「海峽兩岸服務貿易協議」開放二類電信之安全風險評析

蔡志宏
國立台灣大學

針對此次「海峽兩岸服務貿易協議」近來各方相關評估意見多僅由經濟層面進行， 較少見到由國家整體安全及各服務體系之風險管理、資安防護及永續經營的角度進行之評估。但事實上後者對我國長遠穩定未來更為重要，因此本文乃專注於此角度並針對二類電信之開放進行評析。

目前全球各先進國家在911事件之後,特別是已開發之高度資訊化國家，對其維繫國家整運作之關鍵基礎建設的資訊安全均極為重視；因為多種資安實證分析與駭客攻防實兵演練皆證實有組織的直接、間接網路攻擊都可能對一個國家的關鍵基礎建設形成重大破壞而導致其經濟與社會運作停擺。過去在愛沙尼亞、韓國等發生的事件皆已達到類似的攻擊規模。而本次服務貿易協議我方擬開放項目涉及海運陸運(公路運輸)、電腦相關服務、第二類電信服務、醫院服務、銀行金融等在許多歐美先進國家中皆早被納為關鍵基礎建設的高度資安防護範圍。**特別若從各關鍵基礎建設的相互依賴關係來看，包含二類電信的電信網路其實是其他關鍵基礎建設除電力外最特別依賴的支援體系， 可算是關鍵設施的關鍵設施**；因此一旦電信網路失靈，我國的經貿運輸物流、銀行與證券等金流活動都可因此停擺，因此其資安影響豈可略而不談。

最近根據通傳會對外發佈新聞稿的說明,NCC似乎認為其二類電信此次開放範圍僅限於所謂「特殊業務」且限制業者以封閉網路型態對「企業」提供服務，因此對於一般網路使用者的影響較小。但其實若由我國整體安全風險或對個人之潛在威脅來看，可能並非如此。

首先我們應該要探討所謂企業封閉網路所承載的資訊，是否就對國家或民眾而言比較不敏感或不重要？其實其答案相當不一定，在許多案例中可能相反,因為這些企業網路也可能承載其企業客戶/使用者的重要資訊。至於企業網路中是否均已經是加密之資訊,其答案也不一定,因為許多業者(特別是內容業者或資訊網站業者)為求資訊內容之快速交換,其後端專屬網路不一定對所有內容加密。

另一方面，開放範圍中所謂「企業」一詞其實於電信產業用語中幾乎可是任何非個人之機構與單位,其中也可以是包括前述關鍵基礎建設中的物流、金流業者、甚至包括醫療體系。「企業」也可以是一家提供雲端服務或網站服

務的資訊業者，甚至是其他 ISP。雖然該二類業者可能只是提供如 ethernet 交換服務且是封閉式網路，但其影響力也可足以影響台灣 ISP，或是企業的穩定經營。

以台灣學術網路為例，過去數年台灣學術網路各大網路中心的骨幹路由器間連線事實上是運用國家高速網路與計算中心的 L2VPN 互連服務，而使得國家高速網路與計算中心雖然僅提供第二層(Layer 2)封閉式網路服務，它依然成為台灣各大學網際網路互聯的最主要頻寬來源。

前述場景可以完在中資進入台灣二類電信後複製發生。換言之，如果本次開放的二類電信特殊業務於中資投資後以低價競爭業務來持續成長，當有足夠多的小 ISP、內容網站業者、社群網站或企業網路向它靠攏、它可以成為台灣 ISP 或金流、物流體系、甚至數位內容體系的交換網路中心之一。**當該業者成為台灣重要的交換網路中心，即使它沒有一類電信的執照或是一般二類電信業務的執照，它要截取網路中傳遞的資訊、或分析使用者行為也將十分容易，而對我國的國家安全、企業資安與民眾個人隱私，則都是全新的重大威脅。**

通常國際上各高度資訊化國家在涉及維繫關鍵基礎建設持續運作之防護機制設計一般仰賴政府與業者採行共同合作方式(所謂公私聯防、Public Private Partnership)來進行，我國各體系的運作基本上也不例外。因此一旦業者中有部份形成防護缺口，一方面外來攻擊即可能由該缺口長驅直入，另一方面我國廣大民眾個資或企業之商業機密也可能因此而長期外洩。由於中資進入台灣電信體系或網路資訊服務體系後可能指定使用隱藏既有後門之中方資通訊系統，對我國關鍵基礎建設體系之威脅將可能防不勝防，因為該類後門要偵測所須人力物力可以相當驚人。而在資安領域中著名的水桶理論，就是指水桶儲水能力是有其位置最低的缺口決定。**如果中資進入我國二類電信體系又不予以嚴格規範，假以時日，將使我國運輸、金融、ISP 等體系形成聯防(水桶)中出現我方最底層的缺口，那我國主要關鍵基礎建設之防護體系幾乎等於蕩然無存。**

目前我國醫療、金融證券、電信、以及部份運輸體系已經高度資訊化，而各業者之資通訊系統呈現高度相聯及高度相互倚賴的狀況。因此當有電信業者資訊系統出現漏洞而被對方所遠端掌控，該體系聯防措施即等於出現漏洞，對外部防護的各項作為可能迅速被外部網路攻擊者掌握。因此即使中方投資於我國某關鍵基礎建設體系之比例不高，但其影響可影響整體電信網路體系之穩定度與在外部網路攻擊時之存活度。特別是如果由中方所引進系統於出廠時即隱藏有軟體安全缺陷，或是中方派駐台灣技術人員於原本正常網路設

備中動手腳，要防範此類資安漏洞我方可能所費不貲。而且筆者認為即使修正我國目前對電信業的資安規範也未必是有效之解決方案。

因為採用事前保密之關係，我國貿易協議負責談判的單位與我國負責國家基礎建設資訊安全防護單位的溝通於此協議內容曝光前應該非常有限。我也不認為通傳會被給予充份時間來推演此一漏洞打開後對其他體系的影響。目前各單位急需進行安全評估之作業時間與額外資源。依個人專業經驗，他們也急需針對其關鍵基礎建設體系之進行全新思維的安全評估與沙盤推演，因為**有別於過去以外部威脅為主之防護，他們要調整因應來自產業體系內部的威脅**。如加上強化安全防護之法源建立與機制調整之工作，依政府預算程序，其完成盤點與整備時間將長達兩年以上。 我國電信法規對二類電信長期以來皆採低度管制，因此相關法規(特別是二類電信之管理規則等)是否需要調整，以及中資投資之二類電信是否應該有特別的安全審查與業務範圍規範等議題都有必要迅速檢討，而且都有必要於服貿協議評估是否該通過前就應該先完成內部檢討與外部公聽程序等工作，並對公眾充分說明。

幾乎任何資安防護措施皆需投入額外經費。而在整個電信體系就新增威脅完成沙盤推演以前，應該尚沒有任何單位有能力提出未來資安成本增加之有效估算。但台灣整體社會因此而增加的風險或不安程度若遠高於開放之經濟效益，那此次協議的妥適性就非常需要重新考量。