資訊安全

網路攻防理論策略發展與資訊安全研究分析探討(下)

教授　吳嘉龍

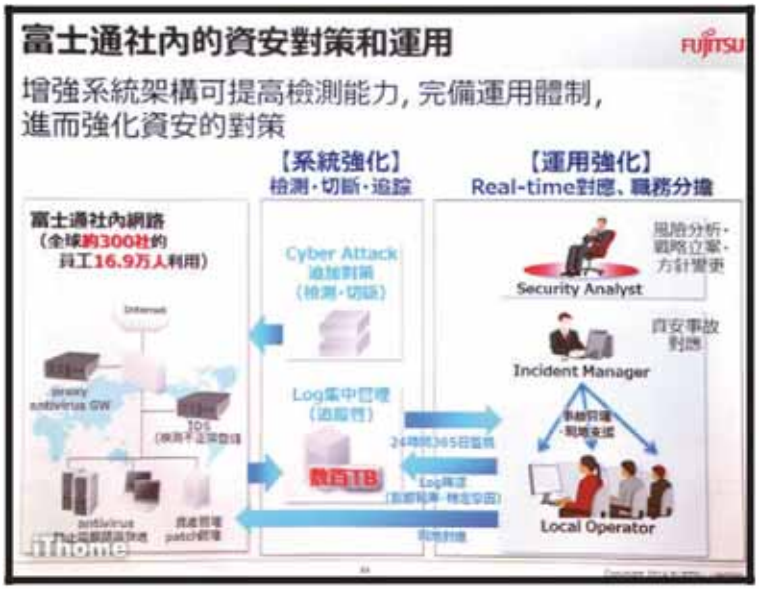
(文接上期)

日本富士通在2014年成立安全方案中心，由太田大州總經理帶領培育內部資安人才，在2014年4月起全面採用新安全方案，整理如表六。富士通公司為了有效抵擋每天數億次的網路攻擊，富士通公司新的安全防禦機制改採全面自動化以取代人工因應，能自動分辨事件重要性排定處理順序；富士通安全方案中心表示，富士通在全球有300家分公司，將近17萬名員工，每天要處理數億次針對公司內部網路發動的網路攻擊，網路攻擊已經儼然成為組織永續經營需面臨的一大課題，要因應這些人為網路攻擊，除了提高檢測能力來察覺並即時(Real Time)阻斷之外，而運用強化部分則將對應程序自動化，最後關鍵是人和組織的經驗與技術。富士通新的安全方案分成系統強化和運用強化兩個部分，在系統強化上，包括檢測、切斷與追蹤等三大重點。富士通搭配不同資安檢測技術來分析，並在經過防火牆時檢測通過的網路流量，適時切斷未經許可的應用程式通訊，網路封包經過防火牆之後，還設

表六、富士通安全方案中心資訊安全方案分析表(自行整理)[24]

多層防禦Log分析大量資料後續追蹤	富士通新防禦機制策略是即時切斷攻擊流程，從攻擊整體架構來找出攔截點，建立多層防禦，來防堵未知病毒攻擊或是針對脆弱性的Zero-Day攻擊，再藉由整理、分析Big Data大量事件通報和Log資訊管理，來建立防禦攻擊的組織和因應對策，以預防不斷更新的攻擊手段。
防禦機制自動化分辨事件重要性優先處理順序	將整套防禦機制全面自動化，資安防禦系統會自動判定資安警告訊息的重要性、風險等級計算出處理優先順序。系統也會判斷出遭駭對象是否為營運部門的電腦或是重要的伺服器，再依據威脅等級和終端設備類型來決定處理的優先順序，並自動取得受駭電腦所對應的使用者窗口資訊，將資訊交由特定的IT管理者來處理這些受感染的終端電腦。
掌靜脈應用於行動支付領域	富士通展示應用掌靜脈技術的PalmPass一掌通管理系統，可隔空掃描掌靜脈，並即時辨別出使用者身分，掃描距離約4～6釐米左右，優點是不用直接接觸感應設備，在辨識度上，使用PSN900掃描掌靜脈，拒絕本人登入(拒真率)的機率為萬分之1，而非本人成功登入的機率(認假率)則小於百萬分之1，幾乎不可能讓非本人成功登入系統。

置了未知惡意軟體檢查設備，來進行第二層的檢測分析，以便及時通知Proxy來關閉不正當的通訊；在資安人才培育上，富士通設立安全方案中心，並整合研究所、外部團體、資安供應廠商以及富士通的研究所和內部部門等資源，再加上公司內部對網路攻擊所累積的實踐經驗，包括因應對策、運用、教育訓練等，來形成一個安全方案體制(Fujitsu Security Initiative)，從裝置、網路、平臺到應用層，為每個層級做技術、裝置與人才認證，並累積這些人和組織的經驗與技術[24-25]。



圖三、富士通公司資訊安全策略與運用圖示[24]

由於網路威脅的頻率與複雜性不斷增加，美國將持續高度優先重視網路防禦與網路能力。當美國總統核准及國防部長下令後，美國防部將對威脅美國利益的敵網際空間作戰實施嚇阻、截斷與拒止。為此，美國必須能捍衛自身網路的完整、保護重要系統與網路、一旦接獲命令後即遂行有效的海外網路作戰、捍衛美國重大利益並避免國家遭受有可能會發生的毀滅性網路攻擊。美軍部隊將遵守適用的法律、政策與法規，保護美國國民的隱私和公民自由。此外，美國防部作業時將遵照有關戰爭法的政策原則與法律架構。嚇阻與擊敗網路威脅需要一種能夠結合多方利害關係人的強大聯盟，俾將既有的職權、責任與能力合法的應用於美國政府、產業，以及國際盟國與夥伴。美國防部提供聯邦政府網路安全小組支援，並將持續與國土安全部(Department of Homeland Security, DHS)合作，改善重大基礎設施的網路安全，並與國土安全部及聯邦調查局共同合作來支援執法行動。美國防部仍將戮力與產業界及國際夥伴進行合作，以分享能夠保護並捍衛美國重大基礎設施的威脅情資與能力，包括維護國防工業基礎特定產業機構的運作功能，美軍各部門內部已建立了負責網路安全工作的單位。像隸屬於國防部的美國家安全局、國防資訊系統局、戰略司令部和空軍等方面都擁有從事網路戰攻防的部隊。美國透過協助改善夥伴的網路防禦能力與降低共同網路威脅的聯合行動，俾確保國際同盟與夥伴關係在威脅環境的挑戰中仍能緊密結合。美國防部將持續投資於新增與擴充網路戰力，並以近年在

人才招募、訓練與維持網路人員所獲之大幅進展作為基礎，重點在於致力發展國防部「網路任務部隊」(Cyber Mission Force)。該部隊包括操作與防護國防部網路並支援全球軍事作戰行動的網路防護部隊、支援作戰司令從事軍事任務規劃與執行作業的戰鬥任務部隊，以及反制對美網路攻擊的國家任務部隊。網路任務軍將於2016年編配人員，除人員以外，美國防部正投資最先進的工具與基礎設施以遂行其任務。為保護網路，美國國防部亦將其資訊系統移至名為「聯合資訊環境」(Joint Information Environment，JIE)的共用全軍網路基礎設施。聯合資訊環境對要發展更具防禦性的網路架構，以及改善網路作戰而言極為重要。美國防部將持續與其他部會、海外盟國與夥伴合作，建立其本身的網路防禦能力以減輕共有的網路風險。美國積極規劃網際空間與太空中有效作戰，現代化軍隊不能夠在沒有可靠的資訊與通信網路，以及安全使用網際空間與太空的情況下採取快節奏的有效作戰行動。當前的太空系統及其支援的基礎設施面臨一系列可能會削弱、破壞或癱瘓資產的威脅。據此，美國防部將繼續與國內外盟邦和夥伴共同投資於防禦自身網路、作戰能力，及網際空間與太空彈性的先進能力[26-29]。

國家與國家的戰爭從兩軍正式交戰前就已開打，網路虛擬世界的攻防戰，成為了真實世界戰爭的前哨戰，因此美國網路作戰防禦司令部技術指揮官Rob Boshonek說，網路作戰防禦司令部的任務就是要監控並協調海軍的網路系統，並防禦網路攻擊，而負責的單位包括艦隊網路司令部及美國網路司令部，範疇擴及整個美國海軍網路。指揮官Rob Boshonek表示，他們面臨威脅對象非常多，來自外部的像是駭客、工業間諜、外國間諜、恐怖份子等國家級支助的攻擊，也有來自內部的威脅，諸如對組織不滿的員工或是無知的使用者等，而手法也是非常多樣，諸如釣魚式攻擊、無線或是實體的存取、網際網路伺服器攻擊、抽取式媒體、網頁電子郵件漏洞甚至是社交工程攻擊都有可能發生。美國海軍發展出網路防禦任務支援系統(Cyber Defense Mission Support System)，這系統必須以即時或類即時的速度，接受、處理、整合以及關聯多重網路的資源，並深入了解特定網路的環境，並辨識出其中異常的活動，進而擔任支援決策系統的角色，以傳統報告和互動視覺化的形式，顯示具時效以及對應的資訊。在資訊爆炸的年代，戰爭的方式也會改變，Rob Boshonek說，資訊支配了一切，需要從三方面著手，第一是整合火力，中斷並擊敗敵方，加強同盟合作，第二為對於戰場要有警戒心，就虛擬戰場來說，關鍵資料以及關鍵服務可能是敵方攻擊的熱點，需要了解網路環境並設立攻擊停損點，第三需確保下達指令的可靠性，避免指令遭到攔截或是干擾和無法正確作用[30-35]。

肆、資通訊安全政策發展與網路戰攻防理論技術探討

我國為強化國家資通訊安全能力，行政院於90年1月17日第2718次會議通過「建立我國通資訊基礎設施安全機制計畫(90年至93年)」(簡稱第一期機制計畫)，並成立「行政院國家資通安全會報」，積極推動我國通資訊安全基礎建設工作。94年至101年，行政院賡續推動「建立我國通資訊基礎設施安全機制計畫(94年至97年)」(簡稱第二期機制計畫)及「國家資通訊安全發展方案(98年至101年)」(簡稱第三期發展方案)，在中央各部會、直轄市及縣市政府共同努力之下，已逐步達成「建立整體資安防護體系、健全資安防護能力」階段性目標。我國政經情勢特殊，面對全球複雜多變資通訊環境，以及日益嚴重資通訊安全威脅，持續落實並精進各項資通訊安全防護工作為當務之急，行政院會報提出國家資通訊安全發展方案(102年至105年)，供各機關現階段推動辦理資通訊安全防護計畫之重要依據。此方案定位為我國102~105年推動資安防護計畫之依據，透過宏觀的資安科技發展趨勢分析，進行資安整體性規劃，透過資安防護資源之投入與執行，提升我國資安產業競爭力，作為資安防護與產業創新的關鍵推手，國家資通安全會報願景與策略目標如圖四、發展藍圖如圖五與行動方案如圖六。行政院為積極推動國家資訊通信安全政策，加速建構國家資訊通信安全環境以提升國家競爭力，國家資通安全會報為了落實優質網路社會願景，特提出4項策略目標(整理如表七)，方案也將透過推展資安基礎環境安全設定、加強資安防護管理二線監控機

圖四、國家資通安全會報願景與策略目標(自行整理)[11]

圖五、國家資通安全會報發展藍圖[11]

制及情蒐、強化資安應變功能復原能力及建構資安專案管理(SPMO)機制等行動方案，達成策略目標[11]。

我國國防部依據《國防法》第31條相關規定，公布民國102年《四年期國防總檢討》報告，旨在向立法院及國人說明，國防戰略與建軍方向，並藉以檢討過去與策勵未來，有效提升國防實力。其中提及聯戰指揮機制精進構想係依據「國防二法」規範，參謀本部為部長之軍令幕僚及三軍聯合作戰指揮機構，未來持續因應組織變革、員額精簡及防衛作戰需要，透過組織整併、資源整合與作業流程調整，使高司組織運作更具效率，兵力結構更趨精實，堅益聯合作戰效能，完備國軍聯合作戰指揮機制，達到「平戰一體、權責相符」，充分發揮聯合作戰之

圖六、國家資通安全會報行動方案(自行整理)[11]

表七、國家資通安全會報四大策略目標分析表(自行整理)[11]

強化國家資安政策建立安全資安環境	網際網路的快速發展已帶來政治、經濟、社會、文化、科技及軍事等各層面的資安威脅，我國要如何建立安全及可信賴的資通安全環境，保護個人、企業及政府各部門的資通安全，維護國家關鍵基礎設施，增進民眾的信心，確保經濟、社會及國家安全，乃政府必須優先處理的課題。在複雜的網際網路環境中，因為資通安全是全方位的工作，必須就適法性、外在競爭環境的變遷、資產風險評估原則、資產價值，以及相關資訊服務等因素擬訂資安策略，不斷精進國家資安政策，投入相當資源，強化自我資通安全防護能力，建構國家整體性的資通安全服務環境，才能有效杜絕資安危害，維護國家資通安全。
完備資安防護管理分享多元資安情報	為建立可信賴的資通安全環境，確保資料、設備及網路系統安全，保障民眾權益，建置政府專屬G-ISMS(Government-Information Security Management System)體系，以提升政府機關資通安全管理作業，妥善保護各機關資訊之機密性、完整性與可用性並建立機關聯防機制，降低資安事故之風險至可接受程度，並加強G-SOC(Government-Security Operation Center)資安防護管理二線監控機制及情蒐與分享之整合，透過資安技術服務雲端化，擴大資安監控範圍；另透過G-ISAC(Government-Information Sharing and Analysis Center)分享平台，建立具資安自動通報作業之平台。
奠基資安技術能量整合科技實務應用	加強與企業及學研機構之資安技術研發合作，發展新一代全方位資安整體技術解決方案，涵蓋資安弱點偵測、滲透測試、入侵威脅、網站應用程式(Web AP)安全、防火牆應用與事故通報管理等領域核心技術。同時在網路應用方面，研究新興資安科技應用及技術標準，掌握雲端、虛擬與行動資安防護等關鍵自主技術，提升資安威脅整合分析之鉅量資料運算能力，並進行新興資安技術實務之應用。
擴大資安人才培育加強國際資安交流	擴大資安科研人才培育合作，制訂政府資安人才引進與培育配套規劃，發展資安專業職能及相關認證機制，參考國際資安人才培訓經驗，建置資安人才訓練與實習之專業學習環境；積極佈建國際資安合作交流平台，參與國際資安組織相關活動，掌握國際資安最新發展趨勢，並透過G-ISAC資安資訊分享機制，與國際資安組織擴展國際資安相關合作計畫，以加強國際資安交流。

表八、我國聯合作戰主要精進重點(自行整理)[29]

聯戰重點	聯合作戰主要精進重點分析
整合聯戰指管效能	藉 C4ISR 作戰指揮系統精進三軍聯戰指管能力，整合各主要武器系統與載臺，強化戰場管理與指管效能，提升聯戰指揮能力。
強化情資整合以及運用效能	發展各級情報中心協同作業工具，增強單位間情資整合、分析及四年期國防總檢討 Quadrennial Defense Review 情報傳遞能力，擴展情報協調機能，支援聯合作戰任務。
有效提升資電作戰統合戰力	依整建規劃建案整合網路戰、電子戰、心理戰、軍事欺敵及實體攻擊等戰力，以支援聯合作戰需求，藉整合軟、硬殺及三軍戰力靈活運用資電作戰計畫，發揮整體戰力。
簡化動員組織以及作業機制	考量未來動員機構之功能、編組、體系及戰時運用，以功能整合為導向，進行組織簡併與流程簡化，使平戰任務相結合。另將後備事務司調整為全民防衛動員室，主管全民防衛動員等事宜。有關後備部隊組建、訓練及運用，回歸作戰系統，俾達指管一元與平戰結合效能。
完善全民戰力綜合協調機制與訓練	各作戰區檢討「全民戰力綜合協調中心」開設作業，配合國軍演訓定期實施演練。另將全民戰力綜合協調組織之功能與運用，納入軍士官團教育訓練課目，使各級人員瞭解與熟稔機制運作方式，有效發揮綜合協調與支援軍事作戰之效能。
落實後勤協調聯繫支援效能	各軍司令部建立軍種後勤指管、各修護單位機動搶修及緊急籌料等作業程序，依演習驗證、檢討及修訂相關計畫與規定，以確保戰時各軍司令部有效執行後勤指管作業。
精進心理戰與整體精神戰力	精進心理戰結合資訊戰與法律戰以強化三戰效能，設立專責之「政治作戰中心」，編設「文宣心戰」及「新聞傳播」小組，兼顧對敵心戰及強化整體精神戰力，有效支援軍事作戰任務。

指揮與管制效能。聯戰指揮機制精進規劃國軍聯合作戰指揮機制為作戰決策與指揮之核心，經歷年「漢光演習」驗證，編組運作、功能間協調及軟、硬體設施已上軌道。今後將持續調整組織架構規劃，並且擴建數據鏈路系統，以加快作戰反應速度，我國聯合作戰主要精進重點整理如表八。行政院在2014年2月14日所屬機關的資訊主管會議中發布，政府網路攻防演練成果以及首次資安情境演練成果。行政院資通安全辦公室主任蕭秀琴表示，7成機關於規定1小時時限完成通報，平均65分鐘完成，整體資安應變能力以主計總處、法務部、金管會、中央銀行及海巡署等5個機關最佳。不過，測試33個機關的482個系統，也發現了108個弱點，以網頁權限控管不佳是政府機關主要問題，其次為網站未過濾特殊字元和使用簡單、預設或易猜的弱密碼。蕭秀琴主任表示，近年來國際間資安事件層出不窮，各國紛紛規畫辦理

圖七、國家實驗研究院國家高速網路與計算中心惡意程式知識庫網站[30]

系列網路演練活動，以培養政府機關在面對網路攻擊時之應處能力，如美國的Cyber Storm、歐盟的Cyber Europe及馬來西亞的X-Maya等，這次的實兵演練過程中，攻擊小組為能先了解各機關網站和系統的弱點，先進行系統探測、資訊蒐集及弱點掃描等作業，之後在不影響演練機關系統正常運作情況下發動網路攻擊，所有的攻擊過程則由裁判組負責記錄和監控。由於權限控管範圍較廣，若要改善權限控管問題，必須要從攻擊者的思維出發，思考攻擊者會怎樣進行攻擊，而驗證機制及資料，須存放在伺服器端，以免在客戶端遭竄改破解，圖七為高速網路與計算中心惡意程式知識庫參考網站。事實上，為強化資訊戰能力與爭取資訊優勢，網路攻擊與防禦訓練具有兩個重要目的，其一是藉由深入了解系統運作與攻擊機制，以奠基資訊防護之設計與整合能力，其二是改善資訊戰部隊之組織、指揮與作戰能力。目前國際發展趨勢是採用先進的建模與模擬方法(Modeling and Simulation Methodology)，來發展訓練模擬系統，以滿足此兩面向之運用需求，網路攻擊防禦訓練模擬系統發展分析整理如表九[29-35]。

表九、網路攻擊防禦訓練模擬系統發展分析(自行整理)[31]

模擬系統	網路攻擊防禦訓練模擬系統發展分析
ARENA系統	Kuhl, Michael E.等學者運用ARENA軟體來建立網路與攻擊模型，模擬網路攻擊過程，觸發入侵偵測系統(IDS)警訊，以測試資安事件管理軟體(Security Information Event Management, SIEM)。系統可以自動模擬網路攻擊，節省測試資安事件管理軟體所需人力，並提供可指定的攻擊模式，產生具代表性的測試樣本。
MAADNET網路	Surdu, J.等學者運用NetBuilder建立網路模型，以攻擊樹建立攻擊防禦模型，以DES(Discrete Event Simulation)方法來模擬攻防並針對攻防過程進行評分，以作為資安教學使用。本系統之特色是紅/藍軍可運用攻防程式搭配攻防策略，進行對抗並評估成效。
NADSTS系統	陳剛等學者設計一個大型的攻防訓練模擬系統，包括介面、應用與呈現等三個功能階層與資料庫(如圖四)，運用HLA/RTI(High Level Architecture/Run Time Infrastructure)，建立虛擬的模擬網路以供紅/藍軍及監控組訓練網路攻防手段。
Testbed@TWISC	成功大學賴溪松、楊竹星教授運用Emulab軟體及多部機架式伺服器與交換器等實體設備，建置了Testbed@TWISC，作為網路安全測試平台。本系統之特色是以Emulab軟體所建立之網路模型可在真實的電腦與交換器上自動部署，具有大幅減少網路架設時間及人為錯誤之優點。
Network Defense Trainer	Scalable Networks公司開發網路防禦訓練模擬器，提供多種網路威脅模式及威脅模式擴充集，可讓使用者動手練習各種攻擊技術，以了解攻擊之實際效果及其防護對策。藉由它的環境整合功能，可演練多步驟、適應性、連結式、合作式等複雜的攻擊模式。
Honeypot及Snort誘捕駭客及蠕蟲攻擊	Honeypot是當時最早偵測出SQL Slammer蠕蟲的方法之一。在Honeyd與駭客攻擊或蠕蟲攻擊的交談過程中，可以使用Snort來進行攻擊行為樣本的過濾篩選，將樣本供警報或鑑識分析之用。

伍、未來因應建議與結論

近來層出不窮的駭客攻擊事件，證明從SONY影業、美國陸軍、美國陸戰隊無人機單位以至於五角大廈的雲端系統，資訊安全的重要性無所不在。再加上網路發展一日千里，美軍決策者在2015年勢將正視「網路統合」的大趨勢，將網路與資訊安全概念整合於決策之中。現今資訊安全已非機構中的單一分支所能夠掌控，也不再是無足輕重的領域。相反地，資安問題早已成為機構或公司生存的關鍵。美國軍事電子通訊協會(AFCEA)副總裁瓦立克近日撰文指出，要成功將新科技導入實際運用，除了嶄新的觀念、大量的資金挹注，更要有產、官之間通暢的溝通。綜上所言，目前網路攻擊與資安觀念雖已大幅提升，但廣泛的產官整合與合作仍是必要、並值得再三強調。早在1961年，美國前總統艾森豪便高瞻遠矚地表示，民間企業在未來的世代，將成為推動資訊科技與軍事實用的重要推手，因為僅賴政府之力，並無法支撐從研發到生產的全部成本。依據國際報導敵情分析可以觀察共軍成立資訊網路作戰部隊，積極研製資訊作戰平臺，並結合民間能量，大幅提升網路作戰能力；另中共為強化電子戰能力，近年研製之各式電戰裝備已配備全軍，具備電磁參數偵蒐及電子軟、硬殺能力。中共未來將加速資訊化建設規劃，以完備數據鏈路通信系統，精進網路攻防技術，有效遂行網路作戰任務；並持續發展電磁參數偵蒐，以及提升電子作戰能量。因應於此，我國國防部訂定《四年期國防總檢討》成為國防最高戰略指導文件，並規劃國防部「十年建軍構想」及「五年兵力整建計畫」策訂之準據，對內具有指導建軍整備方向的功能，對外則有助國內民眾及國際社會瞭解政府國防目標。國部配合總統任期，於民國98年3月完成第一版《四年期國防總檢討》，具體提出國防發展及建軍方向，102年公布第二版《四年期國防總檢討》，象徵我國以4年為週期的國防檢討工作已成常態機制，對我國防政策透明、凝聚全民國防意識等均具重大意義。現階段國軍已整合各項資安防護機制，並持續擴充電磁參數資料庫及重要指管陣地電戰防護能力，有效提升聯合資電作戰能力。面對未來複雜資電作戰環境，國軍須精進資訊、網路與電戰防護能量，俾確保資訊、網路安全，強化電戰防護效能。聯合指管通資情監偵能力願景分析，國軍聯合指管通資情監偵(C⁴ISR)係以建構網狀化系統以達到網路中心戰(Network-Centric Warfare，簡稱NCW)作戰目標，藉先進通資科技，整合指管中心、武器載臺及監偵系統，並運用創新思維與戰場管理系統，掌握戰場即時資訊。國軍已整合主要指管與情監偵系統數據鏈路，建構自動化防空指管系統、制定指管共通作業環境規範、提升聯合通信系統能量、強化通信保密機制，以及建置中、長程偵蒐系統，提升聯合指管通資情監

偵能力[33-37]。

資訊的衝擊力量，可能改變當事者的認知、態度乃至行為；破壞敵方的決策運作，威脅甚至超過軍事行動。美軍據此整合資訊戰、心理作戰、軍事欺敵、電子戰等相關能力，以策略性傳播(strategic communication)形塑資訊環境；中共也大力發展心理戰、法律戰、輿論戰等概念，以強化其心理作戰優勢，都是因應現代戰爭發展而採取的重要措施。國軍須強化戰場管理、指管情傳及早期預警能量，俾精準掌握敵情動態，靈活指揮部隊作戰。聯合資電作戰未來目標為聯合資訊戰能力，包括：其一、整合各項資安防護系統及機制，以提升早期預警及聯合資訊安全防護能力；其二、統籌規劃國軍網路資安防護措施，透過聯合監偵等方法，持續強化各項資安防護網能量；其三、導入最新通資安全技術於軍事用途，提升我資訊安全防護與作戰能量；其四、規劃國軍資訊組織及人力編配基準，並執行資訊專業人員培育及訓練流路，以強化資安應變處置能力；其五、持續發展綜合性資訊戰力，以確保國軍資電優勢[29]。面對大陸網軍對我威脅，立委陳鎮湘於2014年底報告指出，對岸只要發展出新的攻擊技術，就會把臺灣和美國當成練兵對象，若未能有效防制網路駭客入侵，小則企業受創，大則國安威脅隨之而來。尤其我國是全世界感染電腦蠕蟲前三名的地區，政府除各部會間橫向與縱向的協調合作外，更應結合學術、產業與全民力量，與國際接軌，形成具有統合戰力的防護網，方為「防患未然、弭禍無形，制亂初動、止亂復甦」的最佳方案。陳鎮湘強調，網路戰已是現代戰爭的第五維形式，美國國防部長黑格認為它是「陸戰、海戰、空戰，以及太空戰之外，能夠造成威脅之一種新的軍事行動。」政府與國人都應深切體認網路安全是國家安全的基石，無平、戰時之分的不對稱戰力展現。要確保網路空間安全，絕非單一部會就能達成任務，必須靠國家的總體戰力發揮，盼盡速成立強而有力的勁旅，提升網路戰戰力，才能因應大陸網軍對我威脅。為強化國家資通安全防護作為，國防部常務次長高天忠中將於2014年11月20日表示，因應中共網軍可能威脅，國軍為政府整體安全防護一環，將持續與各部會配合致力推動各項資安防護工作與培育專業人才，建置嚴密的防護機制；國安局李翔宙局長指出，除規劃成立網域安全專責部門外，並藉此深化與先進國家合作交流，進而完備各項網路安全防護機制，捍衛國家安全；國防部通信電子資訊參謀次長室次長胡延年中將強調說明，國防部為避免駭客透過網際網路入侵國軍網路，嚴格落實軍民網路實體隔離，並精進資安防護管理機制，同時為強化資安警覺，每月均會進行網路滲透測試，以檢視國軍網路防護強度，並結合年度兵推、演習遂行網路安全演練，驗證關鍵資訊基礎設施防護能量，作為未來資安整備參考依據，提升資安防護能力。為強化國防資安意識與防微杜漸

，國軍官兵應有的認知與作為包括有：其一、慎用資訊器材，防範網路洩密；其二、深植安全警覺，勇於檢舉反映；其三、完善內控機制，肅清滲透敵諜；其四、綿密稽核措施，遏止洩密管道。總而言之，我方必須做好平戰一體的萬全防禦準備，政府應參酌先進國家網路戰作為，以創新思維，集中人、物力與財力，形成重點，建構強力網軍，確保我網路戰不對稱戰力優勢，才能使網路安全固若金湯[36-40]。

陸、參考文獻

〔1〕林盈達，“媒體被駭政府怎能置身事外-資安危機就是國安危機系列之一”，2015年1月14日，取自蘋果日報網。
〔2〕翁浩正，“更大的網路攻擊等著台灣-資安危機就是國安危機系列之二”，2015年1月14日，取自蘋果日報網。
〔3〕湯佳玲，“中國18萬網軍威脅我將分級聯防”，2015年1月13日，自由時報。
〔4〕Information Security資安人科技網，“台灣名列全球惡意網站造訪第五名防護刻不容緩”，2014年10月3日，取自資安人科技網。
〔5〕阿波羅新聞網，“中華民國：中共網軍18萬人研發各類的惡意病毒”，2014年11月20日阿波羅新聞網5232-11-21訊，2015年01月13日存取。
〔6〕資安人科技網，“掌握未來十大資安技術，有效做好攻擊防禦”，2014年7月31日，取自資安人科技網。
〔7〕資通安全資訊網，“國家資通安全會報”，2014年1月3日,取自第201401002期資通安全資訊網電子報。
〔8〕美國國防部，《2014四年期國防總檢報告》(Quadrennial Defense Review Report， QDR)，2014年3月4日。
〔9〕陳清泉，“制霸網路者，制霸世界”，2014年8月14日，取自蘋果日報。
〔10〕Chohan Wu，“〔資安小常識〕認識進階持續性滲透攻擊(APT)”，臺灣微軟資安部落格，2013年7月8日，http://blogs.technet.com/b/twsecurity/archive/2013/07/08/。
〔11〕資通安全資訊網，“國家資通訊安全發展方案(102年至105年)”，2013年12月，取自行政院國家資通安全會報。
〔12〕陳嘉宏，中山科學研究院資訊管理中心，“新型態戰爭及資安防護策略探討”，新新季刊，42卷第21期，2014年1月，226-232頁。
〔13〕王明華、嚴寒冰、李佳、賀敏、紀玉春，“2013年中國網際網絡安全報告”，2014年12月10日，http://www.cert.org.cn/publish/main/。
〔14〕陳曉莉，IThome電週文化網，“Sony Pictures 25GB員工資料被放上網，FBI發出「毀滅性網路攻擊」警告”，2014年12月3日。
〔15〕陳曉莉，IThome電週文化網，“資安業者分析「毀滅性網路攻擊」惡意程式：Sony Pictures內部網路早就被摸透”，2014年12月5日。
〔16〕Benson，“資安危機就是國安危機系列之三台灣可以成爲資安強國”，2014年7月24日，取自蘋果日報。
〔17〕李忠憲，“未來戰爭是數位戰爭”，2014年7月26日，取自蘋果日報。
〔18〕張維君，資安人科技網，國安局：攻擊38%來自本地嵌入式系統成新目標，Information Security，http://www.informationsecurity.com.tw/article/article，2013年4月29日。
〔17〕Eric L. Haney and Brain M. Thomsen著，國防部譯，論21世紀超越震撼與威懾，國防部軍官團教育參考叢書-613，2010年3月。
〔18〕林盈達，“媒體被駭政府怎能置身事外－資安危機就是國安危機系列之一”，2014年7月22日，取自蘋果日報。
〔19〕崔敬熙編譯，綜合外電報導，“加強防駭美軍網路特遣隊成立”，2014年10月28日，取自青年日報網。
〔20〕賽迪網-IT技術訊，“ 迪 2015年中國網路安全十大 加強防駭”，2015年1月15日。
〔21〕胡光曲，“美軍秘密制定網路戰規則從國內防禦到全球攻擊”，華夏經緯網，2013年5月24日，http://big5.huaxia.com/。
〔22〕USA Department of Defense，譯者李永悌，“2014美國四年期國防總檢討Quadrennial Defense Review2014”，中華民國國防部發行軍官團教育參考叢書640，2014年6月。
〔23〕USA Homeland Security，“Executive Order 13636: Improving Critical Infrastructure Cybersecurity”，Department of Homeland Security Integrated Task Force，Incentives Study Analytic Report，2013年6月12日。
〔24〕辜騰玉，IThome電週文化網，“富士通內部資安對策大揭露”，2015年1月6日。

〔25〕E-NEWS，“Web Security網站安全基礎篇(二)”，2010年第15期,取自中央研究院計算中心通訊電子報。
〔26〕C⁴ISR Go South著，陳克仁譯，“擴大籌建指管通資情監偵戰力(C⁴ISR Go South)”，國防譯粹，40卷5期，35-46頁，2013年5月。
〔27〕青年日報社，“國軍落實資安防護整備-嚴防駭客攻擊手段”，2014年11月20。
〔28〕梁華傑，“青年日報專論：共軍駭客入侵劇增美掌控「制網路權」應戰”，http://news.gpwb.gov.tw/news.aspx，2013年3月27日。
〔29〕國防部，“中華民國102年四年期國防總檢討(QDR)”，第四章國防組織與轉型，2014年9月。
〔30〕李建興，IThome電週文化網，“虛擬攻防成戰爭前哨戰美海軍打造網路戰爭支援決策系統”，2014年11月23日。
〔31〕翁興國，中山科學研究院資訊通信研究所，“網路攻擊與防禦訓練系統之建模與模擬技術探討”，新新季刊，第42卷第2期，210-213頁，2014年4月。
〔32〕黃彥棻，IThome電週文化網，“模擬APT攻擊和資料外洩事件，行政院首度資安情境演練成果出爐”，行政院資通安全辦公室，2014年2月26日。
〔33〕Richard A. Clarke and Robert K. Knake，譯者王文勇，“網路戰爭下一個國安威脅及因應之道Cyber War-The Next Threat to National Security and What to do about it”，中華民國國防部發行軍官團教育參考叢書642，2014年9月。
〔34〕財團法人國家實驗研究院國家高速網路與計算中心，惡意程式知識庫，Malware Knowledge Base，http://owl.nchc.org.tw/km/，存取時間2015年1月20日。
〔35〕Robert A. Miller and Daniel T. Kuehl.著，李育慈譯，二十一世紀之網域與「第一戰」(Cyberspace and the “First Battle” in 21st - century War)，國防譯粹，37卷，5期，21-31頁，2010年5月。
〔36〕政戰局保防安全處，“建立安全共識防敵滲透蒐情”，青年日報社，2014年9月22日。
〔37〕王能斌，“正視網路統合今年美軍發展要務”，青年日報社，2015年1月20日。
〔38〕張晏彰，“陳鎮湘：正視大陸網軍對我威脅”，青年日報社，2014年11月22日。
〔39〕吳柏毅，“跨部會強化資安防護完備安全機制脅”，青年日報社要聞，2014年11月21日。
〔40〕張晏彰，“國是論壇陳鎮湘：提高資安指揮層級確保網安”，青年日報社，2014年9月27日。

作者簡介

空軍上校　吳嘉龍

學歷：中正理工學院電機系電子工程組77年班、美國俄亥俄州空軍理工學院電腦工程研究所84年班、國防大學理工學院國防科學研究所電子工程組93年班。經歷：電子官、區隊長，教官、講師、助理教授、校教評秘書、科主任、副教授、資訊安全學會永久會員、危機管理學會理事、危機管理學會資訊安全主任委員、教授、系主任。現職：航空通訊電子系上校專任教授兼任系主任。專長領域：資訊戰，通資安全，無線通訊，網路通訊協定。