灣的貿易困境著實是個令人頭疼的問題。綜觀各界的評論與意見，作者提出幾個也許能幫助台灣化危機為契機的努力方向：

第一，強化台灣於東南亞經貿整合的地位。在整個東南亞貿易鏈中台灣為不可或缺的零組件供應國，但影響力仍不及中共，若政府能與企業聯手，於東南亞大量投入其欠缺的技術、研發與運籌整合能力，推動在地企業結盟或發展具規模性的跨國公司，除了能幫助台灣企業走出國門，亦能擴大東南亞的經濟效益成為其無法捨棄的命脈。

第二，積極的運用多元管道與各國洽簽 FTA。自 2008 年馬英九總統上任以來即以推動東南亞 FTA 的簽定為主軸，與中國簽訂的 ECFA 只是第一步，唯有多管齊下並以 ECFA 作為一個橋樑，台灣才有發展空間，目前以簽訂台星（新加坡）經濟夥伴協議、台日投資協議、台紐 ECA 為重點目標，未來若能在簽訂 FTA 上有任何的進展，打破「一個中國」的困境，不論對於台灣的經濟或前景都會是極為重要的里程碑。

第三，RCEP 與 TPP 皆可為努力方向。雖然許多人認為 RCEP 無疑是為了抗衡由美國所主導的 TPP 的挑戰而成立，但實際上就其組成會員與性質上來看，兩者並非惡性衝突的關係，且美國對於台灣的未來尚具一定的影響力，故台灣在積極為打入 RCEP 鋪路的同時亦不能放棄加入 TPP 的任何可能，可先與 RCEP 和 TPP 中重複的成員建立良好關係，並以簽訂 FTA 為目標，同時要在中國與美國兩大勢力的平衡木上找到屬於台灣獨有的支撐點，而這個支撐點將會是未來台灣發光發熱的契機。

2012年的國際網路攻擊與安全威脅

沈明室*

隨著資訊科技發展的日益提升，網路安全與衝突事件層出不窮，不僅攻擊事件與次數未見明顯下降，其攻擊方式與所使用的病毒軟體，亦隨著網路防衛科技與作為的發展而相應創新。例如知名的網站「網路戰爭」（Hackmageddon.com）綜合過去一年網路攻擊事件分析指出，網路攻擊動機大致區分為網路犯罪、駭客攻擊、網路戰及網路間諜活動，駭客或具特定意圖者透過不同的方式，進入不同系統電腦中，以進行癱瘓、竊取、阻斷的攻擊行動，由於網路攻擊者的手法推陳出新，也讓網路安全防護工作必須與惡意資訊科技的發展賽跑，防護壓力非常沉重。

除了在企業的網路犯罪行為外，在 2012 年的國際網路安全中，也發生了一些以國家政府或組織為對象的網路攻擊行動，或是難以確認，但被懷疑受到國家資助的網路攻擊行動。如美國與以色列合作開發軟體攻擊伊朗核設施、中共對美國軍火公司的攻擊行動、疑似美國對法國的網路攻擊等，這些攻擊行動通常不會被承認，而且沒有被發現與公諸於世的可能還有更多案例。這些都因國家戰略利益競爭而形成，或是伴隨衝突所發生的網路攻擊行動。在可見的未來，伴隨國際衝突而發生類似的攻擊行動恐怕仍會層出不窮。

* 作者為國防大學戰略研究所副教授

2012 年的國際網路攻擊與安全威脅事例

一、中國網軍攻擊美國白宮軍事辦公室事件

根據美國「華盛頓自由燈塔」(Washington Free Beacon)在 2012 年 9 月 30 日的報導，來自中國的駭客曾意圖入侵美國白宮軍事辦公室(White House Military Office)，企圖竊取總統的行程、醫療資訊、以及核武系統的指揮與控制指令等資料，倘若攻擊成功，其後果將不堪設想。

根據白宮發言人卡尼(Jay Carney)的說法，機密系統都被獨立的網路環境所隔離保護，而核武系統不在這波被攻擊的系統清單內，也因此次攻擊採取魚叉式網路釣魚(Spear phishing)手法。這是一種很普遍的攻擊方式，該辦公室因早已採取防禦措施，沒有任何資料被竊取。在該起事件中，中國駭客透過魚叉式網路釣魚方式，誘使收件人點選信中包含惡意網址連結或惡意附件，藉此機會入侵電腦，並攻擊組織的資訊系統。

魚叉式網路釣魚的攻擊目標通常是竊取組織的機密性資料，其會鎖定特定公司或組織的成員，並偽裝成像是來自認識的人或單位所發出的電子郵件，以降低收件者的警覺性，由於真假難辨，攻擊成功率往往很高。美國聯邦調查局在美國特勤局(US Secret Service)的支援下正在展開調查，美國國家安全署(US National Security Agency)也共同參與。事實上，每年意圖向美國軍方網路展開攻擊的例子非常多，類似釣魚的低階手法因為發生頻率很高，早有多種防範作為而使得成功機率不高，因為美國相關政府單位對電子網路和網路使用採取嚴格的控管所致。由於這起攻擊的伺服器多來自中國，因此外界也將矛頭指向中國政府。

二、疑似美國網路攻擊法國總統府官員電腦事件

根據法國《快訊》(L'Express)週刊 2012 年 11 月 21 日的報導，在 2012 年 5 月間對法國前總統府秘書長繆斯卡(Xavier Musca)等總統資深幕僚電腦進行攻擊、竊取機密資料與「戰略計畫」的駭客，可能來自美國。事實上，早在今年 7 月，法國某些媒體曾報導，法國總統府曾遭駭客攻擊。《快訊》指駭客以臉書交友的方式，騙取法國總統府幕僚的密碼。然後，這些法國資深官員的電腦被植入的惡意程式威力強大，可以擷取檔案、錄製銀幕畫面，並且能透過電腦的麥克風錄下辦公室的對話。美國駐巴黎大使館已出面否認這項指控。

更值得注意的是，這種等級的網路武器需要「大國」的財力和人力才有能力研發。《快訊》引述消息來源，指稱法國調查單位已經做出結論，這起攻擊應該是來自美國。法國國家資訊科技保安部(AgenceNationale de la Sécurité des Systèmesd'Information, ANSSI)曾花了好幾天重建法國總統府的網路系統，保安部則拒絕回答是否來自美國的相關問題。

三、雷神(Raytheon)公司受到進階持續性威脅(APT)攻擊事件

除了國家或政府單位之外，以飛彈及相關系統聞名的美國雷神公司，自從賣武器給台灣之後，就一直受到來自中國的網路攻擊。根據雷神網路安全主管布雷克(Vincent Blake)在年底英國 RSA 研討會所言，「5 年前，從我們賣飛彈給台灣之後，幾乎快掛了」，並提出此一慘痛經驗。他認為某些不樂見台灣政府軍購的駭客試圖入侵雷神，以竊取相關武器設備的機密資料，藉以懲罰雷神公司。

進階持續性威脅(Advanced Persistent Threat, APT)攻擊，簡單的說就是針對特定組織所作的複雜且多方位的網路

攻擊。從蒐集情報開始，可能會持續一段時間，甚至會包含技術和人員情報的蒐集。情報收集工作可以塑造出後期的攻擊，這可能會快速或持續一段時間。在雷神的網路上幾乎每天可偵測到 3 萬個樣本，這些樣本試圖潛伏在內網以感染電腦，並伺機偷偷竊取資料。

因為遭到一連串的目標式攻擊，雷神公司除了強化資安防禦體系，也併購資安廠商，跨足到資安領域，他們的克服方案在透過虛擬環境掃瞄電子郵件的附件及內建的惡意 URL 連結，以阻擋可疑的行為。除了雷神之外，今年 5 月美國著名的洛克希德馬丁公司（Lockheed Martin）網路，所使用的正是 3 月被竊的 RSA SecurID 的雙因素認證產品資訊。另外如 8-9 月間日本三菱重工約有 80 台伺服器及電腦遭入侵，相關潛艦、飛彈等先進技術資料可能已經外洩。

四、美國以網路攻擊阻止伊朗發展核武

早從 2010 年，伊朗核電廠受到 Stuxnet 蠕蟲攻擊，重要基礎建設竟然受到網路攻擊，舉世震驚，當時就有人懷疑是美國或以色列發動的網路攻擊行動。伊朗電廠可以透過高速離心機控制設備來提煉濃縮鈾原料，以製作核武之用，這次攻擊就是特別針對伊朗電廠的離心機，主要目的是抑制伊朗發展核武。美國所使用的 Stuxnet 的攻擊其實是源於一隻 Windows 釋放程式，首先讓這隻程式進入到設備工程師使用的電腦（Windows 系統），再透過 USB 隨身儲存裝備植入系統。美國曾有匿名官員承認此事，證明 Stuxnet 蠕蟲攻擊的運用，使國土安全的攻防首次提升到網路攻擊層級。

除了 Stuxnet 的攻擊外，事實上，資安攻擊已經提昇至國家戰爭的層次。例如，因為攻擊伊朗石油部而被發現的超級間諜病毒火焰（Flame），有媒體報導這也是美國與以色列政府聯手開發而成的軟體，目的在延緩伊朗的核武計畫。《華盛頓郵報》（Washington Post）於 2012 年 6 月 19 日的報導，美國官員表示，美國和以色列政府共同發展的火焰間諜程式，目的在蒐集伊朗政府的資料，以做為更進一步網路攻擊的參考依據。伊朗電視媒體同時引用《華盛頓郵報》的報導，指控美國和以色列政府共同開發火焰軟體攻擊伊朗的核能計畫。

火焰與另一個間諜程式 Stuxnet 相較，兩者不論是分布位置或攻擊手法都高度雷同。不過，卡巴斯基實驗室已經發現火焰和 Stuxnet 具有相同原始碼，顯示兩者之間有其關聯。這兩波威脅應該是來自於同一個攻擊單位的兩個開發團隊，差別在於火焰主要任務在進行間諜活動，Stuxnet 則用來執行破壞性的活動。

2012 年網路攻擊與安全威脅的趨勢

一、網路攻防軟體推陳出新

以往的釣魚郵件透過夾帶 rar 或 zip 的附件檔，以不分對象的方式進行大規模散發，近兩年著名的 APT 攻擊資安事件更推陳出新，使駭客已經成為企業或國安機構資安防護的重要核心威脅之一。因為駭客入侵技巧不斷翻陳出新，單位內的防禦設備及資安能量，在 APT 攻擊無情的侵襲下，原有的資安架構將受重大的衝擊。尤其面對有組織、有計畫的國家層級資助的駭客攻擊，各國政府機關、軍火商、學術研究機關紛紛中箭落馬，單位內的機敏資料，於無聲無息中外洩。

駭客針對目標的背景資料做詳盡調查研究，然後「量身訂做」出聳動標題，吸引被害者開啟郵件達到入侵目的，這種

攻擊方式從以往的大規模攻擊變成現在的隱蔽低調，再透過精密的客製化物件對入侵對象的裝置進行遠端控制，以竊取重要的機密資料為最終目的。一般電腦產品的使用者，遇到駭客以量身打造的方式，持續性的攻擊行動，明顯處於不對稱的劣勢。

二、透過社交工程的攻擊方式更為進化

根據檢查點（Check Point）研究，2012 年各種行動裝置的惡意軟體變種數量以倍數成長，往後數年，行動裝置的威脅將受到更多關注。隨著行動上網流行，越來越多廠商鼓勵使用手機掃描快速反應碼（Quick Response Code, QR Code），以取得產品資訊。然而，使用者應注意 QR Code 可能帶有危險性－只要掃描了被駭客破解的 QR Code，就會將手機重新導向某特定惡意網址、檔案或應用程式。

駭客運用社交媒體應用程式，蒐集個人與職業資訊，進而找出企業防護弱點。只要幾分鐘，駭客就能根據被害者在社交媒體上的公開資訊，取得個人資訊。另由 Facebook 打卡功能等定位服務知道目標者所在位置。由於社交工程攻擊所使用的資訊完全符合個人背景，很容易掩蓋非法的痕跡。臉書的 8 億多用戶相當活躍，為網路犯罪大開方便之門。

國際因應作為

一、資安委外服務成長

2012 年，不管是無孔不入的 APT 進階持續威脅，或新型態的 DDoS 攻擊，這種鎖定目標發動攻擊的方式，挑戰企業原有的資安防禦。使企業朝向資安專業服務公司尋求協助，

資安委外服務、安全閘道器、資安事件管理（SIEM）成為 2012 最快速成長的前三名安全領域。儘管 IT 預算在不景氣下受到樽節壓力，但是全球資安預算一直到 2016 年仍然是企業的優先項目，尤其以資安委外服務成長最多。

駭客除了鎖定特定對象發動惡意郵件外，也繼續使用新型態 DDoS 攻擊手法癱瘓各大網路平台。根據連結護衛網站（Nexusguard）的觀點，近年來針對 Web API 發動阻斷服務的攻擊手法有明顯成長，包括 PayPal 與 Amazon 的 AWS 都曾因為持續性的 API 錯誤使網路服務中斷。其所進行的方式，包括故意讓網站所提供的搜尋功能或留言版頻繁的執行。由於攻擊模式持續不斷變化，這讓資訊安全的市場維持 9% 到 11% 的成長。

二、研發網路武器反擊

自 2011 年下半年開始，日本諸多政府及政府委外相關企業遭受到針對式攻擊，根據日本《讀賣新聞》報導指出，美國與中國目前都已經開始投入網路武器於實務應用，而儘管原先日本法令禁止製造電腦病毒，但在保衛國家的前提下，他們也正透過法律修正案來改變這個現況。

日本政府投資 230 萬美元的三年專案當中，日本科技公司富士通（Fujitsu）正在研發「搜尋擊破」（Seek and Destroy）的病毒與設備，可以監控及分析出網路威脅，該病毒仍在封閉環境進行可用性測試。

三、國家資助網路攻擊的升級

各國情報單位都不敢輕忽病毒可能造成的國家機密外洩問題。駭客過招的方式早已大不同，過去流行竊取網路銀行

帳戶或個資已經不夠看，各國政府甚至已經開始利用網路惡意程式來互相攻擊及牽制。美國政府為了避免擴大戰爭的傷害層級，選擇以「蠕蟲病毒 Stuxnet」等侵襲該國核設施，成功阻止伊朗核武發展。但 Stuxnet 病毒卻曾因程式錯誤，造成了全球網路肆虐，使得網民也不免受到蠕蟲病毒的影響。

「Stuxnet 蠕蟲病毒以及變種火焰惡意間諜軟體、Gauss 超級間諜病毒（偷取網銀帳戶資料的間諜程式）等的遊戲規則已經與以往不同，「Stuxnet 蠕蟲病毒」雖然會造成重大損失多半是因為駭客主要是針對國家等級的網路，如水庫、油井、電廠等重要基礎設施發動攻擊，但變形之後的病毒反而會透過消費者幾乎每天使用的隨身碟、外接硬碟等行動儲存裝置散播，一旦被感染，以現在的使用習慣，很可能連手機、平板電腦等都難逃一劫。

四、納入國際安全對話的議題

由於國際網路安全議題日趨迫切，各國除了強化網路安全防護之外，也在各種國際安全對話中，納入網路安全的議題，並積極尋求安全合作，共同解決與處理攸關資訊產業發展與國家安全的網路安全。例如日印雙方在「2+2 對話」中，同意提早舉行有關網路安全的對話。因為日本及印度都深受來自中國駭客入侵威脅之害，希望能共同合作有效因應網路安全威脅。另外，美中在戰略暨經濟對話的架構之下，已經啟動了一個網路安全對話，美中就此交換意見，處理有關兩國的網路安全問題。由於美中兩國是全球最大的網路使用國家，雙方就網路安全問題進行有意義的雙邊對話，發展兩國能夠接受的網路安全行為準則，非常重要。

政策建議

一、整合公民營資安科技與能力防範國家資助型網路攻擊

網路攻擊行動依照其動機、手段，可以區分為針對企業、機構及國家安全單位不同層次，其所造成影響大致也可以歸納為對企業、對國家或是對國際政治等。從去年網路衝突來看，部分區域安全衝突因為直接性軍事行動的衝擊過大，或是因為民族主義所引起的激烈行為延伸到網路世界，由國家資助的駭客行為，或是針對國家或政治組織的攻擊行為會越來越多。因為犯罪證據的難以掌握，未來國家資助的駭客行為，將隨著國際衝突的發生趨於頻繁。過去台灣曾經遭受來自中國的網路駭客攻擊，雖然因為兩岸關係和緩，使得網路攻擊更形隱匿，但不能排除在未來兩岸關係變化時，可能來自對岸的國家資助型網路攻擊，應整合公民營資安科技與能力及早建構針對國家資助型網路攻擊的防禦網。

二、研發網路攻防的攻擊與防護軟體系統

個別國家或機構為了自保，必須針對各種網路犯罪或攻擊行為及早採取防範措施，但是面對國家資助的駭客行為，被動防護或是攻擊性軟體問市後，才相應採取防護作為都略顯消極。資安服務產業相對日趨蓬勃，但對國家而言，一味被動防護似乎不如採取攻擊行為，致力發展防護科技同時，也同樣研發網路攻擊武器，藉以竊取或懲罰發動網路攻擊者。各國正在利用惡意軟件來攻擊對方，網路戰爭革命現已一觸即發。要對抗快速變形、進化的蠕蟲病毒，第一步就是反制潛在敵方網軍，故應從攻擊是最佳防禦的角度，研發網路攻防的攻擊與防護軟體系，強化網路安全嚇阻能力。