◎安全維護宣導

德國政府將傳統網路犯罪推展至國家安全的高度，此等相關作法，值得臺灣借鏡。

－從網路詐欺到國家安全： 淺談德國聯邦政府資訊科技安全法案－

本文主要探討德國聯邦政府所批准資訊科技安全法案（IT-Sicherheitsgesetz）在數位犯罪之新穎觀念。德國將藉由此一法案，擁有全世界最安全的資訊科技系統和最可靠的關鍵基礎設施。該法案主題包括，在關鍵基礎設施上改進企業資訊科技安全、保護公民的網路安全、確保德國聯邦資訊科技、加強聯邦資訊技術安全局的能力與資源、擴展聯邦刑事網路犯罪的調查權力；該法案也修正了德國電信媒體法案（Telemediengesetz），要求電信媒體供應商必須負責提供媒體服務設備的安全，保障用戶個人資料並確保用戶不受外部攻擊或干擾。

所謂的關鍵基礎設施營運者，包括能源、資訊科技、電信、運輸和交通、醫療、水利、食品、金融與保險等領域的企業。德國聯邦政府要求關鍵基礎設施的營運商，要滿足資訊科技安全的最低標準，並且必須強制向聯邦資訊技術安全局通報資訊安全事件。聯邦資訊技術安全局要對關鍵基礎設施營運商的資訊進行評估分析，並供予關鍵基礎設施營運商彙整改善，以提高其基礎設施的保護。

該法案亦針對一般國民的資訊安全，要求電信公司確保顧客的資訊安全；當電信公司發現客戶的手機或電腦已成為殭屍網路的一部分或被濫用攻擊時，必須強制通知該客戶。同時，該法案擴展了聯邦資訊技術安全局的功能，包括通過強化其安全諮詢作用；為了保障資訊科技產品的安全性，並為客戶提供更透明的資訊安全保護；此外，聯邦資訊技術安全局有權在相關商品上市時，檢驗資訊科技產品和資訊科技系統的安全，經評估在必要時公布結果。

基本上，該法案的主旨在提高保護一般人民和公司在網際網路上的資訊安全，並加強聯邦資訊技術安全局和聯邦刑事單位（BKA）的防衛能力，還規定擴展聯邦刑事調查權力，特別是利用資訊科技攻擊聯邦設施的案件。該法案同時修正聯邦犯罪偵防局法，增加網路犯罪的刑責及擴大聯邦犯罪偵防局有關安全敏感範圍，包含影響國家及人民安全的網路關鍵基礎設施，對這些相關設施將採取較高規格的警戒和預防措施，而非被動地犯罪偵防。

德國目前在網路安 s 不同的網路詐欺相關法律，它的目的是確定具體罪行和罰則；執法單位可使用這些法律，加強數位偵防能力，將罪魁禍首繩之以法。任何人自己意圖或透過第三方非法取得財物利益，或令他人因此資產受損，藉由設計的數據處理操作的結果，利用不正確的程式、透過使用不正確或不完整的數據、未經授權使用數據或以其他未經授權的影響方式，將處以監禁長達五年或追加罰款。此外，其他相關法律也包括：數據間諜法條、以欺詐獲利法條、數據竄改法條、妨害電腦使用法條。

綜觀德國資訊安全法案立法精神，除了加強聯邦資訊技術安全局和聯邦犯罪偵防局經費、預算和人力，用以擴大網路安全攻擊防治與數位偵防能量以外，

也強調保障關鍵基礎設施的安全。在網際網路蓬勃發展的今日，人類的生活將和網路息息想關，尤其在將來物聯網的世界，無時不聯網，無物不聯網，國家安全與資訊安全將更密不可分。德國聯邦政府的視野，包括數位議程（Digitale Agenda 2014-2017）和資訊安全法立法進程，都將傳統網路犯罪從個人或公司詐欺事件，推展至國家安全的高度；此等相關作法，值得臺灣借鏡。

（作者為李忠憲成功大學電機系暨電通所教授、德國柏林工業大學博士）

台中榮民總醫院關心您也提醒您！