航空技術學院學報 第七卷 第一期 第 139－148 頁（民國九十七年）
Journal of Air Force Institute of Technology, Vol. 7, No. 1, pp. 139-148, 2008

美國國家安全戰略資通安全規劃與國土防衛策略研究

National Security Defense Strategies on Counterterrorism Challenges

吳嘉龍[1] 左豪官[2] 王文龍[3] 曾仁杰[1]

Chia-Long Wu[1], Hao-Kuan Tso[2], Won-Lung Wang[3]and Jen-Chieh Tseng[1]

[1] 空軍航空技術學院一般學科部航空通訊電子系

[2] 陸軍專科學校電子工程科

[3] 高苑科技大學電子工程學系

[1]Department of Aeronotic Communication Electronics, Air Force Institute of Technology

[2]Department of Profesional Staff, Air Force Institute of Technology

[3]Department of Electronic Engineering, Kao Yuan University

摘要

美國的國家安全戰略以對付強權與潛在威脅為重點，2001 年 9 月 11 日發生於紐約和華盛頓的恐怖份子攻擊行動，充分驗證出恐怖攻擊威脅的危險性，美國與其盟邦在此全球反恐戰役中，正體驗恐怖主義挑戰的戰略部署與因應能力。然而隨者軍事科技發展日新月異，直接造成全球國防安全規劃與國土防衛思維的影響演變，而今日人類面臨產生對於國家安全的衝擊因素包括有：錯綜複雜的族群或宗教衝突、國際恐怖主義、核生化武器、大規模毀滅性武器、資訊戰、航天戰等威脅。過去 10 年中，全球各地事故與危機層出不窮，顯示許多國家從冷戰過渡到後冷戰安全架構與作為的過程中，已經歷重大安全挑戰，而現代恐怖主義威脅無疑是此一新國際體系的最大單一挑戰。針對於強調通資電競爭優勢的因應作法上，應深入瞭解資訊戰與電子戰發展趨勢，研擬相關戰術戰法，並應強化精進國家與軍隊整體網路危機管理與安全作為，有效確保網際網路及重要國家基礎建設，進而達到鞏固國土安全與維持國家長治久安之目標。

關鍵字：反恐主義、國家安全戰略、數位防禦、國防安全規劃、效能作戰

Abstract

After 11 September 2001, we should rise to meet safety challenges and take advantage of emerging opportunity. National attention is focused on the substantial threat posed by international terrorists to the homeland, law enforcement officials must also contend with an ongoing threat posed by domestic terrorists based and operating. Most importantly, we should recognize that the ability to assemble, analyze and disseminate information both internally and with other intelligence and law enforcement agencies is essential to our success in the war on terrorism. The

cyber-threat to us is serious and continues to expand rapidly the number of actors with both the ability and the desire to utilize computers for illegal and harmful purposes rises. We should be working to aggregate the technological and investigative expertise necessary to meet the challenges that lie ahead and to better enhancement the national security and defense of our country.

Keywords: Counterterrorism, national security strategy, information superiority, digital defense, effects-based operation.

一、前言

今日的戰略局勢由各種錯綜複雜以及相互矛盾的勢力架構所形成，由於資訊時代來臨，加上電腦與網路的普遍與便利的特性，徹底改觀了未來戰爭的面貌與作戰型態。資訊科技進步使戰場從傳統的三度空間向任何維度來發展，在數位防禦作為中數據資料鏈路為未來戰場掌握情資、有效遂行指揮管制與發揮兵火力之首要工具，國軍應秉持一貫強化戰備理念，並考量聯合作戰需求與指導，依據現況以整合三軍通資電能量，以取得戰場上通資電優勢。

美國國家安全戰略之所以採取主動方式為主軸，並認定在當前戰略下，採取被動反應之風險太高而不足取，乃是因為恐怖主義所具備之分散、堅決與隱匿本質，使國家遭受攻擊的可能性極高，但卻難以有效偵知或嚇阻。面對美國政治、軍事與經濟基礎建設對於網路科技依賴的程度日益加深，因應現代資訊科技發展對於現代化戰爭與國家安全戰略所造成的的影響，本論文將針對「美國國家安全戰略資通安全規劃與國土防衛策略研究」為主題深入探討，以期國內對相關議題與其理論及技術發展能有深入的瞭解認知。本論文章節說明如下：第 2 章探討主題是國家安全戰略；第 3 章探討反恐主義效能作戰，探討反恐策略；第 4 章探討主題是國防安全資訊優勢；第 5 章為網路威脅安全防護；第 6 章為結論，最後是參考文獻。

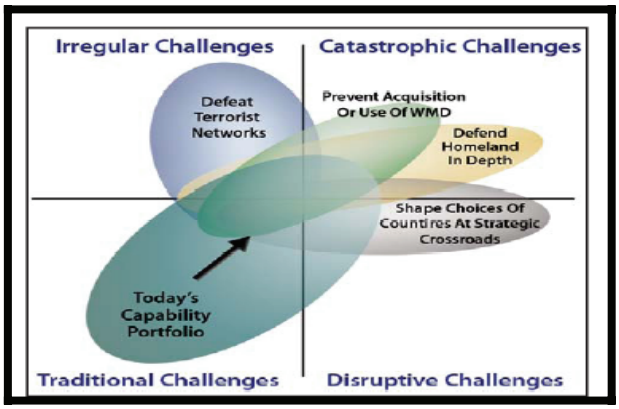
二、美國國家安全戰略

美國對付恐怖主義有其弱點，因為為廣大開放性社會，為避免妨礙遷徙自由及侵犯隱私，而受到安全規定的束縛。美國在冷戰結束後，開始憂心大規模毀滅性武器的擴散與威脅，尤其在「911」事件後，全面加強反恐措施與改革行動，其範圍涵蓋政策宣示、戰略結構、法令制頒、作戰準則修訂、組織整合與資源調配等面向。美國認為堅強的領導中心在恐怖攻擊事件無可避免發生時，必須將注意力集中在長期的戰略目標，而非短期的反應，對於任何恐怖攻擊的第一反應應該著重兩件事，第一在於恐怖攻擊意圖所在，第二則在於恐怖份子所要引發的反應，然後接下來的任何因應作為則必須配合最高戰略評估來貫徹展開。特別強調的是，不僅只是在反恐作戰中求勝利，更要以獲得最後的和平為首要目標。

「2002 年美國國家安全戰略」(national security strategy，簡稱 NSS)確認恐怖主義為將來可預見之威脅，並強調採取「先制」與「預防」兩者作為因應此威脅的準則，防制恐怖組織以大規模毀滅性武器攻擊美國與其盟邦的手段。此種戰略所衍生出一種定義狹窄且具爭議性之用兵準則，對於未來國家軍事戰略將產生諸多後續影響。美國總統所提出之主義通常是以大戰略層次處理外交政策[1]，此層次之主義不律定特定之經濟、政治或軍事戰略，只確認國家施政大原則或目標。對美國國家安全戰略而言，重點在於妥善應用國家各階層資源，鑑於流氓國家與恐怖份子之目標，今日美國已無法單純倚賴過去所使用的被動反應姿態。

美國自建國以來經常採取防禦性攻擊的國家安全政策，美國面對國際局勢演變基於

缺乏嚇阻潛在攻擊者之能力、各種現代威脅瞬息將至之特性、以及敵人所使用之武器可能造成之大規模傷害，被動反應已無法因應。同時，「先制」與「預防」的分野在美國國家安全戰略中的界線已然模糊。在今日，美國布希總統為捍衛美國國家、人民以及國際上盟邦的利益，對於流氓國家撐腰的非理性恐怖組織採用「在威脅接近前加以辨識與摧毀」作為。美國在國防部長倫斯斐的領導下，國防部高層（包括：國防部長與副部長、參謀首長聯席會議主席與副主席、陸海空軍軍部部長、四位軍種參謀長，以及五位國防部次長）成立了高階領導層級檢討組（senior leadership review group，簡稱SLRG），並廣納國防部各組織的主管聯合委員會（corporate board of directors），分析彙整出軍事作戰經驗，美國國防部因而能將相關意見經驗教訓轉化成為組織變革，共同執行國防安全策略總檢討，以下圖一為美國 2006 年四年期國防總檢威脅圖示意圖[2]。



圖一 美國 2006 年四年期國防總檢威脅圖

表一 美國 2006 年四年期國防總檢威脅說明

美國 2006 年 3 月公布四年期國防總檢（quadrennial defense review，簡稱 QDR）戰略環境威脅與挑戰類型分析	
非正規性（irregular）	災難性（catastrophic）
非正規性環境威脅包括有恐怖主義、叛亂、內戰、超限戰等新興構想，非正規性環境威脅可能性極高，為弱勢者採用的戰略	利用大規模毀滅性武器攻擊美國本土、癱瘓全球市場或重要盟國，災難性環境威脅可能性漸漸增高，此戰略造成社會震撼失序
傳統性（traditional）	破壞性（destructive）
傳統性環境威脅是指國家運用軍隊進行軍事競賽和衝突模式，此環境威脅可能性已日漸降低	破壞性技術方面包括生物武器、網路戰或太空戰爭、微型技術，破壞性威脅長期而言對美國不利

以上表一為美國 2006 年 3 月公布四年期國防總檢（Quadrennial Defense Review，簡稱 QDR）戰略環境威脅與挑戰類型分析說明。

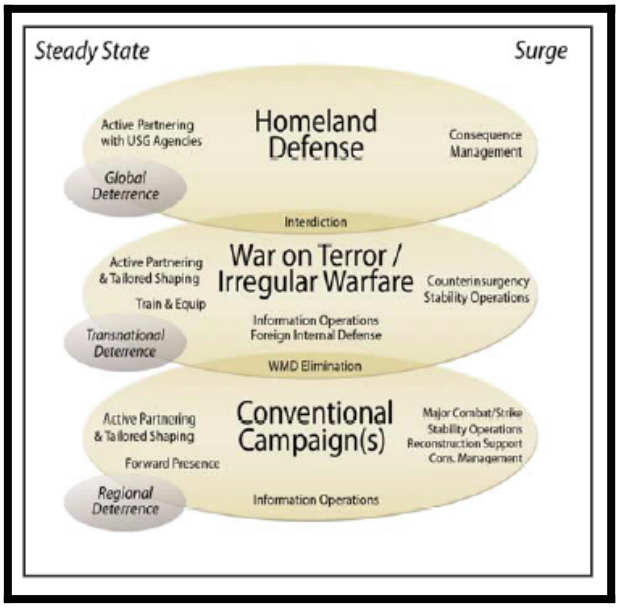
三、反恐主義效能作戰與國土防衛戰略

針對於反恐主義效能作戰與國土防衛戰略分析，美國面對大規模毀滅性武器擴散威脅，正調整國家安全、軍事任務及外交政策，2002 年 12 月 11 日美國白宮公佈「對抗大規模毀滅性武器國家戰略」(national strategy to combat weapons of mass destruction)。布希政府以官方文件宣稱如果大規模毀滅性武器(weapons of mass destruction，簡稱 WMD)被用於攻擊美國本土、海外駐軍或其盟邦[3]，美國將「訴諸一切可選擇的手段」以壓倒性的力量進行反擊此份戰略計畫強調對抗核子武器、生物武器或化學武器的使用與擴散，是國防安全戰略不可或缺的要素。

對抗毀滅性武器的國家戰略將建立在三個互相關聯與促進的支柱上，並在優先建立的四大相互交叉實施功能的前提下，結合形

成整體戰略。綜觀此戰略實質與隱含意涵，顯現美國將採取外交、軍備控制、嚇阻、防禦和打擊等各種措施，預防與阻止核生化武器及其載具所構成的威脅。

美國對抗 WMD 的理念出現重大的轉變，其戰略地位已與反恐怖主義(counterterrorism)、國土安全（homeland security)等戰略並列。美國政府針對大規模毀滅性武器擴散擬定安全面性計畫，實施政策、資源與相關技術等多面整合，以利因應大規模毀滅性武器之評估與執行。美國為來在對抗大規模毀滅性武器時，除採取常規反應和防衛措施(含核武在內的手段)外，還將有效的情報、監測、禁止和國內執法能力來嚇阻使用大規模毀滅性武器所構成的威脅，打擊製造、擴散、運輸、隱匿大規模毀滅性武器的敵對國家[4]。此外，美國國防部並著手部署防衛系統，要求於具備實戰能力，以保護美國本土與海外部隊及其盟邦。美國政府對抗大規模毀滅性武器的政策、戰略與做法，值得我國做為借鏡，並啟發我加強改進應變機制與因應作為，防範毀滅性災難與核生化恐怖攻擊。



圖二 2006 年美國 QDR 國土防衛戰略示意圖

以上圖二為美國 2006 年 3 月公布四年期國防總檢中國土防衛（homeland defense）、非正規反恐戰爭（terror/irregular warfare）與傳統戰爭取勝（conventional campaign）戰略示意圖[2]，本示意圖說明包括聯合作戰、軍事交流與跨國軍事演練相關之國土防衛、非正規反恐戰爭與傳統戰爭勝利指導方針與策略。

「911」恐怖攻擊事件發生後，美國瞭解恐怖主義和大規模殺傷性武器是當今最大威脅所在，而且美國各盟邦和世上多數國家都遭受到此威脅。美國軍事安全的戰略發展，美國很清楚安全決策將會對明日的國際環境產生深遠的影響，美國政府正努力解決兩大議題：(1)針對美國必須使用武力的威脅，如何加以搜尋、發覺、追蹤、列舉優先順序並加以鎖定；(2)針對美國必須使用武力的威脅，如何運用軍事武力。由於流氓國家支持恐怖份子，使恐怖份子在某種程度上呈現區域化情況，故而使確認與鎖定恐怖份子的工作較為簡單。

德國為預防危機並防範和管理衝突，聯合作戰整備性也因而提高，以德國陸軍為例，其轉型目標為持續以作戰任務為導向，透過不斷的拓展戰力並跟上北約及歐盟其他盟友的水準，以確保德國能事映變遷的安全環境，此乃德國能符合軍事需求並對抗變動威脅的原因。德國並清楚的瞭解到唯有在各方面精確提升成本效益與功效，德國才得以集中發展核心戰力，也才能達成強化部隊戰備的目標[5]。

四、國防安全資訊優勢

美國 2005 年 3 月的國防戰略指出，為了因應平時與戰時的狀況，除了研究國防軍備的建置與作戰計畫的效益外，也要運用資訊與通信等現代科技，為國防整體戰力，建體完善有效的指管通資情監偵（command、control、communications、computers、intelligence、surveillance、reconnaissance，簡稱 C^4ISR）系統，以及電子戰、資訊戰、兵器戰等新一代武器系統，以協助國防戰略與戰術各層面的運作。美軍在 2020 年聯戰願景（joint vision 2020）指出資訊優勢

為美軍達到全方為主導地位的關鍵因素。以美軍在 2003 於伊拉克所發動的戰爭來看，美軍對於高科技在戰爭與軍事的運用與上次波灣戰爭相比，已經產生重大的改變。高科技戰爭戰爭運用先進的科技（尤其是資訊科技），將之整合於軍事作戰中。而因為高科技的運用，也使美國軍事安全無論在戰爭型態的變化、影響與戰路戰術的運用都產生了新的變化（包括數位化、衛星通信科技、網路技術的精準動員）。探討美軍在伊拉克所從事新型態的高科技戰爭，可歸納出以下五點的轉變[6]：

一、戰爭影響範圍的模糊化：傳統局部戰爭中，主要是以火力打擊和兵力機動作戰為指標，戰爭範圍有明顯的地域性。而資訊化戰爭中，雖然仍使用火力打擊和兵力機動作戰，但資訊攻防作戰卻擴大為全面性，而沒有前後方的差別。

二、平時與戰時的分界模糊：因為戰爭突發性，使得戰時與平時之間的分界逐漸模糊與淡化。而面對資訊化戰爭的高科技性的影響，戰爭前的兵力集結、國際外交的合縱連橫、以及戰爭資源的籌劃準備，今日已不盡然是發動戰爭前循序漸進的必要步驟，。

三、掌握資訊優勢（information superiority）：隨著軍事科技資訊化程度的提高，傳統作戰的武器也提升其作戰效率，戰術運用也隨之調整，網狀化戰爭(network centric warfare，簡稱 NCW)、網電一體戰等新的作戰形式陸續出現，逐漸改變和取代傳統的作戰型態。

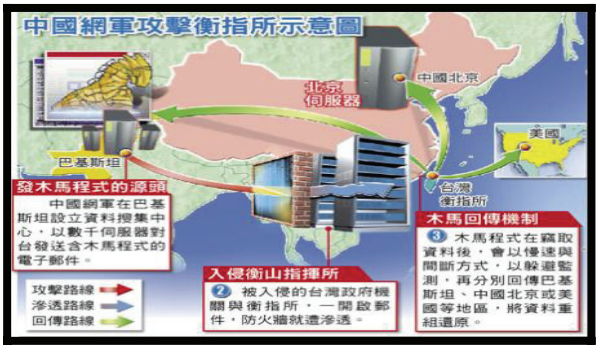
四、軍種作戰任務的聯合化：軍事組織原先依照軍隊作戰區域的不同與功能區分為不同的軍種，在長遠的現代戰爭中，一直是不同軍種的各自獨立作戰，或是依照地理環境遵循一定的接戰程序。

五、不同作戰系統的整合化：在作戰系統的整合中，無論是後勤支援系統、火力打擊系統與作戰指揮系統等都是同等重要。資訊化戰爭呈現出非接觸性、非對稱性與非線性的戰爭形態，而要爭取此三戰爭形態的優勢，不同作戰系統的整合將是重要關鍵。

培養運作於數位化戰場的技能、創造訓練有素之部隊，是美國將其部隊轉型為數位化部隊之重要課題。美陸軍第一個數位化師（第 4 機械化步兵師）揭示的訓練願景為「達成部隊轉型之挑戰[7]，使成為訓練有素、有凝聚力之戰鬥部隊，以發揮資訊系統及處理程序潛在能力」。第 4 機械化步兵師接受數位化訓練的地點是在胡德堡的中央技術支援設施處（central technical support facility，簡稱 CTSF）。CTSF 是由美陸軍指、管、通專案管理辦公室（program executive office for command，control，and communications systems）成立，中央技術支援設施處同時亦負責系統文件版本釋出的管制（release control）、系統測試、某特定部隊所使用的系統版本之管理[8]。

五、網路威脅安全防護

近幾年來，由於網際網路的快速成長，加上電子商務的掘起，使得人們對於網路所可能帶來的商機存在著無限美好的願景，然而在仰賴資訊科技的同時，仍然存在許多潛在的網路安全威脅與駭客攻擊[9]。網路服務的應用為企業節省成本與提高升生產力是最顯而易見的，因為公司不必再去煩惱彼此系統間如何溝通的問題。溝通程序越簡化，就越能提高生產力。生產力一旦提升，成本自然降低。



圖三 中共網軍攻擊衛指所示意圖

由於網路系統比以前更加便利，電腦性能與運算能力越來越強，越來越好用，也提高非法入侵的頻率。然而，經由網際網路的

連結，來自世界各地的駭客入侵、密碼偷取、阻斷服務攻擊等網路攻擊事件促使美國也不例外的必須重視資訊網路安全，圖三為中共網軍攻擊衡指所示意圖。由種種關於電腦網路的發展顯示，未來破壞安全的惡意入侵行為會越來越多。然而，網際網路在軍事上的運用則極為廣泛與重要，透過網際網路使得戰場全球化與三軍聯合作戰的一體化目標得以實現，而且各軍種能於作戰時共享作戰情資，並以最快之速度傳遞交換情資[10]。

為慎防國軍資料外洩，強化資訊安全管理，國防部近期訂定「國軍資訊安全政策」，以期建立「安全」、「穩定」、「便利」的資訊環境。另外，因應中共網軍威脅，國軍除呼籲各級貫徹網路實體隔離、明定標準即時獎懲、嚴禁官兵公務家辦等要求，並將現階段資安重點政策置於「網路安全管理」、「國軍人員資安教育與督考評鑑」、「資安應變暨通報機制」、「資訊系統發展與管理安全」及「資訊資產管理」等五大要項，藉完整的資安防護機制，確保資訊安全，而國防部也要求各司令部、軍團（指揮部）、聯兵旅級（三軍單位比照）均應定期實施資安督檢，落實資安工作。民間合作企業亦應遵循。因應中共網軍威脅與駭客攻擊，國軍刻正積極建構完善且安全無虞的資安環境。國防部特別結合任務和業務需求與國軍保密實施規定等規範，訂頒「國軍資訊安全政策」，要求國軍所屬機關、學校、廠庫、醫院、部隊等單位，以及平行合作之民間企業等均應遵循其中各項資安要求規定；範圍則包含實體與資訊相關辦公室、機房與設備，電腦系統、資訊管理作業流程、人員及資訊紀錄等。

依據美國國防部的調查研究中指出，中共利用集中力量發展資訊技術以及其衍生的資訊戰硬殺（hard-kill）武器，亦將成為對抗強權的重要武力。中共當前正在研究資訊戰的攻擊性運用，以對抗外國的經濟、後勤和指管通電與情報系統（C^4I），並極力建構一個可以攻擊其他國家電腦（包括軍民用電腦）的能力 [11]。

美國重要的基礎建設是由公共以及私人機構所組成，部門類別包括有農業、食物、水、公共健康、緊急服務、政府機關、國防工業基地、資訊和通訊、能源、運輸、銀行和金融、化學和有害物質、以及郵政和貨運。網路空間是國家控制系統裏的中樞神經系統。網路空間是由數以千計的內連電腦、伺服器、路由器、開關和光纖系統所組成並讓國重要的基礎建設得以正常運行。如此，網路空間的健全功能對美國的經濟和國家安全是相當重要的。

美國國家資訊安全策略是用來保護國家的整體努力，此策略是由國家國土安全策略中的國家重要基礎建設項目之一，其中關鍵資產的實體保護策略所組成。此安全策略可以讓美國人具有防禦個人網路空間的能力(engage and empower)。防禦網路空間是勢防禦一個相當困難的策略性計畫挑戰，美國政府體認此困難挑戰必須藉助於美國整個社會，其中包括含聯邦政府、洲和地方政府、私人機構、以及整體人民共同協調和集中注意力的努力才能達成[12]。

值得注意的是，美國資訊安全策略目標有三:(1)預防對於美國重要基礎建設的網路攻擊；(2)減少國家受網路攻擊的脆弱性；(3)當網路遭受攻擊時減低受損程度並降低系統所需回覆時間。由於現代資訊通信科技的快速發展，使得戰場情資可以透過有線或是無線網路，快速且正確的傳播給各個作戰部隊。此一戰場情資傳播能力若是勝過敵方，表示具有資電優勢，如此可進一步透過網路執行跨軍種或是跨兵種的聯合作戰，並倍增制敵機先的能力[13]。

針對於美國網路安全五大重要優先順序為例研究，有下列五點因應作為，茲說明如下：

一、國家安全反應系統對蠕蟲等惡意網路入侵攻擊活動所造成的損害快速的識別、資料交換和進行交換。針對於足以影響國家安全層級攻擊活動，美國將運用政府和工業間的

合作關係進行相關分析、警報提示以及協調性反應作為。

二、國家安全網路安全威脅評估和弱點修補，由於攻擊者藉著對於國家網路系統的弱點發掘，條理具有規模層次的攻擊最具威脅的弱點者存在於重要的基礎建設的資訊資產系統裝備以及網際網路的連結機制外連。

三、加強網路安全管理措施，國家網路安全認知與訓練計畫大部分網路弱點威脅來自於人們（電腦使用者、系統管理著、科技的研發者、資訊長、執行長）對於網路安全認知缺乏，這個弱點威脅產生了對重要基礎建設嚴重危機。

四、重視政府網路安全防禦，雖然國家重要的基礎建設的電腦系統只有少數的政府主管會掌管到政府各個層級執行對於農業、水、食品、郵政和貨運的重要設施，然而重要的資訊傳遞正倚賴著網路的安全得以正常遂行。因此政府對於商業活動與通訊網路安全的防禦相當重要，有效防範網路犯罪，針對市場的交易上建立更加的研發安全的技術與機制。

五、由於網路的便利特性，恐怖組織網路攻擊可以不分國界由全球網路擴展的網路系統在任何角落以極快的速度進行惡意攻擊。美國並藉助國際合作模式與系統架構來控制執行資訊的分享減少弱點，阻止惡意的攻擊行為。

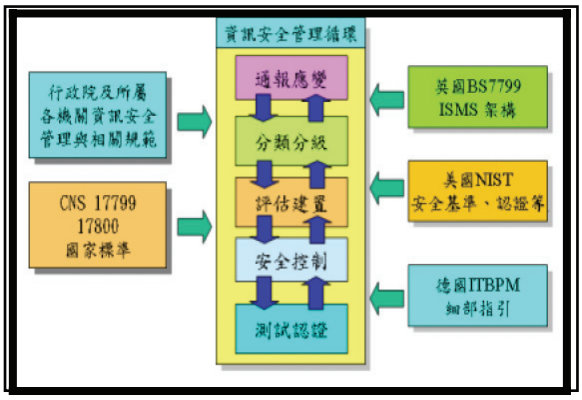
針對於美國網路安全防禦角色與責任剖析，防禦角色分類為以下五種:家用電腦使用者/小企業（home user/small business）、大企業（large enterprise）、重要部門/基礎設施（important infrastructure）、國家議題及弱點（national issues and vulnerabilities）、全球性（global）[14]。針對於資訊安全惡意攻擊的危機管理，世界幾個重要性的資安團隊組織例如有：CERT（computer emergency response team）與FIRST（forum of incident response and security teams）。

一般而言，系統的安全等級大都以美國國防部提出的橘皮書分為 A1、B1、B2、B3、C1、C2、D 為一評估標準如表二所示。一般防火牆大都介於 Class B 與 Class C 之間用於商業用途以及線上電子交易之大小企業，Class B 是以系統強制控制安全機制如銀行等重要機構均需架設此一類防火牆，並結合可信賴作業系統，做到正規化的防護。Class C 是人為控制的方式，可能因人為疏忽，導致某種漏洞，後續的發展之防火牆也相繼導入人工智慧及定期下載更新程式，填補漏洞以防止有心或惡意人士入侵。

安全等級	使用環境說明
A	提供特別安全的防護的資訊安全使用環境(例如：外交、國防、戰場情報)
B1-B3	提供正規防護的資訊使用安全環境 (例如：電子交易、商業秘密等敏感資料)
C1-C3	提供普通防護資訊使用安全環境
D	提供最少防護的資訊使用環境

表二 美國國防部橘皮書資安防護評估標準

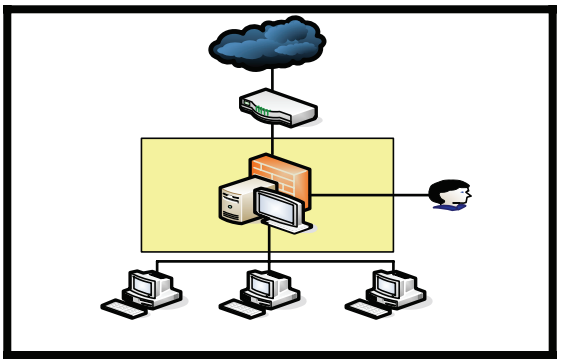
其中，CERT 是電腦危機的處理團隊，其起源是由美國政府在卡內基美隆大學 CERT/CC (coordination center)所建立的[15]，而這個最早的 CERT 組織起源是美國政府在 Morris 電腦病蟲事件後所因應運作的。後來各國政府也相繼成立自己的 CERT 組織（我國稱為 TW-CERT），FIRST 所指的是 CERT 組織間的協調組織。美國 NIST SP800 系列之資訊安全基準、系統生命週期與認證授權等機制。資諳規範藍圖發展參考相關規範如圖四所示，其中，美國 NIST SP 800 資訊安全相關文件是依據時間序列從 1980 年代末期開始發展，各時期依當時需求發展不同之參考文件，目前包含草案已發展了約 84 份資安文件，若進一步分析 NIST 已完成之資安文件，可將文件歸納成通報應變、分類分級、評估建置、安全控制與測試認證等五大類。



圖四 美國資訊安全規範與參考藍圖指引圖示

根據論文研究，美國資訊安全政策從 2001 年的 911 事件區分為兩個時期，在 911 之前以電腦安全與電子商務安全為主軸，在 911 之後，則著重在國土安全保護及電子化政府安全之議題上。其中 2002 年通過「電子化政府法案」（e-government act）中的「聯邦資訊安全管理法案」（Federal Information Security Management Act，簡稱 FISMA）即是針對資訊安全相關推動與控制措施作強制性之要求，包括律定相關單位職掌、建立年度資安績效稽核與評鑑、建立資安事件處理中心、發展資訊安全規範與指引等工作[16]。

以我國為例，TW-CERT 提供了以下的服務：事件回報、遠端掃描、電子報及研討會，GSN（government service network）-CERT/ CC 提供了以下的服務：電腦緊急事故處理建議、定期公布電腦安全相關資訊、推廣教育訓練及提供課程訓練、加強使用者對電腦安全認識並與協助各單位成立自己的電腦緊急事故處理小組協助單位組織改善系統安全，『政府資安作業共通規範』計畫[17]參照世界先進國家資安發展經驗，考量國家資通安全整體與長遠之發展，圖五為典型資安防禦系統架構示意圖，圖六為透過搜尋引擎過濾防止惡意網頁程式[18,19]。



圖五 資安防禦系統架構示意圖

圖六 透過搜尋引擎過濾防止惡意網頁程式

六、結論

在本論文研究結論裡，我們整理以下幾項的心得供大家參考：（一）面對國際性恐怖威脅分析，恐怖份子正圖謀使用大規模毀滅性武器恐怖攻擊對付包括美國與其盟邦；（二）美國安全戰略四年期國防總撿報告分析指出未來武器機動性、快速反應能力與快速部署的重要性；（三）因應反恐戰爭與低強度衝突威脅需增加特戰兵力，配合更多人員情報資產、提升情報用資訊裝備（尤其是無人飛行載具）與快速反應輕裝部隊；（四）德國陸軍是北約反應部隊及歐盟作戰的成員，其轉型目標是持續以作戰任務為導向，不斷拓展戰力，以發展嚇阻戰略效果；（五）儘管反恐戰爭主導了美國國防部作戰思維，我空軍仍須維持空中優勢、提升國防戰力系統性能和培養全球佈局等核心能力，為對抗各種國安威脅作好充分準備。「保密」是軍人的天職，「資安」更是現代軍人必須具備之基本素養。現代戰爭勝負取決於頃刻，

任何機密資訊如遭敵刺探蒐集，極可能造成關鍵性的影響，機密資訊的維護絕不僅止於保防或資訊人員，而是全體國軍官兵共同的責任。所有的保密安全措施及資安監控機制均沒有萬無一失的必勝公式，惟有建立國軍官兵保密習性及提升資安素養，時時加強資安警覺，資安防護才不會流於形式、淪為口號，而能實實在在鞏固國軍內部，使有心之人無可乘之機。最後值得注意的是，面對因應現代反恐主義發展，在論文探討國防安全資訊優勢的章節中，可多加參考美國 2020 年聯合作戰願景與心得，深知善用我創新研發能力與科技優勢是為當前現代反恐主義挑戰中國防安全規劃與國土防衛理論策略研究首要工作，也唯有做好當務工作與因應，才能有效提升國防整體戰力與確實確保國土整體安全。

參考文獻

1.U. S. Government，The National Security Strategy of the United States of America，Washington D. C.，September，2006。

2.The Project on Defense Alternatives The Commonwealth Institute，The Quadrennial Defense Review 2006，Office of the Secretary of Defense，February，2006。

3.Sam C. Sarkesian、John Allen Williams、Stephen J. Cimbal，美國國家安全，Offense and Defense in The International System，國防部史政編譯室，45-69 頁，2005。

4.Adam J. Hebert，譯者/高一中，九一一事件經過重現，取材/2004 年 10 月美國空軍月刊 (Air Force Magazine，October/2004)，國防譯粹第 32 卷第 7 期，4-16 頁，2005。

5.Wolfgang H. Korte，譯者/章昌文，德國陸軍未來作戰與轉型，取材/2006 年 8 月美國路軍月刊 (Army Magazine)，國防譯粹第 33 卷第 10 期，48-52 頁，2006。

6.潘進章，共軍資訊化戰爭戰鬥精神之研究，空軍軍官雙月刊第 133 期，58-75 頁，2007。

7.Dennis Steele，譯者/謝豐安，實戰前之最後訓練，取材/2004 年 5 月美國陸軍月刊(Army，May/2004)，國防譯粹第 32 卷第 4 期，44-47 頁，2005。

8.Robert S. Ferrell，Army Transformation and Digitization - Training and Resource Challenges，USAWC Strategy Research Project，2008。

9.Arnel B. Enriauez，譯者/黃文啟，2002 年美國國家安全戰略，取材/2004 年航太空權季刊秋季號 (Air & Space Power Journal，Fall/2004)，國防譯粹第 32 卷第 4 期，48-62 頁，2005。

10.林宗達，以弱勝強的考量剖析中共信息戰之不對稱戰的戰略考量，全球防衛雜誌軍事家點評論，4-13 頁，2005。

11.寧大強，中共網路(絡)戰發展對我防衛作戰影響之研析，國防雜誌第 20 卷第 7 期，104-112 頁，2005。

12.桑治強，中共航天戰發展與我國應採之策略，國防雜誌雙月刊，96 年 12 月刊，第 22 卷，第 6 期，81-94 頁，2007。

13.Stoneburner G.、Goguen A.、Feringa A.，Risk Management Guide for Information Technology System，NIST Special Publication 800-30 Revise，NIST，January，2004。

14.U. S. Government，The National Strategy to Secure Cyberspace，Washington D. C.，2003。

15.CERT/CC，Computer Emergency Response Team/Coordination Cente，CERT® Coordination Center，http://www.cert.org/。

16.鐘榮翰，行政院及所屬各機關資訊安全管理規範，規劃與訂定資通安全共通規範網站，C12 行政院及所屬各機關資訊

安全管理規範(修訂草案)_941102.pdf，2005。
17. 國家資通安全會報技術服務中心，政府資安作業共通規範，資安共通規範發展藍圖整體規劃，規劃與訂定資通安全共通規範網站，http://www.giscc.org.tw/giscc/，2008。
18. William Stallings，賴榮樞譯，網路安全精要應用與標準，第二版，普林斯頓國際有限公司，2005。
19. 雲首博，網站安全之研究與系統開發，電信研究雙月刊（TL Tech. JOURNAL），97 年 2 月刊，第 38 卷，第 1 期，1-19 頁，2008。