初探物聯網的資通安全與法制政策趨勢

初探物聯網的資通安全與法制政策趨勢

資訊工業策進會科技法律研究所
2021年03月25日

壹、事件摘要

在5G網路技術下，物聯網（Internet of Things, IoT）的智慧應用正逐步滲入各場域，如智慧家庭、車聯網、智慧工廠及智慧醫療等。惟傳統的資安防護已不足以因應萬物聯網的技術發展，需要擴大供應鏈安全，以避免成為駭客的突破口[1]。自2019年5月「布拉格提案[2]」（Prague Proposal）提出後，美國、歐盟皆有相關法制政策，試圖建立各類資通訊設備、系統與服務之安全要求，以強化物聯網及相關供應鏈之資安防護。是以，本文觀測近年來美國及歐盟主要的物聯網安全法制政策，以供我國借鏡。

貳、重點說明

一、美國物聯網安全法制政策

（一）核心網路與機敏性設備之高度管制

1.潔淨網路計畫

基於資訊安全及民眾隱私之考量，美國政府於2020年4月提出「5G潔淨路徑倡議[3]」（5G Clean Path initiative），並區分成五大構面，包括：潔淨電信（Clean Carrier）、潔淨商店（Clean Store）、潔淨APPs（Clean Apps）、潔淨雲（Clean Cloud）及潔淨電纜（Clean Cable）；上述構面涵蓋之業者只可與受信賴的供應鏈合作，其可信賴的標準包括：設備供應商設籍國的政治與治理、設備供應商之商業行為、（高）風險供應商網路安全風險緩和標準，以及提升供應商信賴度之政府作為[4]。

2.政府部門之物聯網安全

美國於2020年12月通過《物聯網網路安全法[5]》（IoT Cybersecurity Improvement Act of 2020），旨在提升聯邦政府購買和使用物聯網設備的安全性要求，進而鼓勵供應商從設計上導入安全防範意識。本法施行後，美國聯邦政府機關僅能採購和使用符合最低安全標準的設備，將間接影響欲承接政府物聯網訂單之民間業者及產業標準[6]。

另外，美國國防部亦推行「網路安全成熟度模型認證[7]」（Cybersecurity Maturity Model Certification, CMMC），用以確保國防工程之承包商具備適當的資訊安全水平，確保政府敏感文件（未達機密性標準）受到妥適保護。透過強制性認證，以查核民間承包商是否擁有適當的網路安全控制措施，消除供應鏈中的網路漏洞，保護承包商所持有的敏感資訊。

（二）物聯網安全標準與驗證

有鑑於產業界亟需物聯網產品之安全標準供參考，美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）提出「物聯網網路安全計畫」，並提出各項標準指南，如IR 8228：管理物聯網資安及隱私風險、IR 8259（草案）：確保物聯網裝置之核心資安基準等。

此外，美國參議院民主黨議員Ed Markey亦曾提出「網路盾」草案[8]（Cyber Shield Act of 2019），欲建立美國物聯網設備驗證標章（又稱網路盾標章），作為物聯網產品之自願性驗證標章，表彰該產品符合特定產業之資訊安全與資料保護標準。

二、歐盟物聯網安全法制政策

（一）核心網路安全建議與風險評估

歐盟執委會於2019年3月26日提出「5G網路資通安全建議[9] 」，認為各會員國應評鑑5G網路資通安全之潛在風險，並採取必要安全措施。又在嗣後提出之「5G網路安全整合風險評估報告[10] 」中提及，5G網路的技術漏洞可能來自軟體、硬體或安全流程中的潛在缺陷所導致。雖然現行3G、4G的基礎架構仍有許多漏洞，並非5G網路所特有，但隨著技術的複雜性提升、以及經濟及社會對於網路之依賴日益加深，必須特別關注。同時，對供應商的依賴，可能會擴大攻擊表面，也讓個別供應商風險評估變得特別重要，包含供應商與第三國政府關係密切、供應商之產品製造可能會受到第三國政府施壓。

是故，各會員國應加強對電信營運商及其供應鏈的安全要求，包括評估供應商的背景、管控高風險供應商的裝置、減少對單一供應商之依賴性（多元化分散風險）等。其次，機敏性基礎設施禁止高風險供應商的參與。

（二）資通安全驗證制度

歐盟2019年6月27日生效之《網路安全法[11]》（Cybersecurity Act），責成歐盟網路與資訊安全局（European Union Agency for Cybersecurity, ENISA）協助建立資通訊產品、服務或流程之資通安全驗證制度，確保資通訊產品、服務或流程，符合對應的安全要求事項，包含：具備一定的安全功能，且經評估能減少資通安全事件及網路攻擊風險。原則上，取得資安驗證之產品、服務及流程可通用於歐盟各會員國，將有助於供應商跨境營運，同時能協助消費者識別產品或服務的安全性。目前此驗證制度為自願性，即供應商可以自行決定是否對將其產品送交驗證。

參、事件評析

我國在「資安即國安」之大架構下，行政院資通安全處於2020年底提出之國家資通安全發展方案（110年至113年）草案[12]，除了持續強化國家資安防禦外，對於物聯網應用安全亦多有關注，其間，策略四針對物聯網應用之安全，將輔導企業強化數位轉型之資安防護能量，並強化供應鏈安全管理，包括委外供應鏈風險管理及資通訊晶片產品安全性。

若進一步參考美國與歐盟的作法，我國後續法制政策，或可區分兩大性質主體，採取不同管制密度，一主體為受資安法規管等高度資安需求對象，包括公務機關及八大領域關鍵基礎設施之業者與其供應鏈，其必須遵守既有資安法課予之高規格的安全標準，未來宜完善資通設備使用規範，包括：明確設備禁用之法規（黑名單）、高風險設備緩解與准用機制（白名單）。

另一主體則為非資安法管制對象，亦即一般性產品及服務，目前可採軟性方式督促業者及消費者對於資通設備安全的重視，是以法制政策推行重點包括：發展一般性產品及服務的自我驗證、推動建構跨業安全標準與稽核制度，以及鼓勵聯網設備進行資安驗證與宣告。

[1]經濟部工業局，〈物聯網資安三部曲：資安團隊+設備安全+供應鏈安全〉，2020/08/31，https://www.acw.org.tw/News/Detail.aspx?id=1149（最後瀏覽日：2020/12/06）。

[2]2019年5月3日全球32個國家的政府官員包括歐盟、北大西洋公約組織 （North Atlantic Treaty Organization, NATO）的代表，出席由捷克主辦的布拉格5G 安全會議 （Prague 5G Security Conference），商討對5G通訊供應安全問題。本會議結論，即「布拉格提案」，建構出網路安全框架，強調5G資安並非僅是技術議題，而包含技術性與非技術性之風險，國家應確保整體性資安並落實資安風險評估等，而其中最關鍵者，為確保5G基礎建設的供應鏈安全。是以，具體施行應從政策、技術、經濟、安全性、隱私及韌性（Security, Privacy, and Resilience）之四大構面著手。Available at GOVERNMENT OF THE CZECH REPUBLIC, *The Prague Proposals*, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/ (last visited Jan. 22, 2021).

[3]*The Clean Network*, U.S Department of State, https://2017-2021.state.gov/the-clean-network/index.html (last visited on Apr. 09, 2021)； *The Tide Is Turning Toward Trusted 5G Vendors*, U.S Department of State, Jun. 24, 2020, https://2017-2021.state.gov/the-tide-is-turning-toward-trusted-5g-vendors/index.html (last visited Apr. 09, 2021).

[4]CSIS Working Group on Trust and Security in 5G Networks, *Criteria for Security and Trust in Telecommunications Networks and Services* (2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511_Lewis_5G_v3.pdf (last visited Nov. 09, 2020).

[5]*H.R. 1668: IoT Cybersecurity Improvement Act of 2020*, https://www.govtrack.us/congress/bills/116/hr1668 (last visited Mar. 14, 2021).

[6]孫敏超，〈美國於2020年12月4日正式施行聯邦《物聯網網路安全法》〉，2020/12，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8583（最後瀏覽日：2021/02/19）。

[7]U.S. DEPARTMENT OF DEFENSE, *Cybersecurity Maturity Model Certification*, https://www.acq.osd.mil/cmmc/draft.html (last visited Nov. 09, 2020).

[8]*H.R.4792 - Cyber Shield Act of 2019*, CONGRESS.GOV, https://www.congress.gov/bill/116th-congress/house-bill/4792/text (last visited Feb. 19, 2021).

[9]*COMMISSION RECOMMENDATION Cybersecurity of 5G networks*, Mar. 26, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA (last visited Feb. 18, 2021).

[10]European Commission, *Member States publish a report on EU coordinated risk assessment of 5G networks security*, Oct. 09, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 (last visited Feb. 18, 2021).

[11]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Council Regulation

2019/881, 2019 O.J. (L151) 15.

[12]行政院資通安全處，〈國家資通安全發展方案（110年至113年）草案〉，2020/12，https://download.nccst.nat.gov.tw/attachfilehandout/%E8%AD%B0%E9%A1%8C%E4%BA%8C%EF%BC%9A%E7%AC%AC%E5%85%AD%E6%9C%9F%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E7%99%BC%E5%B1%95%E6%96%B9%E6%A1%88(%E8%8D%89%E6%A1%88)V3.0_1091128.pdf（最後瀏覽日：2021/04/09）。

相關連結

- 物聯網資安三部曲：資安團隊+設備安全+供應鏈安全
- GOVERNMENT OF THE CZECH REPUBLIC, The Prague Proposals
- The Clean Network
- The Tide Is Turning Toward Trusted 5G Vendors
- H.R. 1668: IoT Cybersecurity Improvement Act of 2020
- 美國於2020年12月4日正式施行聯邦《物聯網網路安全法》
- Cybersecurity Maturity Model Certification
- H.R.4792 - Cyber Shield Act of 2019
- Member States publish a report on EU coordinated risk assessment of 5G networks security
- COMMISSION RECOMMENDATION Cybersecurity of 5G networks

相關附件

- Criteria for Security and Trust in Telecommunications Networks and Services [pdf]
- 國家資通安全發展方案（110年至113年）草案 [pdf]

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
- → 112年度「領航臺灣數位轉型」國際研討會-實體場
- → 112年度「領航臺灣數位轉型」國際研討會-直播場
- → 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
- → 電商零售業法制宣導說明會暨產學研座談會
- → 數位海盜時代來臨–抵禦海上資安威脅的實踐與挑戰
- → 零售業個資保護宣導暨座談會
- → 零售業個資保護及資訊安全教育講習
- → 零售業個資保護及資訊安全教育講習

吳采薇
法律研究員 編譯整理

上稿時間：2021年04月

文章標籤

物聯網　資訊安全

推薦文章