

# 國軍資訊硬體架構選擇 與組織變革之探討

海軍備役中校 柯國華

## 提 要

- 一、低成本、高安全的資訊硬體環境建置準則是，除了滿足工作所需，其餘功能全部不要或完全管制。
- 二、命令式禁止的消極管制措施，不能有效防杜資訊違規事件的發生，透過科技的方法或架構的改變，更能達到管制目的。
- 三、資訊儲存裝置易於攜帶與藏匿，數位資料可以恣意的攜出、入營區，將使得這類資訊違規成為無法約束的常態。
- 四、Thin Client低頻寬便能運作妥善的特性，戰時更能確保戰場共同圖像的完整性，因而形成一項資訊優勢。
- 五、當資訊戰已經成為主導戰場勝負重要關鍵時，國軍資訊人力必須配合調整並重新定義任務內容。

關鍵詞：Thin Client、精簡型電腦、資訊戰、資訊安全、組織變革

## 壹、前 言

國軍資訊作業環境使用的沿革，肇始於二、三十年前的大型主機，使用的作業系統是專屬的封閉式系統，使用的程式語言是趨近於機器碼的組合語言或商用COBOL語言；隨著個人電腦的問世，因為方便、低廉以及極具親和介面的操作方式，加上後續網路技術的進步，使得全球幾乎被這波，以個人電腦及網路為平臺的資訊作業環境所影響。

但是個人電腦高度開放的輸出、入介面，相對的增加許多資訊作業風險，包括病毒感染、駭客攻擊、資料竊取等，嚴重危害

資訊作業安全，因此，國軍資訊部門必須窮於因應各種可能的危險因子，一一加以補強，於是必須建置防毒系統、防火牆、入侵偵測系統、自動備份軟體、資產管理系統等安全防護措施，資訊安全投入成本不斷增加，資訊安全威脅卻不減反增，凡此種種，似乎又讓我們懷念起大型主機時代，安全、穩定的作業環境。

然而時間不會倒流，隨著個人電腦以及相容作業系統所開發的套裝軟體，如雨後春筍般紛紛出籠，使用者得以享用各式功能強大的資訊工具，提升工作效率。逐漸的，以個人電腦連接而成的區域網路架構，已經主宰了整個資訊作業環境。

如何利用資訊工具的優點，避免其缺點，是本研究目的所在，本研究並沒有準備全面探討資訊安全議題，而是針對個人資料處理，已經發生危害資訊安全的部分加以分析，並從安全優先為考量，發掘更適於國軍作業屬性的資訊架構，使得整體投入成本最低、安全性最高，讓資訊作業環境更為安全。

雖然透過技術可以解決許多問題，但是一項看似優於舊環境的資訊科技，就能夠保證順利獲得使用者接受而推行成功嗎？不能推行成功的背後又隱含了哪些潛藏的因素？本研究試圖為國軍提出一套符合低成本、高安全的資訊作業環境，並針對推行新環境可能遇到的阻礙，尋求解決方案。技術改變可能帶來效益，同時也引發組織變革的契機，本研究對於可能的資訊組織重整一併提出建議，做為參考。

## 貳、資訊安全與規範

國軍使用個人電腦初期，對於個人處理的資料安全，便訂有極為嚴格的管制規定，諸如個人電腦硬碟不准存放資料，所有資訊媒體（一般是磁片）於下班前必須集中保管於保密軍官處，上班前領用必須填寫磁片使用登記簿，只要新建立的磁片必須填寫磁片管制登記簿，並且張貼磁片管制標籤，甚至檔案的新增、刪除都必須加以記錄，下班後還必須將這些資訊媒體繳回保密軍官處，<sup>註一</sup>往昔為了資料安全所制訂的這些繁瑣的程

序，在今天看來似乎有些不切實際，不過這也說明了國軍注重安全更甚於效率帶來的利益。最後因為戰略性資訊作戰成為一項新戰略思惟<sup>註二</sup>，資訊安全防護更加突顯其重要性。

不過以上僅及於資訊安全中的軟體安全規範，除了軟體安全外，尚包括硬體安全及個人安全<sup>註三</sup>。而在資訊安全的領域中，更要滿足三項基本原則：機密性(Confidentiality)、完整性(Integrity)和可用性(Availability)。機密性是指透過資料進行加密，達到保護資料的目的；完整性是指透過對資料的保護，避免遺失、被竄改等；可用性是指確保資料及時可用，能夠滿足各種使用需求。<sup>註四</sup>

國軍目前遵循的資訊安全規範包括ISO 17799/BS7799及橘皮書二種，概述如后：

### 一、ISO 17799/BS7799

ISO 17799來源於英國標準協會(BSI)在1995年2月提出的BS7799安全規範，可供資訊人員建置、管理、維護資訊安全時使用，ISO17799提供了127個安全控制措施，以協助企業運作過程中，控制對資訊安全有影響的因素，這127個安全控制因素可以分為10個方面：<sup>註五</sup>

- (一)安全政策。
- (二)組織安全。
- (三)資產分類與控制。
- (四)人員安全。
- (五)實體和環境的安全。

註一 陸軍軍官學校，陸軍軍官學校校園學術網路使用管理規定，[http://www2.cma.edu.tw/admin/info\\_center/930810net\\_rule.htm](http://www2.cma.edu.tw/admin/info_center/930810net_rule.htm)

註二 國防部史政編譯局譯印，戰略性資訊作戰的崛起（臺北，國防部史政編譯局，民國89年5月），頁vii-xxxi。（Roger C. Molander, Peter A. Wilson, David A. Mussington, Richard F. Mesic, Strategic Information Warfare Rising, 1998）

註三 張博竣，資訊安全管理實務（臺北，文魁，民國93年4月），頁1-5。

註四 同註三，頁1-18。

註五 同註三，頁1-18至1-23。



- (六)通訊和操作安全。
- (七)存取控制。
- (八)系統開發與維護。
- (九)業務持續性管理。
- (十)符合性。

## 二、橘皮書

美國國家電腦安全委員會(NCSC：U.S. National Computer Security Commission)為美國電腦安全的管制中心，該中心出版一系列的彩虹(rainbow)書籍來描述及訂定電腦系統的安全，其中「計算機系統可信賴評估標準」(Trusted Computing System Evaluation Criteria, TESEC)，由於封面為橘色之故，又稱為橘皮書(Orange book)，為美國政府及軍方各單位採購建置電腦系統時，有關系統安全部份評估之主要依據。<sup>註六</sup>橘皮書將電腦系統定義成各種不同的安全等級，如表一。

表一 計算機系統可信賴評估標準安全定義

| 等 級 | 規 範            |
|-----|----------------|
| D   | 最低限度防護或未制定防護規範 |
| C1  | 自訂式安全防護        |
| C2  | 控制式存取防護        |
| B1  | 標籤式安全防護        |
| B2  | 結構性防護          |
| B3  | 安全領域           |
| A1  | 經驗證的設計         |

資料來源：陳峰棋譯，資訊安全（臺北，麥格羅·希爾，民國93年），頁1-7。（Eric Maiwald, Network Security: A Beginner's Guide, 2<sup>nd</sup> Edition, 2003）。

大部分個人電腦安裝的作業系統安全等級為D、伺服器主機暨網路作業系統的安全等級則達到C2。

## 參、個人電腦的風險暨數位資料的管制漏洞

雖然國軍透過各種資訊安全規範加強資訊安全作為，然而目前這個以個人電腦為主要平臺，透過網路連接的資訊作業環境，仍然必須面對諸多高度不安全的危害因子，除了資料管制不易的風險外，還包括病毒威脅、駭客入侵、資料遺失、資料損毀、重要零件被竊等可能發生的危害，資訊部門必須針對各種危害因子加以防範，因而不斷提高單位的維護管理成本。但是國軍在資訊作業環境中，設置了防毒系統、防火牆、入侵偵測系統、備份系統，甚至用於管理硬體設備的資產管理系統之後，整體的資訊作業環境就算安全了嗎？雖然國軍採取與網際網路的實體隔離政策，降低了許多外部風險，但是對於數位資料的存取與保護，仍然仰賴命令式的規範，國軍內部MINET連接網路的個人電腦便超過萬部以上，每一部個人電腦卻都是風險點。

民國89年間，海軍新江軍艦發生之劉岳龍洩密案<sup>註七</sup>、92年中科院陳士良，涉嫌從辦公室電腦下載國軍極機密的「亢龍計畫」、P-3C反潛機採購、反潛兵力配置等資料，並以電子郵件寄往中國。<sup>註八</sup>96年漢光演習，則傳出多起兵推、想定等機密資料遭中共駭客竊取的報導<sup>註九</sup>。這些重大資訊危安事件發生問題的主要原因，就在於個人電腦毫無管制的輸出、入介面；由於資訊媒體管制不易，加上可以儲存資料的媒體，設計愈

註六 同註三，頁1-21。

註七 監察院網站，「海軍新江艦前艦長任文中少校、現任艦長方長桐少校，未恪遵保密管理規定，致肇生譯電中士劉岳龍重大洩密事件，核有重大違失案」，監察院91年彈劾案，[http://www.cy.gov.tw/record/3-4-4\\_PDF/91\\_008.pdf](http://www.cy.gov.tw/record/3-4-4_PDF/91_008.pdf)

註八 自由時報社論，「國軍政戰部門應加強防杜共諜滲透」，自由時報新聞網，民國92年8月7日，<http://www.libertytimes.com.tw/2003/new/aug/7/today-s1.htm>

註九 盧德允，「玉山兵推機密，疑被中共駭走」，聯合新聞網，民國96年4月9日，<http://tw.news.yahoo.com/article/url/d/a/070408/2/cm3y.html>

臻精巧(例如隨身碟)，易於攜帶與藏匿，導致人員可以恣意的將資料攜出或攜入營區。

雖然國軍早已了解資訊安全不僅只是技術問題，更須從程序面加以防範，並在數年前導入ISO17799的安全規範，要求所有單位，必須針對127個安全控制措施加以檢討並落實執行，但是資訊安全事件還是不斷發生，原因何在？在ISO17799的127個安全控制措施，其中一個稱為「移動式電腦媒體管理」的控制項中，要求單位查核「磁帶、磁碟、卡帶及列印報表等可移動式電腦媒體之管理是否建立管制措施。」<sup>註十</sup>國軍任何一個資訊部門都可以針對此一項目回覆，完成管制妥善的訊息，理由是國軍已經全面要求，所有使用之資訊媒體，必需張貼保密管制標籤，並且集中於單位保密軍官保管。所有程序似乎完全符合ISO17799對於「移動式電腦媒體管理」的規範，但是為何國軍對於人員不當將資訊媒體攜出、入營區使用的違規行為仍舊束手無策？顯然這項措施仍然無

法有效防範違規事件的發生，國軍必須採取更嚴密的管制作為。

雖然大部分人員將公務資料攜出營區，並非有何特定目的，而是為了作業方便，讓個人時間運用更具彈性，或許對於提昇工作績效也能有些幫助，但是將機密資料攜出營區作業，就如同衛兵下哨後，還帶槍去渡假一般的危險；使用者為了工作的便利，而嘗試自我管理風險的資訊違規現象在國軍當中，將可能是一種無法約束的常態，而非少數的個人行為，因此，數位資料遺失或被竊事件的曝光，只是這類違規事件的機率反應罷了。全靠人員自發性的遵守資訊安全規定，絕對無法降低這類違規事件的發生。

個人電腦在資訊安全方面的不利因素，除了資料輸出、入無法管制造成的安全問題外，使用者更可能造成其他諸多違規的行為，為了因應這些危害因素，國軍目前的防範措施，卻幾乎全是命令式禁止的管制措施(如表二)。由於違規行為查察不易，管制效

表二 國軍違規資訊作業行為暨現行防範措施

| 項次 | 違規資訊作業行為                                 | 防範措施                                          |
|----|------------------------------------------|-----------------------------------------------|
| 1  | 攜入不明軟體造成中毒並散播病毒。                         | 1.規定個人不准攜入來路不明資料或軟體。<br>2.要求安裝防毒軟體並定期更換最新病毒碼。 |
| 2  | 被植入木馬，成為駭客攻擊的跳板。                         | 要求不定期進行漏洞修補或安裝防毒軟體並定期更換最新病毒碼。                 |
| 3  | 從網際網路獲得入侵主機工具程式扮演駭客。                     | 規定個人不准攜入來路不明資料或軟體。                            |
| 4  | 自行更換軟體版本，造成軟體衝突、當機、效率變差，引發維修需求或要求電腦硬體升級。 | 規定個人不准攜入來路不明資料或軟體。                            |
| 5  | 資料存於個人電腦硬碟，因磁軌損壞而資料損毀。                   | 規定資料應存放於磁片或具有存取控制的檔案伺服器中。                     |
| 6  | 1.蓄意竊取資料。<br>2.將資料攜出營作業或遺失。              | 非經奉准不得將資料攜出營。                                 |
| 7  | 私自拆裝或竊取電腦主機內重要零件。                        | 1.使用保密封籤，封貼於主機外殼，防止私自拆裝電腦。<br>2.透過資產管理系統監控。   |

資料來源：本研究。

註十 劉永禮，以BS7799資訊安全管理規範建構組織資訊安全風險管理模式之研究，私立元智大學工業工程與管理研究所碩士學位論文，民國91年7月，頁132-143。



果可想而知。

不過，大約在10年前，海軍的一個修護單位，就體認出資料存取安全的重要性，當時這個單位首開先例，採取無軟碟作業環境，收繳所有個人持有的資訊媒體，資訊部門同時在伺服器主機中，提供具有個人帳號、密碼識別及存取控制的資料儲存服務，單位內的資料交換均透過區域網路進行，另外保留一部具有軟碟機的電腦，做為與外單位資料交換使用，而這項作業必須經過層級長官的核准，方得開放。由於當時個人電腦中尚無USB的存取介面，在撤除軟碟機後，人員完全無法隨意將數位資料攜出單位之外，當國軍網路普遍建置，電子郵件普及時，該單位便透過防火牆阻絕所有對外傳輸的資料封包，只允許外部單位資料或郵件進入營區，直到USB介面出現，更使用外力方式將每部電腦的USB介面予以封閉。這項作法看似有些原始，但也最為有效，確實做到了資料存取安全管制效果，是國軍資訊安全的典範。

顯然這個單位認為，命令式的要求個人遵守資訊安全規定的消極性做為不是萬靈丹，透過技術管制的方式，遠比法規命令要求來的更為有效。

而今國軍資料洩密案件仍然不斷發生，為害程度似乎更加嚴重，國防部資訊單位，有責任為國軍規劃出，更為安全的資訊作業環境與架構，達到管制使用者無法任意輸出、入資料的目標，以取代消極性「規定不准做」的舊思惟。

## 肆、國軍資訊硬體採購原則

雖然個人電腦功能強大又價格低廉，但卻造成諸多危安因素，然而我們還有其它選

擇嗎？當大家已經嘗到開放式作業系統平臺下，各式功能強大的應用軟體的效益時，自然不可能再回到從前，使用大型主機及終端機的時代。

不過大家都知道，使用者大部分的作業不會是做基因組合、核爆分析、氣象預測或是計算土星軌道等等需要高速運算的作業，國軍人員的資訊作業，大部分使用的是文書處理器、試算表、簡報軟體、電子郵件，或是一些行政後勤相關的應用程式，他們所需要的只是一部系統穩定，滿足作業需求效能的硬體平臺，而非配備勁爆、功能強大的萬能法寶。

因此，面對一項資訊工作平臺選擇時，符合國軍多數人員資訊作業的要求是什麼？一個大而明亮的螢幕，快速的處理器？超大容量的硬碟？還是超大容量的記憶體？無數的研究報告顯示，新電腦的價格僅佔總持有成本(total cost of ownership, TCO)很小的一部份。支援、維護以及其他無形的成本，才是整體總額的負擔。<sup>註士</sup>然而安全因素對國軍硬體採購選擇，才是更為重要的考量。

低成本、高安全的資訊硬體環境建置準則是：「除了滿足工作所需，其餘功能全部不要或完全管制」。因此，硬體採購與建置必須考量的因素則包括；合理的價格、確實的效能、作業系統完備、採購與使用的簡便性、穩定的平臺、良好的服務與支援、<sup>註士</sup>以及更能確保資訊安全的架構與管理介面。

一項被稱為精簡型電腦(Thin Client)概念的資訊作業環境，相容於現行市售的套裝軟體，除了可以滿足工作需求，降低維護管理成本之外，更能提高資訊安全管制程度，這對資訊安全高度要求的國軍單位，似乎更加

<sup>註士</sup> 樂斌審閱，林妙玉譯，管理資訊系統概論（臺北，美商麥格羅·希爾，民國92年6月），頁82-83。  
(O'BRIEN, Introduction To Information Systems: Essentials For The E-Business Enterprise, 2003)。

<sup>註士</sup> 同註士，頁82-83。

具有採用的誘因。

## 伍、精簡型電腦(Thin Client)概念的作業環境

### 一、何謂精簡型電腦(Thin Client)？

精簡型電腦(Thin Client)也稱為輕量級用戶端（如圖一），或網路電腦(Network Computer)，相較於一般常見的全功能PC的重量級用戶端(Fat Client)，Thin Client 沒有硬碟機、光碟機與軟碟機，僅配備嵌入式功能簡單的處理器及記憶體，所有運算或服務均需透過連上網路伺服器才能運作，是一種封閉、低價的聯網微電腦。<sup>註五</sup>

圖一 精簡型電腦(Thin Client)



資料來源：惠普網站，<http://www.hp.com>。

### 二、Thin Client的優點

採取Thin Client環境的優點有(一)較低的管理成本；(二)較易達成安全目標的作業環境；(三)較低的硬體成本；(四)較低的能源消耗；(五)不易成為竊賊偷竊的目標；(六)可運作於較惡劣的環境；(七)更低的網路頻寬需求；(八)更有效益的資源運用；(九)更簡單的硬體升

級途徑<sup>註六</sup>；(十)管制使用者可操作之軟體等。各項優點分述如后：

#### (一)較低的管理成本

由於用戶端並不儲存軟體，所有用戶端的軟體需求，均由伺服器端設定、管理與服務，因而沒有因為使用者不當使用，導致用戶端系統故障所引發的請修需求，並且因為整體系統的使用環境受到嚴密的管制與保護。使用者不當使用各種不同版本軟體所造成的困擾也得以免除，單位可以更快速的同步進行系統版本的升級，使得作業更有效率並且簡化管理成本。

在採用了Thin-Client之後，國軍為了防範使用者私自拆解主機，要求於機殼接縫處張貼封籤的特殊作法，也可以免除，省卻了相當的管理成本。

#### (二)較易達成安全目標的作業環境

由於用戶端沒有硬碟機、光碟機等輸出、入裝置，使用者無法將資料複製攜出營區，也無法將不明軟體存入電腦中使用，雖然部份Thin Client設備具有資料輸出、入功能的USB介面，但這些介面可以透由伺服器端設定，將該項功能關閉，並在允許下進行開放，而達到確實的資料管制效果，這比現行部分單位，將硬碟機撤除、透過外力封鎖USB介面的作法，更加經濟有效。

另外由於用戶端完全沒有儲存任何的應用軟體或資料，所有的資料均存放於伺服器端，使得資料儲存安全受到更為嚴密的保護。由於這些安全特性，越來越多臺商在中國大陸佈局生產據點，在需要保密產品設計圖、財務人事資料等情形下，能將上述資源留在臺灣或者第三地後端主機。採取避免電腦連同資料被人攜走的Thin Client架構，已

<sup>註五</sup> 同註四，頁87。

<sup>註六</sup> Wikipedia-"Thin client", Wikipedia — The Free Encyclopedia, [http://en.wikipedia.org/wiki/Thin\\_client#Advantages\\_of\\_thin\\_clients](http://en.wikipedia.org/wiki/Thin_client#Advantages_of_thin_clients).



成為臺商部署電腦系統的首選。<sup>註五</sup>

### (三)較低的硬體成本

為何Thin Client架構的硬體成本較低？原因是Fat Client的用戶端仍舊是個人電腦的硬體架構，個人電腦的CPU運用在大部分時間是處於閒置狀態，個人電腦若有餘裕的記憶體及硬體空間也無法提供其他使用者分享與運用，因而形成浪費。但是Thin Client的環境中所有應用軟體只需儲存一套在伺服器端，提供授權後的使用者分享使用，所佔儲存容量僅為一套軟體的空間，而在Fat Client的環境中則必須每部PC都安裝一套才可以運作。

Thin Client架構中，用戶端僅配置功能簡單的處理器及記憶體，而這些原來個人電腦所提供的資料儲存、運算等服務，均由伺服器調度整體資源，執行最佳化的服務分配作業，因而可以充分利用所有硬體資源，使得投資的硬體成本發揮最高效益。

### (四)較低的能源消耗

近來全球暖化以及能源枯竭，已經成為大家關心的議題，減緩全球暖化最直接的方式，就是採用節能設備、採取節能措施或使用替代能源，雖然國軍的任務在於保護國家安全，但國防部是行政院的一個部會，自然不能自外於國家的環保政策。

由於Thin Client精簡的硬體架構，因此耗電極少，同時因為產生的熱能較少，相對的減少辦公室的冷氣用電需求。對於受限於用電契約容量限制，夏日用電尖峰時，經常必須切換備用電力以因應電力負載的國軍營區而言，不啻是一項正面的利益。

### (五)不易成為竊賊偷竊標的

相較於企業，國軍對於門禁管制及各

項裝備的管理已經相當嚴密，卻還是無法避免資訊裝備失竊事件的發生，失竊的標的主要是個人電腦及筆記型電腦。電腦失竊，除了有形財產的價值損失外，影響最大的還是存放在失竊電腦裡的資料。事故發生後單位必須針對事故進行檢討、調查、懲處以及研擬改進措施；上級單位更可能對下級單位進行一波全面的檢查與督導，這些活動所花費的成本，可能遠比被竊的電腦要來的高出更多，但是這些行政活動卻又無法避免，因此，減少電腦失竊率，對國軍具有減少行政成本的價值與意義。

由於Thin Client的用戶端無法獨立運作，必須連接伺服器並且在伺服器進行相關設定才可以使用各項軟體，因此，這類設備不易成為宵小覬覦的對象；用戶端也沒有資料儲存裝置，縱使設備失竊也僅是硬體價值的損失，無關資料洩漏的問題，因而免除了資料安全危害的風險。

### (六)可運作於較惡劣的環境

個人電腦主機內大部分零件均可以拆卸與組合，機體的運作尚需透過風扇加以散熱，並且必須放置於溫、溼度及環境穩定的辦公處所中使用，否則設備容易損壞，但是Thin Client用戶端是密封式裝置，不具可拆卸的零組件，也沒有硬碟，因此，無須擔心震動所造成的硬碟磁軌或磁臂損壞問題。較能使用於溫、濕度條件較差，或顛簸的作業環境中，另外由於設備輕薄短小，更可輕易的附掛在任何空間要求的工作環境，<sup>註六</sup>這項優點對於必須經常航行於海上、處於顛簸、惡劣海象及狹小艙間中，進行資訊作業的艦艇單位更具價值。

### (七)更低的網路頻寬需求

<sup>註五</sup> 曠文濤，「精簡型電腦第二春：臺商市場」，科技資訊網，民國95年11月23日，<http://taiwan.cnet.com>

<sup>註六</sup> 力聖資訊網站，"Winter Thin Client S30",<http://www.leagen.com.tw/touchmaker/front/bin/ptdetail.phtml?Part=m5s30&PreView=1>

在Fat Client的架構中，如果用戶端開啓了儲存於伺服器的一筆檔案，假如這個檔案有10MB，則資料必須透過網路將這10MB的資料由伺服器傳送至用戶端，相同的如果使用者開啓了該筆檔案，要儲存資料時也必須將10MB的資料送到伺服器，因此，這種作業方式非常消耗網路頻寬，常常因為頻寬不足而造成網路擁塞。

在Thin Client架構中，無論是檔案開啓、運算、儲存等作業都是在伺服器端完成，並且僅於滑鼠、鍵盤及螢幕更新畫面時，才需進行資料（命令）的傳送，所需消耗的頻寬極少，在低於5kbps的頻寬下便可以運作，<sup>註六</sup>這對於營區較為分散，不易全面建構高頻寬光纖網路，仍舊使用著老舊、高阻抗傳輸線路的部隊而言，Thin Client低頻寬的運作特性，將使得國軍的連線上網率得以提高，更容易達成全面建構Intranet的目標。

1999年，美國陸戰隊在一項代號為

圖二 美國陸戰隊在一項代號為「城市戰士」(Urban Warrior)的演習中使用掌上型電腦



資料來源：Michael Lutzky, Washington Post, <http://www.washingtonpost.com/wp-srv/national/daily/march99/net6.htm>

「城市戰士」(Urban Warrior)的演習中，陸戰隊某單位所有成員，上起將官下至士兵，對加州海岸發動攻擊，負責進攻灘頭的人員均配備掌上型電腦，能與單位所有成員構連，每一位成員都可以了解戰況（如圖二），<sup>註六</sup>隨著「數位化戰場」來臨，透過網路連結執行C<sup>4</sup>ISR的方式，將對戰技、戰術、戰法產生革命性的改變。

這種新作戰方式，應為國軍所仿效，民國94年8月的臺北國際航太展中，陸軍通校就展出以CTM-218多波道無線電機為基礎，結合民間公司開發的多工器(MUX)研發出寬頻傳輸系統，傳輸頻寬可達2048Kbps，可傳送視訊、數據及語音訊號。<sup>註九</sup>成為未來國軍陸地單位發展戰場管理系統的重要工具。

當國軍戰場管理系統完成建置，有關C<sup>4</sup>ISR的任務，將可能透過光纖、數位微波、高頻、特高頻無線電機、衛星通訊等裝備所構成的傳輸載體互為構連<sup>註十</sup>，並且必須考量平戰結合，納入軍、公、民、警用多環備援線路，以因應戰損時的設施損壞，提高接通率。

一項研究指出，戰爭時C<sup>4</sup>ISR系統常是敵人攻擊的首要目標，所以如何有效保護C<sup>4</sup>ISR系統是一個重要的課題。保護C<sup>4</sup>ISR系統的方法有二：其一是以實體火力提供外來的保護。其二是以「虛擬化」達到自我保護。以聯合後勤資訊系統為例，原來的軟體架構如附圖三，但是這種資訊系統只要核心被攻擊或破壞，即使線路正常，該系統也無法提供作戰支援。<sup>註二</sup>

註六 同註四。

註六 Joel Garreau, "Point Men for a Revolution, Can the Marines Survive a Shift from Platoons to Networks?", Washington Post, March 6, 1999; pp A1, <http://www.washingtonpost.com/wp-srv/national/daily/march99/net6.htm>

註九 郭乃日，看不見的臺海戰爭，（臺北，高手專業出版社，民國94年5月），頁80-87。

註十 同註九，頁82。

註二 高煥堂，「如何保護C<sup>4</sup>ISR系統？」，TASA協會研討會講義，民國94年9月27日，<http://myweb.hinet.net/home8/misootw/c4isr.htm>



因此，該研究主張，Sensors、C2與Actors等作戰單位是分散的、資訊也是分散的，所以軟體元件也分散於各地分別管理當地的資料，然後透過網路溝通交換、互通有無，如圖四。包括實體作戰單位，或是像聯兵旅等臨時快速建立的虛擬作戰單位(virtual entities)，都能夠輕盈敏捷地"plug and play"到「虛擬化」C<sup>4</sup>ISR系統上。<sup>註三</sup>

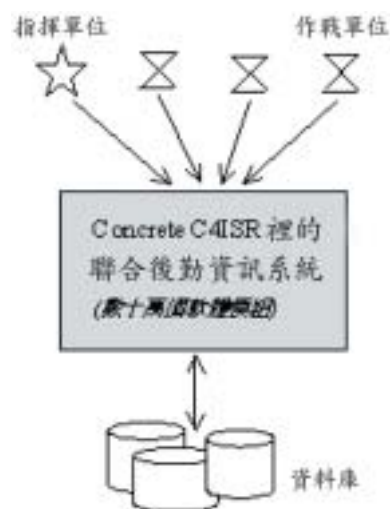
然而，資訊優勢是脆弱而不易維持的<sup>註三</sup>。上述研究所提出的架構，必須確保連接各虛擬系統的通訊線路高度妥善，因此，適應低頻寬的運作特性便極具價值。當通信設備成為敵人優先攻擊目標，各種通訊線路被破壞殆盡時，戰場資訊無法被即時反應，戰場共同圖像失真，將導致指揮官無法執行最佳的決策。

Thin Client只要低頻寬，就能順利作業的特性，使得戰時的連線妥善率更高，確保戰場共同圖像的完整性，使得戰場取得的情資、使用情資的決策人員、以及執行政策的行動，三者之間有幾近完美，毫無罅隙的連結，因而成為一項資訊優勢。<sup>註四</sup>

#### (八)更有效益的資源運用

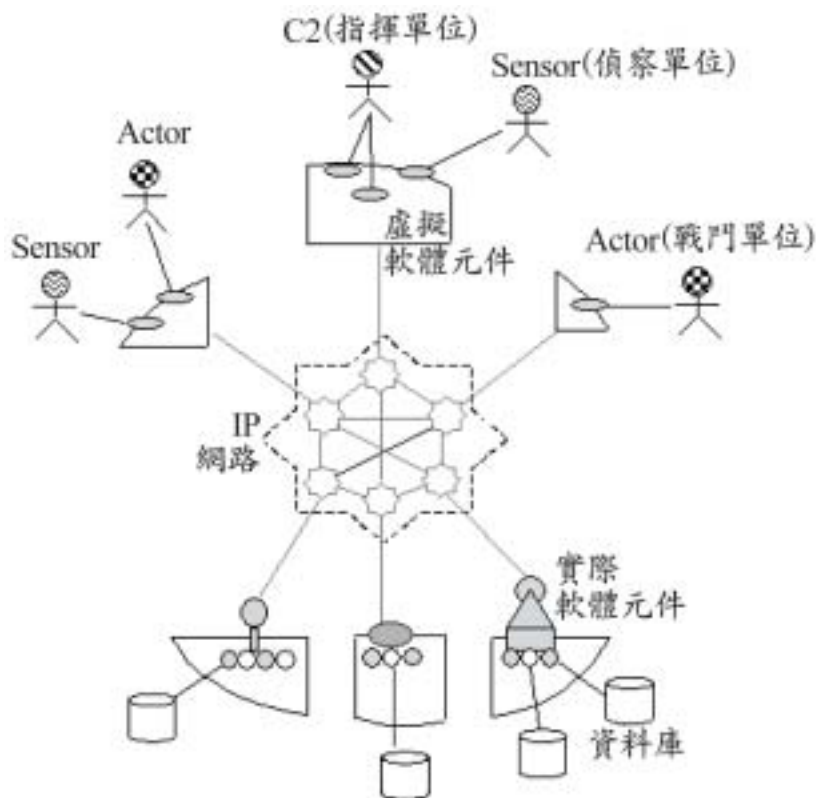
相較於Fat Client架構，CPU運算、記憶體、硬碟機等資源均分散於個人電腦中，即使閒置也無法充分利用，Thin Client則全面集中於伺服器中，真正達到軟、硬體資源分享的目標，因此，具有最佳的資源使用效益。

圖三 未虛擬化的聯合後勤資訊系統



資料來源：高煥堂，「如何保護C<sup>4</sup>ISR系統？」，TASA協會研討會講義，民國94年9月27日，<http://myweb.hinet.net/home8/misootw/c4isr.htm>。

圖四 虛擬化的聯合後勤管理系統



資料來源：高煥堂，「如何保護C<sup>4</sup>ISR系統？」，TASA協會研討會講義，民國94年9月27日，<http://myweb.hinet.net/home8/misootw/c4isr.htm>。

註三 同註二。

註三 國防部史政編譯局譯，戰爭新風貌：二十一世紀作戰方式（臺北，民國92年10月），頁88。（Bruse Berkowitz, The New Face Of The War: How War Will Be Fought In The 21th Century, 2003）

註四 國防部史政編譯局譯，資訊革命與國家安全（臺北，民國90年3月），頁67。（Thomas E. Copeland, The Information Revolution And National Security, 2000）

#### (九)更簡單的硬體升級途徑

單位內只要進行PC升級作業，在資訊部門中不論是程式設計、資料庫管理或是網路管理人員，均可能全部必須投入PC主機的換裝升級作業。

在Thin Client架構中，提升作業效能，卻不需要更動用戶端的硬體設備，而是提昇伺服器主機的效能便能完成任務。當單位電腦使用人數日益增加，或是因為伺服器主機老舊，不足以滿足作業負荷，而必須新增或提升設備等級時，只需增加伺服器主機，新加入的主機便可以並聯運作並降低負載，全體的終端使用者可以立即感受到效能提升的效果。軟體的升級也極為簡單，只要在伺服器端安裝好新版的軟體，並完成所有使用者的教育訓練，當用戶端連上新環境時，即可使用新版本的軟體服務，因此Thin Client的軟、硬體升級方式更具效率。

#### (十)管制使用者可用之軟體

在Thin Client的環境中，使用者使用軟體將受到管制，使用者再也無法將軟體安裝在用戶端的平臺上，所有軟體使用需求必須提出申請，由伺服器管理者授權開放使用，這種方式與大型主機對使用者使用軟硬體資源的管理方式完全相同。因此，Thin Client兼具了大型主機封閉式作業的安全特性，以及相容於個人電腦各式功能強大軟體的優點。

當一個單位開始全面採用Thin Client架構，經過一段學習曲線的熟悉之後，預期單位資訊管理成本開始下降，安全品質迅速提升。由於Thin Client架構所有的管理與服務幾乎在伺服器端完成，用戶端只要嚴守保密自己的帳號與密碼，所有資訊安全防護作為在伺服器端即可完成，用戶端硬體不易損

壞，即使損壞，立即更換便可隨插即用(Plug And Play)，完全不需要任何設定。來自使用者的需求，僅有零星的新進、離退人員的帳號管制、或是少數網路磁碟空間增加的請求，原本來自用戶端的零件損壞、性能升級、軟體衝突、參數設定、BIOS密碼被鎖、中毒、資料損毀等請修需求，因而降至最低，零件備料的採購與管理也相對持續精簡，對各單位的資訊安全檢查似乎也可以省略，資訊人員於是具備較為充裕的時間，得以充實更多推陳出新的資訊技術，或是提供更多的資訊服務，換言之資訊部門可以擴大服務的範圍。

整體的效果是單位資訊維護管理成本降低、資訊安全提升，資訊部門專業人員壓力得以紓解。這種技術改變，所帶來的效益，同時也引發了組織變革的機會。

### 三、推廣Thin Client架構的限制與解決之道

上文列舉了Thin Client架構的十項優點，然而精簡型電腦卻沒有大規模的被政府部門及多數企業所採用，理由何在？以下分析Thin Client架構的限制，並針對各項限制，提出解決的辦法作為參考。

#### (一)與個人電腦價差縮小

以個人電腦為架構的桌上型電腦或筆記型電腦，仍是家用資訊硬體的主流平臺，幾乎成為個人需求用途的不二選擇，由於規模經濟所形成的低成本因素，以至於縮小與Thin Client終端硬體的價差，當PC價格逐漸下滑，讓精簡型電腦喪失價格優勢的情況下，精簡型電腦始終難以進入一般的辦公室環境，停留在諸如客服中心等利基市場。<sup>註五</sup>不過重視高度安全的國軍而言，這些因素不應成為重要考量，而影響國軍對於Thin Client架構的推行評估。

註五 同註五。



## (二)自行開發的系統無法順利運作

一般市售套裝軟體大都可以在Thin Client的環境下順利運作，但是自行開發的軟體，由於程式設計師未能遵從相關技術規範，因而無法相容於Thin Client的作業環境，此時如果硬體代理商技術支援能力薄弱，無法解決單位的問題，將造成Thin Client導入失敗的結局。

解決的方法是在採購合約上，要求得標商必須同時解決單位已上線的系統，得以在Thin Client環境下正常運作，因此，單位進行採購計畫時，便可選擇技術支援能力良好的廠商，進行全系統測試與程式修改評估作業，廠商因為必須了解自我得標後的履約能力，與後續商業機會，而願意進行免費測試與評估，以免得標後無法履行合約。因此，良好的合約規範，更能確保參與競標商，都具有相當的技術支援能力，大大提升了新架構導入的成功機率。

## (三)部分單位資訊能量不足

雖然國軍電腦的使用已經相當普及，但是部份基層單位，因為資訊人員專業能力不足，日常的資訊作業可能處於高度風險的環境中，這些單位若要推動Thin Client架構，在沒有專業人員或完成伺服器各項安全措施前，貿然施行可能承擔更大的風險。

解決的方式是，這些單位僅負責提出使用需求，所有資訊服務由更專業的資訊單位負責提供，這些基層部隊在無須增加資源投入情形下，便可以完全享有高度安全的資訊作業服務。換言之，基層部隊的資訊人力及預算將被整併，以獲取更優質的資訊服務。

這其實只是一種委外的概念。除了資

訊作戰是國軍必須確保的作戰能力外，更多的資訊作業對於多數單位而言，只是一項後勤支援工具而非核心任務。將非核心任務委外處理，不是能夠讓各個單位更加專注於核心任務的執行嗎？

## (四)使用者對變革的抗拒<sup>註六</sup>

PC對於使用者而言除了是一項工作的利器之外，它所配備的軟碟機、光碟機、燒錄器、USB介面及各式軟體等，對使用者而言則更像是一部酷炫的多功能遊樂器，或許我們並不反對，上班時間一邊工作一邊聽音樂，可以提升工作效率的論點，尤其對於以工作場所為家的部隊單位（例如艦艇），PC更有理由成為一項紓解壓力的視聽娛樂裝備（文康器材），因此，當一部「多功能遊樂器」被換成，只能工作而且所有軟體需求、輸出入介面完全管制的「小鐵盒」時，使用者的心情可想而知，這項資訊設備將變得不再可愛。因此，使用者對於變革的抗拒也會影響專案的推行成效。

一個變遷催動者(Change Agent)可能是組織的一個內部成員或外部顧問。<sup>註七</sup>在資訊組織的內部成員中，能夠扮演變遷催動者只有三種角色，分別是主官、資訊主管及承辦參謀。其中以主官所引導的變革意志最為強大，而資訊主管及承辦參謀所發起的資訊變革，往往可能因為工作熱情不敵同儕壓力而草草收場。具有資源分配權力的幹部必須具備一定的理想性與抗壓性，洞察使用者對於硬體的需求是源於「想要」還是「需要」，在滿足使用者工作需求、成本與安全上，採取更為適當的選擇。

## 陸、結論與建議

<sup>註六</sup> 李茂興、李慕華、林宗鴻譯，組織行為（臺北，揚智，民國87年1月），頁377-411。（Robbins, Essentials of organizational behavior, 1992）。

<sup>註七</sup> 張潤書編譯，組織行為與管理（臺北，五南，民國74年1月），頁621。

## 一、對國軍的建議

### (一)採用Thin Client架構，提升資訊安全

由國防部進行全面性評估，形成政策之後，要求所有單位，新購個人電腦升級需求改由精簡型電腦取代，初期採取個人電腦與精簡型電腦混用方式，直至單位所有個人電腦汰除，在個人電腦未汰除前，必須完全封鎖或去除輸出、入介面，以達管制之效。另一項方式則是由軍種檢討施行單位優先順序，從高度機敏作業單位先行使用精簡型電腦，該單位原有之個人電腦則撥轉其他單位運用，逐步完成換裝作業。

### (二)整合所有資訊服務與資源，精簡伺服器數量

在管理資訊資源時，究竟讓所有的服務分散在許多小型伺服器上，還是將所有服務集中在少數功能強大的伺服器中？至於何者較為正確，可能會激發多方觀點與辯論，前者可以避免將所有雞蛋放在同一個籃子裏，因而分散作業同時中斷的風險，但是卻可能形成投資浪費，運作效益不彰；後者可以發揮最大資訊運作效益，但是主機萬一中斷服務，那可就不是一件小事情。

許多企業以往在全組織內的電腦網路中，置放許多小型伺服器電腦系統的作法，現在已經完全改觀，取而代之，他們正逐漸削減區域伺服器的數量，並且將許多伺服器的功能，整合成數量較少的大型網路伺服器，以便集中管理，<sup>註六</sup>發揮較高的經濟效益。國軍目前的資訊系統環境，則是建置在許多小型伺服器上，並且由各單位所屬的資訊部門管理與維護，以致於運作效益不彰。

管理學者Porter認為，達到低成本優勢的主要來源有三，分別是經驗曲線(Experience Curve)、規模經濟(Scale Economies)和

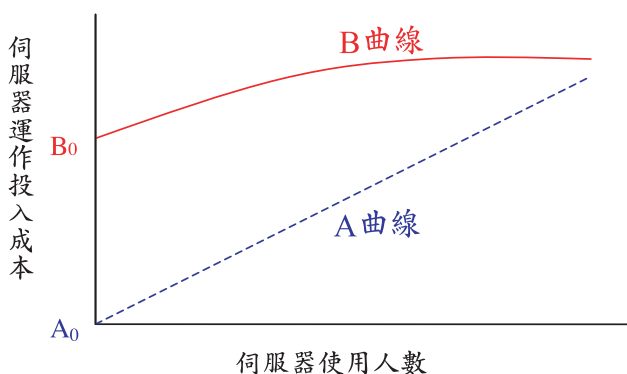
專業化(Specialization)。<sup>註六</sup>而國軍資訊資源運用則存在，諸多未達規模經濟的成本浪費情形；任何一個具有資訊部門的單位都有專人管理各式伺服器，不過所服務的人數最多不過數百人，因為資訊人力分散，以致資訊服務未達規模經濟導致資源浪費。

圖五可以進一步的說明此種現象，即便只要滿足一個使用者的需求，便必須投入相當的學習成本與軟硬體建置成本（如圖E中A0至B0線段），服務的人數愈多，單位成本愈低，因此，現實狀況中，資訊資源運用效益曲線是圖中的B曲線，而非A直線。然而影響所及尚不止於此，因為人力分散，以致無法有太細的分工，因而增長了學習曲線，同時降低了資訊人員的專業化程度。

Thin Client架構可以提供跨單位的資訊服務需求，達到符合規模經濟的成本優勢。當資訊組織重整，資訊人力集中一處提供服務，面對來自不同編制單位使用者的資訊服務申請，管理人員可以在伺服器端完成設定，而不需派出人員到達用戶端處理，由於服務的對象跨越了單位編制的藩籬，使得伺服器管理人員，原先所能提供的作業量由數百人提升至數千人。

因此一個地區基地內，如果存在20個

圖五 伺服器使用人數暨投入成本關係圖



資料來源：本研究。

<sup>註六</sup> 同註士，頁96。

<sup>註六</sup> 方至民，企業競爭優勢（臺北，前程企管，民國89年），頁123。



單位設有伺服器，卻僅有10個單位具有合格的管理人員，整合之後只需編派少數的人員負責例行性的資訊服務，更多的資訊人員可以從事較具價值的活動，由於分工更佳細膩，因而可以達到更高的專業化程度。這種整合使得，原先在資訊安全堪慮環境中作業的單位，安全保障獲得改善，同時伺服器數量得以精簡。由於達到規模經濟、投入成本可以有效發揮，專業化程度得以提升，因此，使得整體資源運用獲得更佳的效益。

另外爲了避免將所有雞蛋放在同一個籃子裏，硬體資源過度集中的現象，目前除了各單位例行的資料備份、分儲作業，已能有效降低風險外，更可以評估建置安全性更高的異地備援系統，以降低系統損壞，服務中斷的危機，而建置異地備援系統，同時也是因應戰損的解決方案之一。

(三)伺服器的設置地點必須考量電子脈衝效應的防護

國軍多數電腦機房大都設置在一般辦公處所內，在進出管制、防震、防火上已經具有相當的防護作爲，但是在戰時，面對電子戰的攻擊將可能無一倖免，因此，機房位址的選定必須將電子脈衝效應防護加以考量。由於伺服器減少並集中，因此，更能易於建構因應電子脈衝效應的防護措施。

(四)結合憑證認證的資料識別機制

國軍多數單位均設有檔案伺服器，提供單位使用者進行公務資料儲存服務，這些資料部份可能具有機密性，但是目前國軍所採取的保密機制，僅爲網路系統所提供的帳號結合密碼予以識別。即使伺服器上的網路

作業系統可以針對使用者密碼設定，強制要求設置較高程度的安全規範，例如：密碼長度、文數字混合等避免被猜中的風險，這些機制對於保護具有機密性的檔案，似乎仍顯不足。

憑證認證系統具有不可否認性、資料隱密性、資料正確性的安全功能，是國軍應該加速建置的安全機制。<sup>註一</sup>唯綜合成本與安全考量，國軍應該以作業人員所處理的資料機密等級高低，做爲配發智慧卡及讀卡機的優先順序，盡速採用憑證認證系統。除了網路帳號、密碼結合智慧卡的安全機制外，甚至可以增加生物特徵(Biometrics)識別系統(如指紋、掌紋或虹膜識別)加以認證，<sup>註三</sup>以提高資料存取安全。

(五)全面調整資訊人力，重新定義任務

當作戰方式已經改變，資訊戰已經成爲主導戰場勝負的關鍵力量時，國軍資訊人力的員額，卻依然大比率的分配於支援後勤任務屬性的單位中，而凸顯出資源分配的主從錯置，因此，國軍資訊人力必須配合調整並重新定義任務內容。

國軍資訊人力分配不均，可能不只是在作戰部隊增加資訊人力如此簡單，而是國軍所有資訊人力必須全面檢討，並進行大規模的組織重整。國軍目前資訊能量大多集中於後勤單位，主要負責支援性的後勤或管理資訊系統的發展與維護，這些系統包括人事業務資訊系統、國防全程籌獲管理系統、預算執行管理系統等<sup>註三</sup>，相對而言投入資訊作戰相關的人員比率較少，爲了因應解決資訊作戰的來臨，資訊人力必須重新全面加以

<sup>註一</sup> 謝文川，林國良，張永志，羅濟群，「中華民國國軍認證中心之建置——以海軍爲例」，第十三屆國際資訊管理學術研討會，<http://163.25.10.166/conference/第十三屆國際資訊管理學術研討會/pdf/A006.pdf>

<sup>註二</sup> 陳峰棋譯，資訊安全（臺北，麥格羅·希爾，民國93年），頁1-11至1-12。（Eric Maiwald, Network Security: A Beginner's Guide, 2nd Edition, 2003）

<sup>註三</sup> 左寧生，國軍資訊組織與人力發展精進策略之研究，私立元智大學資訊管理研究所碩士學位論文，民國94年6月，頁63。

調整，將多數人力調整至負責備戰及作戰指揮相關之資訊系統中，包含C<sup>4</sup>ISR系統、戰場管理系統、聯戰指揮管制系統、軍事訓練管理系統、用兵後勤管制系統、人力戰備管制系統、情報整合資訊系統、資訊安全防護等，這些系統才是現今資訊部門發展的重點。<sup>註三</sup>

其它一般性的後勤資訊與行政管理資訊系統則可採取委外方式辦理，執行這類任務的資訊人力則保留，系統發展專案管理、系統需求分析、整合測試及驗證及相關法規研修部分<sup>註四</sup>，而將大多數的系統發展、維護委外，調整後的資訊人力將集中於軍種直屬，而非基層單位，以發揮較大效益。

## 二、對業者的建議

雖然Thin-Client已經可以有效杜絕大部分資料隨意輸出、入的弊端，但是對於使用者將私用筆記型電腦，連上國軍網路，違規存取資料的行為，仍然無法管制。

爲了防範此一現象，解決的辦法是，安裝一套可以識別網路內所有連線節點的識別軟體；當未授權或被識別的硬體即使接上網路，也無法正常登入伺服器，同時伺服器可以發出警告訊息告知管理者，哪個節點發生不正常硬體連接現象。如果硬體製造商能夠開發並提供這類管理程式，國軍就能有效防範未經授權的裝備，接上國軍網路的情形發生。包含國軍、政府部門或對於機密程度需求較高的企業，都可能有些類似的安全需求，精簡型電腦的業者，正可以開發此一利基性的功能，滿足顧客需求，達到產品差異化(product differentiation)的目的，以創造競爭優勢。<sup>註五</sup>

<sup>註三</sup> 同註三，頁63。

<sup>註四</sup> 同註三，頁63。

<sup>註五</sup> 黃營杉譯，策略管理（臺北，華泰，民國88年2月），頁237。（Charles W. L. Hill & Gareth R. Jones, Strategic Management Theory, 1998）

<sup>註六</sup> 國防部，「第五章軍事戰略調整」，中華民國九十五年國防報告書，頁94，<http://report.mnd.gov.tw/>。

## 三、對後續研究者的建議

本研究限於篇幅並未針對網路傳輸的加密技術深入探討，然「資訊確保」卻是資訊戰極爲重要的一環，後續研究者可以針對「資訊確保」的方向加以研究。另外資訊組織的重整亦是當務之急，爲了增加國軍投入資訊作戰的資源比率，必須在資訊組織重整之後，方能迅速有效的推動，後續研究者亦可針對全軍資訊組織調整，進行全面的分析與探討，以因應國軍邁入新一代戰爭，並符合國防報告書中所揭櫫的「資電先導、過制超限」的建軍指導方針<sup>註六</sup>。

收件：96年05月04日

修正：96年07月05日

接受：96年07月09日

## 作者簡介

柯國華先生，海軍備役中校，中正理工學院專科74年班、中正理工學院80年班、國立中山大學企業管理碩士。

