航空技術學院學報 第九卷 第一期 第 85－90 頁（民國九十九年）
Journal of Air Force Institute of Technology, Vol. 9, No. 1, pp. 85-90, 2010

資訊科技戰場優勢發展分析與先進資訊安全技術研究

Battlefield Superiority Technologies Development and Advanced Computer Information Security Researches

吳嘉龍

Chia-Long Wu

空軍航空技術學院一般學科部航空通電系副教授

Department of Aeronotic Communication Electronics, Air Force Institute of Technology

摘要

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，通資電優勢競爭下，由於電腦在系統中的地位和作用日益增強，指揮自動化又加上電腦，演變成 C4I 系統。以戰備任務為核心，從基層戰力訓練做起，逐步累積訓練成果，才能強化國防武力，精實國軍整體戰力，進而建構政府兩岸談判協商的戰略優勢，使國軍成為區域和平的穩定力量。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了指管通資情監偵（C4ISR）系統，C4ISR 是指揮、管制、通信、資訊、情報及監視與偵察英文的縮寫。通信系統把各指揮中心、預警系統、作戰部隊以及情報部門等有機聯繫起來，形成一個整體。科技高度發展，對於軍事作戰思維產生了革命性影響，其所產生影響包括有：資訊優勢及較強之戰場狀況認知、提供作戰行動更大之運籌空間、利用 C4ISR 系統進行精準攻擊以及提升空中作戰效益等作用。

關鍵字：革命性戰爭、通資電優勢、戰略評估、戰場優勢、先進軍事科技。

Abstract

Accompany with high-technology era, advanced information technology and systems of C4ISR under development for gaining the battle superiority which can satisfy the requirement of the homeland security. In the C4ISR domain, information technology and systems of C4ISR will need the capability to establish crucial links between its first responder military units and civilian first responders to emergency events. Furthermore, information technology and systems would have to be properly adapted to meet the different mission and challenges of homeland security. Revolution of military force put great influence on information superiority including precision attack and airborne defense systems.

Key Words： Revolutionary battle, dominant awareness, strategic environment assessment, battle effectiveness analysis, advanced military technology.

一、前言

電腦網路攻擊行動可擾亂、阻絕、降低、或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，國軍對於資訊安全的發展不遺餘力，從集控式防毒系統、系統修補更新、檔案加解密軟體、電腦輸出入埠管制、AD 網域建置、CERT 監控機制、移動式儲存媒體管制等作法，顯見國軍資訊整體戰力已有顯著的提昇。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，確維資訊安全。值得注意的事，美國國防部積極簡化資安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、並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[1]。

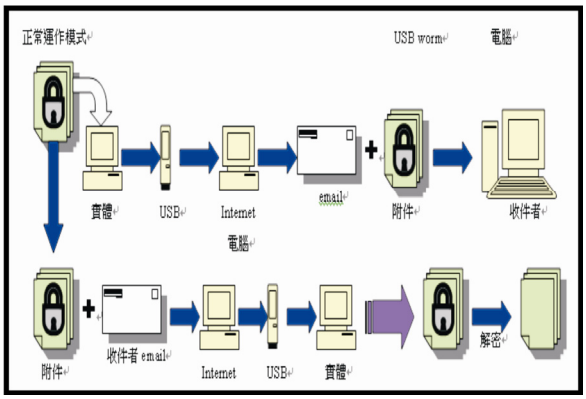
二、資電優勢資安技術與國土安全

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。國軍在資訊系統發展積極投入，許多傳統業務都已仰賴資訊系統的運作，例如電子公文資訊系統、人事資訊系統、財務資訊系統、聯合後勤資訊系統等。由於國軍將逐漸實施募兵制，國軍人力勢必縮減，而隨著通信、資訊、電子環境的逐漸複雜化與多元化，國軍對於資訊系統只會更加依賴。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更廣泛的活動，因此建立了全面事件通報系統）[2]。

美國資訊作戰強調符合國家整體完全目標，並遵守接戰準則，並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。惟近來國軍仍發生多起資訊洩密事件，不僅影響軍譽，也對國軍戰力造成了嚴重的影響，歸納其發生原因如表一[3]：

表一　資安洩密發生肇因分析

項目	資安事件發生肇因分析
1	資訊技術未能更新，無法應付新興威脅，過於著重資訊科技運用，忽略其他資訊外洩管道
2	人員教育訓練成效不彰，缺乏危機意識，缺乏專業資訊人力、技術，良好的科技必須配合適當的控管，應用在適當的位置，才能發揮最大的效益
3	安全管理政策為落實且未按權責區分，包括負責項目如安全管理政策制訂、風險評估、系統設計、系統建置、系統管理
4	缺乏良好風險管理與監控機制，因此人員的教育訓練、實務經驗、專業知識與安全認知都是不可或缺的條件，尤其重要的是必須挑選出信賴人員負責各層級工作，才能確保安全



圖一　資訊存取控制實體隔離示意圖

存取控制與身份管理為資訊系統的第一道防線，其目的在阻礙未經授權人士獲得存取儲存管理工具與設備的權限。實體隔離使

用加密方式，將資料加密後才拿到外網傳送，在技術上已經遭駭客破解，先透過 USB Worm 建立起傳輸管道，透過 Hook API 的方式，搶先攔截加密前的明文資料，使加密方法形同虛設，資訊存取控制實體隔離示意如圖一、。與安全防禦有關的整體策略、管理目標、作業準則、執行細節相關作業程序，涵蓋範圍十分廣泛，包括認證、授權、金鑰管理、安全評估、偵測、預警、應變、復原、重建等程序，為了能有效防禦新的安全威脅，必須隨時檢視相關安全政策與作業程序，適時予以修正。以網路防護層級為例，人員的部分代表單位應具備專業的管理人員；科技的部分則代表需要採用的技術；而作業程序的部分則代表有關網路層級的整體策略、作業程序與管理辦法。資訊外洩防制不能只靠資訊科技或產品，而是需要建構一套完整的系統管理架構。從縱深防禦策略的原則來看，良好的資訊技術可以有效降低資訊外洩的機率，但並無法完全的消除，還是需要配合完善的政策規劃及訓練有素人員，並在彼此之間取得平衡[4]。

三、資訊確保與縱深防禦技術

縱深防禦的觀念可以應用在各種資訊系統及網路，其基本原則是對機密資料所存放的系統或網路等各個層級中，都採取多層式的防護，當某一層級的防護機制被突穿時，其他層級的防護機制就會取而代之提供備援防護功能。縱深防禦策略中多層式防護的概念[3]，由於資訊戰與網狀化作戰對於資訊系統與網路的依賴程度極高，相對的安全需求亦極高，因此為了確保資訊戰與網狀化作戰運作順遂，美國國防部與國安局共同制訂了一套資訊確保技術架構；縱深防禦策略為資訊確保主要核心策略，針對各個資訊系統與網路採取層層防護機制，以全方位防護機制，確保核心資訊的安全[5]。

事實上，美軍資訊確保架構的主要核心就是縱深防禦策略，美軍具體的發展策略是從資訊基礎建設開始，建立所謂的全球資訊網路架構，嘗試將網路上的資源全面連結、互通，建立一個強大具感測能力、協同合作軍事資訊網絡，而在其基礎之上發展資訊戰及網狀化作戰等未來型態作戰，以確保資訊優勢。經過國防資訊系統局區域網路作戰與安全中心的通報流程，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。資訊系統與網路提供防護、偵測、應變與復原等能力，其核心要素如表二[6]：

表二　資訊系統與網路五個核心要素分析

項目	五個核心要素分析
1	有效性：確保資訊服務品質，預防因為外部攻擊或系統錯誤，造成資料無法被存取使用
2	鑑別性：對於資源存取者要求身份識別，並且針對不同機敏等級的資料必須進行權限管控，以防止未經授權存取資訊
3	機密性：當資料遭到未經授權存取或非法竊取時，透過加密進行保護，防止資料內容外洩
4	完整性：當資料在傳輸或使用的過程中，防止資料被未經授權的竄改、偽冒或刪除，以確保資料與原始來源相同
5	不可否認性：資訊傳送者當資料在交換的過程中，可以透過數位簽章的方式，避免因偽冒，否認傳送動作發生

圖二　微軟定義縱深防禦示意圖

資料來源：微軟官網
http://www.microsoft.com/

縱深防禦不只涵蓋資料、應用程式、主機、內部網路與各種邊界，也包括實體安全、政策和資安意識，微軟定義縱深防禦示意圖如圖二。美軍運用全球資訊網絡（Global 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階展開作業，應用縱深防禦策略來探討資料外洩防制時，有幾個值得注意重要原則如表三。

表三　縱深防禦策略分析

項目	縱深防禦策略分析
1	應同時針對內部、外部，各個關鍵點部署足夠的防禦機制，以防範可能的資料外洩風險
2	網路層級依賴較多的資訊防禦技術，而人員層級則仰賴嚴謹的管理辦法與作業程序，採取多層次的防禦機制，面對不同特性威脅，建構整體防禦機制
3	主機、伺服器、應用系統、內部網路、外部網路、作業人員應當分別採取防護措施確保各環節安全，消除各種資安疑慮
4	應結合適當的資訊技術與專業人員，從整體的安全架構進行分析與評估，隨時調整、應變，以適應各種新興的資安威脅

縱深防禦應重視防禦關鍵位置，資料管理人員、主機 I/O 連接埠、應用系統管理介面、網路的通訊埠等，通常是資料傳輸的必經之路，也是常見的資料外洩管道，因此應視為關鍵點加強防禦。為了確保資訊的安全性，在網路上傳送資訊時，均會將資訊先行利用密碼技術進行加密後再透過網路傳送，此時若遭到有心人士截取，由於截取到的只是一堆亂碼，並無法得知所傳送的資訊是什麼，因此能夠避免有心人士解讀我們傳送的祕密資訊，進而確保資訊的安全性。縱深防禦應採取多層式防禦，再好的防禦技術都有可能具有弱點或被破解的時候，每個層級所面臨的威脅也不同。縱深防禦應防護資訊作業環境，除了部署多重防禦機制之外，與資訊作業有關的各個環節。縱深防禦應重視完整的安全機制，良好的安全機制，必須透過完善的整體防禦策略與作業管理程序[7]。從美軍發展軍事網格（Military Grid）策略來看，看似分散的實體資訊架構，實際上是朝向虛擬整合的目標來發展。因為過於鬆散的資訊架構環境，容易造成不易管理的缺點，也相對增加了資訊外洩的機率。透過相同的資訊架構與管理機制，才能有效整合運用所有的資源，並提昇速度、分享資訊、協同合作，相對才能有效監控並防制資訊外洩情事發生[4]。「縱深防禦」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，使其中一項防禦機制得以阻擋攻擊。值得一提的是，縱深防禦須能對抗各種攻擊方法與結合各種對應的補強防禦機制，以互補各項障礙優缺點[6]。

表四　資訊確保技術安全措施

技術安全措施	可用性	機密性	完整性
入侵偵測系統		○	○
病毒偵測機制	○	○	○
弱點檢查機制	○	○	○
系統監控工具	○		○

○　：表示具有此特性

縱深防禦尤其重視密碼學技術與防護理論，在現代密碼學的領域中，其所定義的資訊安全乃指計算時間的安全性，亦即只要有心人士無法在機密資訊的有效期限內完成解密（computation infeasible，CI），就稱為安全。隨著電腦運算技術的快速成長，加上透過網路分散式的平行運算技術也日益成熟[3]，這些傳統的密碼演算法的安全性都已慢慢地受到質疑，況且使用傳統的密碼學

演算法（Cryptographic algorithm）所開發出來的系統都是將機密資訊加密（Data encryption）成亂碼後再行傳送，但正由於密文為亂碼的特性，容易引起非法者的注意而加以攻擊，進而想盡各種辦法加以破解[6]。祕密分享技術（Secrecy sharing）雖能夠提供安全的保護機制，但是大部分技術所產生的分享影像在視覺上近似雜訊，且分享的影像均會產生倍數地擴增，因此若能使分享影像成為具有意義的影像，並且分享影像不至於成倍數地擴大，影像藏密技術（Steganography data hiding）將能夠有效地保護分享影像安全，並將降低資訊儲存空間[9]。

四、結論與未來因應建議

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，然而，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台，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，因此做好資訊安全的工作就是做好戰場管理，這是資訊安全防禦應有的認知。美軍認為，擁有“資訊優勢”是資訊化戰場克敵制勝的主導因素，儘管美軍的資訊技術研究、開發和運用均處於世界前列，但仍不惜拆鉅資為保持資訊作戰優勢做認真的準備，以創造單向透明的戰場環境。而國軍因應人員精減的趨勢，資訊作業環境必須逐漸朝向集中架構發展，以降低人員與技術成本[8]。首要工作就是降低資訊作業環境的複雜度，提高資訊透明度與資源分享的程度，並且逐漸朝向共通的資訊作業環境發展，進行虛擬整合，以達到集中管控，防制資訊外洩的目標。國軍資訊及資安系統整體規劃構想以「強化資安防護能量、提昇通報應變成效、建立聯防動員機制、推廣資安認知教育」為目標，建立安全互通、即時便利之整合系統，唯有遵守「主動監偵、積極防護」原則，建立「早期預警、應變制變」通資安全防護能力，才能有效確保國軍資電優勢與穩固國家整體戰力。資訊戰中的網路戰指的是以現代傳播媒體為作戰的平台，以訊息為作戰武器，侵入敵人的資訊基礎設施進行破壞，造成社會的恐慌及不安，或散布偽造消息以迷惑敵人的指揮中心，造成誤導而產生軍事上或國家政策上致命的失誤，以達到不戰而屈人之兵目的[10]。

參考文獻

[1] 資安之眼（2009），「RSA 資安會議：DLP、NAC 與身份認證為今年焦點」，http://www.itis.tw/node/1731。

[2] R. Layland（2007）, “Data Leak Prevention: Coming Soon to a Business Near You”, Business Communications Review, May 2007, pp.44-49.

[3] 國防部通信電子資訊參謀次長室（2007），「國軍資訊安全政策」，2007 年 7 月，頁 2-3。

[4] P. Rubel, C. Payne, M. Ihde, S.Harp, and M. Atighetchi（2006）, “Generating Policies for Defense in Depth”, IAnewsletter Vol.9 No.3.

[5] 趨勢科技（2008），「善用資料外洩防禦技術保護企業重要資產」, Trend Micro Inc., Jan 2008, http://tw.trendmicro.com/tw/products/.

[6] 資安之眼（2008），「基測個資外洩？教育部：已展開調查」，2008年6月13日，http://www.itis.tw/node/1867。

[7] 楊策淳（2009），導入 WIMAX 救護系統 提昇防災效能，青年日報專論，2009 年 12 月 16 日。

[8] 里・阿米斯德（Leigh Armistead）編（2008），資訊作戰以柔克剛的戰爭，國防部譯印，國防部史政編譯室，2008 年 8 月。

[9] 左豪官、婁德權、吳嘉龍、王開平（2008），看不見的祕密通道技術，資通安全專論 T97009，財團法人國家實驗研究院科技政策研究與資訊中心，2008 年 09 月 30 日。

[10]高一中（2008），全球資訊網絡戰場決策資訊管理模式，國防譯粹，第 35 卷第期，2008 年 5 月，頁 10-21。