possibility that this centralisation could lead to administrative bottlenecks if the ECCF's complex certification procedures fail to keep pace with market innovation. Furthermore, there are concerns that despite the promise of simplification, the multi-layered governance involving ENISA, the Commission, and the ECCF could result in unpredictable timelines for the adoption of new schemes.



The "Trojan horse": The ICT supply chain security framework

The most far-reaching, and arguably most sensitive, component of the CSA2 Proposal is the introduction of a Trusted ICT Supply Chain Security Framework. While presented as a natural extension of the EU's cybersecurity architecture, the framework constitutes an unprecedented expansion of EU-level control over the technological inputs used in critical infrastructure.

Crucially, the Proposal transforms what were traditionally technical, evidence-based security assessments into geopolitically informed determinations, grounded in evaluations of a third country's legal system, political behaviour, intelligence practices, and institutional safeguards.

This section analyses the legal, economic, and constitutional implications of this framework, with particular emphasis on its impact on Member State sovereignty, market functioning, and rule-of-law standards.

The CSA2 Proposal (COM (2026) 11) introduces, for the first time in EU law, a horizontal ICT supply-chain security framework centred on the assessment of non-technical risks posed by suppliers from third countries. This represents a profound expansion of EU-level discretion over the technologies permitted in critical infrastructure sectors.

Although framed as an internal-market harmonisation measure under Article 114 TFEU, this mechanism functionally resembles a centralised national-security screening regime, enabling the Commission to exclude suppliers and mandate the removal of installed equipment via implementing acts. Legal and policy analyses, describe this as one of the most far-reaching and controversial elements of CSA2.

a) Non-technical risks

The CSA2 Proposal would introduce a fundamental regulatory shift by formalising "non-technical risk factors" as primary criteria for security assessments. Under this proposed framework, a supplier's status could be determined not only by technical resilience but by the legal and political environment of its jurisdiction of establishment.[1]

- The Commission would be mandated to verify threats based on "serious and structural non-technical cybersecurity risks" to ICT supply chains[2]. This assessment would include evaluating a third country's "irresponsible state behaviour in cyberspace", which may be identified through public statements made on behalf of the EU or its Member States.
- A key element of the risk assessment would be the existence of laws or practices in a third country requiring entities to "report information on software or hardware vulnerabilities to authorities" of that country prior to such vulnerabilities being publicly known or exploited[3].
- The evaluation process would explicitly incorporate information from "international organisations such as NATO", as well as public political statements and reports from Member States, extending the assessment beyond purely forensic or technical data.
- The framework would require the evaluation of the "absence of effective judicial remedies, and independent and democratic control mechanisms" within the third country to correct security concerns. By empowering the Commission to assess a third country's "willingness to cooperate" in addressing risks, the proposal would establish a subjective legal standard for market exclusion.
- As verification could be initiated based on "other sources" the Proposal might create a "black box" for operators. This lack of transparency regarding underlying intelligence data may undermine the principles of vendor neutrality and legal certainty within the EU's Internal Market.

b) Mechanism for identifying third-country "high-risk vendors" (HRV)

The Proposal would establish a multi-layered, top-down process to label and exclude specific manufacturers at the EU level.

- Coordinated supply chain reviews: Initiated by the Commission or a group of at least three Member States, the NIS Cooperation Group would conduct a EU-level coordinated security risk assessment of specific ICT supply chains.
- Country Designation: Through implementing acts, the Commission would formally designate third countries as posing "serious and structural non-technical risks" to EU ICT supply chains.
- The high-risk vendor list: Based on the country designation and an assessment of ownership and control, specific manufacturers would be labelled as high-risk vendors. This designation would trigger an immediate ban from public procurement, a denial of EU funding, and a prohibition on obtaining European cybersecurity certificates.[4]

[1] CSA2 Proposal, Recital (129)
[2] CSA2 Proposal, Article 100
[3] CSA2 Proposal, Recital (137)
[4] CSA2 Proposal, Article 100, Recital (140) (142)

c) Mandatory phase-out mechanisms: Mobile, fixed, and satellite networks

In Title IV, Chapter II, the CSA2 would introduce unprecedented mandates for the electronic communications sector that extend significantly beyond 5G infrastructure to include legacy mobile generations (3G,4G), fixed networks, and satellite networks, creating a comprehensive security perimeter for the entire electronic communications ecosystem.[5]

- The 36-month deadline: Mobile network operators would be required to remove and replace all ICT components from designated HRVs within a maximum of 36 months from the publication of the relevant high-risk supplier list.[6]

The Commission's own impact assessment indicates this "rip-and-replace" mandate could impose a cost of € 3.4 billion - € 4.3 billion annually on mobile network operators during the transition period.[7]

- However, industry leaders suggest that the Commission may be significantly underestimating the true cost of removal: Telefónica's CEO, Emilio Gayo warns that the aggressive three-year timeline for removing HRV equipment could cost European telecoms up to € 21.5 billion. Other analyses suggest that the total economic impact on the telecom sector alone could reach € 60 billion.[8]

This substantial diversion of capital would risk depleting investment in 5G Advanced and 6G innovation, potentially widening the connectivity gap between Europe and its global competitors, the US and China.

Critical observations: Legislative overreach and sovereignty

The CSA2 Proposal marks a departure from objective, technical cybersecurity assessment toward a politically charged model of "geopolitical risk evaluation." Recent scholarship (notably Tzanou & Vogiatzoglou, European Papers, 2025)[9] underscores that this shift would significantly centralize de facto national security decision-making at EU level, raising concerns of legislative overreach and a potential imbalance between Union and Member State competences.

The CSA2 Proposal's ICT supply-chain framework reaches far beyond traditional internal-market harmonisation. By empowering the Commission to designate third countries and suppliers as presenting "serious and structural non-technical risks", and by mandating EU-wide exclusion measures adopted through implementing acts, the Proposal introduces regulatory tools that closely resemble national-security determinations.

---

[5] CSA2 Proposal, Recital (156) (157)
[6] CSA2 Proposal, Article 110
[7] CSA2 Impact Assessment p86
[8] https://www.expansion.com/empresas/tecnologia/2026/01/22/69716747e5fdead8348b45a0.html
[9] M Tzanou and P Vogiatzoglou, 'National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach' in N Vavoula (ed), The Future of Digitalisation in EU Law Enforcement, European Papers, Vol. 10, No 3, 2025, pp. 803-836, doi: 10.15166/2499-8249/855.s

These competences, however, sit at the intersection of two Treaty provisions with fundamentally different constitutional logic:

- Article 114 TFEU, the internal-market harmonisation provision, traditionally used to eliminate regulatory divergences between Member States that hinder free movement or distort competition.
- Article 4(2) TEU, which explicitly reserves national security as the sole responsibility of each Member State.

The constitutional friction between these provisions forms the core of the legal challenges raised by CSA2.

a) The contested use of Article 114 TFEU

While the Commission relies on Article 114 TFEU (Internal Market harmonisation) as the legal basis, the mandatory designation of "high-risk vendors" (HRVs) directly intersects with national security prerogatives and competences reserved to Member States.

- Under Article 4(2) of the TEU, "national security remains the sole responsibility of each Member State".
- The CSA2 would empower the Commission to identify and exclude suppliers via implementing acts, effectively reallocating core security-related discretion to the Union – outside the procedural safeguards of the Common Foreign and Security Policy (CFSP) governance framework.
- This raises the legitimate concern that regulating private ICT supply chains becomes a "legal veil" for an expanded EU role in national security operations, creating a structural "tug-of-war" between EU-level harmonisation and Member State sovereignty.

b) "Hidden Sanctions": Bypassing the Common Foreign and Security Policy framework

The functional consequences of the CSA2 mechanisms – mandatory exclusion of suppliers and the compulsory phase-out of ICT equipment – constitute, in substance, restrictive measures that significantly impact third-country economic actors and their access to the EU market. According to the European Parliamentary Research Service (EPRS 2024)[10], such sectoral trade and investment restrictions are core elements of the EU's sanctions "toolkit" designed to influence foreign governments. Despite this, the Proposal appears to be avoiding the foreign-policy procedures designed for decisions with such strategic impact.

Under the EU Treaties, measures carrying this degree of foreign-policy significance must be adopted within the Common Foreign and Security Policy (CFSP) framework (Articles 24 and 29 TEU), with their economic implementation grounded in Article 215 TFEU. CFSP decisions require unanimity in the Council, which functions as an essential safeguard ensuring that each Member State retains ultimate control over its strategic dependencies and its national security posture.

The CSA2 Proposal may have foreign-policy significance for the following reasons:

- It empowers the Commission to identify certain third-country jurisdictions as "cybersecurity concerns" via implementing acts[11] and, on that basis, automatically classify suppliers from those countries as "high risk." This labelling is not merely technical, it sends a strategic political signal that particular non EU states may be regarded as sources of systemic cybersecurity risk, which can strain political dialogue, damage bilateral trust, and distort trade and technology policy negotiations with those countries.

[10] https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760416/EPRS_BRI(2024)760416_EN.pdf
[11] CSA2 Proposal p19

- Once a third country supplier is marked in this way, the CSA2 driven mandatory exclusion and phase out mechanisms transform the classification into precise, sanction like outcomes: restricted market access, reputational damage, and disruptions to critical technology supply chains. These could have an impact on the EU's external relations, including strategic partnerships, digital policy dialogues, and security cooperation frameworks, all of which fall squarely within the scope of the CFSP's objectives.

By embedding these sanction-like consequences within an Internal Market instrument based on Article 114 TFEU, the Commission effectively circumvents CFSP scrutiny, explicit political debate, the unanimity requirement and Member State veto in decisions that materially affect foreign-policy relations and national security. This shift not only undermines the institutional equilibrium but also deprives Member States of their sovereign autonomy in national security and critical-infrastructure – where their autonomy is expressly protected under Article 4(2) TEU.

c) Market distortion and the chilling effect

The shift from a technical to a politically driven risk assessment model imposes immediate strains on the Digital Single Market, well before any formal prohibitions crystallise.

The chilling effect

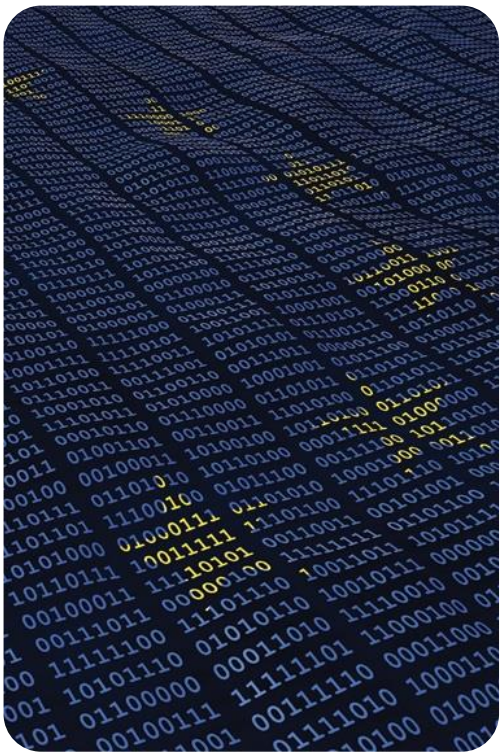
Even the mere prospect of being designated as a "high-risk vendor" deters operators from engaging with certain suppliers. The resulting uncertainty erodes market value and constrains investment, redirecting commercial decisions away from objective technical criteria and toward perceptions of political vulnerability. The mere possibility of a supplier being designated as a "high-risk vendor" or a third country being designated as a "country of concern" (Article 100) deters operators from engaging with those suppliers as a precautionary measure.

Emerging potential technological oligopoly

The compulsory exclusion of particular suppliers, risks consolidating the market around a narrow pool of "politically endorsed" actors. This concentration inflates costs for operators and creates new, and often more fragile, supply-chain dependencies – an outcome that undermines long-term resilience.

Contradiction with the EU's strategic objectives

- By artificially narrowing the market, the Proposal undermines the EU's "Strategic Autonomy". It would replace global competition with a technological oligopoly, eroding long-term resilience.
- As noted by GSMA and Connect Europe, extending phase-outs to all network layers – rather than focusing strictly on the sensitive core – surpasses what is proportionate for security. This broad approach would be an unjustified restriction on the Internal Market.
- Service Disruption: The forced, large-scale replacement of hardware poses a systemic risk to service continuity and availability across the EU, which is fundamentally at odds with the public interest.



NEXT STEPS

It is apparent that the Proposal, in its current form, fails to demonstrate that total exclusion is the least restrictive means to achieve its security goals, thereby inviting potential legal challenges under the general principles of EU law.

Nevertheless, the Proposal is only in its initial form. It is widely expected to be amended throughout the legislative process so that it can meet its original objectives while introducing a new structure consistent with the applicable legal principles of the EU acquis and the laws of the Members States.

PART II.

Impacts of the CSA2 Proposal on selected EU Members States

I. Croatia

II. Hungary

Croatia and cyberspace sovereignty – Legal and strategic risks

Part II of this white paper examines how the CSA2 Proposal conflicts with the Croatian legal system. The analysis is divided in sections to demonstrate that, in its current form, CSA2 represents a breach of Croatia's national security sovereignty as well as several core principles of Croatian constitutional law.

Erosion of national security sovereignty

It is important to note that EU regulations are above national law, i.e. the EU has primacy over national law. The principle of primacy ensures that individuals are uniformly protected under EU law across all Member States. However, the primacy of EU law only applies in areas where Member States have conferred competences on the EU – in fields such as the Single Market, the environment, transport, etc. – and it does not extend to areas such as education, culture, tourism, or national security.

As discussed above, the Treaty on European Union (hereinafter: TEU")[12], Article 4 paragraph 2 states that:

> The Union shall respect the equality of Member States before the Treaties, as well as their national identities, which are inseparably linked to their fundamental political and constitutional structures, including regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order, and safeguarding national security. **In particular, national security remains the sole responsibility of each Member State**.

From the Proposal, it is clear that CSA2 is aimed at ensuring security rather than harmonising the market, despite what is implied by the regulator. The CSA2 Proposal relies on Article 114 TFEU,[13] which gives rise to a well-recognised constitutional tension. If a measure's primary purpose is national security – such as preventing espionage, foreign interference, or strategic dependency – then grounding that measure under the Internal Market competence is fragile under the EU Treaties and places it in conflict with Croatian law.

For Croatia in particular, this represents a constitutional displacement. Decisions that under Croatian law fall within the purview of domestic authorities (e.g., the Ministry of Interior or the Regulatory Authority for Network Industries) become subordinated to uniform EU-level determinations.

[12] Treaty on European Union, OJ C 202, 7 June 2016.
[13] Treaty on the Functioning of the European Union, OJ C 202, 7 June 2016.

Once the Commission declares a third country a cybersecurity concern, Croatia cannot contradict or reinterpret that classification in accordance with its own security doctrine. This shift raises questions of constitutional proportionality, democratic accountability, and compatibility with Croatia's legal order, where national security competences are reserved to domestic authorities.

In other words, the authority of Croatian institutions will be effectively limited by a decision of the European Commission without valid legal grounds in EU law. Croatia is a sovereign state that has transferred only specific and limited competences to the EU. Any further encroachment on the authority of Croatian institutions may lead to an ungrounded limitation of Croatian sovereignty.

Additionally, the CSA2 Proposal (e.g. Articles 112 – 116) introduces mandatory obligations for Member States to share detailed information on supply-chain dependencies, ownership and control structures of suppliers, and findings from coordinated EU risk assessments with ENISA. This includes material that Croatia normally treats as confidential or classified, creating potential friction with national security protections.

Croatia's Classified Information Act, domestic intelligence-handling rules, and strict procedures governing classified procurement are built on the principle of restricted access and controlled dissemination. Under Croatian law, sensitive security assessments – particularly those derived from national intelligence authorities – may not be disclosed to external entities without proper authorisation. CSA2, however, requires Member States to supply such information to supranational bodies for the purpose of EU-wide vendor assessments and enforcement actions. As a result, Croatian authorities may face situations where EU obligations to provide intel-linked supply-chain information conflict directly with national secrecy laws or with international intelligence sharing restrictions that prohibit onward transmission of classified material.

In light of the above, CSA2 in its current form represents a clear erosion of Croatian national security sovereignty contrary to applicable EU and Croatian law.

Current form of CSA2 represents a breach of fundamental principles of Croatian legal system and rule of law

In addition to representing a clear breach of Croatian national security sovereignty, CSA2 also violates fundamental principles of Croatian (and EU) law – most notably the rule of law, including prohibitions on retroactive effect and the requirement of legal certainty.

The Venice Commission of the Council of Europe determined key aspects of the rule of law,[14] one of which is legal certainty. The principle of legal certainty is essential for maintaining confidence in the judicial and legal systems of each Member State. It is also crucial to establish conditions for productive business arrangements, which in turn support development and economic progress. To achieve this confidence, the state (including the EU) must make the text of the law easily accessible. It also has a duty to respect and apply, in a foreseeable and consistent manner, the laws it has enacted. Foreseeability requires that the law, where possible, be proclaimed in advance of its implementation and be predictable as to its effects; it must be formulated with sufficient precision to enable individuals to regulate their conduct. Legal certainty requires that legal rules be clear and precise and that they ensure situations and legal relationships remain foreseeable.[15]

Retroactivity goes against the principle of legal certainty in civil and administrative law insofar as it negatively affects rights or legal interests. Legal certainty also requires that undertakings or assurances made by the state to individuals should, in general, be honoured (the notion of "legitimate expectation").[16]

---

[14] Report on the Rule of Law, European Commission for Democracy through Law (Venice Commission) 86th plenary session (Venice, 25–26 March 2011), Study 512/2009, CDL-AD(2011)003rev. Strasbourg, 4 April 2011.
[15] Ibid, page 10.
[16] Ibid, page 11.

The above is also a fundamental principle of Croatian Constitution. [17] Article 3 of the Constitution identifies the rule of law as one of the highest constitutional principles. Furthermore, Article 90 provides that laws and other regulations adopted by state authorities and bodies vested with public powers may not have retroactive effect. Only in particularly justified cases may individual provisions of a law be given retroactive effect.

The CSA2 Proposal introduces obligations that operate retroactively in effect, even if not expressly retroactive in form. For example, CSA2 mandates that Member States and providers of mobile, fixed, and satellite electronic communications networks remove already installed equipment supplied by entities later designated as high risk vendors and imposes fixed deadlines without distinguishing between legacy systems lawfully procured under previous regimes. This compels said providers to reorganise networks, modify infrastructure, or terminate vendor relationships based on classifications that did not exist when the original investment decisions were made. Such measures undermine legitimate expectations and legal certainty, placing operators and public bodies in a disadvantaged position.

Furthermore, the CSA2 Proposal empowers the European Commission to expand prohibitions and redefine key ICT assets at any time, which means that operators cannot reliably predict which technologies or suppliers may become prohibited in the future. This creates an unstable legal environment, where the scope of obligations may change abruptly and without foreseeability. This is contrary to the Croatian constitutional rule that laws and regulations may not have retroactive effect, except in narrowly justified situations and only for specific provisions. Retroactive effect measures in CSA2 are neither narrowly tailored nor time limited. The combination of mandatory removal of previously lawful equipment and the ongoing risk of new prohibitions raises a credible argument that the CSA2 Proposal conflicts with fundamental rule of law principles, especially legal certainty, predictability of legal order, and protection of legitimate expectations.

The CSA2 Proposal additionally undermines the constitutional principle of legal certainty because it creates a regulatory environment in which operators and public authorities cannot reliably anticipate the scope, stability, or future application of their legal obligations. The Regulation grants the European Commission broad discretionary powers to expand prohibitions, redefine key ICT assets, and introduce new restrictions at any time, without clear criteria or predictable limits. As a result, Croatian operators are unable to foresee which suppliers, technologies, or business models may become restricted in the future, making long term planning, investment decisions, and contractual commitments precarious. This lack of foreseeability conflicts with the requirements articulated by the Venice Commission and embedded in Article 3 of the Croatian Constitution, which require that legal rules be clear, accessible, and sufficiently precise to allow individuals and companies to regulate their conduct with confidence.

By allowing sudden and far reaching regulatory shifts, CSA2 disrupts the stability of legal relationships and undermines legitimate expectations, thereby violating the essence of legal certainty as a core principle of both Croatian and EU constitutional orders.

In light of the above, it is clear that CSA2 in its current form is contrary to the core principle of rule of law guaranteed by Croatian (and EU) law.

[17] Constitution of Republic of Croatia, "Official gazette" br. 56/90., 135/97., 8/98., 113/00., 124/00., 28/01., 41/01., 76/10., 55/01., 5/14., 85/10.).

CSA2 impact on freedom of entrepreneurship and free market – Croatian constitutional law perspective

From the standpoint of Croatian constitutional law, the CSA2 framework raises serious concerns regarding both the freedom of entrepreneurship and the freedom of market and competition. Under Articles 49 and 50 of the Croatian Constitution, economic freedoms may be restricted only by law, and only where the restriction is proportionate and for the protection of the interests and security of the Republic of Croatia, nature, the human environment, and human health. CSA2, however, introduces directly applicable, supranational prohibitions that override Croatian discretion and impose supplier bans derived not from Croatian economic regulation or Croatian security assessments, but from EU level geopolitical and non technical classifications.

In Croatian constitutional doctrine, when a public authority has several legally available means to achieve a desired objective, it must choose the means that is most favourable to the party in the procedure. Because the option preferred by the regulator is not always the one that results in the least interference with the party's rights, the courts have strengthened the proportionality principle by interpreting it to mean that, among several equally effective measures, the one with the mildest impact on the restriction of the party's rights must be used. The same principle applies to the adoption of laws and regulations.

On the other hand, CSA2's bans are blanket prohibitions, triggered regardless of whether Croatian authorities have independently identified a threat. The prohibition is not tied to Croatian security information, and domestic institutions are prevented from adapting or mitigating the measure based on local circumstances. The Impact Assessment published alongside the CSA2 Proposal[18] confirms that these restrictions will impose extremely high compliance and transition costs (e.g., EUR 3.4 billion–EUR 4.3 billion annually for mobile network operators during the phase out), illustrating that the constraints imposed on Croatian businesses are far reaching and structurally reshape the domestic market. The available Impact Assessment provides only a conservative baseline and substantially understates the real financial and operational impact. Public estimates already point to significantly higher figures. For example, Telefónica's CEO warned that the current proposal could force the removal of all Chinese equipment within three years, costing European operators around EUR 21.5 billion, while broader assessments put the total economic impact at up to EUR 60 billion. When compared with these figures, the projected EUR 3.4 billion–EUR 4.3 billion in annual phase-out costs cited in the Impact Assessment appears understated, given the scale of network integration and the complexity of replacing core infrastructure. As a result, the actual pressure on Croatian and wider European operators is likely to be far more substantial than what the initial analysis suggests.

From a constitutional perspective, when a measure so heavily restricts entrepreneurial freedom and imposes foreseeable economic burdens without space for national tailoring or proportionality balancing, it becomes vulnerable to challenge as an overly broad and insufficiently justified intrusion into a constitutionally protected domain.

Beyond individual entrepreneurial freedom, CSA2 also affects the constitutionally protected principles of free market competition. The Croatian constitutional order presumes a market economy based on competition, openness, equal treatment of market participants, and freedom of investment. CSA2, however, mandates the exclusion of entire classes of suppliers not on the basis of their market behaviour, technical performance, or compliance standards – but on EU level political and risk-based classifications.

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

This significantly alters competitive conditions by reducing the number of available vendors, narrowing technology choices, affecting pricing and incentives for innovation, and potentially disadvantaging Croatian subsidiaries of companies from third countries, who may be excluded from procurement solely due to their ownership structure. These concerns extend directly into the domain of foreign direct investment (FDI): Croatia relies on foreign capital – particularly in the ICT and high tech sectors – to support infrastructure development, innovation, and economic growth. By disqualifying or discouraging companies linked to designated third countries, CSA2 could deter future foreign investment, destabilise existing investor expectations, and reduce Croatia's attractiveness as an open and predictable investment destination. The Impact Assessment reinforces this risk by acknowledging that the regulatory package seeks to "enhance competitive equality" by eliminating fragmentation, yet it achieves this not through fostering fair competition but through removing certain competitors from the market altogether, thereby reshaping Croatia's competitive landscape and potentially dampening legitimate foreign investment. In this sense, CSA2 poses a broader constitutional and economic challenge: it restricts competition and investment freedom in ways that Croatia's constitutional framework does not permit without a clear, proportionate, and nationally grounded justification.

CSA2 also raises significant concerns in the area of public procurement. By mandating the exclusion of suppliers designated at the EU level as "high risk," CSA2 effectively prevents Croatian contracting authorities from independently assessing vendor suitability based on Croatian security criteria, technical merit, price, or best value considerations. Instead, procurement decisions become predetermined by supranational classifications grounded in geopolitical or ownership based assessments rather than objective market performance.

In conclusion, Article 49 of the Croatian Constitution guarantees that rights acquired through the investment of capital may not be diminished by law or by any other legal act. From the viewpoint of Croatian constitutional law, CSA2 in its current form represents a clear breach of the regulations of Croatian Constitution guaranteeing entrepreneurship, freedom of market, and competition.

CSA2 represents a breach of property rights guaranteed by Croatian Constitution

The *Elisa Eesti* case is directly relevant for assessing the constitutionality of CSA2 in Croatia, as it addresses whether the forced removal of already installed 2G, 3G, 4G, and 5G telecommunications equipment – lawfully purchased and deployed – constitutes a restriction on use or a deprivation of property. In her opinion, [19] Advocate General Ćapeta concluded that the courts must still determine whether the accelerated phase out of equipment crosses the threshold into a compensable taking.

First and foremost, Article 48 of the Croatian Constitution guarantees the right of ownership, while Article 50 explicitly provides that ownership may be limited or expropriated only in the interest of the Republic of Croatia, and even then, solely with compensation equal to the market value paid to the affected owner. This constitutional framework reveals two central points of tension between the CSA2 and Croatian constitutional guarantees.

Firstly, CSA2 introduces obligations that amount to a serious interference with ownership rights, including the mandatory removal of previously lawful and economically valuable equipment, which in substance represents a clear encroachment upon constitutionally protected property. Secondly, even if one were to accept that such limitations are permissible, they can be legitimate only when adopted for purposes that qualify as being "in the interest of the Republic of Croatia" and only when accompanied by market value compensation. Yet, in its current form, and considering the Opinion of Advocate General Ćapeta in the *Elisa Eesti* case – which recognises that burdens may become disproportionately heavy – CSA2 empowers EU institutions to restrict or effectively deprive Croatian entities of property without a clear obligation to provide market value remuneration.

[19] https://infocuria.curia.europa.eu/tabs/document/C/2024/C-0354-24-00000000RP-01-P-01/CONCL/317929-EN-1-html

This creates a direct constitutional inconsistency: CSA2 allows EU level authorities to impose intrusive property restrictions on Croatian operators for EU level policy objectives, without respecting the compensation requirements that the Croatian Constitution demands for far less intrusive national measures. All this occurs without Croatian institutions having a final say and without a clearly defined national interest of the Republic of Croatia.

Therefore, CSA2 in its current form represents a clear breach of the Croatian Constitution's guarantee of ownership.

SUMMARY & RECOMMENDATIONS

Taken together, the four identified issues show that CSA2, in its current form, raises serious constitutional concerns for the Republic of Croatia, both under Croatian constitutional law and the fundamental principles of EU law. Firstly, CSA2 introduces a significant erosion of Croatian national security sovereignty, as it reallocates core security assessment powers from Croatian authorities to the European Commission. This contradicts Article 4(2) TEU, which reserves national security exclusively to Member States. CSA2 obliges Croatia to accept EU level determinations of which third countries and suppliers pose cybersecurity risks and to share classified or sensitive information with EU institutions, despite strict Croatian rules on secrecy, classified procurement, and intelligence handling. This results in a structural displacement of Croatian sovereign powers and may amount to an unjustified intrusion into a domain that Croatia never transferred to the EU.

CSA2 also conflicts with fundamental principles of the rule of law—most notably legal certainty—which is protected both by Croatian constitutional law and by European standards articulated by the Venice Commission. Article 3 of the Croatian Constitution requires that laws be clear, foreseeable, and stable, while Article 90 prohibits legal frameworks that create unpredictable or shifting obligations. CSA2, however, grants the European Commission broad discretion to expand prohibitions, redefine key ICT assets, and impose new obligations at any time, without clear or predictable criteria, preventing operators and public authorities from anticipating which technologies, suppliers, or business models will be permitted in the future. Such instability undermines legitimate expectations and prevents economic actors from planning their conduct, investments, and contractual obligations with confidence. By creating a regulatory environment marked by uncertainty, abrupt changes, and the absence of foreseeability, CSA2 is incompatible with the essence of legal certainty as a core component of both the Croatian constitutional order and the EU's rule of law framework.

Thirdly, CSA2 impacts freedom of entrepreneurship and free market competition, protected by Articles 49 and 50 of the Croatian Constitution. The Proposal introduces blanket supplier bans that are not based on Croatian risk assessments but on EU level geopolitical classifications, leaving no room for national tailoring, proportionality balancing, or local context. These bans distort the Croatian market by excluding entire categories of suppliers, reducing competition, increasing costs for operators, and disadvantaging Croatian subsidiaries of third country groups. The Impact Assessment itself predicts significant economic burdens and structural changes to market functioning, confirming the severity of these constraints.

Finally, CSA2 raises a direct conflict with constitutionally guaranteed property rights. Article 48 protects ownership, while Article 50 permits restrictions or expropriation only if (1) they serve the interest of the Republic of Croatia and (2) full market value compensation is provided. Mandatory removal of previously lawful and valuable equipment represents a substantial interference with ownership rights. Yet CSA2 imposes these obligations for EU level policy aims without Croatian discretion and without any compensation mechanism. Even the Advocate General's Opinion in *Elisa Eesti* acknowledges that such measures may impose disproportionately heavy burdens. Consequently, CSA2 as drafted creates a situation where Croatian entities may be deprived of property without a clear right for compensation and without the action being grounded in the national interest of Croatia, contrary to explicit constitutional guarantees.

In light of the identified constitutional concerns, it is recommended that the CSA2 Proposal be reconsidered to take into account the need to respect Member States' exclusive national security competence; ensure legal certainty by preventing retroactive effects and unclear future prohibitions; and protect ownership and establish a clear compensation framework guaranteeing market value remuneration where EU level decisions require the removal or limitation of lawfully acquired property. Only by incorporating these safeguards can CSA2 be aligned with Croatia's constitutional guarantees of ownership, entrepreneurial freedom, market competition, and national security sovereignty.

Hungary and the cyberspace sovereignty – constitutional, regulatory and procurement risks

Procurement and certification

Centralisation of certification and possible marginalisation of national authorities

The CSA2 Proposal significantly strengthens the role of ENISA, transforming it into a "single point of expertise" for cybersecurity at the EU level and introducing a more centralised certification framework (ECCF). While this aims to ensure regulatory consistency and reduce fragmentation across the Internal Market, the current wording of the Proposal – particularly Article 18 (2) – risks over-centralisation at the expense of the national competent authorities (NCAs). Under Article 18 (2), ENISA should be tasked to "monitor and, where relevant, participate and lead in standardisation development activities at the EU level." ENISA's leadership role may reduce the operational weight of national regulatory authorities, whose competences are grounded in both EU and domestic laws.

In Hungary, cybersecurity oversight is a well-diversified architecture established under Act LXIX of 2024 on Hungary's Cybersecurity and its principal implementing decree, Government Decree 418/2024 (XII. 23.).

- **Supervisory Authority for Regulated Activities (SZTFH):** the primary NIS2-supervisory body for essential and important entities within the scope of Act LXIX of 2024, responsible for risk classification, security audits, and enforcement.
- **Special Service for National Security (NBSZ):** operating under Act CXXV of 1995 on National Security Services and with access to classified threat intelligence that is structurally unavailable to EU-level bodies.
- **Hungarian National Bank (MNB):** sectoral regulator for the financial sector, exercising cybersecurity supervisory functions in parallel with the requirements of Regulation (EU) 2022/2554 (DORA), including ICT risk management and incident reporting obligations.

This multi-layered architecture reflects the functional complexity of cybersecurity governance and enables regulatory responses calibrated to sector-specific threat profiles. The potential marginalisation of these authorities may lead to a less sector-specific approach, which could be detrimental to organisations operating in highly regulated sectors.

The proposed shift towards ENISA-led standardisation under Article 18 (2) of the CSA2 Proposal risks undermining the principle of subsidiarity, which requires that common objectives be pursued at the EU level only if they cannot be sufficiently achieved by the Member States, and only to the extent that the added value of EU action outweighs the costs of harmonisation. To maintain resilient cybersecurity posture, certification, and standardisation, it may be wise to consider to keep Member State led processes, for the following reasons:

- National authorities (such as SZTFH, MNB, or NBSZ) should play the central role in defining certification criteria. They possess the direct enforcement experience, sector-specific knowledge, and legal mandates under both EU law and national legislation that EU-level bodies such as ENISA may lack.
- ENISA's role should be strictly limited to that of a facilitator and coordinator. Instead of leading standardisation, ENISA should focus on ensuring cross-border interoperability of certification schemes and providing a platform for best-practice sharing among national regulators and sectoral authorities.
- A centralised framework is inherently limited by its lack of access to classified national intelligence. If ENISA dictates standards without the specific threat-intelligence insights held by national security bodies, the resulting framework may be structurally incomplete or misaligned with actual national security risks.
- If ENISA assumes the lead in standardisation, NCAs are effectively relegated to mere implementers. This disrupts the professional autonomy of national regulators and disconnects policymaking from the ground-level supervision of critical entities, which is inconsistent with the subsidiarity oriented institutional design of EU cybersecurity and security policy.

The legal effect of CSA2 Article 86(1) and the "non-technical risk" issue

The centralisation envisaged by CSA2 may result in the displacement of national cybersecurity frameworks and could transfer elements of national security risk management to the EU level.

Article 86(1) of CSA2 provides that national cybersecurity certification schemes "shall cease to produce effects" once a corresponding EU scheme is adopted. As the Proposal significantly broadens the scope of the ECCF – including domains such as managed security services and the "cyber posture" of entities – Hungarian certification mechanisms established under Act LXIX of 2024 and Government Decree 418/2024 could be effectively superseded. This would prevent Hungary from maintaining enhanced or sector-specific certification requirements grounded in domestic risk assessments or national strategic priorities.

The legal effect of this part of the Proposal would represent a potential fundamental reallocation of decision-making power within the EU. Rather than proceeding under the Common Foreign and Security Policy (CFSP) – where Member States retain full sovereignty through the unanimity requirement – this shift would be executed via an internal-market instrument based on Article 114 TFEU. As a result, the original national-security safeguard enshrined in Article 4(2) TEU could become significantly less operational. As centralised EU frameworks might displace national regulations, the legal landscape would change. For instance, Member States might no longer possess the autonomous authority to determine which technologies, suppliers, ICT services, or components are permissible for their own critical infrastructures.

This structural tension is amplified by the CSA2's introduction of "non-technical risks" as a criterion both for certification and for the designation of high-risk vendors. These "non-technical" elements encompass assessments of third country legal systems, geopolitical risk indicators, and state behaviour in cyberspace – determinations that are inherently intelligence-dependent and may be politically sensitive. [20]

[20] CSA2 Proposal, Recital (129), Article 117

In our opinion, it remains highly questionable whether EU-level bodies such as ENISA could effectively replicate these functions. Since EU-level bodies lack access to Member States' intelligence and national security information, cannot classify national threat assessments, and are not directly accountable to a national supreme body, they are structurally ill-equipped to assume such responsibilities. Incorporating "non-technical risks" into an Article 114 TFEU instrument does not alter the inherently security-sensitive nature of these determinations, but it may centralise their determination at the EU level.

This is similar to the structural problem identified in the Tobacco Advertising (C-376/98) "predominant purpose" doctrine, which prohibits internal-market measures from regulating matters that lie outside the scope of Article 114 TFEU under the guise of harmonisation.

Furthermore, the proposed centralisation could create a state of "retroactive legal uncertainty". Any subsequent Commission implementing acts[21] might override formal national security determinations or authorisations issued by competent domestic authorities.

According to Hungarian legal practice, the rule of law is not merely a formal requirement but a substantive guarantee, requiring legal norms to be clear and foreseeable. This ensures that economic operators can build long-term strategies upon the continuity of legal relationships established under previously applicable law. [23]

The CSA2 Proposal would fundamentally undermine this stability by effectively voiding national security clearances that were previously granted by sovereign domestic authorities. It imposes prohibitive new burdens on large-scale infrastructure investments that were entirely lawful and officially authorised at the time they occurred. If an EU-level geopolitical designation can transform a sanctioned investment overnight into a prohibited liability, the very essence of legal certainty is compromised.

Such an EU-level decision would trigger a mandatory 36-month phase-out period[23], effectively nullifying prior sovereign assessments. This would force the removal of critical infrastructure that national security organs had explicitly deemed safe and authorised for use, creating a direct conflict between EU-level mandates and the primary responsibility of Member States to protect their own national security enshrined in Article 4 (2) TEU.

Public Procurement: From technical compliance to political exclusion

Under the CSA2 Proposal, the designation of a supplier as a "high-risk vendor" pursuant to Article 100 of the CSA2 would trigger a series of automatic exclusions from public contracts and sub-contracting chains, denial of EU funding, and ineligibility for European cybersecurity certificates.[24] These consequences flow automatically from designation, without individualised assessment of the specific procurement context or the technical characteristics of the goods or services offered.

Departure from the Hungarian and EU Procurement Framework

This automatic exclusion mechanism may represent a material departure from the individualised, procedurally protected assessment model established by Act CXLIII of 2015 on Public Procurement (Kbt.) which transposes Directive 2014/24/EU into Hungarian law.

---

[21] CSA2 Proposal, Article 100-104

[22] CSA2 Proposal, Recital (166)

[23] CSA2 Proposal, Article 110

[24] CSA2 Proposal, Recital (139)

Under the current Hungarian framework:

- Exclusion from procurement procedures must be based on transparent, legally defined criteria, as required by Section 2(1) and Sections 73-75 of the Hungarian Public Procurement Act (Act CXLIII of 2015, Kbt.).
- Contracting authorities must conduct an individualised assessment of whether a specific tenderer meets the exclusion grounds.
- Consistent with Section 62 Kbt. and Article 57(1) of Directive 2014/24/EU, automatic, category-based exclusion is not permissible, except for the mandatory exclusion grounds exhaustively listed in the statute.
- Tenderers have a statutory right to "self-cleaning" under Section 188 Kbt., which directly transposes Article 57(6) of Directive 2014/24/EU.
- A tenderer may demonstrate that it has restored its reliability and therefore cannot be excluded automatically.
- Decisions on exclusion are subject to effective judicial or administrative review, guaranteed by Sections 148-152 Kbt., which establish the system of remedies before the Public Procurement Arbitration Board and the courts.

The HRV designation mechanism could bypass these safeguards. If the Commission were to make designations through implementing acts – potentially based on undisclosed "non-technical risk" factors – it would result a black-box mechanism. The automatic, direct exclusion under Article 100(4)(e) would restrict contracting authorities' ability to consider actual technical risk, nullifying the right to self-cleaning, as origin-based risks are structurally irremediable by the operator. Furthermore, this mechanism would easily replace a merit-based procurement system and would create significant friction between national and EU law, including the principle of non-discrimination and Article 47 of the Charter.

International Trade Dimension: WTO Government Procurement Agreement

The proposed origin-based exclusion mechanism in public procurement under CSA2 also engages Hungary's and the EU's obligations under the World Trade Organisation (WTO) framework, including the WTO Government Procurement Agreement (GPA) and the core GATT[25] disciplines on non-discrimination and national treatment. By shifting from objective technical evaluations to "non-technical risk factors" based on a supplier's country of origin, the CSA2 Proposal creates significant legal risks for both Hungary and the EU.

Under the WTO GPA, an automatic exclusion based on a supplier's country of origin or "non-technical risk factors" rather than procurement-specific qualifications may constitute unjustified discrimination contrary to GPA Article IV (non-discrimination). While GPA Article III(1)(a) provides a national security exception, it strictly prohibits measures applied in an "arbitrary or unjustifiable discrimination" form, which limits how broadly a jurisdiction based exclusion scheme such as CSA2's HRV mechanism can be framed.

The CSA2 Proposal, particularly its "high-risk vendor" and "third-country" assessment mechanisms, may therefore be inconsistent with several core WTO obligations. For example, CSA2 may violate the non-discrimination principle under GATT Articles I & III, since the security assessment of an ICT product is linked to its country of origin or the political system of the supplier's home state (e.g., "lack of democratic checks"), rather than to the intrinsic technical characteristics of the product itself. This may create de facto discrimination that breaches the most-favoured-nation [26] and national treatment[27], as "like products" are treated differently based on non-technical, origin-based criteria.

---

[25] General Agreement on Tariffs and Trade (GATT 1947)

[26] GATT Article I (1)

[27] GATT Article III (4)

Moreover, the Proposal is currently addressing routine digital transformation and cyber defence challenges, where cybersecurity vulnerabilities represent inherent technical and long term operational risks, not an "emergency in international relations" in the sense of the national security exception under GATT Article XXI. To the extent that CSA2 measures are justified under a broad national security carve out, the logic of their origin based, systemic exclusion must be carefully tailored so as not to amount to an arbitrary or disproportionate departure from the standard WTO treatment of "like products", as otherwise the EU and the Member States risk significant WTO compliance challenges and international trade policy backlash.

The shift from technical assessment to a "non-technical" exclusion generates several systemic legal concerns:

- Unlike standard procurement evaluations, the HRV mechanism may disqualify a vendor regardless of the technical security practices or technical integrity of the specific equipment offered.
- Affected suppliers would face severely restricted access to the underlying intelligence basis for their designation. This lack of transparency hinders the right to a fair hearing and renders an effective judicial challenge nearly impossible.
- The potential for disproportionate interference with the principles of equal treatment could expose Member States to significant litigation and international trade retaliation, undermining the stability of global supply chains.

Property rights and economic freedom

Mandatory phase-out obligations and constitutional property protection

One of the most intrusive elements of the CSA2 Proposal is the prospective imposition of mandatory phase-out obligations in Title IV (ICT supply chain security), in particular, Article 110 would require operators – particularly in the telecommunications sector – to remove and replace previously lawfully deployed infrastructure supplied by designated "high-risk vendors" and used in key ICT assets of 5G networks, as listed in Annex II to the Proposal, within a fixed 36-month timeframe from the publication of the relevant high-risk vendors list.

From the Hungarian legal perspective, such measures directly engage the protection of property under Article XIII of the Fundamental Law, which permits expropriation only exceptionally and against full, immediate, and unconditional compensation. It also engages Article 17 of the Charter of Fundamental Rights of the European Union, which protects the right of everyone to own and use their lawfully acquired possessions. The European Commission's own Impact Assessment acknowledges that these "rip-and-replace" mandates could cost mobile network operators between €3.4 billion–€4.3 billion annually, yet the CSA2 Proposal does not establish any corresponding compensation scheme for affected operators.

Limitation vs. deprivation:

Guidance from the CJEU (C-354/24, *Elisa Eesti* case)

The central legal question, currently debated in the *Elisa Eesti* AS v Vabariigi Valitsus (Case C-354/24, AG Opinion delivered 19 March 2026), is whether such obligations constitute:

- a deprivation of property, which under both Hungarian and EU standards typically requires fair and timely compensation
- a limitation on the use of property, which may be justified under certain conditions.[28]

In her Opinion, Advocate General Ćapeta clarified that – while national measures excluding equipment on security grounds generally constitute a limitation of use rather than a deprivation (thus not triggering automatic compensation) – this power is inherently tied to Member State competence under Article 4 (2) TEU, which stipulates that national security remains the sole responsibility of each Member State.

The AG emphasises that such security-based restrictions must remain subject to strict proportionality and individualized assessment at the national level, based on specific and evidence-based risk assessments rather than general suspicion.[29] However, the CSA2 Proposal seeks to replace this domestic margin of appreciation by establishing mandatory, EU-wide lists of high-risk vendors through implementing acts. By replacing case-by-case national discretion with centralised, binding designations, the Proposal creates significant legal uncertainty and constitutes a potential competence overreach, as it may bypass the very national security safeguards the AG Opinion – and Article 4(2) TEU – seek to protect.

Proportionality and the "heavy burden" exception

The Opinion in *Elisa Eesti* emphasises that any restriction on the use of hardware or software must be:

- based on a specific and evidence-based risk assessment (rather than generalised suspicion), which involves an analysis of the intended equipment and the specific risks associated with its manufacturer or country of origin, rather than relying on generalised suspicion, and
- subject to full judicial review.

Crucially, the Advocate General acknowledges that while a limitation of use does not generally trigger automatic compensation, a "system of reasonable compensation" may still be required where the restriction imposes an exceptionally heavy burden on the operator. Under the Hungarian Fundamental Law (Article XIII), any state intervention that causes disproportionate financial loss without a remedial mechanism risks violating the constitutional protection of property. As the Commission's Impact Assessment estimates the annual cost of the "rip-and-replace" mandate at €3.4 billion to €4.3 billion, the CSA2's rigid 36-month timeline – applied without regard to the remaining lifecycle of the equipment or a structured indemnity framework – likely meets the legal threshold of an "exceptionally heavy burden".[30] This tension is further accentuated by the fact that CSA2, unlike the national regime examined in *Elisa Eesti*, would operate as directly applicable EU law, leaving Member States limited room to introduce their own compensation arrangements without distorting the internal market.

Systemic risks: The lack of individualised assessment

Unlike the national measures examined in *Elisa Eesti*, CSA2 would introduce origin-based, centralised restrictions via implementing acts adopted by the Commission under Articles 100-104 and 110 CSA2. This approach is difficult to reconcile with the AG's requirement for concrete risk evaluation.

- Under the Hungarian Fundamental Law (Article M), which ensures fair economic competition, the automatic exclusion of a vendor based on a centralized EU list – without allowing for a technical assessment of the bid – undermines the principle of equal treatment and technological neutrality in public procurement.

---

[28] C-354/24, F. The sixth question

[29] C-354/24, E. The fifth question, Article 12 (1) of Directive 2018/1972 and the principle of proportionality

[30] C-354/24, F. The sixth question 128-138

- While the AG suggests compensation is not “automatic” for mere limitations, the scale of the CSA2 mandate transforms a temporary restriction into a systemic economic drain. Without a pre-defined compensation framework in the Proposal to mitigate the loss of lawfully acquired assets, the measure would fail the required test of proportionality, particularly when assessed against the combined requirements of Article 17 of the Charter and Article XIII of the Fundamental Law.

Substantive burden vs. formal classification

The key implication of the evolving CJEU case law is that the formal label of "limitation" does not shield a measure from rigorous proportionality scrutiny. For Hungary, the CSA2 Proposal represents a dual challenge:

- It would impose a massive financial burden on operators (and potentially the Member State) without the compensatory safeguards required for “heavy burdens” under Article XIII of the Fundamental Law.
- It would strip national authorities (such as the SZTFH) of the right to conduct the very individualised proportionality balance that AG Ćapeta identifies as the legal prerequisite for such intrusive security measures. The Proposal replaces case-by-case national discretion with an EU-level sequence of implementing acts. Under Articles 100-104, the Commission – rather than the Member State – would define the relevant risks, establishes the underlying evidence base (often derived from classified intelligence), and issues the final designation of high-risk suppliers.[31]

These implementing procedures would effectively replicate a sanctions designation process. However, they lack the procedural guarantees, unanimity requirements, or CFSP-based legal safeguards (Articles 24 and 29 TEU) typically required for restrictive measures. As such, they centralise national-security decision-making within the Commission while denying Member States the ability to carry out the very case-by-case proportionality analysis that EU law requires for security-based restrictions.

Ultimately, the Proposal’s reliance on Article 114 TFEU as a legal basis for what are effectively security-driven sanctions may create a “Trojan horse” mechanism. This framework would potentially bypass the institutional safeguards and unanimity requirements of the Treaties. The introduction of these centralised implementing acts intensifies this risk by enabling the Commission to impose binding, sector wide exclusion measures through a procedure that is structurally foreign to both CFSP decision making and the constitutional framework of Hungary under Article E) (2) of the Fundamental Law.

[31] CSA2 Proposal Article 104

SUMMARY & KEY TAKE-AWAYS

Overall, the CSA2 Proposal – as currently drafted – gives rise to a set of constitutional and EU law concerns when assessed from the perspective of Hungary's legal order.

The planned shift toward EU-level certification and supplier-risk designation may significantly narrow the practical role of Hungarian authorities in matters that rely on national competence and intelligence security expertise. This would raise questions about the appropriate balance of competences and the preservation of Member State responsibility for national security under Article 4(2) TEU.

In addition, the Proposal may affect the predictability of the regulatory environment. The prospect that in the future, the Commission's implementing acts could introduce new restrictions or require the replacement of infrastructure that was previously authorised risks weakening the stability and foreseeability expected by operators investing in critical ICT systems and ICT products.

The Proposal also introduces procurement consequences that differ markedly from the established model of individualised assessment in EU and Hungarian public procurement law. Automatic supplier exclusions, combined with limited opportunities for case-by-case review, may create tensions with the principles of equal treatment, effective remedies, and open competition.

Finally, the obligation to phase-out existing infrastructure within a fixed (36-month) timeframe, without a clearly defined compensation mechanism, could impose a disproportionate financial burden on operators and raise concerns regarding the protection of property and the principle of proportionality under both national and EU fundamental-rights standards.

During the legislative process, it is our view that it would be advisable to consider:

- maintaining a substantive role for national authorities in security-sensitive risk evaluation;
- ensuring that high-risk vendor designations rely on transparent and reviewable criteria;
- establishing a predictable compensation framework for mandatory infrastructure replacement; and
- aligning procurement effects with the individualised assessment and remedies system.

These adjustments would not only safeguard Hungary's constitutional requirements, but in our opinion would also support the EU's objective of technological sovereignty by preserving supplier diversity while strengthening cybersecurity resilience.

Nevertheless, the Proposal is only in its initial form. It is widely expected to be amended throughout the legislative process so that it can meet its original objectives while introducing a new structure consistent with the applicable legal principles of the EU acquis and the laws of the Members States.

CONTRIBUTORS

Tímea Bana
Partner, Head of the local Technology service line HU

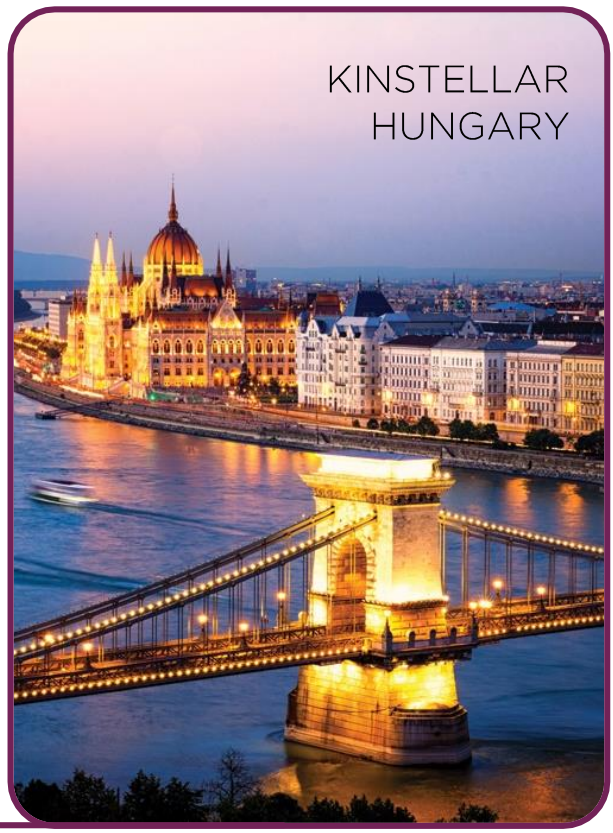
+36 1 428 4411
timea.bana@kinstellar.com

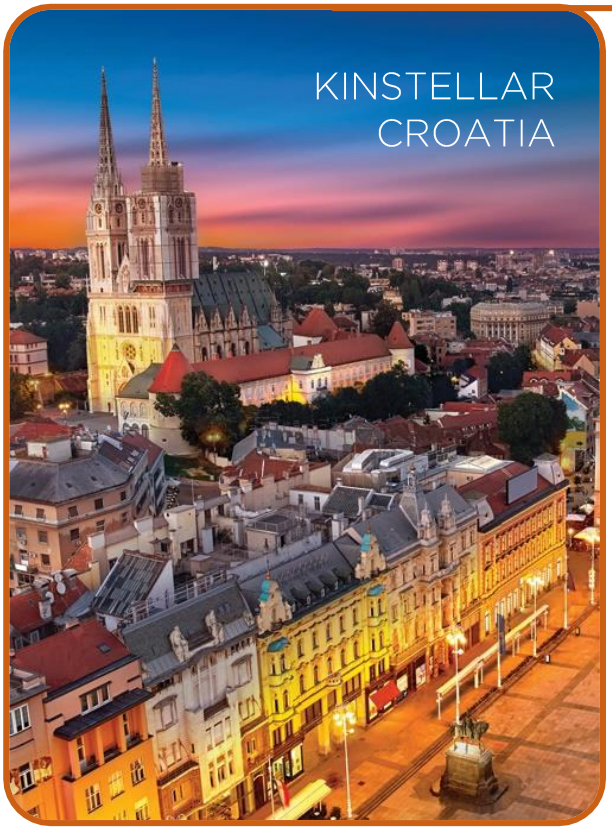
Ákos Kovács
Associate, Technology HU

+36 1 428 4487
akos.kovacs@kinstellar.com

Dária Zsófia Szabó
Junior Associate, Technology HU

+36 1 428 4412
dariazsofia.szabo@kinstellar.com





Vedran Kopilović
Counsel, Technology HR

+38515556772
vedran.kopilovic@kinstellar.com

Andrej Skljarov
Managing Associate, Technology HR

+38515556770
andrej.skljarov@kinstellar.com

Jakov Hadžija
Associate, Technology HR

+38515555643
jakov.hadzija@kinstellar.com

Leading independent law firm in Central and Southeastern Europe and Central Asia

With offices in 12 jurisdictions and over 300 local and international lawyers, we deliver consistent, joined-up legal advice and assistance across diverse regional markets — together with the know-how and experience to champion your interests while minimising exposure to risk.

ALMATY | KAZAKHSTAN
ASTANA | KAZAKHSTAN
BELGRADE | SERBIA
BRATISLAVA | SLOVAKIA
BUCHAREST | ROMANIA
BUDAPEST | HUNGARY
ISTANBUL | TÜRKIYE
KYIV | UKRAINE
PRAGUE | CZECH REPUBLIC
SOFIA | BULGARIA
TASHKENT | UZBEKISTAN
VIENNA | AUSTRIA
ZAGREB | CROATIA

KINSTELLAR