



軍事教育

國軍推動數位學習資訊安全考量及因應規劃

助理教授 王玉強

提

要

為因應國軍推動「數位學習」政策，提供符合軍職人員特殊任務型態的數位學習方式，並據以建構符合資訊安全之「數位學習」環境，降低資訊應用的風險，本研究將藉由探討國軍推動數位學習資訊安全考量及因應規劃，提出推動國軍數位學習之資安整體策略之建議，供後續建構「數位學習」作業環境及學習機制之參考，期能有效提升國軍人才培育效益及品質。

壹、緒論

知識經濟時代強調知識為組織最有價值的資產，也使得知識分享與學習的角色更受社會的重視，隨著資訊科技發展及網際網路的日益普遍，數位學習已成為新興學習模式。而透過數位學習，不僅可提高知識的分享性與再利用性，還可突破時間與空間的限制，進行遠距離與非同步的學習。故提供符合軍職人員特殊任務型態的數位學習方式乃成為必然之考量，而建構以遠距數位學習為基礎的終身教育體系，就目前科技發展的成熟度與商業模式而言，網路線上學習已成為學習主流趨勢的一部分。

完善的數位學習規劃，對學習的知識本體所轉化成的數位內容，必須能夠在蒐取、應用及分享的過程，都能在有效的安全環境下進行。國軍推動數位學習，也會面臨各類國防軍事知識轉成數位內容以後的資訊安全問題。因此，規劃推動國軍數



位學習策略時，資訊安全研究須特予重視。

為了解在國軍現有資安問題下，如何安全推動與營運數位學習，本研究將先針對數位學習與知識管理的關鍵、知識管理應用與資訊安全等議題做深入探討，再從「知識」管理作業與資訊安全的使用特性及關係，以及國軍推動數位學習的資安政策，來解析國軍各類組織間，知識蒐取儲存、應用、傳輸及交流等的特性，最後再行說明影響國軍推動數位學習之資訊安全因素與可行因應策略。

貳、數位學習與知識管理關連探討

數位學習是利用電子設備與資訊技術，透過網際網路傳播來協助學習之教學科技。構成數位學習的要素，除了人員，施教者、學習者、教材提供者外，還包含了軟硬體設施等；硬體方面包含了電腦周邊設備、網路設施等；軟體設施則需有數位學習系統、e化教材等。而所謂e化教材乃是將紙本或書面教材內容轉化為可供以電腦呈現的數位教學內容。

數位學習系統中不可缺少的教材庫(Content Repository)，則是透過資料倉儲(Data Warehouse)與文件/內容管理系統(Document/Content Management System)技術，用以支援數位教材/內容之取得與儲存；除了必要之內容分享功能外，教材庫也應包含內容整理、分類、搜尋、查詢等功能，亦即須包含內容管理技術，例如：內容的版本控管功能，確保學習者所取得的數位教材均為最新版本；再者，為便於教材分類整理，也須先適當地定義每一教材及其相關的描述性摘要資訊稱之為「後設資料(Metadata)」，以促進數位教材之共享性與搜尋的便利性。

以目前在數位學習中最受注目與最具權威標準之SCORM(Sharable Courseware Object Reference Model)而言，其所規劃之學習管理系統提供下列七項服務機制(如圖1所示)，其中本地教材庫(Local Content Repository)與遠端教材庫(Remote Content Repository)主在儲存包含有文字、圖片、影像、聲音，資訊等資源學習內容。

- 一、內容管理服務(Content Management Service)：此功能負責提供學習內容的管理，如新增、刪除、編輯及查詢等管理學習內容功能。
- 二、課程管理服務(Course Administration Service)：提供教學者製作課程及管理課程等功能。
- 三、測驗/評量服務(Testing/Assessment Service)：此功能負責管理測驗及評量的題庫，並提供測驗或評量給內容管理服務與傳送服務，將教學內容傳送給學習者。



- 四、學習者檔案服務(Learner Profiles Service)：記錄每個學習者的個人資訊，如帳號、密碼、選修的課程、成績及學習日期時間等資訊。
- 五、順序服務(Sequencing Service)：負責讀入含有教學順序定義的教學清單，依教學所定義的順序，選出適當的教學內容，告訴內容管理服務與傳送服務，將教學內容傳送給學習者。
- 六、追蹤服務(Tracking Service)：此功能負責抓取學習者與學習管理系統互動時的一些資訊，如學習時間、次數、進度及成績等，提供給順序服務與學習內容管理服務決定出適當的學習內容給學習者。
- 七、傳送服務(Delivery Service)：負責把決定好要傳送的教學內容傳給學習者。

數位學習系統主要是用以提供數位教材、散播知識為目的，故多數數位學習管理系統亦具備知識管理之概念與特性，包含分析、存取、管理、分享、演譯與創新知識等程序，提供即時且適當的數位內容與知識，藉以增進數位學習之成效。而圖2說明數位學習與知識管理相輔相成關係結構圖，目的在於有效的應用與創新知識與教材內容，其運作概念說明如下：

- 一、數位學習提供了知識管理中必要之知識分類原則，可使數位學習內容與教材品質穩定且正確；而知識管理則可用以建構數位學習中不可或缺之學習概念地圖

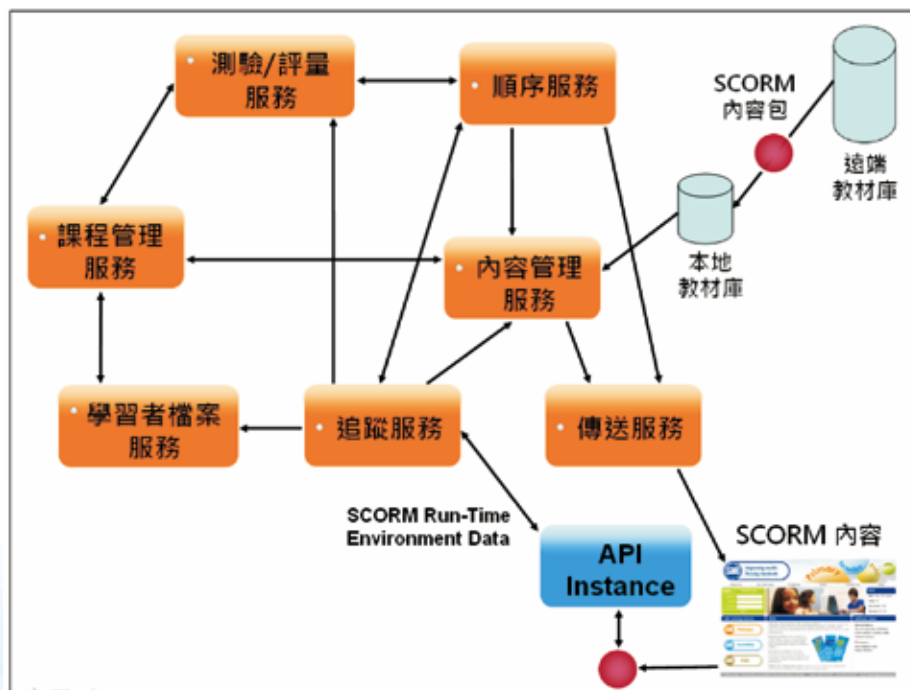


圖1：符合數位學習SCORM標準之數位學習管理平台

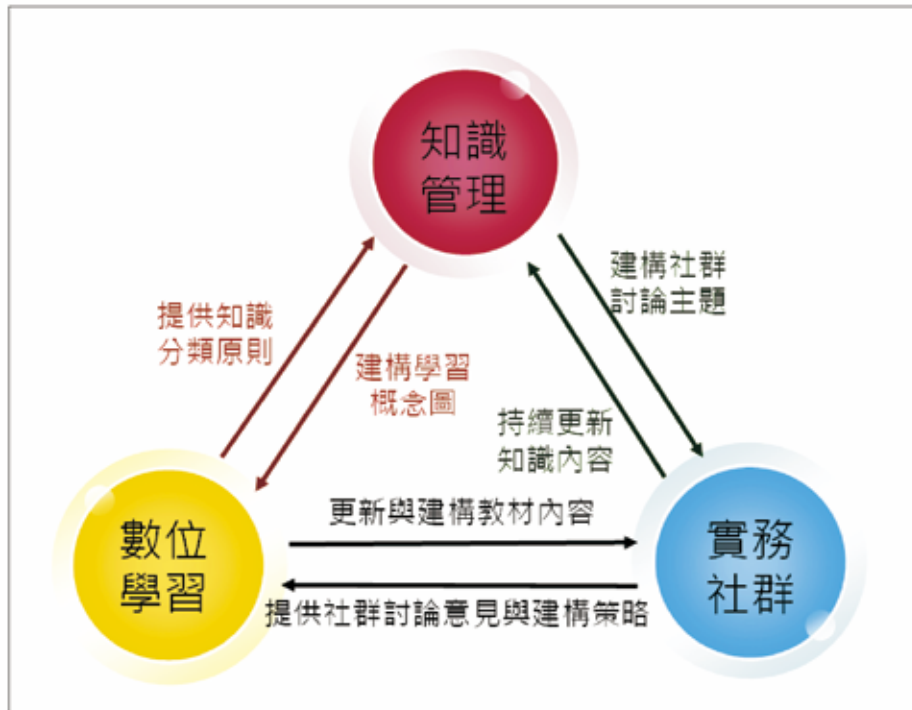


圖2：數位學習與知識管理關係圖

，提供並建議學習者有效之學習路徑。

二、數位學習則供給實務社群更新與建構學習教材與內容之依據；實務社群則能提供數位學習內容作為提升教材內容之參考；而所謂實務社群是為彼此分享專業知識與想法概念所組成之非正式團體，可透過電子郵件或線上討論等溝通方式相互分享概念、經驗、工具或技術等資訊。

三、知識管理則協助實務社群建構並找出討論之主題與方向，並協助推動社群運作；實務社群則能持續更新知識內容。

Senge (1997) 指出未來競爭優勢的來源就是組織所擁有的知識，及組織比競爭對手有更快速學習能力。另知識管理的基礎在於知識分享，組織若要促進內部的知識交流或創新知識，須依靠知識分享之力量 (Liao et al., 2004)。故在國軍教育中，建議可以開發數位學習教材作為分享與傳遞知識來源，有效結合數位學習與知識管理則能提升知識創新與成長，進而帶動國軍各單位提升知識之分享與傳遞效率。

參、資訊安全與知識管理

一、知識管理：如圖3所示，數位學習的作業過程，正如知識管理般，包含四個步驟：知識取得 (Acquisition)、知識產生 (Generation)、知識儲存 (Storing)、



及知識分享(Sharing)；因此，其過程所有資訊(即知識本身)的安全，也就成為數位學習的關鍵因素，因此，重視知識管理安全與重視數位學習安全是一體兩面的概念。

(一)知識取得：

數位學習的開始，在於知識的取得；學習的過程也就是知識的分享與知識的轉移，知識成功移植的關鍵在提供知識者的意願以及獲取知識者接受的手段，此類過程，可分為組織間觀點與組織內觀點來觀察。惟此過程間強調組織知識取得或轉移的重要性，係因國軍推動數位學習，將會存在跨校院間、跨部門間、跨軍種間取得知識、學習與交流，所以數位學習的推動，必須掌握此等特性。組織間的觀點有Norman(2004)的研究，其結果發現，不同組織間，若合作推動數位學習意願高，組織對知識的保護程度會提升；但若組織對合作夥伴的信任度高，組織知識流失的情況及知識保護程度會降低；從合作夥伴取得知識相對容易，或是採取共同擁有及持份的合作關係，也會降低部門知識的流失。Wang et al. (2004)研究結果發現，當各單位擁有豐富的數位化知識，在各單位數位學習者能力越好、合作單位間的關係越好的情況下，各單位會願意擴大知識的轉移。Yli-Renko et al. (2001)探討結果發



圖3：數位學習中知識管理過程與資安考量



現，不同教育或學習單位間，透過雙方關係取得知識會較容易，且對單位內成員學習效益的人際關係互動及線上交流關係提升有助益。此外該研究也發現，社會資本以及人際關係，會影響到知識的取得，進而影響知識發展 (Knowledge Exploitation)。Tsang (2002) 研究發現，有效的監督及管理介入兩個因素，會影響知識取得及學習效果。整體而言，制度化與組織功能往往是組織機構推動數位學習及知識取得的關鍵。Hult (2004) 的研究藉由知識基礎觀點、組織資訊流程及組織學習等三個構面，探討知識創造的過程，結果發現知識的學習與資訊的分享的確存在相關的影響。

綜上所述，在影響知識取得的因素上，若以組織間觀點而言，包括彼此的信任程度、學習的能力、學習的意圖、社會資本、監督的投入與管理的涉入等，都有關連；若以組織內觀點而言，包括制度因素及組織管理的因素、組織既有的知識與記憶等，也是影響學習的因素。

(二) 學習知識產生：

有關於知識產生的文獻，可分為組織內部自行研發及從組織外部取得知識，當組織外部環境有相當多的知識來源時，且外在的環境變動很大時，企業組織(國防組織也不例外)會希望由外部取得知識。不過，如果企業組織擁有許多知識開發的先前經驗且掌握關鍵的知識開發能力時，企業組織會傾向於以自有知識延伸自行發展知識。Young & Baumer (2003) 研究發現，組織間的合作伙伴關係，會增加組織知識的產出。Rodan & Galunic (2004) 的研究則發現，知識的多樣性與社交網絡的多元性，會正向地影響到內部管理的績效及知識創新績效。

組織領導者的領導風格，若是能和部屬進行知識資源交換，將正向影響組織成員的知識學習及創新。Ritter & Gemnden (2003) 的研究則發現，技術能耐及網絡能耐會正向影響知識學習的創新，因此，推動數位學習及知識學習，在作業能量上，擁有數位技術及網路運用技術，會是推動策略成效的關鍵。Farmer et al. (2003) 則提出組織創造力的價值，會與學習創新的角色認同，以及作業相關人員創造力間的互動，彼此呈現正向關連。這也提示我們，在規畫數位學習推動的組織時，作業規劃人力能夠掌握技術發展及應用模式，以及具發揮創新能力特色的組織，會是其推動數位學習成功的重點之一。

綜上所述，影響知識的因素可分為：(一) 環境因素，例如外在環境的動態性、外在資源的豐富性；(二) 企業組織，例如管理者的領導風格、組織



氣候、組織開發知識的能耐及經驗、組織成員的個人屬性；(三)企業組織發展關係屬性，例如網絡關係的數量與強度、網絡關係的多元性及彈性、夥伴間的信任程度；(四)知識屬性，例如知識的多樣性、知識的專屬性等。

(三)學習知識儲存：

任何人學習行為過程中所獲得的知識及儲存的方式，可以分為內化於個人腦中、存於數位資料庫以及轉為外顯化的文件資料中。Bonora & Revang (1991)的研究發現，知識的儲存模式包含：(一)客觀的知識，如文件資料，統計數據及調查報告等，可以讓他人直接分享，進行知識轉移，也就是達到一般學習的效益；(二)主觀的知識，是隱藏的知識或技能，它是公司成功或生存的關鍵，也是學習者將知識理論轉化為實際工作能力的過程，也就是可達成關鍵性學習成果的效益。

Argot (1999)在研究中認為，企業組織成員學習的知識，可以透過個人技術能力的改良，轉變成企業組織的能力提升，再成為組織的資產或專利。此意涵對國軍推動數位學習效果的詮釋即為：當國軍官兵因為有效執行數位學習而達到的知識能力或技術能力的提升，也將會直接反應到整個部隊的運作能力，或是反應在軍事作戰的戰力。此即為知識學習反應在組織經營及運作的實質效力(效益)。另外，知識學習的結果也可以被儲存在組織的管理作為中。Levitt & March (1988)即認為，學員生技術與設備操作的能力水準，也是組織成員學習成果的表現，例如改善組織運作配置的合理性與效率化等。事實上，這些都需要透過學習經驗與知識的累積，改善獲得知識與經驗轉化的組織運作效益(部隊的作業或作戰能力也就自然達到轉換)。Nonaka & Konno (1998)更加指出，組織學習的知識，可以儲存在人與人或部門與部門間的溝通互動平台，也就是數位學習或知識平台上。

綜上所述，在影響知識儲存的因素上，組織中個人的學習為主要知識被學習的儲存內容；透過資料庫的技術，可以協助及擴展知識的儲存，完整的紀錄及分類則可以累積組織的知識；最有效的知識學習記錄，是呈現在個人執行工作或一般作業，或是官兵作戰的能力展現上。簡言之，個人或組織，在個人行為或組織行為的效益改善，也就是個人或組織學習的成果。這就是為什麼本研究要特別強調個人及組織學習行為對國軍組織化推動數位學習的重要性。

(四)學習與知識分享：

數位學習的重要過程，為知識學習的分享，其中的特色則為知識的社會



化和情境化。Jensen & Szulanski (2004)的研究發現，接受者對企業組織成員知識學習的轉移，與個人意願呈現反向關連，而兩個企業組織間制度差異越大時，接受者對組織的成功經驗移轉動機就會越小。Bjorkman et al. (2004)研究則認為，上層組織對下層單位學習績效評估考核及社會化的機制，會對下級單位執行數位學習及知識移轉有相當影響。Chen (2004)研究發現，當企業組織對知識學習的吸收能力越佳時，以及內部單位間的互信與協調關係強度越大時，組織內部知識移轉的績效會越好。Minbaeva et al. (2003)則發現，組織內部成員能力越好及動機越強烈，加上實施員工學員考核機制，會使組織學習的吸收能力越好。而越集權化的組織學習管理、督導架構，組織學習單位間的知識分享程度就越低，而人際關係越好組織分享的程度就高。Tsai (2001)研究發現，組織單位越趨於網絡中心位置時，或某組織單位的吸收能力越好時，組織的創新能力將越能被激發。

綜上所述，在影響知識分享的因素上，大致分為：(一)組織間的因素，如組織間的制度差異、公司績效及社會化機制、知識的屬性以及以知識擁有權等基礎聯盟；(二)組織內的因素，例如：員工的能力及動機、集權化程度及人際關係程度、知識屬性、組織複雜性及文化、組織的距離及經驗等，構成了組織學習與知識管理間的各類關係。所以籌備企業或部隊組織，數位學習既以知識本體為獲得、融合及分享為主，故知識安全與數位學習安全的重要性應屬一致。

二、資訊安全：

推行數位學習之主要目的是為數位教材與內容之傳遞與分享，然而，國軍之教育內容應考量是否有洩漏國家機密之疑慮，並將資訊安全之概念一併納入。所謂資訊安全首要考量是為不安全行為直接造成重要資源的損失及生產力的下降，對於數位學習而言，這些重要資源則為數位學習教材與內容，而生產力則為學習者之學習意願與教材提供者或施教者提供數位學習教材之意願。Sodhi et al. (2004)則指出資訊安全主在防範電腦的資源不被未授權的使用者存取，故國軍推行數位學習策略中，須考量下列四項資源之資訊安全防護：

(一)數位教材與知識內容的安全：針對國軍之教育內容，涉及國家機密之教材則不建議開發為數位內容與教材；而一般之數位教材若考量資安問題，建議可採行數位加密技術；加密及數位簽章技術，可加以強化施教者或是教材提供者在開發與建構數位教材與內容過程中安全的保護機制。

(二)數位學習系統安全：為限制國防資料外流，軍方內部網路(Intranet)與民網



網路(Internet)為資安考量，原則上互不相連，建議可再以實體防火牆(Firewall)加以隔離。

- (三) 傳輸安全：由於數位學習的網路(線上)學習模式進行過程，涉及資訊(知識)傳輸的安全。因此，在資安的考量中，網路建置與傳輸安全為必要的發展考量。
- (四) 管理層面的安全：為防止非軍方人員不正常存取系統資源，對於使用人員可再以IP位址或ID+PW(用戶帳號及密碼)等相互配合，以期解決管理層面中使用者與使用權之資安問題。另建議可使用資訊安全管理系統(Information Security Management System, ISMS)定義出屬於國家機密等不可傳遞與共享之資產，並給予適當的控制措施以保護重要之數位教材與資訊內容。
- (五) 整體環境安全：建議可使用入侵偵測系統(Intrusion Detection System, IDS)加強整體的資訊安全的防護環境。另外，放置系統的機房，在整體環境安全上，亦應重視，納入數位學習整體資安的一部分。

肆、數位化知識學習與資訊安全

知識管理的主要目標是知識創新，透過知識的分享和整合程序創造出新的知識，提升組織競爭力。從知識的取得、產生、儲存、及分享的活動中，組織可以有效地創造知識資產的價值。而知識創新對任一組織而言就是一種資產，和其它重要的企業營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營運、將營運損失降到最低、得到最豐厚的投資報酬率及商機。在知識分享過程中，導入資訊安全機制後，限制了可以使用的對象及方式，然而卻無法進行全面性的知識擴展。

資訊安全管理系統將研發知識管理過程中所使用或產生的知識給予不同的價值，讓知識的流通能受到必要的管制，其知識的價值導致資訊安全管理機制對於知識的管制行為。然而，在導入資訊安全機制後，由於知識或資料的機密等級關係，限制了知識的創造，管制的行為也分別造成研發人員在研發過程中知識取得、知識產生、知識儲存、及知識分享的影響。在研發過程中，跨部門或單位協調在資訊安全管理系統的推行後，無法與其他同仁直接的相互溝通來產生所需要的資訊，由此可以發現到知識管理與資訊安全管理機制兩者是會造成相互間的影響。因此，在進行資訊安全管理系統前，必須先瞭解重要營運流程中所面臨的風險環境，因特定的威脅會利用單一或一群資產的脆弱點造成資產的損失或損壞的潛在可能性。

目前國軍各教育單位，為因應資訊科技普及化，改變了基本知識表達、呈現與



處理方式，也進而推動數位學習以期符合現今發展教育趨勢。為了有效整合教學資源，數位學習科技發展與應用以建立校園數位化學習環境，豐富教學內容以強化師生資訊应用能力，藉以期望可擴大數位教育於正規教育與終身學習上。目前軍事教育訓令在建立數位化、模擬化及網路化之遠距教學及系統包含電腦模擬兵棋教學、視訊會議(含同步遠距教學)、數位典藏、隨選視訊及校園資訊化專案之數位學習平台等不同技術，這些技術的運用，也須同時建立資訊安全的考量。

在考量相關資訊安全因素，國軍導入數位學習平台規範指導中，特別明定數位教材資源共享須依據下列安全原則：

- 一、國軍各單位在發展數位教材之前，應先檢視其他政府機關已發展完成之教材，對於單位適用之教材，應由單位優先協調以交換或贈送方式辦理，以安全方式進行資源共享的方式，取得相關課程，避免投資浪費。
- 二、各單位自民網導入移植之數位教材需先完成檢疫程序，完成惡意程式及弱點掃描等，確認無資安顧慮，並經單位資安長同意後，方可移入軍網使用。
- 三、各軍事單位製作之數位教材，除提供在校生學習外，應逐步規劃開放國軍在職人員運用，並進行資訊安全措施規劃，擴大學習成效。

另外，而在數位平台法規第八條，也明訂了數位學習安全與保密：

- 一、自製、委製之數位教材或課程，完成內容製作後，需經單位保防部門審認無機敏疑慮，簽奉單位權責長官核定後，始可製作開放(上網)使用。
- 二、數位學習服務單位，應秉持服務國軍官兵精神，開放學習平台提供服務，除維護期間外，不得藉任何方式中斷服務(或防火牆阻擋)，並應不定期更新平台病毒碼、漏洞修補程式等，以規劃發展及應用平台符合資訊安全之數位教材或課程。

目前國軍資安政策的限制概略蒐整如下：

- 一、多數單位之保防部門仍無法界定哪些教材內容屬於可共享數位流通教材。(事實上傳送公文資料之機敏分類屬各單位權責，故此項規定實施形同具文)
- 二、為限制國防資料外流，所有軍方單位、校園嚴禁在公有電腦設備使用非經核准之USB存取與流通資料。
- 三、軍方內部Intranet與民網Internet網路為資安考量，亦規定須實體隔離互不相連，導致教官無法離開辦公室，在家中作業時無法獲取軍網資料與更新教材。因此，如何區隔使用公私或可加密的儲存設備，實為國軍欲推動數位學習有待突破之必要作為。
- 四、以國防大學為例：各學院與各兵科校園數位學習平台與網路均為封閉式，互不



表1：影響國軍推動數位學習資安因素與基本解決方案建議

目前國軍資安政策限制	基本解決方案建議
(1)數位內容保密機制，無法界定何種教材內容屬於可共享數位流通教材。	(1)由教材設計者人員明確定義是否該屬於管制資料。
(2)隨身碟USB存取限制。	(2)涉及機敏之資料與教材本不適用於數位學習。
(3)國軍內部Intranet與Internet網路互不相連，教官無法在家中更新教材。	(3)可以實體Firewall加以隔離不適合分享之資源(軍網與民網本已採實體隔離)，再由IP、ID+PW等相互配合確保資安。
(4)各學院與各兵科校園數位學習平台與網路均為封閉式，互不相通，教材亦不同步。	(4)各國軍單位院校圖書館設固定座位與IP可跨校存取專屬數位內容。

相通，教材亦不同步。因此，教材分類分網使用與管理為極需解決問題。

為了克服上述限制對推動數位學習的影響，表1整理出如何在現有資安問題下推動與運作數位學習之建議。國軍未來推動策略的作為中，有關保防部門無法界定教材流通的問題，可應責由教材設計人員或其權責單位定義其分類，至於高機敏之資料與教材，則可歸屬為不適用於網路聯網式數位學習，並使用數位版權(Digital Rights Management, DRM)加密文件，開啟課程須先取得加密金鑰。而USB式攜帶運用問題，應可用安全管制方式避免不當運用而洩密之虞。

而軍方內部Intranet與民網Internet網路已互為獨立且互不相連，導致教官無法在家中處理一般教材之問題，則應可就網路實體Firewall及使用者身分認證及授權隔離非法入侵及不適合分享資源之接觸，再由IP、ID+PW等相互配合來保障資安。最後，就軍方機構與校園數位學習平台的互聯性安全問題，則可改以設立國軍數位學習統一管理的服務中心，扮演中央控管，對國軍各單位院校跨校(單位)存取專屬數位內容時，將取固定地點與IP管制，做為跨校存取跨校數位教材與資源所用之安全管制作為。

伍、國軍推動數位學習資訊安全的因應作為

在上節所提到數位學習克服資安因素的基本策略外，最重要的還是要從數位學習系統與內容的「數位」特性中，尋求可以「技」制「技」的系統性解決方案。此類系統技術的因應作為可以分成針對學習者個人學習行為過程的防護以及數位內容(含機敏資料)來規劃考量，其內容分述如下：

一、數位學習參與者的個資與學習歷程的資訊安全管理：

先管人後管內容是數位學習資安的管理思維。因為人員資料管理的好，就可以防止非法人員接觸資料，進而防止機敏或個人智財權的資料外洩。在機敏資料不納入(或加以管制)數位學習的教材創作及集中管理後，因應國軍內部對



機敏資訊與開放性數位學習的作為間，除一般資安的防範外，數位學習平台管理及人員管理，都須進行安全控管。本研究所規劃之數位學習平台架構間，皆可規劃設計透過中介伺服器(Server)模式，批次與現有國軍相關資料庫等相關系統進行介接，不直接接線，以確保機敏資訊的安全，其系統規劃作法分成下列四個面向：

(一) 管理面向：

1. 慎選系統管理者及使用自然人憑證或動態密碼方式登入管理(入口網站的安全管理詳述於後)。
2. 訂定軍人保密相關規定與制度。
3. 從一般性課程推廣至重要性課程再推到機敏課程。
4. 分工與分散機敏課程儲存位置。

(二) 系統面向：

1. 使用者簽入權限管理，必要時加入個人憑證認證。
2. 課程閱讀權限。
3. 資料庫文件加密管理。
4. 課程分享時間/人員/IP位置管制。
5. 病毒防護。
6. 資料庫備援管理。

(三) 稽核面向：

1. 課程閱讀紀錄。
2. 課程下載記錄。
3. 異常狀況主動通知。
4. 機敏課程存取狀況分析。
5. 使用者使用分析。

(四) 課程安全面向：

1. 使用數位版權加密文件，開啟課程須先取得加密金鑰。
2. 預防使用者按右鍵、Print Screen擷取螢幕畫面等方式將文件取回。
3. 機敏課程限制列印功能。

二、數位學習平台入口授權登入之安全管理作法：

數位學習平台網站的入口，多以身分認證，一般而言大都使用帳號與密碼，如自然人憑證之管控模式，未採用其他技術。故只要竊取到使用者之帳號、密碼，即可進入網站，存取相關資料。雖然，各階層管理單位會一再宣導要定



期更換密碼，並制定密碼選取原則，避免遭人盜用，惟不經意中仍可發現電腦螢幕上、辦公桌旁，張貼個人帳號密碼。目前，較能有效改善的做法為一次密碼(One-Time Password, OTP)認證(或稱動態密碼)等相關技術，國軍推動數位學習的資安策略，基於有相當比率的數位內容或使用人員具有機敏性，因此，要求使用者採用此OTP的安全管理機制，應予實現及採用。

本研究建議，針對國軍數位學習參與人員的身分認證可規劃採取此最新的入口平台安全管理登入的動態密碼技術。動態密碼顧名思義是一次性密碼，意味者每次使用時密碼都不一樣，可確保系統使用者能在授權下安全登入，並提升整個數位學習系統的安全。

一次性使用的動態密碼技術，目前已大量使用在銀行客戶網路轉帳的身分核對使用，其最主要原因是使用方便，客戶接受度高，安全性強。因此，在國軍的數位學習平台網站上若使用動態密碼技術，也可以減少資安事件發生。

數位學習平台使用動態密碼後，對於國軍各單位原有發展不同之資訊應用系統，當目前必須重複登入的困擾獲得改善，亦即當國軍數位學習OTP系統也同樣導入其它的資訊系統登入管理功能，則可同時發揮相同安全效益，不會造成重複投資。

因此，使用一次密碼驗證技術，對使用者(官士兵)而言，可以不用記憶多組密碼，避免密碼洩漏或遺忘，減少官士兵作業負擔，並促進資訊安全；對系統管理人員而言，可大量減少因使用者忘記密碼，無法進入系統所造成過多人為疏失之處置作業，系統管理人員可專心致力於系統維護調校工作或處理突發狀況，有效提高系統管理人員之作業效能。此項多效的資訊安全作為，可以依數位學習推動的短中長期目標，配合推動如下：

(一)短期目標：

1. 以數位學習系統為主，建利OTP網站登入的安全管理。
2. 防止帳號、密碼被竊取的問題。
3. 進行後續與國防部入口網站及公文流程系統整合。
4. 結合Single Sign On機制。

(二)中期目標：

1. 全面實施國防部轄下各應用系統之資訊安全之檢視與認證。
2. 全面推廣資訊安全教育。

(三)長期目標：

1. 建立國軍專屬動態密碼驗證中心。



2. 資訊安全認證拓展至國軍各類綜合性管理資訊應用系統。

三、數位內容安全管理：

數位學習在採取線上服務的模式中，其接觸的數位內容，所涉及個人/機構版權及機敏性安全的作法，則可採取版權管理的概念解決。

Internet(網際網路)是一個開放的網路，其快速發展下負面結果就是嚴重的網路資料安全問題和數位內容的版權問題。那麼如何解決網路內部的安全，防止國軍的機敏資料或是涉及智慧財產權的資訊取用在非法授權情況下，從網路途徑流通出去，可以採用的方式之一，即為數位內容管理的技術與系統應用。

使用數位內容安全管理系統，對軍中各類機敏資料或智財性個人資料，有加密安全的防護，同時可以提高軍中關鍵文件內容的安全防護能力。同時，在對文件安全保護的基礎上，通過檔案的授權使用，可以有效阻止內部人員洩漏機密資訊，防止竊密事件發生，而且一旦發生竊密事件，管理者能夠通過日誌審察功能，詳細追查到竊密人員、檔案資訊、途徑等資訊。

數位內容安全管理系統實現對共用檔案或資料夾更細項的權限劃分管理。在用戶、權限和內容之間建立關聯，用戶擁有權限，權限作用於內容，用戶使用內容，將三者緊密地結合。其主要功能可包含：

- (一)通過對共用檔案使用許可權的設置，靈活的實現對共用檔案「唯讀」、「列印」、「複製」、「編輯」、「完全控制」、「貼上」、「有效時間」、「失效時間」、「使用次數」、「列印次數」等細部權限的控制，以及相關權限之間的組合。
- (二)檔案或資料夾在共用和分配權限的過程中，不會改變原有檔案傳輸和共用方式。
- (三)利用數位內容安全管理的檔案權限管理功能，對檔案共用進行權限設置，不會改變用戶原有的檔案共用的操作習慣。
- (四)對於使用權限，可以加入時間的限制，對共用檔案的權限有相應的使用時間限制，根據檔案的機敏性與使用者的權限不同，DRM系統則可以提供完整的管理功能，讓系統所設定不同的權限及使用狀況，例如讀取、修改、列印等多種權限。在作業過程中，DRM系統會自動記錄用戶使用狀況，從而防止使用者之間非法複製、拷貝、對外發行、光碟拷貝，並杜絕了使用隨身碟、軟碟、光碟，電子郵件等方式竊取數位學習系統資料或知識庫中的資訊/知識/機敏教材方案/作戰演習兵棋推演資訊，以及所有參予各人的相關資料等重



要內容，可達到「事前有防禦、事中即時控制、事後審計追蹤」，並為國軍數位學習的運作提供完整的內容保護。

- (五)個人使用系統權限管理：權限修改技術能夠使已經授予用戶使用檔案的權限立刻解除，防止人員離營或轉調後將內部重要資訊外洩。刪除用戶，取消登入伺服器的權限。當離營和轉調人員的權限被回收之後，將無法登入伺服器，從伺服器端下載檔案。以前能夠閱讀和使用的檔案不能再打開，即使打開看到的也是密文無法解讀，防止了洩密。同時伺服器端及時控制已經被下載檔案的使用權限。

數位內容安全管理乃順應網際網路應用普及時代對網路安全的新資訊安全技術。通過數位內容安全管理的應用，國軍推動數位學習環境的運作管理，將可以有效管理官兵的網路行為，保障網路資源合理使用，避免人為的網路安全憂患，擁有更加安全的網路環境，從而利用網路創造更多學習與知識應用分享價值。

陸、結語

國軍要推動數位學習政策，策略思維上，必須將數位學習環境的建立與區分所屬管制資料等工作同時展開，要用「政策、作為、投資、系統建立、管理考核機制、以及善用資訊通信技術，加上國防資訊安全法規與管理措施」等，來建立適合我國國家環境以及國軍整體環境與使用需求的數位學習環境，也才能支持後續推動數位學習策略的有效執行。在顧及國軍資訊安全規範之前提，藉由引進完善的數位學習內容及管理平台，可將無關軍事機密之教育、訓練、職能等長期典藏運用與分享，未來自可完善應用於國軍數位學習，並可行永續經營之效。

柒、參考文獻

1. rgote, L. (1999). Organizational learning: Creating, retaining and transferring knowledge. Boston: Kluwer Academic Publishers.
2. Bj rkman, I., Barner-Rasmussen, W., & Li, L. (2004). Managing knowledge transfer in MNCs: The impact of headquarters control mechanisms. Journal of International Business Studies, 35: 443-455.
3. Bonora, E. A., & Revang, O. (1991). A Strategic Framework for Analyzing Professional Service Firms-Development Strategies for Sustained Performance. Strategic Management Society Interorganizational Conference, Toronto, Canada.
4. Chen, C. (2004). The effects of knowledge attribute, alliance characteristics, and absorptive capacity on knowledge transfer performance. R&D Management, 34(3): 311-321.
5. Farmer, S. M., Tierney, P., & Kung-Mcintyre, K. (2003). Employee creativity in Taiwan: An application of role identity theory. Academy of Management Journal, 46(5): 618-630.
6. Hult, G. T., Ketchen, D. J., & Slater, S. F. (2004). Information processing, knowledge development,



- and strategic supply chain performance. *Academy of Management Journal*, 47(2): 241-253.
7. Jensen, R., & Szulanski, G. (2004). Stickiness and the adaptation of organizational practices in cross-border knowledge transfers. *Journal of International Business Studies*, 35: 508-523.
 8. Levitt, B. & March, J. G. (1988). Organizational Learning. *Annual Review of Sociology*, 14: 319-340.
 9. Liao, S. H., Chang, J. C., Cheng, S. C., & Kuo, C. M. (2004). Employee relationship and knowledge sharing: A case study of a Taiwanese finance and securities firm. *Knowledge Management Research & Practice*, 2(1), 24-34.
 10. Minbaeva, D., Pedersen, T., Björkman, I., Fey, C. F., & Park, H. J. (2003). MNC knowledge transfer, subsidiary absorptive capacity, and HRM. *Journal of International Business Studies*, 34: 586-599.
 11. Nonaka, I. & Konno, N. (1998). The Concept of 'Ba': Building a Foundation for Knowledge Creation. *California Management Review*, 40(3): 40-54.
 12. Norman, P. M. (2004). Knowledge acquisition, knowledge loss, and satisfaction in high technology alliances. *Journal of Business Research*, 57:610-610.
 13. Ritter, T., & Gemünden, H. G. (2003). Network competence: Its impact on innovation success and its antecedents. *Journal of Business Research*, 56: 745-755.
 14. Rodan, S., & Galunic, C. (2004). More than network structure: How knowledge heterogeneity influences managerial performance and innovativeness. *Strategic Management Journal*, 25: 541-562.
 15. Senge, P. (1997). Sharing knowledge: The leader's role is key to a learning culture. *Executive Excellence*, 14(11), 17-20.
 16. Sodiya, A. S., Longe, H. O. D., & Akinwale, A. T. (2004). A new two-tiered strategy to intrusion detection. *Information Management & Computer Security*, 12(1): 27-44.
 17. Tsai, W. (2001). Knowledge transfer in intraorganizational networks: Effects of network position and absorptive capacity on business unit innovation and performance. *Academy of Management Journal*, 44(5): 996-1004.
 18. Tsang, E. W. K. (2002). Acquiring knowledge by foreign partners from international joint ventures in a transition economy: Learning-by-doing and learning myopia. *Strategic Management Journal*, 23: 835-854.
 19. Wang, P., Tong, T. W., & Koh, C. P. (2004). An integrated model of knowledge transfer from MNC parent to China subsidiary. *Journal of World Business*, 39: 168-182.
 20. Yli-Renko, H., Autio, E., & Sapienza, H. J. (2001). Social capital, knowledge acquisition, and knowledge exploitation in young technology-based firms.
 21. Young, G., Sapienza, H., & Baumer, D. (2003). The influence of flexibility in buyer-seller relationships on the productivity of knowledge. *Journal of business Research*, 56: 443-451.

作者簡介

助理教授 王玉強

學歷：美國國際大學教育行政博士、美國空軍理工學院電子工程碩士、空軍官校71年班、高苑科技大學數位影視傳播設計後學士學程、樹德科技大學經營管理研究所碩士PMBA在職專班(肄業)。經歷：空軍官校通識教育中心外文系上校助理教授兼主任、空軍官校學員生大隊副大隊長、空軍官校學員生大隊中隊長、國防部總政治作戰部資訊中心電腦系統工程官、空軍官校協管中心資訊科講師兼系統工程官。現職：樹德科技大學應用外語系助理教授。