我國資訊安全機制之研究
—以海軍為例

邱意雯、葉道明、孫培真

提　　要：

近幾年來，政府、軍事、及企業等單位的入侵事件時有耳聞，雖部分被披露在報章雜誌，但隱藏在背後的損失恐怕更是無法估計。國軍為防衛國家的第一道防線，對於資訊安全的防護更是不容忽視，本文將就資訊安全的規範、事件等相關文獻進行探討，並就我國海軍資訊安全機制之現況，進行分析及提供精進方向，冀能提供各單位於建置資訊安全管理後續策進參考，以創造低風險、更優質的資訊作業環境。

關鍵詞：資訊安全、ISMS、資安事件

壹、前言

1990年教育部電算中心成立台灣學術網路(TANet)〔註一〕，如今電腦網路普及各大學校園，甚或各個地方，運用這項新科技處理資訊，成為現代人日常生活的一部分。根據資策會FIND的最新調查指出，2009年台灣家戶電腦普及率已達85.7%，並推估擁有電腦家戶數為6,629千戶，擁有電腦家戶平均擁有2.4台電腦〔註二〕，另截至2009年12月底止，我國有線寬頻網路用戶數已達4,960千戶〔註三〕，顯見資訊網路具有超越時空限制的特性與優點，已成為現代不可或缺的傳輸媒體。

然而在資訊網路應用普及下，同時也形成今日資安事件的手法千變萬化且層出不窮。經我國行政院主計處電子處理資資中心就肇生資安事件的統計分析中，30人以上的人力規模的電腦用戶，曾遭遇資安事件者有54.77%，在遭遇者的資安事件，以電腦病毒攻擊53.20%為最，次為被植入後門程式10.68%，再次為遭阻斷式攻擊(DDoS) 2.96%〔註四〕。另根據美國電腦安全局及聯邦調查局(CSI/FBI)2009年對於電腦犯罪及安全所做的調查統計報告中〔註五、註六〕，追溯2009年肇生資安事件主要種類的百分比

註一：李呈奇，〈大學推動校園e化之探討〉，《國立中山大學人力資源管理研究所碩士學位論文》，2001年。

註二：吳佩玲，〈2009年我國家庭寬頻現況與需求調查--家戶與個人連網指標〉，資策會FIND網站http://www.find.org.tw/find/home.aspx?page=many&id=249。

註三：陳均輔、李雅萍，〈2009年12月底止台灣上網人口〉，資策會FIND網站http://www.find.org.tw/find/home.aspx?page=many&id=251。

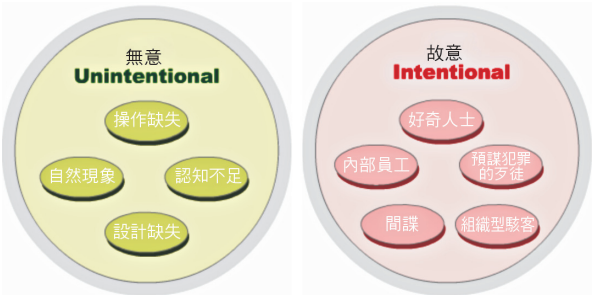
註四：行政院主計處電子處理資料中心，〈2009電腦應用概況報告〉，中華民國統計資訊網http://www.stat.gov.tw/ct.asp?xItem=25562&CtNode=5210&mp=4。

註五：Robert Richardson,”2009 CSI Computer Crime and Security Survey Executive Summary”,Computer Security Journal,December 2009.

，發現發生率的前4類分別為「病毒64.3%」、「移動式電腦的失竊及欺騙42.2%」、「內部不當網路存取29.7%」、「阻斷式攻擊29.2%」。

正所謂預防勝於治療，為確保我國資訊運用與網路建設在具有安全防護的機制中發展，預防機密資料外洩、重要資訊系統遭受破壞以及網路犯罪等資安事件，行政院於1999年頒訂所屬各機關資訊安全管理要點〔註七〕，並陸續頒訂許多規範，以推動我國資通安全整體防護。配合各項國家政策及規定，各政府機關也紛紛據以建立資通安全機制，並遵行政院2004年「各政府機關(構)落實資安事件危機處理具體執行方案」，依機關責任分級要求通過資安範圍之第三者(BSi7799-2/CNS17800）資安管理之認證，使得標準化的資訊安全管理機制由政府部門帶頭做起。

擔任保衛國家的國軍也在邁入「資訊化」及「電子化」後面對嚴峻的挑戰，因為稍有不慎即可能發生軍機外洩等情事，而對國家造成莫大的傷害。為解決資訊保密安全的困境，國軍相關機構不斷研擬各項資安精進作法，以降低事件發生的風險，在本研究將就以海軍為例，就資訊安全機制規劃及建置之現況進行闡述，並依其現況分析優勢、弱點、機會和威脅，同時提供精進建議，期能盡早準備以防患未然。



圖一　危害資訊安全的因素

資料來源：電子化政府網路文官學，〈B01-001 資安管理-資訊主管篇〉，本文張貼電子化政府網路文官學院之資訊安全教學課程簡報http://elearning.nat.gov.tw。

貳、有關資訊安全

一、資訊安全的定義

資訊安全一詞，已有30餘年的歷史。美國聯邦政府的安全準則，將資訊安全定義為「保護資料，使之免於遭受故意或無意的洩露、移轉、變更、破壞」〔註八〕。所謂無意的，是指如因停電、地震、失火等非人為的因素，使得資訊外洩或損害；所謂故意的，是指破壞的源頭是源於人為的設計〔註九〕。其「無意」及「故意」的因素(如圖一)：

所以資訊安全就是要達到資訊的機密性(Confidentiality)、可用性(Availability)與完整性(Integrity)；另外也包含如鑑別性、可歸責性、不可否認性及可靠性等特性(CAN 17799)〔註十〕，而有效的安全措施必須賴於新科技對於運用資訊的新方法，並且要未雨綢繆事先預防(Eugene C.

註六：Robert Richardson,”2008 CSI/FBI CSI Computer Crime and Security Survey”,Computer Security Journal,2009.
註七：行政院，〈行政院所屬各機關資訊安全管理要點〉，http://cissnet.edu.tw/purpose02.aspx。
註八：湯耀中，《從戰爭的觀點論資訊安全》(台北市：全華書局，西元2003年），頁1-2。
註九：電子化政府網路文官學，〈B01-001 資安管理-資訊主管篇〉，本文張貼電子化政府網路文官學院之資訊安全教學課程簡報http://elearning.nat.gov.tw。
註十：International Organization for Standardization,”ISO/IEC 27001 Information technology–Security techniques –Information security management systems – Requirements,first edition,ISO,2005。

表一　組織資訊安全的弱點與威脅

	項目	說明
組織內部弱點項目	資訊資產	組織內部資料庫、資料檔等相關文件或電子檔。
	文件	對於組織內部合約文件、指導文件、使用手冊、操作手冊、公司資料等書面文件。
	軟體資產	內部業務運作用之應用軟體、自行設計軟體、系統軟體等與智慧財產權有關之項目。
	實體資產	內部業務運作所需之電腦、伺服器、磁片、磁帶、電源供應器、空調等硬體設備資產。
	人員	組織內部人員、外部顧客及協力合約商等人員。
	服務	企業服務之應用系統、通訊服務等服務性質之項目。
	形象及宣傳	組織本身的形象及有心人士的宣傳等。
外在威脅項目	駭客攻擊	企業內部網路或應用系統，被駭客透過各種方式進行攻擊。
	資訊竊取	組織文件或資料被內部員工竊取。
	間諜	外在敵對單位派任間諜進行組織滲透竊取資訊。
	病毒或木馬	因中毒或木馬感染，導致企業內部電腦自動傳送或外洩重要電子資料。
	故意或非故意刪除	組織內部人員或外部人員以故意或非故意方式，刪除、毀損組織資料。
	察覺	對於各項應用系統或作業流程遭受破解而不自知。
	電力中斷	組織運作所需之能源供應中斷。

資料來源：何瀛州，〈區域級學術網路組織之資訊安全風險評估－以宜蘭縣學術網路為例〉，《佛光大學資訊學系碩士論文》，2007年。

Schneider Gregory W. Therkalsen，1990），以確保單位的永續經營。

二、資訊安全的風險

「安全」和「風險」是息息相關的，一個組織面臨的弱點與威脅構成了風險的基礎〔註十一〕，弱點主要是針對內部組織本身的人員、資訊資產、實體資產等項目進行評估，因為內部的弱點會造成外在的威脅；威脅的項目主要是組織外部駭客攻擊、工業間諜、病毒或木馬等項目，因為外在的威脅通常都是由內部的弱點所引起。組織資訊安全的弱點與威脅整理(如表一)：

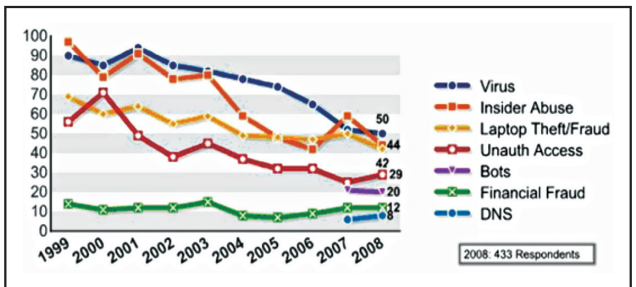
三、資訊安全事件

事件是一個威脅起源對於一個組織造成傷害的方法〔註十二〕。資訊安全事件是指系統、服務或網路發生一個已識別的狀態，其指示可能的資訊安全政策違例或保護措施失效，或是可能與安全相關而先前未知的狀況等(ISO/IEC TR 18044：2004)。

美國電腦安全局及聯邦調查局(CSI/FBI)對於電腦犯罪及安全所做的調查統計報告中〔註五〕，在追溯到1990年至2008年肇

註十一：何瀛州，〈區域級學術網路組織之資訊安全風險評估－以宜蘭縣學術網路為例〉，《佛光大學資訊學系碩士論文》，2007年。

註十二：Eric Maiwald, Fundamentals of Network Security, (U.S.A.：McGraw-Hill Technology Education,2004）。



圖二　肇生資安事件主要種類的百分比

資料來源：Robert Richardson,”2008 CSI/FBI CSI Computer Crime and Security Survey”,Computer Security Journal,2009.

生資安事件主要種類的百分比(如圖二及表二所示)，可以發現風險最高發生率的前4類分別為「病毒」、「內不當網路存取」、「移動式電腦的失竊及欺騙」、「未授權存取」，在2007年「內部不當網路存取」一度高於位於首位的「病毒」，另外可以發現在「未授權資訊存取」的部分在2008年較2007年成長。

在教育部提升校園資訊安全服務計畫服務團將安全訓練、認證與研究機構SANS公佈的「2008十大網路安全威脅」報告歸納之後區分為「網站威脅」、「行動威脅」、「病毒威脅」、「內部威脅」、「社交工程威脅」四大類〔註十三〕，在此參考行政院訂頒之「各機關處理資通安全事件危機通報緊急應變作業注意事項」〔註十四〕內，及國內外資安事件調查報告整理區分資安事件如下：

(一)人為事件

又依來源可分為「內部危安」、「外部入侵」，就「網路安全」方面資安事件包含：竊聽、竄改、阻斷服務；就「系統安全」方面事件包含電腦病毒、網路蠕蟲、後門程式、木馬、入侵、弱點威脅；就「管理安全」方面事件包含不當存取、帳號盜用、未授權登入、社交工程、失竊、資訊資產毀壞。

(二)天然災害

如遇颱風、水災、地震等天然災害。

(三)突發事件

火災、爆炸、核子事故、重大建築災害、硬體設備電子損壞、突發斷電等不可抗力之意外事件均屬之。

四、資訊管理系統

依據2006年7月20日國家資通安全會報第十五次工作小組會議，為明確各政府機關(構)資訊安全責任等級分級作業流程，特訂定「各政府機關(構)資訊安全責任等級分級作業研訂施行計畫」，透過有效的資訊安全管理，來防止資訊受到潛在威脅的破壞，進而全面提升國家資通安全防護水準，以管理手段考量主客觀之形勢，明確律定資安等級之規範，將單位依資安等級區分為A級(重要核心)、B級(核心)、C級(重要)、D級(一般)〔註十五〕，並規範各類資安系統等級應執行之工作事項(如表三)：

其中對於資訊安全管理系統(Information Security Management System，簡稱ISMS)的推動列入管理的工作事項，ISMS為

註十三：教育部，〈網路安全威脅分析〉，教育部提升校園資訊安全服務計畫服務網站 http://cissnet.edu.tw/knowledge_11.aspx。

註十四：行政院國家資通安全會報，〈各機關處理資通安全事件危機通報緊急應變作業注意事項〉，2002年8月5日行政院國家資通安全會報(2002)資安發字第0615號函發布，http://www.tcfd.gov.tw/02mid/07trouble/96/96-02-01.doc。

註十五：行政院國家資通安全會報，〈政府機關(構)資訊安全責任等級分級作業實施計畫〉，2005年7月22日資安發字第0940100615號函頒，http://www.hjes.tpc.edu.tw/mediafile/445/fdownload/589/64/2009-9-14-23-19-55-64-nf1.pdf。

表二　肇生資安事件主要種類的百分比

	2004	2005	2006	2007	2008
阻斷服務(Denial of service)	39%	32%	25%	25%	21%
移動式電腦失竊(Laptop theft)	49%	48%	47%	50%	42%
電信詐騙(Telecom fraud)	10%	10%	8%	5%	5%
未授權存取(Unauthorized access)	37%	32%	32%	25%	29%
病毒(Virus)	78%	74%	65%	52%	50%
財務詐騙(Financial fraud)	8%	7%	9%	12%	12%
內部不當網路存取(Insider abuse)	59%	48%	42%	59%	44%
系統入侵/滲透(System penetration)	17%	14%	15%	13%	13%
蓄意破壞(Sabotage)	5%	2%	3%	4%	2%
竊取或遺失隱私資料(Theft/loss of proprietary info)	10%	9%	9%	8%	9%
-來自行動裝置(from mobile devices)					4%
-來自所有其他來源(from all other sources)					5%
濫用無線網路資源(Abuse of wireless network)	15%	16%	14%	17%	14%
網站的損壞(Web site defacement)	7%	5%	6%	10%	6%
隨意瀏覽網站(Misuse of Web application)	10%	5%	6%	9%	11%
機器人程式(Bots)				21	20
DNS攻擊(DNS attacks)				6%	8%
濫用即時傳訊(Instant messaging abuse)				25%	21%
密碼偵測(Password sniffing)				10%	9%
竊取或遺失顧客資料(Theft/loss of customer data)				17%	17%
-來自行動裝置(from mobile devices)					8%
-來自所有其他的來源(from all other sources)					8%

資料來源：Robert Richardson,”2008 CSI/FBI CSI Computer Crime and Security Survey”,Computer Security Journal,2009.

國際現行五大管理系統之一，乃整體管理系統的一部分，以營運風險方案為基礎，以人員、資料、設備、存取、系統安全、環境安全作為資訊安全的範圍，用以建立、實施、操作、監督、審查、維持及改進組織的資訊安全(ISO/IEC 27001:2005)。

ISMS依「規劃-執行-檢查-行動」(Plan-DO-Check-Act，簡稱PDCA)過程模式來進行ISMS的矯正，以確保ISMS之有效性，其模式(如圖三)，模式簡要說明：

(一)規劃(建立ISMS)

建立安全政策、目標、標的、過程及相關程序以管理風險及改進資訊安全，使結果與組織整體政策與目標相一致。

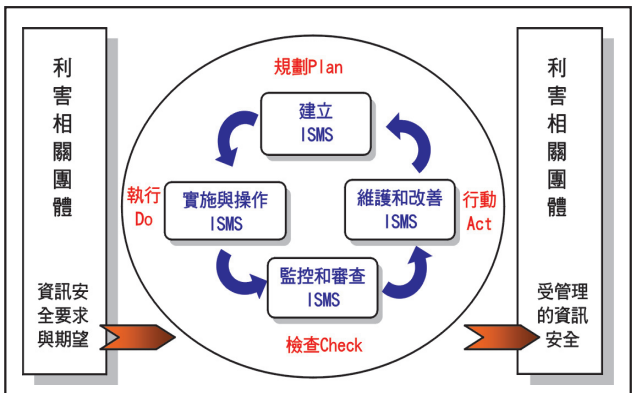
(二)執行(實施與操作ISMS)

實施與操作ISMS政策、控制措施、過程

表三　各類資安系統等級應執行之工作事項

作業／內容／等級	防禦機制強　度	防護縱深	ISMS推動作業	稽核方式	資安教育訓練(主官、主管、技術、一般)	專業證照
A級	強度等級4	NSOC/SOC、IDS、防火牆防毒	2007年通過第三者認證	每年至少執行2次內稽	(4, 6, 18, 4小時)/每年	96年資安專業鑑定證照2張
B級	強度等級3	SOC(OP)IDS、防火牆防毒	2008年通過第三者認證	每年至少執行1次內稽	(4, 6, 18, 4小時)/每年	96年資安專業鑑定證照1張
C級	強度等級2	IDS,防火牆防毒	各單位自行成立推動小組規劃作業	自我檢視	(2, 6, 12, 4小時)/每年	資安專業訓練
D級	強度等級1	防火牆防毒	推動ISMS觀念宣導	自我檢視	(1, 4, 8, 2小時)/每年	資安專業訓練

資料來源：行政院國家資通安全會報，〈政府機關(構)資訊安全責任等級分級作業實施計畫〉，2005年7月22日資安發字第0940100615號函頒，http://www.hjes.tpc.edu.tw/mediafile/445/fdownload/589/64/2009-9-14-23-19-55-64-nf1.pdf。



圖三　PDCA模式應用到ISMS過程

資料來源：唐雨漁，〈ISMS政策探討〉，http://sab.tycg.gov.tw/files/download/455d7741.ppt，2006年。

與程序。

(三)檢查(監視及審查ISMS)

依據ISMS政策、目標與實際經驗，評鑑及在適用時測量過程績效，並將結果回報給管理階層審查。

(四)行動(維持和改善ISMS)

依據ISMS內部稽核與管理階層審查結果或其他相關資訊採取矯正與預防措施，以達成ISMS的持續改進〔註七〕、〔註十〕、〔註十六〕。

在ISMS國際標準未制定前，目前我國經濟部標準檢驗局業依ISO/IEC 27001:2005做為我國受理ISMS驗證之標準〔註十七〕。ISO 27001認證是國際資訊安全管理系統標準，它不是一種技術，而是一種管理制度，包含了11個管理領域、39個控制目標、133個控制要點〔註十一〕、〔註十七〕。11個管理領域簡要說明如下：

1. 安全政策：為資訊安全提供管理方向

註十六：唐雨漁，〈ISMS政策探討〉，http://sab.tycg.gov.tw/files/download/455d7741.ppt，2006年。

註十七：經濟部標準檢驗局，〈ISO 27001：2005資訊安全管理系統要求〉，經濟部標準檢驗局之最新消息http://www.bsmi.gov.tw/wSite/public/Data/f1228114692438.ppt，2008年。

及支持，以符合企業的需求及相關法律、法規上的規範。

2. 資訊安全組織：建立一個管理架構，用於單位內部資訊安全的管理和控制，以及執行現有的資訊安全規定。

3. 資產管理：確保對組織各項資產的安全進行有效保護。

4. 人力資源安全：明訂所有人員在安全方面的職責和角色。

5. 實體和環境安全：對單位作業場所及人員提出簡單明確的安全要求。

6. 通訊與作業管理：盡可能完善公司內外的溝通連繫，以利於資訊安全管理系統的順利運行。

7. 存取控制：管理對資訊的存取行為。

8. 資訊系統取得、開發和維護：確保公司IT專案和相關的支援活動已實施安全控制，必要時進行資料管制和加密。

9. 資訊安全事故管理：確保在某種程度上傳達與資訊系統有關的資訊安全事件與弱點，始能採取即時的矯正行動。確保實施一致與有效的方法管理資訊安全事故。

10. 營運持續管理：發展和維護企業營運持續計畫，保護關鍵的業務活動免受重大災難或中斷的影響。

11. 遵循性：符合資訊安全法或規定的相關要求。

參、海軍資訊安全機制規劃及建置之現況

隨著現代資訊化的來臨，面對如何防範電腦網路犯罪與危機，並維護資通系統安全成為政府施政最迫切的課題，因此行政院於2001年1月通過第1期「建立我國通資訊基礎建設安全機制計畫」(2001-2004年)，並於行政院下成立「國家資通安全會報」(National Information & Communication Security Taskforce，簡稱NICI)，從此開啟政府有計畫的推動我國資通安全建設之路〔註十八〕。

我國先後經過兩期總計8年推動「建立我國通資訊基礎建設安全機制計畫」(2001-2008年)〔註十九〕、〔註二十〕。在第一期(2001-2004年)進行設立國家資通安全組織、國家資通安全應變中心、推動政府機關設立「資通安全處理小組」以「確保我國擁有安全、可信賴的資訊通訊環境」為願景；第二期(2005-2008年)規劃「提升通報應變時效」、「健全資安防護能力」、「深化資安認知及教育」、「促進國際合作」四大政策目標，訂立政府機關資訊安全長(Chief Information Security Officer；CISO)責任制度、資通安全責任等級分級作業等，依單位重要性區分A、B、C及D四個等級，並持續辦理資通安全攻防演練、通報演

註十八：行政院國家資通安全會報，〈國家資通訊安全發展方案(民國98年至101年）〉，http://www.hdais.gov.tw/13/0104726A00_ATTCH1.pdf，2009年1月。

註十九：行政院國家資通安全會報，〈建立我國通資訊基礎建設安全機制計畫(94年至97年)〉，http://www.libcc.nsysu.edu.tw/file.php/16/100210.pdf，本計畫於2007年2月15日行政院核定修正。

註二十：林翠娥，〈國軍人員資訊安全素養與資訊違規認知關係之研究〉，樹德科技大學/資訊管理研究所未出版之碩士學位論文，2006年。

練、及推廣資通安全管理制度、資通安全教育宣導、稽核服務等，積極建設資通安全基礎建設工作；另於2004年7月完成「國家資通安全會報」組織調整。在完成階段性任務後，並依「國家資通訊安全發展(National Information and Communications Initiative plan, NICI)方案」(2009-2011年)進一步以建置優質網路化社會為目標。

行政院國家資通安全會報組織架構中，國防即列屬「標準規範組」、「稽核服務組」、「法規偵防組」及「通報應變組」編制中，並積極推行國軍各項資安防護建設，為籌建「早期預警、應變制變」的資安防護能力，採取「主動監偵、積極防護」手段，構建資安防護機制，並頒布多項資安管控措施，研擬資安獎懲規範，推動資安認證機制，貫徹網路實體隔離，普及資安認知教育，規定專人專責管理，加強資安管控稽核，建立多層防護、及時管控的資安防護體系，以達到「進不來、出不去、看不懂、帶不走」的資安防護目標。

一、海軍資安防護機制

(一)電腦緊急應變處理

海軍司令部遵循國防部頒訂資安政策指導辦理，建立「海軍電腦緊急應變處理實施計畫」，由政策計畫、通報處理、研發諮詢及各單位電腦緊急應變(Computer Emergency Response Team, CERT)等分組結合海軍電腦緊急應變(NCERT)，以針對資訊系統、網路等事件，加強危安通報，提供早期預警，有效減低災損、快速復原，確保國軍通資網路暨系統安全，有效支援作戰任務。

(二)資安管控中心

海軍於2007年建立「海軍資安管控中心」，整合各類資安防護系統，及配合國軍資安監控系統建置營區監控點，並結合防火牆、入侵防禦系統等防護功能，以達成資安事件蒐整、回報、處置之統一標準，增強資安管控系統防護能力〔註二一〕。

(三)資安防護組織

在單位資安管理部分，依行政院及國防部政策指導，建立各級「一級輔導一級」資安防護組織，以逐級執行資安管控稽核及督(輔)導作業〔註二二〕，並定期召開資安長會議及資安工作檢討會，以消弭資安事件肇生，資安體系編組分述如下：

1.資安長體系：由各級副主官擔任，負責單督導各項資安工作推動。

2.資安幕僚主管體系：由各通資(業管)部門正(副)主管擔任，貫徹執行資安各項工作。

3.資安官體系：各單位設置資安官，負責資安管控維護、稽核與通報責任。

(四)資安防護技術

面對當前的資安威脅，並配合國防部資安發展規劃，現已運用單一閘口機制以達實體隔離目標、部署目錄集中控管權限、發展新一代電子憑證系統、使用加密式軟體及隨身碟、USB偵測軟體監控、無線網路監控、資安小幫手、資訊資產系統管理、檔案安全

註二一：國防部青年日報，軍事新聞網2007/7/3之軍事新聞，http://news.gpwb.gov.tw/newsgpwb_2009/news.php?css=3&nid=19199&rtype=2。

註二二：中華民國國防部，國防部網站最新消息2008/11/3之軍事新聞， http://www.mnd.gov.tw/Publish.aspx?cnid=65&p=29363。

表四　資訊安全防護相關規範及計畫

年份	名稱
2001	網路作業安全
2001	個人電腦資訊安全防護作業
2004	實體隔離管制要點
2005	資安管控機制精進作法
2005	資訊網路標準作業程序
2005	個人電腦輸出入裝置使用管制
2006	廢舊及不適用物資處理作業
2006	資訊設備及資訊儲存媒體管制
2006	網路實體隔離及資訊設備庫存管理
2006	資訊設備及媒體管理作業
2006	網址管理作業
2006	筆記型電腦管理作業
2007	資訊安全政策
2007	網站管理作業
2007	光碟機使用管制作法
2007	電腦輸出入裝置暨移動式資訊儲存媒體
2007	資安管控機制精進作法
2007	無線網路監控系統
2007	因公出國人員資訊安全管理
2008	資安違規人員講習
2008	資訊(安)設備籌補管制
2008	加密式隨身碟使用管理
2008	新一代個人電腦系統測評估
2008	資訊安全獎懲基準
2008	移動式媒體管控軟體管理
2009	修訂民網軍事資料稽核
2009	資安管控中心標準
2009	修訂資訊備配賦
2009	通資安全數位學習課程
2009	修訂電腦緊急應變處理
2009	各級單位連接網際網路單一閘口
2010	資訊資產管控
2010	資訊教育訓練
2010	資安合格簽證
2010	修訂資安管控稽核「一級輔導一級」具體作法
2010	智慧卡部署

資料來源：林翠娥，〈國軍人員資訊安全素養與資訊違規認知關係之研究〉，樹德科技大學/資訊管理研究所未出版之碩士學位論文，2006年。

管理系統等，未來更推行數位文件保護及強化電子憑證結合各式系統應用等，以加強「實體安全」、「人員安全」、「系統安全」、「網路安全」、「電腦安全」、「資料安全」的資安需求〔註二三〕、〔註二四〕。

二、資訊安全規範

海軍司令部遵循國防部頒訂資安防護規範及計畫辦理，以要求各單位嚴禁便宜行事、公務家辦，力圖達到法無盲點，確保官兵落實資安防護有法可依。茲將近年來訂頒資訊安全防護相關規範綜整(如表四)：

三、資訊安全認知教育與宣導活動

為強化官兵「資安防護如同作戰整備」的觀念，使官兵能深入瞭解資訊洩密的嚴重性，並將資安課程納入海軍之基礎、進修、深造教育課程施教，加強官兵的在職訓練和資安宣導，同時強化資安保密和相關法律教育，建立資安須知卡、資安管控光碟等宣導資料，於人員新進時實施資安教育及鑑測，以強化資安認知。

資安一般教育訓練即以定期舉辦各類講習辦理，如資安巡迴講習、資安官合格簽證、資安違規人員講習、因公出國人員資訊安全講習等，並建立通資安全數位學習平台，以提供官兵隨時可上網自我學習。

資安專業教育訓練則以內部施訓或委外授課方式實施，如國軍各類系統操作講習、專題教育、各式研討會等，委外授課則由各級編列教育訓練經費委民間資訊專業訓練機構，以派種子教官接受訓練或開班授課方式，進行資訊、網路、系統等安全作業技術學

註二三：中華民國國防部，國防部網站最新消息2009/1/7之軍事新聞，http://www.mnd.gov.tw/publish.aspx?cnid=65&p=31639。

註二四：中華民國國防部總政治作戰局，總政治作戰局網站知識大補帖之國軍演訓資通安全維護整備要點2007/4，http://gpwd.mnd.gov.tw/onweb.jsp?webno=3333333027&webitem_no=1053。

表五　海軍資訊安全防護SWOT分析

	優勢 (Strengths；S)	弱點 (Weaknesses；W)	機會 (Opportunities；O)	威脅 (Threats；T)
資通安全認知與環境	1. 資安認知與警覺性較高。 2. 對於國軍人員違規嚴懲不怠。 3. 高階主管對於資安政策大力支持。 4. 人員可信賴度較高。 5. 資安知識汲取及推廣較普遍。	1. 資安參與意願與共識度低。 2. 資安體系未落實權責區分，僅少數資訊人員執行資安作業。 3. 人員心存僥倖。	1. 上級要求與規範較嚴謹。 2. 鼓勵參加各界資安教育訓練或研究會，資安認知較全面性。	1. 仍因少數人於未依規定使用儲存媒體或網路服務而提高誤入釣魚網站、或感染惡意程式等。 2. 資安績效評量不易，潛在效益也常無法彰顯，致使經費投資不足，造成單位推動上的瓶頸。
整體資通安全防護能力	1. 定期推行各項資安政策及稽核，使單位資安管控更加落實。 2. 基礎資安防護設備架構完整。	1. 系統網路安全設定多，版本變化快速，專精人數不多。 2. 資安攻擊之手法日新月異，弱點防不勝防。 3. 預算不足致使現有系統網路無法獲得新技術及設備。	1. 政府及國軍大力推行各項資安防護資源。 2. 資安事件損失刺激資安防護技術發展及應用之增長。	1. 國軍為外界不良份子喜好之攻擊目標。 2. 網路充斥著各式的木馬、病毒等威脅。 3. 對於單位心存不滿之人士恐蓄意破壞。
緊急應變功能	1. 建立明確之應變計畫及組織，並實施演練，有效提升資安應變及回報能力。 2. 具備完整值勤體制，可立即接收事件及處置。	1. 未列入資安監控之設備發生資安事件，會有隱匿不報之情事。 2. 接獲事件通知人員不熟悉應變處置作為。	1. 事件回報均實施事後檢討，以提升對事件應變之重視。 2. 在資安事件蔓延、法令規範效應下，促使資安事件備受重視。	1. 蓄意人士發佈不實事件，值勤人員未發覺。 2. 發生重大危安事件無法即時復原。

資料來源：本研究整理。

習，並於結訓後實施單位內部擴訓，以提升資訊安全專業能力。

為配合資安教育深入推廣，各類軍事(學術)刊物(如海軍學術雙月刊、海軍官校季等)或國軍論壇，均刊登資訊安全相關專題文章，甚至建立專欄報導，以為現役軍人、資訊專家交流平台，深入探討宣傳資訊安全作業要點、防護關鍵及經驗，向官兵全面灌輸「資訊安全、人人有責」的資安觀念。

四、資訊安全督檢暨稽核

國軍為針對當前資安威脅，現階段主要資安需求以「國防資料不外流」、「資訊作業不中斷」為主，故為驗證各項防護作業，除國軍年度攻防演練外，海軍並接受國防部每年定期資安(訊)督檢及不定期突檢，並貫徹一級輔導一級作法，由海軍各級對下級實施督(輔)導，相關優缺均假資安工檢會進行檢討，表現良好及違規人員均依規定議與(處)，期望官兵均能依循資安維護之要求，落實資安維護作為。

除了國防部內部的資安稽核作業外，海軍司令部更推行ISO 27001資訊安全管理認

證，在ISMS模式下，透過PDCA模式不斷檢視審查單位資訊作業的安全管理，並於2008年10月取得證書，除了在資訊安全管理機制符合國際標準外，更期許未來仍將持續透過資安稽核，降低組織因資訊風險形成對工作的影響，並使海軍官兵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〔註二五〕。

肆、SWOT分析

近來，海軍基於國防部當前的戰略構想，將資訊戰重點放在網路安全防護上，並全方位思考部隊資安的狀況，建立有效防護措施與及時監控系統，並在各項資安作為中採取多種手段，已大幅提升資訊安全的防護能力。雖在資訊安全推行上配合國防部政策已行之有年，但仍有待改善之處及精進的地方，如將被動性防護轉變為主動性監偵和反制、發展數位鑑識能力等〔註十八〕。在此對於海軍的資訊安全防護作為進行SWOT進行分析(如表五)，以更清楚瞭解如何善用優勢及機會，並補強弱點及預防威脅〔註二六〕、〔註二七〕。

伍、結語

海軍在建立資訊專業部隊的基礎上，大力強化資訊安全防護作為，積極建構嚴密的資訊安全防護機制與能量，除多層次、全方位地強化各級單位的資訊安全防護機制外，更應精進專業資訊安全技能，以結合產、官、學、研界的資源，將被動防護轉為主動反制，並朝向構建自動化、系統化和資訊化的安全防護系統目標邁進，以保持我國資訊戰場的優勢。就對外攻擊資訊安全防護，及內部不當資訊外傳偵察，提供以下五項精進建議〔註二一〕：

一、加強資通安全教育訓練，培養專業資訊技能，厚植資通專業人才，以發揮通資電優勢。

二、加速整合國軍資源，完成資通人力轉型，做好資源整合作業，以提升通資電作戰能力。

三、持續透過產官學界相關資訊技術交流，及收整各國資訊戰具體作為，藉以提升單位資通系統及防護作戰技術。

四、加強人員資訊安全紀律，嚴守命令貫徹，建立完善保密的資訊安全管理。

五、精進單位資安管理工作，落實資安規範，加強交叉稽核，杜絕違規洩密事件。

作者簡介：

邱意雯上尉，國防管理學院資管系92年班，現服務於澎湖馬公高級中學。
葉道明教授，美國猶他大學電腦科學博士，現服務於國立高雄師範大學軟體工程學系。
孫培真教授，中山大學資訊管理博士，現服務於國立高雄師範大學資訊教育所兼所長兼電算中心主任。

註二五：中華民國海軍司令部，海軍司令部網站最新消息http://navy.mnd.gov.tw/Publish.aspx?cnid=846&p=30579&Level=1。
註二六：江通儒、郭真祥、張瑞益、許凱平，〈學術機關資訊安全管理建置成熟度模型〉，《教育部「2008臺灣網際網路研討會(TANET)」》，2008年，http://ccnet.km.nccu.edu.tw/xms/index.php?view=content_show&id=977
註二七：蔡忠翰，〈政府部門資訊安全管理之研究〉，國立政治大學公共行政研究所未出版之碩士論文，2003年。