論歐盟「網路安全法」修正草案中受信任資通訊供應鏈架構之貿易問題

林意庭 編譯

指導老師 楊培侃

摘要

歐盟「網路安全法」修正草案旨在透過受信任資通訊供應鏈架構因應地緣政治等非技術性風險，並對指定之高風險供應商實施排除與逐步淘汰機制。然而，從國際經貿法角度觀之，該修正草案在《關稅及貿易總協定》、《服務貿易總協定》及《技術性貿易障礙協定》下的合法性存在顯著爭議，其核心問題在於該法案是否對同類產品或服務構成歧視性，以及歐盟能否成功援引一般例外或國家安全例外條款為其貿易限制行為辯護。目前該草案仍在審議程序中，但預計會對全球電信及科技等產業帶來深遠影響。

（取材資料: Peter Van den Bossche, *Preliminary Thoughts on the European Commission Proposal for the Cybersecurity Act 2.0*, INT'L ECON. L. & POL'Y BLOG（July 28, 2026）, https://ielp.worldtradelaw.net/2026/07/guest-post-preliminary-thoughts-on-the-european-commission-proposal-for-the-cybersecurity-act-2-0/.）

今（2026）年 1 月 20 日，歐盟提出「網路安全法」修正草案（以下簡稱 CSA 2.0）[1]，CSA 2.0 提案建立了兩項對資通訊（Information and Communications Technology，以下簡稱 ICT）產品與服務之國際貿易尤為重要的主要機制，即 ICT 供應鏈安全機制[2]與歐洲網路安全認證機制[3]。

關於第一項機制，CSA 2.0 提案建立「受信任 ICT 供應鏈架構」，旨在處理非技術性風險，亦即該風險並非源於 ICT 產品或服務之軟硬體漏洞，而是源於 ICT 供應鏈對第三國在地緣政治、法律及系統性依賴相關的風險[4]。

[1] *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)*, COM (2026) 11 final (Jan. 20, 2026).
[2] *Id*. at 130.
[3] *Id*. at 26.
[4] *Id*. at 128.

以下本文先解析該架構之五大核心概念與三項市場排除措施，再評估其違反 WTO 不歧視義務之爭議，最後檢視歐盟援引一般例外與國家安全例外抗辯的可行性，並做一結論。

壹、受信任 ICT 供應鏈架構之核心概念

首先，此「受信任 ICT 供應鏈架構」的核心包含五個相互關聯的概念，分別為「關鍵領域」、「關鍵與重要實體」、「關鍵 ICT 資產」、「存在網路安全疑慮之國家」以及「高風險供應商」。

在這些概念中，前三項展現了 CSA 2.0 提案極為廣泛的適用範圍。共有十八個經濟領域被定義為「關鍵領域」，其中包括能源、交通、醫療、金融、水務、數位基礎設施與 ICT 服務、公共行政及製造業等；「關鍵與重要實體」是指在上述 18 個「關鍵領域」中營運的所有大型及中型企業；「關鍵 ICT 資產」則是指由「關鍵與重要實體」所製造之 ICT 產品或提供之服務[5]。

第四個概念，即「存在網路安全疑慮之國家」，是指經歐盟執委會（European Commission，下稱執委會）依據安全風險評估或其他公開來源認定，對 ICT 供應鏈構成非技術性風險的第三國。而在認定「存在網路安全疑慮之國家」時，執委會應考量四項要素。第一，該第三國之法律或實務作法是否要求受其管轄之實體，在軟體或硬體漏洞被已知利用前，即須向主管機關報告；第二，是否缺乏能夠糾正此類安全疑慮的有效司法救濟與獨立民主監督機制；第三，是否具備關於自該國領域內運作的威脅行為者所進行之惡意網路活動或行動的具體證實資訊；第四，該第三國是否缺乏與執委會或成員國合作處理該等風險的能力或意願[6]。

最後，第五個概念，即「高風險供應商」，在 CSA 2.0 提案中被定義為設立於經指定為存在網路安全疑慮之第三國的實體；或受該等第三國控制的實體；或受設立於該等第三國之實體所控制的實體；或受該等第三國國民所控制的實體[7]。

簡而言之，執委會係基於 ICT 產品製造商或服務提供者的設立地、所有權及控制結構，將其指定為「高風險供應商」。

[5] *Id*. at 130.
[6] *Id*. at 128-129.
[7] *Id*. at 64.

此外，儘管僅限於例外情況下，執委會亦得直接將某一實體指定為「高風險供應商」，即使該實體與經指定為存在網路安全疑慮的國家並無任何關聯[8]。

貳、CSA 2.0 對高風險供應商之排除與限制措施

依據 CSA 2.0 提案，歐盟執委會得對「高風險供應商」之 ICT 產品及服務產生不利影響時，採取三種排除措施。

第一，執委會得禁止歐盟電子通訊網路提供者在運營「關鍵 ICT 資產」時，使用、安裝或整合來自「高風險供應商」的 ICT 組件，並要求已安裝之「高風險供應商」組件須在不超過 36 個月內逐步淘汰[9]。

第二，執委會得禁止在 18 個「關鍵領域」運營之「關鍵與重要實體」，在運營「關鍵 ICT 資產」時使用、安裝或整合來自「高風險供應商」的 ICT 組件[10]。

第三，執委會得直接排除由特定實體所提供的 ICT 組件被「關鍵與重要實體」使用、安裝或整合，毋須單獨進行「關鍵 ICT 資產」之認定或「存在網路安全疑慮國家」之指定[11]。亦即，CSA 2.0 提案賦予執委會權限，禁止歐盟「關鍵與重要實體」在運營「關鍵 ICT 資產」時使用、安裝或整合來自「高風險供應商」的 ICT 組件。

此外，「高風險供應商」亦被排除參與網路安全領域之歐洲標準化活動、與提供用於「關鍵 ICT 資產」之 ICT 組件相關之公共採購程序以及與提供用於「關鍵 ICT 資產」之 ICT 組件相關之歐盟資助計畫[12]。

總體而言，CSA 2.0 提案旨在將歐盟認定為存在與特定第三國相關之「非技術性風險」的「高風險供應商」及其 ICT 產品與服務排除於歐盟市場之外。

參、CSA 2.0 措施違反 WTO 不歧視義務之合法性分析

《關稅及貿易總協定（General Agreement on Tariffs and Trade，以下簡稱 GATT[13]）》與《服務貿易總協定（General Agreement on Trade in Services，以下

[8] *Id*. at 132.
[9] *Id*. at 136.
[10] *Id*. at 130-131.
[11] *Id*. at 132.
[12] *Id*. at 129.
[13] General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 190 [hereinafter GATT].

簡稱 GATS[14]）》下之不歧視義務，顯然適用於 CSA 2.0 提案所針對「高風險供應商」產品與服務的限制措施；相比之下，《技術性貿易障礙協定（Agreement on Technical Barriers to Trade，以下簡稱 TBT 協定[15]）》的可適用性則較不直接，須由潛在控訴方進一步提出論證。

關於這些措施是否符合前述義務的核心問題之一，在於 WTO 協定下的「同類性」檢驗。這可以透過比較相關因素來展現，或者若該措施是基於原產地所採取，則可直接予以推定。無論何種方式，控訴方皆很有可能證明該等產品屬於「同類」產品。

在受影響產品構成「同類」產品的基礎上，根據 GATT 第 1 條[16]最惠國待遇原則，CSA 2.0 所設立的全面禁止措施，未能立即且無條件地將給予其他國家供應商之優待，給予來自特定會員國高風險供應商的 ICT 產品。

此外，依據 GATT 第 3 條第 4 項[17]國民待遇原則，控訴方亦不難證明進口之高風險供應商 ICT 產品所受待遇劣於其他供應商之「同類」國內 ICT 產品，因為其產品直接被排除於歐盟市場之外。

此在 GATS 第 2 條[18]及第 17 條[19]下之主張亦同。然而，另一方面，鑑於 TBT 協定第 2.1 條[20]及第 5.2 條[21]背後蘊含的正當管制區分原則[22]，要證明違反 TBT 協定下的不歧視義務可能會較為棘手。

---

[14] General Agreement on Trade in Service, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 [hereinafter GATS].
[15] Agreement on Technical Barrier to Trade, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1868, U.N.T.S. 120 [hereinafter TBT Agreement].
[16] GATT, art. I:1.
[17] *Id*. art. III:4.
[18] GATS, art. II:1.
[19] *Id*. art. XVII:1.
[20] TBT Agreement, art. 2.1.
[21] *Id*. art. 5.2.
[22] Appellate Body Report, *United States—Measures Affecting the Production and Sale of Clove Cigarettes*, ¶182, WTO Doc. WT/DS406/AB/R (adopted Apr. 24, 2012);「美國—丁香菸案（*US—Clove*）」初步訂定 TBT 協定第 2.1 條中「較低待遇」之審查標準， 而此審查標準分為兩階段：（1）檢視進口產品與本國同類產品受到之差別待遇（different treatment）是否改變同類產品間之競爭關係（competitive relationship），造成進口產品遭受不利 影響（detrimental impact）；（2）該不利影響是否源於正當管制區分（legitimate regulatory distinction）。若系爭措施之設計或適用無構成恣意或歧視之手段，即屬正當管制區分，不構成歧視待遇。參考：趙思博，論 WTO 會員國於 TBT 協定中「國民待遇原則」之政策空間，國立政治大學國際經營與貿易研究所碩士論文，頁 33、58（2014 年）。

肆、歐盟引用例外條款主張正當化之可行性

當控訴方成功證明歐盟違反了 GATT 與 GATS 下之不歧視義務時，歐盟極可能會主張 CSA 2.0 依據這些 WTO 協定中適用的例外條款而具備正當性。

就一般例外而言，即使假設任何主張的正當化事由均具相關性，歐盟仍須證明 CSA 2.0 對於保護自身免受網路安全風險而言屬「必要」。唯有在控訴方所提出的所有可能替代措施中，不存在合理可得且貿易限制較小、同時又能達到歐盟預期保護程度的措施時，CSA 2.0 才會被認定為具有「必要性」。

然而，若要最終獲得正當性， CSA 2.0 之適用不得構成專斷及無理歧視。就此而言，可能需要處理以下問題：第一，歐盟在適用 CSA 2.0 時是否過於僵化且缺乏彈性，並且未適當考量 ICT 產品或服務來源國之實際狀況；第二，歐盟在採取如 CSA 2.0 等單邊措施前，是否曾嘗試透過多邊談判來解決其對網路安全的疑慮；第三，CSA 2.0 在具體適用上，是否顯露出與歐盟所追求之網路安全防護政策目標無法調和或缺乏合理關聯的歧視。要證明 CSA 2.0 之適用方式不構成專斷及無理歧視，對歐盟而言恐將是一項相當棘手的考驗。

歐盟亦可能嘗試援引 GATT 第 21 條[23]及 GATS 第 14 條之二[24]之國家安全例外條款，為原本不符合 GATT 或 GATS 規範之 CSA 2.0 主張正當化。在本案中，這兩個條文之 b 款、特別是其中第 iii 目，堪稱具備一定程度關聯性。第 iii 目係指於戰爭或其他國際關係緊急時期所採取之措施，第一種情境即「戰爭」，幸運地並未發生，但網路不安全、網路威脅與網路攻擊是否能被主張構成國際關係之緊急時期？

在「俄羅斯—轉運過境案（Russia—Measures Concerning Traffic in Transit）[25]」中，爭端解決小組將國際關係之緊急時期界定為「武力衝突、潛在武力衝突、緊張局勢或危機加劇、或籠罩或圍繞一國之普遍不穩定狀態」[26]。該案小組進一步澄清，會員國之間的政治或經濟分歧本身並不足以構成「國際關係之緊急時期」，除非該等分歧影響到國防與軍事利益，或是法制與公共秩序之維護利益[27]。

---

[23] GATT, art. XXI (“Nothing in this Agreement shall be construed ... (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests ... (iii) taken in time of war or other emergency in international relations.”).
[24] GATS, art. XIV (“Nothing in this Agreement shall be construed ... (b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests ... (iii) taken in time of war or other emergency in international relations.”).
[25] Panel Report, *Russia — Measures Concerning Traffic in Transit*, WTO Doc. WT/DS512/R (adopted Apr. 26, 2019).
[26] *Id*. ¶7.75.
[27] *Id*. ¶7.76.

伍、結論

執委會之草案提案目前正處於漫長的歐盟立法程序中，然若未來草案照案通過，其引發的貿易限制措施勢必面臨 WTO 法律架構下的嚴格檢驗，其合法性與潛在貿易爭議將是全球電信及科技產業持續關注的焦點。

Research Center for Int'l Organization & Trade Law