歐盟《網路韌性法》對 WTO 與國際貿易之影響

陳立承 編譯

摘要

近年，歐盟官方愈加重視於單一市場中流通，具數位元素之產品的網路安全問題，將其視為須盡速解決之問題。對此，歐盟執委會於 2022 年 9 月提出《網路韌性法》之草案，其文本歷經談判與修正後，於今（2024）年 10 月 10 日正式通過。《網路韌性法》要求此類可連網之軟硬體產品之製造商、通路商以及進口商遵循一定義務，以確保系爭產品於其生命週期中不受網路安全問題侵擾，進而確保歐盟消費者及其他市場參與者得到網路安全之最大保障。惟其規範內容亦引起個別 WTO 會員之貿易關切以及產業界人士之擔憂，認為部分條文逾越比例原則，廠商將負擔過重的法令遵循成本，並有過度限制貿易之疑慮。待《網路韌性法》實施後，將對國際貿易造成何種影響，以及歐盟對此之應對措施，皆值得持續關注。

（取材資料：European Commission Press Release IP/752/24, Cyber Resilience Act: Council Adopts New Law on Security Requirements for Digital Products (Oct. 10, 2024); PAULO MONIZ, JORGE LIBÓRIO & LUÍS AVILEZ, NAVIGATING THE CYBER RESILIENCE ACT: ORGANIZATIONAL COMPLIANCE, OVERSIGHT, CHALLENGES, AND IMPACT ON STAKEHOLDERS (2024).）

歐盟於今（2024）年 10 月 10 日通過「針對具有數位元素產品之水平網路安全要求規則（Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements）」[1]，亦稱《網路韌性法》（Cyber Resilience Act, CRA）。該法旨在透過對企業設下統一之網路安全[2]規範，確保如家用監視器、數位冰箱、電視以及玩具等具有數位元素之軟、硬體產品（下稱具數位元素產品）於市面流通時符合網路安全要求，使得消費者在選擇購買或使用具數位元素產品時能夠將網路安

[1] Regulation (EU) 2024/2847, 2024 O.J. (L series) 1 [hereinafter CRA].

[2] 網路安全係指保護網路、可連網設備與資料免於未經授權之存取行為與網路犯罪行為，確保資訊的機密性、完整性與可用性之實踐。*What is Cybersecurity?*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Feb. 1, 2021), https://www.cisa.gov/news-events/news/what-cybersecurity.

全要求納入考量，且更容易識別具備適當網路安全之產品[3]，並使企業免於遵循多套不同之網路安全規範，降低相關法遵成本[4]。

《網路韌性法》旨在填補網路安全漏洞、釐清相關法規之關聯性，使歐盟現有之網路安全法規架構更加連貫，確保如物聯網（Internet of Things, IoT）產品等具數位元素產品於其供應鏈及產品生命週期中之網路安全[5]。

本文首先簡述《網路韌性法》（下稱本規則）之制定背景，並簡介本規則下包含一般性義務、實體與程序性義務、罰則等主要內容，再透過歸納本規則部分條文引發之貿易關切與其他利害關係人之擔憂，分析該等規範不符比例原則之處及其對 WTO 與國際貿易之可能影響，最後作一結論。

壹、本規則之制定背景

《網路韌性法》係由歐盟執委會（下稱執委會）主席馮德萊恩（Ursula von der Leyen）於 2021 年 9 月的歐盟國情咨文（State of the Union address）中首次提出[6]，並再次出現於 2022 年 5 月 23 日歐洲理事會（下稱理事會）關於歐盟網路安全立場之決議中。該決議呼籲執委會於 2022 年底前提交針對可連網設備與相關製造流程及服務設下一般性網路安全要求之《網路韌性法》草案[7]。

基於上述決議，執委會隨即於 2022 年 9 月 15 日提出「網路韌性法草案」（下稱草案）[8]，補充歐盟既有之網路安全法律架構[9]。隨後，草案被安排於歐洲議會（下稱議會）下之產業、研究暨能源委員會（Committee on Industry, Research and Energy, ITRE）接受審議，並歷經談判與修正後，於去（2023）年 9 月進入執委會、理事會與議會間之跨機構協商程序[10]。經三方談判後，共同立法者於 2023

[3] European Commission Press Release IP/898/23, Cyber Resilience Act: Council and Parliament Strike a Deal on Security Requirements for Digital Products (Nov. 30, 2023).
[4] *Commission Staff Working Document Executive Summary of the Impact Assessment Report*, at 2, SWD (2022) 283 final (Sept. 15, 2022).
[5] CRA, *supra* note 1, pmbl. paras. 2, 4.
[6] *2021 State of the Union Address by President von der Leyen*, EUR. COMM'N (Sept. 15, 2021), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701.
[7] Council Conclusions on the Development of the European Union's Cyber Posture, at 6, EUR. COUNCIL Doc. (9364/22 LR/es 1 JAI.2) (2022).
[8] *Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020*, COM (2022) 454 final (Sept. 15, 2022).
[9] 歐盟現有之資安法律架構主要由《全歐高水準網路安全措施指令》（NIS 2 指令）以及《歐盟網路安全法》（Cybersecurity Act）等規範組成。*Cybersecurity Policies*, EUR. UNION, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies (last visited Dec. 25, 2024).
[10] *Legislative Train Schedule, Horizontal Cybersecurity Requirements for Products with Digital Elements in "A Europe Fit for the Digital Age"*, EUR. PARLIAMENT (Dec. 15, 2024), https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act?sid=8601.

年 11 月 30 日就修正後之文本達成暫時性政治協議[11]。該修正版文本隨後於同年 12 月經理事會採納、由 ITRE 於 2024 年 1 月批准後，經議會於 3 月同意，最終於 10 月 10 日由理事會正式通過，並於 12 月 10 日生效[12]。

貳、本規則主要規範內容

一、一般性規範與適用範圍

本規則第一章為一般性規範，包含規範客體、適用範圍以及名詞定義等。其中，第 2.1 條規定，本規則適用範圍涵蓋：「已於市面流通（made available on the market），具有數位元素，且其預期或合理可預見之用途包括直接或間接與裝置或網路進行邏輯或物理數據連接之產品（具數位元素產品）」[13]；第 3(1)條則進一步將具數位元素產品定義為：「軟體或硬體產品及其遠端數據處理解決方案，包括獨立上市（placed independently on the market）之軟體或硬體元件」[14]；而第 6 條則規定，具數位元素產品僅有在遵循本規則附件一第二部分之網路安全要求[15]，且製造商已建立並實施相關法遵流程之條件下，始得於歐盟上市流通[16]。

二、市場營運者之具體義務

本規則第二章則係對市場營運者（economic operator）[17]設下具體義務，其主要包含以下規範：

（一）系爭產品製造商之具體義務

1. 保障產品之網路安全

製造商將具數位元素產品上市前，應採行相關內部流程以確保產品於設計、研發、製造階段符合本規則附件一之網路安全要求[18]，包含編製產品技術文件

---

[11] *Id.*
[12] *Id.*
[13] CRA, *supra* note 1, art. 2.1.
[14] *Id.* art. 3(1).
[15] 本規則附件一第二部分揭示製造商處理網路安全漏洞時應遵循之程序，包含：1. 制定軟體物料清單（software bill of materials, SBOM）以識別並記錄漏洞及產品中的元件；2. 透過提供安全更新等方式即時修補漏洞；3.對系爭產品定期進行安全測試與檢查；3. 提供安全更新後，公布已修復漏洞之相關資訊，同時建立網路安全相關之諮詢管道；以及 4.原則上應免費提供安全性更新等。Annex I, Part II.
[16] *Id.* art. 6.
[17] 按本規則定義，「市場營運者」係指包含系爭產品之製造商、進口商與通路商等，因生產或將系爭產品上市而受本規則規範之市場參與者。*Id.* art. 3(12).
[18] *Id.* art. 13.1. 本規則附件一第一部分揭示系爭產品應具備之網路安全要求，包含如：1.市面上流通之產品應無已知可利用的網路安全漏洞，且應具備預設之安全性功能；應提供安全性更

（technical documentation）並對產品實施「符合性評估程序（conformity assessment procedure）」[19]、於產品上標示歐洲合格認證標章（Conformité Européenne Marking，CE 標章）並發布書面之「歐盟符合性聲明（EU Declaration of Conformity, EU DoC）」[20]，以及對產品進行網路安全風險評估等[21]，製造商並應於產品支援期間（support period）製作、保存相關風險評估報告並納入產品技術文件中[22]，並於市場監督機構要求下提供歐盟符合性聲明以及產品技術文件等足以證明系爭產品符合網路安全要求之文件[23]。

2. 持續提供產品網路安全支援與維持安全性更新

製造商應訂定五年以上之產品網路安全支援期間[24]，並於支援期間結束後至少十年內確保其已提供之網路安全更新可以取得[25]。

3. 即時對網路安全漏洞採取因應措施

製造商一旦發現系爭產品存在網路安全漏洞，應立即採取相關修補措施，或視情況將產品撤回或召回[26]。

（二）進口商與通路商之具體義務

1. 確保製造商已遵循相關法令要求

進口商與通路商將產品上市前，須確保產品製造商符合本規則之法令要求，例如：已實施符合性評估程序、已編制產品技術文件，並已在產品上標示 CE 標章[27]。

新，並確保產品得通過該更新解決漏洞；2. 應通過身份驗證、身份或訪問管理系統等控管機制，阻絕未經授權的訪問；3. 應通過加密技術等手段保護資料之機密性；4. 於網路安全事件發生後，提供適當補救機制並降低影響等。*Id.* Annex I, part I.

[19] *Id.* art. 13.12. 產品技術文件紀錄著製造商確保系爭產品及其實施之流程符合附件一之基本網路安全要求時使用之所有相關測試數據及其他詳細資訊。*Id.* art. 31.

[20] *Id.* Annex VIII, art. 4. 系爭產品通過本規則所定之符合性評估程序後，始取得 CE 標章，該標章並作為系爭產品遵循本規則之唯一證明。*Id.* pmbl. para.(89). 製造商於達成包括本規則在內之歐盟法規的法遵要求時均應發布相應之歐盟符合性聲明，以便主管機關查驗，減少行政負擔。*Id*. pmbl. para. (88).

[21] *Id.* art. 13.2.

[22] *Id*. arts. 13.2, 13.3, 13.4.

[23] *Id.* arts. 13.12, 13.22.

[24] *Id.* art. 13.8.

[25] *Id.* art. 13.9.

[26] *Id.* art. 13.21.

[27] *Id.* arts. 19.2, 20.2.

2. 確保製造商對網路安全漏洞採取因應措施

進口商與通路商知悉透過其上市之產品存在網路安全漏洞時，應採取修補措施或於必要時撤回或召回產品[28]。

三、程序性規範

本規則主要於第二章、第三章與附件一，訂有本規則下相關義務之遵循程序，以確保具數位元素產品在設計、開發與生產過程中具備適當的網路安全水準，並能有效應對潛在的網路安全風險，主要包含以下規範：

（一）製造商之義務

1. 產品重大網路安全風險之通知與通報程序

若產品之網路安全漏洞已遭受主動滲透攻擊（actively exploited）或發生影響產品網路安全之重大事件（severe incident），製造商應即時通知受影響之用戶並提供可用之緩解措施[29]，以及應於一定時程（24 小時、72 小時、採取矯正措施後 14 日）內，分別以早期預警通知（early warning notification）、漏洞通知（vulnerability notification）或事件通知（incident notification）以及最終報告（final report）之形式，分階段向主管機關歐盟網路安全局（European Union Agency for Cybersecurity, ENISA）與其指定之資安事件應變小組（Computer Security Incident Response Team, CSIRT）通報該漏洞與重大事件[30]。

2. 符合性評估程序

如前所述，製造商應對具數位元素產品實施符合性評估程序，以確定產品是否符合附件一中規定的基本網路安全要求[31]，本規則並於附件八中列出該程序之詳細要求，分為四個部分[32]：第一部分為，實施包含編制技術文件、建立產品設計製造與漏洞處理之法遵程序，以及標示 CE 標章並發布 DoC 等內部控制手段；第二部分為，向通報之主管機關申請歐盟公告機構證書（EU-type Examination）；第三部分為，基於本規則之內部產品控制程序（internal production control）提出

[28] *Id.* arts. 19.5, 20.4.
[29] *Id.* art. 14.8.
[30] 上述項目中，須於 72 小時內通報之漏洞通知係對該漏洞或事件之概要描述，以及已採取之補救措施；而須於採取補救措施後 14 日內通報之最終報告則須至少包含：1. 漏洞之嚴重性與影響範圍; 2.已利用或正在利用該漏洞之惡意行為者之資訊（若能取得）；以及 3. 已提供之安全更新或其他修補措施之詳細資訊。*Id.* arts. 14.1, 14.2.
[31] *Id.* art. 32.
[32] *Id.* Annex VIII.

「符合型式聲明（Conformity to type）」以證明產品符合本規則最低要求；第四部分則為，建立品管措施並向主管機關申請查驗，以確保法遵要求之落實。

（二）進口商與通路商之義務

1. 通報產品重大網路風險

進口商與通路商應於發現產品具有重大網路安全風險時，即時通知產品製造商並通報市場監督機構[33]。

2. 提供網路安全資料

應於市場監督機構要求下，提供足以證明產品製造商已採取適當措施使系爭產品符合網路安全要求之文件[34]。

四、罰則

任何試圖規避本規則之企業都將面臨鉅額罰款。依照違規態樣之不同，違規之企業可能被處以最高 1,500 萬歐元，或該企業前一會計年度之全球年營業額 2.5%之之行政罰鍰，以兩者較高者為準[35]；或被處以最高 1,000 萬歐元或前一會計年度之全球年營業額 2%之行政罰鍰，以兩者較高者為準[36]。若企業向市場監督機構提供錯誤、不完整或虛假資訊，將面臨 500 萬歐元或前一會計年之度全球年營收 1%的罰款，以兩者較高者為準[37]。

參、本規則對 WTO 與國際貿易之可能影響

自歐盟公布本規則草案起，其規範內容便引發各界廣泛關注，包含中國等 WTO 會員分別於 2023 年 7 月、11 月以及 2024 年 3 月之 TBT 委員會會議上，就歐盟於 2022 年 11 月 29 日針對草案發布之技術性法規通知文件（TBT 通知）

[33] *Id.* art. 19.3, 20.3.
[34] *Id.* art. 19.7, 20.5.
[35] *Id.* art. 64.2.
[36] *Id.* art. 64.3.
[37] *Id.* art. 64.4.

[38]，對草案及部分條文提出貿易關切[39]；以及草案公開諮詢期間，引起多位產業專家、企業與其他利害關係人之擔憂[40]。對此，歐盟於本規則之審議期間雖有參考貿易關切與利害關係人之意見就草案部分條文進行修正[41]，惟亦有許多重要條文未修正，或修正幅度不如預期等，故相關擔憂依然存在，以下將歸納該等規範不符比例原則之處，並分析其對 WTO 與國際貿易之可能影響。

一、規範手段不具適當性

中國於貿易關切中指出，按本規則附件一第二部分第(1)款規定，製造商應識別並記錄具數位元素產品所含之漏洞與組成元件，包括制定軟體物料清單（Software Bill of Materials, SBOM）[42]，又按附件七第 2(b)款，主管機關於合理情況下得要求製造商將 SBOM 納入其編製之技術文件中[43]，故按本規則第 13.22 條之規定，製造商即可能須於主管機關要求下提供含有 SBOM 之技術文件；惟

[38] Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 (COM(2022) 454 final), G/TBT/N/EU/936 (Nov. 29, 2022), https://www.epingalert.org/en/Search?&viewData=%20G%2FTBT%2FN%2FEU%2F936. 在 TBT 協定下，WTO 會員就其欲制定之技術性法規（technical regulation）或標準（technical standards）等非關稅措施有嚴重影響貿易之虞時，有義務透過 WTO 祕書處通報該規則草案之內容並於 e-ping 平台公告之，對該規範有疑慮之會員並得於 TBT 委員會提起特定貿易關切（specific trade concerns, STCs）並進行協商。*Transparency Obligations*, WTO, https://www.wto.org/english/tratop_e/tbt_e/tbt_notifications_e.htm (last visited Dec. 25, 2024); *Committee on Technical Barriers to Trade*, WTO, https://www.wto.org/english/tratop_e/tbt_e/tbt_com_e.htm (last visited Dec. 25, 2024).

[39] Committee on Technical Barriers to Trade, *Minutes of The Meeting 21-23 June 2023*, paras. 3.25-3.33, WTO Doc. G/TBT/M/90 (Sept. 21, 2023) [hereinafter STC 2023/09/21]; Committee on Technical Barriers to Trade, *Minutes of The Meeting 8-10 November 2023*, paras. 2.117-2.123, WTO Doc. G/TBT/M/91 (Feb. 1, 2024) [hereinafter STC 2024/02/01]; Committee on Technical Barriers to Trade, *Minutes of The Meeting 13-15 March 2024*, paras. 2.66-2.68, WTO Doc. G/TBT/M/92 (May 24, 2024) [hereinafter STC 2024/05/24].

[40] Michael Hill, *Industry Groups Call for Changes to EU Cyber Resiliency Act*, CSO (July 13, 2024), https://www.csoonline.com/article/645994/industry-groups-call-for-changes-to-eu-cyber-resiliency-act.html.

[41] 這些修正以及所參照之意見諸如：刪除草案附件一第 1(2)條：「產品交付時不得有任何已知之網路安全漏洞」之規定，以避免為廠商帶來過高之違約風險；將草案第 11 條下，廠商須於知悉後 24 小時內通報產品網路安全漏洞與相關網路安全事件之規定，改為比照歐盟 NIS2 指令，分階段、分程度之通報程序，避免廠商於來不及修補該漏洞之情況下即須公開漏洞，導致網路安全風險之擴散等。*Horizontal Cybersecurity Requirements for Products with Digital Elements*, LEGISLATIVE TRAIN SCHEDULE, EUR. PARLIAMENT (Nov. 20, 2024), https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act?sid=8601.

[42] SBOM 可視為一份軟體之成分／結構清單，此清單中以電腦可判讀之格式，詳細列舉該軟體之組成元件、元件的相關資訊、元件間之聯結，以及如元件供應商名稱等供應鏈關係，持有清單者將可透過檢視清單內容，找出軟體中之網路安全漏洞及相關元件來源。NTIA MULTISTAKEHOLDER PROCESS ON SOFTWARE COMPONENT TRANSPARENCY FRAMING WORKING GROUP, FRAMING SOFTWARE COMPONENT TRANSPARENCY: ESTABLISHING A COMMON SOFTWARE BILL OF MATERIALS (SBOM) 7, 26 (2d ed. 2021).

[43] CRA, Annex VII, art. 2(b).

SBOM 通常被視為製造商之商業機密，且於應用情境上仍缺乏共識，若因歐盟對其保護措施不足導致軟體技術資訊外洩[44]，可能會使軟體面臨更加精準之網路安全攻擊，使系爭產品暴露於更大之網路安全風險中[45]。

產業專家、企業與其他利害關係人亦有類似擔憂：其向歐盟提出之聯合倡議中指出，本規則第 14.1 至第 14.4 條要求製造商通報網路安全漏洞之規定[46]，意謂數個歐盟主管機關將持有記錄該等尚未修補網路安全漏洞之軟體並即時更新之資料庫，該資料庫所列軟體可能容易成為惡意行為人之攻擊目標，而歐盟卻不一定能妥善利用該資料庫來維護網路環境，徒增系爭產品暴露於網路安全威脅中之風險[47]。

二、規則之要求造成不必要的貿易限制

中國亦於貿易關切中指出，許多條文因設下過苛之義務或過短之時程，致使廠商法遵成本過高，恐有阻礙自由貿易之虞，如本規則第二章第 13.9 條規定，製造商提供之軟體安全性更新應維持至少 10 年[48]，惟考量某些產品，特別是消費性產品的使用壽命不足 10 年，故該條規定之最低期限並不合理[49]；對於第 14.1 至第 14.4 條規定之通報義務[50]，考量到即便是早期預警通知，廠商仍須就網路安全漏洞進行資訊蒐集、漏洞驗證，並識別受影響產品等，故 24 小時內通報之要求仍可能過苛，且分階段之重複通報可能為製造商帶來不必要之負擔[51]；而就第 13.12 條要求廠商須於上市前完成符合性評估程序之規定[52]，考量產品出現網路安全漏洞之時機不可預測，甚至可能在產品運送過程中才被發現，故無法預測產品完成符合性評估程序而達到上市標準之時間點，使製造商於法規遵循上面臨困境[53]。

產業專家、企業與其他利害關係人則擔憂，由於本規則所涵蓋產品之範圍相當廣泛，在目前歐洲之認證機構量能不足，無法負荷如此大量產品的符合性評估程序，故業者將面臨產品無法於歐盟上市之瓶頸。而少了該些關鍵產品之投入，將對供應鏈產生巨大影響，不利歐洲經濟與綠色轉型[54]；另一方面，因為科技公

[44] STC 2024/05/24, *supra* note 39, para. 2.67.
[45] STC 2024/02/01, *supra* note 39, para. 2.121.
[46] CRA, *supra* note 1, arts. 14.1-14.4.
[47] Letter from Tony Anscombe, Chief Security Evangelist, ESET et al., to Thierry Breton, Commissioner for Internal Market, Eur. Comm'n (Oct. 3, 2023).
[48] CRA, *supra* note 1, art 13.9.
[49] STC 2024/05/24, *supra* note 39, para. 2.67.
[50] CRA, *supra* note 1, arts. 14.1-14.4.
[51] STC 2024/05/24, *supra* note 39, para. 2.67.
[52] CRA, *supra* note 1, art 13.12.
[53] STC 2024/02/01, *supra* note 39, para. 2.120.
[54] Letter from Dr. Roland Busch, President and CEO of Siemens AG et al., to Margaritis Schinas, Vice-President, Eur. Comm'n et al. (Nov. 6, 2023).

司與新創企業通常仰賴快速的開發週期以回應市場需求，藉此維持競爭力，故本規則下嚴格之符合性評估程序與法遵要求將造成企業之行政負擔，可能會導致產品開發週期延長，影響新產品上市所需的時間，進而減緩產品創新之步伐[55]。

三、規範不明確而不合比例性

接著，中國於貿易關切中指出，許多條文因規範文字本身或其定義不明確，致使影響範圍難以評估，並有阻礙自由貿易之虞，這些擔憂包含：1. 本規則第一章第 2.1 條與第 3(1)條對於「具數位元素產品」與「已獨立上市流通之軟體元件」之定義與範圍未臻明確，就後者而言，因軟體可由消費者於世界任何一處透過網路下載，故難以判斷該產品是否已於（歐盟成員國）市面流通，企業難以評估本規則所涵蓋之產品範圍或受網路安全問題影響之範圍，使得相關法遵義務窒礙難行[56]；2. 本規則第二章第 14.8 條通知義務中，未明確定義產品用戶（users of the product）之範圍[57]，然而，系爭產品上市後將透過在地管道轉售或銷售，製造商無從得知最終用戶為何，故此規定將導致製造商陷於無法履行該條之通知義務之窘境[58]；3. 本規則第二章第 19.3 條[59]，以及第五章第 54.2 條、第 56.2 條均未釐清條文中「非技術性風險因素（non-technical risk factors）」之判斷標準[60]，因而如其中 19.3 條要求進口商於系爭產品因非技術性風險因素而有重大網路安全風險疑慮時應通報市場監督機構之規定[61]，將使得系爭產品可能因具備非技術性風險而按第 19.5 條須撤回或召回[62]，從而影響歐盟與歐盟成員國之市場開放程度；進一步言，非技術性風險因素模糊之判斷標準，將可能被濫用於制定保護主義之貿易限制措施，從而產生違反最惠國待遇（Most Favorite Nation, MFN）及國民待遇（National Treatment, NT）原則之潛在風險[63]。

四、小結

由此可見，正如 WTO 會員之關切及產官學界人士之擔憂，本規則部分條文之規範模式不僅可能無法達成原有立法目的，反而可能擴大系爭產品之網路安全風險，使得該等規範欠缺適當性；而部分條文雖能達成立法目的，但因其設下之義務過於嚴苛或涵蓋範圍過廣，已然逾越必要限度；抑或是部分條文因規範內容

---

55 Rita Sousa e Silva, *Cyber Resilience Act: From European Cooperation to Exposure Risk*, ITSECURITY (July 2, 2024), https://www.itsecurity.pt/news/compliance/cyber-resilience-act-da-cooperacao-europeia-ao-risco-de-exposicao.
56 STC 2023/09/21, *supra* note 39, para. 3.26.
57 CRA, *supra* note 1, art 14.8.
58 STC 2024/02/01, *supra* note 39, para. 2.120.
59 CRA, *supra* note 1, art. 19.3.
60 *E.g. id.* art. 56.2.
61 *Id.* art. 19.3.
62 *Id.* art. 19.8.
63 STC 2024/02/01, *supra* note 39, para. 2.118.

不明確或未臻詳盡，不但未降低原有之網路安全風險，反而產生其他方面的新風險，使得該等規範造成之效益與損害之間不合比例。綜上所述，本規則部分條文有違反比例原則之虞，並可能影響、限制國際貿易，甚至違反國際貿易規則。

肆、結論

《網路韌性法》誕生於高度互聯，且涉及複雜地緣政治關係的全球數位環境，隨著歐盟在網路安全威脅日益加劇之緊張局勢中加固其網路安全防線，本規則之實施將使得全球範圍之製造商皆需進行相應調整，以符合歐盟嚴格之網路安全要求。其中，中國因為生產多數資通訊產品而在供應鏈中扮演關鍵角色[64]，故成為受本法影響之主要對象，使當地製造商需面臨嚴格歐盟網路安全標準之挑戰，並促使中國於 WTO 提出特定貿易關切。本規則影響廣泛且嚴格之規範內容，不僅可能對市場營運者施加過多法遵義務，影響產品之上市時程；亦可能導致製造商因製造成本上升而將該成本轉嫁，使得消費者福祉降低，且本規則部分條文違反比例原則、影響國際貿易之虞，亦可能導致歐盟與他國緊張之貿易關係。待本規則實施後，將對歐盟市場乃至國際貿易環境造成何種影響，以及歐盟將如何應對，值得後續關注。

[64] 整體而言，中國佔全球 ICT 產品出口的 32%，佔 ICT 服務出口的 6%。2017 年，中國對外直接投資的 11%流向 ICT 產業。LONGMEI ZHANG & SALLY CHEN, CHINA'S DIGITAL ECONOMY: OPPORTUNITIES AND RISKS 5 (2019).