專題探索

5G網路安全與資安防護

蔡佳君

5G行動通訊技術賦予既有通訊產業、數位經濟與服務應用變革動能，惟5G網路涉及國家安全、經濟安全、其他國家利益與全球穩定，因此各國際組織也日益重視資安保護措施。本文分析布拉格提案、歐盟5G網路安全工具箱、美國5G乾淨網路等最新三大指標性5G網路安全與資訊保護提案趨勢，另從資安防護政策方針與策略重點所概括供應鏈威脅安全措施、政策治理措施等面向，概述保障5G網路安全及資安防護，已成為各國監理機關及各產業的重要課題。

根據世界經濟論壇(World Economic Forum, WEF)2018、2019年全球風險報告，網路攻擊(Cyberattacks)被列為全球前五大風險。報告指出5G網路、量子計算及人工智慧創造機會的同時也帶來威脅，缺乏國際組織、國家治理框架，將可能導致網路空間碎裂化(cyberspace fragmentation)，阻礙經濟成長、加劇地緣政治衝突與擴大社會內部分歧，資安防護的重要性不言而喻。

是以，國際組織、國家治理框架推動網路安全及資安防護已蔚為趨勢。2019年5月於捷克首都布拉格舉辦之全球5G安全會議發布「布拉格提案」聲明，以因應未來5G時代潛在的安全威脅，該提案針對「政策」、「技術」、「經濟」與「安全性、隱私及彈性」四大面向提出建言。歐盟執委會(European Commission, EC)於2020年1月29日批准歐盟5G網路安全工具箱(Cybersecurity of 5G networks -EU Toolbox of Risk Mitigating Measures)，以解決歐盟成員國共同評估後所確立的所有風險。美國國務卿蓬佩奧(Mike Pompeo)於2020年4月29日代表川普政府對外倡議，將透過建立「乾淨路徑」(Clean Path)鞏固並提升美國所有外交機構5G通訊網路安全性，並進一步制定5G乾淨網路(5G Clean Network)倡議框架。爰此，

本文擬針對布拉格提案、歐盟5G網路安全工具箱及美國乾淨網路彙整分析，並歸納三大代表性資安防護政策方針面向與策略重點。

布拉格提案針對「安全性、隱私權及彈性」面向提出之建議，強調對供應商與網路技術安全性及風險評估須考量法治、安全環境、供應商責任等，且應符合開放、互操作性及產業最佳作業流程。

布拉格提案

由於5G網路安全對國家安全、經濟安全、其他國家利益與全球穩定相當重要，布拉格5G網路安全會議(Prague 5G Security Conference)針對5G網路架構與功能安全級別制定進行討論。

（一）5G網路架構與功能安全級別制定之考量因素

布拉格提案針對5G網路架構與功能安全級別列出十項考量因素。

1.網路安全不僅是單純技術問題，安全、彈性且有保障的基礎設施具備適當的國家戰略、健全的政策與全面的法律框架，且需要接受培訓與教育的專業人員參與，共同強化網路安全才能保護公民自由與隱私。

2.在處理網路安全威脅時，不僅應考慮其技術性質，更應考慮特定政治、經濟或其他惡意人士濫用國家通訊技術依賴性。

3.基於5G網路廣泛應用，通訊系統未授權接取可能暴露前所未有的訊息量，甚至可能破壞整個社會過程。

4.維護通訊基礎設施的網路安全不僅是經濟或商業問題，因此高水準的網路安全政策或法案制定上，除主要利害關係人（業者或技術提供者）外，亦須考量其他會對安全級別產生重大影響之領域或產業，如教育、外交、研究與開發的利害關係人。

5.制定包含網路安全技術和非技術系統性，且完善的風險評估，對創造並維持真正有彈性的基礎架構而言至關重要，故於風險安全框架制定上，應納入最先進的政策和手段以減少安全風險。

6.網路安全措施涵蓋範圍必須足夠廣泛，以包含整個安全風險，即營運和戰略層面的人員、流程、物理基礎設施與工具。

7.在制定適當措施以提高安全性時，應考量獨特的社會和法律框架、經濟、隱私、技術自給自足及各國其他重要相關因素。

8.創新是現代社會發展和經濟成長的主要動力，同時催化新的安全解決方案，故政策、法律和規範於安全措施制定上應具有靈活性，以兼顧安全性與各國情形。

9.為達適當的安全等級，應容許成本增加。

10.所有利害關係人共同負擔供應鏈安全風險責任，而通訊基礎設施業者通常依賴其他供應商的技術。主要安全風險來自提供資訊與通訊科技(Information and Communication Technology, ICT)設備供應鏈日益全球化與跨境複雜性，而此等風險應被視為風險評估的一部分，並應努力防止受損裝置擴散，以及

惡意程式碼或功能的使用。

（二）布拉格提案四大面向建議

布拉格提案針對「政策」、「技術」、「經濟」與「安全性、隱私權及彈性」等四大面向提出建議。

1.政策

通訊網路和服務的設計應考量到彈性和安全性，應使用國際的、公開的、基於共識的標準和具有風險意識的網路安全最佳實踐來建構和維護，並應促進制定明確的全球可互操作網路安全指南，以支持網路安全產品和服務，提高所有利害關係人的應變能力。根據國際法，每個國家皆得自由制定自己的國家安全和執法要求，並應尊重隱私且遵守資訊保護，免遭不當蒐集和濫用的準則；網路管理和連接(Connectivity)服務的法律和政策，應遵循透明性和公平性原則，且須充分監督及尊重法治；亦應考慮到第三國對供應商的總體影響風險。

2.技術

利害關係人應在產品發布之前和系統運行期間，定期在所有組件和網路系統內進行漏洞評估和風險抵免，並促進查找(Find)、修復(Fixes)、修補(Patches)的文化，以降低已發現的漏洞並快速修復或修補。供應商產品的風險評估應考慮包括適用的法律環境和供應商生態系統等所有相關因素，且在建立彈性和安全性時，應考慮到惡意網路活動並非總必須來自技術漏洞（例如有內部攻擊的情況）。為了增加全球通訊的利益，各國應採取政策以實現網路數據流的效率和安全。利害關係人應考慮隨5G網路推出的技術變化，例如使用邊緣運算、軟體定義網路、網路功能虛擬化通訊網路安全性影響。此外，亦必須讓使用者瞭解在最新技術下產品或服務安全等級的元件和軟體來源的影響。

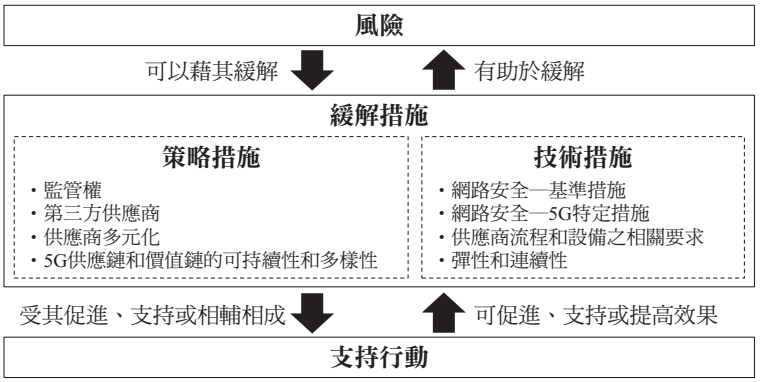
3.經濟

具多樣性且活躍的通訊設備市場與供應鏈對安全性和經濟彈性至關重要。強化研發投資有助於全球經濟與技術進步，並能作為提高技術解決方案多樣性與通訊網路安全的潛在做法。應以最佳實務標準進行通訊網路與網路服務之採購、投資及簽約，且須公開透明。國家對5G通訊網路和服務業者的獎勵、補貼或融資，應注重公平原則、商業合理性、開放市場競爭原則與貿易義務，過程須公開透明。另須有效監督影響通訊網路發展的關鍵金融與投資工具。而通訊網路和網路服務提供者，應有明確透明的所有權、合夥關係及公司治理結構。

4.安全性、隱私權及彈性

產業內之所有利益相關者應相互合作，以提高國家關鍵基礎設施網路、系統和連接設備之安全性和彈性。利益相關者應彼此互助、分享經驗與最佳實踐(Best Practice)，包括面對網路攻擊時提供降低風險、調查、響應、阻止、修復等幫助。供應商與網路技術之安全性和風險評估應考慮法治、安全環境與供應商未履行責任，並應符合開放性、可交互作用性、安全標準及產業最佳實踐，以促進產品與服務之網路安全發展。風險管理框架應遵循資料保護原則，以確保公民於使用網路設備與服務時的隱

附圖　歐盟5G網路安全工具箱關鍵策略與技術措施



資料來源：EC (2020)。

私。

布拉格提案建議各國應把第三國可能對設備商造成的整體影響納入考量，尤其應考慮第三國的治理模式中，是否缺乏安全合作協議或類似機制，以及該國是否為網路犯罪或數據保護協議的締約國等。另外，各國政府針對設備商和網路技術進行安全風險評估時，應考量法治、安全環境、設備商不法行為等，且應符合開放、互操作性、安全標準及產業最佳作業流程。

歐盟5G網路安全工具箱策略措施、技術措施等，皆表示對供應商風險評估的重視，呼籲各界確保採取多供應商策略，且確認供應商流程採取高採購標準；而美國乾淨網路中更具體為供應商評估標準與監督訂定判斷準則方針。

歐盟5G網路安全工具箱

5G網路安全工具箱係根據歐盟對5G網路安全的共同風險評估，提出的一系列安全措施，可有效降低風險並確保在歐洲布建安全的5G網路。歐盟5G網路安全工具箱之風險緩解計畫(Risk Mitigation Plan)，針對各種已識別風險提出對策，包括根據其有效性可能採取的措施組合（附圖），建立一套關鍵策略措施(Strategic Measures)和技術措施(Technical Measures)，提供所有成員國和執委會遵守，並可搭配支持行動提高效果，以下針對策略措施、技術措施與支持行動之內涵分項說明。

（一）策略措施

策略措施涵蓋提高主管機關規管權限，以審查網路採購與布建，辨認非技術性漏洞（Non-technical vulnerabilities，如受第三國干預），推廣永續多元的5G價值供應鏈，以避免系統性風

險及長期依賴性。八項策略措施包含：

1.強化國家主管機關角色。
2.審核業者並要求其提供資訊。
3.評估供應商風險，並限制高風險供應商活動，必要時禁止其對關鍵資產的使用。
4.管制託管服務(Managed Service Providers, MSPs)與設備供應商的第三方服務。
5.採取多供應商策略，確保行動網路業者有多元的供應商選擇。
6.強化彈性。
7.辨認關鍵資產，並在歐盟培育一個多樣且永續的5G生態系統。
8.維護多樣性，並建立歐盟在未來網路技術之能力。

（二）技術措施

技術措施包含提高技術、流程、人員與實體安全性，以強化5G網路與設備安全性。技術措施的有效性因其範圍和風險類型而有所不同，且僅靠技術措施將無法解決非技術漏洞。11項技術措施包含：

1.確保基本安全守則的應用（網路安全設計與架構）。
2.確保和評估現有5G標準中安全措施的執行。
3.確保嚴格的接取控制。
4.增強虛擬網路功能的安全性。
5.確保安全的5G網路管理、營運與監控。
6.強化實體安全性。
7.加強軟體完整性、更新與修補管理。
8.以健全的採購標準，提高供應商流程中的安全標準。
9.須採歐盟認證5G網路元件、設備與供應商流程。
10.非5G的資通訊產品與服務（例如連接設備、雲端服務），須採歐盟認證。
11.強化彈性與持續性規劃。

（三）支持行動

目標性支持行動可協助戰略和技術措施，進而提高前述兩者之有效性。十項支持行動包含：

1.審核與制定網路安全的準則與最佳實例。
2.以國家級及歐盟標準，加強測試與審核能力。
3.支持和形塑5G標準化。
4.制定在現行5G標準執行安全措施的指導方針。
5.透過歐盟認證計畫，確保標準技術與組織安全措施的應用。
6.交流執行策略措施的最佳實例，尤其為評估供應商風險的國家框架。
7.增進在事件處理與危機管理中的協調能力。
8.審核5G網路與其他關鍵服務的相互依存度。
9.加強合作、協調與分享機制。
10.確認政府補助的5G資訊發展計畫，將網路安全風險列入考量。

歐盟5G網路安全工具箱建議所有成員國應加強對行動網路業者的安全性要求、評估供應商的風險概況，並確保每個業者有適切的多元設備供應商策略，以避免或減少主要依賴於單一供應商，於國家層級確保供應商的適切平衡。歐盟執委會與成員國應一同致力於維持多樣化

且永續的5G供應鏈，以避免長期依賴性，以及藉由透過歐盟相關計畫和資金，進一步加強歐盟在5G與B5G技術的能力。同時促進成員國之間協調一致，就標準化實現特定安全目標，並發展有關歐盟範圍內的認證計畫，以促進更安全的產品和流程。為確保此協調方法禁得起時間考驗，須延長歐盟執委會及網路資訊安全協作小組(NIS Cooperation Group)工作授權及與其他相關企業的合作，以確保在委員會與歐盟網路安全機構(EU Agency for Cybersecurity, ENISA)的協助下，定期檢視國家與歐盟在5G與B5G網路安全性的風險評估，並進一步細緻化、調整風險評估的方法，以因應最新的5G科技發展。

美國5G乾淨網路

因應國際新興通訊技術發展及維護美國國家利益，保障並提升美國及理念相近國家之資訊及智慧財產權安全性與信任度極為重要。美國5G乾淨路徑排除華為及中興通訊等敏感設備供應商，為一條端到端(End-to-End)溝通路徑，要求所有往來於美國外交機構之數據，須透過經美國政府認可網路設備進行傳輸、控制、運算以及儲存等，可預期5G乾淨路徑帶來高標準之網路安全性，將有助於美國公民、金融機構及重要通訊基礎設施，抵禦來自敏感供應商之安全風險。以下就「電信網路及服務之安全及可信賴性評估標準」(Criteria for Security and Trust in Telecommunications Networks and Services)說明：

（一）電信網路及服務之安全及可信賴性評估標準

電信網路及服務之安全及可信賴性評估標準主要透過公開資訊，以評估潛在供應商之可信賴性和安全性，並形塑保障電信網路相關必要行動之國內政策。政府得平等及公開透明的使用本標準，客觀並全面的評估所有企業網路之風險及安全性。本標準分為四大面向共31項規範電信網路及服務之安全與可信賴性評估事項，詳細內容說明如下：

1.政治及治理標準(Political and Governance Criteria)

(1)若供應商總部係設立於民主選舉制度之國家（因此受制於國家法律和其他政府措施），則該供應商更值得信賴。本項可透過可行且獨立之反對黨的存在、現任政府政權移轉，以及國家司法、立法和行政職能之間的權力分立等證明。

(2)若供應商總部係設立於具有獨立司法機關的國家或地區，則該供應商更值得信賴。本項可透過紀錄顯示其尊重，如無罪推定原則和公開聽證權等行為、具審判不受不當拖延之權利，以及存在遵循既定程序與法律程序，且不受政治干預的法院或法庭等證明。

(3)若供應商總部設立於某一國家，而該國家治理網路和連通性服務的法律與政策係以尊重法治為原則，則表明該供應商更值得信賴。本項體現在政府行使權力時會受到明確的法律或司法限制，且有證據表明該限制有效。

(4)若供應商總部係設立於與採購方政府具安全

夥伴關係之國家，或採購方政府與供應商政府有簽署合作安全協議之國家，則該供應商更值得信賴。

(5)若供應商總部係設立於擁有明確個人資料保護紀錄之國家，則該供應商更值得信賴。本項可透過多邊協議、法律、法規、執法措施或獨立機關對資料保護的適當決定等證明。

(6)若供應商總部係設立於在遵守國際人權承諾方面具良好紀錄之國家，包含媒體自由且沒有審查、任意拘留或其他違反公認的人權慣例與國際準則等行為，則該供應商更值得信賴。

(7)若供應商係在考量到勞動條件、貿易慣例、人權和環境標準等因素的採購過程下被選擇的，而非基於成本導向，則該供應商更值得信賴。

(8)若供應商在公認的國際商業規範以外，表現出其與地主國政府(Host Government)之間存在相互依存關係的行為模式和慣例，則該供應商的可信賴度較低。評估標準包含法律或正式要求政府，或政黨代表涉入供應商的行政或管理部門，因此得以任意接近該公司的資料與營運，或出於情報目的強迫公司合作或施加義務，且其無權訴諸獨立司法機關。

(9)若供應商總部設立於某一國家，而該國家法律要求其與政府合作或給予政府特權，且不得在法院或國家立法機關提出異議，則該供應商的可信賴度較低。

(10)若供應商或其地主國政府曾從事掠奪性貿易行為（如傾銷、無條件補貼或刻意削價），或其他旨在創造不公平優勢之行為，則該供應商的可信賴度較低。

2.商業行為評估標準(Business Practices Assessment Criteria)

(1)若供應商擁有透明公開的所有權和公司治理結構，且得獨立驗證該結構，則該供應商更值得信賴。

(2)若供應商係公開交易，或在法規要求下須揭露資訊、允許政府對其進行審查，則該供應商更值得信賴。

(3)若供應商係進行公開且透明之融資，在採購、投資及簽約方面採用最佳做法，並有適當紀錄可供公眾或監管機關審查，則該供應商更值得信賴。

(4)若供應商能夠證明遵守並關注國際公認的會計準則（如一般公認會計原則和國際財務報導準則），則該供應商更值得信賴。

(5)若供應商過往皆符合盡職調查且行事合乎道德，包括尊重他人智慧財產權等，則該供應商更值得信賴。

(6)若供應商所有權結構不透明、係屬國有，或所有權僅限於一國公民，則該供應商的可信賴度較低。掩飾何人擁有、控制或影響上游公司，或使用任何其他機制隱瞞供應商與外國之間依存關係等不尋常的所有權安排皆屬不透明。

(7)若供應商有以下情形，則該供應商的可信賴度較低：受益於隱匿或不透明的財務支援或激勵措施、補助或其他商業上不合理的融資機制；缺乏透明度；為涉及掠奪性定價以消

除競爭之行動的一部分；迫使其他供應商退出市場；為政府意圖使競爭對手處於不利之作為的一部分。

3.網路安全風險緩解標準(Cybersecurity Risk Mitigation Criteria)

(1)供應商的電信基礎設施技術已成功通過獨立且可信的第三方評估、可信的國家風險評估、或技術與非技術方面（如供應商可能須遵循的法律和政策框架）的安全性評估流程。

(2)透過採購國或第三方評估或認證，以確保所評估技術確實被使用於產品中。

(3)供應商的產品與服務技術，係根據國際公認、公開且具共識的電信技術標準所設計、製造和維護。

(4)供應商能夠對組件和軟體來源提出保證，且具有政策與程序因應安全性和智慧財產權之要求，該政策與程序適用於其中納入的開源代碼，或用於導出任何提供予客戶的可交付成果。

(5)供應商遵循相關商業與技術慣例，對產品與服務的維護、更新與補救措施，維持透明性。

(6)供應商備有合理期間內告知與修補客戶發現的安全漏洞之紀錄。

(7)供應商所提供的營運支援，與國家網路安全政策及規則一致，供應商維護符合適用數據保護法規與要求的資訊安全治理政策，並能驗證其達成要求。

(8)供應商能夠證明其已進行充分監督，且與第三方產品組件供應商具有合約約束安全性與品質保證。

(9)供應商遵循安全的開發實作，並且能充分記錄軟體工具與原始碼(Source Code)生命週期管理。

(10)供應商已實施可驗證的技術措施，以確保嚴格存取控制的應用（限制授權用戶、代表授權用戶的授權程序或授權裝置），以及對具有與網路業者一致的網路安全政策的受支援網路進行安全監控。

4.政府採取作為提升選擇供應商之信心(Government Actions to Increase Confidence in Choosing a Supplier)

(1)各國政府應具備評估供應商風險狀況的政策與法律工具，並根據獨立性評估及採用上述非技術性標準之評估，確保供應商能證明其可信賴性。供應商應能證明其產品使用安全設計、軟體工程及有效的安全程序。

(2)各國政府與私部門應定期針對所有網路系統進行脆弱性評估及風險緩解。供應商產品的風險評估應包含技術面及非技術面，考量適用之法律環境及供應商生態系的其他面向，因該類因素可能關乎政府和私部門之安全維護措施。

(3)政府於國家網路基礎設施的政策上須避免採取單一化(Monocultures)政策，應鼓勵網路與系統組件供應商建立多樣化、可持續供應鏈。然而多樣性要求無法解決高風險供應商對於風險緩解策略的需求。

(4)各國政府應支持並鼓勵採用網路業者適用的

最佳安全實作(Best Security Practices)與實施現行電信標準中的安全措施，包括安全網路設計與架構、安全操作規則以及對功能外包的監測與限制。

（二）美國乾淨網路擴增計畫

蓬佩奧另亦於2020年8月5日宣布納入「乾淨電信業者」(Clean Carrier)、「乾淨應用商店」(Clean Store)、「乾淨應用程式」(Clean Apps)、「乾淨雲端」(Clean Cloud)，以及「乾淨電纜」(Clean Cable)等標準，以擴充及落實倡議框架。

結論與建議

5G行動通訊技術賦予既有通訊產業、數位經濟與服務應用變革動能，各國際組織也日益重視5G網路安全以及資訊安全保護措施，本文分析最新三大指標性5G網路安全與資訊保護提案趨勢，資安防護政策方針面向與策略重點可概括至兩大面向：供應鏈威脅安全措施與政策治理措施。

行動通訊業者需要依靠供應商所提供的基礎設施、產品及服務，而行動通訊業者的下游客戶則依靠基礎設施、產品及服務以管理或維持生活與業務，供應鏈威脅發生於當供應商出現風險或漏洞時，可能讓供應鏈成為攻擊目標(GSMA, 2020)。布拉格提案針對「安全性、隱私權及彈性」面向提出之建議，強調對供應商與網路技術安全性及風險評估須考量法治、安全環境與供應商責任等；歐盟5G網路安全工具箱策略措施、技術措施等，皆表示對供應商風險評估的重視，呼籲各界確保採取多供應商策略，且確認供應商流程採取高採購標準；而美國乾淨網路中更具體為供應商評估標準與監督訂定判斷準則方針。

布拉格提案將「政策治理措施」列為四大面向建議之一，目的在於呼籲各界以立法者之角度，針對通訊網路規管、法律政策制定框架；歐盟5G網路安全工具箱之策略措施，亦建議提高主管機關權限，進行網路採購審查與布建；而美國乾淨網路則強調，各國政府評估供應商風險狀況與網路業者最佳實務之重要性。5G帶來超大頻寬、超大連結、超可靠低延遲之創新技術與應用，影響將擴及政府、企業與民眾生活各層面，如何保障5G網路安全及資安防護，已成為各國監理機關及各產業的重要課題。

（作者為台灣經濟研究院助理研究員）

■參考文獻

1.World Economic Forum (2020), "The Global Risks Report 2020".
2.Government of the Czech (2019), "The Prague proposals".
3.European Commission (2020), "The EU toolbox for 5G security".
4.U.S. Department of State (2020), "The Clean Network".
5.CSIS (2020), "Criteria for Security and Trust in Telecommunications Networks and Services".