航空技術學院學報　第十七卷　第 139 - 152 頁 (民國一○ 七年)
Journal of Air Force Institute of Technology, Vol. 17, pp. 139-152, 2018

空軍基層部隊人員資訊安全素養之評量與分析

Evaluation and Analysis of Information Security Literacy of Air Force Grassroots Personnel

鄭宇凱 [1] 吳俊緯 [1] 呂冠毅 [2]

Yu Kai Cheng [1] Jun Wei Wu [1] Kuan Yi Lu [2]

[1] 國防大學空軍指揮參謀學院
[2] 空軍航空技術學院機械工程科

[1]Air Command and Staff College of N.D.U.
[2] Department of Mechanical Engineering, Air Force Institute of Technology

摘要

近幾年來，政府機關、軍事單位、學校及企業的入侵事件時有耳聞，而在新聞事件的背後，資料竊取所帶來的損失往往無可估計，尤其是軍中的資料，大多牽涉到限閱或機敏性的問題，所損及的不只是資料遭竊或金錢的損失，更嚴重的是危及整個國家的安全。電腦運用的普及與網際網路的蓬勃發展，已帶給人類急速而巨大的衝擊，也改變了人類生活模式。然而隨著資訊便利而來的則是令人擔憂的資訊安全題，因此，我們必須做好資訊安全防護措施，唯有在確保資訊安全之前提下享受資訊便利，才是面對資訊世紀來臨的正確態度，進而迎接未來更大的挑戰與衝擊。因此，建構有效的資訊安全防護網，不僅是企業的重要課題，對於國軍單位更是不容忽視、勢在必行。

關鍵詞：資訊安全、網路犯罪、網路安全、資訊安全素養。

ABSTRACT

Along with the computer utilization popularization and the Internet vigorous development, has taken to the humanity rapidly and huge striking, also changed the humanity mode of life.However is the anxious information security topic which comes along with the information convenience, therefore, we must complete the information safe protective measure, only has in guarantees premise of under the information security to enjoy the information to be convenient, faces the correct manner which the information century approaches, then welcome future bigger challenge and impact.In the past few years network technology has become popular and pervasive, what was originally a single operation platform spanned into now an inter-net environment. But while it brings convenience it also brings up the network security problem. Within the past few years, network break-ins among government organizations, military units, schools, and business organizations are often heard, behind such incidents are data being stolen, causing huge amount of damage. This is a problem especially serious to the military units, where data are classified and limited to reading, The damage is not just data stolen or money lost, but something lot more serious endanger national security. Within this

perilous network world, cybercrime increases year by year, showing the importance of network security. Military force holds responsibility of national security facing war at the front line, military security is therefore showing more importance each and every day. Because of this, the construction of an information security net is no longer an issue business organizationonly, but something that the military unit must not neglect but engage.

This research focus on analyzing the present information security literacy of military personnel man, and the relation between information security literacy and law-breaking recognition, which would provide suggestions for information security

***Keywords*:** Information security, network crime, network security, information security accomplishment

1. 緒論

資訊科技的快速發展，「數位化」已成為影響組織管理的一大革命性變革，隨著網際網路（Internet）與行動通訊（Mobile Communication）的快速成長，網路資訊安全問題一再浮現，但大部份造成資訊安全事件的原因都不是專業技術的層面，而是在人性面上出現漏洞所導致，不可否認，蓄意違規人員的專業素養，及用功認真的程度是遠高過於我們一般的資訊管理人員。

本研究主要在探討目前空軍基層部隊人員資訊安全素養的現況，及其資訊安全素養與資訊違規認知兩者間之關係，進而提供空軍資訊業管部門研擬或修定相關政策之建議，以期建立較專業、完善的稽查體制，提高資訊違規事件查察成效，防範機密軍事資訊外洩。

1.1 研究背景與動機

根據台灣網路資訊中心最新的調查結果顯示（截至 2017 年 6 月初止），2017 年台灣寬頻網路使用調查與國發會 2016 年數位機會調查報告顯示，全國地區個人曾經上網率達 83%以上。（如圖 1）；個人近半年無線區域網路上網比例呈現大幅度的成長趨勢，調查結果約有近 52%民眾近半年內曾使用無線區域網路上網，近半年曾經使用無線區域網路上網人數為 1,089 萬人。（如圖 2），其中個人近半年使用行動上網的比例 2016 年達到 67.3%後，仍繼續成長至 2017 年的 69.3%，近半年曾經使用行動上網人數為 1,462 萬人，顯示過去一年民眾使用行動上網的比例仍有繼續成長的趨勢。（如圖 3），而由歷次調查中發現，網民行動上網率有逐年提升的趨勢，且從 2012 年開始呈現大幅的上升，2017 年較 2016 年增加 8.0%。（如圖 4），網民無線區域網路上網的比例有逐年提升的趨勢，雖然提升的幅度不如行動上網，但亦隨同行動上網在 2012 年開始大幅提升，2017 年較 2016 年增加 7.5%。（如圖 5）

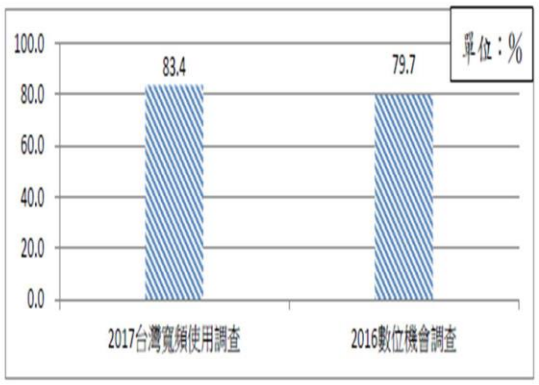

圖1 個人曾上網比例比較（單位：%）

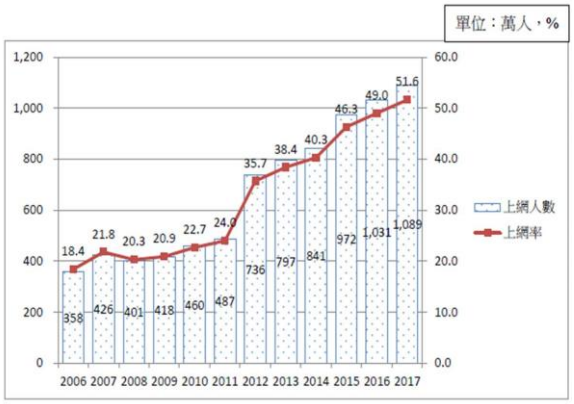

圖 2 個人近半年使用無線網路上網人數與上網率趨勢圖(單位：萬人/%)

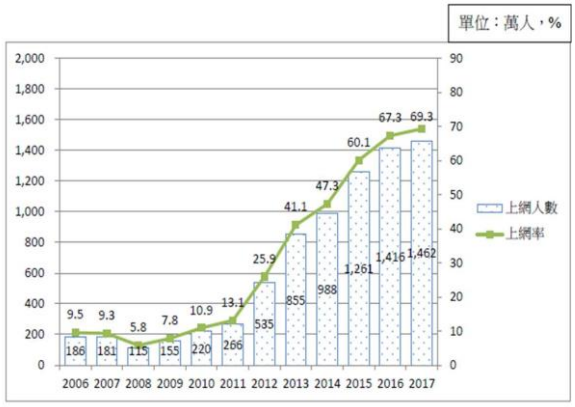

圖 3 個人近半年使用行動上網人數與上網率趨勢圖(單位：萬人/%)

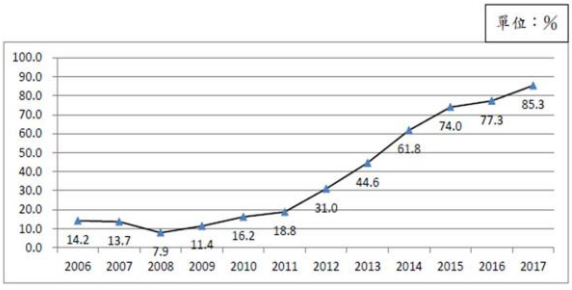

圖 4 網民行動上網率趨勢圖(單位：%)

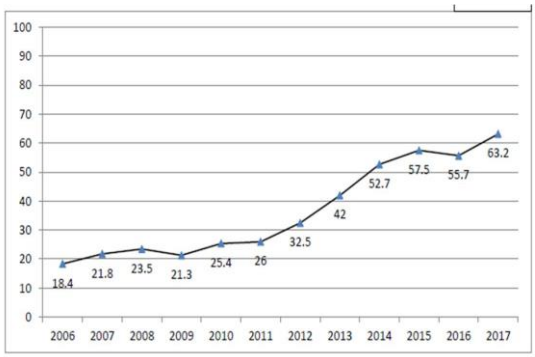

圖 5 網民無限區域網路上網率趨勢圖
(單位：%)

台灣網路資訊中心，2017，“2017 年台灣寬頻網路使用狀況調查摘要分析”，http://stat.twnic.net.tw。

根據上述調查報告顯示，我國國人網路基礎設備擁有度持續提升，上網與寬頻連網的戶數與人數穩定成長，不同年齡層的使用率亦逐漸提高，肯定台灣網路發展成效與國人資訊操作能力的普遍提升。值得注意的是，隨著行動載具的日漸普及，民眾在網路上的使用行為開始有了轉變，而上網的行為也隨著載具科技及應用服務而有日新月異的變化，如多屏多雲的混搭應用服務，也讓載具間的功能與特性變得更為模糊。

近年來隨著資訊網路科技的發達與盛行，多樣化的有線、無線通訊設備，帶給人們更便捷的生活，造就了 C2C(Consumer to Consumer electronic commerce)、B2C(Business to Consumer Electronic commerce)等電子商務的蓬勃發展，交易方式不再侷限於傳統的交易方法，使得網路漸漸成為人類生活中所不可或缺的傳輸工具，已經讓人們強烈感受到這股資訊流所帶來的便利與衝擊，然而電子交易的便捷同時提供犯罪者另一犯罪的途徑，相對延伸許多負面的問題，如最常見的網路駭客、網路誹謗、網路援交、網路詐欺、侵犯智慧財產權等，在在都說明了，網路的不當使用將會對社會造成相當程度的不良影響。

1.2 研究目的

國防二法自九十一年三月一日施行,我國國防體制正式邁入軍政、軍令一元化時代,在此同時,中共近年來挹注大量國防預算,處心積慮地對我國進行情蒐、電偵,不斷研發網路作戰能力，已對我國軍網路安全造成嚴重威脅,國軍為國防安全的第一線,倘若,國軍人員缺乏資訊安全素養,或資訊存取未配套縝密防護機制,而遭攻擊者竊取、竄改機密資訊,不論企業或國軍部隊,都將對組織造成無法彌補的傷害,網路的資訊安全勢將成為國軍邁向E 化的重要關鍵。

近年來,在國軍人員共同努力下,相關資訊保密機制不斷地精進,使得國軍的資訊安全工作,已奠定一定的基礎,為建立國軍人員個人資訊安全防護觀念，強化國軍整體資訊安全,透過相關文獻探討與實證分析,期能達到下列之研究目的：

1.瞭解空軍基層部隊人員資訊安全素養的現況：
藉由問卷調查瞭解空軍基層部隊人員之資訊安全素養及其程度。

2.探討空軍基層部隊人員其不同背景變項在資訊安全素養及資訊違規認知之差異性：
研究不同背景（年齡、階級、教育程度、初次學習電腦時間、電腦使用時間、工作單位）之空軍基層部隊人員，其資訊安全素養與資訊違規認知是否存有差異。

3.探討空軍基層部隊人員資訊安全素養與資訊違規認知兩者間之關係：
透過研究調查結果，探討國軍人員資訊安全素養與資訊違規認知之關係，藉以瞭解如何加強查察,以避免類似案件再度發生。

4.針對分析與研究結果提出建議，提供空軍基層部隊人員、稽查單位擬定或修訂相關對策及後續研究之參考。

1.3 研究範圍與限制

1.研究範圍

本研究係以南部地區某軍事單位之空軍基層部隊人員為研究對象,涵蓋的範圍包括教學、訓練及後勤部隊等單位。

2.研究限制

（1）對象受限：
因部份基層部隊士兵，平時專職戰備訓練任務，運用電腦作業時間並不多，為考量研究結果之適切性，因此排除上述人員。

（2）任務受限：
空軍基層部隊人員任務區分幕僚、教學、訓練及部隊等單位,任務性質不同,上班時間相對亦有所不同，本研究受測對象以擔任教學與後勤支援任務之人員為主，因此，部份受試者在時空上將有所受限。

（3）研究方法受限：
本研究以問卷調查方式蒐整受試者資料，本研究僅能假設受試者均能發自內心，不受主觀因素、情緒、壓力或其它外力因素影響，而能據實以答。

（4）問卷內容受限：
本研究編製之問卷內容，雖參考相關文獻、國軍法令政策整理修定而來，但由於資訊安全素養與資訊違規認知領域範圍廣泛，且國軍相關作業規定有可能因考量其適用性或上級要求，而隨時修正調整，僅能以現行之法令政策作為參考依據，所以問卷內容可能無法一一涵蓋，恐有疏漏之處。

2. 文獻探討與理論基礎

從文獻中回顧發現,有關探討國軍人員資訊安全素養與資訊違規相關學術研究尚不多見,對於國軍人員資訊安全素養之研究仍處於起步階段,目前全國相關之研究有：資訊安全素養 55 篇、資訊素養 5,727 篇、網路素養

1,817 篇、電腦素養 1,445 篇(全國碩博士論文網 107 年 2 月 27 日統計數據),因此,關於這方面的議題實值得再進一步深入探討。本研究根據研究動機與目的,針對資訊安全、網路犯罪、資訊違規事件等作一完整性之介紹,並多方蒐集整理相關理論及研究,予以分析、歸納並找出適當的量表作驗證,以徹底了解資訊安全素養與資訊違規兩者間關係及其相互之影響。

2.1 資訊安全理論基礎

BS 7799 為英國標準協會 (The British Standards Institution, BSI) 所推動的資訊安全管理標準。它不僅已成為國際資訊安全管理的準則及規範(ISO 17799 及 ISO 27001),更是各國政府單位和企業團體在資訊安全能力上的最佳證明,根據資訊安全管理系統國際標準 ISO17799 對資訊下的定義為:資訊(Information)意指以各種型態儲存的資料與知識,包括電子方式、文件方式---等,如同企業其他重要資產一樣,需要被妥善地保護。對「資訊安全」之界定上,Smith(1989)主張,任何電腦安全政策之廣義目標,必需能保護存於系統中資料之完整性(integrity)、可用性(availability)、與隱密性(confidentiality)。其為資訊安全的基本要素(本質),示意如圖 6。

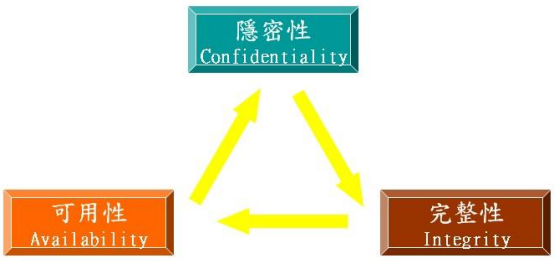

圖6 資訊安全之界定示意圖
資料來源:Smith, M., 1989, "Computer Security-Threats,Vulnerabilities and Countermeasures", formation Age,UK, pp.205-210.及本研究整理

李志文(2003)指出,資訊安全可以說是目前最受矚目的資訊議題,由於網際網路的興盛,不論是政府、企業或個人,均與網路有密不可分的關係,也因此資訊安全的建置完善與否,其所帶來的影響將與日俱增。Simson and Gene(1991)認為,電腦系統能被使用者所倚賴,且其軟體運作表現如使用者所預期,則該系統便可稱之「安全」。江高飛(2000)等人指出,資訊安全包含了通訊安全與電腦安全,通訊安全是確保電腦的訊息(文件、資料、檔案),在傳輸時不於中途遭到竊取或被盜拷,其範圍不能僅限於網際網路的傳輸,還應包含一般方式的傳輸,電腦安全指的則是確保電腦能夠正常運作,資訊的儲存能無顧慮,不論是系統的操作、資料庫的儲存、病毒的防範等,其所謂的安全即是指確保事物的安全,事物指的是一個檔案、一封電郵、一個應用程式、一套系統等,至於安全性應包括下列五大項要素,分別為機密性、資料完整性、不可否認性、授權性、真實性等。

2.2 資訊安全素養之相關研究

一般而言,人類的「理解以及和外界做有意義溝通」所「需要的能力」,隨著時代的變遷而有所不同。外界的大環境若是文字世界,人要和文字世界溝通,最基本的便是要識字,在早期西方工業國家,一般民眾受教育的機會不多,若指有「素養」之人,即指具有識字能力之人,故早期的素養教育即教導民眾具有識字能力。Luke(1992)將素養定義為一套會隨著社會的文明科技而改變的策略與技術。李堅萍(1994)指出,一組人人都需要的基本能力(skills, abilities 或 competencies),因此,素養必須是某層次的能力、技能或技術的總和,而這組能力應具有基本的、人人必備的特性。「資訊素養」(information literacy)由「資訊」和「素養」組合而成。「素養」

（literacy）為一般性的名詞，其內涵隨時代而有不同。「素養」（literacy）一詞原來指的是語文說、讀、寫的能力，「素養」亦可解釋為：「理解以及和外界做有意義溝通所需要的能力」。「資訊素養」便是指「在資訊時代個人所具備的一套技能，以學習以及和外界環境做溝通的基本技能」。Caissy(1992)指出素養是遠超過傳統的讀與寫的能力，素養包含著在不斷變遷的資訊社會環境中仍能存活的能力。

國內對「資訊素養」一詞解釋，首見於李德竹(1994)在其主持國科會專案研究計畫「由資訊素養研究圖書館資訊服務之意義與內涵」中指出，培養國民具備瞭解資訊的價值、在需要資訊時能有效查詢、評估資訊、組織資訊與利用資訊。黃世雄(1996)認為，資訊素養是廿一世紀知識工作者必備的條件，其範圍涵括全球的資訊資源，資訊素養能力應界定在培養獲取資訊、解決問題、決策訂定以及評估資訊的能力。Luehrmann(1981)則指出，電腦素養是操作電腦的經驗與能力。吳正已與邱貴發（1996）認為，電腦素養應包括：（1）認識電腦、（2）應用電腦與（3）了解電腦與社會間的互動關係。網路素養依據陳雪華（1996）的定義包括：（1）網路之基本概念、（2）網際網路與台灣地區網路之源起、發展與現況、（3）網際網路之功能、（4）網路資源類型、（5）全球資訊網的介紹、（6）檢索資訊之比較與（7）檢索策略。

楊美華(1999)認為，「資訊素養」是指一個人知道何時需要資訊，並且具備找到資訊、評估資訊及有利用資訊能力的人，其目的是學習成為一位知道如何學習的人，而資訊技能的層次為：（一）對於資訊服務與資訊的認知；（二）了解資訊的結構；（三）具有分解資訊問題（需求）的能力；（四）懂得如何檢索資訊；（五）評估資訊；（六）管理資訊。郭麗玲(1999)認為，「資訊素養」是指蒐集、整理、評鑑及利用資訊的能力。

魏令芳（2002）指出，資訊素養是培養國民具備瞭解資訊的價值、在需要資訊時能有效查詢資訊、評估資訊、組織資訊和利用資訊。陳伯榆（2003）認為，全面提昇資訊安全的素養，將和提昇資訊素養一樣重要。綜合上述學者對資訊素養所作的定義整理如表 1。

表 1 國內外學者對資訊素養所作的定義綜合整理表

國內研究者	定　義
吳正已與邱貴發（1996）	認為電腦素養應包括：（1）認識電腦、（2）應用電腦與（3）了解電腦與社會間的互動關係。
陳雪華（1996）	網路素養的定義包括：（1）網路之基本概念、（2）網際網路與台灣地區網路之源起、發展與現況、（3）網際網路之功能、（4）網路資源類型、（5）全球資訊網的介紹、（6）檢索資訊之比較與（7）檢索策略。
郭麗玲（1999）	「資訊素養」是指蒐集、整理、評鑑及利用資訊的能力。
魏令芳（2002）	培養國民具備瞭解資訊的價值、在需要資訊時能有效查詢資訊、評估資訊、組織資訊和利用資訊。
陳伯榆（2003）	行為乃是個體表現於外，且能被直接觀察記錄或測量的動程。

資料來源：本研究彙整

2.3 資訊違規與資訊犯罪研究理論基礎

資訊違規乃指「違犯保密規定」，依據「國軍人員違犯保密規定行政懲處標準表」對其所作之定義為：違反國家機密保護法規，及「國軍保密實施規定」等有關保密之規定或命令，違成國防機密資訊有洩密顧慮，但未構成洩密者。其中，國軍人員在處理、保管國防機密資訊（即「國家機密」、「軍事機密」、「國防秘密」、

「一般公務機密」),未善盡職責,致肇生洩密事件,洩密者依法偵辦,相關失職人員依照「國軍人員違犯保密規定行政懲處標準表」,依情節輕重檢討議處。

我國「國家機密保護法」於 2003 年 2 月 6 日公佈實施,該法中第 4 條將國家機密區分為「絕對機密」、「極機密」、「機密」三個等級,並在第 2 章中明確規範國家機密核定之權責、保密與解密之條件等。國防部為了配合國家機密保護法的制定與陸海空軍刑法第 78 條之規定,於同年 4 月 25 日修訂「軍事機密與國防秘密種類範圍等級劃分準則」,以處理軍事及國防機密。「通訊科技」與「網際網路」的精進與普及,除衝擊原有的國家限界外,也危及國家的整體安全。於此同時,國軍經歷多年的努力,已使軍隊邁入「資訊化」與「電子化」,有效提昇指揮管理與用兵作戰之效率;然而,資訊作業的便捷性,就像劍之雙刃,稍有不慎即可能為自己帶來莫大的傷害,而這也就是國防軍機維護,所必須面對的嚴峻挑戰。如何制止犯罪的發生,從人類有社會行為以來,一直都是值得討論議題。

另外,為解決國軍資訊保密安全之困境,國軍相關機構不斷地研謀精進措施,使國軍網路一旦遭受外來因素破壞或不當使用等緊急事故發生時,能迅速作必要之通報及緊急應變處置,並在最短時間回復正常運作,以降低該事故可能帶來之損害,促使國軍能真正成為「數位化」之國軍。本研究將參考國軍相關資訊安全管理標準,以作為問卷內容,國軍資訊安全相關管制規定與精進作法摘錄如下:

1.「個人電腦資訊安全防護作業規定」

為促使本軍人員瞭解資訊安全的重要性,以防止個人電腦遭入侵、竊取或破壞,有效維護個人資料及系統安全,以建立資訊安全一級防護概念,其內容包括:實體隔離政策、資料分級處理、個人電腦安全設定檢查等要項。

2.「國軍通資安全常見違規事件暨應行注意事項」其內容包括:

通信安全違規事件應注意事項如:密碼(語)本表暨通信密件管理、行動電話管制規定等計 14 要項;資訊安全違規事件應注意事項如:密級(含以上)資料儲存管制、資訊媒體稽核檢查、資訊系統與通資網路之設備存取管理、刑法修正條文等計 51 要項。

3.「電腦緊急應變處理實施計畫」

針對空軍資通系統、網路所發生之安全事件,提供早期預警、狀況處置程序,有效減低災損、快速復原,俾支援作戰。依「有效嚇阻、防衛固守」之作戰指導,及就各單位資訊系統、網路現況及可能之威脅與突發狀況,結合政策計畫、指揮管制、通報處理、研發諮詢及各單位 CERT 等分組,建立國軍電腦緊急應變處理機制,掌握遭受資訊攻擊或突發事件影響期間全般狀況及協調處理,以確保國軍通資安全。

4.「資訊網路安全監測作業實施規定」

有效落實「資安監控機制要求事項」為當前國軍重要政策,其置重點於陸軍連接國軍資訊主幹網路單位,實施系統偵測體檢、安全漏洞掃瞄及記錄分析檢討,採固定監測為主、機動監測為輔,不定期對連接國軍資訊網路單位,執行資訊安全「弱點掃瞄」作業,俾先期發掘問題及改進缺失,以杜絕資訊危安事件。其稽核項目包括:個人電腦權限管理、機密資料管理、防毒及漏洞修補、個人電腦保密設定、違反實體隔離、影響國軍安全、軍紀、軍譽等資訊作業行為。國軍資訊安全管控機制。

5.「資訊設備及資訊儲存媒體管制規定」

藉嚴格限制單位公務用電腦「輸出(入)裝備」,俾防制機敏資訊洩密管道,以確保資料檔案管理安全。各類型公務用電腦(包括:桌上及筆記型)輸出(入)裝置均納入管制。

其管制項目有:「軟碟機」、「燒錄器」、「USB」、「RS232」及「印表機」連接埠等電腦輸出（入）裝置，包括拆除「燒錄器」及「軟碟機」、移除「USB 連接線」、安裝偵測軟體、資料交換(輸出/輸入）等管制規定。

6.「個人電腦輸出（入）裝置使用管制規定」

本規定之目的為落實單位及個人「資訊設備」、「資訊儲存媒體」管制，以防止設施器材遺損，內存公務資料、檔案、文件、圖像及機敏系統等洩（違）密，確保資訊安全，其管制項目有：裝備採購、管制識別標籤、器材、無線設備管制、網路實體隔離及相關違規懲處規定等要項。

7.「通資業務手冊密碼選取規則」

其目的為律定密碼選取規則要點，以強化電腦之保密機制，包括個人帳號及電腦各式密碼（包含作業系統上之使用者及管理者、開機密碼、BIOS 密碼等）作業規定。

8.「００號演習」通資安全監察維護實施規定

為確保演習機密維護及演訓任務之遂行，每年定期修頒演習期間保密安全應行注意事項，包括：落實個人保密、保密作業紀律、復原階段之裝備與資料保管等要項。

9.「網路實體隔離及資訊設備庫存管理觀摩實施計畫」

藉由觀摩示範，統一國軍「網路實體隔離」、「資訊設備」及「資訊設備媒體」等管制作法，俾要求各相關單位落實辦理，以防杜肇生洩密事件。

3. 研究方法

本研究根據前述之研究動機及目的，透過相關文獻的探討，建立研究架構及研究假設，進行問卷內容之設計與調查，資料的蒐集整理採用文獻探討、問卷調查法、訪問調查法、統計分析與專家檢核等方法，並依據國軍電腦緊急應變處理(CERT)實施計畫、資安監控機制作法、空軍人員違犯保密規定懲處標準表、資安督考實施計畫及資訊安全相關法規，另參考其他適用之量表，用以設計「空軍基層部隊人員資訊安全素養與資訊違規認知關係之研究」調查問卷。

3.1 研究架構

本研究以空軍基層部隊人員之背景因素為自變項、資訊安全素養為依變項，探討空軍基層部隊人員資訊安全素養的現況及分析比較其背景因素對資訊安全素養之影響及資訊安全素養與資訊違規認知兩者間之相互關係。本研究架構如圖 7 。

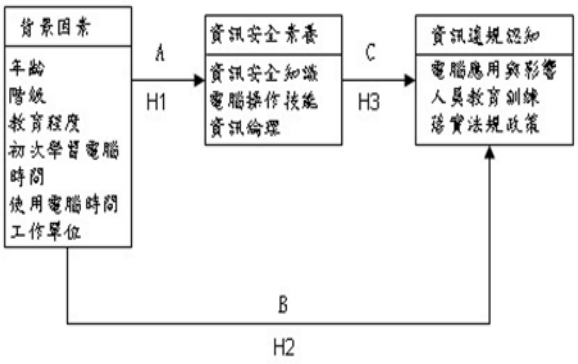

圖7 本研究架構圖

資料來源：本研究整理

3.2 研究假設

根據上述研究目的及研究架構，擬訂下列研究假設，進行相關假設檢定：

假設 1：空軍基層部隊人員背景之不同，在資訊安全素養上應無顯著之差異。

假設 1-1 空軍基層部隊人員年齡之不同，在資訊安全素養上應無顯著之差異。

假設 1-2 空軍基層部隊人員階級之不同，在資訊安全素養上應無顯著之差異。

假設 1-3 空軍基層部隊人員教育程度之不同，在資訊安全素養上應無顯著之差異。

假設 1-4 空軍基層部隊人員初次學習電腦時間之不同，在資訊安全素養上應無

顯著之差異。

假設 1-5 空軍基層部隊人員使用電腦時間之不同，在資訊安全素養上應無顯著之差異。

假設 1-6 空軍基層部隊人員工作單位之不同，在資訊安全素養上應無顯著之差異。

假設 2：空軍基層部隊人員背景之不同，在資訊違規認知上應無顯著之差異。

假設 2-1 空軍基層部隊人員年齡之不同，在資訊違規認知上應無顯著之差異。

假設 2-2 空軍基層部隊人員階級之不同，在資訊違規認知上應無顯著之差異。

假設 2-3 空軍基層部隊人員教育程度之不同，在資訊違規認知上應無顯著之差異。

假設 2-4 空軍基層部隊人員初次學習電腦時間之不同，在資訊違規認知上應無顯著之差異。

假設 2-5 空軍基層部隊人員使用電腦時間之不同，在資訊違規認知上應無顯著之差異。

假設 2-6 空軍基層部隊人員工作單位之不同，在資訊違規認知件上應無顯著之差異。

假設 3：空軍基層部隊人員資訊安全素養之不同，在資訊違規認知上應無顯著之差異。

假設 3-1 空軍基層部隊人員資訊安全知識之不同，在資訊違規認知上應無顯著之差異。

假設 3-2 空軍基層部隊人員電腦操作技能之不同，在資訊違規認知上應無顯著之差異。

假設 3-3 空軍基層部隊人員資訊倫理之不同，在資訊違規認知上應無顯著之差異。

3.3 研究變項與衡量

本研究為達研究目的，驗證研究假設，以自編之「空軍基層部隊人員資訊安全素養與資訊違規認知關係之研究」調查問卷，作為問卷調查的研究工具，其內容共分為「個人背景」、「資訊安全素養」、「資訊違規認知」等三部分。

在人員屬性變項方面，其主要內容歸納為年齡、階級、教育程度等四項基本人口統計變數；「資訊安全素養」內涵應包括「資訊安全知識」、「電腦操作技能」、「資訊倫理」等三個研究構面；「資訊違規認知」內涵應包括「電腦應用與影響」、「人員教育訓練」、「落實法規政策」等三個研究構面，其問項均為單選項目。

3.4 研究工具及預設

本研究原則上參考楊境恩(2004)的「國內警察人員資訊安全素養對資訊犯罪偵查能力影響之研究」調查問卷、國軍資訊安全相關法規及相關研究文獻，據以發展設計問卷題目。本研究其問項均為單選項目，採用李李克特（Likert）五點量表計分方式，以語意差異量表給予評等，其選項計分為「非常同意」5 分、「同意」4 分、「普通」3 分、「不同意」2 分、「非常不同意」1 分等。

本問卷雖已參考相關法規、量表及研究文獻，但為求問卷調查結果能更加正確與嚴謹，將編製好之量表進行預試，以提高問卷的可行性。預試問卷在擬定初稿後，於民國 107 年 2 月 8 日利用某空軍天氣中心莒光日資訊安全法令宣教時間，針對 30 名現職人員（含軍、士、官及聘雇人員）進行預試。為求量表之精確，本研究除依據預試問卷進行信度與效度之檢驗外，另以專家檢核方式，親自邀請兩位指導教授、一位專業教授與 10 位資訊專業軍官，針對預試問卷內容各題項逐一檢視後，作語意修改與校正。

3.5 研究對象及問卷施測

本研究屬地區性之研究，僅以空軍南部某基層部隊之現職人員為施測對象，問卷以親自送交及委託方式進行，採取「隨機取樣」方式進行抽樣問卷調查。並採取問卷調查法為衡量方法，問卷依上述文獻探討中之理論基礎與學者之相關研究分析結果，找出合適問卷調查資料，進行實證資料蒐集。本研究採樣時間從106 年 12 月 18 日至 107 年 2 月 14 日，問卷共發送 350 份，回收 323 份，回收率達 92.3%，其中不完整（資料不全或無效問卷）予以剔除計 13 份，共計有效樣本 310 份，有效回收率為 88.57%，各單位問卷發放及回收情形如表 2。

表 2 問卷發放及回收情形表

發放單位	發放份數	回收份數	回收率	有效份數	有效回收率
A 單位	**150**	**145**	**96.67%**	**140**	**93.33%**
B 單位	**100**	**93**	**93.00%**	**90**	**90.00%**
C 單位	**100**	**85**	**85.00%**	**80**	**80.00%**
合計	**350**	**323**	**92.30%**	**310**	**88.57%**

3.6 信度與效度

張紹勳（2000）從科學的觀點切入認為，一個良好的衡量工具應具備足夠的信度與效度。信度是指衡量工具的正確性與精確性。一般而言，一個具有信度的測量工具，必須在不同條件下都能獲得穩定的測量結果。葛樹人（1987）指出，Cronbach's α 係數為各種信度中較為嚴謹者，有時被稱為信度的低限，是目前採行最廣的指標。故以 Cronbach's α 值來測量問卷的內部一致性，若 Cronbach's α 係數值高，則顯示量表內各變項的相關性愈大，亦即其內部一致性愈一致性。Nunnally（1967）建議 Cronbach's α 係數要≧0.7 才屬於很可信的範圍，或至少要達到 0.5 以上方合乎信度要求。

本研究以此建議來作為信度之衡量標準。所謂效度則是指衡量工具能夠真正測出研究人員所想要衡量事務的程度。為瞭解本研究問項量表的信度情形，本研究乃參考相關文獻與法規政策之內容，另依據指導教授及實務專家根據各層面所包括之題項一一檢視修改提供修訂意見，確定各構面變項所涵蓋的題項後，先對各構面變項進行 Cronbach's α 信度係數分析，再逐題進行檢視，最後再以 SPSS 進行驗證性因素分析，以瞭解各構面變項與衡量題項間的內在一致性情形，及符合表面效度、內容效度及專家效度。

4. 研究結果

4.1 研究方法與分析

本研究以 SPSS For Windows12.0 中文視窗版統計軟體進行統計分析，本研究資料分析方法如下：

1.描述性統計（Descriptive statistics）：分析本研究之樣本結構，以次數分配平均數及標準差，分析國軍人員之樣本基本資料的分佈情形。

2.卡方檢定（Chi-Square.test）：檢測國軍人員使用電腦時間及初次學習電腦的時間是否因背景變項不同而有所差異；經檢定後，具有顯著的差異變項，則進一步透過交叉分析瞭解其差異情形。

3.t 檢定（t-test）及單因子變異數分析（One-wayANOVA）：來比較不同背景變項之國軍人員在資訊安全素養差異情形，若達顯著水準，則進一步透過平均數或進行 Scheffe 事後比較法瞭解其變項間是否達顯著差異。

4.本研究各項統計考驗顯著水準均訂為 α=.05。

4.2 空軍基層部隊人員背景與資訊違規認知關係研究結果

本研究將空軍基層部隊人員背景與資訊違規認知差異性檢定結果彙整如表 3。

表 3 空軍基層部隊人員背景
與資訊違規認知差異性檢定彙整表

構面	年齡	階級	教育程度	初次學習電腦時間	使用電腦時間	工作單位
電腦應用與影響	T=.138**	T=1.300	F=.258	F=1.108	F=2.202*	F=5.134*
	P=.000	P=.162	P=.654	P=.303	P=.012	P=.001
資訊教育訓練	T=3.560**	T=1.848	F=.286	F=1.321	F=.388	F=4.555*
	P=.000	P=.051	P=.761	P=.246	P=.725	P=.001
落實法規政策	T=1.378	T=2.374	F=.808	F=1.486	F=.607	F=1.316
	P=.169	P=.018	P=.346	P=.225	P=.488	P=.110

資料來源：本研究整理　*：P<0.05　**：P<0.01

由表 3 分析結果得知：

1.年齡方面，對於空軍基層部隊人員之資訊違規認知，在電腦應用與影響與資訊教育訓練構面有顯著差異。

2.階級方面，對於空軍基層部隊人員之資訊違規認知無顯著差異。

3.教育程度方面，對於空軍基層部隊人員之資訊違規認知無顯著差異。

4.初次學習電腦時間方面，對於空軍基層部隊人員之資訊違規認知無顯著差異。

5.使用電腦時間方面，在電腦應用與影響構面有顯著差異。

6.工作單位方面，對於空軍基層部隊人員之資訊違規認知，在電腦應用與影響及資訊教育訓練構面有顯著差異。

4.3 空軍基層部隊人員資訊安全素養與資訊違規認知各構面之相關分析

經皮爾遜積差相關分析，空軍基層部隊人員資訊安全素養與資訊違規認知各構面之相關係數為.469 到.785 (顯著性均為.000)，分析結果如表 4。

表 4 資訊安全素養
與資訊違規認知各構面相關分析摘要表

構面		資訊違規認知 電腦應用與影響	資訊教育訓練	落實法規政策	整體
資訊安全素養	資訊安全知識	.560** (.000)	.768 ** (.000)	.469** (.000)	.684** (.000)
	資訊操作技能	.720** (.000)	.674** (.000)	.587** (.000)	.681** (.000)
	資訊安全倫理	.683** (.000)	.682** (.000)	.785** (.000)	.765** (.000)

資料來源：本研究整理　** 在顯著水準為 0.01 時 (雙尾)，相關顯著。

由表 4 分析結果得知：

一、「資訊安全知識」與資訊違規認知整體層面積差相關值為.684，各構面的相關分析為.469 到.768 均呈顯著相關。

二、「資訊操作技能」與資訊違規認知整體層面積差相關值為.681，各構面的相關分析為.587 到.720 均呈顯著相關。

三、「資訊安全倫理」與資訊違規認知整體層面積差相關值為.765，各構面的相關分析為.682 到.785 均呈顯著相關。

5. 研究結論與建議

5.1 研究發現結論與建議

根據本研究發現，提出下列幾點結論與建議：

1.空軍基層部隊人員年齡之不同，在資訊安全素養上之差異比較結果，在資訊倫理構面分析有顯著差異，表示不同年齡之空軍基層部隊人員，其在資訊利用的倫理議題上顯然有不一樣的價值觀。

2.空軍基層部隊人員工作單位之不同，在資訊安全素養上之差異比較結果，在「資訊安全知識」、「資訊操作技能」及「資訊倫理」等構面，均有顯著差異，顯然不同任務特性之空軍基層部隊人員，其資訊安全之素養亦明顯不同。

3.在資訊安全知識、電腦操作技能及資訊倫

理等構面，以「資訊安全知識」的認知程度最高，而「電腦操作技能」的認知程度最低。顯示大部份空軍基層部隊人員在電腦操作技能上，仍有待加強，因此空軍資訊相關部門應加強不同階層人員資訊作業能力之培養，避免因不閒電腦之操作，而產生資安事件，影響單位整體資訊作業安全。

4.最後經由分析與研究結果發現，資訊倫理量表對資訊違規認知有顯著影響，顯示具有較高資訊倫理觀念的人員，較不易發生資訊違規事件。

5.2 後續研究建議

1.研究方法方面：

本研究藉由問卷調查瞭解空軍基層部隊人員資訊安全素養現況，及不同背景變項在資訊安全素養及資訊違規認知之差異性，僅能探討影響受試者行為與有關變項間之關係，或變項間的相關情形，較難了解空軍基層部隊人員實際經驗或內心感受，故建議除量化資料蒐集外，應再輔以質性研究，例如將調查問卷加入建議事項、實地觀察或訪談等方式，採「質」與「量」相互印證比較，使研究結果更適切周延。

2.橫斷面與縱斷面研究並重：

以研究時間點來看，本研究屬於橫斷面（cross-sectional）的研究方式，對於研究變項隨時間的變化（如工作環境變動、職缺任務的調整、人員受訓進修）等，未能長時間加以探究，後續研究者可以針對此方向從事跨時間點縱斷面研究（longitudinal study）。

參考文獻

[1]翁錳揮，2006，“資訊管理暨通資安全成效檢討與策進”，陸軍 94 年學用會報研討會，陸軍司令部，1 月。

[2]翁錳揮，2006，“當前通資安全政策指導”，陸軍 95 年度通資安全巡迴講習資料，陸軍司令部，頁 2，3 月 21 日。

[3] 國家資通安全會報技術服務中心（ICST），2005，“由資安案例談資安防護”，9 月。

[4] 林宜隆，2000，“網路犯罪之案例分析”，中央警察大學學報，37 期，9 月。

[5] 林宜隆，2000，“網際網路與犯罪問題之研究”，2 版，中央警察大學，桃園。

[6] 黃毓怡，2006，“93-94 年警政署網路犯罪發破數統計調查”，內政部警政署服務信箱(電腦編號：951Z001871)，4 月 13 日。

[7] 黃世銘、謝名冠，2001，“網路行為規範之研究”，台灣台北地方法院檢察署八十九年度研究報告，台灣台北地方法院檢察署印行。

[8] 陳伯榆，2001，“Code Red 從癱瘓學術網路看校園網路主機管理問題”，台灣區學術網路研討會暨網路學習與繼續專業教育國際會議，10 月 24 日。

[9]經濟部工業局，2009，“電信平台應用發展推動計畫”，資策會 ACI-IDEA-FIND：http://www.find.org.tw/find/home.aspx?page= many&id=133，5 月 20 日。

[10]楊境恩，2004，國內警察人員資訊安全素養對資訊犯罪偵查能力影響之研究，樹德科技大學，資訊管理研究所碩士論文。

[11]楊美華，1999，“由多元入學方案談圖書館資訊之運用”，全國高中圖書館主任業務研討會會議資料，頁 45-51，台北。

[12]葛樹人，1987，心理測驗學，桂冠出版社，台北。

[13]劉淑娟，1998，我國公共圖書館技術服務館員資訊素養之研究，淡江大學，碩士論文，6 月。

[14]魏令芳，2002，大學資訊素養之研究，國立台灣師範大學，圖書資訊學研究所碩士論文。

[15]馮震宇、劉志豪，1998，“我國網路犯罪類型及案例探討”，月旦法學雜誌，41 期，10 月。

[16]蘇諼，1997，“談資訊素養與使用者導向的圖書館服務”，輔仁學誌─文學院之部，26 期，頁 152-153 ，6 月。
[17]Behrens, Shirley J., 1994, A Conceptual Analysis and Historical Overview of Information Literacy, College and Research Libraries 55 : 4, pp.302-309.
[18] Caissy, Gail A. , 1992, “Curriculum for the Information Age Learning connections: Guidelines for media and technology programs. ” North Carolina Department of Public Instruction. Bob Etheridge, State Superintendent, pp.1.
[19] Doyle, Christina S.,1992, “Outcome measures for information literacy within the National educational Goals of 1990”, Final report to national forum on Information literacy, Summary of findings .
[20] Jelinek, F., 1968, Probabilistic information Theory, McGraw-Hill, New York.
[21] Karen, D.L., Houston, H.C., and Mellerrill, E.W., 1992, “Threates to Information Systems: Today’s Reality, Yesterday’s Understanding. ”, MIS Quarterly, pp.173-186,.
[22] Luke, A.,1992, “Read and Critical literacy : Redefining the Great Debate.”,ERIC ED345211.
[23] Luehrmann, Authur. , 1981, “Computer literacy-what should it be? Mathematics Teacher ”, 74(9), pp.682-686.
[24] McClure, C. R., 1994, “ Network literacy: A role of libraries? ”, Information Technology and Libraries, 13(2), pp.117-118.
[25] Malisow Ben, 2004, “Valuing Secure Access to Personal Information.”, http://www.securityfocus.com/infocus/1797, visited on 2006/6/8.
[26]Nunally J. C. , 1978, Psychometric Theory, New York: McGraw Hill.
[27] Parker, D. B., “Fighting Computer Crime.” ,Wiley Computer Publishing. pp.72,1998.
[28] Smith, M., 1989, “Computer Security-Threats, Vulnerabilities and Countermeasures”, formation Age, UK, pp.205-210.
[29] Simson, G., and Gene, S., 1991, Practical UNIX Security, O, Reilly & Associates ,Inc.
[30]Shelly, G. B., Cashman, T.J., & Waggoner, G. A.,1996,Using computers: A gateway to information, Danvers, MA: Boyd & Fraser publishing company .
[31] Steven, J.,1992, Applied multivariate statistics for the social sciences (2nd ed.),New Jersey: Lawrence Erlbaum Associates, Hillsdale.