英國NCSC針對使用高風險供應商之電信網路提出風險管理建議

英國於2020年1月31日正式脫歐，同時積極爭取與重要貿易夥伴美國簽訂自由貿易協定（Free Trade Agreement, FTA）。然而，美國認定中國大陸華為的5G設備存在資安風險，可能被用於間諜活動進而威脅國家安全，故主張美英貿易合作與情報共享的前提，必須建立在英國排除使用華為5G網路基礎建設之上，對此英國嘗試透過政策研擬，在5G經濟發展與國家安全間求取平衡。英國國家網路安全中心（National Cyber Security Centre, NCSC）於2020年1月28日，即針對使用「高風險供應商（High risk vendors簡稱HRV）」之電信網路，提出風險管理建議，說明如何因應HRV帶來的網路安全風險及挑戰（須注意高風險供應商HRV不一定是關鍵供應商Critical Vendor，必須透過關鍵與否及風險高低兩個變動因素加以細部區分）。目前英國5G及光纖到戶（Fiber To The Home, FTTH）計畫推動處於關鍵階段，NCSC向電信營運商提出有關使用HRV設備的非拘束性技術建議，將有助於保護營運商免於外部攻擊，並降低英國電信網路的國家安全風險。

NCSC在報告中，針對何謂高風險供應商，及如何管理這些供應商帶來的特定安全風險，提出詳盡判斷標準包括：供應商在英國及其他地區網路中的戰略地位及規模、對網路安全控管品質及透明度、過去商業行為及慣例、向英國營運商供應技術的穩定性及彈性等。另外供應商有無接受外國政府補貼及營業地點是考量重點：包括該廠商所屬國家政府機構對其施加影響之程度、是否具備攻擊英國網路能力、業務營運的重要組成部分是否受到本國法律監管，進而與英國法律相抵觸甚至進行外部指導等。

又為減少由HRV引起的網路安全風險，NCSC對於HRV控管提出具體建議。包括應限制在5G或FTTP網路核心功能中使用HRV產品及服務，並將高風險廠商供應上限設定為35%，有效進行網路安全風險管理，平衡安全性風險和市場供應多樣化彈性需求。另外，其他具備敏感性的網路營運模式，例如大量個資蒐集、語音系統、記錄備份系統、寬頻遠端接入系統（BNG / BRAS）等，必須根據具體情況，對HRV進行限制；且不得在與政府營運或重要國家基礎設施，及任何與安全系統直接相關的敏感網路中使用HRV設備。目前，中國大陸華為是英國NCSC唯一認定的HRV廠商，華為被禁止參與英國5G網路建設的核心部分且受有市占率35%的供應限制；華為亦需遵守NCSC要求，訂定風險緩解策略，確保產品及服務不致威脅英國網路即國家安全。

本文為「經濟部產業技術司科技專案成果」

相關連結

- NCSC advice on the use of equipment from high risk vendors in UK telecoms networks
- 歐盟《5G網絡安全風險聯合評估報告》

你可能會想參加

- → 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
- → 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
- → 供應鏈資安國際法制與政策趨勢分享會
- → 新創採購-政府新創應用分享會
- → 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- → 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- → 商業服務業個資保護宣導說明會
- → 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
- → 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
- → 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

許祐寧
專案經理 編譯整理

上稿時間：2020年05月

進階閱讀：
劉芷宜，歐盟《5G網絡安全風險聯合評估報告》，科法新知快遞，2020年2月，https://stli.iii.org.tw/article-detail.aspx?tp=5&i=0&d=8392&no=67（最後瀏覽日:2020/03/29）。

文章標籤

資訊安全 | 5G | 資通安全管理法

推薦文章