LEGAL OPINION

SUMMARY

This Opinion assesses the compatibility of the European Commission's proposed revisions to the European Union (EU) Cybersecurity Act, *The Cybersecurity Act 2* (Proposed Regulation),[1] with the law of the World Trade Organization (WTO) and focuses on Title IV, termed 'Security of ICT Supply Chains'.

My conclusions are as follows:

1. Title IV establishes two routes for designating specific entities, or categories of entities, as 'high-risk suppliers' of ICT products. Under the *third-country route* (Article 100 of the Proposed Regulation), the European Commission (Commission) may designate a third country, largely discretionarily, as posing specific cybersecurity risks, leading all suppliers connected to this country by establishment, ownership or control, to be labelled as high-risk suppliers. Under the *entity route* (Article 103(7)), the Commission may designate as high-risk suppliers, essentially discretionarily, individual entities established in third countries, affecting the designated entity and all entities controlled by that entity. 'EU suppliers', that is, suppliers that are wholly domestic EU entities – established in the EU, owned by EU nationals, and controlled by EU nationals and EU entities – are immune to designation under either route.

2. The designation of a supplier under either route results in:
   - (i) a ban on the use of the supplier's ICT components in key ICT assets in EU electronic communications networks, as well as in EU cybersecurity certified products and services, with components already installed subject to compulsory phasing out; the Commission may extend the ban to key ICT assets in all eighteen sectors identified under EU law as 'critical';
   - (ii) a ban from participation in EU-regulated public procurement and in EU-funded programmes (*direct ban*), as well as a ban from the supply of ICT components to participants in EU-regulated public procurement and in EU-funded programmes, for inclusion in key ICT assets (*indirect ban*);
   - (iii) the exclusion of the supplier from European cybersecurity certification and withdrawal of certificates it already holds, operating as a prohibition on supply wherever EU law or national law requires certification;
   - (iv) exclusion from accreditation as a conformity assessment body, from authorisation as an attestation provider, and from participation in standardisation activities.

[1] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (the Cybersecurity Act 2, CSA 2.0), Strasbourg, 20.1.2026, COM(2026) 11 final, 2026/0011 (COD).

3. As a matter of WTO law – and regardless of the implementation of any specific designations – the Proposed Regulation alters the conditions of competition on the EU market in favour of EU suppliers. It therefore is in breach of the most-favoured-nation and national treatment obligations of the EU under the *General Agreement on Tariffs and Trade 1994* (GATT 1994) Articles I:1 and III:4 and the *General Agreement on Trade in Services* (GATS) Articles II:1 and XVII:1. Additionally, the restrictions and procedures also violate the EU's market access commitment under GATS Article XVI:2(f) and the *Services Domestic Regulation* commitments inscribed in the EU's Schedule.

4. Furthermore, the prohibitions on the use of designated suppliers' ICT components by entities established in the EU are trade-related investment measures inconsistent with Article 2.1 of the *Agreement on Trade-Related Investment Measures* (TRIMs Agreement). Also, in markets from which designation removes the principal non-EU participants, this removal may also violate Article 3.1(b) of the *Agreement on Subsidies and Countervailing Measures* (SCM Agreement).

5. Finally, the bar on applying for or holding a European cybersecurity certificate, and the mandatory withdrawal of certificates already held, are inconsistent with Articles 5.1.1 and 5.1.2 of the *Agreement on Technical Barriers to Trade* (TBT Agreement) wherever Union or national law prescribes certification; and the exclusion from European standardisation is inconsistent with Article 4.1 of the TBT Agreement, since it requires standardising bodies to act contrary to paragraphs L and N of the *Code of Good Practice* in Annex 3 to the TBT Agreement.

6. The violations of the GATT and the GATS – and, by incorporation, those under the TRIMs Agreement – are not justified under the General Exceptions in those agreements (Articles XX and XIV respectively). The blanket supplier exclusions that Title IV introduces are more trade-restrictive than necessary to fulfil its objective. The Proposed Regulation itself outlines, as exceptions to the blanket exclusion, available alternatives: origin-neutral, conduct-based assessment and mitigating measures. Blanket exclusion on grounds unrelated to any supplier's conduct, from which EU suppliers presenting the same risk are exempt by law, without criteria, review or – on the entity route – any exemption, also amounts to arbitrary or unjustifiable discrimination between countries where the same conditions prevail.

7. The Security Exceptions under the GATT and GATS are equally unavailing. A standing, peacetime regime, adopted to preserve the proper functioning of the internal market, is not action taken in time of war or other emergency in international relations; and ICT components are neither implements of war nor goods supplied for provisioning a military establishment.

Title IV, if adopted as drafted, would entail violations of the EU's obligations across the GATT 1994, the GATS, the TBT Agreement, the TRIMs Agreement and possibly the SCM Agreement.

Amsterdam, 9 September 2026.

Geraldo Vidigal

Associate Professor, Public International Law and International Trade Law

Amsterdam Law School, University of Amsterdam

LEGAL OPINION

I. Scope of the Opinion

1. This Legal Opinion, requested by VVGB Advocaten, examines the compatibility with the law of the World Trade Organization (WTO) of the provisions of the European Union (EU)'s proposed revisions to its Cybersecurity Act (Proposed Regulation) governing the security of supply chains in information and communication technology (ICT) and, in particular, the designation and treatment of 'high-risk suppliers' under Title IV. The provisions examined are those of the Commission's legislative proposal of 20 January 2026.[2]

2. The core of this Opinion applies to any WTO Member whose suppliers are affected. Additionally, the modification in the conditions of competition produced by the Proposed Regulation will take place regardless of designation. The prospect that China and Chinese suppliers will be targeted under Title IV seems particularly significant, in light of the Commission's statements on the 5G Toolbox[3] and of the press release accompanying the Proposed Regulation.[4] Accordingly, where relevant, this Opinion will take into account normative texts and interpretations supported by both the EU and China.

3. Section II describes the relevant measures. Section III assesses the violations of the non-discrimination and market access commitments under the GATT and the GATS. Section IV assesses the possible invocation of the General and Security Exceptions. Section V identifies consequential violations of the TRIMs and SCM Agreements. Section VI examines possible violations of the TBT Agreement. Section VII concludes.

II. The Relevant Measures[5]

A. Two Routes to Designation as a 'High-Risk Supplier'

4. Article 2(39) of the Proposed Regulation provides two possibilities for an entity to be considered a 'high-risk supplier'. Pursuant to subparagraph (a), a third country may be designated as posing cybersecurity concerns under Article 100, affecting all entities established in or controlled by such a country, or owned or controlled by one of its nationals.[6] Pursuant to

[2] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (the Cybersecurity Act 2, CSA 2.0), Strasbourg, 20.1.2026, COM(2026) 11 final, 2026/0011 (COD).

[3] European Commission, Communication from the Commission – Implementation of the 5G cybersecurity Toolbox, 15 June 2023 (C(2023) 4049 final), p. 2 ('Huawei and ZTE represent in fact materially higher risks than other 5G suppliers').

[4] European Commission, Commission strengthens EU cybersecurity resilience and capabilities, Press Release, 20 January 2026 ('building on the work already carried out under the 5G security toolbox').

[5] Factual issues relevant to the opinion are discussed below.

[6] Although the provision itself does not refer to ownership, the identification of suppliers under Article 104 relies on ownership and control.

subparagraph (b), an entity may be designated separately by the Commission under Article 103(7), affecting all entities that it controls.

5. **The third-country route.** Under Article 100, the Commission may designate an entire third country as 'a country posing cybersecurity concerns to ICT supply chains' where it concludes that the country 'poses serious and structural non-technical risks to ICT supply chains'.[7] Article 100(1) lists five factors to be taken into account, none of which is determinative, and these factors do not exhaust the permissible criteria.[8] Once a country is designated, the Commission will map and list the suppliers connected to it, on the basis of their place of establishment and their ownership and control structure.[9] No supplier-specific conduct need be identified for a supplier to be listed.

6. **The entity route.** The entity route operates independently of any country designation. The application of Article 103(7) follows action under Article 103(6), applicable in 'exceptional circumstances, which justify an intervention to preserve the proper functioning of the internal market'. Where the Commission has 'sufficient reason to consider' that the components of a specific entity 'established in or controlled by a third country or entities from a third country, or a national from a third country' represent a significant non-technical cybersecurity risk for the economic or societal activities of at least three Member States, Article 103(6) requires the Commission to consult the Member States. The Commission may then adopt an implementing act prohibiting the use of the targeted entity's components in specified sectors considered to be critical.[10] The prohibition extends automatically to all entities controlled by the designated entity, wherever they are established.[11] The third country in question need not have been designated under Article 100, and the elements listed in Article 100(1) need not be verified. The entity route does not entirely dispense with the connection between a supplier and a third country. The procedure may only apply to entities 'established in or controlled by a third country or entities from a third country, or a national from a third country' – thus carving out EU-originating entities, i.e. entities established in the EU that are owned and controlled by EU nationals.[12]

---

[7] Proposed Regulation, Article 100(2). The verification may be triggered by a security risk assessment under Article 99 or where the risk 'appears' from 'other sources, such as a public statement on behalf of the Union or a Member State' (Article 100(1)).

[8] Proposed Regulation, Article 100(1), listing five elements to be 'tak[en] into account': third-country laws and practices requiring pre-disclosure of vulnerabilities to that country's authorities; the absence of effective judicial remedies and of independent and democratic control mechanisms; substantiated information about incidents involving threat actors controlled from that country, together with that country's unwillingness or inability to cooperate; and information from Union-level coordinated risk assessments or from Member States or international organisations.

[9] Proposed Regulation, Article 104(2)–(3). Under Article 104(4), where a supplier fails to provide requested information within the deadline, the Commission 'may conclude' that it is established in a designated third country or controlled by that country, its entities or its nationals, or that it is controlled by an entity designated under Article 103(7).

[10] Proposed Regulation, Article 103(7), first sentence. Pursuant to the same sentence, the sectors are those referred to in Annexes I and II to Directive (EU) 2022/2555.

[11] Proposed Regulation, Article 103(7), final sentence.

[12] Proposed Regulation, Article 103(6).

B. Risks Addressed by Title IV Designations

7. The two routes for supplier designation under Title IV refer to different risks. As regards the third-country route, Article 100(1) refers to 'the risk posed by [a] country', specifically 'a serious and structural non-technical risk to ICT supply chains'. The Proposed Regulation does not define this specific risk, although Article 2(42) defines 'non-technical risk' more broadly, as 'the likelihood of the supplier being subject to influence by a third country with the potential to cause loss or disruption of the service provided or to compromise the product manufactured by an entity or to lead to exfiltration of data, including for the purposes of espionage or revenue generation'.[13] As regards the entity route, Article 103(6) refers to 'a significant non-technical cybersecurity risk for the economic or societal activities of at least three Member States', originating from 'the use, installation or integration of ICT components or components that include ICT components from a specific entity established in or controlled by a third country or entities from a third country'. Article 2(43) defines 'a significant non-technical cybersecurity risk' as 'a non-technical cybersecurity risk which can be assumed to have a high likelihood to cause an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption'.[14]

8. The label 'non-technical' may be misleading. The risk that Article 2(42) identifies is 'loss or disruption of the service provided', the compromise of 'the product manufactured by an entity', or 'exfiltration of data'. These are technical events, occurring through technical channels. Elements of the Proposed Regulation address them as such: Article 103(2)(c) provides for third-party audited technical measures, among them on-device processing, the segmentation of network systems, the disabling of remote or physical access to key ICT assets and of non-essential features, operational network monitoring, and the testing of hardware and software; Article 103(2)(d) restricts operational control and the outsourcing of organisational functions.[15] Additionally, the security risk assessments that may lead to a designation under Article 100(1) rely primarily on technical risk factors, and only optionally on non-technical ones.[16]

9. The risk with which Title IV is concerned is accordingly, at least in meaningful part, a technical risk, with perhaps a non-technical cause. The risk itself can be identified, measured and mitigated by reference to the assets to be protected, and the Proposed Regulation mentions means of doing so. The consequences of this for the necessity of origin-based designations and supplier exclusions are considered in Section IV below.

---

[13] Proposed Regulation, Article 2(42).

[14] Proposed Regulation, Article 2(43).

[15] Proposed Regulation, Article 103(2)(c) and (d). Subparagraph (c) covers 'technical measures to be audited by a third party, including: (i) the use of on-device processing; (ii) specific segmentation of network systems; (iii) the disabling of any remote or physical access to key ICT assets; (iv) the disabling of non-essential features; (v) operational network monitoring; (vi) testing of hardware and software'. Subparagraph (d) covers 'restrictions related to operational control, including outsourcing of organisational functions to managed service providers'. Subparagraph (b) prohibits 'transfers of data to third countries and remote data processing from a third country'.

[16] Proposed Regulation, Article 99(1), cross-references Article 22 of Directive (EU) 2022/2555, which provides for coordinated risk assessments 'taking into account technical and, where relevant, non-technical factors'.

C. Consequences of Designation

10. Both third-country designations and entity designations result in affected entities being labelled 'high-risk suppliers' under the Proposed Regulation.[17] This is particularly relevant because, although Article 103(7) itself provides for selective, sector-specific prohibitions, various far-reaching prohibitions set out in other provisions in the Proposed Regulation apply to high-risk suppliers indiscriminately, thus impinging on their ability to supply ICT components in the EU market.[18] ICT components include all 'ICT products, ICT services or ICT processes that may be used in the operation of ICT assets'.[19]

11. Designating a supplier as a 'high-risk supplier' under the Proposed Regulation entails a number of consequences for the supplier:

a. The supplier is banned from supplying ICT components for key ICT assets in all electronic communications networks, be they mobile, fixed or satellite, and the supplier's components must be phased out from these networks' key ICT assets.[20]

b. The supplier is banned from supplying ICT components to holders of European cybersecurity certificates for inclusion in their certified ICT products, ICT services, ICT processes or managed security services identified by the Commission, 'for their entirety or parts thereof, as key assets'.[21]

c. The Commission may, by implementing act, ban ICT components supplied by the supplier from being used, installed or integrated in any form by entities in sectors designated as critical under EU law, either in key ICT assets or altogether.[22] The relevant sectors – currently, eighteen – are listed in Annexes I and II to Directive (EU) 2022/2555. They include energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration, and space (Annex I); and postal and courier services, waste management, chemicals, food, the manufacture of specified products, digital providers and research (Annex II).

d. The supplier is banned from (i) participating in EU-regulated public procurement, including both for critical infrastructure and for other large public procurement by EU Member States; as well as (ii) participating in programmes, procurement and activities funded with the EU budget. The supplier is also banned from supplying ICT components to be used, installed or integrated in 'key ICT assets' by participants in these procedures and programmes.[23]

---

[17] Proposed Regulation, Article 2(39).
[18] This is provided expressly in Article 103(9) of the Proposed Regulation. It is also a direct consequence of the definition of 'high-risk supplier' in Article 2(39) encompassing both entities designated under the entity route and entities affected through the third-country route.
[19] Proposed Regulation, Article 2(33).
[20] Proposed Regulation, Articles 111(1), 110(2).
[21] Proposed Regulation, Article 85(9).
[22] Proposed Regulation, Articles 103(7), 103(1). The Commission may determine, alternatively or additionally, the adoption of mitigation measures (Proposed Regulation, Articles 103(2), 103(8)).
[23] Proposed Regulation, Articles 100(4)(e), 100(4)(f).

e. The supplier is banned from participating in EU processes concerning standards or standardisation in the area of cybersecurity, be it at the stage of development, assessment, consultation, or decision-making.[24]

f. The supplier is banned from holding European cybersecurity certificates or becoming an accredited conformity assessment body capable of issuing such certificates, within the European Cybersecurity Certification Framework.[25]

g. The supplier is banned from becoming an authorised attestation provider of European individual cybersecurity skills.[26]

12. As regards the ban on European cybersecurity certification, Article 71(3) of the Proposed Regulation provides that 'European cybersecurity certification shall be voluntary, unless otherwise specified in Union or national law'.[27] Whether the bar in Article 100(4)(b) operates as a commercial disadvantage or as a prohibition on supply therefore depends on the specific EU or national regulation of the market segment in question. Currently, at least three instruments impose, or may come to impose, a requirement of European cybersecurity certification. Under the European Digital Identity Framework, certification is already mandatory for European Digital Identity Wallets, at present through national schemes covered by the EUCC, and a European scheme is in preparation.[28] Under Article 8(1) of the Cyber Resilience Act, the Commission may by delegated act require certain products to obtain a European cybersecurity certificate at assurance level at least 'substantial'.[29] And, under Article 24 of Directive (EU) 2022/2555, Member States may require essential and important entities to use certified ICT products, ICT services and ICT processes, and the Commission may by delegated act specify the categories of entities required to do so or to hold a certificate.[30]

13. Wherever certification is required, the bar in Article 100(4)(b) is not a procedural or reputational disadvantage but a ban on supply to relevant segments of an ICT supplier's market. The withdrawal of the certificate of all entities designated as high-risk suppliers, required by

---

24 Proposed Regulation, Article 100(4)(a).

25 Proposed Regulation, Article 100(4)(b), (c). Article 100(4)(b) bars a high-risk supplier from 'apply[ing] for or be[ing] a holder of' any European cybersecurity certificate; Article 100(4)(c) separately bars it from 'becom[ing] accredited conformity assessment body'. The European Cybersecurity Certification Framework is established in Title III of the Proposed Regulation (Articles 71-97).

26 Proposed Regulation, Articles 100(4)(d), 21(4). The attestation scheme for individual cybersecurity skills is established in Title II, Section 4 of the Proposed Regulation (Articles 19-23).

27 Proposed Regulation, Article 71(3). Article 1(2) provides that the certification framework 'applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification'.

28 Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, Article 5(c). See Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024, laying down the certification requirements for European Digital Identity Wallets and referring, for cybersecurity, to national certification schemes covered by the EUCC. A candidate European scheme for the certification of these wallets was submitted for public consultation in April 2026. See https://certification.enisa.europa.eu/publications/draft-candidate-eudiw-scheme-v04614-public-review_en.

29 Regulation (EU) 2024/2847, Article 8(1). The product must have the core functionality of a category set out in Annex IV to this regulation. The delegated act may be adopted only where a scheme covering the categories concerned has been adopted and is available to manufacturers, and must provide for a transitional period of at least six months.

30 Directive (EU) 2022/2555, Article 24(1) and (2). The Commission may adopt delegated acts under Article 24(2) 'where insufficient levels of cybersecurity have been identified'.

Article 100(5), means that designation alone converts a lawful market operator into a banned supplier in markets where certification is required.[31] And, whether or not certification is expressly designated as compulsory, Article 85(9) precludes every holder of a European cybersecurity certificate from using, installing or integrating a high-risk supplier's components in its certified products, services and processes identified as key assets. The designated supplier is thereby banned from the certified segment of the downstream market whenever its customer needs to, or elects to, be certified.

14. Under the country designation route (but not under the entity designation route), a designated supplier may seek relief from some of the consequences set out above. Even then, relief is not an entitlement. The applicant must demonstrate with clear evidence that effective mitigating measures will be put in place. The Commission may then decide on the matter, within nine months, through a highly discretionary assessment that includes whether an exemption 'would not be detrimental to the Union's interest'. In case of an affirmative decision, the Commission may attach conditions, limit the exemption in time, and withdraw it on its own initiative.[32]

D. The Measure as Such

15. Neither Article 100 nor Article 103(7) requires the Commission to designate any country or any entity. It does not follow that the inconsistencies identified below arise only upon designation. The discretion that these provisions confer may be exercised only against suppliers satisfying an origin condition, and can never be exercised against a wholly EU-originating supplier. This feature arguably already modifies the conditions of competition vis-à-vis third country suppliers. This Opinion accordingly addresses both the provisions as such and their foreseeable application.

III. Non-discrimination and Market Access Commitments under the GATT and the GATS

A. Non-Discrimination Obligations – GATT 1994

16. The bans and other restrictions above are incompatible with the EU's key obligations under the GATT 1994 that 'prohibit discrimination among like products originating in or destined for different countries'[33] to the prejudice of products from a WTO Member. GATT Articles I:1 (Most-favoured Nation Treatment) and III:4 (National Treatment) prohibit regulatory measures that impair the competitive conditions of a WTO Member's products, compared, respectively, to the like products from other third countries and to like domestic

[31] Proposed Regulation, Article 100(4)(b) (a high-risk supplier may not 'apply for or be a holder of' any European cybersecurity certificate) and Article 100(5) (certificates already obtained 'shall [be] withdraw[n] … without undue delay'). Article 85(11) enlists the certification machinery in enforcing the ban.

[32] Proposed Regulation, Article 105(2)–(8).

[33] Appellate Body Report, *Canada – Autos*, para. 84 (with respect to Article I).

products.[34] The prohibitions on the supply, use, installation and integration of components are internal regulations affecting the internal sale, purchase and use of the imported components within the meaning of Article III:4. Most recently, the Panel in *EU – Palm Oil (Indonesia)* noted that 'Article III:4 covers not only laws and regulations which directly govern the conditions of sale or purchase but also those which might adversely modify the conditions of competition between domestic and imported products'.[35] A categorical prohibition on the use of imported components, while like domestic components and components from other importers remain freely usable, is an extreme modification of those conditions for the markets in which it applies.

17. The fact that the direct targets of the measure are suppliers rather than products does not alter the existence of discrimination. The legal effect of designating as 'high-risk suppliers' either entire third countries or specific third-country entities is that every product that every affected entity supplies will be excluded from certain or all EU markets. The expected result is a modification of the applicable competitive conditions, to the detriment of all imported products supplied by the designated supplier, and the consequent advantage of like EU-originating products and products supplied by non-designated suppliers.[36] In *Canada – Autos*, the Appellate Body found that a benefit accorded to motor vehicles 'imported by a limited number of designated manufacturers who are required to meet certain performance conditions' violated GATT Article I:1, because it failed to extend the same advantage 'immediately and unconditionally to like motor vehicles of *all* other Members'.[37] In *EC – Bananas III*, the Appellate Body concluded that the restricted distribution of hurricane-related import licences to certain market operators created 'an incentive for operators to purchase bananas of [EU] origin', thus violating Article III:4.[38]

18. **The third-country route.** The designation of a WTO Member under Article 100 is origin-based discrimination in its most direct form. The eligibility of an ICT component to be marketed in the EU so that it can (a) be used in infrastructure projects and incorporated in key ICT assets, (b) be supplied within EU-regulated procurement and EU-funded programmes, and (c) be contained in a product holding a European cybersecurity certificate, is in each case an 'advantage' within the meaning of Article I:1 and 'favourable treatment' under Article III:4. Upon designation, market access is withdrawn from the products of entities established in, or

---

[34] GATT Article III:4 applies 'in respect of all laws, regulations and requirements affecting … internal sale, offering for sale, purchase, transportation, distribution or use'. Article I:1 applies, among others, 'with respect to all matters referred to in paragraphs 2 and 4 of Article III'.

[35] Panel Report, *EU – Palm Oil (Indonesia)*, para. 7.1010. Under the GATT, the justifiability of discrimination must be argued under Article XX, examined in Section IV, rather than under Articles I and III:4 (Appellate Body Report, *EC – Seal Products*, para. 5.125).

[36] Where a measure distinguishes exclusively on the basis of origin, likeness may be presumed: Panel Report, *US – Poultry (China)*, para. 7.424 ('when origin is the sole criterion distinguishing the products, it has been sufficient for a complainant to demonstrate that there can or will be domestic and imported products that are "like"'). Under Article 103(7), origin is a necessary but not a sufficient condition of designation, so that the presumption may be unavailable and likeness would have to be established on the four ordinary criteria: '(i) the properties, nature and quality of the products; (ii) the end-uses of the products; (iii) consumers' tastes and habits – more comprehensively termed consumers' perceptions and behaviour – in respect of the products; and (iv) the tariff classification of the products' (Panel Report, *US – Poultry (China)*, para. 7.425).

[37] Appellate Body Report, *Canada – Autos*, para. 85.

[38] Appellate Body Report, *EC – Bananas III*, para. 212.

owned or controlled by nationals of, the designated Member, while remaining available to like products of every other origin. Because the consequences follow *ipso jure* from the listing, and because the listing turns on nothing but the supplier's connection to the designated Member, the discrimination is *de jure* origin-based, in the manner of the funding restriction condemned in *US – Poultry (China)*.[39] The availability of a discretionary exemption under Article 105 does not eliminate the advantage and more favourable treatment held by an entity not designated – and, in the case of EU-originating entities, not subject to designation. Additionally, the time it takes for such an exemption to be determined – a time during which the supplier's ICT components would be banned – might itself lead purchasers to rule out purchasing from suppliers that they assess to be liable to designation in the future.

19. **The entity route.** Where a single entity is designated under Article 103(7), the discrimination is not effected against the suppliers of a Member as a class. The inconsistency nonetheless arises, for two reasons. First, the products of the designated supplier are denied advantages that remain available to like products of every other origin, including like products of EU origin, so that the ordinary standards of Articles I:1 and III:4 apply, covering discrimination in fact as well as in law.[40] Secondly, and independently, the exposure of third-country suppliers to designation is itself a modification of the conditions of competition. Only suppliers satisfying the origin condition may be designated at all; EU-established, EU-controlled suppliers are immune as a matter of law. In *Canada – Autos*, the Panel found that Article III:4 creates 'an obligation addressed to governments to ensure effective equality of competitive opportunities between domestic and imported products'.[41] In addition to the discriminatory effects of a concrete designation under Article 103(7), the very regime under which every foreign-controlled supplier of ICT components stands permanently exposed to an unreviewable and unexemptible prohibition, while its EU-controlled competitors do not, modifies the conditions of competition in favour of EU suppliers whether or not any designation is concretely made.

20. As a final note, as regards EU-regulated procurement, GATT Article III:8(a) may permit the EU and its Member States to discriminate when procuring ICT equipment for their own use.[42] It does not permit imposing discriminatory conditions on the components used by all participants in procurement within the EU. The derogation in Article III:8(a), for 'procurement by governmental agencies of products purchased for governmental purposes and not with a view to commercial resale', is doubly confined. It exempts only discrimination as regards the products procured and products in a competitive relationship with them, and does not authorise requiring contractors to discriminate in their purchase of inputs;[43] and

[39] Panel Report, *US – Poultry (China)*, para. 7.431 ('[t]he funding restriction imposed … is origin-based in respect of the products it affects … By targeting only China, [the budget rule] imposes origin-based discrimination').

[40] Appellate Body Report, *Canada – Autos*, para. 78 ('Article I:1 covers also "in fact", or de facto, discrimination').

[41] Panel Report, *Canada – Autos*, para. 10.84.

[42] This refers to the prohibitions in Proposed Regulation, Article 100(4)(e) and (f). The argument does not apply to the prohibitions in Articles 85(9), 103(1), 103(7) and 111.

[43] Appellate Body Report, *Canada – Renewable Energy*, paras. 5.56–5.79; Appellate Body Report, *India – Solar Cells*, para. 5.36 ('in order for Article III:8(a) to apply, the product purchased should always be in a competitive relationship with the product discriminated against').

'procurement' requires governmental acquisition, which 'cannot be equated with merely financing or regulating the acquisition of products'.[44]

21. In sum, a designation under either route would modify the competitive conditions to the detriment of affected third-country suppliers, violating Articles I:1 and III:4 of the GATT 1994.[45] The very fact that an entity's designation is possible alters the competitive conditions between products supplied by third-country entities liable to designation under the Proposed Regulation – whose products, in case of designation, must be 'phased out'[46] – and products supplied by EU entities, for which designation is impermissible under the very terms of the regulation.

B. Restrictions on the Supply of Services – GATS

22. The GATS applies to 'measures by Members affecting trade in services',[47] including measures that do not have services as their primary focus. The GATT and the GATS apply simultaneously to, and may both be violated by, measures involving a service relating to, or supplied in conjunction with, a particular good.[48] The GATS expressly provides that trade in services takes place when juridical persons are established in a WTO Member to provide services through commercial presence (or could be so established) and are owned or controlled by another WTO Member's nationals or legal persons.[49]

Most-Favoured-Nation Treatment and National Treatment

23. The GATS non-discrimination obligations are similar to those in the GATT but with some important distinctions. First, both obligations involve the same legal standard: 'treatment no less favourable', encompassing the modification of the conditions of competition 'to the detriment of like service or service suppliers of any other Member'.[50] Second, under the GATS, 'likeness' involves both 'like services' and 'like service suppliers'.

24. GATS Article II:1 – the Most-Favoured-Nation Treatment obligation – requires that services and service suppliers of all WTO Members be accorded, immediately and unconditionally, treatment no less favourable than that accorded to like services and service suppliers of any other country. The obligation applies across all sectors and modes of supply, irrespective of specific commitments, subject only to exemptions recorded in 1994. None of the EU's exemptions appear relevant.[51] The prohibitions on entities determined to be connected to a designated Member or designated under Article 103(7) – on holding and issuing certificates, on accreditation, on participation in standardisation activities, on supplying

[44] Award of the Arbitrators, *Turkey – Pharmaceutical Products*, para. 6.58, upholding Panel Report, *Turkey – Pharmaceutical Products*, paras. 7.104–7.107.

[45] In WTO litigation, both 'likeness' among products and disparities in treatment may need to be demonstrated concretely. See footnote 36.

[46] Proposed Regulation, Articles 110(2), 103(7).

[47] GATS, Article I:1.

[48] Appellate Body Report, *EC – Bananas III*, paras. 220–221.

[49] GATS, Article XXVIII(m)(ii) and (n).

[50] Appellate Body Report, *Argentina – Financial Services*, para. 6.115.

[51] See WTO, *European Communities and their Member States – Final List of Article II (MFN) Exemptions*, 15 April 1994 (GATS/EL/31).

installation, maintenance and managed-security services to operators of key ICT assets – constitute less favourable treatment than that accorded to like service suppliers not subject to these prohibitions. The conditional and discretionary recovery of those opportunities under Article 105, where possible at all, is not treatment accorded 'immediately and unconditionally'.

25. In sectors in which the EU has undertaken specific commitments, the designation also violates Article XVII:1 (the GATS' National Treatment obligation). A number of committed sectors are foreseeably affected, under Mode 1 (cross-border supply, including electronic supply), Mode 3 (commercial presence) and Mode 4 (presence of natural persons). Examples, with the corresponding commitments, are set out in Table 1.

Table 1 – EU services commitments and services affected by the Proposed Regulation[52]

Service	Examples of affected supply	EU Market access *	EU National treatment *	CPC
Consultancy services related to the installation of computer hardware	Advice on the configuration of ICT hardware for key ICT assets, supplied cross-border or electronically (Mode 1) or through a foreign-controlled subsidiary established in the EU (Mode 3).	Full access	Full national treatment	841
Software implementation services	Systems analysis, design, programming and maintenance of software incorporated in key ICT assets – supplied cross-border or electronically (Mode 1), through a foreign-controlled subsidiary (Mode 3), or by technicians present on-site (Mode 4**).	Full access	Full national treatment	842
Data processing services	Remote data processing and hosting, including processing carried out from outside the EU (Mode 1), or through a foreign-controlled subsidiary established in the EU (Mode 3).	Full access	Full national treatment	843
Database services	Provision and management of databases, supplied cross-border or electronically (Mode 1) or through a foreign-controlled subsidiary (Mode 3).	Full access	Full national treatment	844
Maintenance and repair of office machinery and equipment, including computers	Maintenance and repair of computers and office machinery – whether remote (Mode 1), through a foreign-controlled subsidiary (Mode 3), or by technicians present on-site (Mode 4**).	Full access	Full national treatment	845
Other computer services (including managed-security and monitoring services)	Managed-security services, monitoring and remote diagnostics, supplied cross-border or electronically (Mode 1) or through a foreign-controlled subsidiary (Mode 3).	Full access	Full national treatment	849

[52] WTO, *European Union – Schedule of Specific Commitments*, 7 May 2019 (GATS/SC/157). The supply of other services may also be affected by the Proposed Regulation and Title IV designations.

Service	Examples of affected supply	EU Market access *	EU National treatment *	CPC
Technical testing and analysis services (conformity assessment and certification)	Testing, inspection and certification of ICT products – the commercial conformity-assessment and attestation layer – supplied cross-border (Mode 1), through a foreign-controlled subsidiary (Mode 3), or by assessors present on-site (Mode 4**).	Full access	Full national treatment	8676

* The schedule text states 'None', designating a commitment to provide full market access and national treatment (with no limitations). Some EU Member States have individual limitations in certain sub-sectors.

** Mode 4 is committed only for the categories set out in the horizontal section of the EU's Schedule – principally intra-corporate transferees, business visitors, and contractual service suppliers and independent professionals in listed activities. It is otherwise unbound.

26. Where full national treatment is required under its schedule, the EU must accord to services and service suppliers of all WTO Members treatment no less favourable than that accorded to its own like services and service suppliers.

27. Establishing comparability under the GATS requires establishing that there are 'like services' provided by 'like service suppliers'. If origin is the only factor on which a measure bases a difference in treatment, the 'like service suppliers' requirement can be met, provided that there can be domestic and foreign suppliers that are the same in all material respects except for origin.[53] In *Argentina – Financial Services*, the Appellate Body noted that the presumption might not apply where a distinction among service providers originating in different WTO Members is 'not based on "origin per se", but on "the regulatory framework inextricably linked to such origin"'.[54] Although the wording used by the Appellate Body was inconclusive, it would be prudent for a complainant raising the breach of the non-discrimination obligations in WTO dispute settlement to identify specific services and service suppliers and demonstrate their 'likeness'. The Appellate Body found that 'the fundamental purpose of the comparison to be undertaken in order to determine "likeness" in the context of trade in services [is] to assess whether and to what extent the services and service suppliers at issue are in a competitive relationship'.[55]

28. In case of designation under the Proposed Regulation, affected suppliers will be prevented from supplying their like services in the EU in a variety of ways. These suppliers are banned directly, under the prohibitions applicable to affected suppliers (precluding provision of services by them, as well as purchase of their services by others). Their services may also be banned from markets indirectly, through their own exclusion from providing certification, accreditation and attestation services, or because others are prohibited from purchasing services from non-certified entities (or even become wary of purchasing them from entities perceived as liable to designation). Finally, an entity whose products a services supplier specialises in servicing – a common configuration in ICT markets, where purchasers are frequently required, contractually or technologically, to obtain servicing from the equipment supplier or entities it designates – may be barred from supplying those products. In *EC – Bananas III*, a licensing

[53] Panel Report, *China – Publications and Audiovisual Products*, para. 7.975.

[54] Appellate Body Report, *Argentina – Financial Services*, para. 6.56.

[55] Appellate Body Report, *Argentina – Financial Services*, para. 6.34.

system allocating the vast majority of licences to operators based in the EU or in specified countries was found to violate both the most-favoured-nation and the national treatment obligations of the GATS.[56] Through a different path – exclusion rather than inclusion – the designation of high-risk suppliers modifies the conditions of competition to the detriment of the affected service suppliers.

Market Access

29. For services in which full market access is scheduled, GATS Article XVI:2 imposes specific prohibitions on limiting WTO Members' market access. Two prohibitions are relevant.

30. Most directly, subparagraph (f) prohibits 'limitations on the participation of foreign capital in terms of maximum percentage limit on foreign share-holding or the total value of individual or aggregate foreign investment'. The provision covers limitations on the participation of capital belonging to, or coming from, another Member, and is 'specifically concerned with limitations tied to the fact that the capital originates outside the Member adopting the limitation'.[57] The designation of a third country under Article 100 entails a prohibition on the supply of services by entities controlled by that country, its entities, or its nationals. The outcome is a maximum threshold for the participation of capital from a designated country; the country, its nationals and entities may not hold controlling participation in suppliers of ICT products without entailing an exclusion of these suppliers.[58] That the limitation is framed negatively, as a prohibition on supply by (certain) foreign-controlled entities, rather than as an affirmative national ownership requirement does not make it less incompatible with subparagraph (f).

31. Additionally, subparagraph (a) prohibits limitations on the number of service suppliers in the form of numerical quotas, monopolies, exclusive service suppliers or economic needs tests. In *US – Gambling*, the Appellate Body found that this provision covers 'limitations that are, in form *or in effect*, monopolies or exclusive service suppliers'.[59] Where designation of countries and entities results in a market in a committed sector being left with a single supplier or a closed set of suppliers, subparagraph (a) is arguably violated 'in effect'.

Domestic Regulation

32. The *Services Domestic Regulation* disciplines have been inscribed in the EU's Schedule and apply in every sector in which the EU has undertaken specific commitments, including all those in Table 1.[60] Two of the disciplines bear directly on the design of Title IV designations. Measures relating to authorisation for the supply of a service must be 'based on objective and transparent criteria', and the procedures must be impartial and 'adequate for applicants to

[56] Appellate Body Report, *EC – Bananas III*, paras. 240–248.

[57] Panel Report, *EU – Energy Package*, paras. 7.709 and 7.712.

[58] Proposed Regulation, Article 104(3) requires the Commission to 'assess the place of establishment as well as the ownership and control structure of the suppliers'.

[59] Appellate Body Report, *US – Gambling*, para. 230 (emphasis in the original).

[60] The *Services Domestic Regulation* commitments were inscribed in participants' schedules and certified with full legal effect from 27 February 2024: *European Union – Schedule of Specific Commitments Supplement 1*, 27 February 2024 (GATS/SC/157/Suppl.1), *Disciplines on Domestic Regulation*.

demonstrate whether they meet the requirements'.[61] Under Title IV, the criteria for authorising – or rather, for not prohibiting – the supply of a service relate to the supplier's national connections. The Article 104 procedure for 'identification of high-risk suppliers' – applicable both to the third-country route and to the entity route[62] – turns entirely on a supplier's 'place of establishment … ownership and control structure', rather than on any conduct, or any risk it may present.[63] Under Article 105, a Commission decision may exempt a supplier from some of the consequences of its designation. This Commission decision is not, however, 'based on objective and transparent criteria', instead featuring criteria that grant the Commission a large degree of discretion in making its decision.[64]

33. Finally, Members are to encourage their competent authorities to adopt technical standards 'developed through open and transparent processes'.[65] While this is an obligation of conduct rather than of result, a measure requiring the exclusion of interested suppliers from the development of such standards runs directly counter to the object and purpose of this obligation.

IV. Possible Justifications under the GATT and GATS Exceptions

A. General Exceptions

34. In WTO law, the General Exceptions may be invoked as a matter of legal right. However, as cautioned by the Appellate Body, 'the chapeau is animated by the principle that while the exceptions of Article XX may be invoked as a matter of legal right, they should not be so applied as to frustrate or defeat the legal obligations of the holder of the right under the substantive rules of the General Agreement'.[66] Article XX of the GATT and Article XIV of the GATS may be read in parallel.[67] In either case, three questions arise: whether cybersecurity is an objective protected under the General Exceptions; whether the measures are 'necessary' to protect it at the level the EU has chosen; and whether they constitute arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade.

35. **Legitimate objective.** Cybersecurity does not feature among the objectives that can be pursued under GATT Article XX or GATS Article XIV. In practice, WTO Panels and the Appellate Body have accepted a variety of objectives as (at least potentially) falling under the

---

[61] *Disciplines on Domestic Regulation*, paragraph 22(a) and (b).

[62] Proposed Regulation, Article 104(1).

[63] Proposed Regulation, Article 104(3).

[64] Proposed Regulation, Article 105(4). In the absence of objective and transparent *criteria*, the fact that this provision mandates 'a fair and transparent process' carries little weight.

[65] *Disciplines on Domestic Regulation*, paragraph 21.

[66] Appellate Body Report, *US – Gasoline*, pp. 18 and 22. See also Appellate Body Report, *US – Shrimp*, para. 121.

[67] Appellate Body Report, *US – Gambling*, para. 291.

scope of Article XX.[68] The invocation of any of the available provisions is subject to the same two requirements: the necessity of the measure and compliance with the chapeau.[69]

36. **Necessity.** To be 'necessary', a measure must make a contribution to the fulfilment of its objective that cannot be made by an available, less trade-restrictive measure. An argument that a measure is not necessary therefore often turns on identifying an alternative that is less trade-restrictive, reasonably available, and capable of making an equivalent contribution to its objective.[70] In *China – Audiovisual Products*, the Appellate Body explained that, in a 'necessity' assessment, 'a panel must examine whether the responding party could reasonably be expected to employ an alternative measure, consistent (or less inconsistent) with the covered agreements, that would achieve the objectives pursued by the measure at issue'.[71]

37. The objective of the Proposed Regulation must be characterised at the level of the risk rather than of the proxy chosen to address it. An analysis of the Proposed Regulation shows that its objective is to reduce the risk that ICT components in key assets may be exploited to compromise the confidentiality, integrity or availability of essential networks. In this regard, the Preamble of the Proposed Regulation provides examples of 'risks of a non-technical nature':

> …non-technical risks may be linked, but not limited, to the jurisdiction to which a supplier of certain components is subject, in particular where a third country or threat actors controlled from that country engage in economic espionage, carry out malicious cyber activities or campaigns against the Union or its Member States, or engages in irresponsible State behaviour in cyberspace. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. For instance, kill switches could be used to negatively impact the availability of communication networks and electricity grids.[72]

38. Addressing these risks and vulnerabilities – economic espionage, malicious cyber activities, irresponsible behaviour, backdoors, supply disruptions, kill switches – constitutes

---

[68] WTO Panels have accepted as objectives covered by these provisions objectives as varied as social inclusion and access to information (Panel Report, *Brazil – Taxation*, para. 7.602), the prevention of misappropriation and unfair competition (Panel Report, *US – Tariff Measures*, para. 7.140), the reduction of over-reliance on imported pharmaceutical products (Panel Report, *Turkey – Pharmaceutical Products*, para. 7.177), and the collection of tax revenue (Panel Report, *Dominican Republic – Cigarettes*, para. 7.215).

[69] I consider that the EU might conceivably invoke GATT Article XX(a), (b) or (d), and GATS Article XIV(a), (b) or (c)(iii). Invoking any of these provisions requires demonstrating the necessity of the measure and compliance of its application with the chapeau.

[70] Panel Report, *EU – Palm Oil (Indonesia)*, para. 7.384 (an alternative must 'be less trade-restrictive, be reasonably available, and make an equivalent contribution to the objective'); Appellate Body Report, *Brazil – Retreaded Tyres*, para. 232.

[71] Appellate Body Report, *China – Audiovisual Products*, para. 318 (with respect to Article XX(a)). See also Appellate Body Report, *Korea – Beef*, paras. 165-166 (under Article XX(d)); Appellate Body Report, *EC – Asbestos*, paras. 171-172 (under Article XX(b)).

[72] Proposed Regulation, Preamble, Recital 129.

the Proposed Regulation's ascertainable objective, whether at the origin of the exploitation lies the supplier itself, a State exercising influence over it, or a malicious actor.

39. Once the objective of the Proposed Regulation is characterised in this way, the extreme trade-restrictiveness of Title IV, applied largely discretionarily and directed at specific third-country entities and third countries, becomes unjustifiable under the requirement of necessity. Less trade-restrictive, and less discriminatory alternatives are not merely reasonably available but are stated in the Proposed Regulation itself. Article 103(2) empowers the Commission to, among others, require, in respect of the same key ICT assets and on the basis of the same risk assessments, transparency as to the identity of suppliers, prohibitions on data transfers to and remote processing from third countries, third-party audited technical measures including on-device processing, network segmentation, the disabling of remote access and of non-essential features, operational monitoring and the testing of hardware and software, restrictions on operational control and on outsourcing, restrictions on contractual relations, the vetting of personnel by national authorities, and the diversification of supply.[73] Article 103(2)(c) requires the technical measures it prescribes to be 'audited by a third party', and Article 103(2)(f) provides for the personnel operating the service to be vetted by the national competent authorities. Verification is thus a component of the alternative as the Commission has legislated it. If third-party audit is an adequate means of establishing compliance when the Commission imposes these measures, it must be an adequate means of establishing compliance when a supplier offers them.

40. Importantly, none of these alternative less restrictive measures depends on the origin, ownership or control of suppliers. They address the risk directly rather than through a proxy, and they are available whether or not any country or entity has been designated. Thus, the alternatives featuring in the Proposed Regulation itself would be able to address each of the harms by which the Proposed Regulation itself defines the risk it seeks to avert.

41. One issue is whether measures of this kind are incapable of addressing the 'non-technical' element of the risk – the specific risk that 'influence by a third country' engenders the relevant harms. In this regard, Article 105(2)(b) imposes on an applicant for exemption the duty to demonstrate precisely, 'with clear evidence', that 'effective mitigating measures will be put in place to address non-technical risks and ensure the absence of any possible exercise of undue interference'.[74] The Proposed Regulation thus concedes the possible efficacy of the alternative, but withholds from designated or affected entities the right to demonstrate it before their exclusion; exemptions are unavailable altogether on the entity route, and discretionary on the third country route.

42. A similar excessiveness of the means chosen appears from the Commission's own explanation of the European cybersecurity certification framework. The Explanatory Memorandum provides that the regulation 'ensures that the proportionality principle is respected' because 'certification remains voluntary and can help entities demonstrate

[73] Proposed Regulation, Article 103(2)(a)–(g).

[74] Proposed Regulation, Article 105(2)(b).

compliance with Union's cybersecurity requirements'.[75] Under Title IV, however, the favoured path is outright exclusion of designated entities – either by reference to country of establishment and nationality of control or following the Commission's discretionary determination – rather than a requirement of demonstration of compliance with EU cybersecurity requirements.

43. Two further features are evidence of a lack of necessity. First, the exclusion by law of EU-controlled suppliers limits the contribution that the measure can make: a critical supply chain may remain fully exposed to risky influences – including by a third country – provided that the exposure runs through an EU-established and EU-controlled entity. In the absence of clear evidence of contribution, restrictiveness with respect to specific Members weighs against a finding of necessity.[76] So does a compliance system whose burden disproportionately falls on imported products and their suppliers.[77] Secondly, on the entity route the Commission is not required to assess the availability of alternative suppliers or the economic and societal impacts of a prohibition, nor to review it at any interval. A highly restrictive measure is thus ostensibly adopted without any inquiry into less burdensome means, and maintained without any provision for reassessment on the basis of objective criteria.

44. **Arbitrary or unjustifiable discrimination.** Under the chapeau of both GATT Article XX and GATS Article XIV, measures may not be applied in a manner that entails arbitrary or unjustifiable discrimination between countries where the same conditions prevail. Discrimination is arbitrary or unjustifiable, even when a rational motive underlies a decision, where it 'is explained by a rationale that bears no relationship to the objective of a measure … or goes against that objective'.[78] That appears to be the position here, in three respects.

45. First, the criteria adopted are expressly discriminatory as regards origin. The country route excludes benign suppliers connected to a designated country while admitting suppliers of equal or greater actual risk connected to any other. The entity route may be used to target foreign-controlled suppliers while safeguarding EU-controlled suppliers that present, on the Proposed Regulation's own definition of the risk, an identical exposure. In *US – Shrimp*, the Appellate Body found unjustifiable discrimination in part because shrimp caught by methods identical to those employed in the United States were excluded solely because they had been caught in the waters of an uncertified country.[79]

46. Secondly, the procedures lack the transparency and procedural fairness that the chapeau requires. In *US – Shrimp*, the absence of 'certain minimum standards for transparency and procedural fairness in the administration of trade regulations' was itself sufficient to render the discrimination arbitrary.[80] In the Proposed Regulation, country designation rests on non-exhaustive and non-determinative criteria, and the entity designation rests on no specified

[75] Proposed Regulation, Explanatory Memorandum, under 'Proportionality'.

[76] See Panel Report, *Colombia – Ports of Entry*, para. 7.614.

[77] Appellate Body Report, *Korea – Beef*, para. 181 (regarding an enforcement procedure that disproportionately burdened 'imported goods and retailers of imported goods').

[78] Appellate Body Report, *Brazil – Retreaded Tyres*, para. 232.

[79] Appellate Body Report, *US – Shrimp*, para. 165.

[80] Appellate Body Report, *US – Shrimp*, paras. 181 and 183.

criteria at all. Moreover, a supplier is assessed on its ownership and control but not on the risk it poses; there is no reasoned determination of risk addressed to the supplier, no criterion by which the supplier might adjust its conduct, and – on the entity route – no review and no exemption.

47. Thirdly, the text and context of the Proposed Regulation suggest objectives other than the one asserted. The Preamble attributes the risk not only to concealed vulnerabilities or backdoors, which can be verified technically, but to 'potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency'.[81] The Preamble also invokes the *Joint Communication on Strengthening EU economic security*, whose stated aims include to 'develop the EU's internal capacity and capability' and to 'maintain and develop strategic manufacturing capacity and capabilities in the EU'.[82] These objectives would seem to require excluding the suppliers that are most successful in producing competitive ICT equipment. The high competitiveness of certain third-country suppliers – rather than any ascertainable conduct or identifiable risk in the products and services supplied – would thus appear to form part of the risks the measure was designed to address.

B. Security Exceptions

48. Besides the General Exceptions, both the GATT and the GATS feature dedicated Security Exceptions. Under GATT Article XXI(b) and GATS Article XIV*bis*:1(b), a WTO Member may take 'any action which it considers necessary for the protection of its essential security interests' in the circumstances set out in items (i)–(iii).[83]

49. Adopting, at the EU level, measures for the protection of essential security interests presents its own challenges as a matter of EU law. EU institutions are bound by Article 4(2) of the Treaty on the European Union, which provides that 'national security remains the sole responsibility of each Member State'. In *La Quadrature du Net*, the Court of Justice of the European Union (CJEU) noted that this sole responsibility 'encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities'.[84] The risks that the regulation purports to address seem to fall under this category and might be under the 'sole responsibility' of the individual EU Member States.

---

[81] Proposed Regulation, Preamble, Recital 129.

[82] *Joint Communication to the European Parliament and the Council, Strengthening EU economic security*, 3 December 2025, JOIN(2025) 977 final (referred to in Proposed Regulation, Preamble, Recital 130).

[83] GATT Article XXI(b); GATS Article XIV*bis*:1(b). There are debates among WTO Members regarding the overall meaning of the security exception. The European Union and China, in their arguments before panels that have examined this provision, agree that: (a) the security exceptions in subparagraph (b) apply solely in the circumstances set out in items (i)-(iii); (b) a Member's ample leeway to determine that specific measures are 'for the protection of' its essential security interests is constrained by the duty to apply treaties in good faith; and (c) WTO panels have jurisdiction to assess the justifiability of measures under the invoked security exception. See, e.g., Panel Report, *Russia – Traffic in Transit*, para. 7.41 (China), 7.43 (European Union); Panel Report, *US – Steel and Aluminium Products (China)*, Annex B-1, para. 85 (China); Annex C-2, paras. 43, 45 (European Union).

[84] CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others v. Premier Ministre and Others* (Judgment of 6 October 2020), para. 135.

50. Under WTO law, justifiability under the Security Exceptions requires three elements: one of the circumstances in items (i)-(iii) must objectively be present; the Member must articulate the essential security interests it is seeking to protect with some specificity; and, although each WTO Member may determine which action it considers necessary for the protection of its stated security interests, in light of the principle of good faith, the measures must 'meet a minimum requirement of plausibility in relation to the proffered essential security interests'.[85] The only item that has been subject to adjudication is item (iii), covering measures taken 'in time of war or other emergency in international relations'.

51. The Panel in *Russia – Traffic in Transit* defined an 'emergency in international relations' as a 'situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state'.[86] In this regard, 'political or economic differences between Members are not sufficient, of themselves, to constitute an emergency in international relations for purposes of subparagraph (iii)'.[87] In *US – Origin Marking (Hong Kong, China)*, tensions and mutual accusations that were the subject of concern at the international level, and to which a range of Members had adjusted policy settings, did not attain the requisite gravity.[88] In *US – Steel and Aluminium Products (China)*, international concern regarding global excess capacity did not either; and the Panel reasoned that concerns relating to the domestic situation of the industries in question did not bear on the existence of an emergency at all.[89]

52. Title IV of the Proposed Regulation would constitute a standing, peacetime regime of general application, whose designation mechanisms are not predicated on any rupture in the EU's relations with another Member. On the entity route this is express: the trigger is the preservation of 'the proper functioning of the internal market' in 'exceptional circumstances', an internal market objective rather than an international relations one.[90]

53. Absent an exceptional and serious crisis in the relations between the EU and the WTO Member concerned, a designation under Article 100 (or the designation of a supplier under Article 103(7) on the ground that it is subject to the influence of a WTO Member) is not action taken in time of an emergency in international relations. Even where such a crisis exists between two WTO Members, measures affecting nationals of WTO Members uninvolved in the relevant emergency may still be impermissible. In *Saudi Arabia – IPRs*, measures affecting intellectual property right-holders from WTO Members other than Qatar (with whom an emergency in international relations existed) were deemed 'so remote from, or unrelated to, the "emergency in international relations"' that they could not plausibly protect Saudi Arabia's security interests triggered by the emergency.[91] Similarly, an emergency in international

[85] Panel Report, *Russia – Traffic in Transit*, para. 7.138.
[86] Panel Report, *Russia – Traffic in Transit*, para. 7.76.
[87] Panel Report, *Russia – Traffic in Transit*, para. 7.75.
[88] Panel Report, *US – Origin Marking (Hong Kong, China)*, paras. 7.353–7.354.
[89] Panel Report, *US – Steel and Aluminium Products (China)*, paras. 7.142–7.143 and 7.147–7.148.
[90] Proposed Regulation, Article 103(6).
[91] Panel Report, *Saudi Arabia – IPRs*, para. 7.293.

relations would not automatically allow restrictions of the type established in Title IV of the Proposed Regulation vis-à-vis nationals of Members uninvolved in the emergency in question.

54. In conclusion, outside the specific context of an emergency in international relations neither set of exceptions justifies the violations identified in Section III. Even accepting that ICT supply-chain security might be a legitimate regulatory objective, the design of Title IV both makes the Proposed Regulation more trade-restrictive than necessary for the fulfilment of its objective and produces arbitrary or unjustifiable discrimination between countries where the same conditions prevail.

55. Under the General Exceptions, measures must remain the least trade-restrictive available to fulfil their objective, and may not arbitrarily or unjustifiably discriminate against WTO Members. The General Exceptions thus preserve the guardrails that safeguard the rule of law in trade relations; the Security Exceptions suspend them, and are accordingly confined to narrow circumstances. If Security Exceptions are invoked for the pursuit of continuously applicable, peacetime objectives, it is difficult to envisage how the rules-based trade relations enshrined in the WTO Agreements can continue to apply.

V. Other Violations

56. The measures found in Section III to constitute a violation of GATT Article III:4 may entail two additional violations: of Article 2.1 of the TRIMs Agreement and of Article 3.1(b) of the SCM Agreement. These possibilities are examined in turn.

57. **TRIMs Agreement.** The prohibitions on the use, installation and integration of designated suppliers' components by entities established in the EU are investment measures related to trade in goods: they affect the purchase and use of imported ICT products within investments in the Union. Article 2.1 of the TRIMs Agreement prohibits the application of any such measure 'that is inconsistent with the provisions of Article III or Article XI of GATT 1994'.[92] The Annex to the TRIMs Agreement provides an Illustrative List that identifies TRIMs deemed inconsistent with Articles III:4 and XI:1, dispensing the interpreter from a separate demonstration. The Illustrative List does not exhaust the incorporated obligation.[93] The applicable standard for a measure outside the List is accordingly GATT Article III:4 itself. It is immaterial that an operator precluded from using ICT components from designated suppliers is free to substitute components of any non-designated origin; a legal prohibition on the use of the designated supplier's components, while like EU components remain freely usable, modifies the conditions of competition to the detriment of the affected imported products when compared to EU like products. The use prohibitions in Articles 103(1), 103(7),

[92] TRIMs Agreement, Articles 1–3 and Annex. In *Canada – Renewable Energy*, the Appellate Body stated that the TRIMs Agreement establishes 'cumulative obligations' with Article III of the GATT 1994 and Article 3.1(b) of the SCM Agreement (Appellate Body Report, *Canada – Renewable Energy*, para. 5.5).

[93] Appellate Body Report, *Canada – Renewable Energy*, para. 5.26 (although Article 2.2 and the Illustrative List focus on 'the specific provisions where [the] obligation [under Article 2.1] is reflected – that is, Article III:4 of the GATT 1994', the Appellate Body did not consider that this 'responds to the question of whether such measures are inconsistent with Article III of the GATT 1994 in its entirety').

111(1) and 85(9), and the phase-out obligation in Article 110(2), are therefore inconsistent with Article 2.1 of the TRIMs Agreement; and, for the reasons given in Section IV, they are not justified under the exceptions of the GATT 1994 incorporated into the TRIMs Agreement by Article 3.

58. **SCM Agreement.** Article 100(4)(f) of the Proposed Regulation bars high-risk suppliers from any activity under EU funding programmes in relation to key ICT assets. The Preamble provides that the EU 'should not fund projects involving high-risk suppliers' and that implementing partners should refrain from supporting such projects even at their own risk.[94] Union funding of this kind will in many instances constitute a subsidy.[95]

59. Article 3.1(b) of the SCM Agreement prohibits subsidies contingent upon the use of domestic over imported goods. The term 'contingent upon' requires a condition, rather than a mere incentive or foreseeable result. In *US – Tax Incentives*, the Appellate Body found that 'a *condition requiring* the use of domestic over imported goods' may 'be discerned from the terms of the measure itself, or inferred from its design, structure, modalities of operation, and the relevant factual circumstances'.[96] A single designation will not necessarily meet that standard, since recipients remain free to source ICT components from any non-designated supplier. The position differs, however, in concentrated markets: where the designation of a WTO Member, or the cumulative designation of the principal non-EU participants in a given market, leaves EU suppliers as the effective residual source for the subsidised demand, the exclusion operates as a condition requiring the use of domestic over imported goods. To restrict Article 3.1(b) to measures excluding imports altogether – as the Panel in *EU – Palm Oil (Indonesia)* did[97] – would make circumvention too easy, contrary to the object and purpose of the SCM Agreement.[98] A violation of Article 3.1(b) may therefore arise if, on the facts, the exclusion of third-country suppliers *de facto* requires participants in EU funded projects to use EU-supplied products.

[94] Proposed Regulation, Article 100(4)(f) and Preamble, recital 139.

[95] SCM Agreement, Article 1.1. A grant from the EU budget or a favourable loan from an implementing partner is a 'direct transfer of funds' under Article 1.1(a)(1)(i); a benefit is conferred whenever the recipient is placed in a better position than the market would afford (Appellate Body Report, *Canada – Aircraft*, para. 157). Under Article 2.3, a subsidy falling under Article 3 is deemed specific.

[96] Appellate Body Report, *US – Tax Incentives*, paras. 5.18, 5.22 and 5.51 (contingency requires 'a condition requiring the use of domestic over imported goods … discerned from the terms of the measure itself, or inferred from its design, structure, modalities of operation, and the relevant factual circumstances'; contingency 'is not limited to cases where the measure requires the subsidy recipient to use domestic goods to the complete exclusion of imported goods'); Appellate Body Report, *Brazil – Taxation*, paras. 5.254–5.255 (distinguishing 'a contingency requirement, as opposed to a mere incentive, to use domestic goods').

[97] Panel Report, *EU – Palm Oil (Indonesia)*, paras. 7.1385–7.1386.

[98] Appellate Body Report, *Canada – Autos*, para. 142 (finding that confining Article 3.1(b) to contingency in law would 'be contrary to the object and purpose of the SCM Agreement because it would make circumvention of obligations by Members too easy').

VI. Technical Regulations, Conformity Assessment and Standardisation – TBT Agreement

A. Technical Aspects of the Exclusion of Suppliers

60. The question may arise whether the exclusion of suppliers under Title IV of the Proposed Regulation, and its various effects, are measures that can be assessed under, among others, Article 2 of the TBT Agreement, as a 'technical regulation'. A technical regulation is a document laying down product characteristics or their related processes and production methods, with which compliance is mandatory.[99]

61. Product characteristics are 'objectively definable' features, qualities, attributes or distinguishing marks of a product.[100] Many attributes on which Title IV operates – the country of establishment of the supplier, the nationality of its owners and controllers, and the presumed influence of third countries – are not attributes of the product but of the supplier. On the other hand, the Proposed Regulation also refers to technical attributes of the ICT products – 'concealed vulnerabilities or backdoors'[101] – as well as to 'technical measures' that can be implemented to mitigate risks, including (i) the use of on-device processing; (ii) specific segmentation of network systems; (iii) the disabling of any remote or physical access to key ICT assets; (iv) the disabling of non-essential features; (v) operational network monitoring; (vi) testing of hardware and software.[102]

62. To determine whether measures with technical and non-technical aspects are technical regulations, the Panel in *EU – Palm Oil (Malaysia)* applied a 'centre of gravity' assessment, concluding that measures providing for some product characteristics may amount to technical regulations, even if they also included non-technical elements.[103] By contrast, in *EC – Seal Products*, the Appellate Body found that the 'integral and essential' aspects of the EU's measure concerned the origin of the hunters and the purpose of the hunt, concluding that, in the EU seals regime, the technical aspects were accessory.[104]

63. Without proceeding to an in-depth assessment of Article 2 of the TBT Agreement, it is worth noting that, in a number of disputes, the Appellate Body found that the TBT Agreement and the GATT 1994 strike a similar balance between, on the one hand, the prohibition of unnecessary restrictions on trade and of unjustifiable discrimination and, on the other hand, the recognition of the entitlement to regulate in a non-discriminatory manner.[105]

[99] TBT Agreement, Annex 1.1. See Appellate Body Report, *EC – Sardines*, para. 176.

[100] Appellate Body Report, *EC – Asbestos*, para. 67 (product characteristics 'include, in our view, any objectively definable "features", "qualities", "attributes", or other "distinguishing mark" of a product').

[101] Proposed Regulation, Preamble, Recital 129.

[102] Proposed Regulation, Article 103(2)(c).

[103] Panel Report, *EU and Certain Member States – Palm Oil (Malaysia)*, para. 7.106.

[104] Appellate Body Report, *EC – Seal Products*, paras. 5.29, 5.52 and 5.58.

[105] Appellate Body Report, *US – Clove Cigarettes*, para. 96; Appellate Body Report, *EC – Seal Products*, para. 5.122.

B. Conformity Assessment Procedures

64. The EU has notified Title III of the Proposed Regulation to the TBT Committee of the WTO as a Conformity Assessment Procedure.[106] Title III establishes the European Cybersecurity Certification Framework, which attests, by evaluation, that ICT products, services and processes comply with specified security requirements. These requirements are at least standards within the meaning of Annex 1.2 of the TBT Agreement. Where this certification serves as the means of demonstrating compliance with EU or national requirements in such a way that access to the market is conditional upon this demonstration of compliance, they are requirements in a technical regulation.[107]

65. A mechanism attesting compliance through evaluation is a conformity assessment procedure.[108] The disciplines of Article 5 attach to such procedures of central government bodies where a positive assurance of conformity is required.[109] The schemes being prepared by ENISA at the Commission's request will be subject to these disciplines wherever EU or national law prescribes certification as the route to a positive assurance of conformity, including, at present, for European Digital Identity Wallets; upon adoption of a delegated act under Article 8(1) of the Cyber Resilience Act, for the critical categories identified therein; and wherever a Member State exercises the option conferred by Article 24(1) of Directive (EU) 2022/2555. The findings that follow are made in respect of these applications.[110]

66. Article 5.1.1 of the TBT Agreement requires that access to conformity assessment be granted to suppliers of WTO Members on conditions no less favourable than those accorded to suppliers of like products of national origin or of any other country, 'in a comparable situation'. The provision requires an assessment of whether the conditions of access modify the conditions of competition to the detriment of suppliers of like imported products.[111] Under the Proposed Regulation, the conditions of competition are plainly modified: a supplier designated as 'high-risk' via the country route or the entity route may not apply for or hold a European cybersecurity certificate, and certificates it already held must be withdrawn.

67. The question under Article 5.1.1 is whether the suppliers so excluded are in a 'comparable situation' to those admitted. In *Russia – Railway Equipment*, the Appellate Body found that factors bearing on that question 'should have a bearing on the conditions for granting

[106] Committee on Technical Barriers to Trade, Notification, G/TBT/N/EU/1235 (26 August 2026).

[107] Proposed Regulation, Articles 71(2)(a), 73, 74, 82 and 85(4).

[108] TBT Agreement, Annex 1.3 and Explanatory note ('[a]ny procedure used, directly or indirectly, to determine that relevant requirements in technical regulations or standards are fulfilled', including 'evaluation, verification and assurance of conformity; registration, accreditation and approval as well as their combinations').

[109] TBT Agreement, Article 5.1 (chapeau).

[110] Where certification is not required, the exclusion remains disciplined under the GATT and GATS. Eligibility for a certificate, which carries the presumption of conformity provided for in Article 27 of Regulation (EU) 2024/2847, and eligibility for accreditation as a conformity assessment body and for authorisation as an attestation provider under Article 100(4)(c) and (d), are advantages in the marketplace whether or not the underlying certification is compulsory.

[111] Appellate Body Report, *Russia – Railway Equipment*, para. 5.123.

access to conformity assessment in a particular case and should pertain to or affect the specific suppliers of like products to which these conditions relate'.[112]

68. Under Article 100(4)(b) of the Proposed Regulation, a supplier labelled as 'high-risk' is denied access to European cybersecurity certificates, without any argument that the conformity of the supplier's products cannot be assessed, or that assessments already conducted are unreliable. On the third-country route, the supplier is assessed based only on its establishment, ownership and control. Since conformity assessment was previously available to that supplier and no change in the conformity of its products has occurred, it remains 'in a comparable situation' to its competitors that retain their certificates.

69. The conclusion follows *a fortiori* for the mandatory withdrawal of certificates already held. In *Russia – Railway Equipment*, the justification advanced for suspending certificates was pertinent to conformity assessment: inspection control at the suppliers' facilities, it was argued, had become unfeasible.[113] Article 100(5) offers no attempt at an analogue justification. The products concerned have been assessed and found conforming under applicable EU procedures; the certificates are withdrawn by reason of the identity of their holder. No assessment result is called into question. Suppliers whose conformity the EU has itself verified are, by every measure relevant to conformity assessment, in a situation not merely comparable but identical to that of every other holder of a valid certificate.

70. Additionally, Article 5.1.2 of the TBT Agreement prohibits conformity assessment procedures prepared, adopted or applied 'with a view to or with the effect of creating unnecessary obstacles to international trade'. Panels have found procedures inconsistent with that provision where their design or operation meant that conforming products could not in fact obtain certification.[114] Under Title IV this occurs by design: a designated high-risk supplier may not apply and may not hold a certificate, and any certificate obtained is withdrawn, whatever the conformity of its products with the applicable security requirements.

71. The bar on applying for or holding a European cybersecurity certificate, and the mandatory withdrawal of certificates already held, are accordingly inconsistent with Article 5.1.1 and with the first sentence of Article 5.1.2 of the TBT Agreement.

C. Standardisation

72. Under the Proposed Regulation, a designated high-risk supplier may not 'participate in the development of, assessment, consultation or decisions concerning European standards and

[112] Appellate Body Report, *Russia – Railway Equipment*, para. 5.144. The Panel had incorrectly examined comparability of situations from the perspective of the regulating government, rather than as regards the suppliers concerned. The Panel had also erred in weighing and balancing the regulating government's various interests, an exercise with no basis in the language of Article 5.1.1 (Appellate Body Report, *Russia – Railway Equipment*, paras. 5.146–5.148).

[113] The measures at issue in *Russia – Railway Equipment* were suspensions of certificates previously granted, justified on the ground that inspection control at the suppliers' facilities had become unfeasible (Appellate Body Report, *Russia – Railway Equipment*, para. 5.145).

[114] Panel Report, *EU – Palm Oil (Indonesia)*, para. 7.860. See also Panel Reports, *EC – Seal Products*, para. 7.528 (substantive findings under the TBT Agreement were subsequently declared moot and of no legal effect; see Appellate Body Report, *EC – Seal Products*, para. 5.70).

European standardisation deliverables' or common specifications in the area of cybersecurity; the authorities in charge of these procedures are directed to give effect to the exclusion of designated suppliers.[115] European standards are prepared by CEN, CENELEC and ETSI – non-governmental standardising bodies within the meaning of Article 4.1 of the TBT Agreement.[116]

73. Article 4.1 provides that Members 'shall not take measures which have the effect of, directly or indirectly, requiring or encouraging [non-central] standardizing bodies to act in a manner inconsistent with the Code of Good Practice'.[117] In the Proposed Regulation, Article 100(4)(a) does not encourage but mandates that the supplier 'shall not be entitled' to participate; the 'authorities in charge' are enlisted to enforce that ban.[118] The conduct so mandated is inconsistent with paragraphs L and N of the Code, under which a standardising body must allow at least 60 days for comments on a draft standard by interested parties within the territory of any WTO Member, and must take those comments into account.[119] Designated suppliers will ordinarily be interested parties within the territory of a Member – frequently, through subsidiaries, within the EU itself. The commenting stage is the consultative core of the European standardisation procedure, and Article 100(4)(a) bars participation in 'consultation'. The standardising body is thus required to close, against a class of interested parties defined by their national connections or assumed susceptibility to third country influence, a window for participation that the Code requires it to hold open, and to disregard any input that those parties might submit – and which the Code requires it to take into account.

74. Article 100(4)(a) of the Proposed Regulation is therefore a measure having the effect of directly requiring the European standardisation bodies to act in a manner inconsistent with paragraphs L and N of the Code of Good Practice, violating the third sentence of Article 4.1 of the TBT Agreement.

VII. Conclusion

75. Title IV of the Proposed Regulation makes foreign establishment, ownership or control both a necessary condition of exclusion from substantial segments of the EU market for ICT components and related services and, in the case of country designations, the criterion for this exclusion. Even accepting that the origin of certain risks (influence by a third country) is a

[115] Proposed Regulation, Article 100(4)(a).

[116] Regulation (EU) No 1025/2012, Articles 2(8) and 10(1) and Annex I, listing the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI).

[117] TBT Agreement, Article 4.1, third sentence. Under the fourth sentence, '[t]he obligations of Members with respect to compliance of standardizing bodies with the Code of Good Practice shall apply irrespective of whether or not a standardizing body has accepted the Code of Good Practice'.

[118] Under the final subparagraph of Article 100(4), the 'authorities in charge' of the relevant procedures 'shall conduct the necessary assessments for the purpose of this paragraph' and may rely on the list of high-risk suppliers established under Article 104.

[119] TBT Agreement, Annex 3, paragraphs L and N. Under paragraph L, a standardising body 'shall allow a period of at least 60 days for the submission of comments on the draft standard by interested parties within the territory of a Member of the WTO'; under paragraph N, it 'shall take into account, in the processing of the standard, comments received during the period for commenting'.

specific risk that can be addressed as a legitimate objective, the measure as designed does not map onto this risk.

76. The designation of a WTO Member and of the suppliers connected to it, and the designation of an individual supplier under Article 103(7), each place the European Union in breach of GATT Articles I:1 and III:4 and of GATS Articles II:1, XVII:1 and XVI:2(f), and are inconsistent with the *Services Domestic Regulation* commitments in the EU's Schedule. The use prohibitions violate Article 2.1 of the TRIMs Agreement; and, in concentrated markets, EU funding granted with exclusion of the key non-EU suppliers may violate Article 3.1(b) of the SCM Agreement. The exclusion from certification and the withdrawal of certificates already held are, wherever EU or national law prescribes certification, inconsistent with Articles 5.1.1 and 5.1.2 of the TBT Agreement, and the exclusion from standardisation is inconsistent with Article 4.1 read with the Code of Good Practice.

77. None of these violations is justifiable under the GATT or GATS General Exceptions. The Proposed Regulation offers, in Article 103(2), origin-neutral, conduct-based alternative measures that address the same risk in the same assets. In Article 105(2)(b), the Proposed Regulation itself acknowledges that mitigating measures of the same kind can address non-technical risks and preclude undue interference. This makes the existing exclusions regime more trade-restrictive than necessary to fulfil its legitimate objectives. Under the chapeau of the GATT 1994, a regime that excludes third-country suppliers on grounds unrelated to their conduct, exempts by law the domestic suppliers, specifies no criteria against which a designated supplier might conform, and – on the entity route – provides neither periodic review nor any exemption, entails discrimination both unjustifiable and arbitrary between countries where the same conditions prevail.

78. The Security Exceptions are inapplicable. Though exclusions of this type might be conceivable in time of war or other emergency in international relations, Title IV is a standing regime of general application, adopted to preserve the proper functioning of the internal market.

79. It follows that Title IV, if adopted in its present form and applied to the suppliers of a WTO Member, would expose the EU to findings of violation across the GATT 1994, the GATS, the TBT Agreement, the TRIMs Agreement and, in defined market conditions, the SCM Agreement, without an available justification.