# 提升後備指揮部網際網路資安防護效能關鍵成功因素之研究

作者／李建鵬中校、林靳原少校


## 提要

一、後備指揮部為長期與民間資訊交流的單位，隨著科技發展，網路攻擊手法日新月異，再加上資訊專業從業人力不足，相關資訊政策會因設備及人員異動而需修訂，故「資安防護設備不足」、「資安人員素質待提升」及「資安政策仍需修訂」為本研究之主要動機。

二、針對現今網路攻擊手法及資安威脅，資安政策與人員資安素質重要性，以及網際網路資安防護技術發展趨勢等相關文獻進行研析，並經過專家問卷後建立層級架構，確認達成研究目標之主準則計「防護設備」等 4 項，次準則計「APT 防護設備」等 22 項。

三、研究分析後，發展出「爭取高階主管支持、具資安專業人員及全體員工參與」、「增設 APT 設備及相關防護機制」、「落實資料加密及非法連線偵測作為」、「執行資安治理成熟度評估及資訊安全管理認證」及「運用巨量資料分析及相關聯防機制」等作法，可提供後備指揮部提升網際網路資安防護效能之參據。


**關鍵詞：**資安防護、資安政策、分析層級程序法。

## 前言

自從傳輸控制協定(Transmission Control Protocol, TCP)和網際網路協定(Internet Protocol, IP)被定義了之後，網際網路隨著科技的發展廣泛地被運用，至全球資訊網(World Wide Web, WWW)瀏覽網站、透過檔案傳輸協定(File Transfer Protocol, FTP)傳輸資料，以及利用郵件傳輸協定(Simple Mail Transfer Protocol, SMTP、Post Office Protocol - Version 3, POP3)傳送郵件等，都成為我們日常生活中不可或缺的事情。「水可載舟，亦可覆舟」，網際網路的便利性，也成了駭客侵佔破壞、竊取資料及恐嚇勒索的途徑，導致近幾年的攻擊手段日新月異，進階持續性威脅(Advanced Persistent Threat, APT)、分散式阻斷服務攻擊(Distributed Denial of Services, DDoS)及阻斷存取式攻擊(Denial-of-Access Attack)，也就是勒索軟體的攻擊等，都是現今我們耳熟能詳的新型態攻擊手法，且資安事件層出不窮的主因。

國家資通安全會報技術服務中心在民國 102 年 11 月 8 日公布了「政府組態基準(Government Configuration Baseline, GCB)」，源起為 Intel IT 中心針對美國及英國等 400

個行政機關與企業組織，進行個人電腦安全防護議題調查。其中，端點設備安全防護議題位居第 3 名，相關資安弱點包含預設組態設定風險過高、帳號權限控管不落實及弱密碼設定等，但其目的僅在於規範個人電腦一致性的安全設定(例如密碼設定長度及安全更新期限等)，而未能防護特定攻擊手法或惡意病毒感染。

國軍現行網路的使用狀況，區分為軍網和民網(以下皆稱為網際網路)，軍網採取了實體隔離的政策，降低了資安威脅的風險，但因進行學術研究及與民間資訊交流的關係，網際網路成了我們不可忽視的重點防護範疇。後備指揮部負責動員管理、召集訓練、留守撫卹及輔導組織服務等相關工作，正是長期與民眾資訊往來的單位，故網際網路設定無法過於封閉，且其網際網路已依單一閘口方式設置，亦納入行政院政府組態規範。但「道高一尺，魔高一丈」，資安攻擊手段防不勝防，而後備指揮部現資安人員不足，且人員素質也可再提升。另現今資安科技蓬勃發展，許多技術方法皆可加以運用，本研究將依「資安設備」、「人員素質」、「技術方法」、「政策策訂」等 4 個面向，進行提升後備指揮部網際網路資安防護效能之研究，以防止遭受駭客攻擊，並確保能在網際網路安全無虞情況下，提供民眾最為完善的感動服務。承上所述，就後備指揮部網際網路在「資安設備」等 4 個面向現況問題分述如下：

## 一、資安防護設備不足

後備指揮部網際網路已納入國軍資安防護中心監控範疇，惟其防護設備僅民國 102 年建置的日誌收集器事件收容模組(Event Aggregation Module, EAM)，以及後備指揮部自行購買的防火牆(FortiGate 300A)與卡巴斯基防毒伺服器。後備指揮部全球資訊網站具有線上服務功能，須輸入相關個人資料，無具獨立的網頁防火牆(Web Application Firewall, WAF)，難以防範駭客入侵網站竊取個人資料之舉；面對現今攻擊手法與日俱增，不具進階持續性威脅或分散式阻斷服務攻擊(DDoS)等相關防護設備，難以抵抗駭客發動流量攻擊，影響網路、破壞網站，以及利用電子郵件發送惡意程式等行為。

## 二、資安人員素質待提升

因應國防部在民國 100 年推動的「精進案」兵力調整計畫，後備指揮部資訊(安)人員職缺，各地區及縣市指揮部電子資料處理官(以下簡稱電資官，負責資訊及資安相關業務)，先後由少校調降為上尉職缺，在業務推動及任務執行等方面影響甚鉅；後續，國防部又在民國 103 年推動「精粹案」之兵力調整計畫，導致現今後備指揮部部分所屬單位面臨無電資官，僅有 1-2 位聘僱人員負責資訊業務的情況，且部分電資官並非本科專業出身，恐影響資訊業務推動執行，並因此肇生資安事件。

## 三、資安科技可加以運用

後備指揮部雖已建置日誌收集器事件收容模組，納入國軍資安監控中心管理範疇，惟 EAM 僅蒐集相關日誌，又因資訊人力不足，導致執行一般資訊業務負擔沉重，無

暇運用相關科技，提升資安防護效能。現今資安科技蓬勃發展，可運用資料探勘(Data Mining)、雲端資料加密、蜜罐(HoneyPot)技術、資料庫活動監控、自動偵測非法連線等技術，以增加資安防護強度，提高資安防禦縱深。

### 四、資安政策執行需重新檢視

後備指揮部網際網路已依國防部規定，納入行政院「政府組態基準」規範，此規範僅針對個人電腦依群組原則做部分安全性設定，仍須嚴謹且廣泛的資安政策來要求系統及個人電腦防護設定。國防部通次室於督考時，雖會驗證各單位是否完成 ISO 27001 資訊安全管理系統認證，惟後備指揮部常因經費、人力問題，而導致無法全面執行，且若要在「資安設備」、「人員素質」及「技術方法」等方面，來提升防護設備、增進人員能力及增加技術方法，就必須在「政策策訂」方面增加規範來律定，藉以相輔相成。

本文旨在運用分析層級程序(Analytic Hierarchy Process, AHP)法作為研究工具，首先藉由蒐集現今網路攻擊手法、資安威脅與資安政策等相關文獻，以利掌握未來提升後備指揮部網際網路資安防護設備的重點，以及探討提升後備指揮部網際網路資安防護效能的能力與限制。進而運用分析層級程序法，探究後備指揮部執行網際網路資安防護效能提升時，所需考量的評估準則，透過專家問卷方式，建立達成目標的層級架構，並設計 AHP 問卷，透過問卷調查產出準則權重，作為分析依據。最後，提出結語及建議，期可作為未來後備指揮部提升網際網路資安防護效能參據。

## 文獻探討

資訊安全的重要性是眾所皆知的，駭客攻擊、間諜入侵、病毒感染、系統漏洞、人員疏失、天然災害或設備故障等都是現今資訊安全面臨的問題，除了建置防護設備可解決外，管理政策訂定、人員安全管理及技術手法應用等都是不可或缺的。透過文獻蒐集與探討，在第一段將介紹現今重大網路攻擊手法與資安威脅，第二段將說明資安政策及人員資安素養的重要性，第三段為提升資安防護效能趨勢發展說明，第四段運用分類比對方式，將提升資安防護效能的文獻歸納出相關主層面及次要素，本文所參考的文獻皆列屬 ISO/CNS 27001 資訊安全管理系統(Information Security Management System, ISMS)國際標準範疇，所規範的實體及環境安全、資訊安全政策、人力資源安全及運作安全等目標與控制措施之範疇，以利有效設計專家訪談問卷。

### 一、網路攻擊手法與資安威脅概述

(一)進階持續性威脅

進階持續性威脅是攻擊者利用充分的資源，針對鎖定的組織，進行全面性、複雜度高且循環週期長的網路攻擊；通常組織型駭客會運用 APT 攻擊竊取國家、軍事及商

業機敏資料，或影響金融系統運作，獲得金錢利益。2013 年南韓發生大規模 APT 攻擊事件，造成數萬臺電腦及數千臺提款機受創；同年，國家發展委員會檔案管理局電子公文交換系統(e-Client)遭駭事件，約數千臺電腦遭入侵，另 2017 年遠東銀行系統遭駭事件，數十億元遭盜轉，均為近年發生的重大 APT 攻擊事件。季祥在研究中提出防範駭客攻擊為現今網路時代重要的課題，鎖定特定目標的進階持續性威脅手法，使得傳統防護方式無法因應這種高複雜威脅，如何設計安全原則實為至當重要的目標。

(二)分散式阻斷服務攻擊(Distributed Denial of Services, DDoS)

阻斷服務攻擊是使受害電腦的系統或網路服務中斷，導致其無法正常存取的網路攻擊手法；攻擊者使用兩個或以上的電腦發動「阻斷服務」，稱分散式阻斷服務攻擊。2016 年美國的網域名稱系統(Dynamic Network System, DNS)提供商 Dyn 遭到迄今規模最龐大的 DDoS 攻擊，造成北美及歐洲網路大癱瘓的事件。林紹驊在研究中提及網路上不時存在著惡意的使用者，利用系統電腦的漏洞、網路通訊協定的缺陷來進行攻擊，又以分散式阻斷服務攻擊對網路影響最大；2014 年第 1 季全球 DDoS 攻擊總量比前一年同時期增加了 47%，如何有效減低 DDoS 攻擊為現今面臨的重要問題。[1]

(三)勒索病毒

陳信綸研究提及近來惡意軟體已由破壞電腦主機方式，轉變為對重要檔案加密，並向受害者勒索贖金，也就是勒索病毒的攻擊行為。防毒軟體雖可提供基本的防護，但遇到新穎或變種的勒索病毒攻擊，防毒軟體就無法即時防護，對重要資料進行防護，以避免遭勒索病毒之攻擊，為可行性方案。2017 年 5 月，史上最大規模的勒索病毒想哭(WannaCry)蔓延全球，在短短不到 24 小時內，造成數百個國家、數十多萬臺電腦受到感染，又以烏克蘭、俄羅斯及臺灣為最大受災區。

(四)殭屍網路(Botnet)

在陳勝裕研究提出殭屍網路攻擊為現今網路環境中危害最深的攻擊方式之一，為受到感染的電腦所組成之群體，除受害的電腦主機資料會遭竊外，控制者亦會利用殭屍電腦，透過特徵及通訊策略改變等方式，以規避追緝，並進行非法行為(如 DDoS 攻擊、傳送病毒或垃圾郵件，以及竊取銀行授權憑證或信用卡號碼等個人重要資訊)，成為資安人員最迫切防護的議題。[2]在 2016 年的殭屍網路(Mirai)造成全球多起大規模 DDoS 攻擊事件，攻擊流量超過 1Tbps，創下近年來最高攻擊流量，臺灣亦為 10 大來源國之一。

(五)資料外洩

---

[1] 林紹驊，〈防禦 DDoS 攻擊之異質性追蹤器部署〉，中華大學資訊工程學系碩士論文，民國 103 年，頁 1。
[2] 陳勝裕，〈植基於網域查詢群體行為相似度之殭屍網路偵測機制〉，國立成功大學電腦與通信工程研究所碩士論文，民國 103 年，頁 6。

資料外洩事件，通常是駭客直接進入組織，或破壞網路安全防禦入侵組織內部，或迫使內部人員，直接或間接取得組織內部資料。呂軍儀在研究中提及現今組織內部人員造成資料外流問題日趨嚴重，為避免造成資料外洩事件，可藉個案研究之方式，依據 NIST SP800 及 ISO 27001 國際標準規範，建置中端型資料外洩防護(Data Loss Prevention, DLP)管控機制，以確保資訊安全。[3]

(六)網頁入侵

網頁入侵是指攻擊者藉瀏覽器，針對網頁伺服器發送特定的請求字串，獲得系統重要資料，進而對伺服器進行各種入侵行為(如隱碼攻擊及注入攻擊等)。王茂吉在研究中提出網頁入侵是最常遭受攻擊的網路攻擊，網頁伺服器之應用型入侵偵測系統應以「偵測異常行為偵測」為主，「錯誤行為偵測」為輔，始可偵測已知攻擊行為，並預防新式攻擊事件。

(七)設備故障

蕭仲辰研究提及災害總是在無法預警的情況下發生，發生時也會造成資訊系統停擺，建立異地備援系統是為了讓組織能夠營運而不中斷，現行異地備援機制多著重軟體備援方面，然而硬體備援設備的管理才是備援機制的關鍵成功因素。

(八)整合威脅管理

姜緝熙及林應穩兩位研究者針對現今網路攻擊手法日新月異，組織對資訊安全防護之要求也須不斷改變，具備整合威脅管理(Unified Threat Management, UTM)裝置才有辦法面對多變的攻擊手法。UTM 裝置則需具備防火、入侵偵測(防禦)、閘道防毒及虛擬私人網路(Virtual Private Network, VPN)等整合威脅管理功能。[4]

(九)小結

網路上的惡意者為了達成攻擊破壞或入侵竊取等目的，攻擊手法會隨著資訊科技進步而複雜化，行為是連續且不曝露其蹤跡的，資安威脅的來源也不僅是駭客攻擊，天然災害、設備中斷或人員操作等都可能是威脅，造成設備損壞、系統停擺或資料外流等情形，除了政策的訂定及人員的管理外，最普遍且基本的防護方式為因應各式攻擊手法，建置相關資安防護設備，或者演變為整合型防護設備，當然，備援設備的建置也是相當重要的手段；吳世璋在針對評估國軍網路資料中心資安防護能力研究中，以德爾菲法及層級分析法進行歸納研析，結果亦發現「設備建置」為最高權重。

## 二、資安政策與人員資安素養重要性研析

(一) 資安政策

[3] 呂軍儀，〈一個基於終端型 DLP 的資訊安全管理系統 -以 IC 設計公司為例〉，國立交通大學管理學院資訊管理學程碩士論文，民國 103 年，頁 14。

[4] 林應穩，〈破壞式創新對網路安全產業之影響〉，國立臺灣大學工業工程學研究所碩士論文，民國 105 年，頁 28。

1.資安治理成熟度評估

「105 年國家資通安全防護整合服務計畫」經研析政府資安法規及相關國際標準，訂定 A、B 及 C 級政府機關資安治理架構。[5]黃紅姣透過個案研究方式，以資安治理成熟度來評估政府機關的資安治理情形，衡量內部人員面對新的機制所產生抗拒與不信任感，機關應採取適當應對方式，使人員接受且落實於日常工作中，個案之資安治理成熟度評估，可作為政府資安政策策訂之參考。[6]

2.ISO 27001：2013 資訊安全管理系統認證

ISO 27001 為資訊安全國際認證標準，源起於 2005 年，為 ISO 27001：2005，歷經 8 年後改版為 ISO 27001：2013。林春吟於研究中以通過 ISO 27001:2013 之政府機關為案例，分析 ISO 27001 新舊標準之差異部分及相關資安管控作為，產生轉版後組織所面對的問題及其解決方法，期能提供各組織實施轉版之參考，協助組織繼續持有資訊安全管理系統認證，共同維護資訊安全。

3.BS 10012：2009 個人資訊管理系統規範

英國標準協會於 2009 年公布任何組織均可適用的「個人資料保護管理系統 (Personal Information Management System, PIMS) BS 10012：2009 標準」，以確實保護個人資料。鄭伊雯於研究中表示，「個人資料保護法」於 99 年立院三讀通過，個人資料保護成為重要的議題，透過比對 ISO 27001 資訊安全管理系統認證與 BS 1002 個人資訊管理系統規範條文之差異，建立以 ISO 27001 為基礎並符合 BS 10012 標準之自我評鑑模式。

4.OCTAVE-S 風險評估方法

資安風險評估執行程序(Operationally Critical Threat, Asset, and Vulnerability Evaluation, OCTAVE)為美國卡內基美隆大學(Carnegie Mellon University, CMU)所發展的資安風險評估方法。陳亮僖於研究提及，現今組織針對資訊安全風險評估大多存在過程過於繁瑣且耗時費力、評估多偏定性分析難以提供客觀評估環境，以及缺乏專業資安風險評估人員管控評估過程，運用 OCTAVE-S 風險評估方法，結合層次分析法及情境模擬，可建立一種快速且定量化的資安風險評估方法。

5.COBIT 5 資訊與相關技術控制目標

美國資訊系統審計與控制協會(ISACA)於 1992 年創建資訊與相關技術控制目標 (Control Objectives for Information & Related Technology, COBIT)，提供資訊管理測量架構，為使組織利益最大化。陳昱安以 COBIT 5 為基礎，針對雲端運算環境建構資訊治

[5] 財團法人資訊工業策進會，《資安治理成熟度評審使用手冊》，國家資通安全防護整合服務計畫，民國 106 年，頁 2。

[6] 黃紅姣，〈政府機關資安健康檢查-資安治理成熟度評估〉，國立臺灣科技大學資訊管理系碩士論文，民國 105 年 6 月，頁 1。

理的機制，以利企業在導入雲端運算環境後，對於資訊治理制度調整部分，避免產生相關問題。

6.小結

資安治理成熟度評估、資安風險評估，資安、技術及個人資料國際認證標準，皆可作為資安政策發展的依據，但機制對於組織的適用性甚為重要。鄭博心研究提出，目前各單位資安政策存在一體適用的普遍性，常造成不符合該組織、任務需求的情況，為提升資訊安全，必須以「適合的」資訊安全政策為基礎。

(二) 資安素養

1.高階主管支持

翁文宏在基於國際資訊安全稽核規範(BS7799)，以高階主管支持、資訊倫理及資訊安全管控等面向，建構與資訊安全之關聯性，發現高階主管支持有顯著影響。[7]林宇溱在資訊安全政策導入資訊安全管理系統認證(ISO 27001)關鍵成功因素之研究中，亦發現高階主管乙項有顯著影響。

2.全體員工積極參與

洪智力研究發現因應近年來資安威脅，大部分組織紛紛導入資訊安全系統，聚焦在通過 ISO 27001 認證之組織，以 AHP 層級分析法找出，全體員工共同參與為導入 ISO 27001 之關鍵成功因素。[8]

3.具資安專業人員

翁燕秋經研究發現政府部門導入資安管理系統之關鍵成功因素為：具資安專業人員、高階主管支持、全體員工積極參與及提供完善教育訓練，將會產生降低重大資訊外洩、改善資訊安全環境及提升資安防護能力等效益。

4.資安人員工作敬業度

徐敏耕在研究中利用橫斷研究法，針對工作壓力、工作投入及工作滿意度等構面，探究醫療資訊人員工作情形及 3 個構面的關係，並以 SPSS 軟體進行分析統計，結果發現人員具有較高的敬業度及工作認同，則能有效提高組織運作效能。[9]

5.完善教育訓練

高勇明之研究為明瞭組織員工對資訊安全教育接受度，並以 SPSS 軟體分析，結果發現規劃完善的教育訓練，並使人員樂意接受，建立人員正確的資安素養，效益

[7]翁文宏，〈資訊倫理、資訊安全控管與高階主管支持對資訊安全之影響〉，崑山科技大學企業管理研究所碩士論文，民國 98 年，頁 33。

[8] 洪智力，〈資訊安全規範影響因素評估〉，中原大學資訊管理研究所碩士論文，民國 105 年，頁 42。

[9] 徐敏耕，〈醫療資訊人員工作投入、工作壓力及工作滿意度之探討〉，亞洲大學資訊多媒體應用學系碩士論文，民國 102 年 11 月，頁 105。

遠大於獎懲制度規範。[10]

6.鑑識能力培育

陳啟中現今為資訊網路時代，國軍對外面臨駭客攻擊，對內須慎防洩(違)密事件，除須建制完善的資安防護體系外，加強資安鑑識能力培育亦是刻不容緩的要務。[11]

7.小結

對資安的理解與認知，以及對資安的內、外在能力，或對資安有幫助的作為，皆可稱為資安素養，資安素養對資安實施影響甚大，舉凡高階主管的支持，全體員工的參與，資安人員具備與否及其敬業度，還有完善的資安專業教育訓練，皆可提升組織的資安防護效能；蘇世宏在研究中以 SPSS 軟體工具，透過因素分析及積差相關分析等統計學方法，分析空軍人員資訊安全素養現況，及其人員背景因素、政策與組織影響資安實施之研究，發現人員資安素養與影響資安實施的積差相關分析達中度顯著相關。

## 三、提升網路資安防護效能發展趨勢

(一) 資料探勘技術應用

資料探勘是運用統計學理論，透過人工智慧或機器學習的方法，在資料庫中進行演算，以蒐集相關資料的過程。魏道楠在研究中提及學者認為在攻擊生命週期，蒐集並分析資料關聯性是有效的防護策略，入侵偵測為良好的解決方法，資料探勘技術則為優化入侵偵測適合的應用方式。

(二) 雲端資料加密與金鑰管理

李明陽於研究中提及雲端的廣泛使用，帶給使用者存取資料的便利性，為確保資料保存安全，可使用進階加密標準(Advanced Encryption Standard, AES)進行加密上傳，並運用金鑰管理機制，可安全且有效地傳輸資料及管理金鑰，使機敏資料獲得保障。進階加密標準是美國國家標準與技術研究院(National Institute of Standards and Technology, NIST)於 2001 年所提出的對稱加密演算法，已經多方驗證且廣為全世界所使用。

(三) 蜜罐技術運用

蜜罐是指用來偵測、抵禦駭客攻擊的陷阱，其原理類似誘捕昆蟲的蜜罐。謝宏業在研究中整合了蜜罐技術與入侵偵測系統(Snort)，建置一個配合防火牆能防禦網內或網外攻擊的系統。利用蜜罐技術模擬實體機進行誘捕，並與實體機進行地址解析協議(Address Resolution Protocol, ARP)交換，根據黑名單與 Snort 實施整合，達到區域聯防

[10] 高勇明，〈探討特定機關員工對資訊安全教育〉，華梵大學資訊管理學系碩士論文，民國 101 年，頁 1。
[11] 陳啟中，〈國軍電腦鑑識專業人才培訓之研究〉，國防大學管理學院資訊管理學系碩士論文，民國 99 年，頁 56。

的效果。

(四) 資料庫活動監控

吳翊郡研究提及資料庫活動監控(Database Activity Monitoring, DAM)主要是根據組織網路架構，從應用平臺與終端設備等，來分析資料庫各系統構成因素，並依據結構化查詢語言(SQL)記錄判定為資安事件，以完善稽核作業，提升資安防護效能。[12]

(五) (五)自動偵測非法連線

葉毓輝研究提出現今防火牆及入侵偵測系統等防護設備，雖可防護外部攻擊行為，但這些設備對內部有心人員蓄意以假冒網址連線，卻無法防範。運用 ARP 數據監聽器(ARP WATCH)結合動態主機配置協定(Dynamic Host Configuration Protocol, DHCP)方式，可建立一套自動偵測非法 IP 連線並進行阻擋之系統，以減少資安罅隙。

(六) 小結

資安即國安，不堪一擊的網路防護，等同於沒有戰力的國防，因應現今瞬息萬變的駭客攻擊手法，運用技術方法建構與時俱進的防護機制，為組織需關切的重要議題。因此，基於資安相對重要的原因下，駭客的攻擊手法又多變詭譎，單靠基礎的防護設備恐無法做到萬無一失，必須依賴資料探勘、雲端資料加密、蜜罐技術、資料庫監控及非法連線偵測等新穎的科技方法，來增強防禦縱深，落實資安防護。

## 四、資安防護效能提升評估要項歸納

蒐集針對影響網際網路資安防護相關文獻，並依據上述各小結，綜整出 4 個關鍵面向為：防護設備、資安政策、資安素養及技術方法，即為本研究運用 AHP 法之主層面。接著針對各層面相關參考文獻進行研析與比對，並重新分類及命名，向下發展為各次要素，將分述如後。

(一) 防護設備主層面

針對所蒐集之相關文獻，就屬於防護設備部分進行分類，並命名為次要素，說明如後：

1.APT 防護設備：季祥於〈APT 攻擊對企業資安政策之影響〉研究中，提及進階持續性威脅攻擊的嚴重性。

2.DDoS 防護設備：林紹驊於〈防禦 DDoS 攻擊之異質性追蹤器部署〉研究中，提及分散式阻斷服務攻擊的嚴重性。

3.防毒系統：陳信綸於〈勒索病毒行為與防治措施之研究〉，以及陳勝裕於〈植基於網域查詢群體行為相似度之殭屍網路偵測機制〉研究中，分別提及勒索病毒與殭屍網路的嚴重性。

[12] 吳翊郡，〈資料庫活動監控系統之企業應用與商機擴展之研究〉，國立臺灣科技大學管理研究所碩士論文，民國 102 年，頁 43。

4.DLP 設備：呂軍儀於〈一個基於終端型 DLP 的資訊安全管理系統-以 IC 設計公司為例〉研究中，提及資料外洩的嚴重性。

5.WAF 防護設備：王茂吉於〈適用於網頁伺服器之應用型入侵偵測系統〉研究中，提及網頁入侵的嚴重性。

6.備援設備：蕭仲辰於〈運用 IPMI 建構異地備援系統之研究〉研究中，提及設備故障的危害性。

7.UTM 裝置：姜緝熙於〈中小企業整合威脅管理裝置遴選策略之研究〉，以及林應穩於〈破壞式創新對網路安全產業之影響〉研究中，均提及整合威脅管理裝置的重要性。

(二) 資安政策主層面

針對所蒐集之相關文獻，就屬於資安政策部分進行分類，並命名為次要素，說明如後：

1.資安治理成熟度評估：黃紅妏於〈政府機關資安健康檢查-資安治理成熟度評估〉研究中，提及資安治理成熟度評估的重要性。

2.資訊安全管理認證：林春吟於〈ISO 27001:2013 轉版探討－以某政府機關為例〉研究中，提及 ISO 27001:2013 資訊安全管理系統認證的重要性。

3.個人資訊管理規範：鄭伊雯於〈植基於 ISO 27001 建立符合 BS 10012 之個人資訊管理自我評鑑模式〉研究中，提及 BS 10012：2009 個人資訊管理規範的重要性。

4.風險評估方法：陳亮僖於〈快速實現資安風險評估之研究〉研究中，提及 OCTAVE-S 風險評估方法的運用性。

5.資訊技術控制目標：陳昱安於〈雲端運算環境資訊治理機制之研究-以 COBIT5 為基礎〉研究中，提及 COBIT 5 資訊與相關技術控制目標的運用性。

(三) 資安素養主層面

針對所蒐集之相關文獻，就屬於資安素養部分進行分類，並命名為次要素，說明如後：

1.高階主管支持：翁文宏於〈資訊倫理、資訊安全控管與高階主管支持對資訊安全之影響〉，以及林宇溱於〈資訊安全政策導入 ISO 27001 之關鍵成功因素探討〉研究中，均提出高階主管支持的重要性。

2.全體員工參與：洪智力於〈資訊安全規範影響因素評估〉研究中，提及全體員工積極參與的重要性。

3.具資安人員：翁燕秋於〈政府部門導入資訊安全管理系統之分析〉研究中，提及具資安專業人員的重要性。

4.資安人員敬業度：徐敏耕於〈醫療資訊人員工作投入、工作壓力及工作滿意度

之探討〉研究中，提及資安人員工作敬業度的重要性。

5.教育訓練：高勇明於〈探討特定機關員工對資訊安全教育〉，以及陳啟中於〈國軍電腦鑑識專業人才培訓之研究〉研究中，分別提及完整教育訓練及鑑識能力培育的重要性。

(四) 技術方法主層面

針對所蒐集之相關文獻，就屬於技術方法部分進行分類，並命名為次要素，說明如後：

1.資料探勘：魏道楠於〈基於資料探勘技術應用於網路異常偵測〉研究中，提及資料探勘技術應用的重要性。

2.資料加密：李明陽於〈雲端資料加密與金鑰管理之研究〉研究中，提及雲端資料加密與金鑰管理的重要性。

3.蜜罐技術：謝宏業於〈以 HoneyPot 及 Snort 為基礎之網路入侵與攻擊偵測系統〉研究中，提及蜜罐技術的運用性。

4.資料庫監控：吳翊郡於〈資料庫活動監控系統之企業應用與商機擴展之研究〉研究中，提及資料庫活動監控的重要性。

5.非法連線偵測：葉毓輝於〈自動偵測非法連線及資安監控機制〉研究中，提及自動偵測非法連線的重要性。

(五) 小結

透過文獻蒐集與研析，依據後備指揮部網際網路資安防護不足之研究動機，找出提升資安防護效能之關鍵因素為：防護設備、資安政策、資安素養及技術方法等 4 項，為運用 AHP 法統計之主層面。在防護設備主層面部分區分 APT 防護設備、DDoS 防護設備、防毒系統、DLP 設備、WAF 防護設備、備援設備及 UTM 裝置等 7 項次要素；在資安政策主層面部分區分資安治理成熟度評估、資訊安全管理認證、個人資訊管理規範、風險評估方法及資訊技術控制目標等 5 項次要素；在資安素養主層面部分區分高階主管支持、全體員工參與、具資安人員、資安人員敬業度及教育訓練等 5 項次要素；在技術方法主層面部分區分資料探勘、資料加密、蜜罐技術、資料庫監控及非法連線偵測等 5 項次要素，以做為設計專家訪談問卷，建構 AHP 法層級架構之參據。

## 研究方法與設計

經文獻探討後，建立之主層面及次要素，透過專家訪談問卷，確立層級架構，並運用分析層級程序法設計 AHP 問卷，將問卷結果以軟體產出各準則之權重。第一段將介紹研究方法，第二段為層級架構流程設計。

### 一、研究方法

現今複雜社會中，會面臨到許許多多的抉擇，日常生活的食、衣、住、行，求學或就業階段，甚至政府或企業組織的決策者，都會遇到須考量哪個條件比哪個條件好的問題，決策者將各種條件納入考量範圍，加以抉擇，稱多準則決策(Multiple Criterion Decision-Making, MCDM)。面臨多準則決策的問題，通常運用德菲(Delphi)法、因素分析(Factor Analysis)法及運用分析層級程序法。AHP 法可化繁為簡地將複雜且不同層面的準則，經專家評估後，以數據方式表現出優劣，為多準則決策中一種良好的方法，故本研究將運用 AHP 法來決定提升後備指揮部網際網路資安防護效能之準則的優先順序，並提供最適化的建議，以下將簡要介紹 AHP 法。

(一) 分析層級程序法簡介

AHP 法為 1971 年美國匹茲堡大學教授 Thomas L. Saaty 參與美國國防部應變計畫研究時所提出，經過多年的應用、修正與變革，直到 1980 年 Saaty 始將整個理論更臻完備。[13]是應用在具多數準則的決策問題上，透過擷取專家或高層的意見，建立層級結構，運用評量尺度方式，將主觀的意見加以量化，表現出優劣順序的結果或方案。

(二) 分析層級程序法的運用

AHP 法常被應用於決定優先等級、決定需求、預測結果、評量績效、規劃、分配資源、最佳化、產生替代方案、選擇最佳政策、設計系統、確保系統穩定、解決衝突、風險評估等 13 類決策問題。

(三) 分析層級程序法之層級架構

層級架構的建立是將要素加以分解成數個群，每個群再區分成數個次群，以建立完整的層級架構。層級種類可分為完整層級與不完整層級 2 種，完整層級每個上、下層的要素均具有關聯性，為完整的連線；不完整層級並非每個上、下層的要素具有關聯性，可以處理眾多分歧的問題。

(四) 分析層級程序法之評估方式

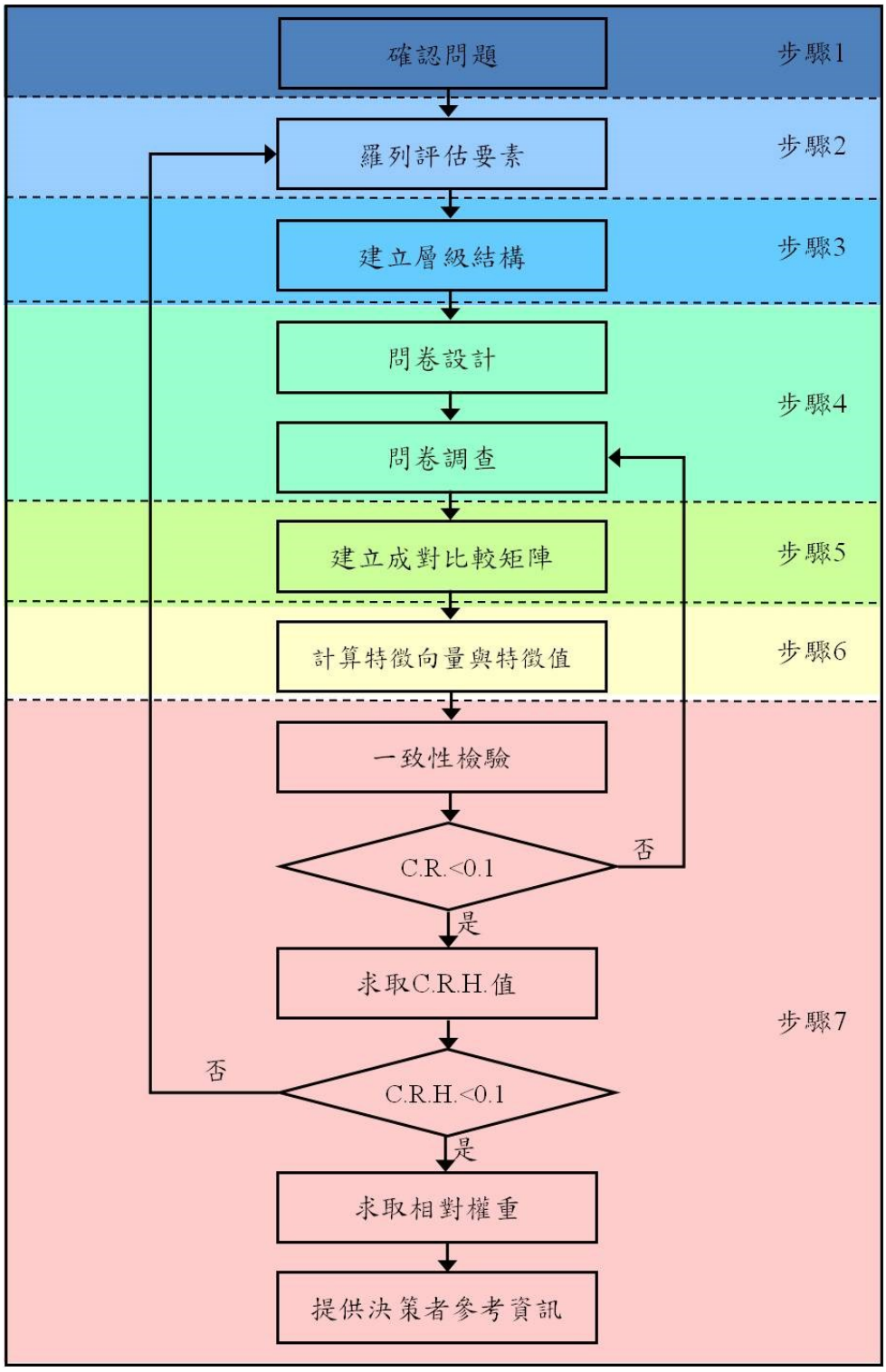
AHP 法在建立層級架構後便要進行評估工作，評估方式是以某一層級中的 2 個要素，依上一層要素為基準，分別評估這 2 個要素對基準的重要性或關鍵程度；各要素兩兩進行比較，來評估相對重要性，評估尺度區分為同等重要、稍重要、頗重要、極重要及絕對重要，並以 1、3、5、7、9 來表示，2、4、6、8 則代表相鄰尺度的中間值。以 AHP 法處理複雜問題進行評估時，可分為以下 7 個程序步驟(如圖一)。

## 二、層級架構流程設計

層級架構流程區分「層級架構建立」及「主、次準則權重確立」等 2 階段做設計，分述如後：

[13]王興國，〈科學工業園區開發工程分標原則之研究〉，國立交通大學工學院碩士在職專班營建技術與管理學程碩士論文，民國 95 年，頁 24。

圖一 AHP 法程序步驟




資料來源：作者繪製。

(一) 層級架構建立

本階段首先透過文獻蒐集所歸納的主層面及次要素，經由設計專家訪談問卷，藉由專業意見篩選成為主、次準則，建立提升後備指揮部網際網路資安防護效能評估要素之層級架構。

1.評估要項歸納

本研究以文獻蒐集方式，針對提升網際網路資安防護效能相關文獻做蒐集及研析，透過分類、比對及命名，訂為運用 AHP 法之主層面及次要素，計有防護設備、資安政策、人員資安素養及技術方法等 4 項主層面，其中防護設備主層面包含 7 項次要素、資安政策包含 5 項次要素、人員資安素養包含 5 項次要素，技術方法包含 5 項次要素，合計 22 項次要素(如表一)。

表一 評估要項彙整表

| 目標 | 主層面 | 次要素 |
|---|---|---|
| 提升後備指揮部網際網路資安防護效能之研究 | 防護設備 | 1.APT 防護設備。2.DDoS 防護設備。3.防毒系統。4.DLP 設備。5.WAF 防護設備。6.備援設備。7.UTM 裝置。 |
| | 資安政策 | 1.資安治理成熟度評估。2.資訊安全管理認證。3.個人資訊管理規範。4.風險評估方法。5.資訊技術控制目標。 |
| | 人員資安素養 | 1.高階主管支持。2.全體員工參與。3.具資安人員。4.資安人員敬業度。5.教育訓練。 |
| | 技術方法 | 1.資料探勘。2.資料加密。3.蜜罐技術。4.資料庫監控。5.非法連線偵測。 |

資料來源：作者繪製。

2.專家訪談

根據文獻蒐集法所訂之主層面及次要素，透過專家訪談方式，以增加主、次準則之可信度。提升後備指揮部網際網路資安防護效能之研究的專家訪談，範圍設定為後備指揮部上級政策業管單位國安會資訊安全辦公室及國防部通次室資安處，技術支援單位國防大學電算中心、中科院資通所、資通電軍指揮部網戰整備處與網路戰聯隊，以及後備指揮部政策業管單位動管處資管科，並指定針對網際網路資安防護具備經驗豐富且績效卓越人員為對象，共計邀請 10 位專家進行訪談(如表二)，專家訪談問卷主次準則勾選表如表三。

表二 資安防護專家背景

| 項次 | 服務單位 | 階級職務 | 最高(或軍事)學歷 | 年資 |
|---|---|---|---|---|
| 1 | 國安會資安辦公室 | 少將主任 | 博士/戰院(略)教育 | 28 |
| 2 | 國防部通次室 | 中校資參官 | 碩士/指參教育 | 18 |
| 3 | 國防部通次室 | 少校資參官 | 碩士/指參教育 | 17 |
| 4 | 國防大學電算中心 | 中校資參官 | 大學(專科)/正規班 | 17 |
| 5 | 中科院資通所 | 聘用技正 | 碩士/指參教育 | 30 |
| 6 | 中科院資通所 | 助理研究員 | 碩士/指參教育 | 12 |
| 7 | 資通電軍網戰處 | 中校副處長 | 碩士/指參教育 | 20 |
| 8 | 資通電軍網戰聯隊 | 中校副主任 | 碩士/指參教育 | 20 |
| 9 | 後備指揮部資管科 | 上校科長 | 博士/戰院(略)教育 | 22 |
| 10 | 後備指揮部資管科 | 中校資參官 | 碩士/指參教育 | 20 |

資料來源：作者繪製。

表三 專家訪談問卷主次準則勾選表

**確立提升後備指揮部網際網路資安防護效能主次準則**

本問卷目的旨在瞭解文獻探討中所獲得之提升後備指揮部網際網路資安防護效能評估要項(確立主、次準則)的必須性。請您就所認為後備指揮部網際網路資安防護效能提升之必須性項目予以評選，並在□內打勾(V)：

(一)防護設備：

| 防護設備(主層面建議修改名稱為：　　) | | |
|---|---|---|
| 次要素評估項目 | 必須性(複選) | 建議修改項目名稱 |
| APT 防護設備 | □ | |
| DDoS 防護設備 | □ | |
| 防毒系統 | □ | |
| DLP 設備 | □ | |
| WAF 防護設備 | □ | |
| 備援設備 | □ | |
| UTM 裝置 | □ | |
| 建議增加其他評估項目： | | |

(二)資安政策：

| 資安政策(主層面建議修改名稱為：　　) | | |
|---|---|---|
| 次要素評估項目 | 必須性(複選) | 建議修改項目名稱 |
| 資安治理成熟度評估 | □ | |
| 資訊安全管理認證 | □ | |
| 個人資訊管理規範 | □ | |
| 風險評估方法 | □ | |
| 資訊技術控制目標 | □ | |
| 建議增加其他評估項目： | | |

(三)人員資安素養：

| 人員資安素養(主層面建議修改名稱為：　　) | | |
|---|---|---|
| 次要素評估項目 | 必須性(複選) | 建議修改項目名稱 |
| 高階主管支持 | □ | |
| 全體員工參與 | □ | |
| 具資安人員 | □ | |
| 資安人員敬業度 | □ | |
| 教育訓練 | □ | |
| 建議增加其他評估項目： | | |

(四) 技術方法：

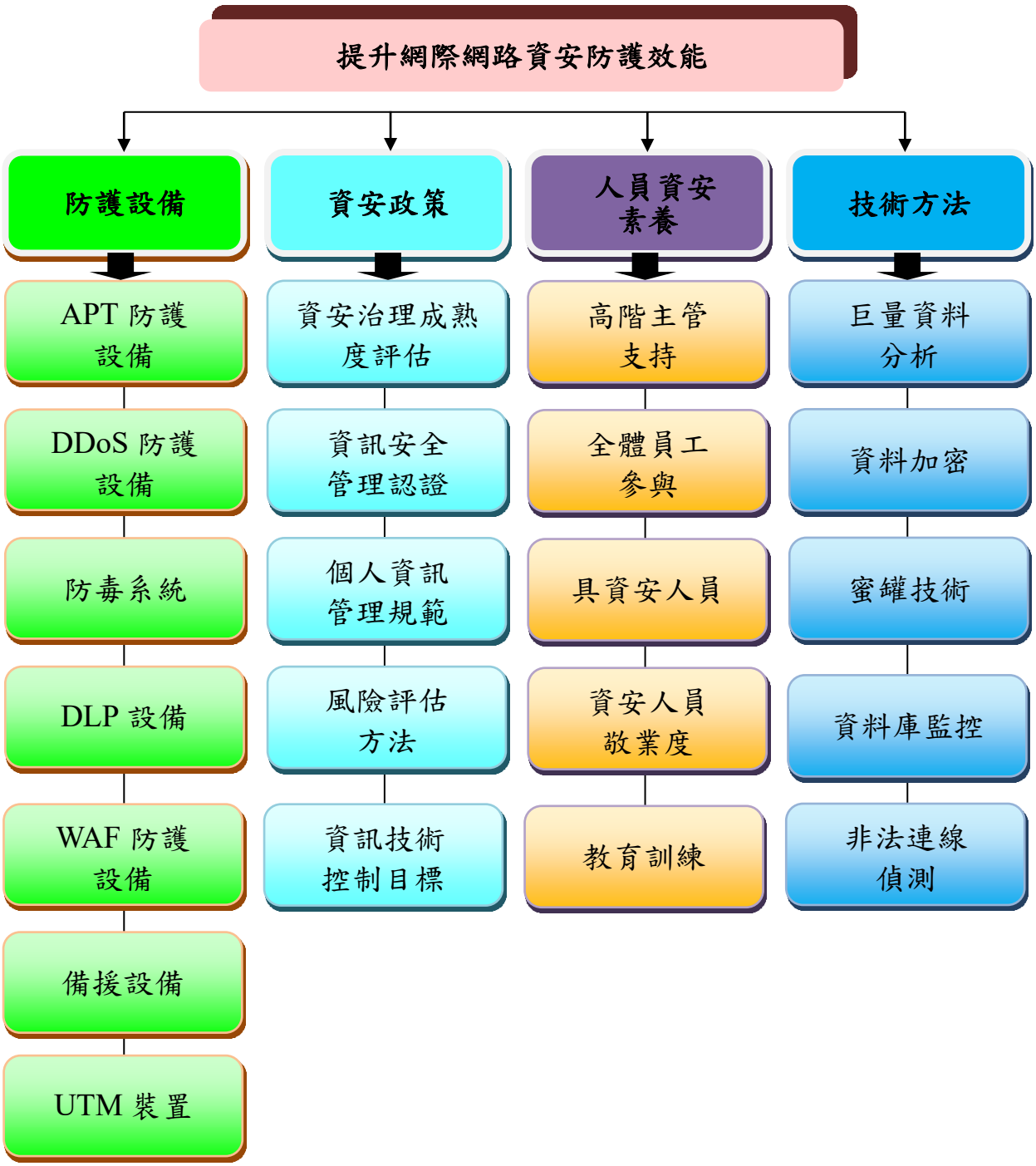
| 技術方法(主層面建議修改名稱為：　　) | | |
|---|---|---|
| 次要素評估項目 | 必須性(複選) | 建議修改項目名稱 |
| 資料探勘 | □ | |
| 資料加密 | □ | |
| 蜜罐技術 | □ | |
| 資料庫監控 | □ | |
| 非法連線偵測 | □ | |
| 建議增加其他評估項目： | | |

資料來源：作者繪製。

3.主、次準則篩選暨層級架構建立

經實施 2 次專家訪談作業，依據專家意見重新修訂評估要項，確認主準則計 4 項及次準則計 22 項。其中，防護設備主準則計含 7 項次準則，資安政策、人員資安素養、技術方法等主準則皆含 5 項次準則。依據所選定之主、次準則，建立提升後備指揮部網際網路資安防護效能之層級架構，可作為運用 AHP 法求得主、次準則權重的參據(如圖二)。

圖二 提升網際網路資安防護效能之層級架構圖




資料來源：作者繪製。

(二)「主、次準則權重確立」

經由專家訪談最終結果所建立之層級架構，設計 AHP 問卷擴大專家訪談之範圍進行調查，並經由 Expert Choice 11 決策分析軟體求得一致性，驗證主、次準則權重，以確立主、次準則權重。

1.AHP 問卷設計

本階段為確立提升後備指揮部網際網路資安防護效能之主、次準則權重，首先透過專家訪談所建立的層級架構，依據 AHP 法設計 AHP 問卷，並擴大專家訪談範圍層級，至後備指揮部、地區及縣市後備指揮部實際從事資安防護業務人員為問卷填寫對象，由填寫者針對主、次準則兩兩進行比較，以利後續利用 AHP 法應用軟體，實施權重驗證及確立。

2. Expert Choice 應用軟體簡介

Expert Choice 為 AHP 法創始人 Thomas L. Saaty 所發展的統計分析工具，運用圖形化界面，提供決策者將複雜的層級架構，經兩兩比較方式，輸入比較數值，經軟體運算後，得到最終的決策結果。其藉由決策者的思維建立出層級架構，並經由決策者兩兩比較反映出重要性的數值，若一個要素變動，其他關係數值則會靈敏地跟著變動，以決定出最後的優劣順序。可應用範圍包含：分析規劃、資源分配、管理人力資源、預測可能結果、選擇替代方案、制定行銷策略、促進群體決策、效益/成本分析、工程設計評估、政策制定與評估、IT 投資管理及創新管理等方面。

## 研究分析結果

第四部分針對發放之 AHP 問卷回收結果運用 Expert Choice 11 軟體實施分析，第一段為問卷資料分析，區分決策、管理、執行及整體等不同階層分析；第二段為綜合分析，針對各主、次準則所得權重比做差異分析，並研析其結果，以作為本研究結論與建議之依據。

### 一、問卷資料分析

本次 AHP 問卷區分決策、管理及執行等 3 個階層進行調查，發放 30 份，回收 30 份，回收率為 100%。其中決策階層對象為後備指揮部上級政策指導業管單位：國安會資通安全辦公室 1 員及國防部通次室資安處 8 員等，實際從事資安防護人員，計 9 員；管理階層對象為後備指揮部管理及其相關研究支援單位：後備指揮部動管處資管科 2 員、國防大學電算中心 4 員，以及資通電軍指揮部 5 員實際從事資安防護人員，計 11 員；執行階層對象為後備指揮部執行及建案執行單位：地區後備指揮部 4 員、縣市後備指揮部 4 員，以及中科院資通所 2 員實際從事資安防護人員，計 10 員。

以 AHP 法應用軟體「Expert Choice 11」檢測回收問卷之一致性，主、次準則中具

Consistency Ratio(C.R.)值>0.1 者則不採用，回收之 30 份問卷，4 份作答時未把握優劣或強度關係之遞移性，為無效問卷；26 份為有效問卷，以 26 份有效問卷為本研究決策體依據。

(一) 決策階層問卷結果分析

1.主準則權重優序分析

決策階層原 9 份 AHP 問卷中，1 份 C.R.值>0.1 不採用，餘 8 份 C.R.值<0.1，表一致性可接受，計算主準則之權重值優序為「人員資安素養」0.396、「技術方法」0.236、「防護設備」0.192、「資安政策」0.177，表示決策階層的受訪者認為「人員資安素養」較其它主準則為重要。

2.各次準則權重優序分析

計算各次準則之權重值，前三優序為「高階主管支持」0.114、「巨量資料分析」0.068、「資料加密」0.064，表示決策階層的受訪者認為，「人員資安素養」主準則中的「高階主管支持」次準則較其它次準則為重要。

(二) 管理階層問卷結果分析

1.主準則權重優序分析

管理階層原 11 份 AHP 問卷中，2 份 C.R.值>0.1 不採用，餘 9 份 C.R.值<0.1，表一致性可接受，計算主準則之權重值優序為「人員資安素養」0.284、「資安政策」0.280、「防護設備」0.271、「技術方法」0.165，表示管理階層的受訪者認為「人員資安素養」較其它主準則為重要。

2.各次準則權重優序分析

計算各次準則之權重值，前三優序為「高階主管支持」0.067、「資安治理成熟度評估」0.066、「風險評估方法」0.065，表示管理階層的受訪者認為，「人員資安素養」主準則中的「高階主管支持」次準則較其它次準則為重要。

(三) 執行階層問卷結果分析

1.主準則權重優序分析

執行階層原 10 份 AHP 問卷中，1 份 C.R.值>0.1 不採用，餘 9 份 C.R.值<0.1，表一致性可接受，計算主準則之權重值優序為「人員資安素養」0.313、「防護設備」0.310、「技術方法」0.229、「資安政策」0.148，表示執行階層的受訪者認為「人員資安素養」較其它主準則為重要。

2.各次準則權重優序分析

計算各次準則之權重值，前三優序為「具資安人員」0.074、「APT 防護設備」0.074、「資安人員敬業度」0.069，表示管理階層的受訪者認為，「人員資安素養」主準則中的「具資安人員」次準則，及「防護設備」主準則中的「APT 防護設備」次準則

較其它次準則為重要。

(四) 整體階層問卷結果分析

1.主準則權重優序分析

整體階層原 30 份 AHP 問卷中，4 份 C.R.值>0.1 不採用，餘 26 份 C.R.值<0.1，表一致性可接受，計算主準則之權重值優序為「人員資安素養」0.313、「防護設備」0.310、「技術方法」0.229、「資安政策」0.148，表示執行階層的受訪者認為「人員資安素養」較其它主準則為重要。

2.各次準則權重優序分析

計算各次準則之權重值，前三優序為「高階主管支持」0.079、「APT 防護設備」0.062、「全體員工參與」0.060，表示整體階層的受訪者認為，「人員資安素養」主準則中的「高階主管支持」次準則較其它次準則為重要。

## 二、綜合分析

發放問卷 30 份，有效問卷為 26 份，區分決策階層 8 份、管理階層 9 份及執行階層 9 份，各階層主、次準則權重及優序分析表如表四，接著針對各主、次準則權重優序實施綜合分析，並提出小結。

表四 各階層主、次準則權重及優序分析表

| 分類 | 項目 | 決策 | | 管理 | | 執行 | | 整體 | |
|---|---|---|---|---|---|---|---|---|---|
| | | 權重 | 優序 | 權重 | 優序 | 權重 | 優序 | 權重 | 優序 |
| 主準則 | 防護設備 | 0.192 | 3 | 0.271 | 3 | 0.310 | 2 | 0.260 | 2 |
| | 資安政策 | 0.177 | 4 | 0.280 | 2 | 0.148 | 4 | 0.198 | 4 |
| | 人員資安素養 | 0.396 | 1 | 0.284 | 1 | 0.313 | 1 | 0.331 | 1 |
| | 技術方法 | 0.236 | 2 | 0.165 | 4 | 0.229 | 3 | 0.210 | 3 |
| 次準則 | APT 防護設備 | 0.055 | 5 | 0.064 | 4 | 0.074 | 1 | 0.062 | 2 |
| | DDoS 防護設備 | 0.023 | 21 | 0.045 | 13 | 0.055 | 5 | 0.038 | 17 |
| | 防毒系統 | 0.033 | 15 | 0.058 | 6 | 0.041 | 15 | 0.042 | 13 |
| | DLP 設備 | 0.023 | 21 | 0.052 | 10 | 0.055 | 5 | 0.040 | 16 |
| | WAF 防護設備 | 0.030 | 18 | 0.054 | 8 | 0.045 | 11 | 0.041 | 15 |
| | 備援設備 | 0.030 | 18 | 0.058 | 6 | 0.061 | 4 | 0.047 | 8 |
| | UTM 裝置 | 0.026 | 20 | 0.049 | 12 | 0.042 | 13 | 0.037 | 19 |
| | 資安治理成熟度評估 | 0.051 | 7 | 0.066 | 2 | 0.024 | 19 | 0.047 | 8 |
| | 資訊安全管理認證 | 0.034 | 14 | 0.054 | 8 | 0.035 | 16 | 0.044 | 10 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 個人資訊管理規範 | 0.046 | 11 | 0.060 | 5 | 0.020 | 21 | 0.042 | 13 |
| | 風險評估方法 | 0.033 | 15 | 0.065 | 3 | 0.019 | 22 | 0.038 | 17 |
| | 資訊技術控制目標 | 0.033 | 15 | 0.033 | 16 | 0.024 | 19 | 0.033 | 21 |
| | 高階主管支持 | 0.114 | 1 | 0.067 | 1 | 0.045 | 11 | 0.079 | 1 |
| | 全體員工參與 | 0.051 | 7 | 0.050 | 11 | 0.055 | 5 | 0.060 | 3 |
| | 具資安人員 | 0.036 | 13 | 0.030 | 18 | 0.074 | 1 | 0.050 | 5 |
| | 資安人員敬業度 | 0.051 | 7 | 0.034 | 15 | 0.069 | 3 | 0.057 | 4 |
| | 教育訓練 | 0.052 | 6 | 0.027 | 20 | 0.052 | 10 | 0.048 | 7 |
| | 巨量資料分析 | 0.068 | 2 | 0.030 | 18 | 0.042 | 13 | 0.043 | 11 |
| | 資料加密 | 0.064 | 3 | 0.039 | 14 | 0.053 | 9 | 0.050 | 5 |
| | 蜜罐技術 | 0.044 | 12 | 0.015 | 22 | 0.026 | 18 | 0.025 | 22 |
| | 資料庫監控 | 0.056 | 4 | 0.021 | 21 | 0.035 | 16 | 0.034 | 20 |
| | 非法連線偵測 | 0.048 | 10 | 0.031 | 17 | 0.054 | 8 | 0.043 | 11 |

資料來源：作者繪製。

(一) 主準則分析

1.決策階層各主準則權重優序為「人員資安素養」0.396>「技術方法」0.236>「防護設備」0.192>「資安政策」0.177。

2.管理階層各主準則權重優序為「人員資安素養」0.284>「資安政策」0.280>「防護設備」0.271>「技術方法」0.165。

3.執行階層各主準則權重優序為「人員資安素養」0.313>「防護設備」0.310>「技術方法」0.229>「資安政策」0.148。

4.整體階層各主準則權重優序為「人員資安素養」0.331>「防護設備」0.260>「技術方法」0.210>「資安政策」0.198。

5.綜上結果，在決策、管理及執行等 3 個階層的受訪者，針對本研究 4 項主準則優先權重排序不盡相同，惟「人員資安素養」為各階層及整體最高優序，代表受訪者皆認為此項較其它 3 項為重要。「人員資安素養」為全體人員對資安的認知、推動的情形及精進的方式，包含「高階主管支持」、「全體員工參與」、「具資安人員」、「資安人員敬業度」及「教育訓練」等次準則，話說萬事起頭難、事在人為，後備指揮部受到國軍「精進案」及「精粹案」兵力調整計畫的影響，資訊人力大幅減少，為提升網際網路資安防護，首先，必須具備專業資安人員及敬業的工作態度，獲得高階主管支持，並透過全體員工共同參與，以及相關教育訓練精進，以上應為「人員資安素養」主準則獲得最高權重的原因。

(二)「防護設備」次準則分析

1.決策階層在「防護設備」主準則之各次準則權重優序為「APT 防護設備」0.251>「防毒系統」0.150>「WAF 防護設備」0.137>「備援設備」0.136>「UTM 裝置」0.117>「DLP 設備」0.105>「DDoS 防護設備」0.103。

2.管理階層在「防護設備」主準則之各次準則權重優序為「APT 防護設備」0.168>「備援設備」0.154>「防毒系統」0.152>「WAF 防護設備」0.142>「DLP 設備」0.138>「UTM 裝置」0.128>「DDoS 防護設備」0.118。

3.執行階層在「防護設備」主準則之各次準則權重優序為「APT 防護設備」0.197>「備援設備」0.164>「DDoS 防護設備」0.148>「DLP 設備」0.147>「WAF 防護設備」0.120> 「UTM 裝置」0.113>「防毒系統」0.110。

4.整體階層在「防護設備」主準則之各次準則權重優序為「APT 防護設備」0.203>「備援設備」0.153>「防毒系統」0.136>「WAF 防護設備」0.134>「DLP 設備」0.131>「DDoS 防護設備」0.123>「UTM 裝置」0.120。

5.綜上結果，在決策、管理及執行等 3 個階層的受訪者，針對本研究「防護設備」之各次準則優先權重排序不盡相同，惟「APT 防護設備」為各階層及整體最高優序，代表受訪者皆認為此項較其它 3 項為重要。「APT 防護設備」為防護進階持續威脅的設備，APT 攻擊具有潛伏期長且匿蹤性高的特點，且近年已演變為將惡意程式藏於更新軟體中，或搭配網頁型木馬之零時差弱點進行攻擊，造成全面性損害，以上應為「APT 防護設備」次準則獲得最高權重的原因。

(三)「資安政策」次準則分析

1.決策階層在「資安政策」主準則之各次準則權重優序為「資安治理成熟度評估」0.258>「個人資訊管理規範」0.236>「資訊安全管理認證」0.172>「風險評估方法」0.168>「資訊技術控制目標」0.167。

2.管理階層在「資安政策」主準則之各次準則權重優序為「資安治理成熟度評估」0.236>「風險評估方法」0.234>「個人資訊管理規範」0.216>「資訊安全管理認證」0.194>「資訊技術控制目標」0.120。

3.執行階層在「資安政策」主準則之各次準則權重優序為「資訊安全管理認證」0.286>「資訊技術控制目標」0.200>「資安治理成熟度評估」0.199>「個人資訊管理規範」0.161>「風險評估方法」0.153。

4.整體階層在「資安政策」主準則之各次準則權重優序為「資安治理成熟度評估」0.232>「資訊安全管理認證」0.217>「個人資訊管理規範」0.204>「風險評估方法」0.186>「資訊技術控制目標」0.161。

5.綜上結果，在決策、管理及執行等 3 個階層的受訪者，針對本研究「資安政策」

之各次準則優先權重排序不盡相同，惟「資安治理成熟度評估」為整體最高優序，代表受訪者皆認為此項較其它 3 項為重要。「資安治理成熟度評估」為行政院依 105 年國家資通安全防護整合服務計畫，為精進政府機關資安治理成熟度評估所訂定的機制，律定 A、B、C 級政府機關，須透過 18 個流程構面，進行資安自我評估，並提出因應措施，可提升資安治理成熟度等級，以上應為「資安治理成熟度評估」次準則獲得最高權重的原因。

另針對「執行階層」受訪者，「資訊安全管理認證」在「資安政策」次準則中獲得最高權重，資訊安全管理認證為 ISO 27001 資訊安全國際認證標準，規範資安國際認證所需具備相關政策、環境、實體、人力及資源等能力，若能達到則可大大提升資安防護效能。

(四)「資安人員素養」次準則分析

1.決策階層在「資安人員素養」主準則之各次準則權重優序為「高階主管支持」0.374>「教育訓練」0.170>「全體員工參與」0.169≧「資安人員敬業度」0.169>「具資安人員」0.117。

2.管理階層在「資安人員素養」主準則之各次準則權重優序為「高階主管支持」0.322>「全體員工參與」0.242>「資安人員敬業度」0.163>「具資安人員」0.143>「教育訓練」0.130。

3.執行階層在「資安人員素養」主準則之各次準則權重優序為「具資安人員」0.252>「資安人員敬業度」0.234>「全體員工參與」0.187>「教育訓練」0.176>「高階主管支持」0.151。

4.整體階層在「資安人員素養」主準則之各次準則權重優序為「高階主管支持」0.269>「全體員工參與」0.205>「資安人員敬業度」0.194>「具資安人員」0.170>「教育訓練」0.162。

5.綜上結果，在決策、管理及執行等 3 個階層的受訪者，針對本研究「資安人員素養」之各次準則優先權重排序不盡相同，惟「高階主管支持」為整體最高優序，代表受訪者皆認為此項較其它 3 項為重要。「高階主管支持」為高階領導者願意支持資安防護的推動，所謂兵隨將轉，若具高階主管支持，相關資安防護政策、設備更換、人員補充等就可藉以推動順遂，以上應為「高階主管支持」次準則獲得最高權重的原因。

另針對「執行階層」受訪者，「具資安人員」在「資安人員素養」次準則中獲得最高權重，可見基層單位對於具備資安防護能力的專業人員較為重視，顯示執行階層資安人力不足之現況。

(五)「技術方法」次準則分析

1.決策階層在「技術方法」主準則之各次準則權重優序為「巨量資料分析」0.242>

「資料加密」0.228>「資料庫監控」0.199>「非法連線偵測」0.172>「蜜罐技術」0.158。

2.管理階層在「技術方法」主準則之各次準則權重優序為「資料加密」0.286>「非法連線偵測」0.226>「巨量資料分析」0.222>「資料庫監控」0.154>「蜜罐技術」0.111。

3.執行階層在「技術方法」主準則之各次準則權重優序為「非法連線偵測」0.258>「資料加密」0.254>「巨量資料分析」0.197>「資料庫監控」0.167>「蜜罐技術」0.124。

4.整體階層在「技術方法」主準則之各次準則權重優序為「資料加密」0.258>「巨量資料分析」0.221>「非法連線偵測」0.219>「資料庫監控」0.173>「蜜罐技術」0.129。

5.綜上結果，在決策、管理及執行等 3 個階層的受訪者，針對本研究「技術方法」之各次準則優先權重排序不盡相同，惟「資料加密」為整體最高優序，代表受訪者皆認為此項較其它 3 項為重要。「資料加密」為透過演算法方式保護資料，以防止內部人員竊取資料，或電腦遭病毒感染致資料外流，且雲端資料加密亦為資料加密重要的一環，以上應為「資料加密」次準則獲得最高權重的原因。

針對「政策階層」受訪者，「巨量資料分析」在「技術方法」次準則中獲得最高權重，防護設備相關資料量龐大，若能以巨量資料分析方法判讀防護資訊，則可迅速、便利、安全地防範於未然。另針對「執行階層」受訪者，「非法連線偵測」在「技術方法」次準則中獲得最高權重，非法連線偵測可自動偵測非法 IP 連線，防止具有網卡的非法資訊設備進入組織內部，國軍現行嚴格管制的營區網路安全管理系統(Base Network System, BNS)，就是非法連線偵測其中之一的方法。

(六) 各次準則整體權重優序分析

1.決策階層各次準則整體權重前三項優序為「高階主管支持」0.114>「巨量資料分析」0.068>「資料加密」0.064。

2.管理階層各次準則整體權重前三項優序為「高階主管支持」0.067>「資安治理成熟度評估」0.066>「風險評估方法」0.065。

3.執行階層各次準則整體權重前三項優序為「具資安人員」0.074≧「APT 防護設備」0.074>「資安人員敬業度」0.069。

4.整體階層各次準則整體權重前三項優序為「高階主管支持」0.079>「APT 防護設備」0.062>「全體員工參與」0.060。

5.綜上結果，「高階主管支持」、「APT 防護設備」及「全體員工參與」等為受訪者認為在 22 項次準則中較為重要的前三項，歸納原因分述如後：

(1)高階主管支持：資安防護效能的提升莫過於從設備、政策、人員及技術等方面來改善，但設備的購買、政策的推動、人員的補實及技術的引進，都需要高階主管的支持，若能取得高階主管的支持，提升資安防護效能的工作就可如魚得水般地進行。

(2)APT 防護設備：APT 攻擊是一種進階式、客製化、潛伏期長，且持續性的威

脅，受害後恐造成資料外流，甚至金錢損失，特別是政府機關、國防軍事及金融商業組織最常被威脅，可見 APT 防護設備或聯防機制的建立是勢在必行的。

(3)全體員工參與：在具備健全資安政策及完善防護設備的環境下，若仍有內部員工一意孤行，不配合政策，刻意或不小心洩漏資料，對單位仍造成嚴重傷害，惟有全體員工共同積極參與，且互相規勸，才能使提升資安防護效能的工作順遂。

## 結論

本研究依據文獻蒐集，彙整評估要項之主層面及次要素，經兩次專家訪談後，訂定主、次準則及層級架構，並透過 AHP 問卷，運用 Expert Choice 11 軟體計算出各主、次準則之權重值，最後將綜整各段落結論，提出結語與建議，以作為後備指揮部提升網際網路資安防護效能之參據。

### 一、實現本研究目標之具體作法

為解決後備指揮部「資安防護設備不足」、「資安人員素質待提升」及「資安政策仍需修訂」等研究動機與窒礙，蒐集相關提升資安防護效能之文獻，以達成掌握防護設備重點，並探討資安政策與人員資安素養重要性等研究目的，經由專家訪談及 AHP 問卷結果，歸納幾點具體作法如後：

(一) 增設 APT 設備及相關防護機制

由於後備指揮部全球資訊網可提供線上申請服務作業，若遭 APT 攻擊，則恐造成個人資料外流之風險，APT 防護因此相對重要。市面上各家廠商已紛紛推出 APT 防護設備，能抵擋 APT 之零時差攻擊或社交工程等，可再依決策模式選擇符合需求之 APT 防護設備。在國軍攻防測試中，原本就有社交工程演練，針對相關防護作為須不斷宣導，且貫徹執行；另國防部通次室之資訊安全通報會發布相關黑名單網址，亦仰賴單位資訊人員確實執行黑名單網址登錄作業，並落實一級輔導一級之資訊安全稽核制度，始能避免遭受 APT 攻擊，造成資安罅隙。

(二) 執行資安治理成熟度評估及資訊安全管理認證

行政院律定 A、B、C 級政府機關須依相關期程完成資安治理成熟度評估，國防部通次室亦會評鑑單位是否完成資訊安全管理認證，資安治理成熟度評估及資訊安全管理認證，兩者皆律定符合成熟度或認證的組織，在資安政策、實體環境及人力技術等方面所須具備的條件。對於後備指揮部來說，執行資安治理成熟度評估時，不可流於形式，並努力積極通過資訊安全管理認證，從學習中獲取經驗，後將經驗傳承至下級單位，落實規劃、執行、檢查、行動(Plan、Do、Check、Act, PDCA)循環模式，做好網際網路資安防護工作，以達「資安即國安」之目標。

(三) 爭取高階主管支持、具資安專業人員及全體員工參與

採購新式資安防護設備，或推動新的資安政策，皆需爭取高階主管支持，若有高階主管支持，具資安專業人員及全體員工參與便有事半功倍之效。後備指揮部應貫徹「資安即國安」的政策，爭取高階主管支持，提升單位資安專業人員之位階，補實單位資安人員之職缺，將後備指揮部、地區及縣市後備指揮部資訊人員交流歷練，充實個人本職學能及經歷，並透過教育訓練、政令宣導，將資安防護意識傳達到全體員工，使全體員工可共同積極參與，以優化網際網路使用環境，提高單位服務聲譽。

(四) 落實資料加密及非法連線偵測作為

資料加密可防止資料遭有心人士竊取，或電腦遭入侵外流；非法連線偵測則可偵測未核准之電腦或網路設備，及早防堵資料外流之風險。後備指揮部現行網際網路雖無加密軟體，惟規定民網電腦不可儲存公務資料，除可研發加密軟體預防外，仍須恪遵網際網路使用規定，另雲端加密演算法運用亦是重要的防護方式；現行國軍網路安全管理系統即為非法連線偵測之作為，惟僅架設於軍網，網際網路亦可效法實施，以達機密性、完整性、可用性之資訊安全管理最終目的。

(五) 運用巨量資料分析及相關聯防機制

當攻擊手法不斷改變，資安防護設備就會隨著增加，異質防護系統就必須整合，才能使資安人員執行防護作業事半功倍，運用巨量資料分析技術，可將各式防護設備的資料檔，加以整合並過濾，使資安人員可快速地瞭解網路環境資訊，進行交叉比對，防止系統與網路產生漏洞。後備指揮部可運用巨量資料分析技術，進行資安事件分析，若未能具備此技術，或經成本考量，則可建請資通電軍指揮部統一購置設備，並依資安事件指管程序，與國軍電腦緊急應變中心(Military Computer Emergency Response Team, MCERT)共同防護，俾達「縱深防禦、區域聯防」之資安架構。

## 二、綜合建議

基於解決後備指揮部「資安防護設備不足」、「資安人員素質待提升」及「資安政策仍需修訂」等窒礙問題與研究動機，本文蒐集現今網路攻擊手法、資安威脅、資安政策及資安防護效能發展趨勢等相關文獻，以達成「掌握防護設備重點」及「探討資安政策與人員資安素養重要性」等研究目的，並透過專家訪談及 AHP 法建立之主次準則、層級架構及權重優序，發展「提升後備指揮部網際網路資安防護效能之研究」的條件與作法。最後，提出以下幾點綜合建議：

(一)恪遵「資安即國安」之國家發展政策

我國於 105 年 8 月 1 日成立行政院資通安全處，並推動「資通安全管理法」於 107 年 5 月 11 日三讀通過，以打造國家級資安制度，針對政府機關及關鍵基礎設施相關企業皆提出明確資安規範。後備指揮部除須恪遵「資安即國安」相關國家發展政策外，可參照本研究針對資安政策面向研析之結果，做好資訊資產及資安防護之風險評

鑑，依機關等級自我落實資安治理成熟度評估，並配合國防部規定，要求各級完成資訊安全管理認證，以確保國土數位安全。

(二)達成「縱深防禦、區域聯防」之資安架構

網路攻擊手法防不甚防，最基本的防護措施為購置新式資安防護設備。依據本研究針對防護設備及技術方法面向研析之結果，且因國軍資安防護建案本由資通電軍指揮部負責，後備指揮部應與資通電軍指揮部溝通協調，建置 APT 防護設備及資安防護相關備援機制，並運用巨量資料分析技術於事件關聯平臺，以避免重複投資浪費資源。另建議網際網路可效法軍網，運用加解密軟體，及營區網路安全管理系統，以落實資料加密及非法連線偵測作為，充實資安防護設備及善用技術方法，並依資安事件處理流程，確遵國軍電腦緊急應變中心聯防機制，俾達成「縱深防禦、區域聯防」之資安架構。

(三)提升資安防護效能促進「全民國防」之理念

後備指揮部負責後備軍人管理、動員、服務及撫卹等相關業務，為長期與民間資訊交流之單位，網際網路資安防護更為其他單位或軍種重要。依照本研究針對資安人員素養面向研析之結果，首先必須爭取高階主管支持，闡述「資安即國安」之理念，增加對提升網際網路資安防護效能之認同，使各級充實專業資安從業人員，透過教育訓練或獎勵機制，增進資安人員之敬業度，向全體同仁透過持續宣導或潛移默化方式，使全體員工共同積極參與提升網際網路資安防護效能之工作，建造良善無虞之軍民數位溝通橋梁，最終達成「全民國防」之目的。

## 參考文獻

一、 國家資通安全會報技術服務中心，〈政府組態基準(GCB)簡介〉，民國 102 年。

二、 經濟部標準檢驗局，〈CNS27001 X6049 資訊技術-安全技術-資訊安全系統-要求事項〉，民國 103 年。

三、 財團法人資訊工業策進會，《資安治理成熟度評審使用手冊》，國家資通安全防護整合服務計畫，民國 106 年。

四、 王茂吉，〈適用於網頁伺服器之應用型入侵偵測系統〉，(中原大學資訊工程研究所碩士論文)，民國 92 年。

五、 王興國，〈科學工業園區開發工程分標原則之研究〉(國立交通大學工學院碩士在職專班營建技術與管理學程碩士論文，民國 95 年)。

六、 李明陽，〈雲端資料加密與金鑰管理之研究〉(育達科技大學資訊管理所碩士論文，民國 105 年)。

七、 吳翊郡，〈資料庫活動監控系統之企業應用與商機擴展之研究〉(國立臺灣科技大

學管理研究所碩士論文，民國 102 年)。
八、 季祥，〈APT 攻擊對企業資安政策之影響〉(中國文化大學商學院資訊管理研究所碩士論文，民國 103 年)。
九、 林新士，〈以資訊科技治理觀點探討國軍資訊安全政策〉(國防大學管理學院資訊管理學系碩士論文，民國 101 年)。
十、 陳亮僖，〈快速實現資安風險評估之研究〉(國防大學理工學院資訊科學碩士班碩士論文，民國 100 年)。
十一、陳昱安，〈雲端運算環境資訊治理機制之研究-以 COBIT5 為基礎〉(國立中正大學會計與資訊科技研究所碩士論文，民國 103 年)。
十二、張登裕，〈資訊安全業務委外關鍵成功因素之研究-以國軍司令部（指揮部）層級為例〉(國防大學管理學院資訊管理學系碩士論文，民國 96 年)。
十三、潘金妮，〈以 ISO/CNS 27001 探討資安管理作為成功關鍵因素之研究-以國軍某單位為例〉(國防大學管理學院資訊管理學系碩士論文，民國 105 年)。

## 作者簡介

李建鵬中校，中正理工學院電機系 87 年班、國防大學管理學院指參班 101 年班，曾任電子官、修護組長、通參官、科長、資參官、電戰官，現任國防大學國防管理學院國管中心教官。

林靳原少校，中正理工學院 93 年班、陸軍通信電子資訊學校通信正規班 96 年班、國防大學理工學院資工系碩士 100 年班，曾任排長、電資官、程設官，現任職國防大學陸軍指揮參謀學院學員。