立法院第 8 屆第 3 會期第 6 次會議議案關係文書

專案質詢
8－3－6－0129

立法院議案關係文書 中華民國 102 年 3 月 27 日印發

案由：本院江委員惠貞，鑑於日前南韓數家電視台與銀行，疑遭北韓駭客攻擊，造成所有公司電腦網路同時癱瘓，導致 ATM 提款業務、跨行金融業務等停擺，受害規模全球罕見。國安局長也表示中共網軍對台攻勢「相當嚴重」，去年一整年國安局的網頁就被侵擾 334 萬餘次，平均一天超過一萬次，密集程度令人咋舌。準此，兵不血刃的「網路戰」早已成為全球趨勢，我國實應在資訊安全方面作足萬全準備。本席建請國防部、國安局積極研發各類網路武器，同時加強國內資訊安全；教育部應制訂計畫培育電腦網路專才，以因應日益擴大的網路大戰，確保國家安全，特向行政院提出質詢。

說明：

一、根據國安局資料顯示，僅去年一年，國安局外網網域遭駭客攻擊次數就高達 334 萬餘次，換算平均每天遭受攻擊數量超過萬次，比熱門文章在臉書被轉貼按「讚」的次數還多。2007 年愛沙尼亞的銀行、媒體和政府網站亦曾遭俄羅斯駭客「分散式阻斷服務攻擊」（DDOS）達三周之久，網路安全界稱這起事件為「第一次網路大戰」（WEB WAR I），也促使北約組織在該國設立網路基地。

二、就軍事角度來看，「網路戰」可兵不血刃破壞敵人軍用、民間網路系統，導致武器無法動用，甚至癱瘓電信、金融秩序等，達到不戰而屈人之兵的效果。就連歐巴馬總統上個月發表國情咨文演說亦表示：「我們知道駭客會竊取人民的身分資料和電子郵件，也知道外國公司會盜取企業機密，如今敵人正在尋求破壞我們電力、金融機構和飛航控制系統的能力。」可見網路大戰並非僅是刺激的電影情節，而是真實發生在國際間的熱戰。

三、世界各國為了打贏網路戰，無不用心研發各式網路武器、培育網路專才，然而我國政府似乎仍不在狀況內，像日本、韓國、中國等，都有專門的科系在教導學生，但台灣完全看不到，學校從不教資訊安全、資訊工程或網路作戰。也就是說，台灣的駭客幾乎都是自行摸

索、單打獨鬥，與其他國家系統培育專才的團體戰相去甚遠。中國目前亦有專門資訊學校，培訓網路軍隊，以目前台灣國安系統的人力與素質，一旦對岸發動更大規模的網路戰，我方將難以抗衡。

四、再者，我國目前個人資料可說是隨手可得，而個人資料以醫院、銀行、學校等為最多，這些單位與機構，主機最多、資料豐富、研究著作汗牛充棟，但系統管理者卻最弱，對駭客來說簡直就是盜取資料、借道攻擊的天堂，可說是國安大漏洞，政府若等閒視之，我國將如何面對往後無數次的網路大戰。

五、國人生活日益依賴網路，不僅媒體、金融、交通等各行各業，都需透過網路服務客戶，就連自來水、核電廠等重要設施也靠網路操作，一旦網路癱瘓後果嚴重。無奈國內資安專家太少，將是資安的一大挑戰。本席建請(一)國防部與國安局應積極研發各類網路武器，例如：各式病毒破壞程式、防火牆等。同時加強國內各機關、單位資訊安全教育。(二)教育部應制訂電腦網路專才培育計畫，培訓網路軍隊，以因應國際網路戰的趨勢。