〈轉載自清流雙月刊 106 年 11 月號〉

私人虛擬網路—資訊攻防主戰場

中華戰略學會研究員 張競

資訊戰是當今不分平時戰時，幾乎每分每秒都要面臨之安全挑戰；基於其執行主體為國家機關，或是非屬國家體系下之私人體系，分別成為國安與治安上不同範疇之威脅。

不過嚴格說來，當治安情況嚴重到影響國家公共秩序，或人民生活重要福祉時，將資訊安全歸納為國家安全範疇內加以應對，確實是當前全球主要先進國家共同具有之主流思維。

網路之所以影響力驚人，在於其通聯能力，其威脅亦係相伴此特質而生。在討論網路資訊攻防之前，必須依據網路聯通方式與範圍，掌握資訊網路的三大類別。

首先，談到專為政治與軍事目的建構之「封閉性網路」；原則上，幾乎所有國家武裝部隊都會建構獨立的作戰指揮網路，並與一般民用

網際網路嚴格實體隔離。

該網路可同時作為情報傳輸、人事調度、後勤管理與財務會計通聯管道，但此網路基本屬性仍以作戰指揮為主。戰時政府領袖將進行戰爭指導，情報機構與外交部門亦須掌握戰爭動態，因此該網路需與國防軍事單位以外部門通聯，但整體來說，其與民間網際網路毫不通聯。由於此種實體隔離架構，且其資料存取具層層管制，增加攻擊上的困難，亦讓駭客不易得手。

其次就是所謂「全球性網際網路」; 原則上，可以將其視為─針對人類共同公益目的存在之開放性網路。架構此種網路之網站，基本上對於資料存取與傳輸並無限制，通常其資訊內容亦不會聯結任何機件或自動控制設施，就算其中所含資訊有所錯誤，對於人類社會所產生之干擾或傷害，都必須是閱讀其網站內容者，願意相信其論點，再配合作出相關舉措。在資訊攻防上，不常成為主要目標。

最後則是本文所要探討之資訊攻防主要對象─「虛擬私人網路」; 虛擬私人網路係架構於全球性公開網際網路上，藉由通信保密規範與加密通道協議 (Tunneling Protocol) 所建立之保密通信規範，其或稱

虛擬專用網路（VPN：Virtual Private Network），所處網路空間，雖與全球性公開網際網路共享，但其通訊內容是由人工保密技術加以隔離，其運作就像是由人工所專門架構，建立出另外存在之網路空間。

成立完全實體隔離網路，並且維持其運作，必須付出極高成本。就算是美國，其仍有諸多遍及全球之保密性政府資料庫或行政性網路，諸如 NIPRNet、OpenNet、NSANet 及 JWICS 等，必須或多或少與公開性網際網路交聯，並藉由虛擬私人網路技術，設定使用權限，限制無權限用戶入侵，但非達到完全實體隔離地步。

同樣地，美國政府幾個事涉機密之敏感資料庫，諸如聯邦調查局及所屬外站用於檢索犯罪偵防資訊之「局內百科」（bureaupedia）資料庫；美國國防部所架設，專供國　　防科技以及軍事採購圈內人士，檢索分享軍事科技資訊之「國防科技百科」（DoDTechipedia）資料庫；美國國務院以及駐外使館所共享之外交檔案電子資料庫「外交百科」（diplopedia），亦是運用虛擬私人網路技術加以防護，並管制使用者存取權限，保密程度則是依據資料機敏性加以區分。

誠然實體隔離之獨立網路可顯著增加保密性，但基於成本考量，

不論是建構階段之硬體鋪設經費，以及日後維護管理成本都極為驚人。在無法負擔高額成本建構實體獨立網路，又有資料保密實際需求時，常求助於虛擬私人網路技術。目前在全球網際網路架構，專為人類社會特定目的存在之封閉性網路，包括交通號誌、飛航管制、金融交換、票券交易、彩券投注、遠距教學、醫療看護、治安監控、環境監測、電力配送、資料檢索與公文交換等，皆須考量保密安全，避免外力介入干擾。

掌握網路性質，對資訊安全政策指導至關緊要，資訊安全防護必須適切配置資源，若以高效率方式分派資源，投入最受威脅資訊攻防目標，就能夠產生最理想防護與應變作為。