ANTAS
DA CUNHA
ECIJA

REVISION OF THE CYBERSECURITY REGULATION:

A DEBATABLE AND DEBATED PROPOSAL

Article by:

José Luís da Cruz Vilaça[1]

Paulo de Almeida Sande

Mariana Tavares

ECIJA 2026

[1]

REVISION OF THE CYBERSECURITY REGULATION:

A DEBATABLE AND DEBATED PROPOSAL

Introduction and Background

On 20 January 2026, the European Commission ("**EC"**) published a legislative package which includes the replacement of the Cybersecurity Act ("**CSA"**).[2]

The package amends NIS2[3] and is interlinked with the CSA, while also complying with other laws and regulations relating to the Digital Omnibus Package.[4]

This article focuses on the proposal to replace the CSA.

The CSA came into force in 2019, developing the role of ENISA[5] and establishing a voluntary framework for the certification of information and communications technology (**"ICT**") security. It replaced "fragmented national schemes" and ensured the security of products,

[2] Regulation (EU) 2019/881 of 17 April 2019 on ENISA (European Union Agency for Cybersecurity).
[3] Directive (EU) 2022/2555 of 14 December 2022, on measures for a high common level of cybersecurity across the Union.
[4] The Digital Omnibus Package was unveiled on 19 November 2025. It aims to simplify and streamline the digital regulatory framework in terms of data access, privacy and cybersecurity. It includes amendments to the EU Data Act; a single reporting point for the GDPR, NIS2, DORA and CER; the abolition of the platform to business (P2B) regulation; changes to the "cookie consent" rule; the amendment of the definition of personal data and special category data; and the allowing the allowance of the processing of personal data to train AI models based on a legitimate interest. On the same date, the EC also launched a Digital Omnibus on AI Regulation Proposal (AI Omnibus), which amends aspects of the EU AI Act. Final reports from the EP committees on the package, as well as a "general approach" from the EU Council, are expected to be delivered by the second quarter of 2026.
[5] European Union Agency for Cybersecurity.

services and processes at different levels, establishing the European Cybersecurity Certification Framework ("**ECCF"**) schemes. It included Internet of Things security, among other cybersecurity aspects.

The CSA revision delivered in January 2026 ("**CSA2"** or **"the proposal"**) has two main objectives: (i) to increase cybersecurity capabilities and resilience, and (ii) to prevent fragmentation across the single market.

Four areas of intervention are considered: (i) reinforcement of the ENISA mandate, (ii) reform of the ECCF, (iii) simplification of procedures, mainly through targeted amendments to NIS2 interlinked with CSA, and (iv) security of ICT supply chains.

Among other provisions, CS2 requires the mandatory phase-out of ICT components in 5G networks listed in Annex II,[6] which are supplied by high-risk suppliers ("**HRS**").[7]

The 5G security toolbox recommendation to restrict the use of 5G equipment from high-risk suppliers was endorsed by the EC on 29 of January 2020, following its non-binding recommendation in March 2019. If the EC's preferred policy package is adopted, this recommendation may become mandatory.

[6] Key ICT assets for mobile and fixed electronic communications networks. The critical infrastructures concerned are (i) 5G electronic communications networks (non-standalone and standalone) (ii), fixed electronic communications networks and (iii) satellite electronic communications networks.

[7] "High-risk suppliers/vendors" is not a consolidated legal category, but rather a functional notion relating to suppliers whose technology, services or position in the supply chain are considered by the EU to be capable of having a systemic impact on critical infrastructure, facilitating the exploitation of technical vulnerabilities or creating excessive dependencies on suppliers from countries that are at risk of state interference and which can pose a high risk to EU security based on their laws, legal systems, practices or evidence of malicious cyber activity. This concept is set out in the "5G Toolbox", which recommends that Member States should exclude these suppliers from the most sensitive and critical parts of telecommunications networks.

The proposal also establishes a more simplified European Cybersecurity Certification Framework ("**ECCF**"), extending its scope to include broader factors such as geopolitical forces and the threat posed by emerging technologies, including AI and quantum cryptanalysis.

The proposal focuses on HRS within its new framework, which aims to ensure the security of the ICT supply chains of entities operating in highly critical sectors, as defined by NIS2. It characterizes HRS - a concept mentioned 63 times in the CSA2 proposal - as being susceptible to influence from a non-EEA government in a way that could undermine service continuity, compromise data security or affect the integrity of products or services provided.

In addition to designating HRS, the EC also intends to identify third countries that pose cybersecurity concerns. From there, are targeted entities established in, or controlled by, a third country posing cybersecurity risks, entities established in that country, or one of its nationals. The EC recognises that significant supply chain cybersecurity incidents often spread across national borders.[8] In the proposal of the Multiannual Financial Framework 2028-2034, there is even a mandate for the exclusion of HRS as a structuring principle, in order to protect the integrity of the EU budget and security interests.

According to the EC, the aim of this new regulation is to create a harmonised framework to tackle "non-technical risks affecting ICT supply chains",[9] in order to reduce 'the current fragmentation of

[8] Explanatory Memorandum, page 6.
[9] Idem.

approaches across Member States". [10] The EC submits that the proposal represents "a substantial simplification and modernisation of the Union's cybersecurity legal framework, fully aligned with the REFIT[11] principles of clarity, efficiency and digital readiness"[12].

In its Impact Assessment Report on the proposal, the EC lists the various possible options for the four aforementioned areas of intervention mentioned above: ENISA's mandate, the ECCF, simplification through NIS2 amendments, and ICT supply chain security.

These options are presented as the result of a comprehensive analysis to determine the most appropriate level and form of intervention, including whether EU action would lead to better outcomes than Member State solutions alone.[13]

It is important to emphasise that the EC's analysis concluded that EU action would lead to better results than Member States acting alone, but this does not allow for the violation of fundamental principles of Union law, particularly concerning the division of competences.

Regarding the different options presented for each of the four areas of intervention, the EC has selected its preferred policy package:[14]

- The functional reform of ENISA;
- Reform of the ECCF, including an extension of its scope, a new procedure and revised governance;

[10] Explanatory memorandum, page 3.
[11] Regulatory fitness and performance program.
[12] Idem.
[13] Impact Assessment, page 39.
[14] Explanatory Memorandum, p. 12. See also pp. 109 *et seq.* of the Impact Assessment.

- A targeted intervention and further simplification of compliance with relevant Union cybersecurity legislative framework (NIS2);
- A comprehensive, horizontal framework to address cybersecurity risks in ICT supply chains.[15]

According to the EC, this combination of options provides "the most balanced and effective response to the policy problems identified in this impact assessment". [16]

While the EC does not completely rule out other less restrictive combinations of its options, the EC considers its preferred package to be the most appropriate, balanced and effective.

This seems to suggest that less radical and less intrusive solutions than those proposed in the preferred package are possible, particularly with regard to HRS or the framework concerning countries of origin with cybersecurity issues.

Nevertheless, CSA2 contains several aspects that will certainly be subject to thorough and in-depth scrutiny regarding their legality and solid foundations throughout the legislative process. In a report from June 2025, the European Parliament's Industry, Research and Energy Committee emphasized that the CSA revision should focus on the interplay between sovereignty and security.

On 5 January 2026, the EP Parliamentary Research Service published a report recognizing potential challenges concerning "sovereignty and the legal limits of ENISA's influence".[17] It pointed out

[15] Idem.
[16] Idem.
[17] Idem.

that the most contentious issue dividing stakeholders and Member States was the difference of opinion between those advocating for EU digital autonomy and those "prioritizing open markets and technical neutrality. [18]

As previously mentioned, this may also relate to the geostrategic dimension of cybersecurity, including the relationship with large technology companies that are not present in the EU's internal market.

Sovereignty issues can therefore be divided into two main categories: (i) EU strategic autonomy in general versus supranational big tech, and (ii) EU level security in relation to national security considerations of EU Member States.

The aforementioned document's explanatory memorandum refers to the principle of subsidiarity under Article 5 TEU and considers that the EU can better achieve cybersecurity than Member States can.

However, such an approach raises questions about the division of powers between the EU and its Member States with regard to national security matters. Firstly, as set out in Article 5(1) TEU, the use of Union competences is governed by the principle of subsidiarity - alongside the principle of proportionality -, which presupposes that the Union has been conferred the respective competence, under the principle of conferral laid down in the same Article. [19] Secondly, Article 4(2) TEU, states that

[18] Idem.

[19] Article 5 TEU states: "1. The limits of Union competences are governed by the principle of conferral. The use of Union competences is governed by the principles of subsidiarity and proportionality.
2. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States."

“national security remains the sole responsibility of each Member State”, which seems to imply that the EU is precluded from taking measures on such matters.

In any case, the new CSA2 is currently being negotiated as a regulation between the European Parliament and the Council, under the ordinary legislative procedure. There is no precise estimate of when it may be adopted at this time.

Geostrategy, strategic autonomy and national security

CSA2 also addresses the issues of sovereignty and strategic autonomy as part of the ongoing global political and geostrategic discussions (with a particular focus on Europe and the EU), the outcome of which will undoubtedly influence the negotiations within the legislative process.

In some ways, CSA2 reflects the growing awareness of the risks associated with the security of communication networks and products in Europe, particularly within the EU. Managing hybrid crises with the potential for a systemic impact is now the norm, with cyber resilience being a security issue at the individual, Member State and Union levels.

Given the growing importance of security in sectors such as transport, water supply, finance and health, as well as its political implications, the EU is emphasizing the need for coordinated national efforts to address the high level of interconnectivity and cascading

effects of threats to digital supply chains, which can impact several states or even the Union as a whole. This is achieved through legislation such as the CSA and NIS2, as well as institutions such as ENISA.

To this end, and with a view to strengthening the Union's resilience, states are invited to develop and enforce national strategies that address supply chain security, vulnerability management and large-scale incident response.

In terms of foreign policy and international relations, however, it is clear that the European dimension is becoming increasingly important in a rapidly changing geostrategic context. The interests of each Member State in the single market and in cross-border communications, which are essential for implementing European public policies, are becoming increasingly important.

Against this backdrop, the question of the EU's relationship with its competitors and political and economic partners arises. In a rapidly expanding and highly volatile geopolitical and geoeconomic environment, decisions on public policy regarding external partners — such as US tariffs or the activities of large technology companies in Europe — become central to European geostrategy and are certainly a common concern of EU countries.

The EU needs partners, and it is clear that previously relied-upon alliances and partnerships are no longer effective, so new agreements are being pursued. This trend will only become more pronounced in the coming years.

Against this backdrop, the Union is seeking to reduce its external dependencies, regulate critical technologies and their resilience, and design strategic relations with its economic competitors.

However, national defense, intelligence and information strategies remain the sovereign responsibility of the Member States. This is, of course, a controversial issue, but the Treaty and case law point in that direction.

The CSA2 legal basis and the apportionment of powers regarding national security

The principle of conferral, enshrined in Article 5 TEU, is a fundamental principle of EU Law.

Article 5(2) TFEU is a key constitutional rule that allocates powers between national and EU levels. It establishes that the Union may only act within the limits of the competences conferred upon it by the Member States in the Treaties and that any competence not attributed to the Union remains with the Member States.

In the case of national security, not only does the TEU fail to confer any competence to the EU, it also explicitly specifies, in Article 4(2), that it “remains the sole responsibility of each Member State”. Furthermore, safeguarding national security is equated with other “essential State functions”, alongside “ensuring the territorial integrity of the State” and “maintaining law and order”.

As emphasised by the CJEU,[20] it is the prerogative of Member States to take appropriate measures to maintain law and order, and to ensure internal and external security, within their territories, while preserving the effectiveness of EU law, under adequate judicial control.

In an article published on EU Law Live titled "EU Law and the limits of invoking national security",[21] José Luís da Cruz Vilaça addresses the interpretation and limits of the concept of national security as well as the compatibility of national security-related measures with EU law.

In this context, choosing Article 114 of the Treaty on the Functioning of the EU ("**TFEU**") as the legal basis for a regulation such as the Cybersecurity Act, whose main object is security (including national security) rather than the internal market, could invalidate the entire regulation.

Referring to Article 114 TFEU as the sole legal basis could legitimately be perceived as encroaching upon an area of exclusive national competence, which makes it difficult to reconcile such a regulation with the limits of EU powers as defined in the Treaties.

In this respect, settled case law of the CJEU holds that "in the context of the organisation of the powers of the EU, the choice of the legal basis for a measure may not depend simply on an institution's

[20] Judgment of 2 April 2020, *European Commission v Polland, European Commission v Hungary and European Commission v Czech Republic*, Joined Cases C-715/17, C-718/17 and C-719/17, EU:C:2020:257, para 143.
[21] Published in EU Law Live Weekend Edition of 12 July 2025 (n. 238).

conviction as to the objective pursued, but must be based on objective factors amenable to judicial review".[22]

It should also be noted that, during the legislative process for adopting the CSA, the parliaments of several EU Member States expressed doubts about the legal basis used and its application to security matters[23].

Therefore, the EU legislature should pay due attention to preserving a clear separation between matters that must be kept under the sole responsibility of the Member States (national security aspects) and matters that may be put under the umbrella of Article 114 TFEU regarding the EU's competence for the establishment and functioning of the internal market (the digital ecosystem), irrespective of how difficult it may be to fine-tune the dividing line. Above all, this is required by the principle of conferral.

---

[22] See judgments of 11 June1991, C-300/89, *Commission v Council* (*Directive on waste from the titanium dioxide industry - Legal basis*), para. 10; of 17 March 1993, C-155/91, *Commission v Council* (*Waste Directive*), paras 7, 19-21. According to the latter, "Where a measure pursues a twofold purpose, and one is identifiable as the main or predominant purpose, the measure must be founded on a single legal basis."

[23] Vg. French Senate, Reasoned Opinion, 27/11/2017: "(…) Regarding Member States' competence on security matters: – the Senate underlines that cybersecurity, given its importance for Member States' security, is on several aspects an area of national sovereignty; – consequently, Member States must keep, on the one hand, their faculty to adopt norms and standards providing a higher security level and on the other hand, their full place on the new European device, based on their voluntary participation to a European cybersecurity; – for that reason, as regards to the proposal's legal base, it considers that a Regulation on cybersecurity cannot only deal with the functioning of the internal market (articles 26 and 114 TFEU), but it also has to integrate security issues (article 5 of the Treaty on European Union)"; Bundesrat, 15/12/2017: "The Bundesrat doubts whether the proposal is in accordance with the principles of subsidiarity and proportionality. Proven certification schemes do exist on the national level already. Excluding such national systems bears the risk that they could not be implemented effectively any longer. Such an infringement into matters of national security is not necessary – instead, a European certification scheme could be supplemented by national measures; Czech Republic, 12/09/2017: "(…) The Senate (…) Remarks that the Member States are primarily responsible for national security including cybersecurity".

This need is emphasised in NIS2, in its Article 2(6), which makes clear that its provisions are “without prejudice” to the responsibility of Member States to safeguard national security and other essential functions of the State, such as territorial integrity and the maintenance of public order.

In accordance with the duty to state reasons imposed on the administration and the legislator[24], including the EU and Member States when applying EU law, as well as the right to good administration conferred on individuals under EU law (Article 41(2)(c) of the Charter of Fundamental Rights of the European Union), any legal act must provide a compelling justification for its intervention. This enables citizens and businesses to ascertain whether the limits of competence have been exceeded and allow them to exercise their right to judicial review. It also enables the courts to conduct that review. This applies, of course, to the draft CSA.

According to consistent case law of the CJEU[25], mere generic considerations are insufficient to provide solid grounds for reviewing the legality of the legal act in a manner that ensures respect for the conferral, legal certainty and predictability principles. Similarly, the use of vague concepts, such as “HRS” or “country of risk” requires their objective components to be specified.

[24] According to Article 296, second paragraph, TFEU, "[l]egal acts shall state the reasons on which they are based”. See also inter alia, judgments of 4 July 1963, Case 24-62, *Germany v Commission*, para 69, and of 14 February 1990, C-350/88, *Delacre e.o. v Commission*, para 15.
[25] Vg., inter alia, 18 June 2015, C-583/13, Deutsche Bahn, paras 56, 60, 62, 63, 64, 65.

Proportionality and subsidiarity

The EC maintains that the proposed measure complies with the principle of proportionality because it does not go beyond what is necessary to achieve the intended objectives. According to the proposal, the scope of Union intervention does not preclude further national action in the field of national security. Therefore, Union action is justified from the perspectives of both subsidiarity and proportionality.

However, this reasoning is problematic. The Commission's argument reflects the typical minimum harmonisation logic, whereby EU legislation establishes a common baseline while allowing Member States to maintain or introduce higher standards. While this approach may be appropriate in areas of shared competence, it is clearly incompatible with Member States' exclusive competence in the field of national security.

According to Article 5(1), the limits of Union competences are governed by the principle of conferral". The principles of subsidiarity and proportionality supplement this principle by establishing the conditions that govern the exercise of these competences. In substance, under the principle of proportionality, the content and form of Union action must not go beyond what is necessary to achieve the objectives set out in the Treaties.

Accordingly, the Union may only act in a given policy area where:

(i) the action falls within the competences conferred upon it by the Treaties (principle of conferral, Article 5(2) TEU);

(ii) in areas of shared competence, the objectives of the proposed action cannot be sufficiently achieved by the Member States alone, but can be better achieved at Union level due to the scale or effects of the proposed action (principle of subsidiarity, Article 5(3) TEU); and

(iii) the content and form of the action are limited to what is strictly necessary to attain the pursued objectives (principle of proportionality, Article 5(4) TEU).

The central issue is not whether Member States are permitted to exceed the Union measure, but whether the Union can intervene at all, given that the proposal limits Member States' freedom to determine the appropriate level of intervention in areas that fall within their exclusive competence by setting a binding regulatory threshold.

Even the most minimal Union requirements necessarily limit the discretion of Member States and therefore constitute an intrusion into a domain reserved for them by the Treaties.

Consequently, the proposal risks creating a situation in which Member States are constrained by Union action that exceeds the Union's competence, failing to ensure an appropriate and proportionate balance between national security objectives and the requirements of the internal market.

Conclusion

The CSA2 proposal is bound to be the subject of lengthy discussions among the European institutions at the heart of the decision-

making process: the Council of Ministers, the European Parliament and the Commission. Several of its provisions are likely to be contested. Given the proposal's various weaknesses, it is unlikely that the outcome will align with the Commission's proposals.

At the core of the issue lies the division of competence between the Union and the Member States, which is particularly sensitive with regard to matters relating to national security.

By its very nature, a proposal on cybersecurity has the national security of EU Member States as its 'main predominant purpose' (Waste Directive, mentioned above). Therefore, it falls within their exclusive competence, provided that the main principles of EU law are respected, including fundamental rights and the essentials of the internal market. This implies that legal measures in this area must be duly motivated and subject to judicial review.

Article 114 TFEU provides a legal basis for internal market measures, which is an area of shared competence between the EU and the Member States. Therefore, it does not constitute an appropriate legal basis for a proposal such as the CSA2.

Furthermore, the use of concepts such as HRS and countries of risk, which are subject to the EC's discretionary assessment, may create great uncertainty.

By relying on the principle of proportionality, the EC is basing itself on a minimum harmonisation logic, which is appropriate for areas of shared competence. However, the EC is mistakenly introducing the principles of proportionality and subsidiarity when defining the limits of

EU intervention in areas outside its remit. By setting a binding regulatory threshold, the proposal limits the freedom of Member States to determine the appropriate level of intervention in areas that fall within their exclusive competence.

Sovereignty is therefore at the heart of the controversy that this proposal will inevitably cause. At the current stage of EU law development and in light of the current geopolitical turmoil, this could exacerbate tensions regarding the relationship between the national and EU levels. The reservations raised by some Member States and different organisations during discussions on the digital package, as well as during the discussions on the original CSA and the 5G Toolbox, are an expression of these tensions.

In the present circumstances, and considering the options presented in relation to the four pillars of CSA2 — ENISA, ECCF, simplified procedures (NIS2) and secure ICT supply chains — it would be advisable to achieve a legislative process that is less restrictive and more balanced, and that respects of the fundamental principles that govern the EU's constitutional architecture.

Lisbon, February 18, 2026