美軍資訊戰與資安技術發展之研究

作者簡介

吳嘉龍中校，中正理工學院48期電機系、美空軍理工學院研究所、中正理工學院研究所；曾任電子官、教官、區隊長、講師、助理教授、科主任，現任空軍航空技術學院副教授。

提　要

一、在現今的時代，由於資訊設備的功能日新月異，資訊網路也日趨便利，造就了人們對資訊設備及網路的使用性與依賴性漸行加深；相對的如何維護資訊安全管理系統，建立防範風險阻斷的機制則是一項重要的課題。

二、依據95年全球資安威脅資料統計，惡意程式攻擊活動次數，臺灣受攻擊比例高占3%，世界排名第九；而電腦感染殭屍病毒數目統計，臺灣占7%，排名第七；針對上網人口數來統計，惡意程式攻擊「密度」計算，則臺灣高居世界排名第二，顯見網路危機四伏，值得網路使用者與資訊安全管理者加以重視。

三、網際國土安全正面臨如何打贏一場無形的戰爭（Winning the Hidden Battle），今日戰爭勝負取決頃刻之間，重要軍事機密如被敵人刺探、掌

握，均可能造成勝負逆轉的關鍵性影響。如何認清資訊戰本質，落實「預防非法入侵、完備管控機制、強化資訊確保」發展方向的現階段資安政策，以建構簡便、優質、安全的資訊作業環境，來有效杜絕資安事件肇生實為重要議題。

關鍵詞：資訊戰、國土安全、資通安全、惡意程式攻擊、資安事件。

前　　言

隨著資訊科技快速發展與創新，無線網路傳輸快速與普及，使得資料存取管道及傳輸更加便利，在此同時，機密資訊遭受竊取與破壞的風險也隨之大幅提升，網際網路已成為一個沒有邊界與無聲的戰爭平臺，資訊戰是一種低成本、高效益的攻擊武器，技術高超的網路駭客，隨時可能藉由網路侵入防護能力薄弱的電腦進行破壞。「網路即戰場」，做好資訊安全工作就是做好戰場管理，這是資訊安全防禦應有的認知。從2005年全球資安技術發展為例說明，產值規模達257億美元，相較於2004年成長17%，而2004至2008年複合成長率（Compound Annual Growth Rate,CAGR）為16.7%❶，顯見資訊科技市場對資訊安全威脅的重視。而針對資安控管作為而言，美國國防部於2008年年底緊急通令全球各單位的所有軍、文職人員，立即全面禁止在公務電腦上使用隨身碟，以防止進一步遭到駭客破壞。基此，美國軍方若干儲存極機密資訊的有關電腦，其USB槽已開始處理使其失去效能（Disable），讓有心者無法順利竊取資料與降低USB槽感染病毒、木馬的機會，正可看出美軍對資安管理的重視程度。中共在1999年底提出「網軍」概念，觀察中共信息戰積極作為，其「網軍」無時無刻不用盡心思，利用網路對我實施資料竊取與情蒐工作，著重侵入敵方指揮網路系統，進行瀏覽、竊取、刪改有關數據或輸入假命令、假情報、破壞敵方整體作戰自動化指揮系統，使其做出錯誤決策。事實上，落實資訊安全作為是全年無休的，嚴密資訊安全也無法保證百分之百的絕對安全，資安防禦是防患未然的工作（其中資安管理技術包括實體隔離、安裝防毒軟體、漏洞修補及相關的資安管制作為），但這些作為不保證電腦不會中病毒，或保證不被惡意程式入侵，因此唯有加強資安教育，讓電腦使用者確切瞭解資安惡意攻擊預防工作的重要性，以有效落實資訊安全防護作為。

資訊作戰發展概念

註❶：何心宇，〈全球資訊安全市場發展現況與趨勢〉《臺灣安全產業月報》，經濟部工業局（MIC），臺北，2006年5月。

數位化戰場係以「科技」為主導、「資訊」為中心之數位戰爭，因此「資電優勢」、「科技先導」是未來決定數位化戰爭的先決條件。隨著資訊技術和高科技工業的高度發展，使得戰場的指揮管制作為、武器接戰效能與情報資訊傳遞程序已迅速邁向數位化時代，高科技、數位化技術的影響，使傳統的作戰型態改變，尤其在指揮管制程序與情資傳遞之數位化戰場時代，指揮戰力整合系統為未來致勝關鍵，網路成為軍事作戰重要工具，而數位化戰爭內容包含指管通資情監偵（C^4ISR）系統❷。此系統是一複雜的人機系統，須整合情報、作戰、後勤、人事不同的軍事領域的龐大系統，牽涉的技術包括情報傳送、信息處理、情報融合、資料庫、圖像處理、人機介面、資訊安全以及決策支援等技術，主要目的是提供指揮官全面的戰場態勢，以消除戰場迷霧，進而遂行判斷狀況、制訂作戰方案、擬定作戰計畫以及下達決心。在資訊化的發展潮流下，在講求便利、快速、效率時，如何防止機密外洩、網路犯罪、遏止駭客入侵等資訊安全議題，已經提升為組織安全之重要政策。依據電腦緊急應變事件分析網路攻擊的發展趨勢，駭客已逐步形成了較為嚴密的組織，並在駭客聯盟內部有明確的分工，發展越來越複雜、破壞性更大的攻擊方法與多種混合型式的攻擊方式，網路攻擊型態也有從毫無目的的感染轉變成有目標性的攻擊。以下針對美國資訊戰發展內容概述加以介紹（如表一）。

美軍資訊戰之作戰模式（如表二），提出幾項當前美國在現今資訊戰所使用的戰法，可以讓我們瞭解到其學習的主要目標為何。

美軍運用全球資訊網絡（Global

表一　美國資訊戰發展

項　　目	內　　容
使用時機	依美軍Joint Pub 3-13（Joint Doctrine for Command and Control Warfare C2W）資訊戰交戰時機（Information Operation Engagement Timeline）指導❸，包含危機與衝突發生時機，資訊戰貫穿作戰全程。
相互配合	資訊戰負責機構與情報界的資源密切結合，以確保對電腦與資訊網路目標能有效的識別與處理。
攻擊模式	利用攻擊性資訊系統，如電腦病毒和高能微波武器等，摧毀敵方的電腦、通訊系統及資料庫。
科技防衛	發展智慧型軟體能量，以侵入敵方的資訊系統。

資料來源：作者自行整理。

註❷：宋家駒，〈資安漏洞危及全軍〉《國防譯粹》，第35卷第5期，2008年5月，頁4～9。

註❸：Defense Technical Information Center，〈JP 3-13 Joint Doctrine for Information Operations〉，http://www.dtic.mil/doctrine/joint_doctrine_information.htm，2006年2月。

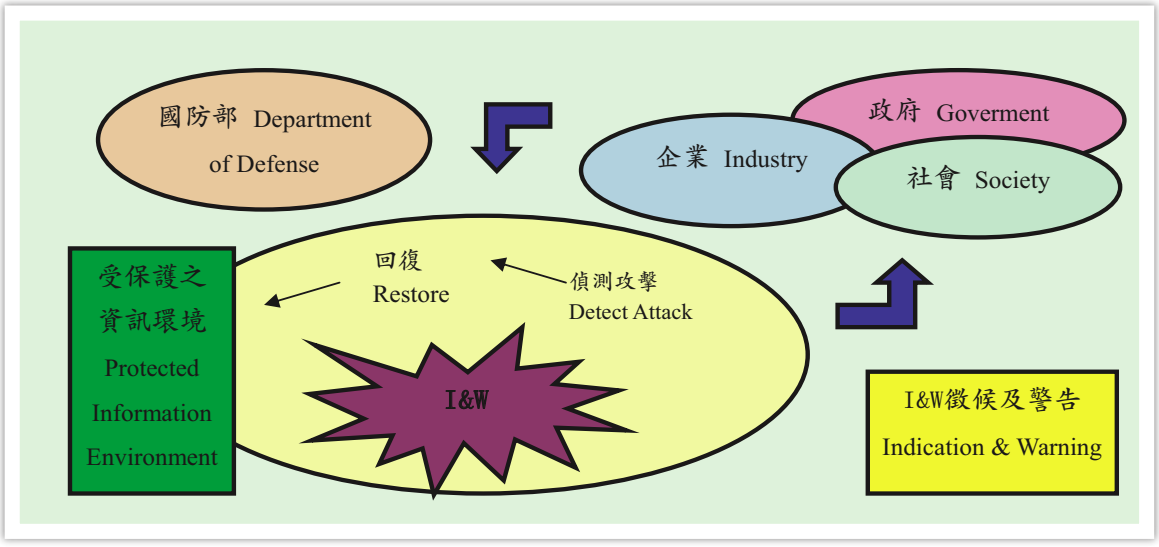
表二　美國資訊戰作戰模式分析

項　　目	內　　容
裝備優勢	以資訊戰武器裝備優勢，實施資訊威嚇。
洞察敵情	以先期偵察，先發制人手段，實施資訊壓制與攻擊。
形式壓制	以資訊壓制與攻擊實施資訊中斷。
攻擊摧毀	以電腦病毒摧毀敵方之資訊系統。
資訊封鎖	以資訊保密和資訊攻擊手段，實施資訊封鎖。
攻守兼併	以資訊攻擊和資訊防護，爭取資訊優勢。
主要目標	美國資訊作戰準則：美國在實行資安防衛部分主要以應用領域、內容服務及構成要素三個方面去動作。

資料來源：作者自行整理。

Information Grid, GIG）建立數位資訊與通訊戰鬥力（包括戰術、作戰與戰略層面的行動），支援「2010年聯戰願景」與「2020年聯戰願景」的全方位資訊作戰概念，保護及防禦資訊及資訊系統，以有效規劃、指導、執行與協調執行資訊作戰行動之資料，資訊作戰行動可能包含攻擊工具，如公共事務、民事、心理作戰及電腦網路攻擊，且均可能於潛在衝突開戰初期展開作業。此外，在攻擊性資訊作戰行動中，致命與非致命武器均是破壞敵方資訊流通及服務的可行手段，圖一為美軍資訊作戰攻擊、偵測與回復示意圖。

美國深切瞭解保護國土安全的重要性，為有效落實資訊安全管理機制效能，完全整合資訊作戰攻擊防禦能力，美國聯邦政府積極與國防部組織合作，以統整國家力量展開防禦性資訊作戰，若要判斷侵入事件係當地獨立事件或屬範圍



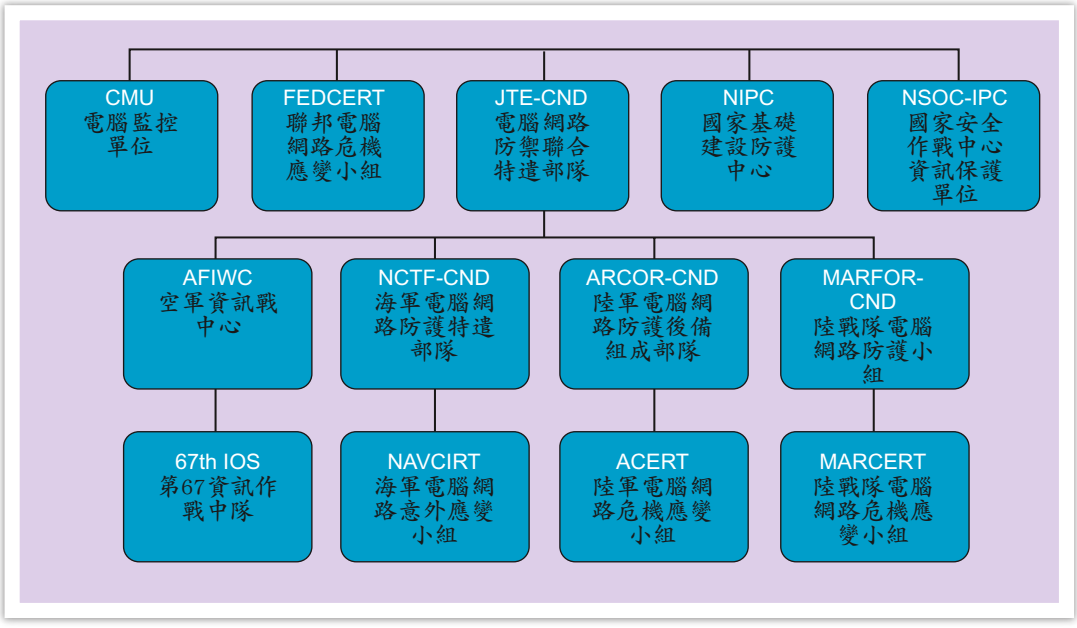
圖一　美軍資訊作戰攻擊、偵測與回復流程示意圖

資料來源：參考〈JP 3-13 Joint Doctrine for Information Operations〉自行整理繪製。

更廣泛的活動，因此建立全面事件通報系統（Incident Reporting System）。這套通報系統必須同時接收來自兩個來源的資料庫系統，分別是入侵偵測系統與防火牆記錄等自動化系統，另外則是人工事件報告（Manual Incident Reporting）。美國國防部並積極簡化事件通報與分析流程（包括通報格式、處理程序、資料傳輸與維護程序標準化，整合各層級的反應能力），建立了四層事件與弱點通報架構，重點針對全球、區域、軍種與當地等四個層級展開通報及分析工作。所有當地軍事網路作戰與安全中心，無論是部署在外或駐紮於基地、營地、哨所和站臺，均透過兩套功能性、指揮系統擇一或兩者併用向上通報，且通報時依系統而採取網路或作戰觀點。經過國防資訊系統局區域網路作戰與安全中心（Regional Network Operation and Security Center, RNOSC）的通報流程，通報作業係透過單一軍種或區域電腦網路危機應變小組執行，符合通報網路問題的傳統網路管理程式。反映出更傳統的作戰通報方式，圖二為美國國防部電腦緊急應變小組（Computer Emergency Response Team, DoD-CERT）組織架構。

電腦網路防禦事務革新

如何免於敵對國對國家的網路攻擊，已成為各國國防整備的要務，以美國為例，美國針對資訊戰積極進行組織變革，1993年將德州凱利空軍基地的聯合電子戰中心（Joint Electronic Warfare Center）更名為聯合指管作戰中心（Joint Command and Control Warfare Center），1994年美國國防大學設立資訊戰爭與戰略學院（School of Information Warfare and Strategy），1995年美國國防部組織了C⁴ISR的整合支援行動小組（CISA），負責研發校對一套標準的架構與定義，其



圖二　美國DoD電腦緊急應變小組（CERT）組織架構示意圖

資料來源：作者自行整理繪製。

架構發展程序提供指揮階層與政府部門作為執行指導方針❹，同年並成立陸海空軍種對應組織，陸軍的陸地資訊戰行動部門（Land Information Warfare Activity, LIWA）、海軍的艦隊資訊戰中心（Fleet Information Warfare Center, FIWC）以及空軍的空軍資訊戰中心（Air Force Information Warfare Center, AFIWC）。1996年底，美國國防科學研究委員會（Defense Science Board）公開了一份以資訊戰爭與防禦為主題研究報告，正式將電腦網路攻擊列為資訊作戰能力。1998年10月第3-13號聯合作戰聯戰準則（Joint Doctrine for Information Operations），深入探討1996～1997年電腦網路攻擊行動，並明白定義資訊作戰的內容與組成要素。

根據美國國防大學（U.S. National Defense University, NDU）國家戰略研究所（Institute for National Strategic Studies, INSS），漢斯派尼班傑克（Hans Binnendijk）與羅洛蒙特波洛（Ronald N. Montaperto）於1998年出版的《中共戰略趨勢》（Strategic Trends in China）一書中所指出的：中共內部對於未來軍事戰略構想，產生以軍事革命、局部戰爭、人民戰爭三者的爭議❺，且近年來積極開展以資訊戰為導向的軍事革命，其著眼在於中共、美國未來有可能發生衝突，在軍力處於相對劣勢情況下，唯有攻擊癱瘓美國軍方與民用的電腦系統方有獲勝可能。所以中共在1995年後，更進一步強調信息戰，致力於研究及推動軍事革命，並以「新軍事革命」一詞，普見於一般有關軍事革命之論述中。美國國防部於去年的「中國軍力報告」中指出，中共為了提升網路作戰能力，提出網電一體戰的作戰概念，加強民網與軍網的攻擊能力，積極發展非對稱戰法的非接觸作戰模式。

觀察美國軍事事務革新研究機構，包括科技提案推演（Technology Initiatives Game, TIG）、國防部淨評估辦公室（Office of Net Assessment）、科學運用國際公司（Science Applications International Corporation, SAIC）、海軍分析中心（Center for Naval Analyses）、陸軍戰爭學院（Army War College）、海軍戰爭學院（Naval War College）、空軍戰爭學院（Air War College）、海軍軍令部部長執行委員會暨2020年遠景（CNO's Executive Panel & Joint Vision 2020）等❻。歸納美國軍事事務革新相關的研究結果發現，美國軍事革命的海軍上將歐文斯（William A. Owens），定義為「系統中的新興系統」（The Emerging System of Systems），視為「系統集成」（System of Systems）之整合，與過去的軍事革命相比較，現在的這場軍事革命具有下列主要的特色❼，分析如表三：

註❹：尚景賢，〈C⁴ISR架構規範內含與運用〉《空軍軍官雙月刊》，第144期，2009年2月5日，頁55～71。

註❺：青年日報社論，〈強化網路資訊攻防戰力、防範駭客入侵竊密〉，2008年4月1日，版2。

註❻：高一中，〈全球資訊網絡戰場決策資訊管理模式〉《國防譯粹》，第35卷第5期，2008年5月，頁10～21。

註❼：里．阿米斯德（Leigh Armistead）著，國防部譯印，《資訊作戰以柔克剛的戰爭》，國防部史政編譯室，2008年8月。

表三　美國軍事事務革新特色分析

特色項目	內容
建立資訊作戰準則積極爭取資訊優勢	發展網狀化聯合作戰（Network Centric Warfare, NCW），建立全方位資訊整合作戰系統與整合型資訊高速公路，爭取優勢機動、精準接戰、全方位防護（Full-Dimensional Protection）與集中後勤的全面優勢（Full Spectrum Dominance, FSD）。
軍事事務革新為有史以來重要軍事革命	它具有歷史性、根本性、整體性、廣泛性（Comprehensive）、長期性、複雜性等，而且其過程必然是長期、深化的，且將持續一段歷史時期，影響所及將會持續到下一個世紀末。
複雜、深化的統合力是軍事革命精義	其整合的系統如次：情報監偵系統(ISR)、先進指揮、管制、通訊、電腦與資訊、情報（C^4I2），統稱為先進指揮、管制、通信、資訊、情報系統及精準導引彈藥(Precision Guided Munitions, PGM)。
資訊戰在軍事事務革新處於核心地位	主要特徵即是以資訊能力為主要作戰手段爭取資訊優勢（Dominant Maneuver），通過最終攻擊敵人的意識與信念，以迫使敵人放棄對抗意識，從而結束對抗，停止戰爭。
數位化部隊和數位化戰場為主要標誌	網路成為軍事作戰的重要工具，數位化部隊和數位化戰場不僅是資訊戰的兩大支柱，精準接戰（Precision Engagement）與集中後勤（Focused Logistics）更是此次軍事革命與過去軍事革命主要區別。
強化資訊作戰能力與活動	自2000年開始結合電腦網路攻擊與防禦成為「電腦網路作戰（Computer Network Operation, CNO）」的分析研究，為因應日趨嚴重的網路犯罪，加強資料加密、電腦入侵狀況演練、網路安全訓練、即時弱點分析評估控管與雙重帳號認證以加強網路安全防護。

資料來源：作者自行整理繪製。

美國認為資訊安全所造成的威脅，已出現在諸多層面，包括對個人、團體、企業、政府部門，乃至整個國家，幾乎已無所不在。而從軍事革命的特色觀之，未來軍事革命的不斷被深化，將對軍事領域的空間、時間、效能與觀念產生重大的變革影響，導致其發生一系列的變化。美國極為重視資訊作戰組織架構，為證實電腦網路攻擊對軍事行動及國家資訊基礎建設所可能造成的衝擊，參謀首長聯席會議下令展開名為「合格接收員」（Eligible Receiver）與「戰士之旗」（Warrior Flag）的演習活動。其中1997年6月演習（ER'97）展現敵對勢力有能力利用電腦網路攻擊與其他技術，滲透國家基礎建設及國防部網路，以削弱美國政府展開軍事行動的能力。1998年12月30日成立了「電腦網路防禦聯合特遣部隊」，做為具有作戰指揮權限的單一指揮部，負責協調和領導國防部電腦系統與網路保護工作。這支部隊組建後便成了司令部，可指示作戰司令部與各軍種單位依作戰需求改變設定，並設定資訊狀態以因應威脅。參謀首長聯席會議主席並於1999年3月發布「資訊狀態」（Information Operations Conditions, INFOCONs）狀況指令，標準化各類狀態報告及宣布程序❽。國防部以外的某些機構亦參與這場演習，包括聯邦調查局、司法部、運輸部、國務院、中情局、國家偵察辦公室與國家安全會議。美國為有效解

註❽：於下頁。

決網路攻擊事件，「電腦網路防禦聯合特遣部隊」自1999年10月1日起改編制為太空司令部的直屬指揮部，太空司令部正式接手整個國防部的電腦網路防禦任務。為整合任務需求，太空司令部並於2001年4月1日將該部隊更名為「電腦網路作戰聯合特遣部隊」，並於2003年1月10日轉由戰略司令部管轄。

資訊確保縱深防禦

據美國國防部統計，平均每天可偵測到3百萬次企圖滲透電腦網路（Compromise）的案例，而根據國際研究中共網路戰專家調查，中共網路駭客攻擊最常用的武器就是「僵屍網路病毒」（Bot Net），當遭受攻擊被植入惡意程式後，成為駭客的傀儡電腦，而這種電腦惡意程式攻擊可潛伏於電腦中數月或數年後發動攻擊❾。有鑑於中共網路戰威脅與三戰發展，美國在軍事事務革新下組建了「戰略駭客部隊」、「網路媒體戰部隊」及「網路戰聯隊」，並建立資訊確保弱點警戒（Information Assurance Vulnerability Alert, IAVA）流程與弱點評估機制，使資訊保護管理者具備更多決策工具以評估資訊威脅。資訊確保弱點警戒流程係全面性的資訊分發流程可通知相關機構的系統弱點警戒狀況及對策，這套流程已發展成極為制式的流程，必須由不同司令部向通報機構確認收到弱點警報，此系統並要求收到警報的單位後，必須做出具體回應已確認其已採取適當對策。美軍發展資訊保護紅色小組主動展開網路弱點評估（Vulnerability Assessment），模擬電腦駭客造成的威脅。依據美國防務新聞報導，美國司令部正積極改進訓練計畫，讓32萬空軍人員接受網路前線（Frontline）的訓練，並且計畫申請簡化網路作戰授權流程（Command Authorization Procedure）以有效提升網路作戰效率。

美國各軍種仍保留資訊戰中心，並在重大演習時才會運用這些中心的能力，紅色小組則不僅確認系統設定，同時測試偵測和回應電腦網路攻擊的程序以及系統使用者與管理員資安弱點分析評估能力，以上措施都是屬於美國政府整體防禦戰略，稱之為縱深防禦（Defense in-Depth, DiD）的一部分。而針對網路武器，美國所使用的技術包括攻擊（病毒、特洛依木馬、阻斷式服務攻擊、蠕蟲、邏輯炸彈等惡意程式）與防禦式（加密器、通訊弱點掃瞄器、防火牆與監視技術）工具❿。有效運用先進資訊技術可促進網路安全，資訊確保技術安全措施（如表四），協助提升網路安全的資訊確保技術計有：

一、公開金鑰基礎建設（Public Key Infrastructure）、電子憑證。

二、檔案（File）與儲存區塊虛擬化

註❽：Major George L. McMullin II, Information Operations Conditions （INFOCONs） In The Real World, USSTRATCOM, 1999, http://www.certconf.org/presentations/1999/infoconsCERT99

註❾：邱銘彰，〈網站掛馬研究-Web惡意程式寫法與偵測技術大公開〉《資安人雜誌》，2009年2月，頁80～87。

註❿：李育慈，〈掌控電子頻譜（Dominatingthe Electronic Spectrum）〉《國防譯粹》，第35卷第5期，2008年5月，頁40～45。

（Storage Block Virtualization）技術[11]。

三、虛擬私有網路（Virtual Private Network, VPN）、防火牆（Firewall）。

四、入侵偵測系統（Intrusion Detection System）、病毒掃瞄（Virus Scanner）。

五、整合邊界安全的防火牆/VPN結合防毒、入侵防禦系統（Intrusion Prevention System, IPS）功能。

六、跨越異質平臺認證（Authentication）、管理（Administration）與授權（Authorization）。

七、安全應用程式（Security Application Program）與複雜攻擊規範產生器。

八、異地備援（Off-Site）、軟硬體加密（Encryption）與金鑰加密系統互通標準技術（Key Management Information Standards）[12]。

九、整合硬體式身分認證技術如Tokens、智慧卡與生物辨識（Biometrics）。

十、蜜罐（Honeypot）、蜜網（Honeynet Worm Trap）病毒蠕蟲誘捕系統等。

攻擊性資訊作戰可能是聯合部隊指揮官任務或作戰行動的主力或支援力量，但其必須支援整體軍事目標，並具備某種可

表四　資訊確保技術安全措施

技術安全措施	可用性	私密性	完整性	認證性	存證性
防火牆、密碼、數位簽證				◎	◎
個人識別碼、生物、特徵辨識				◎	◎
使用安全密碼（Password）		◎	◎	◎	
入侵偵測系統（IDS）		◎	◎	◎	◎
病毒偵測（Antivirus Mechanism）	◎	◎	◎		
弱點檢查機制（Vulnerability Check）	◎	◎	◎	◎	
系統監控工具（Monitoring Tool）	◎		◎		
傳輸安全(Trans. Safety）	◎	◎	◎		
電磁防護(EM Protection, EMP）	◎	◎			
實體防禦（Physical Protection）		◎	◎		
多重路徑（Multi-Path）	◎		◎		
資料備援備份（Backup）	◎		◎		◎

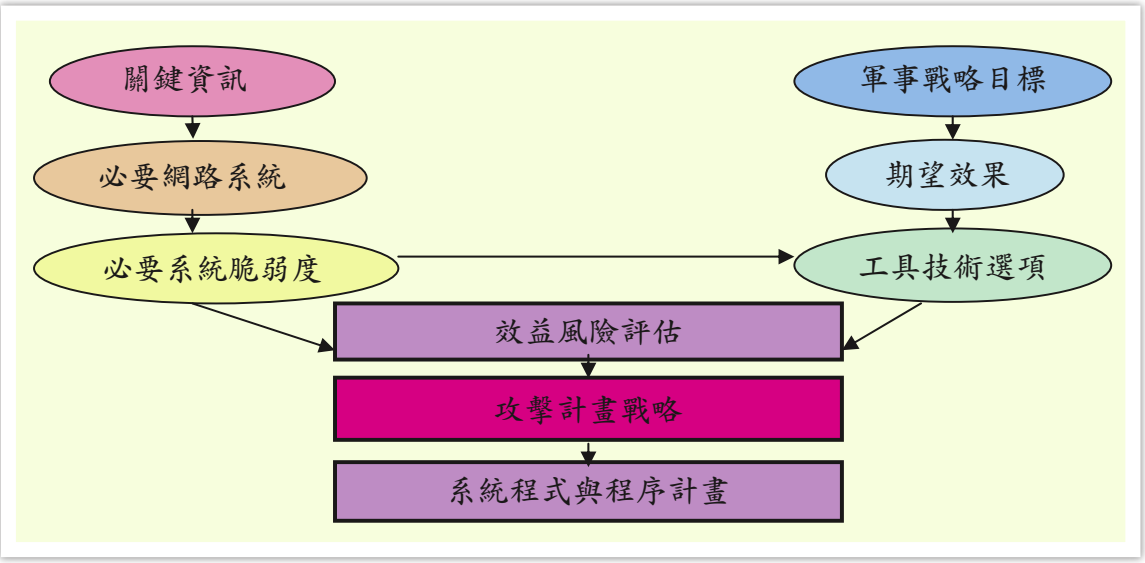
資料來源：作者自行整理繪製　◎表示代表具備此特性

註[11]：吳嘉龍，〈網路儲存虛擬化技術研究與資訊安全應用探討〉《空軍軍官雙月刊》，第144期，2009年2月5日，頁40～54。

註[12]：王宏仁，〈儲存廠商開始推動加密系統互通〉《ITHome電腦報焦點新聞》，第388期，2009年3月，頁14。

行的效能評量辦法。找出此類評量辦法往往是問題的癥結所在，原因就在於資訊作戰的某些面向無法透過觀察簡單量化。資訊作戰工作無法在短時間內或以危機模式完成。因此，在為攻擊性資訊作戰做準備時，前置時間也必須很長，以確保敵方決策人士依己方想要的方式回應，展開任何攻擊性資訊作戰行動前，必須有完善的戰場情報準備。值得一提的是，為求勝利成功，攻擊性資訊作戰必須符合美國整體安全目標，並遵守已確立的接戰準則，此外也必須在特定作戰行動的整個跨部會流程中，與所有非國防部的機構完全結合。在區域環境中，作戰指揮官與美國外交部門人員的關係，對於擬定及執行攻擊性資訊作戰戰略最為重要。因此，前置時間及跨部會作業等需求，在某種程度上並不利於成功運用資訊作戰戰略形塑環境。然而有跡象顯示，隨著資訊作戰在美國政府內部更受肯定，眾人將更能接受這些要素。如圖三為攻擊性資訊作戰戰略示意圖。

美國定義電腦網路作戰包含攻擊與破壞敵人電腦網路、保護美方軍事資訊系統以及入侵敵人電腦系統進行情蒐等能力，其中針對網路弱點評估利用專門的掃瞄軟體主動確認全球資訊網資訊系統的安裝情形與設定，檢查資訊系統是否達到相關防護要求。運用攻擊性資訊作戰也有一般性原則可供遵循，在規劃軍事作戰行動時必須加以考量。美國資訊戰指揮架構中的戰略司令部為戰略部隊之統一作戰司令部，下轄太空全球打擊、情報監視偵察、網路作戰、整合飛彈防禦及打擊大規模毀滅性武器等聯合作戰指揮部，負責管制軍事太空作戰（Space Warfare）、資訊戰（IW）、戰略預警（Strategic Warning）、情報評估（Intelligence Evaluation）及全球戰略作戰規劃（Global Strategic Planning）。美軍網路作戰由網路作戰聯合指揮部及太空全球打擊聯合資訊作戰指揮部（Joint Information Operation Warfare Command,



圖三　攻擊性資訊作戰戰略示意圖

資料來源：作者自行整理繪製。

JIOWC）負責，美國空軍並於2007年9月在路易斯安納州Barksdale空軍基地成立網路指揮部（Cyber Command）編組，有效整合網域與航太作戰能力，遂行全球網路作戰任務。

美軍新成立的「網路戰聯合作戰指揮部」（Joint Functional Component Command for Network Warfare, JFCCNW）肩負美軍資訊戰電腦網路攻擊的任務，該指揮部成員包括各軍種、中央情報局、國安局、聯邦調查局以及蒙國軍文職代表所組成。而縱深防禦整合人員、作戰行動與技術的能力，已獲致堅強、有效、多層次和多方位的防護效果⓭。「縱深防禦」戰略旨在確保系統的防護成效不致因其他構連系統的弱點而降低；並針對與整體環境連結的所有系統，建立必須達到的最低防護標準。這項戰略構想係以接連數層的防禦網來因應穿透或瓦解某項障礙的敵人，使其馬上又遭遇另一個縱深防禦障礙，因而增加偵測的可能性，其中一項防禦機制得以阻擋攻擊。要確實發揮作用，縱深防禦必須能對抗各種攻擊方法；另須運用各種對應的補強防禦機制，俾互補各項障礙的優缺點。針對共軍網路作戰威脅，美國除了一方面建立網路作戰指揮部（Network Warfare Command），另一方面則積極發展網狀化作戰能力，以美國海軍為例說明，美國在查理號（Bonhomme Richard）進行2006年「三叉戟戰士」（Trident Warrior）演習中，聯合作戰中心測試系統針對武力網系統進行海上驗證操演，掌握最新聯合作戰情資包括戰況體認與火力統計，並合作管理頻寬支援高度機動遍布世界的兵力，並發揮網狀化聯合作戰資訊分享的最大利益⓮。

新興資安技術應用

美國國際戰略研究中心（Center for Strategic and International Studies, CSIS）在對第44屆總統歐巴馬提出外交、情報、軍隊、經濟（Diplomatic、Information、Military、Economic, DIME）的網際空間安全建言⓯，本報告由兩位國會議員與智庫提出報告，呼籲歐巴馬成立專職機構以強化網際國土安全。美國也曾評估過認為美國為最容易遭到電腦攻擊的國家，故發動電腦網路攻擊必然也會使美國自身深受其害。根據定義，電腦網路攻擊行動可擾亂、阻絕、降低，摧毀電腦與電腦網路中的資訊，或電腦與網路本身。多數人以為在全球資訊網或網際網路上才能展開電腦網路攻擊，事實上，藉由動態手段實體破壞電腦系統或網路，亦屬於電腦網路攻擊，值得注意的是，警政署資訊室2008年10月提供國際協助發現電腦駭客透過臺灣跳板主機針對重要國家軍事基地持續發出網路攻擊封包，為了確保國土資訊安全，落實端點防護與網路存取控制，實為刻不容緩的重要議題⓰。事實上，假如

註⓭：青年日報社論，〈落實資安保密、防範敵人滲透〉《青年日報》，2009年2月5日，版2。

註⓮：李永悌，〈至關重要的網路連線（Crucial Connectivity）〉《國防譯粹》，第35卷第5期，2008年5月，頁40～45。

註⓯：資安人編輯部，〈給歐巴馬的資安建言打贏一場無形戰爭〉《資安人雜誌》，2009年2月，頁38～41。

註⓰：於下頁。

某臺電腦是未經連結區域或網際網路的獨立式系統，則必須破壞實體，或實際將惡意電腦程式碼植入這臺電腦的軟體程式中⓱。這種形式的電腦網路攻擊可能不再由軍方管轄，而是交由歷來執行這類行動的其他組織負責，以法律限制極可能阻礙美軍運用電腦網路攻擊。現代作戰以戰場情資共享實現作戰行動同步是決定戰爭勝利的關鍵，若以數據網路方向探討，中共信息化武器的特點是武器平臺間實現橫向連網，做到戰場情資共享，以提供武器平臺的作戰效能，表五為中共C^4ISR技術系統發展方向。

電腦網路攻擊的影響難以估計，以至於俄羅斯試圖引用國際法規禁止發動此類攻擊，並已在聯合國提案禁止各國運用資訊作戰。除了法律限制外，發動電腦網路攻擊亦須面臨技術挑戰。為確保攻擊性資訊戰任務遂行，網路攻擊的目標係處理特定任務的單一電腦或電腦系統⓲。發動電腦網路攻擊所需的情報，可能較執行轟炸任務所需者更多。攻擊性資訊戰攻擊目標決定取決於在根據情報將所羅列的目標刪減至剩下一套系統或單一設備後，攻擊的一方必須確定所瞄準的電腦事實上就是正確目標，而非網際網路服務伺服器。電腦網路攻擊的特色在於擾亂、阻斷、降低與摧毀，而這類任務的另一個特徵是實際侵入電腦，我們通常將此行為稱為電腦網路利用（Computer Network Exploitation, CNE），此技術為攻擊性資訊戰行動中最困難的部分。一旦成功侵入電腦，任何人都能造成系統混亂。不過通過安全系統顯然並非易事。雖然法律僅允許特定組織可遂行電腦網路攻擊行動，但電腦網路利用行為卻不一定適用這項規定，此舉導致情況變得更為混亂⓳。根據美國網際國土安全定義，資訊安全威脅包括天災、電信事業自由化、竊聽監錄及網路病毒與駭客等因素，因此可透過技術、法令、教育訓練及道德等層面建立應有的資訊安全觀念外，個人電腦使用也應注重資安防護，以避免國防機密資料外洩、敵人網路入侵與破壞，確實維護資訊安全。

ISO27001資訊安全管理認證，是國際標準化組織（International Organization for Standardization, ISO）對於資訊安全管理的認證規範，透過PDCA模式（P：計畫、D：執行、C：檢查、A：改善），建立一套完善作業流程，其目前不僅是國際資訊安全管理的準則，更是各國政府和企業團體在資訊安全能力上的最佳證明。資訊安全稽核將可確保單位資訊安全管理意向與策略獲得落實外，透過資安稽核，讓資訊安全持續自我提升，降低組織因資訊風險形成對工作的影響，並使內部同仁具備長期自我維護安全的能力，進而創造優質的資訊安全環境。美國國土安全局

註⓰：黃燕棻，〈國立大學淪為駭客打手，計中無法管〉《ITHome電腦報焦點新聞》，第373期，2008年11月，頁17。

註⓱：吳芳姿，〈電子駭客（Electronic Attacks）〉《國防譯粹》，第35卷第1期，2008年1月，頁64～69。

註⓲：同註❻。

註⓳：軍事新聞網，〈國軍強化資安認知，提升防護效能〉，2009年1月20日，http://clc.mnd.gov.tw/ Publish.aspx?cnid=1284&p=30018&Level=2

表五　中共C⁴ISR技術系統發展方向

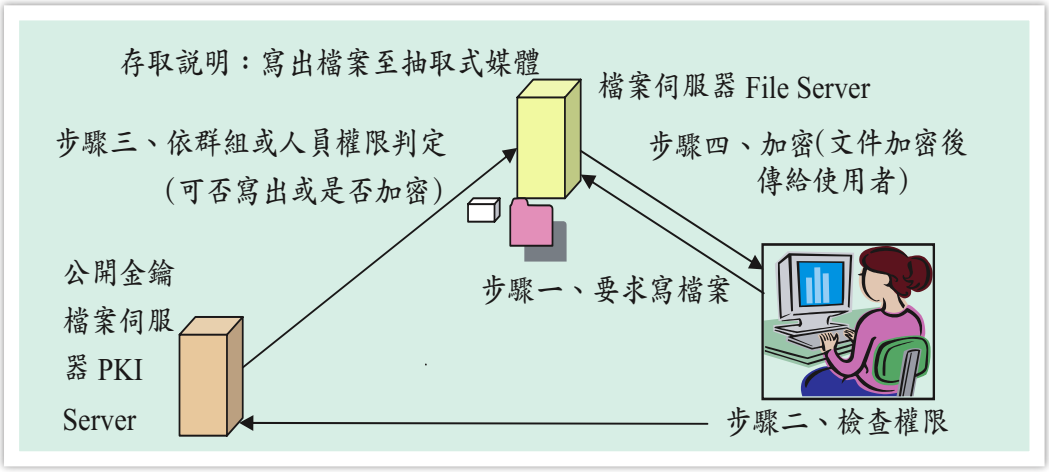
C⁴ISR技術	中共C⁴ISR方向發展說明
偵察監視技術	高解析度照相偵察衛星、新一代天基紅外彈道導彈預警系統、相控陣預警機、空中對地縱深攻擊監視指揮飛機、無人偵察機和夜視裝備將大量採用，感測器成為戰鬥力倍增器，指揮員具有全球態勢感知能力。
平臺一體化資訊戰系統	藉由通資平臺技術的精進，「載臺作戰」方式逐漸演進成「網狀化作戰」方式，大幅強化作戰效能。通過採用多功能通用標準電子模組和具有多頻譜感測器即時資料融合能力的電腦，將多種資訊戰功能集於一身，真正實現雷達告警、導彈發射和攻擊告警、資訊支援、資訊干擾及規避、協同一體化，而且與平臺上其他資訊設備綜合為一體。
數位指揮控制技術	研究和試驗探測、分析和攻擊數位式指揮控制網路技術；人工智慧綜合資訊戰系統；精確的電子戰態勢認知、目標指示和防空壓制技術；多譜告警與干擾技術、紅外成像對抗技術及載體內（外）感測器融合技術等。
電腦病毒技術進行網路攻擊	未來病毒武器將注重智慧可控性，出現所謂的智慧病毒。同時將發展衛星輻射、電腦病毒砲等遠距無線病毒注入方式，透過惡意程式掌握電腦控制權，例如進行精心設計網路攻擊，藉由感染後惡意程式碼的高隱匿特性，進行滅屍行動犯罪（Operation Bot Roast）行為、惡意程式與電腦瀏覽器攻擊，以及對網路封包進行監視，並複製給攻擊者，讓攻擊者由獲得的封包資訊中過濾出想找的資訊，如帳號及密碼。
電磁脈衝武器	可以干擾電子裝備或使電子零件的電壓或電流大幅增加而燒燬，可用於對雷達、通訊及電腦等電子系統的攻擊網路。
戰略彈道導彈	戰略彈道導彈將改進導向管理技術，對彈道的末段或中段也進行制導提高戰略導彈的命中精度；逐步實現導彈固體化、小型化和自動化，進一步提高戰略導彈機動作戰能力和快速反應能力；採用多發射方式和多彈頭導彈；完善大型戰略彈道導彈，發展小型、機動、攜帶單彈頭的戰略彈道導彈，研製超音速的隱身戰略巡航導彈，發展防禦定向能和動能武器新技術，提高戰略導彈突防能力。
高能粒子武器	以高能粒子束照射目標，將能量傳遞到目標內部，使電子甚至機械零件損壞。
軍用衛星與微小型衛星	軍用衛星系統作為航太武器系統的重要組成部分，在未來爭奪制資訊權的鬥爭中將發揮越來越大的作用。除偵察衛星、預警衛星、導航衛星、通信衛星外，部署殺手衛星、攻擊衛星和衛士衛星，未來並規劃構小衛星星座是軍用衛星發展方向。
載人航天器	軍用載人航天器以機動的太空梭、空天飛機類航天器的方向發展，指揮地面部隊和海上艦艇作戰，摧毀敵方衛星和飛船，重點研製反衛星和反洲際彈道導彈等非核能空間武器，包括動能武器和定向能武器、電磁軌道砲、攔截彈等動能武器，及高能雷射光束、粒子束、高功率微波等定向能武器。
天軍與太空站	天軍是獨立於陸、海、空之外的新軍種，成員構成為一個多兵種的合成軍隊，除指揮機關和航太院校，還有許多兵種部隊，大體包括太空艦隊、地基部隊、航太和空天飛機部隊、火箭部隊、C⁴I部隊等。它的主要任務包括太空作戰，支援空中、地面、海上作戰和開發宇宙空間等，太空站則作為未來天基武器系統平臺。

資料來源：作者自行整理繪製。

積極研究資訊安全技術以建立網路安全機制，透過IP Mac Binding和ARP Spoofing技術，鎖定可管控的電腦IP不被盜用，美國將無國界電腦駭客對金融體系發動持續性網路攻擊納為反恐演練重點。我國鑒於資安事件頻傳，屢遭有組織駭客入侵威脅，因此已由行政院主導成立「國家資通安全會報」，透過教育訓練、研討檢測，強化政府資安防護能力與執行成效。圖四為資料存取控制示意圖，步驟一～步驟四說明如下：步驟一為寫出檔案至抽取式媒體，步驟二為檢查使用者權限，步驟三依群組或人員權限判定是否可以寫出或加密，步驟四為文件加密程序。

基本上，資訊安全的類型有三：其一是實體安全；其二是軟體安全，其三是資料安全。相信每一位使用者都曾遭受或因病毒挾帶、或因實體損害、或因駭客入侵、或因網路詐騙等等因素，所造成的資訊安全傷害。尤其是，國軍不同於政府其他部門和民間企業，在遂行戰訓本務，打造堅實國防戰力的過程中，必然擁有許多具有高度機敏性的重要資料，若資訊安全出現漏洞，等於敞開國家安全大門，國土資訊安全必定受到威脅，危機可隨時出現在每一部電腦中，這些即時性威脅與危害，足以說明資訊安全是沒有假期的。尤其是國軍官兵，更必須嚴肅體認中共「網軍」早已完成部署，並且日夜進襲的現實敵情，人人要做好資訊安全防護措施，共同維護國軍資訊網路整體的安全[20]，資訊安全需要每一位軍中同仁從基本動作做起，自我養成時時對抗危害威脅，內建防毒、防駭與反網釣（Anti-Phishing）的習慣，例如嚴守不要隨意點選連結與透露個人資訊的原則，才可以在高度風險的網路連結中，避免置身於隨時都可能遭到獵捕誘殺的危境[21]。

我國未來因應作為與結論



圖四　資料存取控制示意圖

資料來源：作者自行整理繪製。

註[20]：軍事新聞網，〈陳肇敏：強化國軍資安防護能力，確保資電優勢〉，2008年12月18日，http://clc.mnd.gov.tw/Publish.aspx

註[21]：於下頁。

持續精進資安整備是掌握現代作戰致勝的必要條件，創造更安全的資訊環境才能制敵機先。有效維護資訊安全、建立國軍官兵及民眾全民國防共識，期能進一步提升國軍資電作戰戰力，有效防禦網軍入侵威脅。依據美國國防部研究指出，中共持續對臺灣進行軍事威脅正是中共勸降與嚇阻的戰略企圖㉒。為有效防範有組織的網軍入侵危及資訊通信安全，驗證國防資訊防護動員機制運作流程及整體成效，國防部早於95年7月依「全民防衛動員準備法」及「民力徵用實施辦法」規定，在行政院指導下，執行臺灣有史以來首次資訊防護民力動員，並配合「漢光演習」實兵驗證，進行資訊安全防護研討與演練㉓。持續強化資訊安全作為是國防部一貫政策，厚植國軍資訊防護戰力，方能確保指管通連，達成聯合作戰目標與任務。事實上，資訊安全與作戰任務同等重要，以國軍資安教育而言，為普及資安認知教育，重點在於將資安課程納入基礎、進修、深造教育課程施教，以強化資安防護教育，讓國軍官兵能在享受資訊科技便利的同時，亦能以完備的資安防護，降低資安事件引發的風險與損害。國軍各級持續強化各項資訊安全防護工作，方能有效杜絕資安事件肇生，建構優質資訊社會，強化資安防護㉔。

國防部近年來積極提升資安防護，建立良好電腦使用習慣，除安裝防毒軟體、修補漏洞，依國防部的資安設定小幫手自我檢查電腦安全設定，做好資安預防工作外，並讓所有資安長具備執行資安督導的知識與稽核能力，做好單位內部的管控措施，以建立資安防護共識。資訊安全工作是一項防患於未然的風險管理過程，若能成為國軍每一位官兵的習慣後，資安工作便能達到「滴水不漏」境界。國防部為掌握最新資安規定與訊息，於98年1月辦理「97年度高級軍官團資安講習」，邀請專家學者們，透過近期發生的資安事件案例解說及部頒資安規定，說明最新資安威脅趨勢，並提出相關因應建議，以提升國軍對資安事件處理的技術與反應能力，強化資安防護能量及對資安規定遵循之認知與責任感。國軍各級在國防部指導下，除了在資訊基礎建設更新與資安防護設備提升等作業上，已做了大幅度的改善外，對於人員資安防護概念教育的強化，也做了相當的努力。總而言之，「資訊安全始於人性」，資安防護應由自身做起，提高保密警覺，建立資安保密共識，不貪圖方便、不貪小便宜，恪遵保密規定，才能有效強化資訊安全的維護，確保國家整體戰力的穩固。

註㉑：軍事新聞網，〈落實資安管控，國防部訂頒具體作法〉，2009年1月20日，http://clc.mnd.gov.tw/Publish.aspx

註㉒：胡元傑，〈美國2007年中共軍力報告補遺〉（The 2007 Report on The Chinese Military – Top 10 List of Missing Topics）《國防譯粹》，第35卷第1期，2008年1月，頁4～14。

註㉓：軍事新聞網，〈防網軍入侵，國防部首度執行資訊防護動員〉，2006年7月14日，http://clc.mnd.gov.tw/Publish.aspx

註㉔：軍事新聞網，〈資訊安全威脅無所不在，人人應自我警覺〉，2009年2月4日，http://clc.mnd.gov.tw/Publish.aspx