臺灣資安布局 ―由「布拉格提案」談起

淡江大學國際事務與戰略研究所博士候選人 ― 陳永全

資訊來源：法務部調查局清流雙月刊

摘要：

2019 年 5 月，全球 32 個國家齊聚捷克布拉格並公布「布拉格提案（The Prague Proposals)」，這是因應 5G 時代網路安全威脅的首次國際會議。

網路攻擊， 已躍升為全球前十大風險

世界經濟論壇（World Economic Forum，下稱 WEF）每年都會發表「全球風險報告」(The Global Risks Report)。過 去 15 年來的風險前 5 名都與環境有關。 惟根據 WEF 2021 年「 全 球 風 險 報 告 」 （16 th Edition）顯示（如下圖)，「資訊科技基礎設施故障」(IT infrastructure breakdown）已躍升為 2021 年全球風險具影響力的第 10 名；「數位權力集中」 (Digital power concentration)、「數位不平等」(Digital inequality）及「網路安全失效」(Cybersecurity failure）則晉升為 2020 年風險加劇的第 6、7 及第 9 名。

「布拉格提案」

歐盟、北大西洋公約組織、美、德、日、韓、澳等代表，於 2019 年 5 月齊聚於捷克布拉格，為 5G 安全召開國際會議。會議中強調各國於發展 5G 時，應考慮國家安全、經濟、法治與設備商不法行為等因素，以及後續的管理問題。會議成果經主辦國捷克彙整，成為「布拉格提案」。「布拉格提案」為首次探討 5G 議題之國際會議，其強調 5G 網路的開發、部署與商業化，必須建立在自由與公平競爭、透明以及法治基礎上，並提出 5G 安全及關鍵基礎設施防護等面向需進行國際交流與合作。參與國期望此提案內容能成為世界各國之資安防護共識。

「臺美 5G 共同宣言」延續 「布拉格提案」精神

基於「布拉格提案」精神，我國與美國於 2020 年 8 月共同發表「臺美 5G 共同宣言」(Joint Declaration on 5G Security)，臺美雙方宣示承諾在自由、公平競爭、透明及法治的基礎上，對 5G 通訊安全重要性的認知，通過加強對 5G 供應鏈的把關，確保 5G 通訊網路的安全，同時深化臺灣與美國在 5G 資安上的合作關係。 此項臺美 5G 安全共同宣言，代表美國與我國政府均認同 5G 通訊服務安全的重要性，為確保 5G 軟硬體供應商與供應鏈安全，應評估供應商是否可信賴，具體做法包括評估 5G 供應商是否在沒有獨立司法審查下，受外國政府控制；資金來源是否公開；還有供應商的所有權、管理結構、採

購、投資等資訊是否透明；是否尊重智慧財產權等。共同宣言中也倡議透過定期的更新與評鑑，將現有不受信任的軟硬體供應商，移轉為可信賴的供應商，提升雙方的資訊安全，善用 5G 通信網路提供的各項服務，同時確保提供一個更安全、具韌性與可信賴的 5G 行動通訊網路生態系統，並為民間提供創新的機會，在自由公平的環境中，促進數位經濟發展。

他山之石，可以攻錯

蔡總統在 2020 年就職演說中提出 6 大核心戰略產業，其中一項就是「發展結合 5G 時代、數位轉型及國家安全的資安產業」。在「資安即國安」的戰略指導前提下，保持高度的資訊安全意識。在 5G 布設建置過程中，臺灣應竭盡所能，想方設法，完全排除具有資訊安全疑慮的軟硬體設備及相關供應服務。基此，我國可參考以下先進國家之資安戰略：

一、 英國 2016 年 11 月「國家網路安全戰略 」(National Cyber Security Strategy 2016 to 2021)，內容聚焦網路資安防禦、嚇阻、發展，並期望達成： 1. 政府網路及關鍵基礎設施防護、 2. 遏制網路犯罪、3. 發展網路安全相關科學研究等目標。

二、 新加坡 2018 年 3 月「網路安全法」 (Cybersecurity ACT 2018 (No.9 of 2018))，置重點於網路空間安全防護，包含關鍵基礎設施安全防護、網路攻擊反制與偵蒐、資訊、網路安全情資共享及建制資安服務供應商之管理機制。

三、 日本 2018 年 7 月「網路安全戰略」 (Japan’s Cybersecurity Strategy)， 包含以下策略：1. 實現網路安全供應鏈及架構安全物聯網系統。2. 建構大學院校之資訊與網路安全教學研究環境。3.制定網路犯罪之因應對策。4.強化政府網路防禦應變、反制網路攻擊與應變大規模網路破壞之能力。

四、 美國 2018 年 9 月「國家網路戰略」 (National Cyber Strategy)，置重點於採取主動防禦作為，保護國家資產及民眾隱私安全，並提高惡意攻擊破壞者代價。

五、 韓國 2019 年 4 月「國家網路安全戰略 」(National Cyber Security Strategy)，內容重點包括：1. 加強國家關鍵基礎設施安全、2. 提高網路攻擊應變與復原能力、3. 建立具信任的網路治理能力、4. 奠定網路安全環境、 5. 培養網路安全文化、6. 領導國際網路安全合作。

六、 加拿大 2019 年 5 月「國家網路安全行動計畫」(National Cyber Security Action Plan 2019-2024)， 內容有 3 大目標：1. 強化關鍵基礎設施防護並增強網路犯罪偵查能力、2. 支持前瞻研究並協助創新企業發展、3. 國內、 地方與民間具體合作，結合國外盟友共同塑造網路防護環境。

七、 歐盟 2019 年 6 月「網路安全法」(The European Cybersecurity Act)，重點 為：1. 強化網路環境治理權限，2.挹注更多人力與財務資源，3. 建立「歐盟網路安全驗證框架」驗證計畫，4.評估網路資通訊產品、供應商服

務及製程是否符合國際安全規範。

八、 澳洲 2020 年 8 月「網路安全戰略」（Australia’s Cyber Security Strategy 2020），重點為澳洲政府預計將於 10 年內投資 16.7 億澳幣，投資要項：1.強化對人民、企業及關鍵基礎設施的具體防護能力，2. 保護企業產品和相關資通訊服務免受威脅或防護弱點的侵害，3. 透過公、私部門通力合作，促進網路安全。

綜合上述各國資安戰略，歸納重點：國家應於初始規劃階段，即建置安全的網路環境、建構國家網路資安聯防體系、培養大量優質的資安人才及尋求跨國合作之可信賴供應商等作為，方能超前部署，防範未然。共同構建綿密的國家資安防護網我國於 2019 年 1 月正式施行《資通安全管理法》，成為我國首部「資安專法」； 調查局旋即於 2020 年 4 月成立「資安工作站」，具體落實了我國資通安全戰略的重要關鍵作為，持續強化網路安全的具體防衛機制，構建綿密的國家資安防護網。

未來更應在戰略層級規劃：賡續推動政府網路資安集中共享，擴大國際參與及深化跨國情資分享，制敵機先阻絕境外攻擊，提升科技偵查能量，防制新型網路犯罪。在政策面向考量：輔導企業強化數位轉型之資安防護能量提升，強化供應鏈安全管理具體作為，建構智慧國家網路資訊 安全環境。在教育面向推動：擴增高等教育網路資安師資員額與教學資源，挹注資源投入高等網路資安科研，培育頂尖網路資安實戰及跨域人才。在執行面向具體：建立各領域公、私部門協同治理運作機制，增強人員網路資安意識與安全防護能力建構，公、私部門合作深化平、變時情資交流與相關預防、應變、復原演習演練等；建立各層級持續營運能力，及強韌、相依、可靠的網路資通訊安全環境。