

# 國防管理學報

第四十三卷 第二期

JOURNAL OF NATIONAL DEFENSE MANAGEMENT

Volume 43, No. 2



創辦人：果 芸

發行人：林 振 裕

出版者：國防大學管理學院

總編輯：張珈進 國防大學資源管理及決策研究所  
(02)28966301#604908  
nduemailtw@gmail.com

技術編輯：鍾秉正 國防大學法律學系  
王中允 國防大學運籌管理學系  
劉憲明 國防大學財務管理學系  
蘇品長 國防大學資訊管理學系  
賴智明 國防大學資源管理及決策研究所

編輯委員：張應中 國防部整合評估司效益評估處  
齊立平 國家中山科學研究院航空研究所

|     |                    |
|-----|--------------------|
| 陳海雄 | 國家發展委員會檔案管理局       |
| 陳宥杉 | 國立臺北大學企業管理學系       |
| 董澤平 | 國立臺灣師範大學全球經營與策略研究所 |
| 郭財吉 | 國立臺灣科技大學工業管理學系     |
| 張譯尹 | 國立臺灣科技大學企業管理學系     |
| 蔡君明 | 國立臺北護理健康大學高齡健康照護系  |
| 孟昭宇 | 國防大學資源管理及決策研究所     |
| 陳勁甫 | 元智大學社會暨政策科學學系      |
| 盧文民 | 文化大學國際企業管理學系       |
| 羅新興 | 健行科技大學企業管理系        |

副總編輯：張臺衛  
國防大學資源管理及決策研究所  
臺北市北投區中央北路2段70號  
(02)28966301#604408  
taiwei661105@gmail.com

副總編輯：嚴國晉  
國防大學資源管理及決策研究所  
臺北市北投區中央北路2段70號  
(02)28966301#604935  
kuochingyen@gmail.com

行政助理：陳正忠  
國防大學管理學院教學支援中心  
臺北市北投區中央北路2段70號  
(02)28966301#604833  
journalofndm@gmail.com

## 【發行宗旨】

為因應學術期刊專業化導向之發展趨勢，並提升學術界對「國防管理」專業學術領域之認定與重視，形成專業特色與重點，樹立「國防管理」專業學術權威，並配合國防管理教育訓練與研究發展需要，提升國軍學術水準與研究風氣，增進軍事院校與民間院校及研究機構學術交流，以「國防管理」相關議題為範疇，對外公開徵稿與發行。



## 【編輯的話】

今年 2 月底發生了全球矚目的俄烏武裝衝突，雖然戰爭是大家最不想看見的，但在烏俄戰爭中仍有許多事件是能讓我國有所借鏡，並反思我國軍事型態及後備戰力等國防管理議題。此外，現行兵役制度為徵募並行制，但招募成效仍有相當進步空間，再者臺灣少子化的問題，所以各界也開始有延長役期或男女皆需服役的討論；這些國防議題的影響層面廣泛，還望各界能針對上述需多加研議之課題進行分析討論並能投稿至本刊，本刊將儘速審查以利研究結果之擴散。《國防管理學報》現行的投稿作法，採〈線上系統投稿〉與〈EMAL 信箱投稿〉雙軌同時並行制，即作者完成系統投稿後，須將 word 稿件(含作者資訊)再寄至「國防管理學報信箱」[journalofndm@gmail.com](mailto:journalofndm@gmail.com)，以加速審稿時效，並避免在系統不穩定時無備份使用。

隨著國防議題重要性的提升與學術環境的轉變，《國防管理學報》的審查政策及原則也在適度地進行調整。我們認為給予具發展潛力的論文有調整改善的機會應該是重要的。審查人主要扮演協助作者改善論文的角色，因此若研究議題具有亮點及貢獻力，將盡量給予作者修改機會。另一方面，考量學術環境的艱辛，本學報不收取刊登費用，同時還對接受刊登的稿件支付作者稿酬，並贈送作者當期學報乙冊，另審查人亦給予相當之審查費用。本學報在新團隊努力下，稿件審查速度已提升許多，並以平均 35 天內完成稿件初審為目標，期望更多作者能考慮本刊投稿。

本期共刊出五篇文章。第一篇〈如何衝破逆境、提升部屬復原力？國軍主管家長式領導的效果檢驗與未來時間觀的調節作用〉一文，係分析家長式領導對基層軍官復原力的影響，並將家長式領導的三個向度：仁慈、威權（專權、尚嚴）與德行領導，分別進行檢視其與復原力的直接關係，除發現仁慈領導與德行領導與基層軍官復原力具顯著正向影響外，亦發現未來時間觀在此間扮之調節角色。從時間觀點出發建議未來訓練單位或管理部門在人員培育和職涯規劃時，納入軍人職業生涯發展的相關課程，引導軍人將時間觀置於未來，將有助提升官兵個人面對挫折的態度與因應能力。

第二篇〈強化國軍雲端服務存取權限機制之設計〉一文，係針對軍種資料交換及國軍雲端服務架構提出透過多因子執行強化自我認證與存取控制，並運用橢圓曲線密碼系統與隨機背包機加密系統可提升安全性與效率。此研究提供建立適當資訊安全防護的參考，除確保我軍資訊傳輸系統具備高安全及高效能，未來亦可針對跨部門資訊系統進行客製化設計與評估運用，達到支援網狀化作戰效益。

第三篇〈植基於最低位元取代與像素差值之資訊隱藏技術〉一文，係提出空間域的最低位元取代法與像素差值之資訊隱藏技術，利用人體視覺系統觀察能力有限的情況下於灰階影像中隱藏秘密訊息。此研究是以 Jung 學者於 2018 年所提出混合 LSB/PVD 藏密法為基礎而改良的資訊隱藏方法；具有較高的藏密量，可有效提升藏密量，同時能維持人眼難以察覺的範圍內，故可提供國防資安管理技術研究領域人員實務應用參考。

第四篇〈政治因素對於預算通過率之影響〉一文，係以民國 83 年至 108 年期間的資料，藉由學理上的整理，探討政治因素及經濟因素對於我國預算通過率及法定預算總金額取自然對數的影響；並發現選舉年度對於總預算通過率將增加，其中又以國防預算通過率增加的影響最大。

第五篇〈大數據治理評量模型與層級關鍵要素之實證研究〉一文，係藉由文獻彙整、問卷設計及專家研討來評量大數據治理所需考量的構面及關鍵因素項目，除建立治理的層級架構外，亦評估各項構面及關鍵因素之影響權重。而國軍近年來朝整合資訊方向努力，且大多以人事、財務、醫療及後勤等方向為主，然而在這些資訊處理的過程中，資料保護及個人隱私等也是系統發展中面臨的首要問題。研究指出在面對巨量資料時代的來臨，世界各國如美國、新加坡及中國大陸近年都已成立國防大數據專屬部門，國軍也同樣面臨國防資訊化及巨量資料的問題，目前尚未有專責的部門負責這項工作的整合，後續國防大數據治理政策的推展是有其必要性。

總編輯 空軍上校 張珈進

國防大學管理學院資源管理及決策研究所 專任教授

111 年 11 月

# 國防管理學報

第四十三卷 第二期

## 目 錄

| <u>篇次</u> | <u>篇 名</u>                                                                                                                                        | <u>作 者</u>        | <u>頁次</u> |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------|
| 1.        | 如何衝破逆境、提升部屬復原力？國軍主管家長式領導的效果檢驗與未來時間觀的調節作用<br>Road to Resilience: The Effects of Paternalistic Leadership and Future Time Perspective on Resilience | 邱保龍<br>廖巍庭<br>陳劭濬 | 1         |
| 2.        | 強化國軍雲端服務存取權限機制之設計<br>The Enhancement of Information Security for the Access Authority of Military Cloud System                                    | 蘇品長<br>黃琮仁<br>蘇泰昌 | 26        |
| 3.        | 植基於最低位元取代與像素差值之資訊隱藏技術<br>An Improved Steganographic Method Based on Least-Significant-Bit Substitution and Pixel-Value Difference                 | 劉興漢<br>賀盛志<br>羅玉芬 | 48        |
| 4.        | 政治因素對於預算通過率之影響<br>The Influence of Political Factor on the Budget Pass Rate                                                                       | 傅澤偉<br>張哲豪        | 68        |
| 5.        | 大數據治理評量模型與層級關鍵要素之實證研究<br>An Empirical Study on the Evaluation Model and Critical Factors of the Big Data Governance                               | 陳良駒<br>余明崇        | 83        |

中華民國一一年十一月



## 如何衝破逆境、提升部屬復原力？ 國軍主管家長式領導的效果檢驗與未來時間觀的調節作用

邱保龍<sup>1\*</sup> 廖巍庭<sup>2</sup> 陳劭濤<sup>3</sup>

<sup>1</sup>國防大學政治作戰學院心理及社會工作學系

<sup>2</sup>國立政治大學商學院企業管理學系

<sup>3</sup>陸軍第六軍團指揮部

論文編號：NM43-01-05

來稿 2022 年 2 月 23 日→第一次修訂 2022 年 3 月 17 日→第二次修訂 2022 年 5 月 30 日→

同意刊登 2022 年 6 月 22 日

### 摘要

復原力是軍人遂行作戰任務不可或缺的能力之一，美軍在實戰經驗中，亦強調復原力是協助個人戰場生存的關鍵。既有國內軍隊研究中，傾向將復原力視為調節因子，探討復原力在軍人工作表現的影響。然而，對於影響復原力的相關因素尚待釐清。本研究採用資源保存理論，探討主管家長式領導對基層軍官復原力的影響，並檢視未來時間觀在兩者之間的調節效果。本研究係採問卷調查法，以陸、海、空三軍之基層軍官為研究對象，區分兩個時間點施測，共蒐集 304 份有效資料。本研究結果顯示：（一）威權領導在區分專權領導與尚嚴領導的情況下，專權領導與復原力具顯著負向關聯，而尚嚴領導與復原力則無顯著關係；（二）主管仁慈領導與德行領導與基層軍官復原力具顯著正向影響；（三）未來時間觀在專權領導與復原力間具負向調節效果，而在仁慈領導與復原力間具正向調節效果，在德行領導與復原力間亦具正向調節效果。最後，根據結果進行討論，並提出實務與研究建議。

**關鍵詞：**復原力、家長式領導、未來時間觀、基層軍官

---

\* 通訊作者：邱保龍 email: paupau1980@hotmail.com

## Road to Resilience: The Effects of Paternalistic Leadership and Future Time Perspective on Resilience

Chiu, Pao-Lung<sup>1\*</sup> Liao, Wei-Ting<sup>2</sup> Chen, Shao-Chun<sup>3</sup>

<sup>1</sup>Department of Psychology and Social Work, National Defense University, Taiwan, R.O.C.

<sup>2</sup> Dept. of Business Administration, National ChengChi University, Taiwan, R.O.C.

<sup>3</sup>The 6th Army Command, R.O.C.

### Abstract

The resilience of soldiers has always been one of the indispensable links in carrying out combat missions. In actual combat experience, the US military also emphasized that resilience is the key to the battlefield to survive. The existing studies of domestic military tend to regard resilience as a moderated factor, and discuss the impact of resilience on the performance of soldiers. The relevant factors that affect resilience have yet to be clarified. Therefore, the researchers want to take the primary military officer as an example to explore whether the paternalistic leadership (benevolent leadership, authoritarian leadership, and virtuous leadership) can affect their resilience and the moderation effect of the future time perspective between the two.

Based on this, this research uses the questionnaire survey method, taking the primary military officers of Army, Navy and Air Force as the research object and is a two-time measurement with a total of 304 valid data and hierarchy regression analysis. The results of the study show that the average resilience score of primary military officers is higher than the median number, indicating that most primary military officers have resilience. In addition, the benevolent leadership and moral leadership have a significantly positive relation with the resilience of primary military officers. In the case of authoritarian leadership, Juan-Chiuan leadership has a significantly negative relation with resilience, while Shang-Yan leadership has no significant relation with resilience; and the future time perspective has a positive moderation effect between benevolent leadership and resilience. There is also a positive moderation effect between moral leadership and the resilience, while there is a negative moderation effect between the Juan-Chiuan leadership and the resilience. Finally, based on the results, this study responds to the status of primary military officers under the social situation of different paternalistic leadership, and the moderation results of the future time perspective between the two, providing practical and research suggestions.

**Keywords:** Resilience, Paternalistic Leadership, Future Time Perspective, Primary Military Officers

---

\* Corresponding Author Email: paupau1980@hotmail.com

## 一、緒論

在自然災害、戰爭、政治衝突的環境下，政府單位和企業組織面臨的社會、經濟、產業環境更加不確定。對公部門的人員來說，必須要隨時有效和迅速因應危機，以持續提供公共服務；在企業組織層面，社會上各行業的人則可能需要不斷轉換工作或被離職。不論是社會上哪一個群體，面對風險社會所帶來的模糊和動盪已是不可避免（Liu, Cooper & Tarba, 2019; Masten, 2019）。許多研究顯示，不論是公務員或是一般企業員工，面對上述的環境變化均帶給他們莫大的挑戰和壓力，導致人員情緒低落、工作倦怠、工作表現下降（Liu, Cooper & Tarba, 2019; Heber et al., 2020; Schuster et al., 2020）。隨著社會變遷、制度更迭，國軍也存在上述類似現象。近年來我國軍隊組織進行重大變革，受人口少子化影響，107年起全面實施募兵制，取消徵兵制（國防部106年度施政計畫，2017）。在新的兵役制度全面實施後，義務役人員大幅度減少，造成軍隊組織人源短缺，致使每個人所需承擔的業務量提升，壓力也隨之變大。其中，一般基層軍官年齡普遍介於22-30歲之間，正處於青年轉至成年的歷程，必須在高壓軍事和多重任務環境下擔任單位領導要職。相較於一般工作職場，其所承擔的責任相對較高，所背負的壓力也最為繁重（胡智筆，2017；洪健文，2010；黃泳睿，2013）。因此，近幾年來，除了工作績效的重視之外，職場正向適應議題也受到許多研究者的關注（如：Branicki, Steyer & Sullivan-Taylor, 2019; Davies, Stoermer & Froese, 2019; Liu, Cooper & Tarba, 2019）。

然而，檢視既有軍人適應研究仍主要檢視壓力來源（如：胡智筆，2017；洪健文，2010；黃泳睿，2013；黃睿瑛，2017）以及壓力所致的負向結果（如：丁華、吳濬廷，2016；吳嘉蓉，2018；黃睿瑛，2017；廖昱絜，2018）。前者的論述多是將壓力與管理連結，認為許多軍隊適應不良、精神困擾或自我傷害者所面對困境時往往是來自單位領導者高壓管理或單位人際互動失衡所致；後者的研究則發現壓力源所造成負向結果，包含自我傷害（丁華、吳濬廷，2016）、環境適應障礙（吳嘉蓉，2018）、工作不滿意（Steffy & Jones, 1988）、乃至於離開職場（陳品傑，2018；黃睿瑛，2017；廖昱絜，2018）。

儘管在壓力和適應的研究累積許多成果，但仍有幾個問題仍待探究。第一，許多研究顯示工作壓力，未必會導致負向結果，也可能有正向結果。其中原因在於個人面對壓力或生活事件所做出的認知評價差異便會導致不同的結果（Lazarus & Folkman, 1984）。此外，Cavanaugh et al.（2000）也指出壓力源可以細分為挑戰型壓力源（challenge stressors）與阻礙型壓力源（hindrance stressors），前者是屬於正向壓力，有助於工作動機提升與滿意；後者的壓力源（如：工作負荷、主管打壓）則可能阻礙個人前進動力。根據資源保存理論的觀點，個人在面對壓力和困境時，「復原力（Resilience）」是最有價值的資源，可以視為個人對抗壓力的能力，以及個人正向價值的來源，也就是，個人在面對壓力源時，能運用內外資源解決困境並且保持專注、承諾和活力（Hobfoll, 2011：517-519）。這也就是復原力，其強調在逆境的威脅，儘管有些人適應不良，但也不乏有些人擁有正向資源而能夠積極面對壓力、戰勝逆境（Werner, 1993）。換言之，有必要瞭解基層軍官復原力，檢視個人何以面對壓力化困境仍能化解或復元。

如同上述所及，既有研究常將軍隊適應不良的原因歸因於單位領導者高壓管理（如：黃睿瑛，2017），但亦有研究顯示個人復原力的關鍵亦在於「領導者」（Masten, 2014）。換言之，究竟組織中的領導對個人在面臨挫折和逆境時所扮演的角色值得深入檢視。復原力是指個人經歷逆境、威脅到個人發展時，個人仍能正向適應

(Luthar, 2006; Masten, 2014)。Smith et al. (2008) 也提出類似看法，認為復原力是個人面對挫折、逆境與壓力的適應能力。Lai & Yue (2014) 進一步指出，個人復原力會因其所擁有的資源不同而有所改變。許多學者亦指出，個人復原力具有可塑性 (malleable)，會隨著個人社會互動中，經由經驗、學習與發展的過程而持續累積或消長 (Block & Kremen, 1996; Branicki, Steyer & Sullivan-Taylor, 2019; Davies, Stoermer & Froese, 2019; Liu, Cooper & Tarba, 2019; Masten, 2019)。在西方既有軍事研究已開始關注此議題。許多學者指出領導模式足以影響軍隊組織各成員、部屬的生活方式與工作表現 (Adler & Lopez, 2019; Qian, et al., 2018; Wang, Liu & Zhu, 2018; Wang, Wang, Chang, 2018; Williams, Parker & Turner, 2010)，其對個人復原力的提升扮演舉足輕重的角色 (Cooper, Wang, Bartram & Cooke, 2019; Lengnick-Hall, Beck & Lengnick-Hall, 2011)。尤其壓力往往會是人在緊張狀態下的負面刺激 (Cullen, Link, Wolfe & Frank, 1985)，然而這種壓力亦可能產生正面的影響，當中領導者的務實態度、公平公正以及嚴格紀律，成為追隨者學習與成就的典範時，讓部屬遇到困難有所依循，足以克服各種任務上的障礙，預期能成就自我、提升工作滿意度降低壓力源的產生，不致於花心思面對不確定環境，因而有助於提升官兵的復原力 (Castro, Adler, McGurk & Thomas, 2006)。基於此，有必要檢視組織層面的領導因素對基層軍官復原力的影響。

值得關注的是，在既有西方研究中，多數為探究正向領導模式。例如：轉換型領導 (Transformational leadership)、交易型領導 (Transactional leadership)、真誠型領導 (Authentic leadership)、謙遜型領導 (Humble leadership) (Bartone, 2006; Bass, 1990; Franken, Plimmer & Malinen, 2020; Gaddy, Gonzalez, Lathan & Graham, 2017; Harland, Harrison, Jones & Palmon, 2005; Macintyre, Charbonneau & O'keefe, 2013; Zhu, Zhong & Shen, 2019)。然而，領導模式會因國家、種族與價值觀的殊異性，而產生不同效應 (Chemers & Ayman, 1993; 林姿葶、鄭伯璫、周麗芳, 2014)。因此，學者開始提倡進行本土研究時，需考量華人文化內涵及社會情境，並提出具三元概念的家長式領導，其涵蓋仁慈、威權與德行等三種領導向度 (鄭伯璫、周麗芳、樊景立, 2000)。家長式領導模式源於儒家思想文化，其特色在於具備類似父權的作風，擁有威權，但也有照顧體諒部屬的情懷以及高度的個人操守 (鄭伯璫等, 2000)。其中，隨著時代與社會的變遷，威權領導在現今價值觀當中，部份理念開始無法被大眾接受，其研究開始思考現代化的轉變。周婉茹等人 (2010) 進一步將威權領導的內涵區分為兩部份，分別為控制人的「專權領導」及控制任務目標的「尚嚴領導」。前者易使部屬發生負面的行為；後者則能促使部屬產生動力，進而提升工作各方便表現 (周婉茹等人, 2014)。為能細緻捕捉威權領導的樣貌，本研究在威權領導的界定和測量採用周婉茹等人 (2010) 的觀點。整體而言，在華人社會家長式領導與部屬復原力的關聯性，目前仍缺少足夠的研究討論。因此，本研究以家長式領導為核心探究，檢視其與基層軍官復原力的關聯性。

在壓力和適應的研究面向，第二個待釐清的便是：基層軍官在主管相同的領導行為之下，何以會有不同的感受與反應產生？亦即，適應結果的個別差異意味著有其他因素調節壓力源和適應不良之間的關聯。部分研究便顯示，在工作職場，高度未來時間觀的人，會在困境中為了達成目標而調整自己的行為，以積極正向的態度，朝向未來邁進 (Husman & Shell, 2008)。因而研究者認為個人所持未來時間觀 (Future Time Perspective) 可能是關鍵要素。未來時間觀是有關個人基於未來的期望和構思，進而對目前所採取的行動與抉擇 (Seijts, 1998)。當個人的未來時間觀越強，越能發展具體的目標，並促使個人投入任務、進行規劃，並全力以赴於實現未來目標的行為 (Husman & Lens, 1999)。根據資源保存理論的觀點，個人特性 (如：正向樂觀、自我效能等) 是個人面對壓力的重要資源，而未來時間觀是一種個人對於未來和當下連結所持的正

如何衝破逆境、提升部屬復原力？國軍主管家長式領導的效果檢驗與未來時間觀的調節作用

向認知評估與行為，因此，對個人而言亦是重要的資源。綜上所述，本研究以資源保存理論探討主管家長式領導對基層軍官復原力的影響，並檢視未來時間觀在兩者之間的調節效果。

## 二、文獻探討

### 2.1 資源保存理論

Hobfoll (1989) 所提的資源保存理論亦指出，個體在壓力情境下的表現，取決於個人所擁有的資源是否足以對抗壓力事件。其所描述的資源：實體資源 (Objects)：如居住環境、個人特質資源 (Personal Characteristics)：如自尊、自我效能、狀況資源 (Conditions)：如社會支持、正向工作氛圍；與能量資源 (Energies)：時間、金錢、健康。在資源運作的過程，個人資源獲得 (Resource Gain) 是經由取得、保存、保護和培養其所看重的資源 (Hobfoll & Lilly, 1993)。相對於資源損失 (Resource Loss) 則是個人遭受資源損失威脅、實際遭遇損失，或者是投入資源卻無法得以回報，這會讓個人心理感受到不適 (Hobfoll, 1989)。換言之，面對逆境時，個人會開始運用所擁有的資源來因應，若資源不斷流失，個人知覺資源不足時，逆境所帶來的壓力即會提升，對個人產生負面影響；若個人能保存既有資源或是有龐大後援時，壓力感就會降低。

在華人的文化底蘊中，領導者最常以家長式領導方式帶領部屬，強調仁慈、威權及德行三種核心要素 (樊景立與鄭伯璜, 2000)，透過對部屬照顧的仁慈領導行為、藉正式獎懲及決策權對部屬嚴格監控的威權領導行為及透過自身形象管理、尊嚴與信心，以及對部屬教育要求的德行領導行為 (樊景立與鄭伯璜, 2000; Farh, & Cheng, 2000)，共同形塑出部屬體會、追隨、信服、景仰與效法行為。根據資源保存理論觀點，主管的領導行為能夠影響部屬所處的情境與效能 (Bartone, 2006; Franken et al., 2020)，為部屬所擁有的狀況資源與能量資源。而家長式領導中的仁慈領導是以關懷、照顧部屬為主，避免部屬陷入危機 (林姿葶、鄭伯璜, 2012)；德行領導則是公私分明、以身作則，以獲得部屬的效法 (樊景立、鄭伯璜, 2000)，兩者屬正向領導方式，可被視為部屬的資源。威權領導展現專權作風、貶抑部屬能力的方式，易使部屬感受自身資源的不足或流失 (周婉茹等, 2010)。因此，根據資源保存理論觀點，主管的領導行為能夠影響部屬所處的情境與效能 (Bartone, 2006; Frank et al., 2019)，因而足以影響部屬所擁有的個人特質資源、狀況資源與能量資源的多寡。以下部分則針對家長式領導與復原力的關係進行假設推導。

### 2.2 家長式領導與復原力

復原力是一種複雜的現象 (Wald, Taylor, Asmundson, Jang & Stapleton, 2006)，其定義也會因研究方向不同而有所差異。Smith et al. (2008) 認為復原力乃是個體面對挫折、逆境與壓力的適應能力。Hobfoll (2011) 從資源保存理論具體指出，在面對壓力源時，復原力是一種對抗壓力的能力，協助個人承受壓力並復元。許多學者亦指出，個人復原力具有可塑性 (malleable)，會隨著個人社會互動中，經由經驗、學習與發展的過程而持續累積或消長 (Block & Kremen, 1996; Branicki, Steyer & Sullivan-Taylor, 2019; Davies, Stoermer & Froese, 2019; Liu, Cooper & Tarba, 2019; Masten, 2019)。因此，本研究所界定復原力乃是採用 Smith et al. (2008) 的觀點，並認為個人復原力會因個體所擁有的資源 (保護因子、風險因子) 不同而有所改變 (Lai & Yue, 2014)。

以下進一步推論本研究所著重的焦點：家長式領導與復原力之關係。在威權領導

方面，周婉茹（2009）研究指出威權領導又區分對人的「專權」領導及對事的「尚嚴」領導。既有研究顯示，當主管展現專權領導時，因其以專權、貶抑部屬能力與斥責部屬的方式帶領部屬，會讓部屬感受壓力、丟臉與不被尊重（吳宗祐，2008；周麗芳等，2006；陳皓怡等，2007；趙安安與高尚仁，2005）、引發部屬憤怒等負向情緒感受（吳宗祐等，2002），甚至部屬的身心健康會產生負面影響（陳皓怡等，2007；趙安安與高尚仁，2005）。此外，專權領導對部屬心理賦能中的意義感、自決感及影響力具有負向效果（周婉茹等，2010），也就是專權領導會消耗個人在工作中的心理賦權。因此，根據資源保存理論推論，當部屬知覺主管「專權」領導時，在不斷貶抑部屬能力與斥責過程，會使部屬感到事情難以掌握與處理、隨之容易緊張、生活易產生無望感，也就是部屬會持續知覺到資源不斷流失和感受自身資源的不足，此會降低個人自尊、挫折感增大，進而加劇個人面對壓力感受，因而無助於個人壓力的因應與逆境克服。因此，本研究推論主管專權領導時會降低基層軍官的復原力，並提出假設 1：

H1：專權領導與基層軍官復原力具負向關聯

在「尚嚴」領導部分，當主管展現尚嚴領導時，對於部屬的工作敬業態度、工作滿意度、助人行為均有正向影響（Chen, 2011；Chou, Chen & Jen, 2005）。周婉茹等（2010）研究亦發現，尚嚴領導能強化個人工作意義、自我效能感及影響力，亦即，尚嚴領導有助於提升個人心理賦能，而心理賦能是個人復原力的重要前置因素（O’Leary & Bhaju, 2006）。簡言之，當主管重視紀律，嚴格要求工作程序，在明確地目標任務下，個人能夠覺察單位所賦予的責任。根據資源保存理論，在工作環境中瞭解自身的角色責任，可以視為一種狀況資源，也就是部屬不用花太多心思面對不確定任務而損耗自己內在資源。當個人在角色和任務明確的狀況下有助於個人工作形塑、問題解決步驟，此會提升個人資源的感知。換言之，當部屬面對逆境時，國軍主管尚嚴領導的過程，便是部屬因應困境一個重要資源和保護因子，因此，本研究提出假設 2：

H2：尚嚴領導與基層軍官復原力具正向關聯

研究發現，在華人家長式領導研究中，當主管展現仁慈領導時，部屬會有被關懷與照顧的感受，覺得自己受主管的支持與鼓勵（周麗芳等，2006；陳皓怡等，2007；陽昊，2017；趙安安與高尚仁，2005；鄭伯璦等，2002）、對部屬的心理健康亦有正面作用（趙安安與高尚仁，2005），且能減緩工作壓力（趙安安與高尚仁，2005）。根據資源保存理論推論，主管的關心、主管的建議、工作績效的回饋（Ashford, Blatt, & VandeWalle, 2003）可以被視為部屬自身的一種資源，並且時常嘗試尋求資源與工作要求間的適配（Demerouti & Bakker, 2014），在資源充足的狀況下，部屬在工作過程會感受到支持和賦權。其中，在個人面對挫折或困境時，來自組織的支持（如：上級）和個人感受到心理賦權是個人復原力重要的前置因素（O’Leary & Bhaju, 2006）。因此，本研究推論主管展現仁慈領導能提升基層軍官的復原力，並提出假設 3：

H3：仁慈領導與基層軍官復原力具正向關聯

在德行領導方面，當主管展現德行領導時，其會以正直、公私分明與以身作則的行為帶領部屬，在華人組織文化中，具高度人治主義傾向（姜定宇等，2012），部屬感受主管對組織每位成員一視同仁，會有較大的安全感，不會擔心自己權益有受損的狀況發生（陳皓怡等，2007；陳盈璇，2018；趙安安與高尚仁，2005；鄭伯璦等，

如何衝破逆境、提升部屬復原力？國軍主管家長式領導的效果檢驗與未來時間觀的調節作用

2002）、對部屬的心理健康亦有正面作用（趙安安與高尚仁，2005）。若根據資源保存理論的觀點，主管的高道德操守，能夠為部屬樹立典範、以身作則可以視為個人工作依循的標準。研究亦指出，領導者的務實態度和角色模範是個人在組織環境相當重要的保護因子（Castro et al., 2006; Macintyre et al., 2013）。因此，本研究推論主管展現德行領導能提升基層軍官復原力，並提出假設 4：

H4：德行領導與基層軍官復原力具正向關聯

### 2.3 未來時間觀與復原力之關係

未來時間觀是有關個人基於未來的期望和構思，進而對目前所採取的行動與抉擇（Seijts, 1998）。當個人的未來時間觀越強，越能發展具體的目標，並促使個人投入任務、進行規劃，並全力以赴於實現未來目標的行為（Husman & Lens, 1999）、且在未來想像過程，賦予遭遇的挫折意義性而堅持下去（Oyserman & James, 2011）。在未來時間觀的後設分析發現，員工的未來時間觀與工作滿意度、情感承諾、成長動機、持續工作動機、發展成就、職業承諾及自我效能都具正向關聯性（Henry, Zacher & Desmette, 2017）。從資源保存理論觀點，個人的目標動機、自我學習調整和要求等等，是個人十分重要的內在資源；同時，就復原力觀點來看，個人的特質和態度（如：自我效能、主動學習和解決問題）是個人面對壓力下維持正向適應、克服逆境的保護因子（曾文志，2007）。目前亦有研究證實未來時間觀與復原力呈現正相關（Fusco et al., 2019; Oshri et al., 2018）。Palmer（2016）進一步指出在復原力形塑過程，個人對時間性的知覺是關鍵之一，其認為對於高復原力者而言，逆境或是壓力事件都僅是「暫時性」的，隨著時間更迭而消逝。因此，個人如能把眼光放遠，認知事件所帶來的影響會隨著時間而變動，這就有助於復原力的產生。因此，本研究推論基層軍官未來時間觀能提升個人復原力，並提出假設 5：

H5：基層軍官未來時間觀能提升其復原力。

### 2.4 未來時間觀扮演的調節效果

在上述的討論，已經透過資源保存理論將家長式領導與部屬復原力進行連結。然而，是否在某些因素中，此關係會被強化？本研究對象乃基層軍官，從時間點來觀察，他們正處於職業初始階段，軍官在職業發展歷程中，舉凡晉升、進修與輪調都有時間的規範。以輪調為例，約略每 2-3 年便會因職務歷練而更換單位。在過去研究中，許多軍隊適應不良、精神困擾或自我傷害者面對困境時往往是受到單位領導者高壓管理或單位人際互動失衡，因而耽溺於當下受挫的情緒、限縮自己的認知而無法做決策，也就無法將視域拉至未來的可能性（Kazakina, 2015; Van Beek & Chistopolskaya, 2015；吳嘉蓉，2018）。許多研究亦顯示，未來時間觀是職涯發展過程中適應能力重要的預測因素（Henry et al., 2017; Oyserman & James, 2011）。因此，基層軍官所持的未來時間觀就顯得相當重要，能激發個人對未來的期望、構思和設定目標與實際行動。

既有文獻顯示，未來時間觀具有四個特色：首先，個人願意犧牲現在的快樂以達到未來理想的目標；其次，他們會賦予未來目標重要的價值，透過規劃與安排未來活動，設法投入更多的心力在現在的活動上；再者，目標達成的過程中他們會調整自己的行為以符合未來預期目標；最後，個人會隨時監控自己的績效以及衡量自己的表現是否能夠符合達成目標（Husman & Lens, 1999; Seijts, 1998; Shell & Husman, 2008）。整體而言，未來時間觀涉及對自己未來目標的價值、目標的設定與行動，以及對時間的知覺等認知和能力。故 Husman 與 Shell（2008）明確指出，在工作職場，個人對工作

所持的未來時間觀可以協助個體注重目標，並在達成目標的過程中調整自己的行為，以積極正向的態度，朝向未來邁進。因此，本研究認為，未來時間觀能調節不同的領導與復原力之間的關係。我們主要認為的理由有四：首先，高未來時間觀的人完成目標的動機性較高、自我調整學習的情形更明顯（曾惠琴，2018；黃珮婷，2011），故面對仁慈領導時，在領導者的鼓勵和肯定氛圍之中，會促發個人正向情緒，進而擴展學習經驗與動機，此有助於個人內在能力資源的增加。第二，高未來時間觀的人知覺時間的流逝較快，而不拘泥當下問題，迫使自己規劃未來，這面對負向事件的衝擊時具有緩衝自我威脅程度（Kazakina, 2015; Shell & Husman, 2000；余思賢等，2010）再者，當個人將現在的行動與未來聯結時，便會將遭遇的挫折和困難有其意義性而堅持下去（Oyserman & James, 2011）。換言之，當部屬面對專權領導的情境，如何減緩個人在當下的壓力知覺與受挫經驗十分重要。其中，未來時間觀可以被視為個人素質資源，因個人瞭解現在的付出與未來的關聯性，以完成未來的結果作為規劃，可以減緩個人自身資源流失的知覺，降低個人當下因受斥責而自尊低落。第三，高未來時間觀的人在自我要求和控制的程度較高（Seijts, 1998; Shell & Husman, 2008），故面對尚嚴領導時，較傾向更依循務實和守紀律的態度執行任務與面對生活中的困難（Castro et al., 2006）。第四，高未來時間觀的人重視自己未來目標的價值，也更願意設定計劃與行動（Husman & Lens, 1999; Shell & Husman, 2008），面對德行領導時，在領導者的道德操守和行為處事公正不阿的情況下，會促發角色學習而更願意朝向自己設定的目標達成。基於上述，本研究認為未來時間觀在家長式領導與部屬復原力之間的關係扮演調節作用。以下進一步具體分別說明推論與假設：

由於專權領導主管重視紀律、嚴格要求工作程序，在明確地目標任務下，個人能夠覺察單位所賦予的責任，當部屬面對重視紀律與工作要求的主管時，主管對於工作嚴格視與明確程序與責任，部屬較不會認知及擔心到資源不足或是擔憂面對資源損耗的可能性。正因為如此，部屬在執行任務或面對困難時，個人內心會擁有較高的心理資源與正向情緒，有助於個人工作形塑、問題解決。因此，當個體具備高度未來時間觀，由於主管較能完善工作要求而讓部屬能擁有資源，在工作的過程中會規劃自己未來，較不會因當下短暫受挫等負向壓力源而自尊低落，更能提高部屬復原力的展現；反之，低度未來時間觀的部屬，未能將主管的管理方式視為一種資源，而未能對現況及未來的資源進行調適與反思，形成個人尋求資源的壓力，降低復原力的展現。因此，本研究提出假設：

H6：基層軍官未來時間觀在專權領導與其復原力間具有正向調節效果。

由於尚嚴的領導者擁有高道德操守，要求自己以身作則，能夠為部屬樹立典範，為組織個人與環境塑造高要求工作環境，有明確、嚴格的工作要求與責任律定，部屬為了滿足領導者的工作要求，積極尋求資源進行應處，對於部屬的心理及情緒有正向作用。因此，當個體具備高度未來時間觀，由於主管嚴格的工作要求，讓部屬能積極尋求資源，在工作中能藉由資源的獲得而降低壓力的產生，更能提高部屬復原力的展現；反之，低度未來時間觀的部屬，面對尚嚴領導者的嚴格工作要求，不易獲得未來資源的探索，可能僅較侷限當下的現實環境資源覺知，導致資源逐漸不足而無法調適，降低復原力的展現。因此，本研究提出假設：

H7：基層軍官未來時間觀在尚嚴領導與其復原力間具有正向調節效果。

未來時間觀能讓個體注意到工作環境的目標情境，過程中適時調整自己，能夠以正向態度進行預處。當面對主管的仁慈領導，在領導者的鼓勵和肯定氛圍之中，會促

如何衝破逆境、提升部屬復原力？國軍主管家長式領導的效果檢驗與未來時間觀的調節作用

發個人正向情緒，因而減緩壓力源的存在。當個體具有高度未來時間觀，越會基於現狀及未來的考量，尋找適切的資源，由於仁慈主管較能給予部屬關懷與照顧感受的資源，較易在工作要求找到適配，降低負向壓力源的存在，提高復原力的展現；反之，低度未來時間觀者，未能將主管的關懷與鼓勵視為一種資源，由於因應現況及未來的資源不足，將形成個人尋求資源的壓力，降低復原力的展現。因此，本研究提出假設：

H8：基層軍官未來時間觀在仁慈領導與其復原力間具有正向調節效果。

由於德行領導者能展現正直、公私分明與以身作則的行為，部屬較能感受到領導者一視同仁，對於工作要求及權益有較大的安全感，不會擔心資源的不足，更把主管視為典範與學習榜樣，對於部屬的心理及情緒有正向作用。因此，當個體具備高度未來時間觀，由於主管以身作則的德行領導，讓部屬扮演追隨者的角色義務，為了滿足自我工作要求積極尋求資源，藉由資源的獲得而降低壓力的產生，更能提高部屬復原力的展現；反之，低度未來時間觀的部屬，面對德行領導者的領導行為，不易獲得未來資源的探索，導致資源逐漸不足而無法調適，降低復原力的展現。因此，本研究提出假設：

H9：基層軍官未來時間觀在德行領導與其復原力間具有正向調節效果。

### 三、研究方法

#### 3.1 研究架構

為探究主管家長式領導與基層軍官復原力之關連性，以及未來時間觀在其中可能具有的調節效果，整體研究架構，如圖 1 所示。

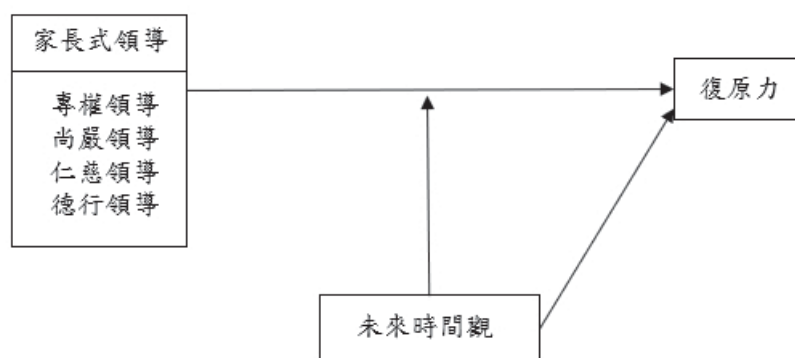


圖 1 研究架構圖

#### 3.2 研究樣本與施測程序

本研究以國軍營、連級之尉官，且到部滿三個月之基層軍官為研究母體，考量所屬單位之屬性、工作特性等，採便利取樣方式，自 2020 年 1 月開始進行網路問卷調查，最終抽取陸軍 34 個營、海軍 6 個營、空軍 12 個營，共計發放 538 份，完整施測共計 304 份有效樣本（陸軍：210 人、海軍：28 人、空軍：66 人），問卷回收有效率為 56.5%。

其次，由於本研究所有變項皆為基層軍官自評，因此可能會有共同方法變異（Common method variance）的問題，且因復原力與未來時間觀語意偏正向，易使受訪者在填寫問卷過程，因訊息的類化，致使結果呈現構念間的相關性膨脹。有鑑於此，本研究四項措施來因應事先預防，分別是運用時間隔離法、受訪者資料隱匿法、題意隱匿法及反向題設計法以避免由同源誤差產生之「共同方法變異」；在事後分析部

分，採用哈門氏單因子測試法（Harman's one-factor test）。首先將本研究進行探索性因素分析，檢定所有題項在未轉軸情況下，所萃取第一綜合因子檢定是否同時解釋自變項及依變項，若某一因素對所有的變數能解釋 50%以上之變異量，就有嚴重的共同方法變異（Podsakoff et al., 2003），以判定 CMV 影響之高低程度。問卷施測分兩階段施測，第一階段由基層軍官填寫家長式領導、未來時間觀變項；約間隔兩週後，填寫復原力量表。再者，研究藉由相關分析與階層迴歸分析驗證家長式領導、復原力及未來時間觀等三個變項之間的假設關係與結果。

### 3.3 研究變項衡量

#### 3.3.1 家長式領導

家長式領導量表採用鄭伯璦等（2000）編製的家長式領導量表與周婉茹（2009）編製的威權領導量表整合。此量表分為三部分，第一部分為威權領導（區分專權領導 8 題與尚嚴領導 10 題），在專權部分，例題如：「他會看輕我的辦事能力」、「他不讓我察覺他真正的意圖」，在尚嚴部分，例題如：「他堅守工作原則，不允許我違背」、「他要求我的工作績效一定不能低於預先設定的標準」；第二部分為仁慈領導計有 10 題，例題如：「當我工作情緒不佳時，他會給予適當的輔導」、「他會根據我個人的需要，來滿足我的要求」；第三部分為德行領導，計有 10 題，例題如：「他為人誠實，不說謊話」、「他公平對待所有的部屬」，整份量表共計 38 題。作答方式依 Likert 六點尺度量表，分別為「從未如此」至「總是如此」依序給予 1-6 分，比較兩分量表分數高低，判斷領導者趨向於哪一種領導風格。量表內部一致性信度 Cronbach's  $\alpha$  分別為.82、.77、.95 與.93。

#### 3.3.2 復原力

復原力量表採用 Smith, Dalen, Wiggins, Tooley, Christopher 與 Bernard（2008）編製的簡明復原力量表（BRS），而中文版 BRS 量表由邱保龍與嚴國晉（2019）所翻譯的版本。例題如：「我很快就能從壓力事件中恢復」、「我需要花很多的時間來克服生活中的挫折」。作答方式依 Likert 五點尺度量表，由 1 分至 5 分各代表「非常不同意」到「非常同意」，負向題則採反向計分。分數越高代表復原力越高，反之則復原力越低。量表內部一致性信度 Cronbach's  $\alpha$  為.76。

#### 3.3.3 未來時間觀

本研究採用陳玉樺（2018）所編製之「未來時間態度量表」，此量表區分「未來時間觀點」計有 6 題、「未來目標價值」計有 6 題、「對未來的準備與行動」計有 7 題，共計 19 題。例題如：「我能具體、清楚的說出我未來要做什麼」、「我對自己的未來充滿期待」、「我會思考實現未來目標時可能遇到的困難」。作答方式為六點量表，受試者依其反應或感受填答，作答方式依 Likert 六點尺度量表，分別為「非常不同意」至「非常同意」依序給予 1-6 分，總分越高代表個體整體的未來時間態度越佳。量表整體內部一致性信度 Cronbach's  $\alpha$  為.95，具有良好信度。

#### 3.3.4 控制變項

檢視既有文獻，不少學者認為性別、軍種、部隊型態、職務類別、服務年資、任官來源、到部時間等（胡智筆，2017；楊可忻，2013；黃睿瑛，2017；Mitchell & Ambrose, 2007）均會影響基層軍官壓力知覺、工作反應、復原力。其次，過去研究指出部屬會因權力距離的高低，而對主管的認知、態度或行為而有不同的反應（蔡松純等，2009）。換言之，基層軍官所認知的權力距離不同，面對主管威權領導的反應亦有可能影響。其中，為排除可能影響結果的外生變數，在控制變項部分填答中進行資料蒐集，本研究參考過去的文獻將性別（1=男性；2=女性）、軍種（1=陸軍；2=海軍；3=空軍）、部隊型態（1=戰鬥部隊；2=戰鬥支援單位；3=支援單位；4=幕僚學校

機關)、職務類別(1=領導職;2=幕僚職)、服務年資(年計算)、任官來源(1=正期軍官;2=專業軍官;3=ROTC;4=士官轉軍官)及到部時間(年計算)等七項個人背景變數作為控制變數予以控制。再者,在探討家長式領導對復原力與未來時間觀的效果時,本研究除運用時間隔離法外,另使用第三因子測試法,加入社會期許作為控制變項。

## 四、研究結果

### 4.1 描述性統計與相關分析

本研究的樣本分布,性別以男性為主 237 人佔 78%,女性為 67 人佔 22%(性別平均值 1.22,標準差.42),軍種分布以陸軍 210 人佔 69.1%最多,海軍 28 人 9.2%,空軍 66 人 21.7%(軍種平均值 1.53,標準差.83),部隊型態以戰鬥部隊 45.7%為最,戰鬥支援部隊 39.8 次之(部隊類型平均值 1.72,標準差.81),職務又以領導職 75.3%居多,幕僚職為 24.7%次之(職務平均值 1.24,標準差.43),服務年資 4 年以上者為 49.4%最多(服務年資平均值 4.66,標準差 4.26),任官來源以專業軍官 46.4%最多,正期軍官 35.2%次之(任官來源平均值 1.97,標準差 2.25),到部時間 1 年者為 50%最多,1-2 年者為 27%次之(到部平均值 1.40,標準差 2.25),顯見樣本抽樣分布能有效涵蓋研究所需。另外,本研究在假設驗證之前,先針對首先將本研究進行探索性因素分析,所有題項在未轉軸情況下 Kaiser-Meyer-Olkin (KMO) = 0.924 > 0.6;另針對各研究變項進行相關分析,觀察各變項的關聯性是否與假設預設符合,專權領導、尚權領導、仁慈領導、德行領導、未來時間觀及復原力等變項衡量題項以 Cronbach's  $\alpha$  值進行分析,顯示各構面的 Cronbach's  $\alpha$  值皆大於 0.7(如表 1),均具有高信度,其結果表示各因素題項具有內部一致性。其中,專權領導與復原力呈顯著負相關( $r = -.150, p < .01$ );尚嚴領導與復原力具正相關,但不具顯著性( $r = .014$ );仁慈領導與復原力呈顯著正相關( $r = .165, p < .01$ );德行領導與復原力呈顯著正相關( $r = .144, p < .05$ )。未來時間觀對復原力呈顯著正相關( $r = .553, p < .01$ ),因此,本研究於驗證專權領導、尚權領導、仁慈領導與未來時間觀與復原力間之關係時,引用上述控制變項是合理可行的。另外,為控制共同方法變異(CMV)之影響,本研究除了事前預防外,並進行事後檢測,以哈門氏單因子測試法(Harman's one-factor test)實施檢測,經將問卷變數所有題項的分數共同實施因素分析,在未轉軸的情況下,第一主成份因子的變異量為 22.93%(未達 50%),顯示所有變項之間沒有嚴重的共同方法變異問題。因此,本研究於驗證專權領導、尚權領導、仁慈領導、德行領導、未來時間觀及復原力間之關係時,引用上述控制變項是合理可行的。

表 1 各變項描述統計值與相關係數

| 變項          | 描述統計 |      | 相關係數矩陣 |        |        |        |        |        |       |         |        |         |       |        |       |        |       |
|-------------|------|------|--------|--------|--------|--------|--------|--------|-------|---------|--------|---------|-------|--------|-------|--------|-------|
|             | M    | SD   | 1      | 2      | 3      | 4      | 5      | 6      | 7     | 8       | 9      | 10      | 11    | 12     | 13    | 14     | 15    |
| 控制變項        |      |      |        |        |        |        |        |        |       |         |        |         |       |        |       |        |       |
| 1.性別        | 1.22 | 0.42 |        |        |        |        |        |        |       |         |        |         |       |        |       |        |       |
| 2.軍種        | 1.53 | 0.83 | .065   |        |        |        |        |        |       |         |        |         |       |        |       |        |       |
| 3.部隊型態      | 1.73 | 0.80 | .102   | -.086  |        |        |        |        |       |         |        |         |       |        |       |        |       |
| 4.職務類別      | 1.25 | 0.43 | .027   | .365** | .185** |        |        |        |       |         |        |         |       |        |       |        |       |
| 5.服務年資      | 4.67 | 4.26 | -.074  | .037   | .075   | .163** |        |        |       |         |        |         |       |        |       |        |       |
| 6.任官來源      | 1.97 | 0.98 | .047   | .009   | .091   | .054   | .317** |        |       |         |        |         |       |        |       |        |       |
| 7.到部時間      | 1.40 | 2.26 | .000   | -.023  | .070   | .074   | .339** | .200** |       |         |        |         |       |        |       |        |       |
| 8.權力距離      | 2.70 | 0.84 | -.029  | -.018  | -.020  | -.020  | .006   | -.039  | (.78) |         |        |         |       |        |       |        |       |
| 9.社會期許      | 3.38 | 1.00 | -.054  | .013   | .100   | .050   | -.002  | .090   | .058  | -.363** | (.83)  |         |       |        |       |        |       |
| 家長式領導       |      |      |        |        |        |        |        |        |       |         |        |         |       |        |       |        |       |
| 10.專權領導     | 2.51 | 1.10 | .069   | -.008  | -.028  | .003   | .125*  | -.072  | .069  | .039    | -.121* | (.82)   |       |        |       |        |       |
| 11.尚嚴領導     | 3.85 | 1.12 | -.020  | -.002  | -.018  | .023   | .092   | -.117* | .084  | -.010   | -.023  | .354**  | (.77) |        |       |        |       |
| 12.仁慈領導     | 3.90 | 1.31 | -.101  | -.020  | .013   | -.015  | -.035  | -.029  | .018  | .092    | .098   | -.534** | .000  | (.95)  |       |        |       |
| 13.德行領導     | 4.84 | 1.11 | -.039  | .066   | .005   | -.005  | -.021  | -.027  | -.002 | .049    | .152** | -.480** | .085  | .695** | (.93) |        |       |
| 復原力         |      |      |        |        |        |        |        |        |       |         |        |         |       |        |       |        |       |
| 14. BRS 復原力 | 3.02 | 0.68 | -.102  | -.001  | -.002  | .021   | .060   | -.009  | .141* | -.186** | .365** | -.150** | .014  | .165** | .144* | (.76)  |       |
| 15.未來時間觀    | 4.66 | 0.74 | .023   | -.022  | -.038  | .068   | -.007  | -.055  | .115* | -.252** | .270** | -.098   | .023  | .010   | .086  | .553** | (.95) |

註：n = 304。性別：1 = 男，2 = 女。M 為平均數；SD 為標準差；括弧內數字為內部一致性信度 Cronbach's  $\alpha$  值。\* $p < .05$ , \*\* $p < .01$

## 4.2 階層迴歸分析

本研究透過階層迴歸分析方法，針對研究推論與假設進行檢驗。首先，將呈現專權領導、尚嚴領導、仁慈領導、德行領導、未來時間觀對基層軍官復原力的主要效果，以檢驗 H1、H2、H3、H4、H5（如表 2）。接著，為了釐清未來時間觀對於基層軍官復原力在專權領導、尚嚴領導、仁慈領導及德行領導間的調節效果，本研究採用 Aiken 與 West（1991）的驗證程序，先將控制變項加入迴歸模型後，依序置入標準化後的預測變項（專權領導、尚嚴領導、仁慈領導、德行領導）、調節變項（未來時間觀）及交互作用項（專權領導×未來時間觀、尚嚴領導×未來時間觀、仁慈領導×未來時間觀、德行領導×未來時間觀），藉以預測效標變項（復原力），並檢驗 H6、H7、H8 與 H9（如表 2）。交互作用若對於效標變項具顯著效果，則表示調節效果成立。

### 4.2.1 主要效果

由表 2 的 M2、M3、M4、M5 與 M6 可知，透過階層迴歸分析，在排除控制變項對效標變項的影響之後，專權領導、尚嚴領導、仁慈領導、德行領導與未來時間觀對於基層軍官復原力的效果，結果顯示專權領導、仁慈領導、德行領導與未來時間觀對復原力具有顯著性，尚嚴領導則不具顯著性。其中專權領導對於復原力整體解釋力為 17.9% ( $\Delta R^2=.015$ )，整體迴歸效果達顯著水準 ( $F=6.409, p<.001$ )，顯示專權領導對復原力呈現顯著負向關係 ( $\beta = -.127, p<.05$ )；尚嚴領導對復原力未顯著 ( $\beta = -.002$ )；仁慈領導對於復原力整體解釋力為 18.1% ( $\Delta R^2=.017$ )，整體迴歸效果達顯著水準 ( $F=6.474, p<.001$ )，顯示仁慈領導對復原力呈現顯著正向關係 ( $\beta = .132, p<.05$ )；德行領導對於復原力整體解釋力為 17.3% ( $\Delta R^2=.009$ )，整體迴歸效果達顯著水準 ( $F=6.123, p<.001$ )，顯示德行領導對復原力呈現顯著正向關係 ( $\beta = .095, p<.05$ )。由上述迴歸分析結果可知，當基層軍官知覺上級主管展現仁慈領導行為或德行領導行為時，會增強基層軍官的復原力，而知覺上級主管展現專權領導行為時，會降低其復原力，故 H1、H3 與 H4 獲得支持，H2 未獲得支持。另 M6 中，未來時間觀對於基層軍官復原力則具有顯著的預測效果，其  $\Delta R^2$  值 .211 ( $p<.001$ )，結果顯示未來時間觀具有顯著的正向影響 ( $\beta = .493, p<.001$ )，故 H5 獲得支持。

### 4.2.2 未來時間觀的調節效果

由表 2 的 M7、M8、M9 與 M10 可知，排除控制變項、預測變項及調節變項的效果後，專權領導、仁慈領導、德行領導與未來時間觀的交互作用對於復原力具有顯著解釋力，其  $\Delta R^2$  值 .012 ( $p<.05$ )、.017 ( $p<.01$ ) 及 .008 ( $p<.05$ )。表示家長式領導與未來時間觀的確具有干擾效果。

表 2 各變項對依變項復原力之迴歸分析表

|                 | 1            | 2        | 3        | 4        | 5        | 6             | 7             | 8             | 9             | 10            |
|-----------------|--------------|----------|----------|----------|----------|---------------|---------------|---------------|---------------|---------------|
| 性別              | -.071        | -.065    | -.075    | -.063    | -.073    | -.097*        | -.086         | -.104*        | -.071         | -.078         |
| 軍種              | .040         | -.005    | -.003    | -.002    | -.011    | .031          | .031          | .029          | .040          | .031          |
| 部隊型態            | -.002        | -.040    | -.036    | -.038    | -.036    | .009          | -.001         | .005          | -.002         | .009          |
| 職務類別            | -.048        | .000     | .001     | .002     | .005     | -.045         | -.056         | -.046         | -.048         | -.042         |
| 服務年資            | .059         | .058     | .038     | .044     | .039     | .048          | .066          | .046          | .059          | .048          |
| 任官來源            | -.024        | -.085    | -.070    | -.065    | -.065    | -.026         | -.025         | -.025         | -.024         | -.024         |
| 到部時間            | .051         | .129*    | .123*    | .118*    | .122*    | .064          | .064          | .067          | .051          | .055          |
| 權力距離            | -.002        | -.059    | -.060    | -.079    | -.071    | .023          | .014          | .017          | -.002         | .015          |
| 社會期許            | .218**<br>*  | .329**   | .342**   | .323**   | .323**   | .235***       | .221***       | .236***       | .218***       | .218***       |
| 專權領導            |              | -.127*   |          |          |          |               | -.080*        |               |               |               |
| 尚嚴領導            |              |          | -.002    |          |          |               |               | .004          |               |               |
| 仁慈領導            |              |          |          | .132*    |          |               |               |               | .124**        |               |
| 德行領導            |              |          |          |          | .095*    |               |               |               |               | .058*         |
| 未來時間觀           |              |          |          |          |          | .493***       | .490***       | .491***       | .493***       | .503***       |
| 專權領導<br>×未來時間觀  |              |          |          |          |          |               | -.133**       |               |               |               |
| 尚嚴領導<br>×未來時間觀  |              |          |          |          |          |               |               | .049          |               |               |
| 仁慈領導<br>×未來時間觀  |              |          |          |          |          |               |               |               | .11*          |               |
| 德行領導<br>×未來時間觀  |              |          |          |          |          |               |               |               |               | .093*         |
| R <sup>2</sup>  | .164         | .179     | .164     | .181     | .173     | .375          | .399          | .378          | .403          | .387          |
| △R <sup>2</sup> | .164**<br>*  | .015*    | .000     | .017*    | .009*    | .211***       | .017**        | .002          | .012*         | .008*         |
| F 值             | 6.415*<br>** | 6.409*** | 5.754*** | 6.474*** | 6.123*** | 17.615<br>*** | 16.126<br>*** | 14.721<br>*** | 16.392<br>*** | 15.322*<br>** |
| 自由度             | 9,294        | 10,293   | 10,293   | 10,293   | 10,293   | 10,293        | 12,291        | 12,291        | 12,291        | 12,291        |

註：n = 304。表中所示為標準化迴歸係數。

\* $p < .05$ , \*\* $p < .01$ , \*\*\* $p < .001$

表 2 的 M2 顯示，探討專權領導為預測變項對依變項復原力的影響，其整體解釋力分別為 0.179 ( $\Delta R^2=.015$ )，加入專權領導與未來時間觀的交互作用時，其整體解釋力由 M2 的 0.179 提升到 M7 的 0.399，共增加了 0.220，整體迴歸效果達顯著水準 ( $F=16.126, p<.001$ )，迴歸係數呈現顯著負向關係 ( $\beta=-.080, p<.05$ )，該迴歸係數變小，顯示其調節作用關係顯著；其次，表 2 的 M4 顯示，在仁慈領導為預測變項對依變項復原力的影響，其整體解釋力分別為 0.181 ( $\Delta R^2=.0017$ )，加入仁慈領導與未來時間觀的交互作用時，其整體解釋力由 M4 的 0.181 提升到 M9 的 0.403，共增加了 0.222，整體迴歸效果達顯著水準 ( $F=16.392, p<.001$ )，迴歸係數呈現顯著正向關係 ( $\beta=.124, p<.01$ )，該迴歸係數變小，顯示其調節作用關係顯著。最後，M5 顯示，探討德行領導為預測變項對依變項復原力的影響，其整體解釋力分別為 0.173 ( $\Delta R^2=.009$ )，加入德行領導與未來時間觀的交互作用時，其整體解釋力由 M5 的 0.173 提升到 M10 的 0.387，共增加了 0.214，整體迴歸效果達顯著水準 ( $F=15.322, p<.001$ )，迴歸係數呈現顯著正向關係 ( $\beta=.093, p<.05$ )，該迴歸係數變小，顯示其調節作用關係顯著。因此本研究 H6、8 及 9 結果成立。

為進一步瞭解調節效果的型態，本研究亦參考 Aiken 與 West (1991) 的作法，將預測變項與調節變項高於與低於平均數一個標準差的值帶入迴歸式中，以預測復原力，並進行繪製交互作用圖，採用高低群未來時間觀進行簡單斜率分析進行檢驗，結果如圖 2 至圖 4 所示，即可分別檢視調節效果的影響。

透過 slope test (Dawson & Richter, 2006) 檢驗及交叉作用圖，由圖 2 可觀察到，當基層軍官具高未來時間觀時，高度未來時間觀與專權領導交互作用時，復原力迴歸係數為 3.22，較低專權領導主管對復原力迴歸係數 3.53 低（斜率為負向），其知覺主管專權領導對復原力具有負向影響；而當基層軍官未來時間觀低時，低度未來時間觀與專權領導交互作用時，復原力迴歸係數為 2.66，較低仁慈領導主管對復原力迴歸係數 2.61 高，其知覺主管仁慈領導對復原力具有正向影響（斜率為正）。此意謂著當基層軍官具高未來時間觀時，專權領導對復原力的負向影響會被強化，H6 獲支持。

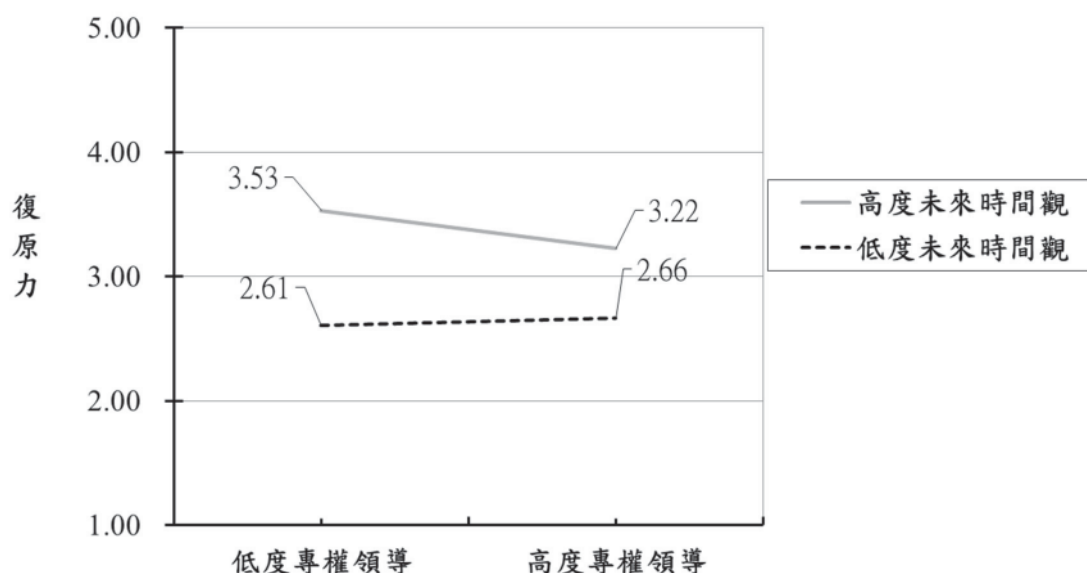


圖 2 未來時間觀對於專權領導與復原力之調節效果

透過 slope test (Dawson & Richter, 2006) 檢驗及交叉作用圖，由圖 3 可觀察到，高度未來時間觀與仁慈領導交互作用時，復原力迴歸係數為 3.57，較低仁慈領導主管

對復原力迴歸係數 3.21 高，知覺主管仁慈領導對復原力具有正向影響（斜率為正）；而當基層軍官未來時間觀低時，低度未來時間觀與仁慈領導交互作用時，復原力迴歸係數為 2.66，較低仁慈領導主管對復原力迴歸係數 2.61 高，知覺主管仁慈領導對復原力具有正向影響（斜率為正），然在仁慈領導對復原力的效果則不顯著（斜率近乎水平）。此代表在高未來時間觀之下，仁慈領導對復原力的正向影響會被強化，H8 得到支持。

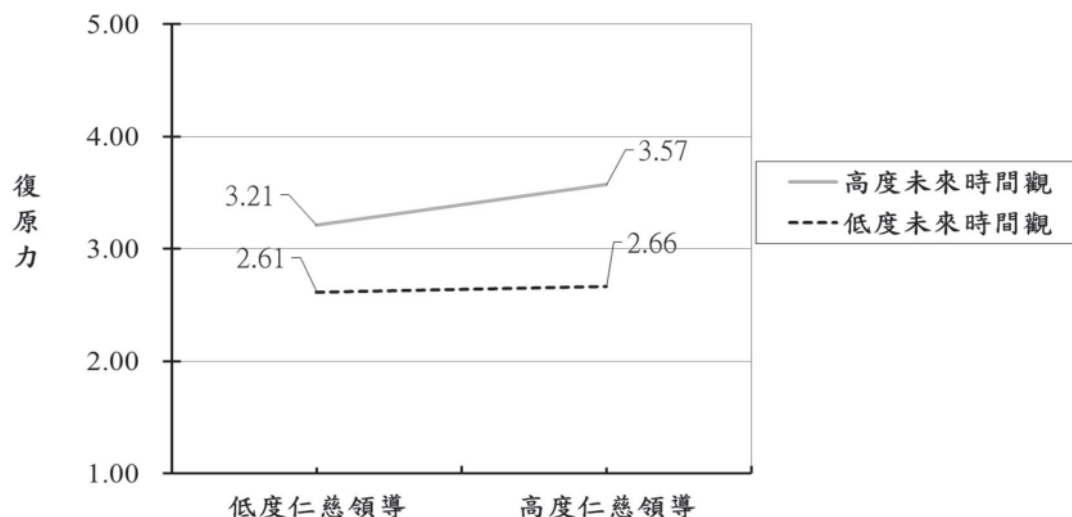


圖 3 未來時間觀對於仁慈領導與復原力之調節效果

最後，透過 slope test (Dawson & Richter, 2006) 檢驗及交叉作用圖，由圖 4 可觀察到，當基層軍官具高未來時間觀時，高度未來時間觀與德行領導交互作用時，復原力迴歸係數為 3.53，較低德行領導主管對復原力迴歸係數 3.25 高（斜率為正向），其知覺主管專權領導對復原力具有正向影響；而當基層軍官未來時間觀低時，低度未來時間觀與德行領導交互作用時，復原力迴歸係數為 2.61，較低德行領導主管對復原力迴歸係數 2.65 低，其知覺主管德行領導對復原力具有負向影響（斜率為負）。德行領導對復原力的效果則不顯著（斜率近乎水平）。此代表在高未來時間觀之下，德行領導對於復原力的正向影響將會被強化，故 H9 得到支持。

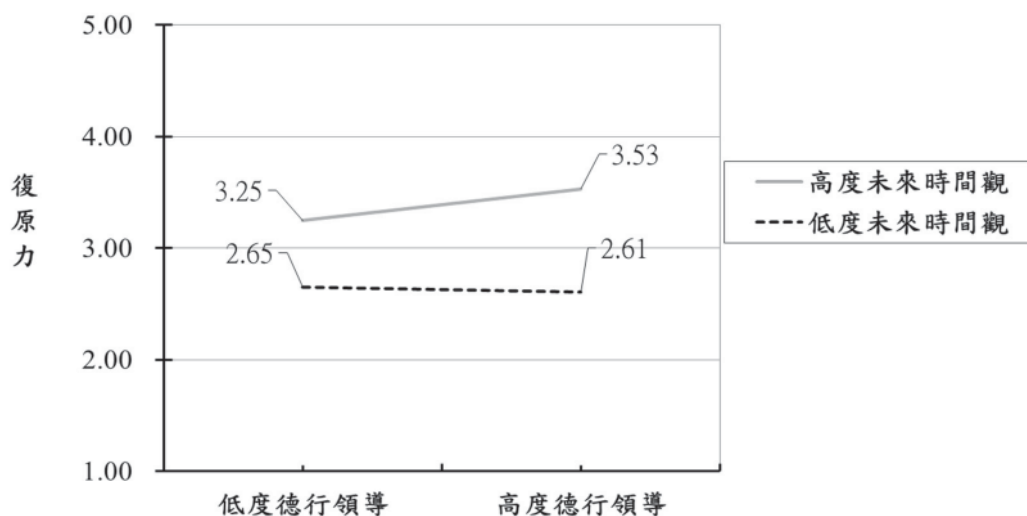


圖 4 未來時間觀對於德行領導與復原力之調節效果

## 五、結論與建議

### 5.1 理論意涵

本研究的核心是想瞭解哪些因素會影響復原力，並區分社會情境因素及個人因素。在情境因素方面，特別是在軍事情境下，領導會影響基層軍官的工作表現及生活，而本研究著重在家長式領導對復原力的影響；個人因素方面，未來時間觀在領導與復原力關係所扮演的調節作用。

整體而言，在家長式領導與基層軍官復原力的關係，研究結果僅尚嚴領導與復原力關係的假設未受到支持，其餘專權領導、仁慈領導、德行領導與復原力關係的假設均受到支持。其次，在未來時間觀與復原力的關係，研究結果支持假設。再者，在未來時間觀的調節效果部分，未來時間觀會調節專權領導與復原力的負向關係，而基層軍官之未來時間觀會調節仁慈領導、德行領導與復原力的正向關係。以下進一步針對理論意涵與貢獻說明。

首先，以往部分研究將威權領導視為單一構面，有鑑於此，本研究將威權領導進一步細分「專權」和「尚嚴」領導兩部分，研究結果顯示專權領導與復原力具顯著負向關聯，然而，尚嚴領導與復原力不具關連性。過去研究曾發現專權領導因其以專權、貶抑部屬能力與斥責部屬，會讓部屬感受壓力、丟臉與不被尊重（吳宗祐，2008；周麗芳等人，2006；許金田等人，2004；陳皓怡等人，2007；趙安安、高尚仁，2005）。本研究從資源保存理論進一步證實專權領導會讓個人覺得資源喪失，而降低基層軍官的復原力。事實上，軍隊在往常給人的印象中，是一個高壓且要求嚴格的組織，其領導方式往往都是以專權領導為主。但是，在本研究也發現，基層軍官感知主管專權領導的平均分數為 2.51，略低於中間值的 3.36，顯然專權領導在部隊中並非主流領導方式。其次，尚嚴領導與復原力雖不具關連性，但透過描述性統計分析，可以觀察尚嚴領導的分數為 3.85，略高於中間值 3.36，顯示基層軍官普遍認為其主管對於任務的要求與效率是嚴格的，且主管注重於工作績效的提升，而尚嚴領導的意涵也正是針對「事」的標準與效率，符合目前軍隊當前的治軍精神。值得關注的是，尚嚴領導在人口背景變項中的任官來源有顯著關聯性，且正期軍官所感知的主管尚嚴領導分數為 4.21，明顯較其他來源高，其原因可能在於主管對於軍校畢業的基層軍官的工作要求相較於其它任官來源要高，因此有顯著的差異性，日後研究取樣建議可以從軍官的來源背景深入探討，藉以觀察復原力的差異性。

其次，過去研究主要側重於領導與工作績效的關係（如：李庭閣、張珈進、黃少宇、嚴國晉，2016；林靜怡，2015；吳宗祐、周麗芳、鄭伯壖，2008；黃秉弘，2015），本研究從資源保存理論觀點，進一步證實仁慈領導、德行領導帶給部屬的影響不僅是工作表現，也影響著個人面對挫折和逆境的復原力。本研究顯示仁慈領導、德行領導均與復原力呈現顯著正相關，此兩種領導方式均能讓基層軍官感受資源的充足，降低壓力感，藉以提升基層軍官的復原力。此與過去研究相似，主管的仁慈領導、德行領導有助於部屬身心健康（趙安安與高尚仁，2005）。換言之，這呼應資源保存理論的觀點，也就是在部屬知覺主管仁慈領導時，會將感受到的支持和心理賦權做為一種資源，能強化個人的復原力、而部屬知覺主管德行領導時，從領導者的道德操守可作為部屬的學習典範，這也增加個人面對挫折的資源因應。其中，研究也觀察到在基層部隊中，德行領導的分數最高，代表著目前主管的領導統御方式普遍以德行領導佔多數，顯示在軍隊情境之中，領導幹部相當重視以身作則，才能作為官兵的表率，且因應世代的改變，民主意識高漲，帶兵須帶心，以德服人也是不可忽略的要素之一。

再者，在組織研究中，「時間觀」甚少被當成主要探討議題，但其重要性不容小覷，特別在大多數研究顯示未來時間觀對正向行為具保護作用（林姿葶、鄭伯璜，2013）。雖然既有研究證實未來時間觀對部屬在職場有正向強化作用（如：工作滿意度、情感承諾、成長動機、持續工作動機、發展成就、職業承諾）（Henry, Zacher & Desmette, 2017），但是，這些研究尚未檢視未來時間觀在家長式領導與復原力關係之間所扮演的角色。此外，本研究進一步將威權領導的內涵進一步區分，以釐清專權領導和尚嚴領導的差異效果。本研究發現高未來時間觀之下，仁慈領導、德行領導對於復原力的正向影響將會被強化，也就是，當基層軍官之未來時間觀越高時，在感知主管高仁慈領導、德行領導的情況下，可以進一步提升復原力的展現。而在基層軍官未來時間觀低時，仁慈領導、德行領導分別與復原力的關係則無顯著影響。此結果顯示軍隊主管的人格具有影響基層軍官的作用。

另外，基層軍官正處於職業初始階段，從時間點來觀察，軍官在職業發展歷程中，舉凡晉升、進修與輪調都有時間的規範。因此，未來時間觀的認知及掌握是個人在從事活動或做決策時一個重要的推動力，勢必會影響軍官的職涯規劃與適應能力。本研究亦初步證實此一關聯性。研究發現未來時間觀與復原力呈顯著正相關，當基層軍官未來時間觀越高，越能促進復原力的展現，且 $\Delta R^2$ 為.211，分析顯示未來時間觀對復原力具有良好的預測力。據此，本研究假設未來時間觀為基層軍官復原力的保護因子可獲得驗證。同時符合復原力理論中「心理脈絡的觀點」，其強調個人特質的發揮，諸如對問題解決能力等，均能提升個人的復原力。

值得注意的是，基層軍官之未來時間觀會調節專權領導與復原力的負向關係。且當基層軍官之未來時間觀越高時，在感知主管高專權領導的情況下，會降低其復原力的展現。而在基層軍官未來時間觀低時，專權領導與復原力的關係則無顯著影響。這代表基層軍官未來時間觀時，在感知主管高專權領導的情境中，對於復原力反而變成幫倒忙的角色，此結果與先前威權領導與自我情緒智力是呈負向調節效果相同（吳宗祐，2008）。本研究亦參考吳宗祐與鄭伯璜（2006）的觀點，推測其原因可能在於當未來時間觀低時，對於未來較無想法，抱持著走一步是一步的心態，不論在高專權或是低專權，面對逆境的能力均不好，無明顯差別，因此復原力皆偏低。但是在未來時間觀高的基層軍官，在主管低專權領導的情境之下，工作自由度較高，面對逆境時的處遇較為彈性，因此復原力也較高。相反地，在面對高專權的主管時，工作彈性低，自覺將來的軍旅發展亦會受到專權主管的影響，導致面對逆境的處置能力變差，復原力也較低。

## 5.2 實務意涵

提升部屬的復原力，並藉以協助個人面對挫折和逆境的因應與復元，是當代風險社會相當重要的事。面對組織任務的改變、人員的精簡，身為軍事組織的主管，其領導方式便扮演著重要的角色。依據本研究結果，在家長式領導中的不同領導方式對部屬復原力有不同程度的影響。首先，本研究發現，在專權領導部分，當未來時間觀的介入後，專權領導與復原力有顯著的負向影響，根據研究結果得知，基層軍官未來時間觀的平均值為 4.66 分，代表著其大部分均有一定程度的未來時間觀，若是在感知主管高專權領導的情境之下，會導致復原力的下降。因此，隨著時代持續變遷的脈絡下，專權領導在部隊的適用性仍需要謹慎的考量。原因在於科技進步，部屬對外社交關係活絡，自由風氣提升。而專權領導仍屬於傳統觀念，維持上尊下卑、權謀操控的形式，就算是在權力距離較高的軍隊環境，部屬也漸漸無法接受，進而會降低部屬效能與復原力等等，導致軍隊執行任務的困難度增加。另外，比起專權領導，尚嚴領導

似乎更為部屬所能接受。雖然與復原力無正向顯著關係，但不至於造成基層軍官復原力的降低。且過去研究已證實尚嚴領導能夠提升部屬的工作績效，建議軍隊組織在推行任務時，能將尚嚴領導取代過去的威權領導，主管應更集中於對「事」的要求，而非無故的責難與貶斥，更能保存部屬的個人特性資源、擴展狀況資源。

其次，研究結果證實仁慈領導能提升基層軍官的復原力，此結果亦顯示軍隊中領導幹部在「知官識兵」方面的表現是不可或缺的，不僅對工作上有所支持，部屬在工作外的各種資訊亦須有一定瞭解的程度，舉凡部屬周遭的親朋好友，在其急、難、病、痛、苦時，給予適當的協助，發揮感動服務，部屬蒙受其恩，進而增進團隊向心力，強化部屬復原力，使組織、個人均能在困難的任務中安然度過，不致挫折所擊潰。另外，當基層軍官未來時間觀越高時，其感知主管高仁慈領導的情況下，可以進一步提升復原力的展現。也就是，在實務執行過程，主管不能忽略部屬所持的未來時間觀，也就是在主管仁慈領導過程，主管要特別強化部屬對未來軍旅目標的設定與計畫，如此一來，透過領導者本身的角色模範和關心部屬未來發展，有助於協助部屬面臨困難時的因應態度與度過危機。

再者，本研究顯示了德行領導的重要性。德行領導在軍隊組織中是一項不可或缺的領導方式，但根據過去研究指出，德行領導屬於個人品德操守，較難界定其好與壞。在軍人養成教育中，不管是軍校亦或是軍官受訓短期班隊，應將軍人武德課程結合部隊實務授課，注重領導者品德的修養，訓練幹部潔身自愛、自我要求，此外，在實際單位任務運作過程，領導者須隨時注意自身品性與操守，這在集體生活環境的組織特性中會潛移默化影響部屬的復原力展現。另外，部屬的未來時間觀亦不能忽視。也就是，領導者在自我要求和品德操守的同時，主管亦可透過設置高標準（特別是關於未來任務與部屬未來期待的連結），經由以身作則、合法且符合道德要求的領導風氣，便能使部屬具備抵抗逆境的能力，展現高復原力。

### 5.3 研究限制與未來研究方向

首先，本研究採用自陳式量表進行問卷施測，且各變項皆屬同源填寫，為了避免因相同來源而可能產生共同方法變異，採用「時間隔離法」將自變項與依變項區分兩個時間點施測，但仍有無法避免 CMV 之疑慮，建議未來研究設計問卷可採對偶方式進行施測。第二，由於本問卷以自陳方式區分兩階段於個人層次部分進行資料蒐集，並未有總體層次的對偶，因此在這部分並未涉及巢套的關係，在這方面的研究方式將可與未來研究方向進行個體層次及總體層次，運用 Mplus、HLM 等統計軟體再深入研究。第三，研究對象為三軍之基層軍官，透過描述統計發現，回收資料在背景變項上的比例有落差，如軍種、任官來源、部隊型態等，未來可特別針對基層軍官的背景差異進行資料蒐集，以利比較其與復原力的關聯性。第四，本研究屬於橫斷面資料，僅能觀察到基層軍官現階段在主管家長式領導情境下，其復原力的現況，未能全面瞭解其變化的過程。因此，建議未來研究可進一步採取縱貫性的研究，納入跨時間性的考量，不僅可以作為變項間因果推論的依據，也能針對不同時間點進行分析比較。第五，本研究僅針對基層軍官為研究對象，而軍官在軍隊組織中比例並不高，士官及士兵才是部隊中的主要戰力，建議未來可納入士官兵為研究對象，藉以剖析全軍復原力的情況。第六，本研究透過家長式領導的三個向度，分別為仁慈、威權（專權、尚嚴）與德行領導，分別檢視其與復原力的直接關係，並發現仁慈與德行領導對於復原力的正向預測效果。事實上，領導者可能同時具備兩種以上的領導方式，如恩威並濟、高德行高仁慈、高威權高德行等不同組合。周婉茹（2009）的研究指出，恩威並

濟對部屬效能具有正向影響，但並未將德行領導納入考量。因此，在家長式領導不同組合的情況下，哪一種組合會影響部屬復原力的展現亦是未來值得探討的方向。最後，既有研究亦指出，團隊凝聚力（黃義翔、聶橋齡，2015）、組織氛圍（鄭雅云，2008）等在主管領導風格與部屬效能間有顯著的中介效果。未來可進一步探討在主管展現不同家長式領導的情境脈絡之下，透過其他中介變項，進而影響基層軍官復原力的展現，藉以讓我們在家長式領導與部屬復原力的關係有更多的瞭解。

## 六、國防領域之應用

未來時間觀代表個人對未來時間態度、對未來目標的價值、規劃與行動。本研究亦顯示，當基層軍官具高未來時間觀時，德行領導、仁慈領導對復原力的正向影響均會被強化；而威權領導對復原力的負向影響會被強化。因此，建議未來訓練單位或管理部門在人員培育和職涯規劃，可以進一步評估個人所持未來時間觀，並將此議題納入軍人職業生涯發展的相關課程，引導軍人將時間觀置於未來，具體規劃生涯各階段的目標，此一過程的心理歷程，會提升個人面對挫折的態度與因應能力。再者，從組織領導方面，亦發現德行領導和仁慈領導足以提升基層官兵面對挫折的因應，因此在軍官養成教育過程，領導風格的形塑是關鍵因素，足以影響單位人員面對困境的能力。

## 參考文獻

- 丁華，吳濬廷，2016。軍人自殺徵兆與自殺行為之關連性分析，復興崗學報，第 108 期，75-93。
- 余思賢，林以正，黃金蘭，黃光國，張仁和，2010。長程取向思維與心理適應之關聯，中華心理衛生學刊，第 23 卷 3 期，347-375。
- 吳宗祐，2008。主管威權領導與部屬的工作滿意度與組織承諾：信任的中介歷程與情緒智力的調節效果，本土心理學研究，第 30 期，3-63。
- 吳宗祐，鄭伯璫，2006。工作投入、調節他人情緒能力與情緒勞動之交互作用對情緒耗竭的預測效果，中華心理學刊，第 48 卷 1 期，69-87。
- 吳嘉蓉，2018。優勢觀點運用於陸軍適應不良類型軍官之探討（未出版之博士論文），國立政治大學社會工作研究所，台北。
- 周婉茹，2009。專權與威嚴領導的效果：心理賦能的中介與仁慈領導的調節（未出版之碩士論文），國立台灣大學心理學研究所，台北。
- 周婉茹，周麗芳，鄭伯璫，任金剛，2010。專權與尚嚴之辨：再探威權領導的內涵與恩威並濟的效果，本土心理學研究，第 34 期，223-284。
- 周麗芳，鄭伯璫，任金剛，2006。情境脈絡影響，載於鄭伯璫，樊景立，周麗芳（主編），家長式領導：模式與證據，台北：華泰文化公司。
- 林姿葶，鄭伯璫，2012。華人領導者的噓寒問暖與提攜教育：仁慈領導之雙構面模式，本土心理學研究，第 37 期，253-302。
- 林姿葶，鄭伯璫，2013。組織中的時間與時間觀：回顧與展望，本土心理學研究，第 40 期，143-195。
- 林姿葶，鄭伯璫，周麗芳，2014。家長式領導：回顧與前瞻，本土心理學研究，第 42 期，3-82。
- 邱保龍，嚴國晉，2019。招生訊息管道、社會支持對軍事基礎學院學生退學影響之研究，108 年國防大學校務議題研究案，桃園：國防大學。
- 姜定宇，丁捷，林伶瑾，2012。家長式領導與部屬效能：信任主管與不信任主管的中介效果，中華心理學刊，第 54 卷 3 期，269-291。
- 洪健文，2010。國軍志願役官兵工作壓力之研究-以新訓部隊為例（未出版之碩士論文），國立中正大學高階主管碩士在職專班，嘉義。
- 胡智筆，2017。陸軍基層部隊官兵適應問題與因應行為關聯性之研究（未出版之碩士論文），國防大學政治作戰學院心理及社會工作學系，台北。
- 國防部，2017。國防部 106 年度施政計畫，台北。
- 陳玉樺，2018。回首向前，轉念成春：反芻思考、未來時間觀與寬恕之關係（未出版之博士論文），國立政治大學教育學系，台北。
- 陳品傑，2018。國軍志願役官兵以精神疾病除役復歸歷程初探（未出版之碩士論文），國立臺北大學社會工作學系，台北。
- 陳盈璇，2018。家長式領導、知覺不當督導與壓力反應之關聯性與研究（未出版之碩士論文），國防大學政戰學院政治研究所，台北。
- 陳皓怡，高尚仁，吳治富，2007。家長式領導對多國籍部屬身心健康之影響：以華人外派主管為例，應用心理研究，第 36 期，223-244。
- 曾惠琴，2018。宜蘭縣國中生未來時間觀與自我調整學習能力境況與相關之研究（未出版之碩士論文），佛光大學未來與樂活產業學系，宜蘭。
- 陽昊，2017。部屬知覺之主管家長式領導風格對其心理健康之影響：部屬自身傳統人格特質之調節作用（未出版之碩士論文），輔仁大學心理學系，台北。

- 黃泳睿，2013。精粹案下政戰軍士官對工作壓力與離職傾向之研究－以陸軍中校階以下軍官為例（未出版之碩士論文），中華大學科技管理學系碩士班，新竹。
- 黃珮婷，2012。大學生未來時間觀、知覺工具性及自我調整學習之相關研究（未出版之碩士論文），國立台灣師範大學教育心理與輔導學系，台北。
- 黃義翔，聶橋齡，2015。教練－選手關係在家長式領導行為與團隊凝聚力關係間的中介角色，大專體育學刊，第 17 卷 2 期，203-219。
- 黃睿瑛，2017。國軍政戰志願役專業預備軍官停役歷程之研究（未出版之碩士論文），國防大學政戰學院社會工作碩士班，台北。
- 楊可忻，2013。海軍艦艇領導軍官工作壓力、社會支持對工作滿意之影響（未出版之碩士論文），國立高雄師範大學人力與知識管理研究所，高雄。
- 廖昱絜，2018。正期軍官離職因素之研究（未出版之碩士論文），國防大學政戰學院社會工作碩士班，台北。
- 趙安安，高尚仁，2005。台灣地區華人企業家長式領導風格與員工壓力之關聯，應用心理研究，第 27 期，111-131。
- 樊景立，鄭伯璜，2000。華人組織的家長式領導：一項文化觀點的分析，本土心理學研究，第 13 期，126-180。
- 蔡松純，鄭伯璜，周麗芳，姜定宇，鄭弘岳，2009。領導者上下關係認定與部屬利社會行為：權力距離之調節效果，中華心理學刊，第 51 卷 1 期，121-138。
- 鄭伯璜，周麗芳，樊景立，2000。家長式領導：三元模式的建構與測量，本土心理學研究，第 14 期，3-64。
- 鄭伯璜，謝佩鴛，周麗芳，2002。校長領導作風、上下關係品質及教師角色外行為：轉型式與家長式領導的效果，本土心理學研究，第 17 期，105-161。
- 鄭雅云，2008。家長式領導對團隊組織公民行為之影響－以員工團隊情感氛圍為中介變數（未出版之碩士論文），國立台北科技大學商業自動化與管理研究所，台北。
- Adler, A. B. and Lopez, A., 2019. The Impact of Leadership on Service Member Health. In Eugenia L. Weiss & Carl Castro(Eds), *American Military Life in the 21st Century: Social, Cultural, and Economic Issues and Trends* [2 volumes](pp. 89-100). California, ABC-CLIO.
- Aiken, L. S. and West, S. G., 1991. *Multiple regression: Testing and interpreting Interactions*. Newbury Park CA: Sage publication.
- Ashford, S. J., Blatt, R., & VandeWalle, D., 2003. Reflections on the Looking Glass: A Review of Research on Feedback-Seeking Behavior in Organizations. *Journal of management*, 29(6), 773-799. doi:10.1016/S0149-2063(03)00079-5.
- Bartone, P. T., 2006. Resilience under military operational stress: Can leaders influence hardiness? *Military psychology*, 18(sup1), S131-S148.
- Bass, B. M. and Stogdill, R. M., 1990. *Bass & Stogdill's handbook of leadership: Theory, research, and managerial applications*. Simon and Schuster.
- Block, J., & Kremen, A. M., 1996. IQ and ego-resiliency: Conceptual and empirical connections and separateness. *Journal of Personality and Social Psychology*, 70(2), 349-361.
- Branicki, L., Steyer, V., & Sullivan-Taylor, B., 2019. Why resilience managers aren't resilient, and what human resource management can do about it. *The International Journal of Human Resource Management*, 30(8), 1,261-1,286.
- Castro, C. A., Adler, A. B., McGurk, D. and Thomas, J. L., 2006. *Leader Actions to Enhance Soldier Resiliency in Combat*. Walter Reed Army Inst Of Research Silver Spring Md Dept Of Military Psychiatry.

- Chemers, M. M. and Ayman, R. E., 1993. Leadership theory and research: Perspectives and directions. Academic Press.
- Chen, T. T., 2011. Structuring versus autocraticness: Exploring a comprehensive model of authoritarian leadership. Unpublished doctoral dissertation, City University of Hong Kong.
- Chou, L. F., Cheng, B. S. and Jen, C. K., 2005. The contingent model of paternalistic leadership: Subordinate dependence and leader competence. Paper presented at the Academy of Management 2005 Annual Meeting, Honolulu, HI.
- Cooper, B., Wang, J., Bartram, T. and Cooke, F. L., 2019. Well-being-oriented human resource management practices and employee performance in the Chinese banking sector: The role of social climate and resilience. *Human Resource Management*, 58(1), 85-97.
- Cooper, D. C. and Bates, M. J., 2019. Military Health Provider Training and Evaluation of a Problem-Solving Intervention to Reduce Distress and Enhance Readiness Among Service Members. *Military medicine*, 184(5-6), 303-311.
- Cullen, F. T., Link, B. G., Wolfe, N. T., & Frank, J., 1985. The social dimensions of correctional officer stress. *Justice Quarterly*, 2(4), 505-533.
- Davies, S. E., Stoermer, S., & Froese, F. J., 2019. When the going gets tough: The influence of expatriate resilience and perceived organizational inclusion climate on work adjustment and turnover intentions. *The International Journal of Human Resource Management*, 30(8), 1393-1417.
- Dawson, J. F. and Richter, A. W., 2006. Probing three-way interactions in moderated multiple regression: Development and application of a slope difference test. *Journal of Applied Psychology*, 91(4), 917-926.
- Demerouti, E., & Bakker, A. B., 2014. Job crafting. In *An introduction to contemporary work psychology*. (pp. 414-437). Hoboken, NJ, US: Wiley Blackwell.
- Doody, C. B., Robertson, L., Uphoff, N., Bogue, J., Egan, J., & Sarma, K. M. (2019). Pre-deployment programmes for building resilience in military and frontline emergency service personnel. *The Cochrane Database of Systematic Reviews*, 2019(1), 1-15.
- Farh, J. L. and Cheng, B. S., 2000. A cultural analysis of paternalistic leadership in Chinese organizations. In J. T. Li, A. S. Tsui, & E. Weldon (Eds.), *Management and organizations in the Chinese context*, 85-127. London: Macmillan.
- Fusco, L., Sica, L. S., Boiano, A., Esposito, S. and Sestito, L. A., 2019. Future orientation, resilience and vocational identity in southern Italian adolescents. *International Journal for Educational and Vocational Guidance*, 19(1), 63-83.
- Gaddy, J. W., Gonzalez, S. P., Lathan, C. A. and Graham, P. K., 2017. The perception of authentic leadership on subordinate resilience. *Military Behavioral Health*, 5(1), 64-72.
- Harland, L., Harrison, W., Jones, J. R. and Reiter-Palmon, R., 2005. Leadership behaviors and subordinate resilience. *Journal of Leadership & Organizational Studies*, 11(2), 2-14.
- Hatala, A. R., Pearl, T., Bird-Naytowhow, K., Judge, A., Sjoblom, E. and Liebenberg, L., 2017. "I have strong hopes for the future": Time orientations and resilience among Canadian Indigenous youth. *Qualitative health research*, 27(9), 1330-1344.
- Henry, H., Zacher, H. and Desmette, D., 2017. Future time perspective in the work context: a systematic review of quantitative studies. *Frontiers in psychology*, 8, 1-22.
- Heber, A., Testa, V., Smith-MacDonald, L., Brémault-Phillips, S., & Carleton, R. N., 2020. Commentary-Rapid response to COVID-19: addressing challenges and increasing the mental readiness of public safety personnel. *Health Promotion and Chronic Disease Prevention in Canada: Research, Policy and Practice*, 40(11-12), 350-355.
- Hobfoll, S. E., 1989. Conservation of resources: A new attempt at conceptualizing stress. *American psychologist*, 44(3), 513-524.
- Hobfoll, S. E., 2011. Conservation of resource caravans and engaged settings. *Journal of*

- Occupational and Organizational Psychology*, 84(1), 116-122.
- Husman, J. and Shell, D. F., 2008. Beliefs and perceptions about the future: A measurement of future time perspective. *Learning and Individual Differences*, 18(2), 166-175.
- Johnson, S. R. L., Blum, R. W. and Cheng, T. L., 2014. Future orientation: A construct with implications for adolescent health and wellbeing. *International Journal of Adolescent Medicine and Health*, 26, 459-468.
- Lai, J. C. and Yue, X., 2014. Using the Brief Resilience Scale to assess Chinese people's ability to bounce back from stress. *Sage Open*, 4(4), 1-9.
- Lazarus, R. S. & Folkman, S., 1984. *Stress, appraisal, and coping*. Springer.
- Lengnick-Hall, C. A., Beck, T. E. and Lengnick-Hall, M. L., 2011. Developing a capacity for organizational resilience through strategic human resource management. *Human resource management review*, 21(3), 243-255.
- Liu, Y., L. Cooper, C., & Y. Tarba, S., 2019. Resilience, wellbeing and HRM: A multidisciplinary perspective. *The International Journal of Human Resource Management*, 30(8), 1,227-1,238.
- Luthar, S. S., 2006. Resilience in development: A synthesis of research across five decades. In D. Cicchetti, & D. J., Cohen (Eds.), *Developmental psychopathology*, Vol 3: Risk, disorder, and adaptation 2nd ed. (pp. 739-795). Hoboken, NJ: John Wiley & Sons.
- MacIntyre, A., Charbonneau, D. and O'Keefe, D., 2013. The role of transformational and ethical leadership in building and maintaining resilience. *Building psychological resilience in military personnel: theory and practice*, 94.
- Masten, A. S., 2014. *Ordinary magic: Resilience in development*. New York: Guilford Press.
- Masten, A. S., 2019. Resilience from a developmental systems perspective. *World Psychiatry*, 18(1), 101-102.
- Mitchell, M. S. and Ambrose, M. L., 2007. Abusive supervision and workplace deviance and the moderating effects of negative reciprocity beliefs. *Journal of Applied Psychology*, 92, 1159-1168.
- Nguyen, Q., Kuntz, J. R., Näswall, K. and Malinen, S., 2016. Employee resilience and leadership styles: The moderating role of proactive personality and optimism. *New Zealand Journal of Psychology (Online)*, 45(2), 13-21.
- O'Leary, V. E., & Bhaju, J., 2006. Resilience and empowerment. In J. Worell & C. D. Goodheart (Eds.), *The handbook of girls' and women's psychological health: Gender and well-being across the lifespan* (pp. 157-165). Oxford: Oxford University Press.
- Oshri, A., Duprey, E. B., Kogan, S. M., Carlson, M. W. and Liu, S., 2018. Growth patterns of future orientation among maltreated youth: A prospective examination of the emergence of resilience. *Developmental psychology*, 54(8), 1456.
- Palmer, D. K., 2016. Taking Time Seriously as a Component of Employee Resilience. *Industrial and Organizational Psychology*, 9(2), 517-522.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y. and Podsakoff, N. P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, 88(5), 879-903. doi:10.1037/0021-9010.88.5.879.
- Qian, J., Li, X., Song, B., Wang, B., Wang, M., Chang, S. and Xiong, Y., 2018. Leaders' expressed humility and followers' feedback seeking: the mediating effects of perceived image cost and moderating effects of power distance orientation. *Frontiers in psychology*, 9, 563.
- Schuster, C., Weitzman, L., Sass Mikkelsen, K., Meyer-Sahling, J., Bersch, K., Fukuyama, F., ... & Kay, K., 2020. Responding to COVID-19 through Surveys of Public Servants. *Public Administration Review*, 80(5), 792-796.
- Smith, B. W., Dalen, J., Wiggins, K., Tooley, E., Christopher, P. and Bernard, J., 2008. The

- brief resilience scale: assessing the ability to bounce back. *International journal of behavioral medicine*, 15(3), 194-200.
- Wald, J., Taylor, S., Asmundson, G. J., Jang, K. L. and Stapleton, J., 2006. Literature review of concepts: Psychological resiliency (No. DRDC-CR-2006-073). Vancouver, BC: British Columbia University.
- Wang, Y., Liu, J. and Zhu, Y., 2018. How does humble leadership promote follower creativity? The roles of psychological capital and growth need strength. *Leadership & Organization Development Journal*, 39(4), 507-521.
- Williams, H. M., Parker, S. K. and Turner, N., 2010. Proactively performing teams: The role of work design, transformational leadership, and team composition. *Journal of Occupational and Organizational Psychology*, 83(2), 301-324.

## 強化國軍雲端服務存取權限機制之設計

蘇品長 黃琮仁 蘇泰昌\*

國防大學資訊管理學系

論文編號：NM43-01-06

來稿 2022 年 2 月 24 日→第一次修訂 2022 年 3 月 8 日→第二次修訂 2022 年 3 月 30 日→

同意刊登 2022 年 4 月 13 日

### 摘要

隨著科技日新月異，雲端空間之使用已進入普及的時代，綜觀民間企業及政府機關均有使用雲端空間功能提供客戶服務或是提供內部員工快速取得所需資料。國軍為達資訊快速傳遞及系統統一管理，故亦須使用雲端空間，惟現行國軍在使用者管理上，僅使用 AD 帳號及密碼的認證方式來登入各項系統，若其帳密遭竊將有機敏洩漏疑慮。本研究將基於橢圓曲線密碼系統、隨機背包密碼系統及結合智慧卡，利用相比 RSA 加密演算法擁有較小的密鑰長度且可達相同安全性的橢圓曲線密鑰與隨機背包密碼系統運算效能快，來強化國軍雲端服務系統的資訊安全及處理速度。

**關鍵詞：**雲端架構、身分認證，混合式金鑰系統

---

\* 通訊作者：蘇泰昌 email: believe50405@gmail.com

## **The Enhancement of Information Security for the Access Authority of Military Cloud System**

**Su, Pin-Chang   Huang, Cong-Ren   Su, Tai-Chang \***

**Department of Information Management, National Defense University.**

### **Abstract**

With the rapid development of technology, the application of cloud space had already entered the general era. More and more private enterprises and government agencies had utilized the cloud space to provide services for their customers or rapidly information acquisition for their employees. To achieve rapid information transmission and system unified management, it is necessary for the National Army to implement cloud space systems. However, only the Active Directory (AD) account and password were used in current National Army user management for the authentication to enter various systems. Therefore, there will be a risk of sensitive leakage if the accounts were been stolen. In this study, the information security and process speed of the cloud space service system of the Nation Army will be enhanced based on the Elliptic Curve Cryptography (ECC), random backpack cryptography system and combined with smart cards, taking the advantages of an elliptical curve key with a smaller key length compared to the RSA encryption algorithm and achieving the same security and random backpack cryptography system operation.

**Keywords:** Cloud Architecture, Identity Authentication, Hybrid Cryptosystem System.

---

\* Corresponding Author Email: believe50405@gmail.com

## 一、前言

雲端時代的到來，影響了我們對 IT 基礎設施管理的思維方式，舉例來說，以軟體服務為基礎的供應商（Service Provider, SP）現在可以透過硬體平台外包方式，發展應用程式、系統或平台等雲端服務；對於使用者來說，不再需要去擔心網路或系統的資源是否充足，基礎設施是否能夠符合需求等問題，只需要關心真正需要的服務是那些，並透過終端設備連接上網路即可取得所需的服務。

綜觀各國軍隊講求陸、海、空三軍聯合作戰，隨著科技進步、網路及航太發展快速，各軍之間亦仰賴戰情資訊同步掌握，方能達到資訊同步、協同作戰之目的，除了聯合作戰，資訊戰亦已成為軍事發展的重要環節，俄國於 2017 年首次承認組建第一支網軍，俄國上議院國防與安全委員會主席受訪時表示，資訊戰部隊主要是保護俄國的數據系統不受敵人攻擊，不會向國外發動任何網路攻擊，美國也於同年宣布將美軍網路司令部升級為最高級別的聯合作戰司令部，其重點強調，網路司令部將進一步強化美國的網路安全，也將加強與盟邦的合作，對全球網路安全威脅做出快速反應（王子承，2017），中共在 2019 年發布的報告中談到，已將「網路安全」與核武、導彈及太空等傳統軍事項目並列，並以相當篇幅論述網路安全面臨的威脅及後續發展規劃，其內容除證實相關國家的警訊外，更符合中共國家主席習近平所提出「沒有網路安全，就沒有國家安全」的指示（劉嘉偉與張家瑛，2021，轉引自中共國防部，2019 與中共新聞網，2018）；但凡可運用電腦及使用網路連線之地點，都有可能成為敵方從事網路攻擊的目標，一旦網路遭受攻擊而癱瘓，將使整個國家受到極大的危害，因此，在面對軍事強國大量運用網路科技的威脅下，如何確保軍隊機敏資訊不外洩、特定資訊如何讓特定人員安全的使用等網際網路安全工作，將成為我軍發展科技作戰時必須重視的問題。

考量我國國軍雲端整合服務及運用上傳遞的大多為機敏情資，為防止資訊傳遞遭受非法存取或惡意存取等行為，並且在各軍種任務屬性不同所需存取雲端中資訊服務，故在系統建置上需要加速資料傳遞及資訊同步並設計更安全的身分認證機制，且必須為不同任務屬性使用者設定不同資料存取權限；因此，本研究所提方法係運用橢圓曲線密碼系統（Elliptic Curve Cryptosystem, ECC）演算法加上改良式隨機背包密碼系統（Random Knapsacks Cryptosystem, RKC）強化系統身分認證及資料交換方式，設計擁有處理時效快、安全性較高且彈性之演算法，做為依不同需求服務之身分驗證及存取權限控制方法，並結合國軍自行研發智慧卡（Smart Card）及一次性密碼的認證機制加強資料傳輸時的安全性，使各軍種合法認證使用者可自行依實際所需向國軍雲端服務中心提出功能使用服務及權限變動，亦可於臨時性任務需求時啟用相對應功能服務並獲取相關資訊。且在國軍雲端後端管理伺服器僅儲存依合法使用者需求所產生之功能服務及權限種類代數，如遭有心人士擷取，亦無法得知授權之功能服務及權限，符合資訊安全所需之管控與資料傳輸存取需求，加上橢圓曲線密碼加解密速度快等優點，期望達成下列目的：

- 設計動態修改權限存取控制方法，以降低雲端服務伺服器因權限集中控管之負擔，增進服務之即時性及國軍分層管制需求，且當使用者與雲端服務系統伺服器間建立認證後，可將所授權之任務功能及使用權適時調整，以提升運用彈性。
- 系統管理者僅存放公開之權限序列及加密保護之權限值，即使攻擊者獲取相關權限值，亦將面臨密碼解譯難題，無法在短時間內完成破解，且可避免服務提供者保留使用者相關參數資料。
- 不同使用者在資訊傳遞及資料交換時，均須透過存取權限認證機制後才可進行，除可依照軍種任務特性分類提高安全性外，透過高效率的運算，亦可加速存取權限認證程序。

## 二、文獻探討

本章分類整理、歸納分析與本研究相關的文獻，首先概述國軍跨軍種資料交換暨雲端架構進行介紹，接著針對雲端運算安全、身分認證機制及密碼學等與本研究有關的技術，加以彙整作為本研究的基礎。分述如後：

### 2.1 國軍跨軍種資料交換暨雲端架構

國軍跨軍種資料交換及雲端架構可概分為現行及未來推展進行說明，以現行雲端架構（如圖 1）來說，在雲端上使用之系統由各軍種機房自行維護，目前較為廣泛使用在公文處理系統、人事管理及門禁休請假系統。前述相關系統雖已使用個人帳密及智慧卡執行，在資料傳遞上仍是以明文方式進行傳輸，有心人士仍可駭進主服務中心端竊取或破壞相關資訊，影響資訊安全，而資料交換則因考量洩密風險尚無規劃軍種間使用雲端資料交換，各軍種僅開放單位間網域磁碟使用。

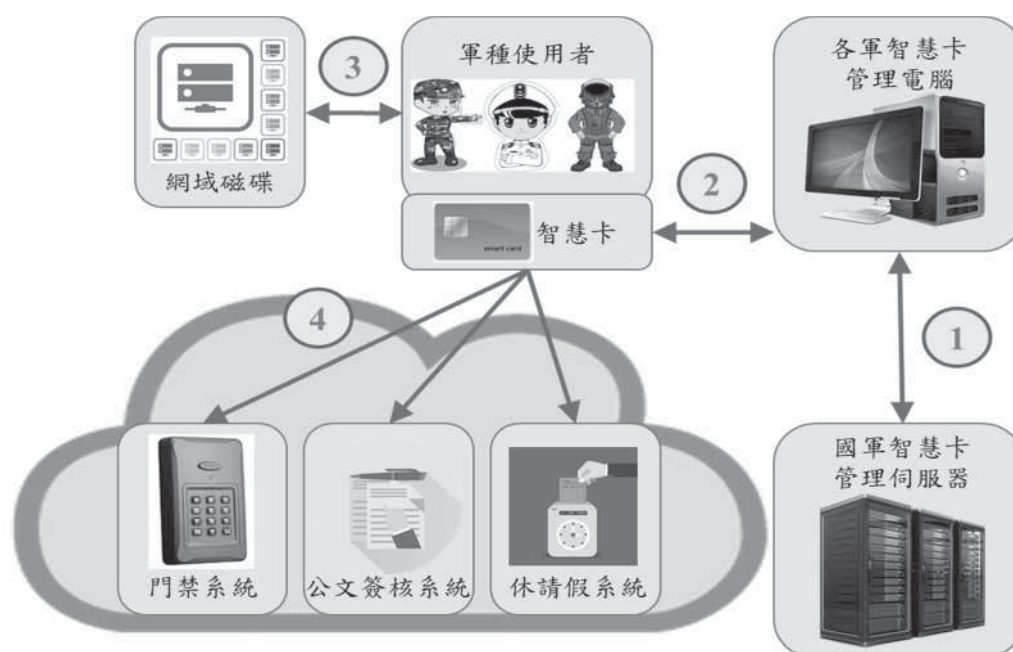


圖 1 國軍資料交換暨雲端架構示意圖

未來隨著科技蓬勃發展，作戰型態轉變，平時如何有效掌握各軍戰備整備情況，戰時如何快速提供各軍即時敵情、迅速與友軍共享部隊資訊將是國軍首重的課題，以現行營門管制為例，舊有的門禁管制主要區分為紙本管制及單點門禁系統，前者須簽奉營區權責長官才能入營，後者則是透過單位門禁系統管制入營，但各單位間使用的系統無法互通，即進入不同營區需有不同智慧卡導致個人與單位管理不易；國防部遂規劃推動全軍雲端整合運用，取代以往資料傳遞模式，並統一全軍門禁雲（如圖 2），往後只需雲端認證身分即可透過同一張智慧卡赴全軍各陣地執行公務，有效減少紙本作業，而門禁休請假及公文管理雲的統一只是其中的環節，重要的是建置一龐大的雲端存儲空間，提供全軍同仁使用及資料交換，這樣的措施不只縮短了軍種間資料傳遞及分享的時效，讓跨軍種公務協調更有效率，亦可使上層管理單位可同時快速傳達重要命令給不同單位，然而在新架構下，使用者的存取權限及資料傳遞上具有安全性上的疑慮，因此本研究便是在此架構下提出改良，以強化其安全性。

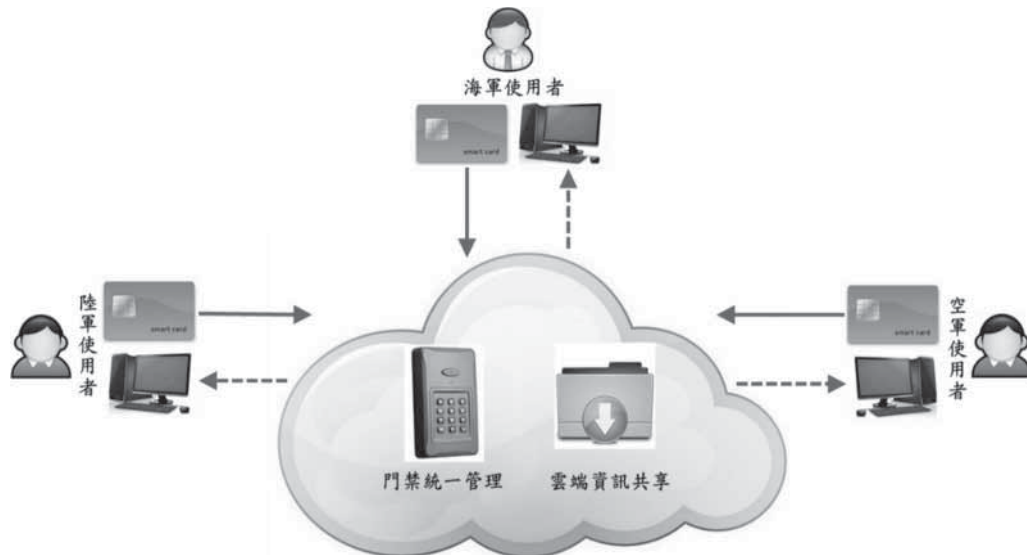


圖 2 國軍未來全軍雲端整合架構示意圖

## 2.2 雲端運算存取權限與安全

依據 NIST 的定義 (Mell and Grance, 2011)，雲端運算是一個模式，能隨時依照需求且便利的透過網路存取設定好的共享運算資源池（如網路、伺服器、儲存裝置、應用程式與各種服務），可以最少的管理工作或服務供應商互動，進行快速配置和發佈，強調雲端運算能按照使用者的需求，進行資源的靈活調配。這種雲端模型提升了服務可用性，可分為五個基本特徵（隨需自助服務、可隨時隨地存取網路、共享資源池、快速彈性與可量測得服務）、三個服務模式（架構即服務 IaaS、平台即服務 PaaS 與軟體即服務 SaaS）及四種佈署模型（私有雲端、社群雲端、公用雲端與混合雲端）。

在存取權限方面，現有知名的雲端運算平台包含 Eucalyptus、OpenStack 及 OpenNebula，將重點介紹這些平台在身分管理上的服務，Eucalyptus 是一種開源私有云軟件，用於構建與 Amazon Web Service (AWS) API 兼容的計算、網路和存儲的私有或混合雲資源，其預設將所有身份存儲在本地雲端控制器 (CLC) 數據庫中 (Eucalyptus Identity and Access Management IAM, 2012)，身份數據也可以從 LDAP 或 AD 中存取，然而在 2017 年發現一些未知功能的使用會使其機密性、完整性和可用性受到影響 (Hewlett Packard Enterprise Development, 2017)；OpenStack 是一個開源雲計算項目，自 2010 年發布以來迅速發展 (Kumar et al., 2014)，其預設身份管理系統是 Keystone，現有的 Keystone 是集中式的，所有用戶都需要在其數據庫中註冊，由 OpenStack 管理員手動或通過從企業數據庫批量加載，然後再使用訪問任何服務，這種設計在使用上有諸多限制且在 2017 年也有發現其安全漏洞 (Abdulla, N., & Erçelebi, E., 2017)；OpenNebula 於 2005 年成立，許多企業在其基於 VMware 上用作開放的雲虛擬化基礎架構，從而實現高度可擴展的託管環境，OpenNebula 包括一個完整的用戶和群組管理系統，通常存取透過內部的用戶帳號密碼進行認證，但也可透過外部身份驗證驅動程序，但在網路性能上遠不及前二者，容易導致網路中斷問題 (Brummett et al. 2015)。

雲端安全聯盟 (Cloud Security Alliance, CSA) 於 2013 年發表的文章中指出，雲端運算服務中最常見的安全威脅，包括資料洩漏、資料遺失、帳號詐騙或服務劫持、不安全的軟體介面、阻絕服務攻擊、內部員工的惡意行為、雲端服務的濫用、審慎評鑑不足、共享技術的漏洞等 9 項 (CSA, 2013)。面對上述的安全威脅，該聯盟早在 2011 年時便闡述雲端運算所面臨的資訊風險及其對應的安全性建議，並提出建構雲端運算安全架構的方法：以「雲端架構 (Cloud Architecture)」、「雲端治理 (Governing in the Cloud)」，

「雲端營運 (Operating in the Cloud)」三部分為主，再細分成十四項安全領域進行評估，其中「第五項」安全領域「資訊管理與資料安全」：提出必須依照機密性、完整性、可用性，以及資料的生命週期，實施相對應的控制措施及「第十一項」安全領域「加密與金鑰管理」：加密與金鑰管理是雲端運算資料保護的核心機制，在雲端環境中，用戶不應依賴雲端供應商所提供的加密安全機制，應當在機敏性資料傳輸至雲端前，利用適當的加密機制（標準且高安全強度的演算法）或資安產品將資料加密，當資料從原先受到良好控制的環境（CSA, 2011）。

### 2.3 身分認證機制

身分認證途徑可看作存取控制 (Access Control) 為最需重視的一環，用戶端必須先與認證伺服器證明自己的身分，來獲得授權 (Authorization)，才有讀寫、執行及刪除等權限，以下介紹幾種常見的認證方式：

- 使用者帳號/密碼 (Username and Password)：現行普遍的方法，由使用者先向伺服器註冊用戶帳號及密碼，登入時必須輸入正確的帳號及密碼，伺服器才會提供正確的資訊及服務。帳號及密碼是相對靜態的，除非使用者自行更改，否則將維持不變，而使用者為提高靜態密碼的安全性，將定期對密碼進行修改或增加密碼的難度，但此舉容易造成密碼不易紀錄，所以使用者使用容易記住的密碼或以明碼紀錄保存，易遭有心人士破解或外洩。因為密碼是靜態的數據，身分認證機制在使用方面非常簡單，且驗證過程中很容易被攔截及破解，從安全性上來講，已經無法滿足網際網路對於身分認證安全性的需求（黃建衛，2011）。
- 一次性密碼 (One Time Password, OTP)：一種產生單次使用密碼的機制，由學者 Lamport (1981) 首先提出，可以確保密碼不會被連續重複使用。當使用者輸入帳號，準備登入系統時，必須再鍵入顯示在此裝置螢幕上的密碼，由後端驗證系統進行核對，使用過後立即失效，若遭受重複使用亦無法獲得系統的存取，藉此保護系統所提供服務之安全性，也保護使用者身分不易因此遭受盜用。其原理是植入一把對稱式金鑰 (Symmetric Key)，再以時間、使用次數或輸入內容等參數為變動值，經由特定的加密演算法及雜湊函數運算，再將結果轉換成密碼。
- 智慧卡 (Smart Card)：一種具運算能力、儲存功能及自我保護的硬體，使用時為證明持有人確實為該卡的授權使用者，必須鍵入預先設定的密碼，並與卡片內儲存的密碼驗證無誤後方能運作。智慧卡具有儲存功能，通常會在卡片上植入一把對稱式金鑰，當使用者完成密碼驗證後，卡片與伺服器會進行挑戰與回應的驗證機制。先由伺服器送數值到卡片並以內建的對稱式金鑰運算後，將密碼送回伺服器後，再以卡片對應的對稱式金鑰進行運算比對，以確認使用者的合法性。

### 2.4 密碼學理論

密碼學 (Cryptography) 既指秘密書寫、加密訊息、隱藏訊息內容的科學，同時也泛指與密碼有關的科學，其中當代密碼系統則應提供機密性、完整性、身分認證及不可否認性等四大功能（鄧安文，2018），而如何強化密碼系統的安全性，取決於演算法的強度、金鑰保護的機制及加密長度，在幾經許多密碼學家與研究學者的努力下，越來越多的加密演算法也漸漸被提出，在本研究中選擇使用橢圓曲線密碼學及隨機背包密碼系統加入機制演算法推導，其優勢概述如後：

橢圓曲線在代數學和幾何學上廣泛研究已超過百年，其理論已豐富且深奧，但在當時沒人認為橢圓曲線有何實質用途；自從 Miller (1985) 及 Koblitz (1987) 兩位學者分別提出橢圓曲線的應用後，橢圓曲線開始在密碼學領域受到重視。與基於大質數因數分解的 RSA 等加密方法不同，其定義為在射影平面上滿足 Weierstrass 方程式所有點的集

合。在密碼學應用上，則主要應用在有限域  $GF(q)$  中取質數  $p$  ( $p > 3$ ) 同餘的橢圓曲線群，以  $E: y^2 = x^3 + ax + b \pmod{p}$  來表示，其中  $a, b$  為小於  $p$  之正整數，且  $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ 。另在橢圓曲線的定義中存在一個元素  $O$ ，稱為無窮遠點，一般可視為在  $Y$  軸上方無窮遠處（張鈞富，2014）；而相比 RSA 等非對稱式加密，其優勢在於安全性相同的前提下，可使用較短的私密金鑰，非常適合在資源有限環境下使用（如智慧卡、智慧型手機及無線行動裝置）。一般認為， $q$  位元域上的 ECC，當  $q$  的長度為 160 位元時，其安全性相當於 RSA 演算法使用 1024 位元模數（如表 1）。私密金鑰較短意味著所需要電腦網路的頻寬和記憶體較小，在執行速度方面較現存其他相對應的離散對數密碼系統要快，且在簽名和解密方面也比 RSA 快（Materese, 2016）；此外，假設一個橢圓曲線是屬於  $F_q$ ，而  $G$  是橢圓曲線  $E$  上一點，給定一個屬於橢圓曲線上的點  $G'$ ，若要找出一整數  $k$  使得  $kG = G'$ ，因其特殊的點加法運算，破密者除了逐一窮舉所有可能的點之外，別無他法。直至目前為止，除了建置成本龐大的量子電腦外，此問題仍符合實際安全。

表 1 橢圓曲線密碼系統與 RSA 在相同安全度下金鑰長度之比較表

|       | 金鑰長度  |       |       |        |        |        |
|-------|-------|-------|-------|--------|--------|--------|
| ECC   | 112   | 163   | 224   | 256    | 384    | 512    |
| RSA   | 512   | 1024  | 2048  | 3072   | 7680   | 15360  |
| 金鑰長度比 | 1 : 5 | 1 : 6 | 1 : 9 | 1 : 12 | 1 : 20 | 1 : 30 |

資料來源：Materese, 2016

背包密碼系統設計思想是把易解背包問題偽裝成一個看似困難的背包問題，其安全性植基於求子集和問題的困難性，假設手邊有一堆物品，其每件物品重量各異之物品表示為  $(v_1, v_2, \dots, v_n)$ 。並以一個背包能固定裝載物品重量計為  $V$ ，如果知道每件物品的重量時，是比較容易知道找出其物品的組合來裝滿這背包，但若只知道背包的總重量時，要反推有哪些未知物品在背包內時就很困難，此即為背包難題（Odlyzko, 1990）。

$$v = v_1y_1 + v_2y_2 + \dots + v_ny_n, \text{ 其中 } v_n \ (i = 1, 2, \dots, n) \in \{0, 1\};$$

$$y_i = 0 \text{ 表示不在背包內, } y_i = 1 \text{ 表示在背包內。}$$

物體重量的序列  $W = (v'_1, v'_2, \dots, v'_n)$ ，其背包向量  $\sum_{i=1}^n v'_n = v$ 。（ $v'_n = v_n y_n$ ）

這個問題，已被證明是一個 NP-Complete 問題（Michael and David, 1979），因此背包密碼系統不是在多項式時間內可解決之問題。基於背包加密系統其優點為加解密較快，缺點是其系統中超增序列的數值密度太低，造成背包密碼系統被破解（Brickell, 1984）。針對背包密碼系統後續有許多學者提出優化，為改良型隨機背包密碼系統（王青龍與趙祥模，2015），提出運用加法及模運算優化其計算時間，另將超遞增背包隱藏在隨機選擇的背包向量中，能抵抗低密度攻擊，其流程如下：

密鑰生成階段：

- 隨機選取任一超遞增背包向量  $\hat{g} = (g_1, g_2, \dots, g_n)$ 。
- 任意選取兩個背包量  $\hat{u} = (u_1, u_2, \dots, u_n)$ ， $\hat{z} = (z_1, z_2, \dots, z_n)$ ， $u_n, z_n$  均為正整數且滿足  $g_n = u_n + z_n, n = 1, \dots, n$ 。
- 隨機取兩個整數  $F_1$  和  $F_2$  為私鑰， $F_1 \geq \sum_{i=1}^n u_n, F_2 \geq \sum_{i=1}^n z_n; \gcd(F_1, F_2) = 1$
- 求出公鑰  $A$  使用中國餘式定理
- $a = (a_1, a_2, \dots, a_n)$

- $a_n \equiv u_n \pmod{F_1}, a_n \equiv z_n \pmod{F_2}, n = 1, 2, \dots, n$

加密階段：

- 將訊息 $m$ 轉換為二進位  $n$  bit,  $(m)_2 \in \{0,1\}$ 。
- 將訊息 $(m)_2$ 與公鑰 $A$ 做加密。
- 密文 $C = A \times (m)_2$ 。

解密階段：

- 接收到密文 $C$ 後，計算訊息 $m$
- $c_p = C \pmod{F_1}$
- $c_q = C \pmod{F_2}$
- 令 $g = c_p + c_q$ ，由 $g$ 和超遞背包 $(g_1, g_2, \dots, g_n)$ 便可恢復明文。

### 三、本研究設計

本研究提出一個有別於傳統的存取控制須依賴龐大資料庫及承受管理負擔與風險等問題之機制設計。此機制角色區分軍種使用者、各軍智慧卡管理系統、國軍雲端服務平臺及國軍認證中心，利用國軍雲端服務平臺的分散式架構，整合現有國軍系統，避免各系統僅存放集中式資料庫，並利用智慧卡管理系統整合各系統的金鑰管理，實現一人一卡登入多系統且不同系統擁有不同的存取權限；研究流程則區分為系統初始、註冊申請、驗證取得及服務使用等4階段（如圖3）。

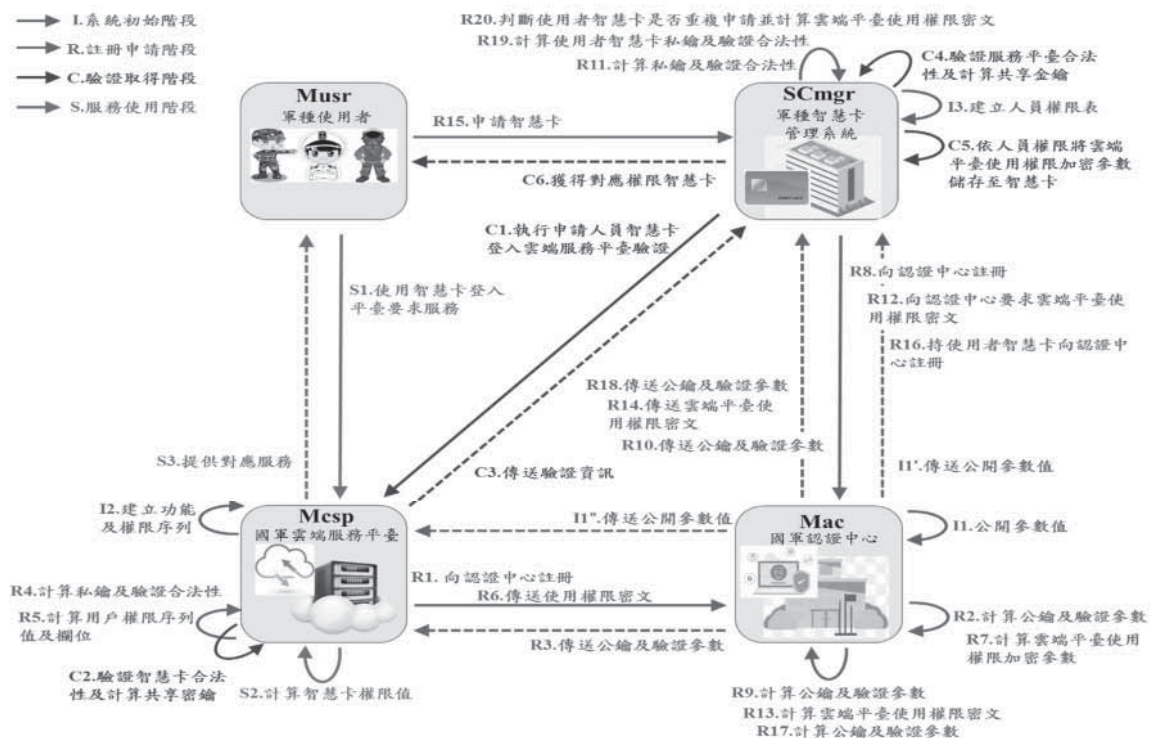


圖3 研究機制流程圖

## 3.1 研究參數及符號說明

本研究各階段使用之符號參數，如表 2 所示。

表 2 研究機制符號說明表

| 項次 | 符號                             | 說明                                          | 項次 | 符號                             | 說明                         |
|----|--------------------------------|---------------------------------------------|----|--------------------------------|----------------------------|
| 1  | Musr                           | 軍種使用者                                       | 22 | $rm_x$                         | 註冊者 $x$ 選取的隨機參數            |
| 2  | SCmgr                          | 軍種智慧卡管理系統                                   | 23 | $ID_x$                         | 註冊者 $x$ 的身分憑證              |
| 3  | Mac                            | 國軍認證中心                                      | 24 | $sig_x$                        | 註冊者 $x$ 的數位簽章              |
| 4  | Mcsp                           | 國軍雲端服務平臺                                    | 25 | $SK_{yz}$                      | 兩角色 $y$ 、 $z$ 間的共享金鑰       |
| 5  | $m_{crd}$                      | Musr 的國軍智慧卡                                 | 26 | $AC1_{mgr}, AC2_{usr}$         | 功能使用權限密文                   |
| 6  | $E(F_q)$                       | 橢圓曲線， $F_q$ 為有限域， $q$ 為一大於 $2^{224}$ 以上之大質數 | 27 | $AU_{usr}, AT_{usr}$           | 用於計算 $AC2_{usr}$ 權限密文過程參數點 |
| 7  | $n$                            | 橢圓曲線上基點的階數 (order)                          | 28 | $rc_{crd}, rc_{csp}$           | 隨機亂數用以建立通訊金鑰               |
| 8  | $G$                            | 橢圓曲線中階數為 $n$ 之基點                            | 29 | $CK_{us}$                      | Mcsp、 $m_{crd}$ 的通訊金鑰      |
| 9  | $\mathcal{O}$                  | 橢圓曲線的無窮遠點                                   | 30 | $(ms_x, ms_y)$                 | Mcsp 的公鑰                   |
| 10 | $h()$                          | 單向無碰撞之值雜湊函數                                 | 31 | $(sc_x, sc_y)$                 | SCmgr 的公鑰                  |
| 11 | $H(), Ver()$                   | 單向無碰撞之點雜湊函數                                 | 32 | $(cr_x, cr_y)$                 | $m_{crd}$ 的公鑰              |
| 12 | $u, v / \bar{u}, \bar{v}$      | 隨機向量／向量參數 (隨機背包)                            | 33 | $Ekey_{csp}$                   | 雲端服務平臺對應欄位加密金鑰             |
| 13 | $j_m, k_m, j_n, k_n$           | 隨機參數 (隨機背包)                                 | 34 | $\bar{A}$                      | Musr 所持 $m_{crd}$ 的加密權限    |
| 14 | $\tilde{u}, \tilde{v}$         | 超增序列值                                       | 35 | $\bar{R}$                      | Mcsp 計算出 $m_{crd}$ 的權限參數點  |
| 15 | $\hat{u}_{mgr}, \hat{v}_{mgr}$ | 雲端服務平臺使用權限對應表                               | 36 | $T_{crd}, T_{csp}$             | $m_{crd}$ 、Mcsp 的時戳驗證參數    |
| 16 | $uSC_{crd}, vSC_{crd}$         | 使用權限種類值、功能權限值                               | 37 | $\mathbb{T}$                   | 時戳門檻                       |
| 17 | $sn_{crd}, ad_{crd}$           | Musr 的智慧卡 $m_{crd}$ 使用 (功能) 權限對應值           | 38 | $Ver(McspA), Ver(McspB)$       | 驗證 Mcsp 身分之參數              |
| 18 | $SK, MK, DK, CK$               | SCmgr、Mcsp、 $m_{crd}$ 、Mac 公開金鑰             | 39 | $Ver(m_{crd}1), Ver(m_{crd}2)$ | 驗證 $m_{crd}$ 身分之參數         |
| 19 | $sk, mk, dk, ck$               | SCmgr、Mcsp、 $m_{crd}$ 、Mac 私密金鑰             | 40 | RequetService                  | Musr 向 Mcsp 請求使用雲端平臺服務     |
| 20 | $id_{mgr}, id_{csp}$           | SCmgr、Mcsp 之身分 ID 識別                        | 41 | AcceptService                  | Mcsp 向 Musr 回傳是否同意服務訊息     |
| 21 | $rd_x$                         | Mac 對應註冊者 $x$ 選取的隨機參數                       |    |                                |                            |

### 3.2 研究機制各階段流程及演算法

本節分別針對機制設計系統初始、註冊申請、驗證取得及服務使用階段之傳輸內容及步驟做說明。

#### 3.2.1 初始階段

國軍認證中心、軍種智慧卡管理系統及國軍雲端服務平臺在此階段執行後續流程所需參數及權限規劃，作業分述如下：

- I1. 國軍認證中心在有限域 $F_q$ 上，選取一安全橢圓曲線 $E(F_q)$ ，並在 $E(F_q)$ 上選取一階數為 $n$ 的基點 $G$ ，使得 $n \cdot G = O$ ；接著選定私密金鑰 $ck$ 後，計算出公開金鑰 $CK$ 並公開系統相關參數 $E(F_q)$ 、 $G$ 、 $n$ 、 $h()$ 、 $H()$ 、 $Ver()$ 及 $CK$

$$CK = ck \cdot G \quad (1)$$

- I2. 國軍雲端服務平臺在此階段建立功能服務及權限對應序列表。
- I3. 軍種智慧卡管理系統在此階段建立人員權限表，以利後續人員申請，可依該申請人員權限核發權限對應之國軍智慧卡( $m_{crd}$ )。

#### 3.2.2 註冊申請階段

- R1. 國軍雲端服務平臺首先使用國軍認證中心的公開參數，並產生一組隨機參數 $rm_{csp} \in [2, n-2]$ 後，國軍雲端服務平臺將身分識別 $id_{csp}$ 與國軍認證中心公開參數計算得身分憑證 $ID_{csp}$ ，將 $id_{csp}$ 、 $ID_{csp}$ 傳送至國軍認證中心申請註冊。

$$ID_{csp} = h(rm_{csp} \parallel id_{csp}) \cdot G \quad (2)$$

- R2. 當國軍認證中心收到 $id_{csp}$ 、 $ID_{csp}$ 後，選取隨機參數 $rd_{csp} \in [2, n-2]$ 計算出國軍雲端服務平臺的公開金鑰 $MK$ 及簽章 $sig_{csp}$ 。

$$MK = ID_{csp} + (rd_{csp} - h(id_{csp})) \cdot G = (ms_x, ms_y) \quad (3)$$

$$sig_{csp} = rd_{csp} + ck(ms_x + h(id_{csp})) \quad (4)$$

- R3. 國軍認證中心回傳公開金鑰 $MK$ 及簽章 $sig_{csp}$ 給國軍雲端服務平臺。
- R4. 國軍雲端服務平臺於接收到公鑰 $MK$ 、簽章 $sig_{csp}$ 後，產生自己的私鑰 $mk$ ，並透過 $sig_{csp}$ 驗證 $MK$ 的合法性如下，若驗證符合將建立共享金鑰 $SK_{cspMac}$ 。

$$mk = sig_{csp} + h(rm_{csp} \parallel id_{csp}) \quad (5)$$

$$MK' = mk \cdot G \stackrel{?}{=} MK \quad (6)$$

$$SK_{cspMac} = mk \cdot CK = ck \cdot MK \quad (7)$$

- R5. 國軍雲端服務平臺分別計算使用者用戶類別與雲端平臺功能服務權限服務向量，並計算使用權限表密文，步驟如下：

- 選擇使用者類別與服務向量，並取隨機四個質數 $j_m$ 、 $k_m$ 、 $j_n$ 與 $k_n$ 。

$$\text{取隨機} m \text{ 向量 } u = \{u_1, u_2, \dots, u_m\}, u_i \text{ 為正整數。} \quad (8)$$

$$\text{取隨機} n \text{ 向量 } v = \{v_1, v_2, \dots, v_n\}, v_i \text{ 為正整數。} \quad (9)$$

$$\text{計算向量 } \bar{u} = \{\bar{u}_1, \dots, \bar{u}_m\}, \bar{u}_i = u_i - 2^{m-1}, i = 1, \dots, m \quad (10)$$

$$\text{計算向量 } \bar{v} = \{\bar{v}_1, \bar{v}_2, \dots, \bar{v}_n\}, \bar{v}_i = v_i - 2^{n-1}, i = 1, \dots, n \quad (11)$$

$$j_m > \sum_{i=1}^m u_i, k_m > 2 \max\{\sum_{\bar{u}_i > 0} \bar{u}_i, -\sum_{\bar{u}_i < 0} \bar{u}_i\} \quad (12)$$

$$j_n > \sum_{i=1}^n v_i, k_n > 2 \max\{\sum_{\bar{v}_i > 0} \bar{v}_i, -\sum_{\bar{v}_i < 0} \bar{v}_i\} \quad (13)$$

- 透過隨選 $j_m$ 、 $k_m$ 、 $j_n$ 與 $k_n$ 參數，並使用中國餘式定理求出使用者類別與功能服務權限序列值 $\tilde{u}$ 與 $\tilde{v}$ 。

$$\tilde{u}_i \equiv u_i \pmod{j_m}, \tilde{u}_i \equiv \bar{u}_i \pmod{k_m}, i = 1, \dots, m \quad (14)$$

$$\tilde{v}_i \equiv v_i \pmod{j_n}, \tilde{v}_i \equiv \bar{v}_i \pmod{k_n}, i = 1, \dots, n \quad (15)$$

$$\tilde{u} = \{\tilde{u}_1, \tilde{u}_2, \dots, \tilde{u}_m\}, \text{ 其中 } 0 \leq \tilde{u}_i \leq j_m k_m - 1 \quad (16)$$

$$\tilde{v} = \{\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_n\}, \text{ 其中 } 0 \leq \tilde{v}_i \leq j_n k_n - 1 \quad (17)$$

- 依軍種使用者軍種使用者使用權限劃分來設定平臺用戶參數 $\hat{u}_{mgr}$ 及功能使用參數 $\hat{v}_{mgr}$ ，並計算出提供軍種使用者使用之國軍智慧卡 $m_{crd}$ 的使用權限種類值 $uSC_{crd}$ 、功能權限值 $vSC_{crd}$ 、使用權限對應值 $sn_{crd}$ 及功能權限對應值 $ad_{crd}$ ，再運用與國軍認證中心的共享金鑰 $SK_{cspMac}$ 計算出權限密文 $AC1_{mgr}$ 。

$$\hat{u}_{mgr} = (\hat{u}_1, \hat{u}_2, \dots, \hat{u}_m), \hat{u}_m \in [0, 1] \quad (18)$$

$$\hat{v}_{mgr} = (\hat{v}_1, \hat{v}_2, \dots, \hat{v}_n), \hat{v}_n \in [0, 1] \quad (19)$$

$$uSC_{crd} = \sum_{i=1}^m \tilde{u} \times \hat{u}_{mgr} \quad (20)$$

$$vSC_{crd} = \sum_{i=1}^n \tilde{v} \times \hat{v}_{mgr} \quad (21)$$

$$sn_{crd} = uSC_{crd} \oplus m_{crd} \quad (22)$$

$$ad_{crd} = vSC_{crd} \oplus m_{crd} \quad (23)$$

$$AC1_{mgr} = (uSC_{crd}, sn_{crd} + ad_{crd}) + SK_{cspMac} \quad (24)$$

- R6. 國軍雲端服務平臺將權限序列值 $\tilde{u}$ 與 $\tilde{v}$ 權限密文 $AC1_{mgr}$ 傳送至國軍認證中心。
- R7. 國軍認證中心使用與國軍雲端服務平臺之共享金鑰 $SK_{cspMac}$ ，自 $AC1_{mgr}$ 解出 $uSC_{crd}$ 、 $vSC_{crd}$ 、 $sn_{crd}$ 及 $ad_{crd}$ ，並予以保留，以利後續軍種智慧卡管理系統向國軍認證中心註冊完成後取得。

$$AC1_{mgr} - SK_{cspMac} = (uSC_{crd}, sn_{crd} + ad_{crd}) \quad (25)$$

- R8. 軍種智慧卡管理系統首先產生一組隨機參數 $rm_{mgr} \in [2, n-2]$ 後，將身分識別 $id_{mgr}$ 與國軍認證中心所提供之公開參數執行計算出 $ID_{mgr}$ ，透過安全通道將 $id_{mgr}$ 、 $ID_{mgr}$ 傳送至國軍認證中心提出註冊需求。

$$ID_{mgr} = h(rm_{mgr} \parallel id_{mgr}) \cdot G \quad (26)$$

- R9. 當國軍認證中心接收到 $id_{mgr}$ 、 $ID_{mgr}$ 後，選取隨機參數 $rd_{mgr}$ 計算出軍種智慧卡管理系統的公開金鑰 $SK$ 及簽章 $sig_{mgr}$ 。

$$SK = ID_{mgr} + (rd_{mgr} - h(id_{mgr})) \cdot G = (sc_x, sc_y) \quad (27)$$

$$sig_{mgr} = rd_{mgr} + ck(sc_x + h(id_{mgr})) \quad (28)$$

- R10. 國軍認證中心回傳公開金鑰 $SK$ 及簽章 $sig_{mgr}$ 給軍種智慧卡管理系統。
- R11. 軍種智慧卡管理系統於接收公開金鑰 $SK$ 、簽章 $sig_{mgr}$ ，產生自己的私鑰 $sk$ ，並透過 $sig_{mgr}$ 驗證 $SK$ 的合法性，若驗證符合將建立共享金鑰 $SK_{mgrMac}$ 。

$$sk = sig_{mgr} + h(rm_{mgr} \parallel id_{mgr}) \quad (29)$$

$$SK' = sk \cdot G \stackrel{?}{=} SK \quad (30)$$

$$SK_{mgrMac} = sk \cdot CK = ck \cdot SK \quad (31)$$

- R12. 軍種智慧卡管理系統向國軍認證中心要求國軍雲端服務平臺的權限序列值 $\tilde{u}$ 與 $\tilde{v}$ 及權限密文 $AC1_{mgr}$ 。

- R13. 國軍認證中心使用與軍種智慧卡管理系統之共享金鑰 $SK_{mgrMac}$ 將國軍雲端服務平臺功能使用權限密文 $AC1_{mgr}$ 進行加密。

$$AC1_{mgr} = (uSC_{crd}, sn_{crd} + ad_{crd}) + SK_{mgrMac} \quad (32)$$

- R14. 國軍認證中心向軍種智慧卡管理系統傳送權限序列值 $\tilde{u}$ 與 $\tilde{v}$ 及功能使用權限密文 $AC1_{mgr}$ ，以利後續提供軍種使用者申請國軍智慧卡 $m_{crd}$ 之用。

- R15. 軍種使用者向軍種智慧卡管理系統提出國軍智慧卡 $m_{crd}$ 申請需求。

- R16. 軍種使用者在使用 $m_{crd}$ 向國軍雲端服務平臺要求功能服務前，須由軍種智慧卡管理系統使用當前申請的 $m_{crd}$ 與國軍認證中心進行註冊，首先於軍種智慧卡管理系統插入智慧卡 $m_{crd}$ 及提供一組隨機碼 $rm_{crd} \in [2, n-2]$ ，計算出 $ID_{crd}$ 後，將 $ID_{crd}$ 及 $m_{crd}$ 傳給國軍認證中心提出註冊需求。

$$ID_{crd} = h(m_{crd} \parallel rm_{crd}) \cdot G \quad (33)$$

- R17. 當國軍認證中心接收到 $ID_{crd}$ 、 $m_{crd}$ ，選取隨機參數 $rd_{crd}$ 計算出當前申請 $M_{crd}$ 的公開金鑰 $DK$ 及簽章 $sig_{crd}$ 。

$$DK = ID_{crd} + (rd_{crd} - h(m_{crd})) \cdot G = (cr_x, cr_y) \quad (34)$$

$$sig_{crd} = rd_{crd} + ck(cr_x + h(m_{crd})) \quad (35)$$

- R18. 國軍認證中心回傳當前申請 $m_{crd}$ 的公開金鑰 $DK$ 及簽章 $sig_{crd}$ 給軍種智慧卡管理系統。

- R19. 軍種智慧卡管理系統於接收到當前申請 $m_{crd}$ 的公開金鑰 $DK$ 、簽章 $sig_{crd}$ ，產生當前申請 $m_{crd}$ 的私鑰 $dk$ ，並透過 $sig_{crd}$ 驗證 $DK$ 的合法性，若驗證符合將建立共享金鑰 $SK_{crdMac}$ 。

$$dk = sig_{crd} + h(m_{crd} \parallel rm_{crd}) \quad (36)$$

$$DK' = dk \cdot G \stackrel{?}{=} DK \quad (37)$$

$$SK_{crdMac} = dk \cdot CK = ck \cdot DK \quad (38)$$

- R20. 軍種智慧卡管理系統計算國軍雲端服務平臺權限密文，以利後續依申請人員權限給予相關對應使用之權限密文，並判斷當前設定之 $m_{crd}$ 是否重複申請，程序如下：

- 軍種智慧卡管理系統使用與國軍認證中心之共享金鑰 $SK_{mgrMac}$ 計算出國軍雲端服務平臺功能使用權限密文 $AC1_{mgr}$ 取得 $m_{crd}$ 的註冊欄位 $uSC_{crd}$ 、位置欄位 $vSC_{crd}$ 、註冊序列值 $sn_{crd}$ 及位置值 $ad_{crd}$ 。

$$AC1_{mgr} - SK_{mgrMac} = (uSC_{crd}, sn_{crd} + ad_{crd}) \quad (39)$$

- 透過 $m_{crd}$ 註冊欄位 $uSC_{crd}$ 值對應出 $\tilde{u}$ 用戶註冊欄位，並使用註冊參數判斷該 $m_{crd}$ 是否註冊，若未註冊則建立其欄位加密金鑰 $Ekey_{csp}$ 。

$$AU_{usr} = (x_1, x_2) = ((uSC_{crd}, sn_{crd} + ad_{crd}) + Ekey_{csp}) \quad (40)$$

- 軍種智慧卡管理系統依當前軍種使用者權限等級所持之 $m_{crd}$ 對應功能使用權限計算出加密之權限表 $AC2_{usr}$ 。

$$AC2_{usr1} = rd_{mgr} \cdot G \quad (41)$$

$$AT_{usr} = rd_{mgr} \cdot SK = (y_1, y_2) \quad (42)$$

$$AC2_{usr2} = AU_{usr} \cdot AT_{usr} = (x_1 \cdot y_1, x_2 \cdot y_2) = (z_1, z_2) \quad (43)$$

$$AC2_{usr} = \{AC2_{usr1}, AC2_{usr2}\} \quad (44)$$

### 3.2.3 驗證取得階段

軍種智慧卡管理系統使用當前軍種使用者申請之 $m_{crd}$ 協助完成第一次連線認證作業，當作業完成後，由軍種智慧卡管理系統依當前軍種使用者權限提供對應 $m_{crd}$ ，軍種使用者下次登入時可直接使用國軍雲端服務平臺之功能，程序為 C1 至 C6。

C1. 軍種智慧卡管理系統使用 $m_{crd}$ 初次連線登入至國軍雲端服務平臺時， $m_{crd}$ 會先傳送時戳參數 $T_{crd}$ 與國軍雲端服務平臺的時戳參數 $T_{csp}$ 進行驗證，通過後即提供連線，若未能通過則中斷聯線，成功連線後則進行雙方身分驗證，並計算出共享金鑰及 Diffie-Hellman 金鑰傳送至國軍雲端服務平臺，程序如下：

- $m_{crd}$ 與國軍雲端服務平臺初次連線執行時戳參數驗證計算是否符合時戳門檻 $T$ 。

$$(T_{crd} - T_{csp}) \leq T \quad (45)$$

- $m_{crd}$ 與國軍雲端服務平臺驗證符合時戳門檻 $T$ 連線後，互相驗證身分是否合法。

$$dk' = DK + h(m_{crd}) \cdot G + (cr_x + h(m_{crd})) \cdot CK \quad (46)$$

$$dk \stackrel{?}{=} dk' \quad (47)$$

$$mk' = MK + h(id_{csp}) \cdot G + (ms_x + h(id_{csp})) \cdot CK \quad (48)$$

$$mk \stackrel{?}{=} mk' \quad (49)$$

- $m_{crd}$ 建立隨機參數 $rc_{crd}$ 後利用所選之橢圓曲線 $G$ 點計算出驗證點參數 $RC_{crd}$ ，並計算出共享金鑰 $SK_{cspcrd}$ 及 Diffie-Hellman 金鑰 $DHRC_{crd}$ 後傳至國軍雲端服務平臺。

$$RC_{crd} = rc_{crd} \cdot G \quad (50)$$

$$SK_{cspcrd} = mk \cdot DK = dk \cdot MK \quad (51)$$

$$DHRC_{crd} = RC_{crd} + SK_{cspcrd} \quad (52)$$

C2. 國軍雲端服務平臺建立隨機參數 $rc_{csp}$ 後利用所選之橢圓曲線 $G$ 點計算出驗證點參數 $RC_{csp}$ ，並計算出共享金鑰 $SK_{cspcrd}$ 及雙方 Diffie-Hellman 金鑰 $DH_{us}$ 後，求出雙方通訊金鑰 $CK_{us}$ 。

$$RC_{csp} = rc_{csp} \cdot G \quad (53)$$

$$SK_{cspcrd} = dk \cdot MK = mk \cdot DK \quad (54)$$

$$DHRC_{csp} = RC_{csp} + SK_{cspcrd} \quad (55)$$

$$RC_{crd} = DHRC_{crd} - SK_{cspcrd} \quad (56)$$

$$DH_{us} = rc_{csp} \cdot RC_{crd} \quad (57)$$

$$CK_{us} = DH_{us} + SK_{cspcrd} \quad (58)$$

C3. 國軍雲端服務平臺傳送驗證參數至 $m_{crd}$ 。

$$Ver(McspA) = H(m_{crd} \parallel id_{csp} \parallel DH_{us}) \quad (59)$$

$$Ver(McspB) = H(m_{crd} \parallel id_{csp} \parallel CK_{us}) \quad (60)$$

C4.  $m_{crd}$ 驗證參數及比對確認合法性，並回傳 $Ver(m_{crd}2)$ 參數至國軍雲端服務平臺驗證是否正確。

$$RC_{csp} = DHRC_{csp} - SK_{cspcrd} \quad (61)$$

$$DH_{us}' = rc_{crd} \cdot RC_{csp} \quad (62)$$

$$CK_{us}' = DH_{us}' + SK_{cspcrd} \quad (63)$$

$$Ver(m_{crd}1) = Ver(McspA) \quad (64)$$

$$Ver(m_{crd}2) = H(m_{crd} \parallel id_{csp} \parallel CK_{us}') \quad (65)$$

C5. 軍種智慧卡管理系統運用國軍雲端服務平臺、 $m_{crd}$ 的通訊金鑰 $CK_{us}$ 計算出智慧卡加密權限 $\vec{A}$ 並依人員權限等級將對應權限儲存至 $m_{crd}$ 中。

$$\vec{A} = AC2_{usr} + CK_{us} \quad (66)$$

軍種使用者取得對應職務權限之國軍智慧卡 $m_{crd}$ 。

### 3.2.4 服務使用階段

在軍種使用者使用國軍雲端服務平臺服務前，須用智慧卡 $m_{crd}$ 與國軍雲端服務平臺完成持有權限運算後，始可使用其提供之服務及功能。

S1. 軍種使用者運用儲存於智慧卡 $m_{crd}$ 內之通訊金鑰 $CK_{us}$ 解出加密之權限表 $AC2_{mgr}$ 後，向國軍雲端服務平臺傳送請求使用雲端平臺服務 RequetService 訊息及服務權限加密參數 $AC2_{usr}$ 。

$$AC2_{usr} = \vec{A} - CK_{us} \quad (67)$$

S2. 國軍雲端服務平臺在接收請求功能使用申請 RequetService 及服務權限加密參數 $AC2_{usr}$ 後，執行當前軍種使用者所持之 $m_{crd}$ 服務權限計算出 $\vec{R}$ ，並自 $AC2_{usr}$ 解出雲端服務平臺用戶及位址加密欄位，再依 $m_{crd}$ 註冊欄位金鑰後解出軍種使用者可使用的功能。

$$\begin{aligned} \vec{R} = (r_1, r_2) &= mk \cdot AC2_{usr1} \\ &= rd_{csp} \cdot (G \cdot mk) = rd_{csp} \cdot MK \end{aligned} \quad (68)$$

$$AU_{usr} = (AC2_{usr2} \cdot \vec{R}^{-1}) = (x_1, x_2) \quad (69)$$

$$(uSC_{crd}, sn_{crd} + ad_{crd}) = AU_{usr} - Ekey_{csp} \quad (70)$$

$$ad_{crd} = (sn_{crd} + ad_{crd}) - (uSC_{crd} \oplus m_{crd}) \quad (71)$$

$$vSC_{crd} = ad_{crd} \oplus m_{crd} = (vSC_{crd} \oplus m_{crd}) \oplus m_{crd} \quad (72)$$

$$(\hat{u}_{mgr})_2 = (uSC_{crd} \bmod j_m) - (uSC_{crd} \bmod k_m) \quad (73)$$

$$(\hat{v}_{mgr})_2 = (vSC_{crd} \bmod j_n) - (vSC_{crd} \bmod k_n) \quad (74)$$

S3. 國軍雲端服務平臺運用彼此通訊密鑰 $CK_{us}$ 將當前軍種使用者所持之 $m_{crd}$ 服務權限加密後回傳 AcceptService 訊息供軍種使用者正常使用服務。

## 四、安全性與效益分析

現行國軍跨軍種資料交換基於資安考量，且無身分辨證機制，故無建立軍種間雲端資料交換空間，仍以實體及檔案加密後以信箱或點對點方式傳輸給對方執行；而各類雲端系統，係各軍種使用者輸入 AD 帳號及密碼做為系統登入方式，若無有效及更安全的身分驗證機制，將導致不法人士偽冒侵入攻擊情事發生，並可能產生使用者帳戶遭不法人士盜取，延伸出機敏資料或情資外洩。本章節主要針對經研究後所提之強化及改善機制的安全性分析進行探討並與現有機制進行比較。

#### 4.1 機密性

本研究機制註冊申請階段中，Mcsp可就Musr層級類別中配賦雲端服務平臺使用權限表，將Musr相關註冊資訊送至Mac；透過Mac計算Musr之使用權限表密文 $AC1_{mgr}$ （如圖 3 R13）及Musr並透過智慧卡 $m_{crd}$ 安全存放 $\bar{A}$ 訊息（如圖 3 C5）達到多因子認證方式。

倘若不法人士想偽冒使用者身分，除了須擁有智慧卡多因子認證外，欲使用中間人攻擊方式來取得解密密文時，首先要破解並取得雲端服務平臺Mcsp提供 $m_{crd}$ 註冊、位置欄位與序列值加密金鑰（如圖 3 S1-2）而將面對橢圓曲線離散對數難題；即使不法人士以其他不當的方式取得欄位及權限類別序列值後，也須要解出欄位及權限類別序列，屆時將面臨隨機背包難題而無法輕易破解。

#### 4.2 完整性

本研究機制註冊申請階段中，Mcsp、SCmgr及使用者 $m_{crd}$ 選取隨機參數，計算各自身分憑證（如圖 3 R1-2、R8-9 及 R16-17）後傳送至Mac；經Mac雜湊運算並結合SCmgr、Mcsp及使用者 $m_{crd}$ 之身分憑證後，分別產生數位簽章並相互完成認證。

不法人士若欲破解將面臨單向雜湊函數及橢圓曲線離散難題；就算取得認證中心管理權限存取資料，但未能獲得私鑰（如圖 3 I1），或是竊得共享金鑰，否則將面對橢圓曲線解離散對數難題。

#### 4.3 可用性

本研究機制驗證取得階段中，SCmgr協助Musr申請之 $m_{crd}$ 與Mcsp確認彼此身分無誤後， $m_{crd}$ 與Mcsp將相互執行交換共享金鑰（如圖 3 C1）與通訊之金鑰（如圖 3 C2）；而在服務使用階段Musr所持之 $m_{crd}$ 使用Mcsp服務時，Mcsp再依據Musr所持之 $m_{crd}$ 之對應權限（如圖 3 S2），將彼此間的通訊金鑰運算出結果後以加密後回傳AcceptService訊息至Musr所持之 $m_{crd}$ 來同意使用雲端服務平臺之各項功能與服務。

不法人士欲偽冒Musr或Mcsp身分時，須面臨橢圓曲線離散對數難題，使不法人士因無授權沒辦法通過身分驗證而終止連線服務，亦可避免Mcsp遭重送式攻擊（Replay attack）而造成的服務中斷，避免Musr因無法執行對應服務而影響業務執行成效。

#### 4.4 不可否認性

本研究機制驗證取得階段中，SCmgr使用當前Musr申請之 $m_{crd}$ 將產生雲端服務平臺欄位權限密文，而Musr申請之 $m_{crd}$ 與Mcsp間生成共享金鑰（如圖 3 C1）與通訊金鑰（如圖 3 C2）；在後續於服務使用階段中，Musr所持之 $m_{crd}$ 提出資料存取及功能服務時，Mcsp再依據Musr所持之 $m_{crd}$ 身分別及功能使用權限，運算結果以其通訊金鑰加密後，回傳Musr

在本研究機制服務使用階段中，Mcsp以其私鑰解密且產製通訊金鑰（如圖 3 C2）過程中，其Musr所持之 $m_{crd}$ 與Mcsp之個人資訊亦包含其中（如圖 3 C4 及 S2），彼此無法否認雙方之前所執行過的關鍵行為。

#### 4.5 存取控制

本研究機制驗證取得階段中，首先將驗證當前申請之 $m_{crd}$ 與Mcsp雙方時戳（如圖 3

C1)，保證在時效內連線，否則將取消，通過後將依照Musr所持之 $m_{crd}$ 應俱備之權限等級，以序列方式定義權限表並利用隨機背包密碼系統計算Mcsp於註冊申請階段向Mac註冊之功能權限值及權限表（如圖 3 R5）；於服務使用階段中，僅回傳當前申請之 $m_{crd}$ 雲端服務平臺使用權限之運算結果。

若發生未授權人士盜用Musr身分，利用Musr來向Mcsp提出雲端服務平臺使用服務時，將經過Mcsp驗證，期間Mcsp判斷為非法授權用戶，Mcsp將否絕其服務使用之請求，以達存取控制與使用權管控之目的；而在使用者Musr所持之 $m_{crd}$ 遭人盜用情況下，也因無法得知該Musr所設定之 $m_{crd}$ 個人密碼導致無法使用。

#### 4.6 身分認證

本研究機制註冊申請階段中，Mcsp及Musr申請之 $m_{crd}$ 向Mac完成註冊後獲得各自公鑰及簽章後（如圖 3 R2-4 及 R17-19），相互傳送認證資訊而無須與Mac保持連線，可離線相互完成身分認證後，建立共享金鑰與通訊金鑰，以Musr申請之 $m_{crd}$ 對Mcsp實施認證為例（如圖 3 C1）。

Musr及Mcsp雙方執行身分認證時，在持有對方之公開認證資訊與Mac之公鑰，可不用經過Mac來獨立進行身分認證。若不法人士欲偽裝Musr或Mcsp身分時，將面臨橢圓曲線離散對數難題而被否決；另外再驗證取得階段中，智慧卡管理系統SCmgr以標準政策給予合法使用者所能擁有之權限，防止未經授權使用者構連藉以提升系統安全性。

#### 4.7 抗同謀碰撞攻擊

本研究機制註冊申請階段中，Musr申請之 $m_{crd}$ 公鑰及私鑰非直接由Mac產製及保管，為結合身分識別、簽章、隨機參數（如圖 3 R16-17）及Mac之隨機參數計算出來的，用以避免遭非授權人員與Mac串聯肆意竊取。

本研究機制中，Mac僅參與計算公鑰過程，無法直接產生、偽造Musr申請之 $m_{crd}$ 私鑰，且Mac未參與服務使用階段，故Mcsp以私鑰並非透過Mac解密資訊取得Musr所持之 $m_{crd}$ 相關權限值資料，有效避免非授權人員藉Mac擁有多項參數之便，防阻同謀攻擊。

#### 4.8 資料保密

本研究機制註冊申請階段中，由Mcsp產生超增序列值（如圖 3 R5）提供Musr使用 $m_{crd}$ 對應的註冊欄位、位置欄位、註冊序列值及位置值建立加密參數。

若不法人士欲由數值反推註冊欄位定義及權限序列，將面臨破解隨機背包難題，而欲破解權限值密文時，亦將面臨破解橢圓曲線離散對數難題而難以達成。

#### 4.9 本研究與現行機制安全性分析比較

表 3 係針對現有雲端系統運作機制與本研究設計之基於橢圓曲線密碼系統並導入多因子身分認證協定機制進行各項安全比較，可發現本機制除符合機密性、存取控制之要求外，亦就可用性及連線資料保密進行改良精進與補足完整性、不可否認性、身分認證及抗同謀攻擊之不足處，故本研究可達到安全性要求；為配合雲端高速運算模型，近年發表雲端服務存取權限機制研究皆是以雙線性曲線對（bilinear pairing）進行加密（Wu

et al., 2017; Deng et al., 2020)，雙線性曲線對起初應用於密碼學是為了將 ECDLP 問題歸約到 DLP 問題而被提出 (Menezes et al., 1993)，因此在相同長度的金鑰下，破譯雙線性曲線對的時間將大幅縮短；為了解決上述問題許多學者提出相應的方案，其中以 Boneh (2001) 等人提出的 BLS 簽章演算法最為著名，該演算法可以有效縮減簽章的位元組大小，但是將簽章複雜度提升，驗證時間相對於傳統的 ECDSA 簽名則因此上升了兩個單位量級；考量現行系統運作機制，在資料儲存空間上非常充足，且為了在一定的安全性上保有較佳的驗證效能，因此本研究設計之機制較為適合。

#### 4.10 執行效能分析

本節以葉昱宗 (2015) 所提之參考表為基準 (如圖 4)，針對本研究所提機制之效益評估整理各階段運算成本概估，且考量本研究屬國軍客製化系統且原系統無相關參照演算法，故無從比較，僅針對本研究設計機制執行各事件之運算成本 (如圖 5)

表 3 本研究與現行系統之安全比較表

| 項次 | 比較項目  | 現行系統運作機制                                           |   | 本研究設計之機制                                                                           |   |
|----|-------|----------------------------------------------------|---|------------------------------------------------------------------------------------|---|
| 1  | 機密性   | 使用者僅輸入 AD 帳號密碼來登入系統，此登入方式無法驗證是否為合法使用者。             | △ | 使用者均須完成註冊與執行身分認證後，並搭配智慧卡多因子認證，才能連線雲端服務平臺要求功能服務 (如圖 3 R15-17 及 C4)。                 | ✓ |
| 2  | 完整性   | 未使用雜湊函數或 RSA 數位簽章等方法，無法確保資訊傳遞間之完整性。                |   | 不法人士若欲偽冒使用者簽章或竄改，則會面對破解單向無碰撞雜湊函數及橢圓曲線離散對數難題，將無法輕易破解 (如圖 3 R19)。                    | ✓ |
| 3  | 可用性   | 目前僅利用防火牆阻擋可疑來源位址及 AD 帳密列表，但對於未紀錄於防火牆的名單，將會面臨重送式攻擊。 | △ | 使用者若未能與雲端服務平臺完成身分驗證，將限制或拒絕該使用者與雲端服務平臺連線，使雲端服務平臺能抵禦重送式攻擊 (如圖 3 S2)。                 | ✓ |
| 4  | 不可否認性 | 目前使用者僅註冊固定憑證，使用者於執行動作之後，將有可能遭遇到事後否認行為。             |   | 運用智慧卡及個人帳密等方式，雙方須使用共同通訊金鑰，資訊傳達可避免曾執行過的關鍵事件或動作遭到否認 (如圖 3 C2、C4 及 S2)。               | ✓ |
| 5  | 存取控制  | 目前運用使用者 AD 帳密列表限制登入，若帳密列表遭盜用將可能面臨各項資料外洩。           | △ | 首先運用時戳來限制服務申請及登入認證，並結合隨機背包密碼系統，給予使用者功能權限，若判斷為非授權時間或身分，將拒絕功能服務使用之申請 (如圖 3 R5 及 C1)。 | ✓ |
| 6  | 身分認證  | 目前僅使用使用者 AD 帳密列表限制登入，沒有第三方安全認證機制。                  | △ | 因應軍種及層級權限特性，為了降低使用者對第三方認證系統之依賴，採用採自我認證機制，以達於受限網路環境下依然能完成相關                         | ✓ |

# 強化國軍雲端服務存取權限機制之設計

|                         |       |                                                                                    |   |                                                                                   |   |
|-------------------------|-------|------------------------------------------------------------------------------------|---|-----------------------------------------------------------------------------------|---|
|                         |       |                                                                                    |   | 認證連線（如圖 3 C1）。                                                                    |   |
| 7                       | 抗同謀攻擊 | 管理方式為採主從管控，若管理人員其管理系統身分帳密遭偽冒或盜用，則使用者將失去安全保障。                                       |   | 本研究運用離線自我認證方式，在雲端服務平臺計算使用者權限密文及使用者使用服務存取功能時，認證伺服器都未參加，故能抵禦同謀攻擊（如圖 3 C1）。          | ✓ |
| 8                       | 資料保密  | 僅使用 AD 帳密列表限制登入，但無多因子認證機制，且使用者間傳輸資料僅仰賴使用者檔案資料加密習慣，若遺忘加密密碼或常使用廣泛加密密碼時，將造成洩密及業務延宕情事。 | △ | 本研究將具有橢圓曲線離散對數及隨機背包雙重難題，藉此保護使用者及雲端服務平臺所計算出權限密文，以保障服務及使用者傳輸資料安全（如圖 3 R4、R5 及階段 I）。 | ✓ |
| 附註：✓代表符合、△代表部分符合、×代表不符合 |       |                                                                                    |   |                                                                                   |   |

| 符號↵                                                 | 定義↵                | 運算成本↵             |
|-----------------------------------------------------|--------------------|-------------------|
| $T_{MUL}$ ↵                                         | 執行一次模式乘法運算所需時間↵    | 參考備註一↵            |
| $T_{ECMUL}$ ↵                                       | 執行一次 ECC 乘法運算所需時間↵ | $29T_{MUL}$ ↵     |
| $T_{ECADD}$ ↵                                       | 執行一次 ECC 加法運算所需時間↵ | $5T_{MUL}$ ↵      |
| $T_{INVS}$ ↵                                        | 執行一次模式乘法反元素運算所需時間↵ | $240T_{MUL}$ ↵    |
| $T_{EXP}$ ↵                                         | 執行一次模式指數運算所需時間↵    | $240T_{MUL}$ ↵    |
| $t_h$ ↵                                             | 執行一次值雜湊函數所需時間↵     | $0.4T_{MUL}$ ↵    |
| $T_h$ ↵                                             | 執行一次點雜湊函數所需時間↵     | $23T_{MUL}$ ↵     |
| $T_{\Sigma mul}$ ↵                                  | 執行一次數值序列乘法運算所需時間↵  | 參考備註二↵            |
| $T_{\Sigma add}$ ↵                                  | 執行一次數值序列加法運算所需時間↵  | 參考備註三↵            |
| $T_{ADD}$ ↵                                         | 執行一次模式加法運算所需時間↵    | 因運算時間<br>短，可忽略不計↵ |
| $T_{\oplus}$ ↵                                      | 執行一次 XOR 運算所需時間↵   |                   |
| $T_{\parallel}$ ↵                                   | 執行一次串接運算所需時間↵      |                   |
| 備註：↵                                                |                    |                   |
| 一、本研究僅以 $T_{MUL}$ 作為運算成本計算基準，詳細視不同機器，規格及執行環境而異。↵    |                    |                   |
| 二、 $T_{\Sigma mul}$ :若該序列長度為 n，則成本為 $nT_{MUL}$ ↵    |                    |                   |
| 三、 $T_{\Sigma add}$ 若該序列長度為 n，則成本為 $(n-1)T_{ADD}$ ↵ |                    |                   |

圖 4 運算成本參考  
(資料來源：葉昱宗，2015)

| 事件 <sup>↵</sup>                                  | 運算式 <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 運算成本概估 <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 初始階段 <sup>↵</sup>                                | $CK = ck \cdot G$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | $1T_{ECMUL}$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Subtotal <sup>↵</sup>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | $29T_{MUL}$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 註冊申請階段 <sup>↵</sup>                              | $ID_{csp} = h(rm_{csp} \parallel id_{csp}) \cdot G$ <sup>↵</sup><br>$MK = ID_{csp} + (rd_{csp} - h(id_{csp})) \cdot G$ <sup>↵</sup><br>$sig_{csp} = rd_{csp} + ck(ms_x + h(id_{csp}))$ <sup>↵</sup><br>$mk = sig_{csp} + h(rm_{csp} \parallel id_{csp})$ <sup>↵</sup><br>$MK' = mk \cdot G = MK$ <sup>↵</sup><br>$SK_{cspMac} = mk \cdot CK = ck \cdot MK$ <sup>↵</sup><br>上述為McsP本階段步驟，SCmgr及m <sub>crd</sub> 註冊步驟同上 <sup>↵</sup><br>$uSC_{crd} = \sum_{i=1}^m \tilde{u} \times \hat{u}_{mar}$ <sup>↵</sup><br>$vSC_{crd} = \sum_{i=1}^n \tilde{v} \times \hat{v}_{mor}$ <sup>↵</sup><br>$sn_{crd} = uSC_{crd} \oplus m_{crd}$ <sup>↵</sup><br>$ad_{crd} = vSC_{crd} \oplus m_{crd}$ <sup>↵</sup><br>$AC1_{mar} = (uSC_{crd}, sn_{crd} + ad_{crd}) + SK_{cspMac}$ <sup>↵</sup><br>$AC1_{mar} - SK_{cspMac} = (uSC_{crd}, sn_{crd} + ad_{crd})$ <sup>↵</sup><br>$AU_{usr} = (x_1, x_2) = ((uSC_{crd}, sn_{crd} + ad_{crd}) + Ekey_{csp})$ <sup>↵</sup><br>$AC2_{usr1} = rd_{mor} \cdot G$ <sup>↵</sup><br>$AT_{usr} = rd_{mor} \cdot SK = (y_1, y_2)$ <sup>↵</sup><br>$AC2_{usr2} = AU_{usr} \cdot AT_{usr} = (x_1 \cdot y_1, x_2 \cdot y_2) = (z_1, z_2)$ <sup>↵</sup> | $T_{ECMUL} + 1t_h + T_1$ <sup>↵</sup><br>$T_{ECMUL} + T_{ECADD} + t_h$ <sup>↵</sup><br>$T_{ECMUL} + T_{ADD} + t_h + T_{MUL}$ <sup>↵</sup><br>$T_{ADD} + t_h + T_1$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup><br>$2T_{ECMUL}$ <sup>↵</sup><br>上述成本乘以 3 <sup>↵</sup><br>$nT_{mul} + (m-1)T_{ADD}$ <sup>↵</sup><br>$mT_{mul} + (n-1)T_{ADD}$ <sup>↵</sup><br>$T_{\oplus}$ <sup>↵</sup><br>$T_{\oplus}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup>                          |
| Subtotal <sup>↵</sup>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | $(639.3+m+n)T_{MUL} + (m-1)T_{ADD} + (n-1)T_{ADD}$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 驗證取得階段 <sup>↵</sup>                              | $dk' = DK + h(m_{crd}) \cdot G + (cr_x + h(m_{crd})) \cdot CK$ <sup>↵</sup><br>$mk' = MK + h(id_{csp}) \cdot G + (ms_x + h(id_{csp})) \cdot CK$ <sup>↵</sup><br>$RC_{crd} = rc_{crd} \cdot G$ <sup>↵</sup><br>$SK_{cspcrd} = mk \cdot DK = dk \cdot MK$ <sup>↵</sup><br>$DHRC_{crd} = RC_{crd} + SK_{cspcrd}$ <sup>↵</sup><br>$RC_{csp} = rc_{csp} \cdot G$ <sup>↵</sup><br>$SK_{cspcrd} = dk \cdot MK = mk \cdot DK$ <sup>↵</sup><br>$DHRC_{csp} = RC_{csp} + SK_{cspcrd}$ <sup>↵</sup><br>$RC_{crd} = DHRC_{crd} - SK_{cspcrd}$ <sup>↵</sup><br>$DH_{us} = rc_{csp} \cdot RC_{crd}$ <sup>↵</sup><br>$CK_{us} = DH_{us} + SK_{cspcrd}$ <sup>↵</sup><br>$Ver(McspA) = H(m_{crd} \parallel id_{csp} \parallel DH_{us})$ <sup>↵</sup><br>$Ver(McspB) = H(m_{crd} \parallel id_{csp} \parallel CK_{us})$ <sup>↵</sup><br>$RC_{csp} = DHRC_{csp} - SK_{cspcrd}$ <sup>↵</sup><br>$DH_{us'} = rc_{crd} \cdot RC_{csp}$ <sup>↵</sup><br>$CK_{us'} = DH_{us'} + SK_{cspcrd}$ <sup>↵</sup><br>$Ver(m_{crd1}) = Ver(McspA)$ <sup>↵</sup><br>$Ver(m_{crd2}) = H(m_{crd} \parallel id_{csp} \parallel CK_{us'})$ <sup>↵</sup><br>$\bar{A} = AC2_{usr} + CK_{us}$ <sup>↵</sup>       | $2T_{ECMUL} + 2T_{ECADD} + t_h + T_{ADD}$ <sup>↵</sup><br>$2T_{ECMUL} + 2T_{ECADD} + t_h + T_{ADD}$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup><br>$2T_{ECMUL}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup><br>$2T_{ECMUL}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_h + 3T_1$ <sup>↵</sup><br>$T_h + 3T_1$ <sup>↵</sup><br>$T_{ADD}$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_h + 3T_1$ <sup>↵</sup><br>$T_h + 3T_1$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup> |
| Subtotal <sup>↵</sup>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | $445.6T_{MUL}$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 服務使用階段 <sup>↵</sup>                              | $AC2_{usr} = \bar{A} - CK_{us}$ <sup>↵</sup><br>$R = (r_1, r_2) = mk \cdot AC2_{usr1}$ <sup>↵</sup><br>$AU_{usr} = (AC2_{usr2} \cdot R^{-1}) = (x_1, x_2)$ <sup>↵</sup><br>$(uSC_{crd}, sn_{crd} + ad_{crd}) = AU_{usr} - Ekey_{csp}$ <sup>↵</sup><br>$vSC_{crd} = ad_{crd} \oplus m_{crd} = (vSC_{crd} \oplus m_{crd}) \oplus m_{crd}$ <sup>↵</sup><br>$(\hat{u}_{mar})_2 = (uSC_{crd} \bmod j_m) - (uSC_{crd} \bmod k_m)$ <sup>↵</sup><br>$(\hat{v}_{mar})_2 = (vSC_{crd} \bmod j_n) - (vSC_{crd} \bmod k_n)$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | $T_{ECADD}$ <sup>↵</sup><br>$T_{ECMUL}$ <sup>↵</sup><br>$T_{INVS}$ <sup>↵</sup><br>$T_{ECADD}$ <sup>↵</sup><br>$T_{\oplus}$ <sup>↵</sup><br>$T_{ADD}$ <sup>↵</sup><br>$T_{ADD}$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Subtotal <sup>↵</sup>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | $279T_{MUL}$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Total <sup>↵</sup>                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | $(1392.9+m+n)T_{MUL} + (m-1)T_{ADD} + (n-1)T_{ADD}$ <sup>↵</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 備註：本研究屬客製化系統設計，考量原系統無相關參照演算法，故無從比較。 <sup>↵</sup> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

圖 5 運算成本

### 五、結論

本研究機制利用橢圓曲線加密金鑰長度短與隨機背包密碼系統運算效能快的優點，且適用於國軍雲端服務之身分認證暨金鑰交換機制。在系統運作機制方面，現有國軍系統雖有雲端整合的案例，但僅有在資料儲存時避免了單一資料庫儲存，且在使用權限上較難整合，因此在擴展性上有諸多限制；而本研究透過存取控制之設計，可使各部會系統更容易導入，並且讓使用者不必保管過多的金鑰儲存工具，或是需要記住不同系統的帳號密碼；另在安全性方面，本研究設計在小幅度增加加、解密長度及處理時間的前提下，配合多因子認證，使國軍在跨軍種資料交換及使用各項雲端服務時，具備更高的安全性，能防止用戶端偽冒、不法人士攻擊及抵禦竊聽，並且藉由求解隨機背包密碼系統之難題，將雲端服務平臺功能及使用者權限均透過序列方式隱藏，大幅增加惡意人士獲取權限開通內容之難度，最後採離線自我認證之方式，可讓使用者在取得對應之權限智慧卡後，在無須依賴第三方認證中心情況下與雲端服務平臺完成相互認證，有效縮短作業時間，且可保持服務提供大幅增加可用性。

### 六、國防領域之應用

本研究針對軍種資料交換及國軍雲端服務架構提出透過多因子執行強化自我認證與存取控制，並運用橢圓曲線密碼系統與隨機背包機加密系統可提升安全性與效率。國軍發揮戰力有賴於各軍種間所偵獲敵情之共享，本研究提供建立適當資訊安全防護的參考，除確保我軍資訊傳輸系統具備高安全及高效能，未來亦可針對跨部門資訊系統進行客製化設計與評估運用，達到支援網狀化作戰效益，並藉由建置雲端服務來改善資源佈署、資安防護及任務遂行等，以利在人力精簡狀況下，不影響任務遂行，以建構多層次資安防護安全機制，且符合相關法規安全述求下更有效發揮國防事務之堅強戰力。

## 參考文獻

- 王子承 (2017)，俄國首次承認組建「網軍」歐洲多國擔心大選遭干預，*上報*。取自 [https://www.upmedia.mg/news\\_info.php?SerialNo=12674](https://www.upmedia.mg/news_info.php?SerialNo=12674)。
- 王青龍、趙祥模 (2015)，隨機背包公鑰密碼的分析與改進，*計算機科學*，42 (6)，158-161。
- 中共國防部 (2019)，《新時代的中國國防》白皮書。取自 <http://www.scio.gov.cn/ztk/dtzt/39912/41132/41134/Document/1660318/1660318.htm>。
- 中共新聞網 (2018)，習近平談網絡安全：沒有網絡安全就沒有國家安全，取自 <http://cpc.people.com.cn/xuexi/BIG5/n1/2018/0817/c385476-30234135.html>。
- 張鈞富 (2014)，*具自我認證之安全並存簽章方法*，國防大學資訊管理學系研究所碩士論文。
- 黃建衛 (2011)，網際網路服務使用者身分驗證機制之安全性研析，財金資訊股份有限公司網站。取自 <https://www.fisc.com.tw/tc/knowledge/quarterly1.aspx?PKEY=0abc938c-0f9b-4ed3-a131-8c9ff86e946b>。
- 劉嘉偉、張家瑛 (2021)，面對中共網軍威脅國軍資訊網路安全之探討，*海軍學術雙月刊*，55 (3)，118-131。
- 鄧安文 (2018)，*密碼學—密碼分析與實驗 (第三版)*，全華圖書股份有限公司。
- Abdulla, N., & Erçelebi, E. (2017). Identify cloud security weakness related to authentication and identity management (IAM) using openstack keystone model. In *International Conference on Engineering and Technology, Computer, Basics and Applied Sciences* (pp. 1-5).
- A. Menezes, T. Okamoto, and S. A. Vanstone, (1993) Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 1,639-1,646.
- Boneh, D., Lynn, B., & Shacham, H. (2001, December). Short signatures from the Weil pairing. In *International conference on the theory and application of cryptology and information security* (pp. 514-532). Springer, Berlin, Heidelberg.
- Brickell, E.F., (1984), August. Breaking iterated knapsacks. In *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 342-358.
- Brummett, T., Sheinidashtegol, P., Sarkar, D., & Galloway, M. (2015, November). Performance metrics of local cloud computing architectures. In *2015 IEEE 2nd international conference on cyber security and cloud computing* (pp. 25-30). IEEE.
- Cloud Security Alliance - CSA, Top Threats Working Group (2013)., The Notorious Nine - Cloud Computing Top Threats in 2013. <http://www.cloudsecurityalliance.org/topthreats>.
- Cloud Security Alliance - CSA, Top Threats Working Group (2011)., "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0," Cloud Computing Alliance, <http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>.
- Deng, H., Qin, Z., Wu, Q., Guan, Z., Deng, R. H., Wang, Y., & Zhou, Y. (2020). Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. *IEEE Transactions on Information Forensics and Security*, 15, 3,168-3,180.
- Eucalyptus Systems. (2012). Inc.: Eucalyptus Identity and Access Management (IAM)2012. Retrieved from [https://www.eucalyptus.com/docs/eucalyptus/4.0/security-guide/security\\_bp\\_access.html](https://www.eucalyptus.com/docs/eucalyptus/4.0/security-guide/security_bp_access.html).
- Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. *Complex Adaptive Systems Modeling*, 2(1), 1-37.
- Hewlett Packard Enterprise Development. (2017). HPE Helion Eucalyptus, Remote Unauthorized Access, Unauthorized Modification, Unauthorized Disclosure of Information.

- Retrieved from [https://support.hpe.com/hpesc/public/docDisplay?docId=emr\\_na-c05363782](https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c05363782).
- Koblitz, N., (1987), Elliptic Curve Cryptosystems, *Mathematics of Computation American Mathematical Society* (48) , 203-209.
- Kumar, R., Gupta, N., Charu, S., Jain, K., & Jangir, S. K. (2014). Open source solution for cloud computing platform using OpenStack. *International Journal of Computer Science and Mobile Computing*, 3(5), 89-98.
- Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, 24(11), 770-772.
- Materese, R., (2016). Recommendation for Key Management, Part 1: General.
- Mell, P., & Grance, T. (2011), The NIST definition of cloud computing, National Institute of Standards and Technology Spec. Publ.
- Michael, R., and David, S., (1979), Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman & Co., Freeman, New York.
- Miller, V. S., (1985), Use of Elliptic Curve in Cryptography, *Advance in Cryptography-Crypto*, New York: Spring-Verlag , 417-426.
- Odlyzko, A.M., (1990). The rise and fall of knapsack cryptosystems. *Cryptology and computational number theory*, 42, 75-88.
- Ren, Y., Ding, N., Wang, T., Lu, H., & Gu, D. (2016). New algorithms for verifiable outsourcing of bilinear pairings. *Science China Information Sciences*, 59(9), 99103.
- Uzunkol, O., Kalkar, Ö., & Sertkaya, I. (2017). Fully Verifiable Secure Delegation of Pairing Computation: Cryptanalysis and An Efficient Construction. *IACR Cryptol. ePrint Arch.*, 2017, 1173.
- Wu, L., Zhang, Y., Choo, K. K. R., & He, D. (2017). Efficient and secure identity-based encryption scheme with equality test in cloud computing. *Future Generation Computer Systems*, 73, 22-31.

## 植基於最低位元取代與像素差值之資訊隱藏技術

劉興漢\* 賀盛志 羅玉芬

國防大學資訊管理學系

論文編號：NM-42-02-02

來稿2021年3月7日→第一次修訂2021年9月15日→第二次修訂2022年4月1日→  
同意刊登2022年5月17日

### 摘要

本研究提出空間域的最低位元取代法與像素差值之資訊隱藏技術，利用人體視覺系統觀察能力有限的情況下於灰階影像中隱藏秘密訊息。本研究是以 Jung 學者於 2018 年所提出混合 LSB/PVD 藏密法為基礎而改良的資訊隱藏方法，其方法是將掩護影像切割成  $1 \times 3$  個像素區塊進行運算，選定區塊中間像素為基底像素。其次，基底像素採用採用 LSB 及 OPAP 藏密法嵌入 4 位元的秘密訊息，其餘像素與藏密後的基底像素作差值計算，採用改良混合 LSB/PVD 法進行藏密，以 LSB 藏密法為基礎將像素區分高位元組及低位元組，在低位元採用 2-bit LSB 藏密法及高位元中 6 位元採用新式 PVD 藏密法。二種藏密法結合以提高影像嵌入容量，並保持低失真的影像品質。

實驗以 Lena 等 8 張灰階影像進行測試，實驗結果本研究的平均藏密量為 1,075,071 位元，與混合 LSB/PVD 藏密法相較，藏密量可提升約略 2.3%（約 24,219 位元），本研究因具有較高的藏密量，當嵌入率達 4.1 bpp，影像品質可維持約 30.82 dB，證明本研究藏密法可有效提升藏密量，同時能維持人眼難以察覺的範圍內。

**關鍵字：**資訊隱藏、最低位元取代法、像素差值藏密法。

---

\*通訊作者：劉興漢 email: liu.hansh@gmail.com

# An Improved Steganographic Method Based on Least-Significant-Bit Substitution and Pixel-Value Difference

Liu, Hsing-Han\* Ho, Sheng-Chih Lo, Yu-Fen

Department of Information Management, National Defense University, Taiwan, R.O.C

## Abstract

This research proposes the least-significant-bit (LSB) substitution combined with the pixel-value differencing (PVD) steganography in the spatial domain, which hides secret information in grayscale images when the observation ability of the human visual system is limited. This research is an improved information hiding method based on the hybrid LSB/PVD method proposed by Jung et al. in 2018, which divides the original cover image into three consecutive non-overlapping blocks and selects the second pixel in each block as a base pixel. Next, the 4-bits secret data are embedded into the base pixels through LSB substitution and the Optimal Pixel Adjustment Process (OPAP). The difference values between the base pixels and their left and right counterparts will then indicate the quantity of information that can be embedded. The improved hybrid LSB/PVD method is used to embed the secret data, and the pixels are divided into high-byte and low-byte groups based on the LSB method. The 2 bits LSB method is used in the low-byte area and the new PVD method is used in the 6 bits in the high-byte area. The least-significant-bit (LSB) substitution combined with the new pixel-value differencing (PVD) steganography increases the image embedding capacity and maintains a low-distortion image quality.

The experiments are tested with 8 grayscale images such as Lena. The experimental results show that the average embedded capacity is 1,075,071 bits. Compared with the original hybrid LSB/PVD method, it can be increased by about 2.3% (about 24,219 bits). When the embedded capacity is up to 4.1 bpp, the image quality can be maintained at about 30.82 dB. The experimental results show that the proposed method not only increases the embedded capacity, but also maintains the acceptable of the human eye image quality.

**Keywords:** Steganography, Least-Significant-Bit Substitution, Pixel-Value Differencing.

---

\* Corresponding Author Email: liu.hansh@gmail.com

## 一、緒論

### 1.1 前言

隨著電腦及網際網路迅速發展，人們利用資訊傳遞管道與方式亦有極大的轉變，因為只要透過一隻智慧型手機，就能連結上網路可以挖掘到數不清的資料，閱覽來自四面八方的各種資訊，涵蓋新聞、股市、理財、購物、旅遊等各方面的資訊，正所謂「大千世界，盡收眼底」。由於科技的進步，使用者能以最短的時間與成本達到互相通訊，只要透過手機幾個按鈕，即可完成曠日廢時才能完成的傳送郵件工作，為日常生活帶來許多便利，當網際網路成為資訊大量流通時，資安問題也隨之而來，讓大家不得不重視這議題。秘密通訊發展為迎合人性及人類生活的需求孕育而生，密碼系統運作方式是將機密文件經由加密運算處理成密文後，成為無法辨識的亂碼，經加密的資料在網路傳輸中即使遭到攔截亦無法解密，進而達到資訊保密的目的。而藏密學是一種在非機密文件中隱藏秘密資訊以避免被發現的技術，其目的是讓有心人士難以察覺。

密碼學（Cryptography），即希臘語「藏匿」之意，密碼系統運作方式是將機密文件經由加密程序處理後，轉譯成為無法辨識的文字或符號，在網路傳送過程中容易引起中間者的好奇，訊息容易受偵測或監視，使資訊傳輸的安全性備受考驗。我國早在中國周朝的兵書六韜中，便已運用密碼作為軍事通訊的方法與策略，例如陰書與陰符。古羅馬時期，凱薩也將密碼運用於軍事通訊中。第二次世界大戰期間，英格瑪密碼機的破解，成為最後聯軍勝利的關鍵。藏密學（Steganography）一詞源自希臘語「隱藏」、「書寫」之意，為雙方建立一個秘密通訊的掩護下傳遞秘密訊息，其目的是避開第三方的懷疑將秘密訊息傳遞出去。早期傳遞訊息的媒介如岩石、竹片、銅片等做掩護，十六世紀義大利科學家喬凡尼·波塔，利用煮熟的蛋傳遞訊息，其原理使用明礬和醋酸混合而成的液體作為墨汁，將秘密訊息寫在蛋殼上，此液體會穿透蛋殼，在蛋白表層留下秘密訊息，利用化學變化的效果來達到隱藏目的。由上述案例發現，資訊隱藏的概念從以前就開始建立，藏密學與密碼學存在的目的皆在保護秘密資訊，於1999年Petitcolas等學者對資訊隱藏技術分類，見圖1所示。

現今的資訊隱藏技術，主要由傳輸方利用數位多媒體掩護藏匿秘密訊息，透過微幅修改多媒體的原始內容，將有意義資訊嵌入無意義的數位多媒體內容資訊中。本研究主要利用一張數位影像作為掩護影像（Cover Image）來藏匿資訊，藉由傳送者使用藏密程序把影像像素改變，將秘密訊息藏入影像，已藏訊息的載體稱偽裝影像（Stego Image）使人類視覺系統（Human Vision System, HVS）觀察的細緻程度有限，不易察覺數位影像中像素值細微變化，讓偽裝影像能發送出去給接收者，而接收者必須知道對方所使用藏密方法才能將訊息提取出。

基本的資訊隱藏流程是發送方先將秘密資料嵌入載體影像後成為藏密影像，然後透過網路方式將藏密影像傳遞給接收方，接收方在接收後再從藏密影像中把秘密資料抽取出來，如圖2所示。

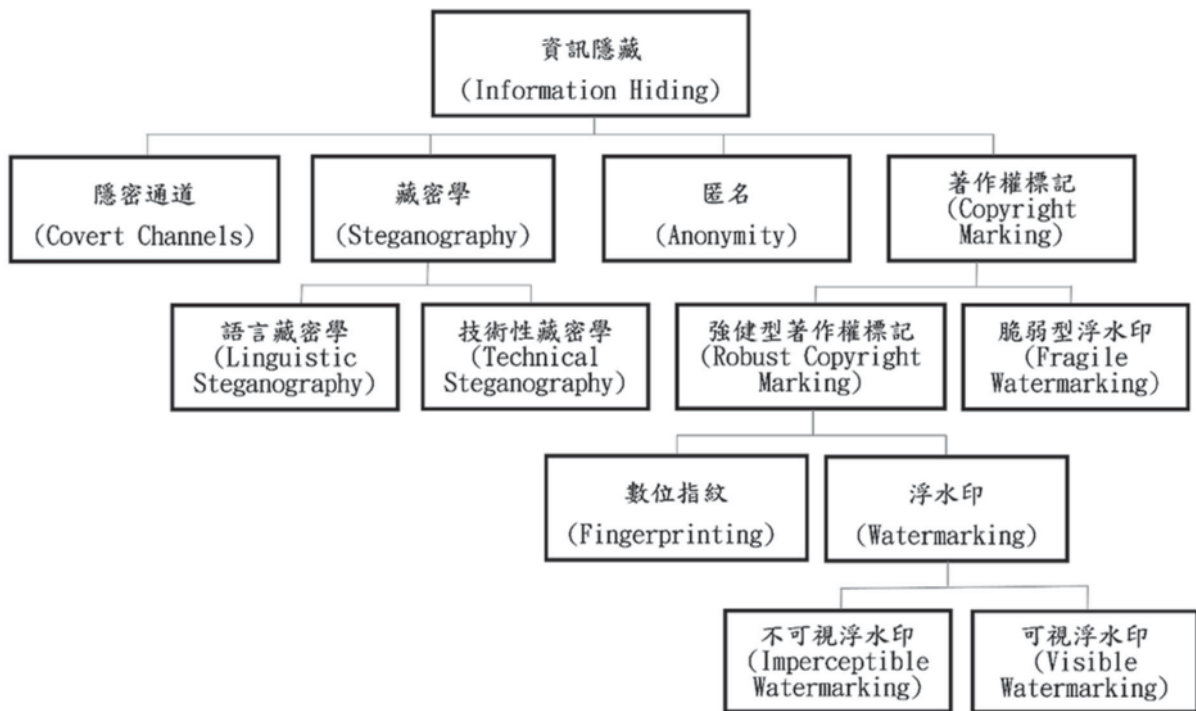


圖 1 資訊隱藏技術分類圖

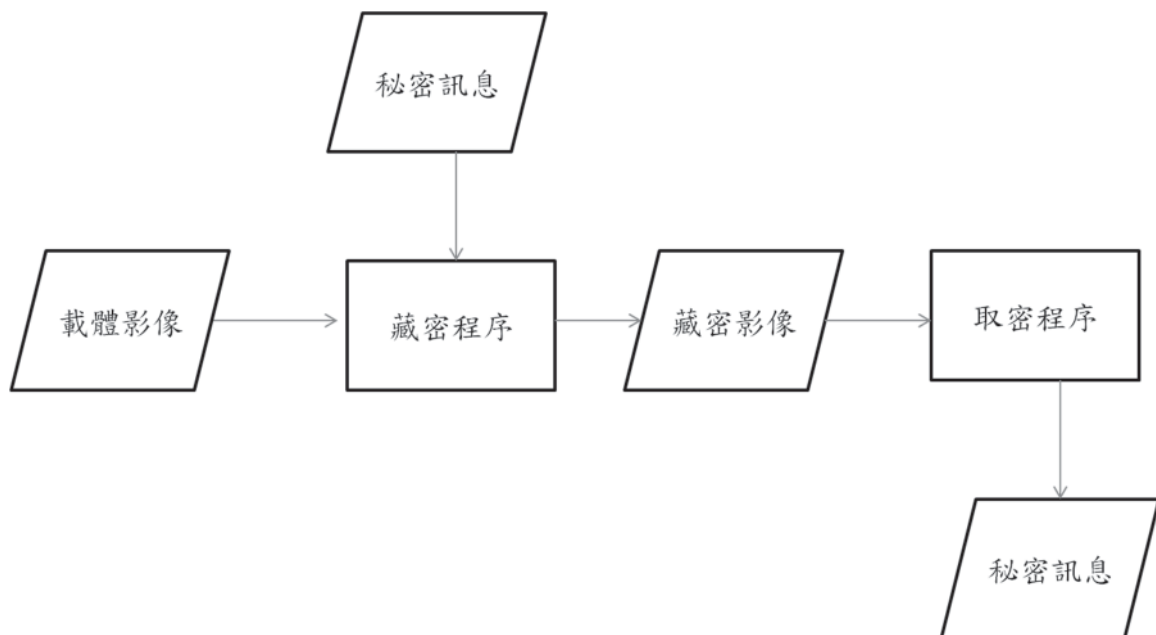


圖 2 資訊隱藏基本流程

目前資訊隱藏技術可區分二種方向，分別為空間域 (Spatial Domain) 及頻率域 (Frequency Domain) 技術 (Johnson & Jajodia, 1998)。應用在空間域者，主要藉由直接改變影像像素值達到隱藏目的，通常以不破壞原始影像的視覺效果下達成高容量的資訊隱藏，是最常見的隱藏方式，基礎空間域資訊隱藏技術包括最低有效位元取代法 (Least-Significant-Bit, LSB)、像素差值藏密法 (Pixel-Value Differencing, PVD)。而頻率域的技术則是先將影像由空間域的像素值轉換成頻率域的係數值，再藉由改變頻率域

的係數值嵌入秘密訊息。其中空間域最常用的方法最低位元取代法 (LSB)，最初由 Bender 等 4 位學者於 1996 年提出使用影像像素最低位元進行訊息藏密，其利用人類視覺對影像輕微調整不易察覺的特性達到隱藏目的，當使用過多的位元數來隱藏機密訊息時，將使偽裝後影像品質降低，甚至會讓偽裝影像造成嚴重的失真，缺點在於藏密量大受到限制。因此後來學者相繼以 LSB 技術為基礎做改良，提出有效率又不會使影像失真的方法，而 Chan and Cheng 兩位學者於 2004 年提出像素值調整最佳化方法 (Optimal Pixel Adjustment Process, OPAP)，此方法是以 LSB 藏密法為基礎，在嵌密完後藉由調整其他位元，來比較是否與原影像像素值差距更小，以提升偽裝影像的品質。為了有效增加藏密量，Wu and Tsai 學者於 2003 年提出像素差值藏密法 (Pixel Value Differencing, PVD)，計算兩像素間的差值，依預先設定固定區間決定嵌入秘密訊息長度，所以藏密量較低，將使偽裝影像產生特定特徵，易遭統計分析的攻擊。後續 Wu 等學者於 2005 年提出基於 PVD 藏密法與 LSB 替代藏密法提出一種高容量藏量法，透由像素差值門檻值設定，分別採用 LSB 與 PVD 的藏密法。Wang 等學者於 2008 年提出植基於模運算之像素差值藏密法 (Modulus PVD, MPVD)，利用模數運算修改相鄰像素的餘數來隱藏訊息，並選擇最少失真度的像素值，以降低藏密影像失真，後續由劉江龍等三位學者於 2012 年提出改良 MPVD 藏密法，改善秘密訊息提取不正確問題。Khodaei and Faez 兩位學者於 2012 年提出新式 LSB 和 PVD 藏密法，將掩護影像切割成 3 個連續且不重疊的區塊，針對區塊中間像素嵌入時採用最低位元取代藏密法，最後區塊兩側像素與中間像素分別計算差值，運用改良 PVD 藏密法嵌入秘密訊息。Liu 等學者於 2018 年提出結合邊緣吻合 (Side match) 和像素差值藏密技術，將掩護影像切割成 3×3 個連續且不重疊的區塊，使用中間像素作為基底，對基底像素的上、左、右、下的像素採用原始 PVD 藏密法，區塊剩餘的四個像素使用 Side match 藏密方法，產生八對像素差值來達到最大藏量，藏密後的影像品質雖然比原始 PVD 方法低，仍在容許影像品質範圍之上。Jung 學者於 2018 年提出混合最低位元取代藏密法和像素差值藏密技術二種藏密法結合以提高影像嵌入容量，並保持低失真視覺影像質量，其缺點藏密後像素值容易產生溢位及藏密前後像素差值在不同區間範圍問題。本研究所提出的方法是結合上述方法優點，改良混合最低位元取代藏密法和像素差值藏密技術及調整像素差值區間表範圍，以提升藏密量情況下，並維持人類視覺可接受的偽裝影像品質。

因應資訊全球化的來臨，國家安全威脅已不再侷限於實體，全球駭客持續入侵網路系統，竊取個資、智慧財產及各類機密資訊，對人權、經濟甚至國家安全都會造成莫大威脅，故資訊隱藏技術的發展仍有其必要。

## 1.2 研究目的

本研究提出結合空間域資訊隱藏技術中最低位元取代法 (LSB) 及像素差值 (PVD) 藏密法，以 Jung 學者於 2018 年提出混合最低位元取代和像素差值藏密法為基礎，改良其藏密後會產生溢位狀況，導致無法正確提取秘密訊息問題。研究過程中運用 Python 程式語言進程式撰寫，以驗證本研究提出的藏密及取密程序之正確性。本論文主要目的在能維持人類視覺可接受的影像品質下提高藏密量，以提升資訊傳送的利用率。

## 二、文獻探討

### 2.1 混合最低位元取代法和像素差值藏密法

Jung 學者於 2018 年提出混合最低位元取代藏密法和像素差值藏密技術，以往都是兩種藏密法單獨或組合使用，而這個藏密方法是以 LSB 藏密法為基礎將像素區分高位元組及低位元組，低位元組採用 2-bit LSB 藏密法和在高位元組中 6 個位元採用 PVD 藏密法，二種藏密法結合以提高圖像嵌入容量，並保持低失真視覺圖像質量。本文後續稱此藏密法為混合 LSB/PVD 藏密法，藏密流程如下：

步驟 1：將掩護影像切割  $1 \times 2$  個連續不重疊的區塊。

步驟 2：計算像素值商數（高位元）及餘數（低位元），設定低位元最低有效位元取代法之置換量為 2 位元（ $k = 2$ ），公式（1）之  $(P_i^m, P_{i+1}^m)$  與  $(p_i^l, p_{i+1}^l)$  分別代表像素值二進位之高位元與低位元的部分。

$$\begin{aligned} (P_i^m, P_{i+1}^m) &= (p_i \text{ div } 2^k, p_{i+1} \text{ div } 2^k) \\ (p_i^l, p_{i+1}^l) &= (p_i \text{ mod } 2^k, p_{i+1} \text{ mod } 2^k) \end{aligned} \quad (1)$$

步驟 3：計算兩像素商值之差值  $d_i^m$ 。

$$d_i^m = |P_{i+1}^m - P_i^m| \quad (2)$$

步驟 4：設定藏密區間範圍表，如表 1 所示。

表 1 混合 LSB/PVD 藏密法差值區間範圍表

| Range ( $R_i$ ) | $R_1$ | $R_2$  | $R_3$   | $R_4$   |
|-----------------|-------|--------|---------|---------|
| 範圍 $[l_i, u_i]$ | [0,7] | [8,15] | [16,31] | [32,63] |
| 可藏位元數 ( $n$ )   | 3     | 3      | 4       | 5       |

步驟 5：對照藏密區間範圍表，得知可藏密位元數  $n$ ，從二進位秘密訊息取  $n$  位元，並轉換十進位為  $b_i^m$ ，計算新差值  $d_i'^m$ 。

$$d_i'^m = l_i + b_i^m \quad (3)$$

步驟 6：利用公式（4）計算新舊差值，及下列公式（5）計算嵌密後的像素值  $(p_i'^m, p_{i+1}'^m)$ 。

$$m = |d_i'^m - d_i^m| \quad (4)$$

$$(P_i'^m, P_{i+1}'^m) = \begin{cases} \left( P_i^m - \left\lfloor \frac{m}{2} \right\rfloor, P_{i+1}^m + \left\lfloor \frac{m}{2} \right\rfloor \right), & \text{if } d_i^m \text{ is odd} \\ \left( P_i^m - \left\lfloor \frac{m}{2} \right\rfloor, P_{i+1}^m + \left\lfloor \frac{m}{2} \right\rfloor \right), & \text{if } d_i^m \text{ is even} \end{cases} \quad (5)$$

步驟 7：區塊像素值各嵌入  $k$  位元 LSB，從二進位秘密訊息取  $k$  位元，並轉換成十進位  $b_i^{l1}$  及  $b_i^{l2}$ ，最後計算偽裝像素值  $(P_i', P_{i+1}')$ 。

$$(P_i', P_{i+1}') = \left( (p_i'^m \times 2^k) + \sum_{i=0}^{n-1} b_i^{l1}, (p_{i+1}'^m \times 2^k) + \sum_{i=n}^{2n-1} b_i^{l2} \right) \quad (6)$$

Jung 學者所提方法密文取出程序說明如下：

步驟 1：將偽裝影像切割成兩個連續相鄰且不重疊的區塊，偽裝像素( $P'_i, P'_{i+1}$ )分別提取  $k$  位元，並計算新的像素值( $p_i^m, p_{i+1}^m$ )。

$$(p_i^m, p_{i+1}^m) = \begin{cases} (P'_i - (P'_i \bmod 2^k)) \div 2^k \\ (P'_{i+1} - (P'_{i+1} \bmod 2^k)) \div 2^k \end{cases} \quad (7)$$

步驟 2：計算相鄰兩像素差值，並對照表 3 藏密差值區間範圍表，得知可藏密區間  $R_i$  及區間範圍最小值  $l_i$ 、藏密位元數  $n$ ，計算秘密訊息  $b_i^m$ ，將十進位  $b_i^m$  轉換二進位提取密文。

$$\begin{aligned} d_i^m &= |p_{i+1}^m - p_i^m| \\ b_i^m &= |d_i^m - l_k| \end{aligned} \quad (8)$$

Jung 學者所提方法藏密時會產生溢位問題的範例說明如圖 3 所示，將掩護影像切割成  $1 \times 2$  個連續且不重疊像素之區塊，假設原始像素區塊的像素值為  $(0, 255)$ ，欲藏入秘密訊息為  $(11110 \ 00 \ 11)_2$ 。首先，將 0 與 255 分別轉換成二進位後，分別取出高位元（2 進位之前 6 個位元）與低位元（2 進位之後 2 個位元）。將高位元轉換成十進位後，分別得到 0 與 63，依公式 (2) 計算其差值  $d_i^m$  為 63，對照步驟 5 之藏密區間範圍表，計算出可藏入之密文數量為 5，故將前 5 個密文 11110 轉成 10 進位後的值  $b_i^m$  為 30。並依公式 (3) 計算其新差值為 62，續依公式 (4) 計算出  $m$  值為 1。再依公式 (5) 計算出 PVD 藏密後高位元像素值為  $(-1, 63)$ 。最後分別將高位元像素與低位元像素相結合後，可得藏密後的像素值  $(-4, 255)$ ，此時 -4 已小於灰階影像最低像素值 0，故產生溢位問題。

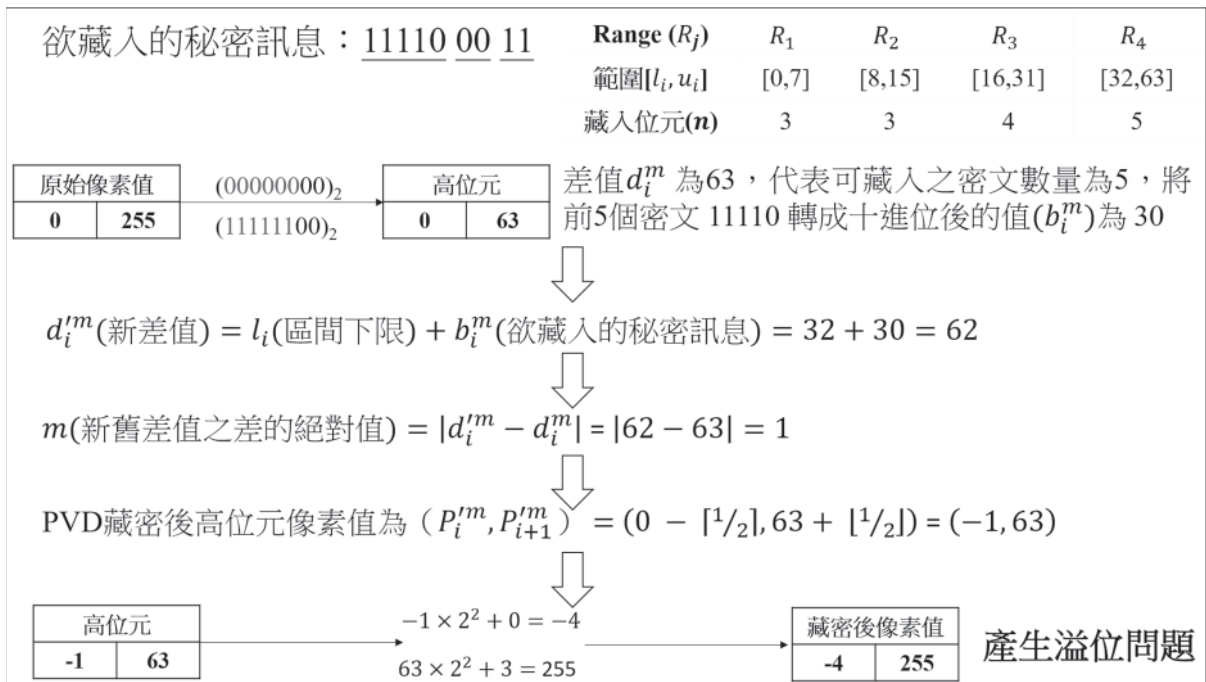


圖 3 Jung 學者所提方法藏密時會產生溢位問題的範例說明

## 2.2 藏密技術衡量標準

在藏密過程中，影像品質與藏密量通常是一個難以取捨問題，當藏密量愈高時，其藏密後影像品質失真就愈大，而藏密影像技術中失真性評估最常利用峰值信號雜訊比（Peak Signal-to-Noise Ratio, PSNR）來做衡量，其單位為分貝（Decibels, dB），如公式（9）所定義，為 Zhou 和 Bovik 學者於 2002 年提出的一個計算影像的失真量化數據的方法。在計算 PSNR 前，必需先計算出掩護影像與偽裝影像像素間的均方差（Mean Square Error, MSE），計算平均每個像素變動的幅度，公式中均方差值分子計算影像藏密前後的誤差程度，均方差值愈大表示誤差程度大，愈小表示誤差程度小。

$$MSE = \sum_{i=1}^{W \times H} \frac{(x'_{ij} - x_{ij})^2}{W \times H}$$

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE}\right) \quad (9)$$

一般灰階影像像素值以 8 位元表示，其值介於 0 到 255 之間，在 MSE 公式中， $W$ 、 $H$  表示掩護影像長與寬，而  $x'_{ij}$ 、 $x_{ij}$  分別代表於  $i$ 、 $j$  位置的偽裝像素與原始像素的值，當 PSNR 值越大，就代表掩護影像跟偽裝影像的差異度越小，一般而言，PSNR 值小於 30 dB 時，表示人類視覺看起來不能容忍的範圍，因此大部份 PSNR 值皆要大於 30 dB（王旭正等，2016）。

由於 PSNR 未考慮到人眼視覺的特性，而人眼對空間頻率較低的敏感度較高、對亮度比對色度差異更敏感、對一個區域的感知會受其周圍鄰近區域所影響等因素，因此常出現 PSNR 評價結果與人的主觀感受不同的情況。因此，另一種符合人類直覺的影像品質評量標準，稱結構相似性（Structural Similarity, SSIM），由 Zhou Wang 等人在 2004 年發表的論文中提出，主要測量掩護影像和偽裝影像之間結構相似大小，其值藉於 0 到 1 之間，值愈大表示兩張影像的相似度越高，分別從公式（10）計算影像亮度、公式（11）計算對比度、公式（12）計算影像相似性，而結構相似性（SSIM）計算如公式（13）所示。

$$l(x, y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (10)$$

$$c(x, y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (11)$$

$$s(x, y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \quad (12)$$

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (13)$$

### 三、研究方法

本研究將探討在偽裝影像品質可接受的情況下，儘可能提高秘密訊息的藏密量。在文獻收集的過程中，發現混合 LSB/PVD 藏密技術有改進的空間，本研究以混合 LSB/PVD 藏密法為基礎而提出改良的資訊隱藏方法。本節首先探討研究設計架構，其次為藏密與取密程序介紹，並針對藏密方法實施範例說明。

#### 3.1 研究設計

在 2018 年 Jung 學者所提出的混合 LSB/PVD 藏密技術中，以 LSB 藏密法的概念，將像素值區分為高位元及低位元，在高位元組以相鄰像素間的差值來決定藏密量，而低位元組利用人類視覺對低像素修改不易察覺的特性來隱藏訊息，而得到較高的藏密量，但此藏密演算法在藏密後容易造成像素值溢位問題，導致在提取秘密訊息時，無法正確完整復原秘密訊息。

本研究設計將掩護影像切割成  $1 \times 3$  個連續且不重疊的區塊，採用 LSB 及 OPAP 藏密法對中間像素嵌入 4 位元的秘密訊息，中間像素藏密後就不再變動，分別計算藏密後中間像素與區塊兩側相鄰像素的差值，本研究將採用混合 LSB/PVD 藏密法，針對其演算法進行改良，其技術是以 LSB 藏密法為基礎，將像素值區分高位元組及低位元組，有別於該技術高位元組 6 個位元結合原始 PVD 藏密法，本研究高位元像素組改採用改良新式 PVD 藏密法 (Khodaei & Faez, 2012)，實驗中試著改良新式 PVD 藏密法運算式，讓每個機密資訊位元都能從偽裝影像中正確完整的取出，使得秘密訊息能夠完整的復原，並試著調整像素差值區間數量及嵌入秘密訊息的位元數，以提升藏密量為目的，同時能維持可接受的偽裝影像品質。

#### 3.2 藏密及取密程序

藏密相關詳細的流程為以下步驟：

步驟 1：將掩護影像 (Cover Image) 進行劃分，形成分別含有  $1 \times 3$  個連續且不重疊的像素區塊。

步驟 2：區塊的中間像素  $P_{ic}$  表示為第  $i$  個區塊之基底像素 (圖 4)，基底像素使用 4-bit LSB 藏密法，基底像素  $P_{ic}$  採用 4-bit LSB 轉換成十進位的值稱為  $LSB_i$ ，預藏入的 4 位元密文轉換十進位稱為  $s_i$ ，計算  $LSB_i$  與  $s_i$  差值如公式 (14) 所示。

$$d_{ic} = LSB_i - s_i \quad (14)$$

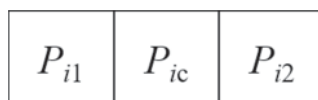


圖 4 基底像素選定示意圖

步驟 3：基底像素  $P_{ic}$  採用 4 位元 LSB 嵌密後的像素值  $P'_{ic}$ 。

$$P'_{ic} = P_{ic} - (P_{ic} \bmod 2^4) + s_i \quad (15)$$

步驟 4：使用最佳化像素調整程序調整基底像素 $P'_{ic}$ 。

$$P'_{ic} = \begin{cases} P'_{ic} + 2^4, & \text{if } d_{ic} > 2^3 \text{ and } 0 \leq P'_{ic} + 2^4 \leq 255 \\ P'_{ic} - 2^4, & \text{if } d_{ic} < -2^3 \text{ and } 0 \leq P'_{ic} - 2^4 \leq 255 \\ P'_{ic}, & \text{otherwise} \end{cases} \quad (16)$$

步驟 5：分別計算像素 $P_{i1}$ 、 $P'_{ic}$ 、 $P_{i2}$ 的商數（高位元）和餘數（低位元），設定低位元最低有效位元取代法之置換量為 2 位元（ $k = 2$ ）。

$$Q'_{ic} = P'_{ic} \div 2^k, \text{ and } Q_{iv} = P_{iv} \div 2^k, v=1, 2$$

$$R'_{ic} = P'_{ic} \bmod 2^k, \text{ and } R_{iv} = P_{iv} \bmod 2^k, v=1, 2 \quad (17)$$

步驟 6：分別計算 $Q'_{ic}$ 與 $Q_{i1}$ 與 $Q_{i2}$ 差值。

$$d_{iv} = |Q'_{ic} - Q_{iv}| \quad v=1, 2 \quad (18)$$

步驟 7：定義藏密區間範圍表，見表 2 所示。

表 2 本研究區間範圍表

| Range ( $R_j$ )   | $R_1$ | $R_2$  | $R_3$   | $R_4$   |
|-------------------|-------|--------|---------|---------|
| 區間範圍 $[l_i, u_i]$ | [0,3] | [4,11] | [12,19] | [20,63] |
| 可藏位元數 ( $n$ )     | 2     | 3      | 3       | 4       |

步驟 8：依差值 $d_{i1}$ 、 $d_{i2}$ 對照表 2，判斷差值的範圍區間 $R_j$ ，即可得知區間的最低範圍 $l_i$ 及嵌入秘密訊息的位元數 $n$ ，從二進位秘密訊息取 $n$ 位元，並轉換十進位為 $b_{iv}$ ，計算新差值 $d'_{iv}$ 。

$$d'_{iv} = l_i + b_{iv}, v=1, 2 \quad (19)$$

步驟 9：計算像素 $Q_{iv}$ 嵌密後可能之值 $Q''_{iv}$ 及 $Q'''_{iv}$ 。

$$Q''_{iv} = Q'_{ic} - d'_{iv} \text{ and } Q'''_{iv} = Q'_{ic} + d'_{iv}, v=1, 2 \quad (20)$$

步驟 10：以下列公式重新調整藏密後的值。

$$Q'_{iv} = \begin{cases} Q''_{iv}, & \text{if } (Q'''_{iv} > 63) \text{ or } |Q_{iv} - Q''_{iv}| < |Q_{iv} - Q'''_{iv}| \\ & \text{and } 0 \leq Q''_{iv} \leq 63 \text{ and } 0 \leq Q'''_{iv} \leq 63 \\ Q'''_{iv}, & \text{if } (Q''_{iv} < 0) \text{ or } |Q_{iv} - Q'''_{iv}| < |Q_{iv} - Q''_{iv}| \\ & \text{and } 0 \leq Q''_{iv} \leq 63 \text{ and } 0 \leq Q'''_{iv} \leq 63 \end{cases}, v=1, 2 \quad (21)$$

步驟 11：從二進位秘密訊息取 $k$ 位元像素值，分別嵌入像素值 $P_{i1}$ 、 $P_{i2}$ 之 $k$ 位元 LSB，並轉換成十進位 $R'_{i1}$ 及 $R'_{i2}$ ，最後計算偽裝像素值 $P'_{i1}$ 與 $P'_{i2}$ 。

$$P'_{iv} = Q'_{iv} \times 2^k + R'_{iv}, v=1, 2 \quad (22)$$

取密方法較藏密流程簡易，詳細說明如以下步驟：

步驟 1：將偽裝影像（Stego Image）切割成 $1 \times 3$ 像素為單位之區塊。

步驟 2：首先將 $P'_{ic}$ 轉二進位提取最低 4 個位元及 $P'_{i1}$ 、 $P'_{i2}$ 轉二進位提取最低 2 位元，並依下列公式分別計算 $Q'_{ic}$ 及 $Q'_{i1}$ 、 $Q'_{i2}$ 。

$$Q'_{iv} = P'_{iv} \div 2^k, v=1, 2$$

$$Q'_{ic} = P'_{ic} \div 2^k \quad (23)$$

步驟 3：計算 $Q'_{i1}$ 、 $Q'_{ic}$ 差值 $d'_{i1}$ 與 $Q'_{i2}$ 、 $Q'_{ic}$ 差值 $d'_{i2}$ 。

$$d'_{iv} = |Q'_{ic} - Q'_{iv}|, v=1, 2 \quad (24)$$

步驟 4：對照差值區間表 2，得知 $d'_{iv}$ 是屬於區間 $R_j$ ，此區間像素最低範圍 $l_{iv}$ ，藏密量為 $n$ 位元，依下列公式計算秘密訊息 $b_{iv}$ ，將十進位 $b_{iv}$ 轉換二進位提取秘密訊息。

$$b_{iv} = |d'_{iv} - l_{iv}|, v=1, 2 \quad (25)$$

### 3.3 藏密及取密過程範例說明

本研究藏密過程範例說明見圖 5 所示，將掩護影像切割成  $1 \times 3$  個連續且不重疊像素之區塊，假設一像素區塊的像素值 $(P_{i1}, P_{ic}, P_{i2}) = (132, 122, 80)$ ，預藏入秘密訊息 $s = (0101 \ 010 \ 100 \ 01 \ 11)_2$ ，若定義 $k = 2$ ，首先進行依據公式(14)計算 $LSB_i$ 與 $s_{ic}$ 之間差值 $d_i$ ， $LSB_i = (1010)_2 = 10$ ，取 4 位元密文 $s_{ic} = (0101)_2 = 5$ ， $d_i = 10 - 5 = 5$ ，將基底像素轉二進位 $P_{ic} = 122 = (01111010)_2$ ，基底像素使用 4-bit LSB 嵌密，並依公式(15)計算最低位元取代法置換 $P'_{ic} = 122 - (122 \bmod 2^4) + 5 = 117$ ，並依公式(16)調整基底像素後， $P'_{ic}$ 仍為 117。依據公式(17)計算區塊像素值的商數分別為 $Q_{i1} = 33$ 、 $Q'_{ic} = 29$ 、 $Q_{i2} = 20$ ，餘數分別為 $R_{i1} = 0$ 、 $R'_{ic} = 1$ 、 $R_{i2} = 0$ ，分別計算 $Q_{ic}$ 與 $Q_{i1}$ 、 $Q_{i2}$ 差值 $d_{i1} = |29 - 33| = 4$ 與 $d_{i2} = |29 - 20| = 9$ ，依其值對照區間範圍表 2 判定 $d_{i1}$ 及 $d_{i2}$ 屬於區間 2，且得知嵌入秘密訊息位元數分別為 $n_{i1} = 3$ 位元、 $n_{i2} = 3$ 位元，依照所決定的位元數，將預藏入之二進位秘密訊息轉換十進位值，獲得 $b_{i1}^m = (010)_2 = 2$ 與 $b_{i2}^m = (100)_2 = 4$ ，再依據公式(19)計算新差值 $d'_{i1} = l_{i1} + b_{i1}^m = 4 + 2 = 6$ 、 $d'_{i2} = 4 + 4 = 8$ ，計算像素 $Q_i$ 嵌密後可能的值 $Q''_{i1} = Q'_{ic} - d'_{i1} = 29 - 6 = 23$ 與 $Q'''_{i1} = Q'_{ic} + d'_{i1} = 29 + 6 = 35$ ，並計算 $Q''_{i2} = 29 - 8 = 21$ 、 $Q'''_{i2} = 29 + 8 = 37$ ，依據公式(21)重新調整藏密後的值獲得 $Q'_{i1} = 35$ 、 $Q'_{i2} = 21$ ，接續，像素低位元嵌入 2 位元，並轉換成十進位 $R'_{i1} = (01)_2 = 1$ 、 $R'_{i2} = (11)_2 = 3$ ，最後依據公式(22)計算偽裝像素值 $P'_{i1} = Q'_{i1} \times 2^2 + R'_{i1} = 35 \times 4 + 1 = 141$ 、 $P'_{i2} = 21 \times 4 + 3 = 87$ ，最終的偽裝像素為 $(P'_{i1}, P'_{ic}, P'_{i2}) = (141, 117, 87)$ 。

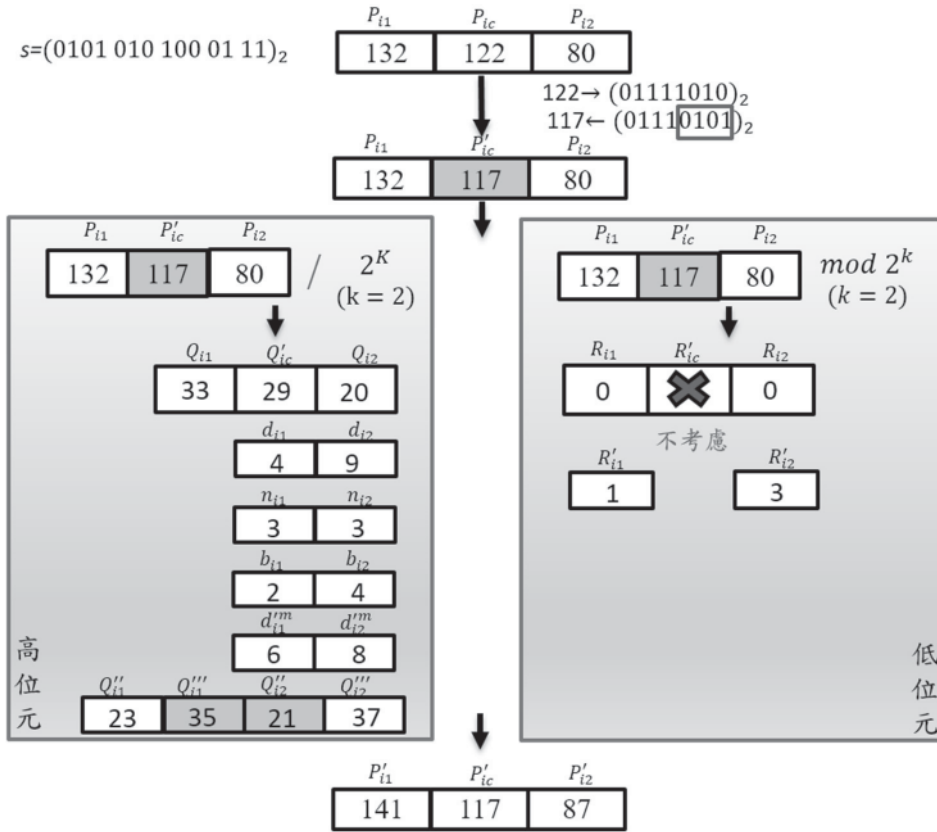


圖 5 本研究藏密過程示意圖

本研究取密過程範例說明見圖 6 所示，假設藏密像素區塊為  $(P'_{i1}, P'_{ic}, P'_{i2}) = (141, 117, 87)$ ，首先將基底像素  $P'_{ic}$  轉二進位  $117 = (01110101)_2$ ，提取基底像素  $P'_{ic}$  最低 4 位元，其值為 0101。依公式 (23) 計算藏密像素值商數分別為  $Q'_{i1} = 141 \div 4 = 35$ 、 $Q'_{ic} = 117 \div 4 = 29$ 、 $Q'_{i2} = 87 \div 4 = 21$ ，並計算  $Q'_{ic}$  與  $Q'_{i1}$ 、 $Q'_{i2}$  差值  $d'_{i1} = |29 - 35| = 6$ ，對照差值區間表 2 得知  $d'_{i1} \in R_2$ ，藏密量為 3 位元，此區間最低範圍  $l_{i1} = 4$ ，另  $d'_{i2} = |29 - 21| = 8$  得知  $d'_{i2} \in R_2$ ，藏密量為 3 位元，此區間最低範圍  $l_{i2} = 4$ ，依公式 (25) 計算  $b'_{iv} = |d'_{iv} - l_{iv}|$ ， $v=1, 2$ ， $b'_{i1} = 6 - 4 = 2$ ，將  $b'_{i1}$  轉二進位其值為  $(010)_2$ ，另  $b'_{i2} = 8 - 4 = 4$ ，將  $b'_{i2}$  轉二進位其值為  $(100)_2$ ，再將  $P'_{i1}$ 、 $P'_{i2}$  像素值轉二進位並提取最低 2 位元，獲得  $(01)_2$  及  $(11)_2$ ，最後，依序結合所提取的訊息，即獲得完整秘密訊息  $s = (0101\ 010\ 100\ 01\ 11)_2$ 。

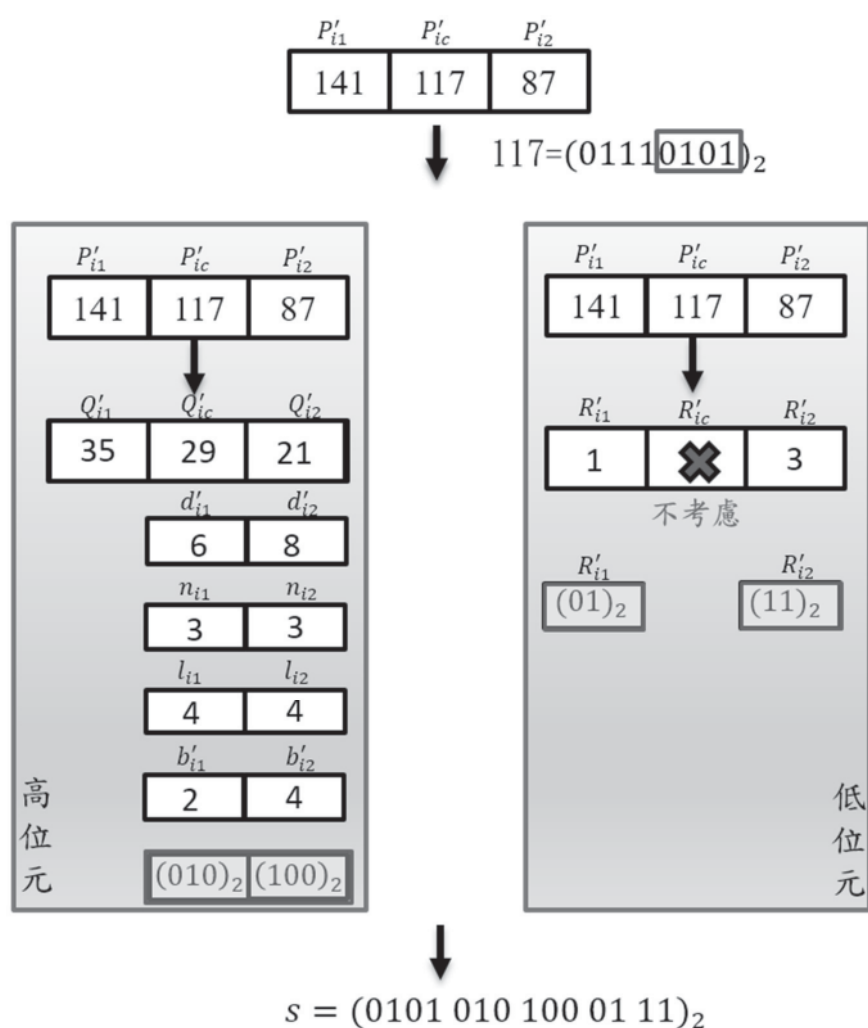


圖 6 本研究取密過程示意圖

因本研究旨在改善 Jung 學者所提藏密法於藏密後會產生溢位狀況，導致無法正確提取秘密訊息問題。而本研究之所以能解決溢位問題，主要在於藉由公式 (21) 重新調整藏密後的高位元像素值，使其值不會超過 63 或小於 0，故與低位元像素值結合後，不會產生溢位問題，本研究經實作表 3 所列程式後，所得各實驗影像溢位數量如下，證明本研究可改善溢位狀況。

表 3 溢位狀況統計表

| 方法<br>影像 | 原始<br>PVD<br>2003 | 新式<br>LSB/PVD<br>2012 | 新式Side<br>Match/PVD<br>2018 | 混合<br>LSB/PVD<br>2018 | 新式LSB/<br>MPVD<br>2020 | 本研究 |
|----------|-------------------|-----------------------|-----------------------------|-----------------------|------------------------|-----|
| Lena     | 0                 | 7                     | 0                           | 0                     | 0                      | 0   |
| Airport  | 11                | 0                     | 0                           | 0                     | 0                      | 0   |
| Boat     | 37                | 4                     | 0                           | 41                    | 0                      | 0   |
| Goldhill | 1                 | 0                     | 0                           | 0                     | 0                      | 0   |
| Baboon   | 28                | 0                     | 0                           | 75                    | 0                      | 0   |
| Tiffany  | 1110              | 1138                  | 0                           | 2534                  | 0                      | 0   |
| House    | 45                | 12                    | 0                           | 5                     | 0                      | 0   |
| Peppers  | 383               | 0                     | 0                           | 4113                  | 0                      | 0   |
| Average  | 201.87            | 145.12                | 0                           | 529.5                 | 0                      | 0   |

## 四、實驗結果

本節將對本研究所提出之改良混合最低位元取代法與像素差值之資訊隱藏技術與其他學者所提藏密法進行藏密量與偽裝影像品質比較，藉由實驗數據驗證本方法可行性。而為驗證本方法是否可抵抗藏密分析方法之偵測，以像素差值直方圖及內容選擇殘差分析技術進行偽裝影像偵測。

### 4.1 實驗環境

實驗影像以資訊隱藏經常使用的 Baboon、Boat、House、Airplane、Goldhill、Lena、Tiffany、Peppers 等 8 張大小 512x512 的標準灰階影像進行測試（見圖 4），測試影像中包含平滑及粗糙紋理之影像。嵌入的秘密訊息以隨機亂數 0 或 1 的字串組成，實驗結果以藏密量、峰值信噪比（PSNR）及結構相似性（SSIM）作為衡量標準。

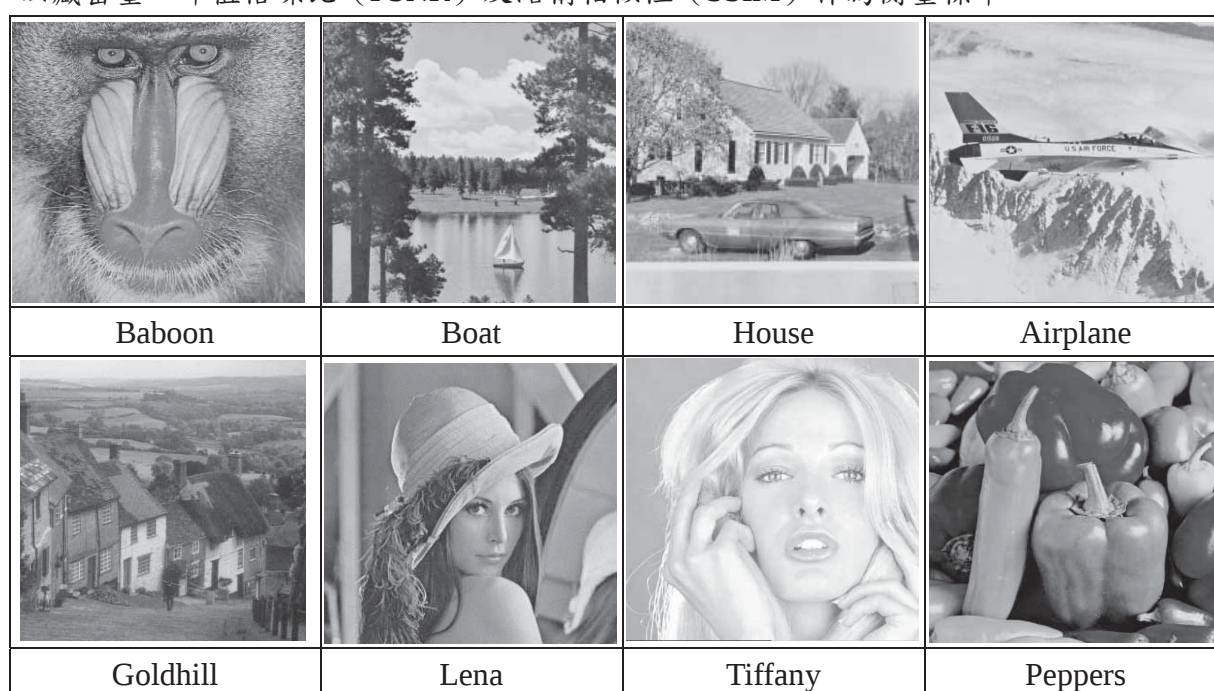


圖 7 本研究使用之測試影像

### 4.2 實驗結果分析

本研究所提出之方法，分別與原始 PVD 藏密法（Wu & Tsai, 2003）、新式 LSB/PVD 藏密法（Khodaei & Faez, 2012）、新式 Side Match/PVD 藏密法（Liu et al., 2018）、混合 LSB/PVD 藏密法（Jung, 2018）、新式 LSB/MPVD 藏密法（Liu et al., 2020）進行比較，其藏密量比較結果見表 4、PSNR 與 SSIM 比較結果見表 5 所示。在表 4 針對各方法藏密量與嵌入率（bit per pixel, bpp）（括弧內的值）進行比較，可發現原始 PVD 藏密法，在藏密上因以單一藏密法為主，故藏密量與嵌入率相較低。而新式 LSB/PVD 藏密法、Side Match/PVD 藏密法與混合 LSB/PVD 藏密法和新式 LSB/MPVD 藏密法因結合了 2 種藏密方法，故相較原始 PVD 方法，具有較高的藏密量與嵌入率。而本研究提出的方法與混合 LSB/PVD 藏密法最大的不同，在於針對高位元採用改良新式 PVD 藏密法

及調整像素差值區間表，此步驟可有利於提高藏密量與嵌入率及維持可接受的影像品質。

表 4 各方法藏密量與嵌入率比較表（單位:bit）

| 方<br>法<br>影<br>像 | 原始<br>PVD<br>2003               | 新式<br>LSB/PVD<br>2012           | 新式Side<br>Match/PVD<br>2018     | 混合<br>LSB/PVD<br>2018             | 新式LSB/<br>MPVD<br>2020          | 本研究                               |
|------------------|---------------------------------|---------------------------------|---------------------------------|-----------------------------------|---------------------------------|-----------------------------------|
| Lena             | 409,807<br>(1.56)               | 809,966<br>(3.09)               | 712,112<br>(2.72)               | 1,049,742<br>(4.00)               | 962,452<br>(3.67)               | 1,067,749<br>(4.07)               |
| Airport          | 409,834<br>(1.56)               | 809,262<br>(3.09)               | 717,511<br>(2.74)               | 1,050,973<br>(4.01)               | 963,471<br>(3.68)               | 1,062,797<br>(4.05)               |
| Boat             | 420,638<br>(1.60)               | 820,391<br>(3.13)               | 735,413<br>(2.81)               | 1,051,124<br>(4.01)               | 965,764<br>(3.68)               | 1,080,448<br>(4.12)               |
| Goldhill         | 411,896<br>(1.57)               | 813,968<br>(3.11)               | 720,574<br>(2.75)               | 1,049,093<br>(4.00)               | 962,633<br>(3.67)               | 1,072,427<br>(4.09)               |
| Baboon           | 457,105<br>(1.74)               | 886,516<br>(3.38)               | 808,760<br>(3.09)               | 1,054,327<br>(4.02)               | 977,179<br>(3.73)               | 1,113,184<br>(4.25)               |
| Tiffany          | 407,365<br>(1.55)               | 806,847<br>(3.08)               | 709,764<br>(2.71)               | 1,049,513<br>(4.00)               | 961,484<br>(3.67)               | 1,062,916<br>(4.05)               |
| House            | 420,123<br>(1.60)               | 818,580<br>(3.12)               | 729,785<br>(2.78)               | 1,051,474<br>(4.01)               | 965,871<br>(3.68)               | 1,074,960<br>(4.10)               |
| Peppers          | 407,643<br>(1.56)               | 802,228<br>(3.06)               | 713,062<br>(2.72)               | 1,050,571<br>(4.01)               | 961,563<br>(3.67)               | 1,066,084<br>(4.07)               |
| Average          | <b>418,051</b><br><b>(1.59)</b> | <b>820,970</b><br><b>(3.13)</b> | <b>730,873</b><br><b>(2.79)</b> | <b>1,050,852</b><br><b>(4.01)</b> | <b>965,052</b><br><b>(3.68)</b> | <b>1,075,071</b><br><b>(4.10)</b> |

表 5 針對衡量偽裝影像品質之 PSNR 及 SSIM 值（括弧內的值）進行比較，可察覺原始 PVD 藏密法、新式 LSB/PVD 藏密法、新式 Side Match/PVD 藏密法因藏密量較低，故偽裝影像品質較佳，而本研究藏密法的 PSNR 值平均約為 30.82 dB，與混合 LSB/PVD 藏密法相比，在藏密量提升 2.3%（約 24,219 位元），而偽裝影像品質 PSNR 值僅下降 6%（約 1.96 dB），SSIM 值下降約 0.013，實驗結果顯示本研究藏密法可提升藏密量，並維持可接受的影像品質（平均約 30.82 dB）。

為了驗證本研究所提出的藏密技術可應用於不同類型的廣泛性影像，針對 BossBase 影像資料庫（BOSSBases v0.93）10,000 張影像大小為 512×512 灰階影像進行藏密量及影像品質的計算，實驗結果見表 6 所示，本研究藏密技術藏密量平均約為 1,063,855 位元，PSNR 值平均約為 31.11dB，與混合 LSB/PVD 藏密法相比，藏密量提升 1.3%（約 14,210 位元），而影像品質 PSNR 值下降 4.2%（約 1.365 dB），SSIM 值下降約 0.013，實驗結果證實本研究方法與其他藏密技術進行數據比較，可具備較高藏密量，且維持可接受的影像品質。

表 5 各方法 PSNR 與 SSIM 比較表

| 方法<br>影像 | 原始<br>PVD<br>2003              | 新式<br>LSB/PVD<br>2012          | 新式Side<br>Match/PVD<br>2018    | 混合<br>LSB/PVD<br>2018          | 新式LSB/<br>MPVD<br>2020         | 本研究                            |
|----------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
| Lena     | 41.18<br>(0.978)               | 37.63<br>(0.936)               | 36.70<br>(0.929)               | 33.21<br>(0.805)               | 35.35<br>(0.896)               | 31.47<br>(0.801)               |
| Airport  | 40.20<br>(0.973)               | 37.53<br>(0.931)               | 36.19<br>(0.923)               | 33.19<br>(0.787)               | 35.33<br>(0.882)               | 31.8<br>(0.797)                |
| Boat     | 39.71<br>(0.981)               | 36.53<br>(0.941)               | 34.97<br>(0.941)               | 32.84<br>(0.846)               | 34.91<br>(0.918)               | 30.65<br>(0.829)               |
| Goldhill | 41.00<br>(0.983)               | 37.55<br>(0.944)               | 36.23<br>(0.944)               | 32.54<br>(0.859)               | 35.31<br>(0.920)               | 31.16<br>(0.843)               |
| Baboon   | 36.96<br>(0.987)               | 36.29<br>(0.934)               | 32.04<br>(0.934)               | 31.74<br>(0.927)               | 33.93<br>(0.956)               | 29.67<br>(0.901)               |
| Tiffany  | 40.89<br>(0.974)               | 37.79<br>(0.922)               | 36.84<br>(0.922)               | 32.47<br>(0.780)               | 34.76<br>(0.876)               | 30.37<br>(0.758)               |
| House    | 39.15<br>(0.977)               | 36.44<br>(0.937)               | 35.47<br>(0.937)               | 32.73<br>(0.838)               | 34.96<br>(0.908)               | 30.96<br>(0.834)               |
| Peppers  | 40.61<br>(0.978)               | 37.97<br>(0.927)               | 34.83<br>(0.927)               | 33.55<br>(0.806)               | 34.89<br>(0.900)               | 30.49<br>(0.785)               |
| Average  | <b>39.96</b><br><b>(0.978)</b> | <b>37.21</b><br><b>(0.932)</b> | <b>35.40</b><br><b>(0.932)</b> | <b>32.78</b><br><b>(0.831)</b> | <b>34.93</b><br><b>(0.907)</b> | <b>30.82</b><br><b>(0.818)</b> |

表 6 BossBase 影像資料庫影像運算平均值

| 方法<br>影像 | 原始PVD<br>2003 | 新式<br>LSB/PVD<br>2012 | 新式Side<br>Match/PVD<br>2018 | 混合<br>LSB/PVD<br>2018 | 新式<br>LSB/MPVD<br>2020 | 本研究       |
|----------|---------------|-----------------------|-----------------------------|-----------------------|------------------------|-----------|
| 藏密量      | 409,780       | 805,717               | 719,708                     | 1,049,645             | 962,718                | 1,063,855 |
| PSNR     | 40.858        | 35.146                | 35.502                      | 32.475                | 34.906                 | 31.11     |
| SSIM     | 0.969         | 0.919                 | 0.909                       | 0.783                 | 0.878                  | 0.77      |

### 4.3 安全性分析

資訊隱藏技術的原則是指在網路上傳遞訊息時不被其他人察覺，而不可察覺除了要避免被人類視覺發現影像失真情形，也要避免被藏密分析技術偵測出異常狀況。本節將探討本研究所提出藏密技術是否可有效抵抗藏密分析方法偵測，採用空間域常見的像素差值直方圖（Pixel Difference Histogram, PDH）及內容選擇殘差（Content-Selective Residuals, CSR）兩種藏密的分析技術進行偽裝影像偵測。

#### 4.3.1 像素差值直方圖分析

一般灰階影像像素以 8 位元表示，其值介於 0 到 255 的範圍，表示灰色深淺。像素差值直方圖用來統計偽裝影像相鄰像素差值出現的次數，一般載體影像相鄰像素會呈現

常態分佈見圖 8 (a) 所示，直方圖橫軸為像素差值，縱軸為像素差值的統計量，影像經藏密演算法計算後會改變像素間彼此的相關性，像素差值直方圖會呈現不正常的分佈見圖 8 (b) (c) (d) 所示，若直方圖呈現不正常階梯狀的分佈狀態，此顯著分佈的差異變化容易成為藏密偵測特徵，可偵測出影像內是否隱藏秘密訊息。

本研究針對原始 PVD 藏密法、新式 Side Match/PVD 藏密法、混合 LSB/PVD 藏密法、新式 LSB/MPVD 及本研究所提出藏密方法分別進行藏密運算後所產生的像素差值直方圖進行安全性分析。（以 Lena 圖為例，掩護影像的像素直方圖見圖 8 (a) 所示，各方法藏密後所產生像素差值直方圖見圖 8 (b) (c) (d) (e) (f) 所示）。在圖 8 (b) (c) (d) 所示，原始 PVD 藏密法、新式 Side Match/PVD 藏密法與新式 LSB/MPVD 藏密法經藏密演算法運算後所產生像素差值直方圖明顯呈現不正常的階梯狀分佈，這類特徵容易遭藏密分析方法偵測。而圖 8 (e) (f) 所示，混合 LSB/PVD 藏密法與本研究所提藏密方法所產生的像素差值直方圖呈現常態分佈趨勢，較能有效抵禦像素差值直方圖藏密分析偵測。

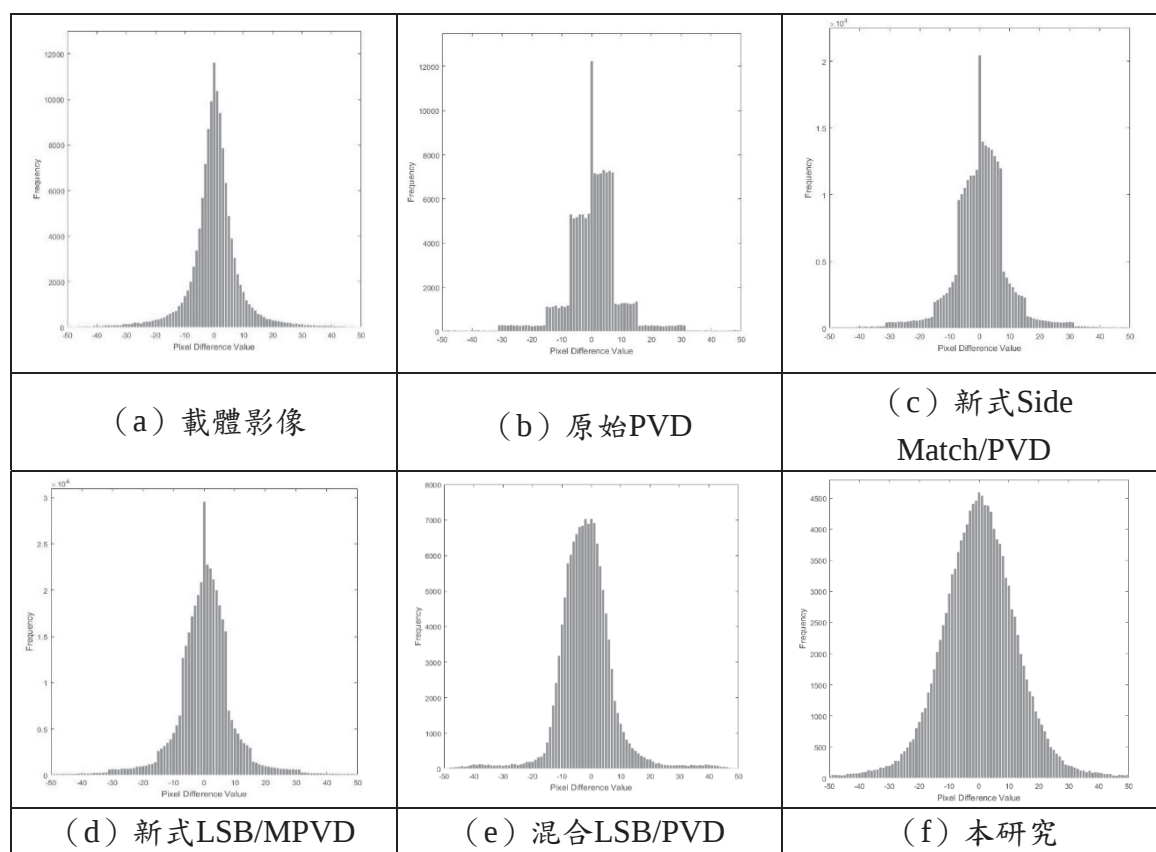


圖 8 各藏密方法之像素差值直方圖

#### 4.3.2 內容選擇殘差分析

內容選擇殘差 (Content-Selective Residuals, CSR) 影像藏密分析技術，是由 Denmark 等學者於 2014 年提出，針對測試影像擷取 1183 個藏密特徵，使用統計分析技術來判斷是否隱藏秘密訊息。本研究採用 BossBase 影像資料庫挑選 10,000 張影像大小為 512×512

灰階影像及經本研究藏密法藏密後影像進行偵測分析，最後藏密分析效能以類別預測最常用的評估指標準確率（Accuracy）計算，見公式（26）所示，準確率愈低表示藏密的安全性較高。其中正確分類區分二項分別為 TP（True Positive, TP）為實際偽裝影像預測為偽裝影像、TN（True Negative, TN）為實際掩護影像預測為掩護影像，錯誤分類區分二項分別為 FP（False Positive, FP）為實際為掩護影像預測為偽裝影像、FN（False Negative, FN）為實際為偽裝影像預測為掩護影像。

$$Accuracy = \frac{TN+TP}{TN+TP+FN+FP} \times 100\% \quad (26)$$

本研究針對新式 Side Match/PVD 藏密法、混合 LSB/PVD 藏密法、新式 LSB/MPVD 及本研究所提出藏密方法分別採用 CSR 影像藏密分析方法進行藏密偵測，實驗結果見表 7 所示，本研究所提出的藏密方法，所獲得的偵測正確率為 56.22%，雖然較新式 LSB/PVD、新式 Side Match/PVD 藏密法與混合 LSB/PVD 分別高出 2%、3.12%及 0.13%，但仍高於隨機判斷之機率 50%，根據實驗結果，本研究藏密方法可有效抵抗 CSR 影像藏密偵測，當藏密量愈高的藏密方法，在藏密後所產生的特徵值較高容易遭分析方法偵測。

因本研究所提藏密技術為藏密學（Steganography）之應用，而非屬於浮水印（Watermarking）的範疇，這二類技術應用範圍不同，所需抵抗之相關攻擊亦不同。故本研究乃針對相關藏密分析技術進行實驗與討論，而不針對浮水印技術所會遭受的攻擊（如胡椒鹽雜訊、高斯白雜訊、旋轉等）進行說明。

表 7 CSR 影像偵測結果

| 方法 \ 分類           | TP     | TN    | FP     | FN  | Accuracy (%) |
|-------------------|--------|-------|--------|-----|--------------|
| 新式 LSB/PVD        | 4999.1 | 423.2 | 4576.8 | 0.9 | 54.22%       |
| 新式 Side Match/PVD | 5000   | 310.4 | 4689.6 | 0   | 53.10%       |
| 混合LSB/PVD         | 4996.8 | 611.8 | 4388.2 | 3.2 | 56.09%       |
| 新式 LSB/MPVD       | 5000   | 659.2 | 4340.8 | 0   | 56.6%        |
| 本研究               | 4999   | 623.3 | 4376.6 | 1   | 56.22%       |

## 五、結論與未來研究方向

### 5.1 結論

本研究中提出了高容量資訊隱藏技術，改良 Jung 學者的混合像素差值藏密法及最低位元取代藏密法，然而要提出一種高隱藏的容量的方法，相對的會降低不可察覺性及安全性，因此，經過反覆實驗後，決定將掩護影像分割成  $1 \times 3$  不重疊的區塊大小，選定

區塊中間像素為基底像素，基底像素採用採用 LSB 及 OPAP 藏密法嵌入 4 位元的秘密訊息，其餘像素與藏密後的基底像素作差值計算，採用改良混合 LSB/PVD 法進行藏密，以達到提升藏密量為目的，同時維持可接受的影像品質。實驗影像以 Lena 等 8 張灰階影像進行測試，實驗結果顯示本研究的平均藏密量為 1,075,071 位元，與混合 LSB/PVD 藏密法相較，藏密量可提升約略 2.3%（約 24,219 位元），而偽裝影像品質 PSNR 值僅下降 6%（約 1.96 dB），SSIM 值下降約 0.013。

為驗證本研究所提出的藏密技術可應用於不同類型的廣泛性影像，針對 BossBase 影像資料庫 10,000 張影像大小為 512×512 灰階影像進行藏密量及影像品質的計算，藏密量平均約為 1,063,855 位元，PSNR 值平均約為 31.11 dB，與混合 LSB/PVD 藏密法相比，藏密量提升 1.3%（約 14,210 位元），而影像品質 PSNR 值下降 4.2%（約 1.365 dB），SSIM 值下降約 0.013，證明本研究藏密法可有效提升藏密量，同時能維持人眼難以察覺的範圍內。本研究安全性分析採用空間域常見的像素差值直方圖（PDH）及內容選擇殘差（CSR）兩種分析技術進行偵測，其分析結果證明本研究所提藏密技術之安全性。

## 5.2 未來研究方向

未來可以本研究為基礎探討與其他藏密技術的整合，若能依每種不同類型影像特性，如影像亮度、對比度等因素，若可動態調整每個像素適合嵌入的秘密訊息藏密量，可提升藏密的安全強度，是未來研究值得探討的方向。

## 5.3 國防領域之應用

近年來網路駭客攻擊及犯罪事件頻傳不斷，有心人士若運用資訊隱藏技術將不法資訊嵌入至灰階或彩色影像、視訊影片及音訊檔案內，提供恐怖份子執行非法的行為之依據，將可能對個人或國家安全造成損害的疑慮。所以身為國防資訊安全研究人員，必須熟悉相關資訊隱藏與資訊隱藏分析技術之方向。因此，本研究可提供國防資訊安全管理技術研究領域人員實務應用參考。

## 參考文獻

- 王旭正、翁麒耀、黃正達，2016。數位資訊@多媒體安全與應用。台北市：博碩文化。
- 劉江龍、賴泰宏、李翊豪，2012。可抵抗直方圖攻擊的像素差值藏密技術。第十一屆離島資訊技術與應用研討會。
- Bender, W., Gruhl, D., Morimoto, N., and Lu, A., 1996. Techniques for data hiding. *IBM Systems Journal*, 35(3), 313-336.
- BOSS Break Our Steganographic System, BOSSBases (v0.93) (available online: <http://agents.fel.cvut.cz/boss/index.php?mode=VIEW&tmpl=materials> [visited on 2021/05/08]).
- Chan, C. K. and Cheng, L. M., 2004. Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37(3), 469-474.
- Denemark, T., Fridrich, J., and Holub, V., 2014. Further study on the security of S-UNIWARD, SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics. *International Society for Optics and Photonics*, 9028, 902805.
- Johnson, N. F. and Jajodia, S., 1998. Exploring steganography: Seeing the unseen, *Computer*, 31(2), 26-34.
- Jung, K. H., 2018. Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane, *J Real-Time Image Proc*, 14(1), 127-136.
- Khodaei, M. and Faez, K., 2012. New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing, *IET Image Processing*, 6(6), 677-686.
- Liu, H. H., Su, P. C., and Hsu, M. H., 2020. An Improved Steganography Method Based on Least-Significant-Bit Substitution and Pixel-Value Differencing, *KSII Transactions on Internet and Information Systems*, 14(11), 4,537-4,556.
- Liu, H. H., Lin, Y. C., and Lee, C. M., 2018. A digital data hiding scheme based on pixel-value differencing and side match method, *Multimedia Tools and Applications*, 78(9), 12,157-12,181.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G., 1999. Information hiding- a survey. *Proceedings of the IEEE*, 87(7), 1,062-1,078.
- Wang, C. M., Wu, N. I., Tsai, C. S., and Hwang, M. S., 2008. A high quality steganographic method with pixel-value differencing and modulus function, *The Journal of Systems and Software*, 81, 150-158.
- Wu, D. C. and Tsai, W. H., 2003. A steganographic method for images by pixel value differencing, *Pattern Recognition Letters*, 24, 1,613-1,626.
- Wu, H. C., Wu, N. I., Tsai, C. S., and Hwang, M. S., 2005. Image steganographic scheme based on pixel-value differencing and LSB replacement methods, *IEE Proc-Vis Image Signal Process*, 152(5), 611-615.
- Zhou, W., and Bovik, A. C., 2002. A universal image quality index, *IEEE Signal Processing Letters*, 9(3), 81-84.
- Zhou, W., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P., 2004. Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4), 600-612.

## 政治因素對於預算通過率之影響

傅澤偉<sup>1\*</sup> 張哲豪<sup>2</sup>

<sup>1</sup>國防大學管理學院財務管理學系

<sup>2</sup>國防部憲兵指揮部

論文編號：NM-43-01-12

來稿 2022 年 3 月 10 日→第一次修訂 2022 年 4 月 23 日→第二次修訂 2022 年 5 月 25 日→  
同意刊登 2022 年 8 月 17 日

### 摘要

有關政治因素對於我國政府預算的影響較少被討論。本研究以民國 83 年至 108 年期間我國執政黨（包含中國國民黨及民主進步黨）在立法院席次占比、國民所得毛額、我國立法委員選舉年度做為解釋變數且以預算案通過比率及金額為被解釋變數採用 ARDL 模式檢視其長期均衡關係。

研究發現主要為（1）執政黨在立法院席次占比及立法委員選舉年度對於國防預算案通過比率呈顯著正向影響且我國立法委員選舉年度對國防預算案通過比率的影響大於對總預算通過比率的影響。（2）非國防預算案通過比率與執政黨在立法院席次占比在長期上有負向關係，我國立法委員選舉年度對非國防預算案通過比率沒有顯著相關。（3）國防法定預算取自然對數只有執政黨當期在立法院席次占比呈現正向顯著效果。

**關鍵詞：**預算案通過比率、政治因素、國防預算、非國防預算

---

\*通訊作者：傅澤偉 e-mail: futzewe@gmail.com

# The Influence of Political Factor on the Budget Pass Rate

Fu, Tze-Wei<sup>1\*</sup> Chang, Che-Hao<sup>2</sup>

<sup>1</sup>Department of Financial Management, National Defense University

<sup>2</sup>Military Police Command, Ministry of National Defense

## Abstract

The impact of political factors on government's budget is less discussed. In this study, the proportion of ruling party which including Koumintang and Democratic Progress Party in Legislative Yuan Republic of China, the gross national income, and the legislator election year is discussed and data ranges from 1994 to 2019. The budget passed rate and budget amount are used as dependent variables and ARDL model examine the long-term equilibrium relationship.

The main findings of this study are as following: ( 1 ) the proportion of seats in the Legislative Yuan of the ruling party and the legislator election year have a significantly positive impact on the national defense budget pass rate, and the impact of the legislator election year on the national defense budget pass rate is greater than the overall budget pass rate at the legislator election year.

( 2 ) There is a long-term negative relationship between the pass rate of non-defense budgets and the proportion of seats in the Legislative Yuan of the ruling party. There is no significant correlation between the pass rate of non-defense budgets and the legislator election year. ( 3 ) The natural logarithm value of the national defense budget has a significantly positive relationship with current proportion of seats of the ruling party.

**Keywords:** Budget Pass Rate 、 Political Factors 、 Defense Budget 、 Non-Defense Budget

---

\* Corresponding Author Email: futzewe@gmail.com

## 一、緒論

政府預算的取得是政府施政最重要的一環。政府的政策必須依賴取得的預算來實踐。我國目前每年的政府法定預算為新台幣 2 兆 2 千億元。政府部門預定的施政計畫是編列成預算送達立法院審查，送審的預算即便是 1% 的被刪除，其所代表的是 220 億元的預定執行項目就無法實現。所以探討預算的通過率是個很重要的議題。

就國防管理而言，國防預算是政府重要的施政目標，國防部主計局擔任國軍年度概（預）算之擬訂、審議及督導的重責大任，我國預算法第二條：「各主管機關依其施政計畫初步估計之收支，稱概算；預算之未經立法程序者，稱預算案；其經立法程序而公布者，稱法定預算；在法定預算範圍內，由各機關依法分配實施之計畫，稱分配預算。」然而預算案與法定預算差異率（簡稱預算案通過比率）的穩定度會影響到國軍建軍備戰的政策推行，長期穩定的預算案通過比率是很重要的。這引發了本研究除了探討政府整體預算案通過比率以外，還把影響國防預算案通過比率列入研究。為了對比國防預算案通過比率，本研究將非國防預算的通過率也加入探討。

我國是民主國家，政府法定預算的形成是由行政院提出預算申請而由立法院進行核定。在這個過程中，立法院如何審查是個重要因素。然而過往許多對影響國防預算之相關研究上多著重外在環境因素探討，如威脅（Nordhaus, Oneal and Russett, 2012）、國家規模（Murdoch and Sandler, 1982）及貿易（Sheikh and Chaudhry, 2013）等，缺乏從政治因素角度切入之研究。

在國外有關政府預算的影響因素主要有選舉及政府的政黨特性。有關選舉對於預算的影響早就是一個很重要的議題。政治預算循環（political budget cycles）這個專有名詞就在說明政府在選舉前會追求預算的擴張。Nordhaus（1975）及 Rogoff and Sibert（1988）就發展出在有關選舉對財政政策的影響的相關理論。近期有關政治預算循環的研究如 Klomp and Haan（2013）及 Hanusch and Magleby（2014）發現執政黨特性對於政府支出有顯著影響。Artes and Jurado（2018）及 Portrafke（2011）的研究均支持執政黨的政黨特性會影響到預算的內容。我國的研究如黃秀端（2003）研究將我國政治狀況分為三個階段觀察，第一階段為國民黨執政並擁有國會多數支持的多數政府時期，第二階段為民進黨執政，但是國會多數為國民黨所掌握的少數政府時期，第三階段為民進黨執政，國會並沒有任何一黨掌握過半席次，該研究觀察結果是立法院對於行政院所提出的總預算的刪減比例，並未顯示少數政府與多數政府的差異。黃秀端（2003）的研究只探討總預算刪減，但並未探討預算的內容；例如國防預算的刪減比率與非國防預算的刪減比率。長期以來，經濟因素對於國防預算的影響是一個重要議題。其基本的想法在於經濟能力強的國家越有能力負擔軍事費用；以及任何國家均需要國防來保衛國家。很多學者以古典經濟學理論來探討國防支出

對於經濟成長的影響（如 Oladotun and Gumedé, 2019）。在實證研究上也有多的研究，有支持國防預算有助於經濟成長的如汪進揚、趙一鳴（2005）及 Oladotun and Gumedé（2019）。但也有研究發現有些國家國防預算對經濟成長為負向的影響，如張阜民、楊浩忠、柯俊禎與陳建宏（2013）針對台灣及南韓的研究；傅澤偉、蔡欣樺（2017）針對亞太地區國家的研究。

本研究的目的即在於控制經濟因素後，探討政治因素對我國總預算案、國防預算案、非國防預算案等的通過率及法定預算金額的影響。

## 二、文獻回顧

### 2.1 政治因素與預算的關聯性

政治預算循環的基本觀點認為在民主社會中，當面對選舉時政府會操縱預算以確保他們選舉的得勝。相關的研究很多，近期的研究如 Klomp and Haan（2013）及 Hanusch and Magleby（2014）。Klomp and Haan（2013）以 65 個民主國家的 1975-2005 年的資料進行分析，實證研究發現政治預算循環因素顯著正向影響政府支出且參與選舉的政黨數目越多會顯著減少政府支出。Hanusch and Magleby（2014）加入考量政府的聲望（支持度）對於預算擴張的影響，他們模式驗證出高支持率的政府在預算擴張的考量最主要是對於他們偏好的政策，亦即高支持度的政府對於特定的預算的偏好程度愈高。

執政黨特性對於政府支出會造成顯著的影響。Artes and Jurado（2018）將市政府的政黨狀態分為單一大黨（single majority）執政或是多個小黨（coalitions）聯合執政的兩種狀態進行分析。以西班牙多個市政府的資料進行實證分析。實證結果是執政政府是單一大黨政府預算收入比多個小黨（coalitions）聯合執政多 2%，執政政府是單一大黨政府預算支出比多個小黨（coalitions）聯合執政 1.5%，研究發覺執政政府的政黨組合特性會影響財政收入與支出。Portrafke（2011）以 20 個經濟合作暨發展組織（Organization for Economic Co-operation and Development, OECD）國家 1970 到 1997 以及 1990 到 2006 的期間進行分析，他將政府的生態分為左翼政府及右翼政府。其研究發覺左翼政府在 1970 到 1997 年之間對於公共服務的預算及 1990 年到 2006 年的教育預算顯著偏高。他的研究支持政府的政黨屬性會影響到預算的內容。Hankla（2013）研究發現政黨越分散，會採用較緊縮的預算。

許多文獻發現政黨對於政府支出的內容有很大的影響，尤其是對國防支出的影響。Kauder and Potrafke（2016）探討德國的軍費支出，發覺右派（保守派或傳統派）政黨執政時，軍事支出的成長率顯著偏高。傅澤偉、李政翰、林曼莉（2016）研究日本國防及社會福利預算與日本執政黨佔國會席次比例之關聯性，採用共整合分析結果顯示執政黨席次顯

著正向影響國防預算及社會福利預算佔總預算之編列比例。劉秀秀（2015）發現總統與立法委員之選舉對各部會總歲出與經常門預算刪減率的影響皆具有統計上的解釋力，經濟成長率對各部會總歲出與經常支出預算審議結果有顯著影響。湯國斌（2015）發現社會福利支出占國內生產毛額比率顯著受到執政黨屬性影響。

## 2.2 經濟因素與預算的關聯性

經濟對於政府支出的影響有很多實證研究，其中大部分的研究支持經濟成長有助於國防預算。汪進揚、趙一鳴（2005）研究 162 個國家發現經濟能力強的國家越有能力負擔軍事費用。楊登隆（2010）以系統動態學的因果回饋環路圖，研究發現當台灣上年度的國內生產毛額成長率增加，則下年度的國防預算成長率亦同時增加，說明國防預算規模與國家經濟發展有著密切的關係。陳勳慧、葉正國（2010）以階層迴歸模型實證分析結果發現：各國國防預算規模最重要受制於該國經濟實力的支持，經濟能力愈強，國防預算獲得額度愈高。傅澤偉、蔡欣樺（2017）研究發現國民所得毛額（Gross National Income, GNI）顯著負向影響國防預算，符合部分學者認為國家經濟能力越強時，政府傾向將預算資源分配到其他類別支出以促進經濟成長，造成排擠效果造成國防預算額度減少。

## 三、研究方法與模型

參考前述文獻，本研究以執政黨在立法院席次占比及立法委員選舉年度作為立法院審議時的 political 因素。以國民所得毛額當作經濟因素。針對我國預算案通過比率及法定預算金額進行長期均衡關係的分析。

### 3.1 資料來源與定義

本研究以民國 83 年至 108 年期間資料進行分析。所有變數資料皆採用年資料，共計 26 筆年資料。茲整理本研究變數之定義如表 1。

表 1 模型變數說明表

| 變數名稱／代號       | 變數說明                               | 資料來源      |
|---------------|------------------------------------|-----------|
| 總預算案通過比率／ALL  | 當年度法定預算金額除以預算案金額                   | 中華民國統計資訊網 |
| 國防預算案通過比率／D   | 當年度國防法定預算金額除以國防預算案金額               | 中華民國統計資訊網 |
| 非國防預算案通過比率／ND | 當年度（總法定預算扣除國防法定預算），除以（總預算案扣除國防預算案） | 中華民國統計資訊網 |

|                        |                         |                                             |
|------------------------|-------------------------|---------------------------------------------|
| 法定預算總金額取自然對數／SBLN      | 當年度法定預算總金額取自然對數         | 中華民國統計資訊網                                   |
| 國防法定預算總金額取自然對數／DSBLN   | 當年度國防法定預算總金額取自然對數       | 中華民國統計資訊網                                   |
| 非國防法定預算總金額取自然對數／NDSBLN | 當年度法定預算扣除國防法定預算總金額取自然對數 | 中華民國統計資訊網                                   |
| 執政黨在立法院席次占比／RP         | 當年度執政黨占立法院總席次比率         | 中央選舉委員會網站                                   |
| 我國立法委員選舉年度／LEY         | 設虛擬變數，立法委員選舉年度為 1，反之為 0 | 中央選舉委員會網站                                   |
| 國民所得毛額／GNI             | 平均每人國民所得毛額              | 台灣經濟新報資料庫<br>(Taiwan Economic Journal, TEJ) |

### 3.2 單根檢定

由於時間序列資料的特性是不確定的，因此我們在使用時間序列變數進行實證研究時，必須先確定變數的定態特徵。檢驗變數定態階次以便後續分析。如果變數呈現非穩定之性質時，此狀況下進行迴歸估計大多數時候會導致估計結果與實際上不符合的推論偏誤或可能會發生假性迴歸 (Spurious regression) 的狀況。本研究採用被經常使用的 Augmented Dickey-Fuller (ADF) 檢測來檢定變數的單根特性。

### 3.3 自我迴歸分配落後模型 Autoregressive distributed lag model, ARDL 模型

本文分析我國執政黨在立法院席次占比、我國立法委員選舉年度及國民所得毛額對我國預算案通過比率與法定金額的長期均衡關係。進行分析前要確定應變數或自變數屬於原變數即定態的  $I(0)$  或一階差分後呈現定態的  $I(1)$ 。針對這些變數的長期均衡關係，採用 Pesaran and Shin (1998) 提出自我迴歸時間落後分配模型 ARDL，不管潛在變數是  $I(0)$  或是  $I(1)$  均能有效檢定解釋變數和被解釋變數之間是否存在長期均衡關係。除了上述的優點之外，採取此方法亦能解決當遇到小樣本資料時，能改善檢定力低弱的問題，還有能分辨兩變數中何者是解釋變數何者是被解釋變數。Pesaran, Shin and Smith (2001) 推導的邊界檢定方法 (Bound Test) 來檢測變數間的長期均衡關係。自我迴歸分配落後 Autoregressive Distributed Lag (ARDL) 模型如下：

ARDL 模型中同時包含自變數  $x$  時間落差項與應變數  $y$  時間落差項，下例為  $y$  擁有  $p$  個時間落差項，而  $x$  有  $q$  個時間落差項的一般化 ARDL ( $p, q$ ) 模型，公式如下：

$$y_t = \alpha + \phi_0 x_t + \phi_1 x_{t-1} + \cdots + \phi_q x_{t-q} + \theta_1 y_{t-1} + \cdots + \theta_p y_{t-p} + v_t$$

其中  $X$  為自變數， $Y$  為應變數， $\alpha$  是截距項， $v_t$  是白噪音， $p$  為應變數差分項之落後期數， $q$  為自變數差分項之落後期數，以 ARDL ( $p, q$ ) 表示，雖然 ARDL 模型不需要預先測試單根，但為了避免變數有大於  $I(1)$  的隨機趨勢的情況下，我們應該進行單根檢定。本研究採取 AIC 準則做為模型中選取最適落後期數的標準。以 Bound Test 檢測模式中應變數與自變數的長期均衡關係。

#### 四、實證分析

本研究運用了 Pesaran and Shin (1998) 發展的自我迴歸時間落後分配模型 (ARDL model) 以解決本研究變數間不同階次的整合問題，以及運用 Pesaran et al. (2001) 推導的邊界檢定方法 (Bound Test) 來檢測我國執政黨在立法院席次占比、國民所得毛額、我國立法委員選舉年度對我國預算案通過比率及法定預算金額是否存在長期均衡關係。

##### 4.1 敘述統計

主要變數做基本統計，結果如表 2。其結果顯示，總預算案通過率的平均值是 0.983968，中位數是 0.986584，而最大值是 0.999826，最小值是 0.949625。國防預算案通過率的平均值是 0.984938，中位數是 0.988002，而最大值是 0.9992，最小值是 0.942633。非國防預算案通過率的平均值是 0.983727，中位數是 0.986793，而最大值是 0.999948，最小值是 0.942337。由各通過率的最大值與最小值差異均有 5% 左右，如以新台幣 2 兆元的總預算案而言，可能高達 1000 億元的預算就在立法院的審議中刪除，此現象顯現探討影響通過率的很重要的議題。

法定預算總金額取自然對數部分平均值是 21.1999，中位數是 21.22819，而最大值是 21.5274，最小值是 20.75206。國防法定預算取自然對數部分，平均值是 19.49606，中位數是 19.5059，而最大值是 19.81428，最小值是 19.34596。非國防法定預算取自然對數部分，平均值是 20.99603，中位數是 21.0212，而最大值是 21.32858，最小值是 20.4709。執政黨在立法院席次占比部分平均值是 0.549513，中位數是 0.556515，而最大值是 0.71681，最小值是 0.38666。最後國民所得毛額的部分，平均值是 18332，中位數是 17403，而最大值是 26528，最小值是 12343。樣本期間有 7 年為選舉年所以其平均數為 0.26923，最大值為 1 (選舉年)，最小值為 0 (非選舉年)。

表 2 敘述統計表

|                     | 平均數      | 中位數      | 最大值      | 最小值      | 標準差     |
|---------------------|----------|----------|----------|----------|---------|
| 總預算案通過率/ALL         | 0.983968 | 0.986584 | 0.999826 | 0.949625 | 0.00966 |
| 國防預算案通過率/D          | 0.984938 | 0.988002 | 0.999200 | 0.942633 | 0.0131  |
| 非國防預算案通過率/ND        | 0.983727 | 0.986793 | 0.999948 | 0.942337 | 0.01147 |
| 法定預算總金額自然對數/SBLN    | 21.1999  | 21.22819 | 21.5274  | 20.75206 | 0.21539 |
| 國防法定預算自然對數/DSBLN    | 19.49606 | 19.5059  | 19.81428 | 19.34596 | 0.11893 |
| 非國防法定預算取自然對數/NDSBLN | 20.99603 | 21.0212  | 21.32858 | 20.4709  | 0.24698 |
| 執政黨在立法院席次占比/RP      | 0.549513 | 0.556515 | 0.716810 | 0.38666  | 0.11571 |
| 國民所得毛額/GNI          | 18332    | 17403    | 26528    | 12343    | 4617    |
| 我國立法委員選舉年度/LEY      | 0.26923  | 0.00000  | 1        | 0        | 0.45234 |

## 4.2 單根檢定

本研究採取 Augmented Dickey-Fuller (ADF) 檢定及 AIC 準則做為模型中選取最適落後期數的標準，各變數之單根檢定結果於表 3。在原始值部分，在顯著水準 5% 下，國防預算通過比率、國防法定預算取自然對數、執政黨在立法院席次比及國民所得毛額等四個變數在三種檢測型式下均呈現非定態的時間數列。此 4 個變數經過一階差分之後在顯著水準 5% 下均呈現定態的現象。國防預算通過比率、國防法定預算取自然對數、執政黨在立法院席次比及國民所得毛額屬於  $I(1)$  時間數列。總預算通過比率、非國防預算案通過比率、法定預算總金額取自然對數及非國防法定預算取自然對數等四個時間數的原始值及一階差分結果顯示此四個時間數列為  $I(0)$  時間數列。由於變數的階次不同且階次均不大於 1 故而很適合採用 ARDL 分析。

表 3 各變數單根檢定值表

| 變數                         | 原始值                   |                        |                    | 一階差分                  |                        |                       |
|----------------------------|-----------------------|------------------------|--------------------|-----------------------|------------------------|-----------------------|
|                            | 有截距項                  | 有截距項<br>及趨勢            | 無截距項<br>及趨勢        | 有截距項                  | 有截距項<br>及趨勢            | 無截距項<br>及趨勢           |
| 總預算案<br>通過比率<br>/ALL       | -4.686***<br>(0.001)  | -4.936***<br>(0.0029)  | 0.3411<br>(0.774)  | -4.618***<br>(0.0015) | -4.47***<br>(0.0094)   | -4.724***<br>(0.0001) |
| 國防預算案<br>通過比率/D            | -2.82*<br>(0.0698)    | -2.752<br>(0.226)      | 0.0374<br>(0.6854) | -4.542***<br>(0.0017) | -4.425***<br>(0.0098)  | -4.659***<br>(0.0001) |
| 非國防預算案<br>通過比率/ND          | -4.803***<br>(0.0008) | 5.068***<br>(0.0021)   | 0.41587<br>(0.79)  | -5.92***<br>(0.0001)  | -5.786***<br>(0.0005)  | -6.03***<br>(0.000)   |
| 法定預算總金額<br>自然對數<br>/SBLN   | -2.201<br>(0.2106)    | -12.418***<br>(0.0000) | 1.3331<br>(0.9495) | -2.569<br>(0.1147)    | -3.9674**<br>(0.0261)  | -3.257***<br>(0.0024) |
| 國防法定預算<br>自然對數<br>/DSBLN   | -2.871*<br>(0.0631)   | -3.7368**<br>(0.0383)  | 0.4335<br>(0.8001) | -6.4255***<br>(0.000) | -5.200***<br>(0.0028)  | -6.4858***<br>(0.000) |
| 非國防法定預算<br>自然對數<br>/NDSBLN | -2.167<br>(0.222)     | -11.813***<br>(0.0000) | 1.4034<br>(0.9555) | -3.561**<br>(0.0157)  | -3.902**<br>(0.0297)   | -3.105***<br>(0.0035) |
| 執政黨在立法院<br>席次占比/RP         | -1.569<br>(0.482)     | -1.71<br>(0.7122)      | -0.386<br>(0.5343) | -4.887***<br>(0.0007) | -4.967***<br>(0.0029)  | -4.985***<br>(0.000)  |
| 國民所得毛額<br>/GNI             | 1.461<br>(0.998)      | -1.902<br>(0.6206)     | 3.665<br>(0.9997)  | -4.811***<br>(0.0009) | -5.5472***<br>(0.0009) | -1.427<br>(0.139)     |
| 我國立法委員<br>選舉年度/LEY         | 虛擬變數所以不做單根檢定          |                        |                    |                       |                        |                       |

註：\*、\*\*、\*\*\*分別表示在 10%、5%及 1%的顯著水準下，拒絕虛無假設。( ) 內為機率值

#### 4.3 ARDL Bound Test 共整合檢定法

本研究以 Pesaran et al. (2001) 提出的 ARDL 邊界檢定法 (Bound Test) 實施共整合檢定來檢測是否有長期均衡關係。邊界共整合檢定法的虛無假設為無長期均衡關係存在。如果計算出的 F 檢驗值落在上界值以上，代表拒絕無長期均衡關係的虛無假設；亦即接受變數間有長期均衡關係。

由於後續的 ARDL 模式的樣本數及變數個數相同，每個模式的 Bound Test 的  $I(0)$  的 10% 上界臨界值均為 3.17，故個別模式的 F 檢驗值大於 3.17 時即代表拒絕虛無假設，亦即自變數與應變數存在長期均衡關係。總預算案通過比率檢定結果的 F 檢驗值為 17.11，國防預算案通過比率檢定結果的 F 檢驗值為 3.37，非國防預算案通過比率檢定結果的 F 檢驗值為 12.53，法定預算總金額取自然對數檢定結果的 F 檢驗值為 2.693，國防法定預算取自然對數檢定結果的 F 檢驗值為 4.25，非國防法定預算取自然對數檢定結果的 F 檢驗值為 2.37。

綜合上述，法定預算總金額取自然對數及非國防法定預算取自然對數與模式的自變數（政治因素）無長期均衡關係，故後續本研究只針對總預算案通過比率、國防預算案通過比率、非國防預算案通過比率及國防法定預算取自然對數為應變數時進行後續的 ARDL 模式分析。

### 4.4 ARDL 模型估計結果

由上節的邊界檢測（Bound Test）所得出的結果，我們發現總預算案通過比率、國防預算案通過比率、非國防預算案通過比率、國防法定預算取自然對數與執政黨在立法院席次占比、國民所得毛額及我國立法委員選舉年度存在長期均衡關係。後續並一一以 ARDL 模型進行分析。

總預算案通過比率 ARDL 模型的部分，根據 AIC 值選擇出最佳模型為 ARDL(1,2,2)；此代表應變數總預算案通過比率取前一期時間落差項，執政黨在立法院席次占比及國民所得均取前兩期時間落差項，估計結果整理如表 4。由表 4 調整後 R 平方值為 0.5229，顯示具有解釋能力，F 值為 4.1512，P 值為 0.0085，在顯著水準 1% 下代表模式整體具有解釋能力。在顯著水準 10% 下，顯著影響總預算案通過比率有前一期執政黨在立法院席次占比、前二期執政黨在立法院席次占比、當期國民所得毛額、前兩期國民所得毛額及我國立法委員選舉年度。由於前一期執政黨在立法院席次占比為正向影響及前二期執政黨在立法院席次占比為負向影響，加總前一期執政黨在立法院席次占比及前二期執政黨在立法院席次占比對總預算案通過比率係數值（0.052-0.037），得出 0.015 其總和值高於零；亦即執政黨在立法院席次占比在長期上與總預算案通過比率有正向關係，針對總和係數值 0.015 進行合計數值的 Wald test 其 p 值為 0.42 未達 10% 顯著。故而執政黨在立法院席次占比對於總預算通過比率無顯著影響。

當期國民所得毛額及前兩期國民所得毛額對於對總預算案通過比率的係數值加總接近於零，以加總值進行 Wald test 也未達 10% 顯著水準；亦即國民所得毛額在長期上與總預算案通過比率沒有相關性。立法委員選舉年度係數是 0.007716，在顯著水準 10% 下，呈現正向顯著效果。

綜合上述，只有立委選舉年度對總預算案通過比率有顯著正面影響。此與政治預算循環一致，預算會受選舉因素的影響。我國  $t+1$  年的政府預算在  $t$  年時審定。我國的立委選舉常見的現象是立委會不斷的在其政見上顯示其為民眾爭取了那些政府預算，為了在選舉當年能有更吸引選民的政績，在選舉前一年審查次年預算時會較寬鬆以有利於其次年度的選舉，故而造成只要是選舉那年的總預算案通過比率較高。

表 4 總預算案通過比率 ARDL 模型估計結果表

| 變數                     | 變數係數值     | 標準差                | P 值      |
|------------------------|-----------|--------------------|----------|
| 前 1 期總預算案通過比率 ALL (-1) | -0.187773 | 0.171276           | 0.2902   |
| 執政黨席次比率 RP             | 0.015439  | 0.017835           | 0.4003   |
| 前 1 期執政黨席次比率 RP (-1)   | 0.052435  | 0.022889           | 0.0369** |
| 前 2 期執政黨席次比率 RP (-2)   | -0.036978 | 0.016787           | 0.0437** |
| 國民所得毛額 GNI             | 3.26E-06  | 1.61E-06           | 0.0616*  |
| 前 1 期國民所得毛額 GNI (-1)   | 6.75E-07  | 2.11E-06           | 0.7538   |
| 前 2 期國民所得毛額 GNI (-2)   | -3.94E-06 | 1.51E-06           | 0.0199** |
| 選舉年虛擬 LEY              | 0.007716  | 0.003207           | 0.0295** |
| 截距項                    | 1.147384  | 0.164581           | 0.0000   |
| R-squared              | 0.688862  | F-statistic        | 4.151264 |
| Adjusted R-squared     | 0.522922  | Prob (F-statistic) | 0.008548 |

註：\*、\*\*、\*\*\*分別表示在 10%、5%及 1%的顯著水準

國防預算案通過比率 ARDL 模型的部分如表 5。根據 AIC 值選擇出最佳模型為 ARDL (1,3,2)，此代表應變數總預算案通過比率取前一期時間落差項，執政黨在立法院席次占比取前三期時間落差項及國民所得均取前兩期時間落差項，估計結果整理如表 5。由表 5 調整後 R 平方值為 0.615，顯示具有解釋能力，F 值為 4.909，P 值為 0.0051，在顯著水準 1%下代表模式整體具有解釋能力。在顯著水準 10%下，顯著影響總預算案通過比率有前一期國防預算通過比率、當期執政黨在立法院席次占比、前三期執政黨在立法院席次占比、當期國民所得毛額、前一期國民所得毛額、前兩期國民所得毛額及我國立法委員選舉年度。

前一期國防預算通過比率顯著正向影響當期國防預算通過比率，此代表立法院在審查國防預算考量國防的持續性。當期執政黨在立法院席次占比及前三期執政黨在立法院席次占比均對於國防預算案通過比率為顯著正相關。加總當期執政黨在立法院席次占比及前三期執政黨在立法院席次占比對國防預算案通過比率的係數值，其總和值大於零；進行合計數值的 Wald test 其 p 值為 0.009 達 1%顯著；亦即執政黨在立法院席次占比在長期上與國防預算案通過比率有顯著的正向關係。

加總當期國民所得毛額、前一期國民所得毛額及前兩期國民所得毛額對於對總預算案通過比率的係數值，其總計數接近於零，合計數值的 Wald test 其 p 值為 0.197 未達 10%顯著亦即國民所得毛額在長期上與國防預算案通過比率沒有相關性。

我國立法委員選舉年度對國防預算案通過比率部分，當期立法委員選舉年度係數是 0.01609。估計結果於 1%顯著水準之下，呈現正向顯著效果且此值大於選舉年度對總預算通過比率係數值 0.007716。這個特性可能來自於全民都很關切國家安全，造成國防預算案通過比率的係數值較高。

表 5 國防預算案通過比率 ARDL 模型估計結果表

| 變數                   | 變數係數值     | 標準差                | P 值       |
|----------------------|-----------|--------------------|-----------|
| 1 期國防預算案通過比率 D (-1)  | 0.714097  | 0.195417           | 0.0029*** |
| 執政黨席次比率 RP           | 0.072510  | 0.030599           | 0.0340**  |
| 前 1 期執政黨席次比率 RP (-1) | -0.014576 | 0.036270           | 0.6943    |
| 前 2 期執政黨席次比率 RP (-2) | -0.024238 | 0.034092           | 0.4897    |
| 前 3 期執政黨席次比率 RP (-3) | 0.047622  | 0.026134           | 0.0915*   |
| 國民所得毛額 GNI           | 5.26E-06  | 2.42E-06           | 0.0490**  |
| 前 1 期國民所得毛額 GNI (-1) | -1.04E-05 | 3.35E-06           | 0.0082*** |
| 前 2 期國民所得毛額 GNI (-2) | 4.35E-06  | 2.30E-06           | 0.0816*   |
| 選舉年虛擬 LEY            | 0.016096  | 0.004798           | 0.0052*** |
| 截距項                  | 0.247484  | 0.189981           | 0.2153    |
| R-squared            | 0.772661  | F-statistic        | 4.909256  |
| Adjusted R-squared   | 0.615272  | Prob (F-statistic) | 0.005116  |

註：\*、\*\*、\*\*\*分別表示在 10%、5%及 1%的顯著水準

非國防預算案通過比率 ARDL 模型的部分，根據 AIC 值選擇出最佳模型為 ARDL (1,2,3)，估計結果整理如表 6，調整後 R 平方值為 0.479，顯示具有解釋能力，F 值為 3.252，P 值為 0.0267，在顯著水準 1%下代表模式整體具有解釋能力。在顯著水準 10%下，顯著影響非國防預算案通過比率有前一期執政黨在立法院席次占比、前兩期執政黨在立法院席次占比及當期國民所得毛額。加總前一期執政黨在立法院席次占比係數值及前兩期執政黨在立法院席次占比係數值對非國防預算案通過比率的係數值，其總和值小於零；合計數值的 Wald test 其 p 值為 0.74 未達 10%顯著亦即無相關。

表 6 非國防預算案通過比率 ARDL 模型估計結果表

| 變數                    | 變動率係數     | 標準差                | P 值      |
|-----------------------|-----------|--------------------|----------|
| 前 1 期非國防預算通過率 ND (-1) | -0.303827 | 0.223936           | 0.1980   |
| 執政黨席次比率 RP            | 0.033905  | 0.025661           | 0.2092   |
| 前 1 期執政黨席次比率 RP (-1)  | 0.055599  | 0.028941           | 0.0769*  |
| 前 2 期執政黨席次比率 RP (-2)  | -0.063128 | 0.023047           | 0.0169** |
| 國民所得毛額 GNI            | 4.51E-06  | 2.25E-06           | 0.0669*  |
| 前 1 期國民所得毛額 GNI (-1)  | 1.35E-06  | 2.74E-06           | 0.6291   |
| 前 2 期國民所得毛額 GNI (-2)  | -2.52E-06 | 2.79E-06           | 0.3820   |
| 前 3 期國民所得毛額 GNI (-3)  | -3.51E-06 | 2.94E-06           | 0.2536   |
| 選舉年虛擬 LEY             | 0.006926  | 0.004188           | 0.1221   |
| 截距項                   | 1.263145  | 0.215828           | 0.0001   |
| R-squared             | 0.692442  | F-statistic        | 3.252053 |
| Adjusted R-squared    | 0.479518  | Prob (F-statistic) | 0.026728 |

註：\*、\*\*、\*\*\*分別表示在 10%、5%及 1%的顯著水準

當期國民所得毛額對於對非國防預算案通過比率有顯著正相關性。這可能顯現非國防預算只有在國家經濟能力較高才會有所增加。我國立法委員選舉年度對非國防預算案通過比率部分，檢定結果不顯著。

綜合上述表 4、表 5 及表 6，總預算案通過比率與國防預算案通過比率與執政黨在立法院席次占比有正向相關性，非國防預算案通過比率與執政黨在立法院席次占有負向無關。此與 Portrafke (2011)、Hankla (2013)、Hanusch and Magleby (2014) 及傅澤偉、李政翰、林曼莉 (2016) 研究發現一致，立法機構的特性影響預算的編列及預算內容。執政黨在預算審查上在意的是其偏好的政策是否能夠解由預算通過來執行。國防預算相較於非國防預算是執政黨較關心的議題。選舉年度會影響總預算及國防預算的通過率，此與政治預算循環的基本觀點一致。相較於總預算案通過比率，選舉年度國防預算案通過比率的影響係數更高。

有趣的是非國防預算案通過比率與執政黨在立法院席次占及選舉年度無關。相較於國防預算案通過比率與兩者均為顯著正相關及預算有相互排擠的特性，非國防預算似乎是受到國防預算的排擠。國民所得對於非國防預算案通過比率有顯著正向關係，這代表所得較高的年度政府才較有餘力去滿足非國防預算。非國防預算案通過比率在選舉年度不顯著，非國防預算案並不存在選舉循環的論點；這可能是政府預算有限之情況，除了國防預算以外不可能面面俱到的提升所有的預算。在我國立法院，不論是中國國民黨或民主進步黨是執政政黨對於國防預算的優先性應該是高於非國防預算。

國防法定預算取自然對數 ARDL 模型的部分，根據 AIC 值選擇出最佳模型為 ARDL (1,0,0)，估計結果整理如表 7，調整後 R 平方值為 0.3701，顯示具有解釋能力，F 值為 4.525，p 值為 0.00912，在顯著水準 1% 下代表模式整體具有解釋能力。在顯著水準 10% 下只有當期執政黨在立法院席次占比呈現正向顯著效果。執政黨在立法院席次占越高越有利於取得國防法定預算。

表 7 國防法定預算值取自然對數 ARDL 模型估計結果表

| 變數                 | 變動率係數     | 標準差                | P 值      |
|--------------------|-----------|--------------------|----------|
| 前期國防法定預算值          | 0.134257  | 0.200230           | 0.5102   |
| 執政黨席次比率 RP         | 0.407683  | 0.207028           | 0.0629*  |
| 國民所得毛額 GNI         | 7.27E-06  | 5.56E-06           | 0.2058   |
| 選舉年虛擬              | -0.010369 | 0.044022           | 0.8162   |
| 截距項                | 16.52972  | 3.835014           | 0.0003   |
| R-squared          | 0.475109  | F-statistic        | 4.525782 |
| Adjusted R-squared | 0.370130  | Prob (F-statistic) | 0.009129 |

註：\*、\*\*、\*\*\*分別表示在 10%、5%及 1%的顯著水準

## 伍、結論

政府的政策必須藉由預算來實踐，故而編列預算且能順利通過立院審查成為法定預算是個重要課題。本研究以民國 83 年至 108 年期間的資料，藉由學理上的整理，探討政治因素及經濟因素對於我國預算案通過比率及法定預算總金額取自然的影響。

以執政黨在立法院席次占比、我國立法委員選舉年度及國民所得毛額作為自變數以我國三種預算案通過比率及預算金額為被解釋變數採取單根檢定確定數列的階次並採用適合不同階次特性的 ARDL 分析。

根據 ARDL Bound test 的結果，只針對有長期均衡關係的模式進行分析，包括總預算案通過比率、國防預算案通過比率及非國防預算案通過比率及國防法定預算取自然對數為應變數的 ARDL 分析。實證結果顯示：（1）在顯著水準 10% 下，立法委員選舉年度呈現正向顯著總預算案通過比率。執政黨在立法院席次占比正向影響總預算案通過比率。（2）在顯著水準 10% 下，執政黨在立法院席次占比及我國立法委員選舉年度對國防預算案通過比率有顯著正向效果且我國立法委員選舉年度對國防預算案通過比率的影響大於選舉年度對總預算通過比率的影響。（3）非國防預算案通過比率與執政黨在立法院席次占比在長期上有負向關係，當期國民所得毛額對於對非國防預算案通過比率有顯著正相關性。立法委員選舉年度對非國防預算案通過比率沒有顯著相關。（4）國防法定預算取自然對數 ARDL 模型的部分只有當期執政黨在立法院席次占比呈現正向顯著效果。

比較非國防預算案通過比率與執政黨在立法院席次占比無關，而國防預算案通過比率及國防法定預算金額與執政黨在立法院席次占比有長期正向影響。這代表強化國防能力是我國所有政黨執政時必須承擔的義務與責任。相較於非國防預算案通過比率與國民所得有關，而國防預算案通過比率及國防法定預算金額與國民所得無關。這顯示只有政府有較寬裕的財政能力時才會增加非國防預算，國防預算是既定政策，不論財政能力為何，政府會鼎力支援。選舉年度對於總預算案通過比率增加尤其是國防預算案通過比率增加的影響最大，這可能是選舉時期更確保國防安全無虞的結果。

## 參考文獻

- 汪進揚，趙一鳴，2005。經濟發展與國防需求關係之研究，真理財經學報，12，23-52。
- 陳勳慧，葉正國，2010。國防預算影響因素之研究，國防管理學術暨實務研討會，235-249。
- 黃秀端，2003。少數政府在國會的困境，台灣政治學刊，7（2），3-49。
- 張阜民，楊浩忠，柯俊禎，陳建宏，2013。總體經濟因素對國防支出之影響-以台灣及南韓為例，財金論文叢刊，第18期，84-97。
- 湯國斌，2015。所得分配，執政黨派與社會福利支出，德明學報，39（1），27-39。
- 傅澤偉，李政翰，林曼莉，2016。日本政黨政治與國防預算及社會福利預算之關係，亞太經濟管理評論，19（2），87-116。
- 傅澤偉，蔡欣樺，2017。政府治理對國防預算之影響-亞太地區國家分析，商管科技季刊，18（2），175-198。
- 楊登隆，2010。國防預算配置與景氣循環相關之研究，佛光大學經濟系碩士論文。
- 劉秀秀，2015，臺灣中央政府總預算審議之影響因素：民國70年至102年度，台灣大學政治學系碩士論文。
- Artés, J. and Jurado, I., 2018. Government fragmentation and fiscal deficits: a regression discontinuity approach. *Public Choice*, 175(3-4), 367-391.
- Hankla, C. R., 2013. Fragmented Legislatures and the Budget: Analyzing Presidential Democracies. *Economics & Politics*, 25(2), 200-228.
- Hanusch, M. and Magleby, D. B., 2014. Popularity, polarization, and political budget cycles. *Public Choice*, 159(3-4), 457-467.
- Kauder, B. and Potrafke, N., 2016. The growth in military expenditure in Germany 1951–2011: did parties matter? *Defence and Peace Economics*, 27(4), 503-519.
- Klomp, J. and De Haan, J., 2013. Political budget cycles and election outcomes. *Public Choice*, 157(1-2), 245-267.
- Murdoch, J. C. and Sandler, T., 1982. A theoretical and empirical analysis of NATO. *Journal of Conflict Resolution*, 26(2), 237-263.
- Nordhaus, W. D., 1975. The political business cycle. *The Review of Economic Studies*, 42(2), 169-190.
- Nordhaus, W., Oneal, J. R. and Russett, B., 2012. The effects of the international security environment on national military expenditures: A multicountry study. *International Organization*, 66(03), 491-513.
- Oladotun, A. and Gumede, M., 2019. Determinant of South Africa's Military Expenditure. *Journal of International Economics*; 10(1), 68-82.
- Pesaran, M. H. and Shin, Y., 1998. An autoregressive distributed -lag modelling approach to Co-integration analysis. *Econometric Society Monographs*, 31, 371-413.
- Pesaran, M. H., Shin, Y. and Smith, R. J., 2001. Bounds testing approaches to the analysis of level relationships. *Journal of Applied Econometrics*, 16(3), 289-326.
- Potrafke, N., 2011. Does government ideology influence budget composition? Empirical evidence from OECD countries. *Economics of Governance*, 12(2), 101-134.
- Rogoff, K. and Sibert, A., 1988. Elections and macroeconomic policy cycles. *The Review of Economic Studies*, 55(1), 1-16.
- Sheikh, M. R. and Chaudhry, I. S., 2013. The determinants of defense expenditures in Pakistan and India: An ARDL bounds testing approach. *Pakistan Journal of Social Sciences*, 33(1), 199-215.

## 大數據治理評量模型與層級關鍵要素之實證研究

陳良駒<sup>1\*</sup> 余明崇<sup>2</sup>

<sup>1</sup>國防大學管理學院資訊管理學系

<sup>2</sup>國防部參謀本部情報參謀次長室

論文編號：NM-43-01-7

來稿 2022 年 2 月 26 日→第一次修訂 2022 年 3 月 3 日→第二次修訂 2022 年 4 月 1 日→

同意刊登 2022 年 6 月 22 日

### 摘要

資料治理係為數據時代組織管理的基礎，許多國際性機構都已從不同面向進行分析與探索。鑑於近年大數據技術的蓬勃發展，組織亟需面對資料治理相關議題，大數據治理的程序、結構及重要關鍵要素因而成為組織資訊管理的重要課題。然而，多數學者之研究僅聚焦於大數據治理概念探索、框架研提、因素識別、領域應用等議題，較缺乏以實證分析方法進行大數據治理模型與關鍵因素之探索。

本研究針對大數據治理相關研究，蒐集多樣化的學術文獻，彙整影響大數據治理的重要構面及要素。透過專家學者之意見調查，以修正式德菲法建構一套組織大數據治理模型，同時以層級分析法來篩選及計算各項影響構面及因素之權重，以瞭解組織面對大數據管理下的關鍵治理流程及重點。研究發現評估構面的重要性依序為安全、政策、組織、品質、標準、詮釋資料及資料生命週期；而評估模型中最為關鍵的三項要素分別為「資料安全」、「機敏資料與隱私」、「風險控管和危機處理」。本研究所建構之治理模型及關鍵要素可做為各級機關在大數據導入之參考。

**關鍵字：**資料治理、大數據治理、修正式德菲法、層級分析法

---

\*通訊作者：陳良駒 email: ndmchorse@gmail.com

## An Empirical Study on the Evaluation Model and Critical Factors of the Big Data Governance

Chen, Liang-Chu <sup>1\*</sup> Yu, Ming-Chung <sup>2</sup>

<sup>1</sup>Department of Information Management, National Defense University, *Taiwan, R.O.C.*

<sup>2</sup>Office of the Deputy Chief of the General Staff for Intelligence, *Taiwan, R.O.C.*

### Abstract

Data governance is the foundation of organizational management in the data age, and many international institutions have analyzed and explored it from different aspects. To view of the vigorous development of big data technology in recent years, the organizations need to face the data governance-related issues; the procedure, structure and critical factors of big data governance have thus become an essential topic of organizational information management. However, most big data governance studies only focus on the concept exploration, framework suggestion, factor identification, and specified field application. To the best of our knowledge, they lack the study of big data governance models and key factors by using empirical analysis methods.

For the related research on big data governance, this study collects a variety of academic literature, and summarizes the essential constructs and factors that affect big data governance. Through the opinion survey of experts and scholars, a big data governance model is constructed by using the modified Delphi technique as a framework to analyze in advanced. Then the method of Analytic Hierarchy Process is adopted to screen and calculate the weights of various impact constructs and factors, so as to understand the critical organizational governance processes and priorities under the big data management. This study found that the importance of evaluation constructs is security, policy, organization, quality, standards, metadata, and data life cycle; and the three most critical factors in the evaluation model are “data security”, “data privacy”, and “risk control, management and crisis handling”. The governance model and key factors constructed in this study can be regard as a reference when agencies have intended to implement big data governance.

**Keywords:** Data Governance, Big Data Governance, Modified Delphi Method, Analytic Hierarchy Process

---

\* Corresponding Author Email: ndmchorse@gmail.com

## 一、緒論

近年來，隨著新一代資訊技術和應用的興起，「大數據<sup>1</sup> (big data)」浪潮席捲全球。在現今資訊爆炸的社會環境下，已成為各行各業極熱門的議題。然而，各級政府機關均擁有許多集中或分散的資料庫以管理組織數據，但對於資料治理 (data governance) 的掌握卻非常困難，例如：機關資料的歸屬、資料的品質與更新週期、資料涵蓋的時空背景及範圍，以及機關內部的資料存取情形等。更重要的是，多數組織並不清楚單位內部資料是否符合該機構發展之目標，以致於單位資料的管理及治理無所依循。

資料治理係為資料管理的相應職責及決策權的分配 (Otto, 2011)，然鑑於近年大數據技術蓬勃發展，在大數據時代下的資料治理問題，卻因數據量遽增、數據型態多樣、數據處理即時等特性而應有不同面向之探討，因而對於大數據治理的程序及重要性相關研究則愈顯重要 (Soares, 2012; Mikalef and Krogstie, 2018; Al-Sai et al., 2020)。

Soares (2012) 認為大數據治理 (big data governance) 是廣義資訊治理 (information governance) 計畫的一部分，透過調整多種功能目標，制定與大數據有關的資料優化、隱私保護與資料價值的政策。因此，大數據治理是指管理組織的大量數據，並使用不同的分析工具以提供組織決策制定之參考 (Al-Badi et al., 2018)。大數據治理涉及組織資料週期的模式、組織結構、參與角色等互動的元素，因而形成大數據生態 (big data ecosystem) 的主要發展重點 (Shah et al., 2021)。Zorrilla and Yebenes (2022) 則認為大數據治理則被視為在工業 4.0 發展下，協助企業組織轉型的重要機制。相關學者已針對大數據治理的概念、要素及框架進行彙整與分析 (張紹華, 2016; 楊琳等, 2017; 鄭大慶等, 2017; Kim and Cho, 2017; Al-Badi et al., 2018; Zorrilla and Yebenes, 2022)，同時也有多位學者提出大數據治理在政府 (堯淦與夏志傑, 2020)、銀行 (李小慶, 2021)、衛生健康 (Li et al., 2019) 等不同領域的框架與應用。

然而，學者進行大數據治理相關研究時，主要聚焦於治理概念之探索、治理框架之研提或特定國家、學域治理應用之論述等議題，較缺乏以實證分析方法進行數據治理相關面向與因素之探索研究。因此，本研究目的係整理不同學者針對大數據治理之論述，建構並發展大數據治理模型，同時透過專家學者之意見調查，以修正式德菲法 (Modified Delphi) 及層級分析法 (Analytic Hierarchy Process, AHP) 來篩選並計算出各項執行構面及關鍵考量因素之權重，以瞭解組織大數據治理運作模型中各面向與因素的重要程度，提供未來相關部門後續推展大數據治理、資源運用及關注重點之執行參據。

---

<sup>1</sup> 本研究為顧及內容的順暢性，同時配合讀者的認知及文意的情境，「數據」及「資料」兩個具相同原文的名詞將會配合術語意涵交互使用，以達成讀者對文章的理解度。

## 二、文獻探討

### 2.1 資料治理

近年來，各級機關與企業組織在數位化及智慧化的科技發展下，開始推動資訊系統與資料應用等各項治理工作。一般來說，組織只要有存取資料的需求，就存在資料治理的問題，在許多研究中均認為資料治理是資料管理中相當最重要的一環，因此資料治理雖非屬新議題，但已成為組織內部相當重要之角色。

Otto (2011) 認為，資料治理是指在企業中，資料管理的相應職責和決策權的分配。資料治理重點是針對不同來源的實際資料元素進行研究，許多資料研究機構或組織針對企業資料資產、資料管理等角度對資料治理進行過定義，而資料治理執行多透過資料治理委員會或其他組織機構來推展；然而形成資料治理決策過程，就是將各項模式化管理方式具體實現（張宇杰等，2018）。

資料治理係為大數據時代治理的基礎，已有許多組織及機構從不同方面進行定義。國際標準化組織（International Organization for Standardization, ISO）提出了資訊技術治理的通用模型和方法論，並認為該模型同樣適用於資料治理領域。在資料治理規範相關的 ISO/IEC38500 標準中，闡述了基於原則驅動的資料治理方法論，提出透過評估現在和未來的資料利用、指導資料治理準備及實施、監督資料治理實施的適切性等（ISO, 2008）。資料管理協會（Data Management Association, DAMA）將資料治理視為資料管理的核心功能。DAMA 提出了目標和原則、活動、主要交付物、角色和職責、技術、實踐和方法、組織和文化等 7 個資料治理的環境要素，做為資料治理的核心（DAMA, 2008）。

國際資料治理協會（The Data Governance Institute, DGI）強調資料治理為組織依據規則對治理範圍進行實施的過程，從「規則和參與規則」、「人及組織」以及「流程」3 個層面，創新提出 DGI 資料治理框架（DGI, 2009）；該框架展示 10 個關鍵要素間的邏輯關係，形成一個從方法到實施的完整系統。IBM 資料治理委員會（IBM DG Council）將資料特徵與實踐相結合，提出資料治理的元素模型，分為支持域，核心領域，貢獻因子及結果 4 個層次（IBM, 2012）。國際電腦稽核協會（Information Systems Audit and Control Association, ISACA）認為資料治理是 IT 治理的重要組成部分和關鍵因素，並視為過程控制的原則驅動方法；資料系統和資訊控制目標（control objectives for information）是基於由上而下原則的 IT 治理和管理框架，也涵蓋資料治理的關鍵領域，例如：利益相關者、影響因素、治理和管理對象等（ISACA, 2012）。

### 2.2 大數據治理

大數據可以說是新世代資訊技術革命與經濟社會發展融合下的產物，已經融入現代社會的許多角落，其與雲端技術及物聯網等技術相互結合，正快速的改變人類的生活方式。一般來說，大數據具有量大（volume）、多樣（variety）、快速（velocity）及準確（veracity）等特性（Lugmayr et al., 2017），政府治理單位可透過大數據分析提高管理效率，企業組織也可以藉由大數據技術彙總產業情報，進而提供消費者需求的

產品（傅文成，2018）。Kitchin（2014）整合 Hey et al.（2009）對於科學研究發展的觀點，批判資料驅動（data-driven）的數據研究是否對於理論終結造成影響，進而形成新世紀的研究典範。Abbasi et al.（2016）藉由觀察大數據的特徵，探索組織資訊價值鏈及資訊系統在行為、設計與經濟等面向的機會和可能挑戰，進而認為大數據的發展將對研究理論與方法產生新型態的影響。許多跨領域學者因而進行大數據分析之綜合性研討（Hashem et al., 2015; Ahmad et al., 2020）及特定議題之應用性探索，包括交通運輸（Ghofrani et al., 2018）、衛生保健（Dash et al., 2019）及財務分析（Hasan et al., 2020）等。

Soares（2012）認為大數據治理將成為公共部門未來的前沿問題，因而對於政府機構具有極大的挑戰；Al-Sai et al.（2020）揭示資料治理問題是大數據分析是否成功的關鍵要素，其議題涵蓋組織或其他利益相關者所開展的社會活動、過程、實施及政策；Zorrilla and Yebenes（2022）更認為數據將成為工業 4.0 環境下的關鍵資產，數據治理被視為協助企業轉型的重要機制。而隨著網路的蓬勃發展和廣泛應用，資訊公開、資料共用及資料開放已成為世界各國認證的發展趨勢，為強化不同領域的大數據治理任務，各國資訊與電子主管部門均相繼提出多項大數據治理政策，多位跨領域的學者也針對大數據治理的多項議題進行研究。

翟云（2018）建議以資料管理為基礎，構建大數據治理的價值模型；該學者認為大數據治理適合以全方位的任務分解及實施部署來進行，包括統籌協調、網路建設、資訊共用、業務應用、安全保密、標準規範、法律法規和績效考核等領域。傅文成（2018）從社會信用評級系統的觀點來解析中國大陸在數據時代的資料治理特性。王俊等（2021）認為以技術為導向的大數據治理包括資料規範、資料清洗、資料交換、資料整合等不同面向的體系結構，其中資料規範主要在強調資料編碼及格式的標準化；資料清洗負責處理資料缺漏、雜訊刪除及數據不一致的問題；資料交換係解決來源模式到目標模式的資料處理；資料整合則可協調多重數據來源的匹配問題。張宇杰等（2018）綜整國外大數據治理相關研究，呈現出多元化的治理原則和法律規範、多維度的治理框架／方法／活動及多行業的治理功能應用等特點；而大數據治理實踐則包括資料治理策略／方法、大數據應用的人員／技術／流程、大數據領域業務管理、大數據價值案例、大數據專案評量指標、資料治理政策／標準與資料集等面向。

學者張紹華等（2016）認為釐訂關鍵性領域、識別資料利益相關角色及建立大數據治理決策機制等體系框架构建之任務，是保證決策效能，進而實現大數據價值的最大化的重要方向。楊琳等（2017）從大數據應用和創新的視角提出資料治理的框架，該框架包括治理目標、治理保障、治理域、治理方法論四個部分，全面展現大數據治理的總體框架和內容，以全域視角描述大數據治理的所涉及的各個方面。例如：在治理域方面，即包括（1）戰略、組織、架構。（2）詮釋資料管理、主資料管理。（3）資料生命週期管理。（4）資料品質管理。（5）資料安全與合規。（6）資料應用與服務創新等六項重要的要素。Kim and Cho（2017）認為資料治理應該實現大數據服務的目標是通過一種新的分析方法來獲取含義並創建數據值；該作者從數據治理策略層級律定個人資訊保護、數據品質等級與數據披露／責任三項要素，從數據治理組件中擷

取組織、標準化和指導方針、政策和流程三項任務，並從審計和控制的角度的角度，認為應該著重於數據蒐集、數據處理、數據分析及數據可視化等各流程之確保。

Shah et al. (2021) 彙整近 25 年的 76 種資料生命週期 (data life cycle) 模型，並與國際資料管理協會 DAMA 提出的 DM-BOK 標準進行比對，提出適用於政府組織的資料管理框架，其中數據治理即為資料驅動政府的核心任務，相關研究也逐步受到重視。Al-Badi et al. (2018) 認為大數據治理框架之研究，有助於企業組織在數據科技時代中建立參考模型。因此彙整各學者或機構提議的大數據治理框架特性及其不足之處進行研討，同時提出一個新的應用框架。該框架包括識別組織結構、識別利益相關者、識別大數據的範圍、制定政策和標準、優化和計算、測量和監控品質、儲存數據、通信和管理數據；同時使用七項核心原則做為大數據治理之指引，包括組織 (organization)、元數據 (metadata)、隱私 (privacy)、數據品質 (data quality)、業務流程整合 (business process integration)、主數據整合 (master data integration) 和資訊生命週期管理 (information lifecycle management)。Zorrilla and Yebenes (2022) 更進一步介紹在工業 4.0 環境下，因應大數據密集、雲端運算和邊緣計算、人工智慧等科技之發展，不同國際標準組織提出數據治理系統的參考框架、滿足要件及實施範例。而亦有多位學者已從不同應用領域來探討大數據治理架構，包括衛生健康 (Li et al., 2019)、政府機構 (堯淦與夏志傑, 2020)、金融銀行 (李小慶, 2021) 等，相關要素或準則均可提供其他研究學者之參照。

綜整上述多位學者之大數據治理相關研究，發現研究重心僅聚焦於治理基礎概念之探索、治理框架及要素之研提、治理技術之運用，以及特定國家、學域治理之應用等論述，針對大數據治理框架或模型則鮮少有學者以實證性方法進行驗證研究。

### 三、研究架構與方法

#### 3.1 研究架構

本研究透過文獻探討大數據治理應考量之構面與因素，參考以往學者建立資料治理考量，匯整大數據治理建構評量因素初步資料，再透過修正式德菲法徵詢並取得專家共識，接續利用專家實務並以層級分析法方式，找出各因素權重比例關係，最後依據因素權重進行排序，探討大數據治理各構面及因素之重要性，研究流程如圖 1 所示。

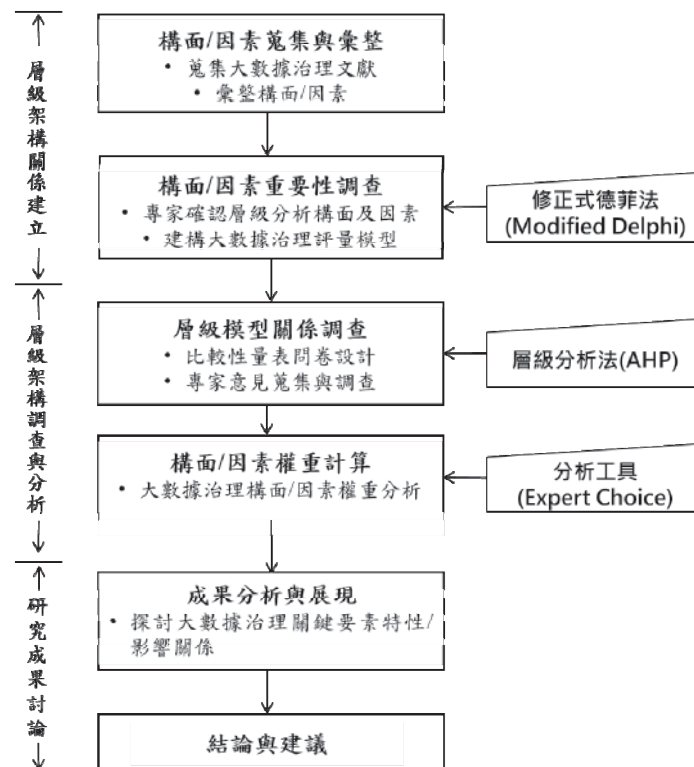


圖 1 研究流程

其中包括層級架構關係建立、層級架構調查與分析、研究成果討論三大階段，以及涵蓋構面／因素蒐集與彙整、構面／因素重要性調查、層級模型關係、構面／因素權重計算、成果分析與展現、結論與建議六大步驟，分別敘述如後。

### 3.2 研究方法

#### 3.2.1 層級架構關係建立

##### 3.2.1.1 構面／因素蒐集與彙整

本研究參酌多位研究學者所提出之大數據治理框架建議，透過彙整規則及小組研討方式進行影響構面及關鍵要素之整合。表 1 係以不同學者提出的構面元素為例進行彙整，本研究擷取至少三位作者認可之共同因素做為大數據治理評估之參考構面。其中主資料管理構面雖有三位學者納入框架設計要素，但部分學者將該構面視為數據標準化層面的治理，其可保障數據完整性及規範性（楊琳等，2017），故本研究參照此特性，並將主資料治理議題納入標準面之範疇；此外，部分文獻將政策與流程視為數據治理的整合元件（Panian, 2010; Kim and Cho, 2017），為簡化構面設計，本研究亦將流程整合納入政策面下的關鍵要素，將作業程序制訂視為大數據治理政策推展的重要基礎。經調修後的評量模型選擇組織、政策、標準、安全、品質、資料生命週期及元數據（metadata）七項構面要素，以利後續研究之推展。

表 1 大數據治理評量模型構面篩選機制與成果

| 項次                                                                 | 治理構面                 | 大數據治理原則與要素    |                       |                          |                  |               |
|--------------------------------------------------------------------|----------------------|---------------|-----------------------|--------------------------|------------------|---------------|
|                                                                    |                      | 楊琳等<br>(2017) | Kim and Cho<br>(2017) | Al-Badi et al.<br>(2018) | Panian<br>(2010) | 李小慶<br>(2021) |
| 1                                                                  | 組織面                  | ✓             | ✓                     | ✓                        | ✓                | ✓             |
| 2                                                                  | 政策面                  | ✓             | ✓                     |                          | ✓                | ✓             |
| 3                                                                  | 標準面                  |               | ✓                     |                          | ✓                | ✓             |
| 4                                                                  | 安全面                  | ✓             | ✓                     | ✓                        |                  | ✓             |
| 5                                                                  | 品質面                  | ✓             | ✓                     | ✓                        |                  | ✓             |
| 6                                                                  | 資料生命週期               | ✓             |                       | ✓                        |                  | ✓             |
| 7                                                                  | 元數據                  | ✓             |                       | ✓                        |                  | ✓             |
| 8                                                                  | 主資料管理 <sup>(*)</sup> | ✓             |                       | ✓                        |                  | ✓             |
| 9                                                                  | 流程整合                 |               |                       | ✓                        |                  |               |
| 10                                                                 | 架構                   | ✓             |                       |                          |                  | ✓             |
| 11                                                                 | 資料應用與服務創新            | ✓             |                       |                          |                  |               |
| 12                                                                 | 數據揭露及管理責任            |               | ✓                     |                          |                  |               |
| 13                                                                 | 工具                   |               |                       |                          |                  | ✓             |
| 註(*)：主資料管理係數據標準化層面的治理，保障數據完整性及規範性（楊琳等，2017），故本研究將主資料治理議題納入標準面進行探討。 |                      |               |                       |                          |                  |               |
| 備註：灰階部分為本研究最終採用之分析構面。                                              |                      |               |                       |                          |                  |               |

確認大數據治理評量模型之影響構面後，依循上述研討方式進行各面向的關鍵因素之蒐整與分析，分別在七大構面下納入 34 項關鍵因素，相關要素定義、內涵說明籍資料來源如表 2。

表 2 大數據治理評量模型構面／因素定義

| 目標        | 構面  | 關鍵因素     | 內涵說明                           | 資料來源                                                                                       |
|-----------|-----|----------|--------------------------------|--------------------------------------------------------------------------------------------|
| 大數據治理評量模型 | 組織面 | 組織建立     | 成立專屬組織，管制工作執行及任務推展             | Data Governance Institute (2009)；Panian (2010)；Kim and Cho (2017)；楊琳等 (2017)；堯淦與夏志傑 (2020) |
|           |     | 角色和責任    | 定義每個成員職務和應負之責任                 |                                                                                            |
|           |     | 培訓和教育    | 進行技術和作業流程面的教育和培訓               |                                                                                            |
|           |     | 組織變革管理   | 建立管理所需使用方法，並鼓勵成員改變組織方向         |                                                                                            |
|           | 政策面 | 任務和願景    | 確認任務目標及未來願景                    | Data Governance Institute (2009)；Kim and Cho (2017)；楊琳等 (2017)                             |
|           |     | 政策和程序    | 明確的政策及作業程序，期使所屬單位統一作法          |                                                                                            |
|           |     | 計畫和優先    | 針對資料建立整體規劃及律定執行優先順序            |                                                                                            |
|           | 標準面 | 標準與指導方針  | 訂定資料治理標準及指導方針，俾利單位遵循           | Kim and Cho (2017)；Panian (2010)；堯淦與夏志傑 (2020)；李小慶 (2021)                                  |
|           |     | 資料定義和分類  | 對資料建立及分類標準                     |                                                                                            |
|           |     | 主資料／參考資料 | 定義主資料，開發資料模型，以及實施與資料相關的開發和技術標準 |                                                                                            |
|           |     | 資料模式     | 資料模式標準建立                       |                                                                                            |
|           |     | 技術和工具標準  | 使用相關技術／工具來定義組織的標準數據模型          |                                                                                            |

## 大數據治理評量模型與層級關鍵要素之實證研究

| 目標 | 構面     | 關鍵因素     | 內涵說明                                | 資料來源                                                   |
|----|--------|----------|-------------------------------------|--------------------------------------------------------|
|    | 安全面    | 個人資料隱私   | 是否建立個人資料隱私保密機制                      | Kim and Cho (2017)；楊琳等 (2017)；Panian (2010)；李小慶 (2021) |
|    |        | 資料安全     | 訂定資料洩漏防範作為及責任歸屬                     |                                                        |
|    |        | 風險管控     | 針對資料洩漏建立風險評估及損害管控機制                 |                                                        |
|    |        | 資料內容變更管理 | 針對資料內容修改，建立權限管控機制                   |                                                        |
|    | 品質面    | 正確性      | 確保資料正確性                             | Kim and Cho (2017)；楊琳等 (2017)；Panian (2010)；李小慶 (2021) |
|    |        | 即時性      | 在符合預期使用的時間內獲取和處理資料                  |                                                        |
|    |        | 完整性      | 確保輸入資料庫的數據完整                        |                                                        |
|    |        | 可信賴性     | 資料庫的資料來源是值得信賴的                      |                                                        |
|    |        | 一致性      | 資料需要模組化、命名及根據組織標準來定義資料一致性           |                                                        |
|    |        | 可存取性     | 除了必要限制因素外，資料需要被隨時存取                 |                                                        |
|    |        | 資料有意義性   | 資料內容具有一定意涵                          |                                                        |
|    | 資料生命週期 | 定義規劃     | 制定資料應如何建立需求，包含誰應該在何時參與需求建立會議        | 鄭大慶等 (2017)；李小慶 (2021)                                 |
|    |        | 盤點評估     | 制定資料在取得前應如何得知內部或外部有無類似資料，以加速資料取得之程序 |                                                        |
|    |        | 資料蒐集     | 制定資料如何取得之程序，若需要自行建立，則須制訂資料集建置標準作業流程 |                                                        |
|    |        | 資料存取     | 制定資料建立後應置於何處供應及使用機制                 |                                                        |
|    |        | 維護       | 制定資料有誤差或錯誤之監測及管控程序                  |                                                        |
|    |        | 使用評估     | 制定資料是否為使用者所需之評估程序                   |                                                        |
|    |        | 歸檔       | 制定資料若已不為當下使用時，如何歸檔、版本管理以及後續取用之程序    |                                                        |
|    | 元數據    | 架構       | 屬於結構性的資料，可來自於不同來源                   | 鄭大慶等 (2017)；李小慶 (2021)                                 |
|    |        | 整合       | 同質性資料予以整合資料                         |                                                        |
|    |        | 控制       | 元數據的管理機制                            |                                                        |
|    |        | 交付       | 元數據的交付方式                            |                                                        |

### 3.2.1.2 構面／因素重要性調查

本研究初期階段採用修正式德菲法 (Modified Delphi Method) 做為層級構面與準則因素的篩選方法。修正式德菲法係由 Murry and Hammons (1995) 所提出，主要是以文獻蒐整及探討之方式確認研究問題的結構式問項，再藉由領域專家的審視及合議獲得共識意見，此方法較具實務的可操作性 (Hill and Fowles, 1975)。因修正式德菲法需要領域專家的評估，故調查對象的選擇係基於立意抽樣的特性來進行 (吳雅玲，2001)，篩選條件則聚焦於專家對於研究議題的認知深度、相關工作經驗、專業能力等面向 (Hill and Fowles, 1975)。

確認問卷及專家後，即透過調查流程邀請相關人員參與。因修正式德菲法需要取的專家的共識意見，故各級專家對於研究議題的判斷需具有一致性，否則應進行反覆式的問卷填答。而一致性的檢定機制係參照 Holden and Wedman (1993) 的建議，若有 85% 以上的題項達到高／中度的一致性，即視為意見趨於一致，完成本次問卷。

### 3.2.2 層級架構調查與分析

確認研究構面與準則因素後，本研究續採用層級分析法 (Analytic Hierarchy Process,

AHP) 來進行權重判斷之方法。層級分析法為 Thomas L. Saaty 教授於 1971 年所發展的方法，主要針對不確定情況下的多準則決策問題進行評估與分析。

依據楊欣哲等 (2015) 及陳良駒等 (2019) 學者針對 AHP 層級分析法的執行建議，本研究的問題界定及與層級架構之確認已透過前述各項方法與機制完成，其餘調查與分析之步驟說明如次：

### 3.2.2.1 層級模型關係調查

- (1) 問卷設計與調查：AHP 的評估是針對同一層級內的構面／準則進行兩兩比較，來計算構面／準則間的相對重要性。依據學者 Saaty 的建議，本研究採用九等尺度來進行調查，問卷需清楚描述每一成對比較的問題，並詳加解說，以利受訪者填答（範例及說明詳如表 3）。

表 3 AHP 成對比較問卷範例及尺度說明

資料來源：陳良駒等 (2019)

|      | 左邊比較重要 |      |      |      |      | 右邊比較重要 |      |      |      |      |
|------|--------|------|------|------|------|--------|------|------|------|------|
| 分析構面 | 重要絕對   | 重要極為 | 重要頗為 | 重要稍微 | 重要同等 | 重要稍微   | 重要頗為 | 重要極為 | 重要絕對 | 分析構面 |
|      | 9:1    | 7:1  | 5:1  | 3:1  | 1:1  | 1:3    | 1:5  | 1:7  | 1:9  |      |
| A    |        |      |      |      |      |        |      |      |      | B    |
| A    |        |      |      |      |      |        |      |      |      | C    |
| B    |        |      |      |      |      |        |      |      |      | C    |
| ...  |        |      |      |      |      |        |      |      |      | ...  |

註：AHP 評估尺度意義與說明

| 評估尺度    | 定義       | 說明               |
|---------|----------|------------------|
| 1       | 同等重要     | 兩準則的貢獻程度具同等重要性。  |
| 3       | 稍為重要     | 經驗與判斷稍微偏好某一準則。   |
| 5       | 頗為重要     | 經驗與判斷強烈偏好某一準則。   |
| 7       | 極為重要     | 實際顯示非常強烈偏好某一準則。  |
| 9       | 絕對重要     | 有足夠證據肯定絕對偏好某一準則。 |
| 2，4，6，8 | 相鄰尺度之中間值 | 介於兩種判斷之間。        |

- (2) 建立成對比較矩陣：依據前述步驟之調查數據建立成對比較正倒值矩陣如公式 (1)，其中  $a_{ij}$  為  $i$  準則與  $j$  準則比較的數值形成矩陣中對角線右上角，對角線左下角的數值恰為右上角數值的倒數，即  $a_{ji} = 1 / a_{ij}$ ，主對角線為準則自身比較，故數值為 1。當進行兩兩成對評比時，以全體之幾何平均數作為代表值。

$$A = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 1/a_{12} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/a_{1n} & 1/a_{2n} & \cdots & 1 \end{bmatrix} \quad (1)$$

- (3) 計算特徵向量與最大特徵值 ( $\lambda_{\max}$ )：本步驟可運用數值分析的特徵值 (eigen-value) 解法，求得比較矩陣之最大特徵值與對應之特徵向量。
- (4) 計算各層級一致性指標：學者 Saaty 認為需要就成對評比結果進行「一致性檢定」，以滿足成對數值的偏好關係與強度關係之遞移性等基本假設。一致性檢定包含一致性指數 (consistency index, C.I.) 及一致性比率 (consistency ratio, C.R.) 之計算，公式分別如 (2)、(3) 所示。其中，R.I. 稱為隨機指數 (random index)，是隨機產生之矩陣的一致性指數 (參照表 4)，R.I. 值與矩陣階數有關，可依據矩陣數查出對應之 R.I. 值。

$$C.I. = (\lambda_{\max} - n) / (n - 1) \quad (2)$$

$$C.R. = C.I. / R.I. \quad (3)$$

當 C.R. 值愈趨近於 0，表示一致性愈高，C.R. 值  $\leq 0.1$  為可容許的範圍，但若 C.R. 值  $> 0.1$  則表示評比結果不一致，則需要重新進行評比。

表 4 隨機指數值表

| 階數   | 1    | 2    | 3    | 4    | 5    | 6    | 7    | 8    | 9    | 10   |
|------|------|------|------|------|------|------|------|------|------|------|
| R.I. | 0.00 | 0.00 | 0.58 | 0.90 | 1.12 | 1.24 | 1.32 | 1.41 | 1.45 | 1.49 |

資料來源：Satty (1990)

### 3.2.2.2 構面／因素權重計算

本階段進行整體層級的權重計算與一致性檢定。各層級要素間的權重計算後，再進行整體層級的權重計算與一致性檢定 (Consistency Ratio of the Hierarchy, C.R.H.)。當整個層級結構通過一致性檢定後，即可進行替代方案的綜合評估，再利用加權平均法求取各替代方案的加權綜合評點，所算出的結果即代表個決策方案對應於決策目標的相對優先順序，便能決定最終目標的最佳決策方案，做為後續導入大數據治理資源分配參考。

### 3.2.3 研究成果討論

#### 3.2.3.1 成果分析與展現

藉由大數據治理各層級構面及關鍵因素之權重與排序關係，說明各項數值代表之意涵，同時透過全面性的彙算，從整體構面角度重新觀察不同要素的相對權重及排序關係，以提供組織做為後續導入大數據治理資源分配參考。

#### 3.2.3.2 結論與建議

依據研究成果，說明大數據治理的關鍵構面及要素之發展重點，並針對國防領域之應用進行闡述。

## 四、研究成果與分析

### 4.1 評量模型構面與因素確認

針對本研究文獻蒐集整理後的構面及關鍵因素，分別與專家群們對評選準則進行調查，以透過專家及學者的實務及研究經驗，確認在執行大數據治理時所應考量之構

面與因素。

#### 4.1.1 專家意見彙整及構面分析

本研究考量到專家團體之背景多元化、不同之理念或其社會地位，能加強研究的成效。邀請國內學術、研究、政府部門及產業界專家來進行修正式德菲法問卷調查，專家代表整理如表 5。關於專家問卷針對各構面風險適合度分析情況，分發問卷 12 份，實際回收 9 份，並完成各構面及關鍵因素評估指標統計，最後達成專家們對大數據治理評選準則的一致性意見後，確立本模式的準則。

表 5 受訪專家代表

| 編號 | 類別 | 單位               | 職稱  | 年資        |
|----|----|------------------|-----|-----------|
| 01 | 學者 | 政治大學電子治理研究中心     | 教授  | 21 至 30 年 |
| 02 | 學者 | 中原大學地理資訊系統研究中心   | 教授  | 21 至 30 年 |
| 03 | 學者 | 元智大學社會暨政策科學系     | 教授  | 11 至 20 年 |
| 04 | 學者 | 國防大學大數據中心        | 教授  | 11 至 20 年 |
| 05 | 業界 | 中華民國 App 跨界交流協會  | 理事長 | 21 至 30 年 |
| 06 | 政府 | 高雄市政府都市發展局資訊中心   | 主任  | 21 至 30 年 |
| 07 | 政府 | 衛生福利部桃園醫院資訊室     | 主任  | 11 至 20 年 |
| 08 | 政府 | 行政院環境保護署環境監測及資訊處 | 處長  | 21 至 30 年 |
| 09 | 政府 | 臺中市政府資訊中心        | 管理師 | 5 至 10 年  |

本研究參考的問卷作法以三等選項方式呈現，主要讓專家針對評選指標勾選是否「保留」、「刪除」與「修正」等意見之表達。專家意見彙整後，採下列準則進行調整：

1. 凡填答「保留」之相對次數統計達 85% 以上者，該構面／要素予以留用；若不足 85% 則納入合併或修正參考。
2. 未達 85% 且有 2 位以上專家建議「刪除」者，該構面／要素予以刪除；若未符合上述要件，則依據專家意見實施修訂。
3. 「修正」選項則視專家意見，透過專業研討適度納入合併或修正考量。

本研究在構面考量計提列「組織面」等 7 項治理構面，經調查回覆後專家僅有兩項建議。其中「資料生命週期」計有 1 位專家建議刪除，因未達刪除門檻（88.9% 同意保留），本構面予以保留；另「元數據」計有 1 位專家提及本術語在多個領域具不同之翻譯，建議可選擇較為普及的用語，或者加上英文原文來進行修正。

經作者蒐整網路資源後，發現國內以「詮釋資料」及「後設資料」兩項翻譯名詞較為學術界所使用；其中「詮釋資料」的代表性資源為國家教育研究院「雙語詞彙資料庫」，而「後設資料」的代表性網站為維基百科，本研究初步趨向以官方認證機構之國家教育研究院所翻譯的「詮釋資料」為修正後術語，因其較具有公信力。為確認此術語之使用頻率，本研究亦以 Google 及 Google 學術搜尋兩項工具進行關鍵字檢索，其中「詮釋資料」分別出現 1670,000 筆及 1,700 筆，而「後設資料」則分別出現 565,000

筆及 648 筆。綜整代表性資源及搜尋結果後，為使「元數據」構面意涵利於後續參考者易於理解，本研究擬修正為「詮釋資料」，同時增加英文名詞之註解與說明。

#### 4.1.2 層級構面之因素分析

1.組織面：計有「組織建立」、「角色和責任」、「培訓和教育」、「組織變革管理」4 項關鍵因素，專家回覆意見及處理說明如下：

- (1)「組織建立」因素僅有 1 位專家提出修正建議：「不需專屬組織，有相關委員會即可」。為明確因素意涵，該因素修訂為「建立專屬組織或委員會」。
- (2)「角色和責任」因素有 2 位專家建議修正術語及意涵為「責任與利害」。參酌專家意見並強化名詞定義，該因素予以修訂。
- (3)「培訓和教育」因素僅 1 位專家建議修正為「組織成員培訓和教育」，為明確律定培訓和教育對象，參酌專家意見修訂為「組織成員培訓和教育」。
- (4)「組織變革管理」所有專家同意保留，該因素維持。
- (5)此外，另有 1 位專家建議「增列和其他組織之資料、知識共享」，因其歸屬於資料處理之週期活動，因此納入「資料存取」因素中探討。

2.政策面：計「任務和願景」、「政策和程序」、「計畫和優序」3 項關鍵因素，專家回覆意見及處理說明如下：

- (1)「任務和願景」因素有 2 位專家提出意見，包括「宣示組織願景，不宜宣示任務導向」及「應加入短、中、長期願景」，故該因素修訂為「組織願景」。
- (2)「政策和程序」因素有 3 位專家提出類似修正建議，認為政策和程序兩者應視為不同之議題，且政策因素具制定大綱，指導方針之意涵，其重要程度較高，故該因素修正為「政策計畫」。
- (3)「計畫和優序」有 1 位專家建議刪除及 2 位建議修正，該因素予以刪除。
- (4)另有 2 位專家考量應用大數據時之績效評估問題，建議新增「政策績效評估」相關因素，為強化整體考量周延性，該因素予以增列。

3.標準面：計「標準與指導方針」、「資料定義和分類」、「主資料／參考資料」、「資料模式」、「技術和工具標準」5 項關鍵因素，專家回覆意見及處理說明如下：

- (1)「標準與指導方針」因素僅 1 位專家建議「應加上作業規範或程序，較為具體」，故該因素名稱修訂為「標準作業程序與指導方針」。
- (2)「資料定義和分類」所有專家同意保留，該因素維持。
- (3)「主資料／參考資料」及「資料模式」因素分別有 2 位及 4 位專家建議修訂，主要均著重於概念定義及說明內容之強化，故保留兩項因素之名稱，但於問卷名詞定義中強化解釋說明。
- (4)「技術和工具標準」因素有 1 位專家建議刪除，1 位專家建議新增資料交換、處理之協定因子，考量兩位專家意見，該因素修正為「協定與技術」。

4.安全面：計「個人資料隱私」、「資料安全」、「風險管控」、「資料內容變更管理」4 項關鍵因素，專家回覆意見及處理說明如下：

- (1) 「個人資料隱私」因素有 2 位專家建議修正，包括「新增敏感資料識別與標記，不應僅限定個資」及「應建立隱私保護機制」，考量兩位專家意見，該因素修正為「機敏資料與隱私」。
  - (2) 「資料安全」因素有 1 位專家認為資料安全的範圍及說明不夠清楚，故保留因素名稱，但強化因素意涵之說明。
  - (3) 「風險管控」因素有 1 位專家提出應同時考量危機處理事宜，故依專家建議修訂該因素為「風險管控和危機處理」。
  - (4) 「資料內容變更管理」因素有 2 位專家同時提出資料內容之存取及變更需要設定權限機制，參酌專家建議，本因素修正為「資料內容變更與權限管理」。
- 5.品質面：計提列「正確性」、「即時性」、「完整性」、「可信賴性」、「一致性」、「可存取性」、「資料有意義性」7 項關鍵因素，專家回覆意見及處理說明如下：
- (1) 「正確性」因素有 1 位專家建議明確資料正確之範疇，故該因素修正為「資料正確性」。
  - (2) 「完整性」所有專家同意保留，該因素維持。
  - (3) 「可信賴性」及「一致性」因素分別有 3 位專家建議整合，且為明確評量之對象，該因素合併並修訂為「資料一致性」。
  - (4) 「可存取性」因素 1 位專家建議併入「資料生命週期」構面的「存取」因素，本研究依循該專家之建議進行整併。
  - (5) 「即時性」、「資料有意義性」分別有 2 位專家建議刪除，該兩項因素予以刪除。
  - (6) 此外，另有專家建議增列「資料之可近性」、「資料獲得之成本」及「資料可比較性」等因素，其中「資料之可近性」與原提列「可存取性」共同併入「資料生命週期」構面「存取」因素說明；「資料獲得之成本」併入「政策面」構面「政策績效評估」因素；「資料可比較性」則併入「元數據」構面「控制」因素進行探討。
- 6.資料生命週期：計「定義規劃」、「盤點評估」、「資料蒐集」、「資料存取」、「維護」、「應用性評估」、「歸檔」7 項關鍵因素，專家回覆意見及處理說明如下：
- (1) 「盤點評估」、「資料蒐集」、「資料維護」、「應用性評估」等四項因素所有專家同意保留，該項因素維持。
  - (2) 「定義規劃」因素有 1 位專家建議刪除，1 位專家建議保留但加入定義規劃流程及工作內容等說明，故該因素擬進行名詞定義之強化說明。
  - (3) 「資料存取」因素如前所述，共有 3 位專家建議修訂。本研究整合「品質面」之相關說明，將「可存取性」及「資料之可近性」整併為「資料存取」。
  - (4) 「歸檔」因素所有專家同意保留，但因另有專家建議增列「資料刪除與應用性評估」因素，本研究參酌專家意見，將此因素名稱整併為「歸檔與刪除」。
- 7.元數據：依據前述意見修正為「詮釋資料」，其準則包括「架構」、「整合」、「控制」、「交付」4 項關鍵因素，專家回覆意見及處理說明如下：
- (1) 「整合」、「控制」、「交付」等因素所有專家同意保留，該項因素維持。

- (2)「架構」因素有 2 位專家提出建議，希望能強化定義數據架構的結構性系統之說明，故參酌專家意見保留因素名稱，但修訂名詞定義及說明。

#### 4.1.3 層級架構關係之建立

經過適合性評估後，原訂 7 個構面及 34 個關鍵因素，其中構面部分除元數據經專家建議修訂為「詮釋資料」且增加英文說明外，其他全數予以保留。關鍵因素部分，「計畫和優序」、「即時性」及「資料有意義性」等 3 項，依循專家議建予以刪除；「可信賴性」及「一致性」亦併同整合為「資料一致性」。其餘因素依據專家意見或保留，或修正名稱，或強化定義說明，經彙整後釐定計有 7 個構面與 30 個關鍵因素。調整後的結果經過第二階段的專家問卷調查，相關構面及因素均符合前述標準獲得保留。彙整後的分析層級架構如圖 2 所示。

#### 4.2 構面與因素權重計算及分析

本研究以修正式德菲法的調查為基礎，進行研修後研提大數據治理層級模型，接續依各構面及因素項目制訂成對比較問卷，進行第二階段的專家調查。此階段調查係以原修正式德菲法發放問卷之專家(9 位)為主，唯有 1 位委員並未於催繳期限內回覆，故最終實際回收之產官學研專家問卷計有 8 份，回收率 88.9%。接續使用 AHP 代表性的分析工具 Expert Choice 2000 來進行層級階層指標數值的彙算，以維持權重運算矩陣的一致性。

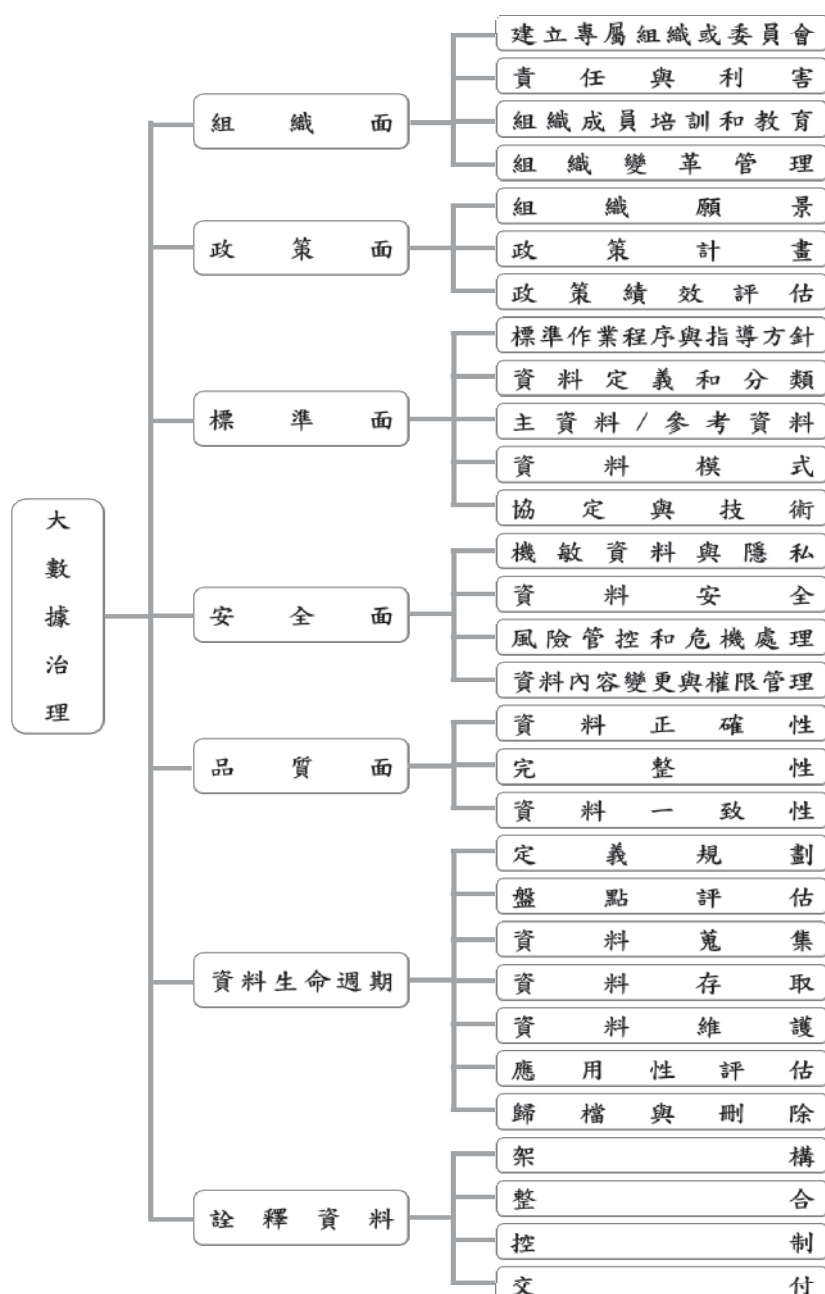


圖 2 層級架構

#### 4.2.1 主構面分析結果

專家問卷數據經軟體計算後，得出一致性比率  $C.R.=0.023 \leq 0.1$ ，表示問卷調查結果達一致性檢定標準；在大數據治理考量因素構面的重要性順序為：安全面（0.293）、政策面（0.163）、組織面（0.143）、品質面（0.141）、標準面（0.115）、詮釋資料（0.077）及資料生命週期（0.068），其評估分析成果詳如圖 3。由此可知，在大數據治理模式中，安全面影響最大，顯示日益複雜的數據環境下，各機構對於資料的安全特別關注；接著是政策面，說明組織在導入大數據治理活動需要有執行的願景及計畫；而組織面強調高階主管的支持來籌建專屬組織及鼓勵員工參與治理的訓練過程，也是很重要的機制。

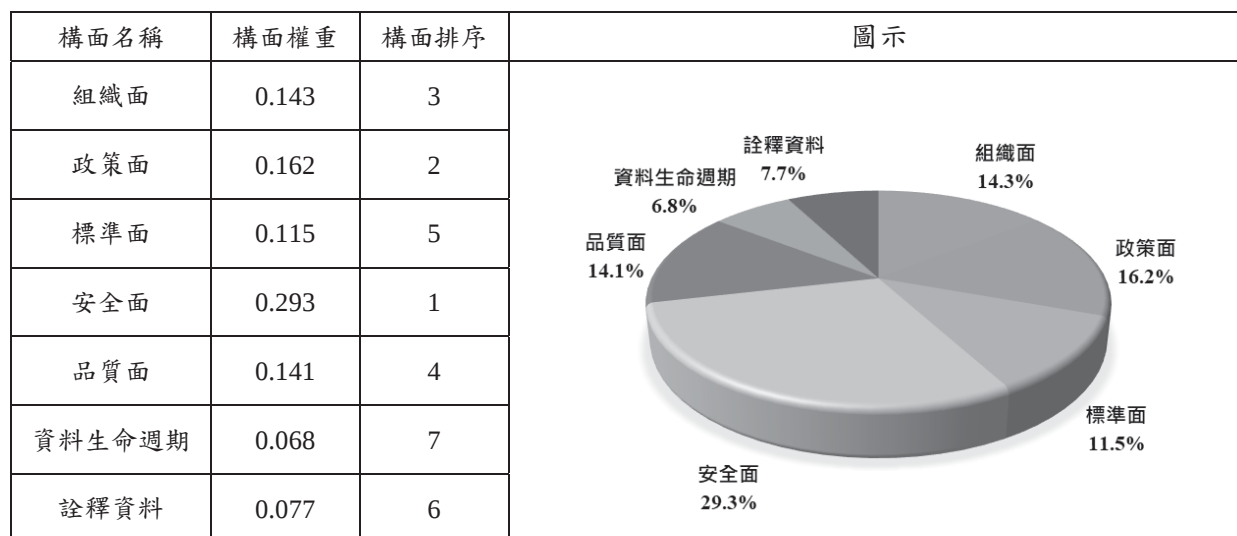


圖 3 大數據治理構面的重要性評估分析

#### 4.2.2 構面因素權重分析

本研究分別呈現個別構面中的因素權重及排序，以及跨構面的整體權重分析成果，相關說明如下：

- 1.組織面：包含 4 項關鍵成功因素 ( $C.R.=0.022 \leq 0.1$ )，達一致性檢定標準；其重要性順序為：建立專屬組織或委員會 (0.346)，責任與利害 (0.302)，組織變革管理 (0.199)、組織成員培訓和教育 (0.153)。
- 2.政策面：包含 3 項關鍵成功因素 ( $C.R.=0.002 \leq 0.1$ )，達一致性檢定標準；其重要性順序為：政策計畫 (0.391)，組織願景 (0.307)，政策績效評估 (0.302)。
- 3.標準面：包含 5 項關鍵成功因素 ( $C.R.=0.018 \leq 0.1$ )，達一致性檢定標準；其重要性順序為：標準作業程序與指導方針 (0.365)，資料定義和分類 (0.212)，資料模式及協定 (0.180)，主資料/參考資料 (0.685) 及協定與技術 (0.113)。
- 4.安全面：包含 4 項關鍵成功因素 ( $C.R.=0.022 \leq 0.1$ )，達一致性檢定標準；其重要性順序為：資料安全 (0.382)，機敏資料與隱私 (0.256)，風險管控和危機處理 (0.213)，資料內容變更與權限管理 (0.149)。
- 5.品質面：包含 3 項關鍵成功因素 ( $C.R.=0 \leq 0.1$ )，達一致性檢定標準；其重要性順序為：資料正確性 (0.607)，資料一致性 (0.207)，完整性 (0.186)。
- 6.資料生命週期面：包含 7 項關鍵成功因素 ( $C.R.=0.015 \leq 0.1$ )，達一致性檢定標準；其重要性順序為：資料蒐集 (0.183)，資料維護 (0.172)，定義規劃 (0.170)，應用性評估 (0.158)，資料存取 (0.131)，歸檔與刪除 (0.095)，盤點評估 (0.091)。
- 7.詮釋資料：包含四項關鍵成功因素 ( $C.R.=0.056 \leq 0.1$ )，達一致性檢定標準。其重要性順序為：架構 (0.347)，整合 (0.295)，控制 (0.235)，交付 (0.123)。

而經跨構面之彙總計算，可以獲得大數據治理關鍵成功因素整體評估分析結果(如表 6)，前 5 項影響及重要的關鍵成功因素依序為「資料安全」、「機敏資料與隱私」、「風險管控和危機處理」、「政策計畫」、「建立專屬組織或委員會」及「資料正確性」。前者著重於數據的安全性，後者則偏向於組織政策及數據品質之特性。

表 6 大數據治理關鍵要素在單一及整體構面的重要性評估

| 構面名稱        | 關鍵因素        | 單一構面  |    | 整體構面  |    |
|-------------|-------------|-------|----|-------|----|
|             |             | 權重    | 排序 | 權重    | 排序 |
| 組 織 面       | 建立專屬組織或委員會  | 0.346 | 1  | 0.052 | 5  |
|             | 責任和利害       | 0.302 | 2  | 0.046 | 8  |
|             | 組織成員培訓和教育   | 0.153 | 4  | 0.023 | 17 |
|             | 組織變革管理      | 0.199 | 3  | 0.030 | 12 |
| 政 策 面       | 組織願景        | 0.307 | 2  | 0.047 | 7  |
|             | 政策計畫        | 0.391 | 1  | 0.059 | 4  |
|             | 政策績效評估      | 0.302 | 3  | 0.046 | 8  |
| 標 準 面       | 標準作業程序與指導方針 | 0.365 | 1  | 0.042 | 10 |
|             | 資料定義和分類     | 0.212 | 2  | 0.024 | 15 |
|             | 主資料/參考資料    | 0.130 | 4  | 0.015 | 26 |
|             | 資料模式        | 0.180 | 3  | 0.021 | 20 |
|             | 協定與技術       | 0.113 | 5  | 0.013 | 27 |
| 安 全 面       | 機敏資料與隱私     | 0.256 | 2  | 0.072 | 2  |
|             | 資料安全        | 0.382 | 1  | 0.107 | 1  |
|             | 風險管控和危機處理   | 0.213 | 3  | 0.060 | 3  |
|             | 資料內容變更與權限管理 | 0.149 | 4  | 0.042 | 10 |
| 品 質 面       | 資料正確性       | 0.607 | 1  | 0.052 | 5  |
|             | 完整性         | 0.186 | 3  | 0.016 | 25 |
|             | 資料一致性       | 0.207 | 2  | 0.018 | 23 |
| 資 料 生 命 週 期 | 定義規劃        | 0.170 | 3  | 0.023 | 17 |
|             | 盤點評估        | 0.091 | 7  | 0.012 | 29 |
|             | 資料蒐集        | 0.183 | 1  | 0.025 | 14 |
|             | 資料存取        | 0.131 | 5  | 0.018 | 23 |
|             | 資料維護        | 0.172 | 2  | 0.023 | 17 |
|             | 應用性評估       | 0.158 | 4  | 0.021 | 20 |
|             | 歸檔與刪除       | 0.095 | 6  | 0.013 | 27 |
| 詮 釋 資 料     | 架構          | 0.347 | 1  | 0.028 | 13 |
|             | 整合          | 0.295 | 2  | 0.024 | 15 |
|             | 控制          | 0.235 | 3  | 0.019 | 22 |
|             | 交付          | 0.123 | 4  | 0.010 | 30 |

整體而言，透過相對比較及權重計算的方式，可得知所有關鍵成功因素對於大數據治理模式的影響及重要程度，進而提供組織進行數據治理任務之參照。

## 五、結論

政府近年極力推動各項資料開放及數據應用之工作，民間企業也紛紛聚焦於資料科學方法對組織數據內容的挖掘，相關研究學者更著眼於數據分析及演算的各類技術，積極進行不同議題的論文研究。這些發展肇因於數據科技時代下，多樣類型及快速產製的大量資料所造成的複雜化現象，因而強調大數據治理議題發展的重要性。

本研究藉由文獻彙整、問卷設計及專家研討來評量大數據治理所需考量的構面及關鍵因素項目，除建立治理的層級架構外，亦評估各項構面及關鍵因素之影響權重。相關成果可提供後續各單位導入大數據治理之參考。研究成果計有以下 2 項重點：

- (一) 評估構面的重要性依序為安全、政策、組織、品質、標準、詮釋資料及資料生命週期，其中「安全面」權重占 29.3% 為最高；而評估模型中最為關鍵的三項要素分別為「資料安全」、「機敏資料與隱私」及「風險控管和危機處理」。此項成果反映出在大數據治理架構中，專業人員認為在資料開放及共享趨勢下，應強化資料本身安全及個人隱私、資料存取及外洩風險管控、資料異常之危機處理等工作，同時亦應籌建完善的數據安全管理與防護機制，以確保組織運用資料時的整體安全性。
- (二) 其他相對重要的因素有政策面的「政策計畫」、組織面的「建立專屬組織或委員會」及品質面的「資料正確性」。前面兩項主要強調大數據治理需要制訂組織處理及運用資料的規範及指引，並籌建專屬機構，來負責整合單位內部大量、即時與多樣型態的數據來源，同時依循治理計畫，管理及維護單位數據的各類問題，以利支援組織大數據的分析及應用。

本研究綜整之大數據治理評量模型，經實證後獲得各構面及因素的重要程度，除補強多位研究學者之框架要素外，亦可做為後續組織或相關機構導入大數據治理模型之指引參照，應有助於政府機構或企業組織面臨數據科技時代的治理議題。未來研究有兩點建議：第一、以本研究之評量模型為基礎，結合深度訪談及個案研究方法進行不同組織個案之探索與分析，期能相互對照或挖掘更為深層的因素；第二、本論文設計為多屬性決策（multiple attribute decision making, MADM）問題，研究重心主要基於層級分析法 AHP 來探索多屬性特徵／因素之評估模型。然而，因應屬性／特徵的複雜性，許多研究已嘗試整合不同分析方法進行設計，包括網絡分析法（Analytic Network Process, ANP）、決策實驗室分析法（Decision Making Trial and Evaluation Laboratory, DEMATEL）、偏好順序評價法（Technique for Order Preference by Similarity to Ideal Solution, TOPSIS）及灰關聯法（grey relation）等。建議後續亦可整合不同評估方法與機制，來分析並解譯大數據治理評量模型可能的不同影響。

## 六、國防領域之應用

數據科技時代的來臨，世界各國政府均著眼於數據整合的重要，並嘗試研擬及執行大數據治理的多重整合性任務。國防軍事各項任務遂行涵蓋人事、情報、作戰、後勤、通信、訓練、主計及醫療等多類型及多層面的訊息，作業環節息息相關，也經常需要跨單位的資料蒐整，而以往的作業流程大多以人工協調方式為主，因此造成作業時間費時、資料缺乏共享機制、分析查詢不易、資料格式各異等問題，進而影響情資分析效率及作戰評估效益。因此，國防軍事相關部門在新興科技發展模式下，也面臨到國防資訊化及數據化轉型的諸多挑戰。

國防大數據政策的推展，初期在資料籌獲方面將面臨跨軍種／部門協調、資料格式不一致及數據安全性等問題。為因應這些困難與阻力，本研究綜合歸納以下 4 點建議：（1）由具主導能力之部門，全般考量國防數據應用之適切性，並負責統籌訂定具體政策計畫；（2）藉由軍民技術合作方式，引入業界資料整合架構，運用科技快速處

理多元且複雜的資料格式，以減低人力彙整資料的額外負擔；（3）完善資料權限管控架構，以支援相關單位有效管制及維護資料的安全；（4）透過數據化管理及規劃，建構數據應用之規範或準則，以有效提升國軍資料運用的整體效益及品質。綜上所述，國軍各單位惟有打破傳統的思維，屏除本位主義包袱，接受智慧型高新資訊科技的發展，以期運用整合性的國防數據，支援國軍整體戰力之發揮，並提升國軍資訊價值與效益。

### 致謝

感謝匿名審查委員的諸多寶貴意見，使本論文之內容更臻完善；本研究承蒙行政院科技部專題研究計畫支持（計畫編號：MOST 107-2410-H-606-006），謹致謝忱。

## 參考文獻

- 王俊、王修來、龐威、趙鴻飛，2021。面向科技前瞻預測的大數據治理研究。計算機科學，第 48 卷 9 期，36-42。
- 李小慶，2021。銀行大數據治理研究和實踐。中國金融電腦，61-64。
- 吳雅玲，2001。德懷術及其在課程研究上的應用。教育研究，第 9 期，297-306。
- 堯淦、夏志傑，2020。政府大數據治理體系下的實踐研究—基於上海、北京、深圳的比較分析。情報資料工作，第 41 卷 1 期，94-101。
- 張宇杰、安小米、張國慶，2018。政府大數據治理的成熟度評測指標體系構建。情報資料工作，第 1 期，28-32。
- 張紹華、潘蓉、宗宇偉，2016。大數據治理與服務。上海：上海科學技術。
- 楊欣哲、陳柔穎、謝永明，2015。企業雲端化移轉的關鍵成功因素之探討。資訊管理學報，第 22 卷 3 期，317-352。
- 陳良駒、田美惠、吳瑞琦，2019。政府網站資料品質評量因素之研究：資料提供者與使用者的雙重觀點。Electronic Commerce Studies，第 17 卷 3 期，197-224。
- 楊琳、高洪美、宋俊典、張紹華，2017。大數據環境下的數據治理框架研究及應用。計算機應用與軟件，第 34 卷 4 期，65-69。
- 傅文成，2018。從社會信用評級系統看大陸大數據治理運用。展望與探索月刊，第 16 卷 5 期，24-31。
- 翟云，2018。中國大數據治理模式創新及其發展路徑研究。電子政務，第 8 期，12-26。
- 鄭大慶、范穎捷、潘蓉、蔡會明，2017。大數據治理的概念與要素探析。科技管理研究，第 15 期，200-205。
- Al-Badi, A., Tarhini, A., and Khan, A. I. 2018. Exploring big data governance frameworks. *Procedia computer science*, 141, 271-277.
- Al-Sai, Z. A., Abdullah, R., and Husin, M. H. 2020. Critical success factors for big data: a systematic literature review. *IEEE Access*, 8, 118940-118956.
- Abbasi, A., Sarker, S., and Chiang, R. H. 2016. Big data research in information systems: Toward an inclusive research agenda. *Journal of the association for information systems*, 17(2), 3.
- Ahmad, I., Ahmed, G., Shah, S. A. A., and Ahmed, E. 2020. A decade of big data literature: analysis of trends in light of bibliometric. *The Journal of Supercomputing*, 76(5), 3555-3571.
- DAMA, 2009. The DAMA guide to the data management body of knowledge. New York : Technics Publications.
- Dash, S., Shakyawar, S. K., Sharma, M., and Kaushik, S. 2019. Big data in healthcare: management, analysis and future prospects. *Journal of Big Data*, 6(1), 1-25.

- Data Governance Institute, 2009. The DGI data governance framework, USA, DGI.
- Ghofrani, F., He, Q., Goverde, R. M., and Liu, X. 2018. Recent applications of big data analytics in railway transportation systems: A survey. *Transportation Research Part C: Emerging Technologies*, 90, 226-246.
- Hasan, M. M., Popp, J., and Oláh, J. 2020. Current landscape and influence of big data on finance. *Journal of Big Data*, 7(1), 1-17.
- Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., and Khan, S. U. 2015. The rise of “big data” on cloud computing: Review and open research issues. *Information systems*, 47, 98-115.
- Hey, T., Tansley S., and Tolle, K., 2009. Jim Grey on eScience: A transformed scientific method. In: Hey T, Tansley S and Tolle K (eds) *The Fourth Paradigm: Data-Intensive Scientific Discovery*. Redmond: Microsoft Research.
- Hill, K. O. and Fowles, J. 1975. The method of logical worth of the Delphi forecasting technique. *Technological Forecasting and Social Change*, 7: 179-192.
- Holden, M. C. and Wedman, J. F., 1993. Future issues of computer-mediated communication: The results of a Delphi study. *Educational Technology Research and Development*, 41(4): 5-24.
- ISACA.COBIT 5. 2012. Business framework for the governance and management of enterprise IT. Rolling Meadows, IL: ISACA Knowledge Center.
- ISO, 2008, Corporate governance of information technology, International Organization for Standardization, Geneva.
- Kim and Cho, 2017. Data Governance Framework for Big Data Implementation with a Case of Korea, Hankuk University of Foreign Studies, Korea.
- Kitchin, R. 2014). Big Data, new epistemologies and paradigm shifts. *Big data & society*, 1(1), 2053951714528481.
- Li, Q., Lan, L., Zeng, N., You, L., Yin, J., Zhou, X., and Meng, Q. 2019. A framework for big data governance to advance RHINs: a case study of China. *IEEE Access*, 7, 50330-50338.
- Lugmayr, A., Stockleben, B., Scheib, C., and Mailaparampil, M. 2017. Cognitive big data: survey and review on big data research and its implications. What is really “new” in big data? *Journal of Knowledge Management*, 21(1), 197-212.
- Mikalef, P., and Krogtie, J. 2018. Big Data Governance and Dynamic Capabilities: The Moderating effect of Environmental Uncertainty. In *PACIS 2018 Proceedings-Opportunities and Challenges for the Digitized Society: Are We Ready?* Pacific Asia Conference on Information Systems (PACIS 2018). Association for Information Systems.

- Murphy, J. W. and Hammons, J. O., 1995. Delphi: A Versatile methodology for Conducting Qualitative Research. *Review of Higher Education*, 18(4): 423-436.
- Otto, B., 2011. A Morphology of the Organisation of Data Governance, ECIS 2011 Proceedings. p.272.
- Panian, Z. 2010. Some practical experiences in data governance. *World Academy of Science, Engineering and Technology*, 62(1), 939-946.
- Saaty, T. L. 1990. Decision Making for Leaders: the Analytic Hierarchy Process for Decisions in a Complex World, RWS publications.
- Shah, S. I. H., Peristeras, V., and Magnisalis, I. 2021. DaLiF: a data lifecycle framework for data-driven governments. *Journal of Big Data*, 8(1), 1-44.
- Soares, S. 2012. Big data governance: An emerging imperative. Mc Press.
- Zorrilla, M., and Yebenes, J. 2022. A reference framework for the implementation of data governance systems for industry 4.0. *Computer Standards & Interfaces*, 81, 103595.



# 「國防管理學報」徵稿與評審辦法

## 壹、目的與範圍

「國防管理學報」係為國防大學管理學院發行之學術期刊，凡舉人力資源、財務管理、物流管理、科技管理、資訊管理、資源決策、國防法制、採購管理、戰場管理等學術領域，尤為與軍事結合之論述，或能闡明其軍事管理意涵之稿件，竭誠歡迎專家學者投稿。凡來函稿件以原創性及回顧性論文為主，已發表在其他期刊或審稿中的文章將不接受刊登，稿件文章力求精簡嚴謹，本學報支付稿酬，不收取刊登費用，贈送作者當期學報乙冊，來稿採隨到隨審方式全年徵稿。

稿件篇幅不得超過 20 頁（約 2 萬字）。本學報不收取刊登費用，來稿採隨到隨審、雙向匿名方式進行審查，全年徵稿；自第四十卷第一期起，來稿一經刊載，即依本刊規定奉致稿酬。

## 貳、投稿方式與格式

本學報為半年刊，每年五、十一月出刊，為便利本學報編審及出版作業，採系統投稿與信箱投稿之雙軌制，來稿敬請將 word 檔逕寄「國防管理學報信箱」journalofndm@gmail.com，並同時於國防大學網站報名（步驟：國防大學首頁左下角→雜誌期刊專區內之雜誌期刊投、審稿作業→報名投稿→送出），以利加速審稿時效。

若有相關問題請洽詢國防大學管理學報 承辦人(陳正忠先生 電話 02-28986771)。

## 參、評審辦法

評審作業方式由主編推薦兩位相關領域審查人員擔任稿件審查工作，審查意見共分四級，分別為拒絕、修改後再審、修改後主編審閱(原審者不須過目)、刊登，凡經審查接受者始得刊登本學報，審查結果處理方式如下表：

|         |                  | 第二位評審意見 |              |                  |              |
|---------|------------------|---------|--------------|------------------|--------------|
|         |                  | 拒絕      | 修改後再審        | 修改後主編審閱(原審者不需過目) | 刊登           |
| 第一位評審意見 | 拒絕               | 不宜刊登    | 不宜刊登         | 送第三人審            | 送第三人審        |
|         | 修改後再審            | 不宜刊登    | 修改後再審        | 修改後送第一位原審者再審     | 修改後送第一位原審者再審 |
|         | 修改後主編審閱(原審者不需過目) | 送第三人審   | 修改後送第二位原審者再審 | 修改後刊登            | 修改後刊登        |
|         | 刊登               | 送第三人審   | 修改後送第二位原審者再審 | 修改後刊登            | 刊登           |

作者須自負文責，並請注意不得違反國軍保密與著作權等相關規定，對審查人員所建議刊登之文章，將隨即進行保密安全查核，凡經查核有疑慮者仍將無法刊登，且編審委員對來稿有刪改或建議修正權，不願刪改時應於稿件上預先註明，不適合刊登之稿件則退還原作者，並附專家學者審查意見供投稿人參考，如有未盡事宜，得經本校編輯委員會補充訂定之。



# 國防管理學報論文格式範例

王曉明<sup>1</sup> 李大華<sup>2\*</sup>

<sup>1</sup> 國防大學資源管理及決策研究所

<sup>2</sup> 國防大學財務管理學系

## 摘要

本文舉例說明國防管理學報所採用之排版格式，供投稿人編排論文參考之用。首先稿件全文中文部分皆使用標楷體，英文的部分則使用 Times New Roman 字型，論文可以中〈英〉文方式書寫，中〈英〉文論文必須加附英〈中〉文題目、作者姓名、單位、摘要及關鍵詞於中〈英〉關鍵詞(Keywords)之後，中文關鍵詞分隔符號以頓號「、」進行分隔，英文關鍵詞分隔符號以半形逗號「，」進行分隔，關鍵詞後均不加句號。英文姓名依護照外文姓名書寫方式，姓在前，名在後，姓之後加逗點，名與名之間加短劃「-」連結。中〈英〉題目為粗體 16 點字，作者姓名粗體 14 點，單位粗體 11 點，摘要標題粗體 12 點，摘要本文 12 點，關鍵詞標題粗體 12 點。當題目過長無法以一行表示時，必須以倒三角的方式排列。題目、作者姓名、單位、摘要標題與摘要本文之間必須間隔一行來表示。

**關鍵詞：**國防大學、管理學院、國防管理學報(3-5 個為宜)

## English Title

**Wang, Siao-Ming<sup>1</sup> Li, Da-Hua<sup>2\*</sup>**

<sup>1</sup> Graduate School of Resources Management and Decision Science, National Defense University, Taiwan,

*R.O.C.*

<sup>2</sup> Department of Financial Management, National Defense University,

*Taiwan, R.O.C.*

## Abstract

Please provide the English abstract in 300 words and keywords.

**Keywords:** National Defense University, Management College, Journal of National Defense Management (3-5 keywords)

---

\* 聯絡作者：李大華 email:wsf@gmail.com 聯絡作者之 email 請以\*註腳方式列示於首頁

<sup>1</sup> 註腳部不論中英文，請附註在當頁下方，且儘可能少用並以參考文獻代之。任何編排上的問題請電 02-28986600-604813 軍線：604813 E-mail：journalofndm@gmail.com 陳先生。

## 一、內容格式（大段落標題一律置中）

文章用 A4 大小的紙張，每頁上下緣及左右側各留 2.5 公分，文章以單欄方式打字且左右對齊，內文字型均採 12 點標楷體，採單行間距。

文章內容依序包含中〈英〉文標題、中〈英〉文作者、中〈英〉文摘要、中〈英〉文關鍵詞、英〈中〉文題目，英〈中〉作者姓名、英〈中〉服務單位、英〈中〉摘要、英〈中〉關鍵詞，本文、誌謝、參考文獻、附錄等順序書寫。文稿以不超過學報 20 頁為原則，並請以清晰之印表機列印，應避免使用有保密標號之浮水印影本，減少影響文稿內容之呈現。

### 1.1 段落編碼方式（中小段落標明靠左對齊）

段落編碼區分中文與英文兩種文稿。中文段落編排分別依一、1.1、1.1.1 順序排列（如圖 1 所示），英文段落編排則依 1.、1.1、1.1.1 順序排列（如圖 2 所示）。

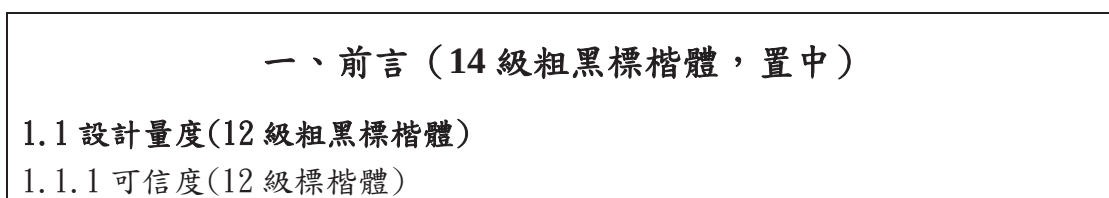


圖 1 中文段落編碼範例



圖 2 英文段落編碼範例

### 1.2 段落

每一段落開始，均需空兩字元，文內所出現之數字部分請使用 Times New Roman 字型文稿，中文稿中之英文詞及括號內之英文對照，除專有名詞外一律小寫表示，文稿經審查被接受時，作者不得擅自於校稿過程中增減內容，僅能就審查委員建議及排版錯誤修正。

## 二、圖表及方程式格式

### 2.1 圖片

不論是圖或表必須著名圖（表）號、圖（表）稱以及資料來源，若資料來源字研究者本身時則不需註明，文中所用之圖表、照片力求清晰，皆應以雷射列表機印出，其圖標題必須置於圖片下方。若圖標題僅使用一行，則必須置中，否則應靠左對齊。圖（表）必須用阿拉伯數字加以編號，之後不需要加任何標點符號如「：」，直接註明圖（表）稱即可。如文中引用時應指出圖號與表號來指引讀者，避免使用「如下圖所示」來表示。

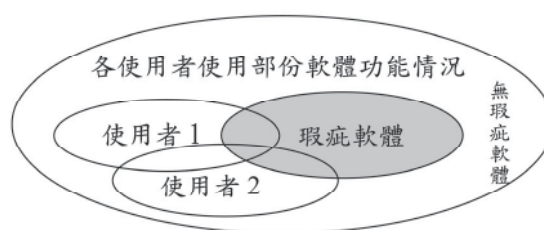


圖 3 軟體使用模式

### 2.2 表格

表標題必須置於表格上方且置中。如下例：

表 1 模組轉換機率表

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|--|--|--|--|

### 2.3 方程式

方程式應於上下各留一行空白，方程式應編號，編號靠右對齊並從(1)開始。如下例：

$$Q_{ij} = R_i p_{m_j} \quad (1)$$

## 三、內文引述格式

### 3.1 內文引述文獻

內文引述文獻應依中、英文稿之不同，遵循不同的格式要求。請同時注意以下範例之字體、斜體、底線、標點符號等規定。

#### 3.1.1

內文中引用文獻需含作者及出版年份，出版年份置於半形括號中，例如：A（年度）。若引用文獻有兩位作者，請用「與」或「and」字連接，例如：A 與 B（年度）或 A and B（年度）。若引用文獻有三人以上時，中文為 A 等（年度）而英文為 A et al.（年度）。

#### 3.1.2

引述文獻的括號內包含參考文獻之作者與出版年份時，請以「逗號」連接，例如：中文為（A 與 B，年度）而英文為（A and B, 年度）。若文獻有三人或以上時，中文為（A 等，年度）而英文為（A et al., 年度）。

#### 3.1.3

英文專有名詞字首以大寫書寫並與縮寫之間用半形分號隔開。例如資料包絡分析法(Data Envelopment Analysis; DEA)。

### 3.1.4

括號內同時有多筆文獻時，中文引述文獻不同作者之間請用全形分號隔開，相同作者不同年代之文獻請用全形逗號隔開；英文引述文獻不同作者之間用半形分號加空格隔開，相同作者不同年代之文獻用半形逗號加空格隔開。

## 四、參考文獻

參考文獻標題不須編碼，參考文獻必須以本文引用才能列出，文獻必須區分中文與英文部分，先列出中文的參考文獻再列出英文的參考文獻，中文文獻依姓氏筆劃順序排列，筆劃較少的優先出現，英文則依字母順序排列。當不同文獻出自同一作者時，應依年代排序，年代較早的文獻先出現。不論中文與外文參考文獻均採西元年代，中文期卷、頁數均採阿拉伯數字，勿用國字表示。英文文獻作者姓名會依人數多寡編排方式有所不同，當作者一人時一律採縮倒寫格式（姓氏在前，名字在後，並用逗號隔開）。當作者不只一人時，只有第一作者採縮倒寫格式，以後作者採縮寫格式（名字在前，姓氏在後，並將名字縮寫）。出版地以總公司所在之程式為準，出版地與出版者之間須以冒號隔開，英文書籍出版地須以城市名或州名方式處理，在出版公司之後不需加上「書局」或「出版社」等字，英文則如 Publishing Co. 或 Book Company 等字，並請注意英文的標點符號全部為半形，而且在標點符號之後需空一格半形，中文則全部為全形，標點符號之後則不需空格。頁數部分則直接註明頁碼不須以「p.」或「pp.」方式，但英文報紙則須加註以表明版頁。參考文獻以凸排方式編排。所有中英文之期刊、書籍、研討會議、論文集、報告、學位論文、編輯書、翻譯書、報紙與網路之編排格式範例，請參照參考文獻部份範例，若有不足部分，請參考 APA 第六版格式相關規範。

## 五、國防領域之應用

本段乃鼓勵作者以 500 字以內簡述本論文於國防相關事務之可能性應用；舉凡人力資源、財務管理、物流管理、資訊管理、資源決策、軍事法律、採購管理、戰場管理等皆可。特別是鼓勵無法直接以軍事單位或國防事務為研究對象之專家學者，依其專業，提出於國防事務應用之價值與可能性，以拓展學刊之多元性，也讓實務工作者可以明瞭此論文於實務之應用與價值。

## 誌謝

若需要於本文末段簡短表達無則可免。

## 參考文獻

- 王文義，1983。談國內百貨公司專櫃制度，經濟日報，1983年4月12日，第16版。
- 毛宣崇，傅敬群，1999。決策理論在軟體使用模式上之應用，陸軍官校七十五年週年校慶綜合學術研討會論文集，33-38。
- 林彩梅，1986。多國籍企業，台北：五南。
- 留忠賢譯，1997。軟體工程，第3版，台北：松崗，譯自 Ian Sommerville。
- 張文貴，1997。從產品使用型態談軟體品質的認證，品質學報，第3卷2期，26-29。
- 許牧彥，2001。從知識經濟的特質談台灣專利，收錄自吳思華編，知識資本在台灣，台北：遠流，297-352。
- 楊國隆，1997。模糊多屬性決策分析評估武器系統，國防管理員院資源管理研究所碩士論文。
- 經濟部投資業務處編印，1993。泰國投資環境簡介，20-30。
- 楊國隆，1999。模糊統計之可靠度分析模式，陸軍官校八十一週年校慶綜合學術研討會，鳳山。
- 楊國隆，2000。模糊多屬性決策分析評估武器系統，下載於 <http://www.ndu.edu.tw/artilcles.htm> (2003年8月23日)。
- 楊壽仁，動態決策理論之研究，國科會補助研究報告，NSC86-2417-H-224-001。
- Baron, R.A., 1993. Affect and Organizational Behavior: When and Feeling Good Matter. In J. K. Murnighan (Ed.) Social Psychology in Organization (66-68) Chichester, England: John Wiley & Sons.
- Kao, C. and Yang, Y. C., 1992. Reorganization of forest districts via efficiency measurement, *European Journal of Operational Research*, 58 (2), 356-362.
- Kotler, P., 1991. *Marketing Management*, trans. John Glueck, 1993.
- Kurtenbach, E., 1995. *Housing Crisis is Real Life Drama*, The China Post, July 11 1995, 12.
- Liang, S. K., Yang, K. L. and Chu, P., 2003. Fuzzy multi-object programming application for time-cost trade-off of CPM in project management, *Protland International Conference on Management of Engineering and Technology'03*. U.S.A.
- Mills, H. D., 1992. *Software Productivity*, 10th ed, NJ: Prentice Hall.
- Shih, Y. C., M. J. Wang, and C. H. Chang, 1996. The effects of handle angle on maximum acceptable weight of lifting, *Proceedings of the 4th Pan-Pacific Conference on Occupational Ergonomics*, 260-263.
- Hock, D. W., 2004. Method for Measuring Intangible Asserts. From <http://www.sveiby.com/articles/Intangiblemethods.htm> (retrieved on May 18, 2005)
- Rosenwein, M., 1986. Design and Application of Solution Methodologies to Optimize Problems in Transportation Logistics, Ph. D. Dissertation, Department of Decision Sciences, University of Pennsylvania, Philadelphia.
- Simpson, B. H., 1975. Improving the Measurement of Chassis Dynamometer Fuel, Society of Automotive Engineers Technical Paper Series 750002.

## 附錄

和本文無直接關係或太過冗長內容請放置附錄，其內容以單欄方式放置文章之最後。

# 國防管理學報

JOURNAL OF NATIONAL DEFENSE  
MANAGEMENT

---

創 辦 人：果 芸

發 行 人：林振裕

出 版 者：國防大學管理學院

網 址：<https://www.mnd.gov.tw/PublishMPPeriodical.aspx?title=軍事刊物&id=22>  
(連結軍事出版品／軍事刊物／(第三頁)國防管理學報)

地 址：臺北市北投區中央北路2段70號

電 話：(02)23116117-604813

登記證字號：行政院新聞局局版台誌第3853號

中華郵政台字第1112號執照登記為雜誌交寄

創 刊 日 期：73年元月

承 印 者：國防部軍備局生產製造中心第401廠北部印製所

TEL：(03)4801145，4801456

發 行 量：350本

展 售 處：五南文化廣場 網址：<http://www.wunanbooks.com.tw>

地 址：400臺中市中山路6號 電話(04)22260330

國 家 書 店：網址：<http://www.govbooks.com.tw>

地址：104臺北市松江路209號1F 電話(02)25180207

定 價：新台幣350元／本

G P N：2007300059

I S S N：1022-4858

中華民國一一一年十一月

## ▲著作權資訊



本刊內容採「姓名標示—非商業性—禁止改作」  
創用授權條款 3.0 臺灣版

