陳良駒、范俊平、謝佳容（2016），『網路作戰安全與管理主題實證探索之研究－使用 GHSOM 技術』，*中華民國資訊管理學報*，第二十三卷，第一期，頁 99-128。

網路作戰安全與管理主題實證探索之研究－使用 GHSOM 技術

陳良駒*
國防大學管理學院資訊管理學系

范俊平
國防部資電作戰指揮部

謝佳容
國防大學管理學院資訊管理學系
國立政治大學資訊管理學系

摘要

網際空間係由相互依存的資訊技術與網路基礎建設所構成的複雜環境，西方國家紛紛推出網際空間戰略，以加強對網際網路的控制與主導，制網路權也是我方近年不斷推動國防現代化與軍事事務革新的重要目標。面對中國「網軍」強大的威脅，本研究目的希望「以敵為師」了解對岸在網際空間作戰的攻防技術與支援規劃。研究中蒐整共計 1358 篇中國網路作戰相關文獻，據以建構「網路作戰安全與管理」概念詞彙，透過增長階層式自組織映射圖（growing hierarchical self-organizing map; GHSOM）的分群技術來建構詞彙的主題類別與層級關係，再進行成果歸納及實證分析。研究成果不僅了解中國大陸在網路作戰安全與管理議題上的重要發展及趨勢，也提供各國政府在網路空間戰略策進之參考。

關鍵詞：網路作戰、文字探勘、增長階層式自組織映射圖

* 本文通訊作者。電子郵件信箱：nctuhorse@gmail.com
2014/07/24 投稿；2014/10/22 修訂；2015/02/26 接受

Chen, L.C., Fan, C.P. and Hsieh, C.J. (2016), 'the study on exploring the topics of cyber warfare security and management: Using growing hierarchical self-organizing map', *Journal of Information Management*, Vol. 23, No. 1, pp. 99-128.

The Study on Exploring the Topics of Cyber Warfare Security and Management: Using Growing Hierarchical Self-Organizing Map

Liang-Chu Chen*
Department of Information Management, National Defense University

Chiun-Ping Fan
Joint Information Operation Command (JIOC), Ministry of National Defense

Chia-Jung Hsieh
Department of Information Management, National Defense University
Department of Management Information Systems, National Cheng-Chi University

Abstract

Purpose－In resistance to the enormous threats from the "Cyber Force" over the Internet, this research aims to examine both attacking and defending techniques, as well as the supporting plans from the People's Republic of China (ROC). This study employs the growing hierarchical self-organizing map (GHSOM) to construct the topic categories and hierarchy of vocabularies as a reference for enhancing the cyberspace war-fighting strategy.

Design/methodology/approach－The framework of this study can be divided into 3 phases, "Data Collection," "Terminology Process," and "Cluster Analysis."

In this research, based on 1,358 PRC's articles focusing on the cyber warfare from 2000 to 2010, a set of terminologies regarding "cyber warfare security and management" was constructed. The topic categories and hierarchy of vocabularies were constructed by using the clustering technique of the GHSOM. The results were then concluded and verified.

* Corresponding author. Email: nctuhorse@gmail.com
2014/07/24 received; 2014/10/22 revised; 2015/02/26 accepted

Findings－The results point out 16 important categories of the cyber warfare, such as "Network Attack Techniques," "Intrusion Detection Security Management," "Network Defense Strategy and Technology," and "Cyber Warfare Strategy and Benefits," etc. The fundamental contributions of this paper can be considered at three different levels: (1)providing a better knowledge representation strategy for the current military observers; (2)discussing progress on the implementation of 5 integrative viewpoints of cyber warfare; and (3)providing 6 cyberspace war-fighting strategies.

Practical implications－The results provide an understanding on the subject matter regarding the important development and trend of the cyber warfare security and management, as well as a reference for enhancing the cyberspace war-fighting policies.

Originality/value－This paper illustrates a novel application for the military and demonstrates the way to apply the proposed framework to building an objective analysis. The study describes the individual layer of the hierarchy, and identifies means to improving the effectiveness of collective knowledge via practice perspectives. It helps the readers form an understanding on the cyber warfare attacking and defending techniques, as well as the supporting plans.

Keywords: cyber warfare, text mining, growing hierarchical self-organizing map

壹、前言

資訊與網路科技的快速發展，對於人際關係溝通、企業營運開發、政府組織運作及社會型態建構等方面均造成重大之影響，軍事作戰領域亦不例外。美軍於1991 年波灣戰事與 2003 年伊拉克戰爭中，利用其資電網路之優勢獲取關鍵性的勝利，因而促使全球各國在軍事事務革新中，積極納入資訊作戰之概念進行研討。美軍將資訊作戰分為影響作戰、網路作戰及電子作戰三大面向（湯添福 2009），其中以「制網路權」為策略核心的網路化作戰，已經成為網際空間（cyberspace）最重要的作戰概念及關鍵手段（Magnuson 2006），亦是現代化軍事思想主流及世界強權軍事發展首要目標。

英國倫敦國際戰略研究所在 2010 年發佈的「世界軍事力量對比」報告中，宣稱未來戰爭的型態將以大規模網路攻擊取代傳統發射導彈的作戰方式（新華網 2010）。美國國防部於 2009 年成立網路戰司令部（cyber command），負責進行網路作戰並加強防範網際空間之威脅。日本則由陸海空自衛隊電腦專家組建網路戰部隊（吳嘉龍 2013）。中國大陸以「質量建軍，科技強軍」為原則，分別就學術、行政、公安、共軍等不同組織體系中籌組相關訓練處所；以共軍系統為例，即先後於 1995 年起陸續成立「國防科技信息中心」、「信息安全研究室」及「軍事情報處」等機構，進行研發資訊軟硬體、電腦病毒、駭客攻擊、電磁脈衝武器等技術，並於 1999 年開始，將訊息戰、駭客攻擊、網路攻擊等納入軍事演習之範圍（蕭懷湘 2010）。故如何瞭解網際空間作戰領域中的攻防措施，將是網際交戰的重要手段（Brett 2011）。然而，網路作戰雖屬於軍事領域之概念，但其安全與管理層面中的各項影響卻是遍及政府與民間不同產業。例如：去年（2014）壹傳媒因支持香港爭取普選而遭受到阻絕服務攻擊，造成連續多天無法順利出刊之現象；因勒索雲端公司 Code Spaces 不成，網際駭客進而滲透該公司 EC2 後台取得控制權，進而刪除全部的資產及資料，造成該公司無法營運而倒閉之情事。各種因資訊安全與管理問題所造成的新聞事例，屢見不鮮。

而公開資訊的蒐集具有數量龐大、內容豐富且取得容易的特性，長期以來即為各國情研部門廣為運用之手段（翟文中 2003）。網際網路及各項應用服務的蓬勃發展，創造出大量的數位化內容，雖有助於使用者以更為便利的方式籌獲資訊，但資料爆炸的現象卻也造成資訊過載之問題（Pattie 1994）；也就是說，大量網路資料若未能有效分類，則會導致不易以人工方式瀏覽及篩選網路資訊的現象，造成時間與人力資源的耗費。故如何藉由資訊檢索及文字探勘等技術，主動過濾不必要的詞彙雜訊，協助使用者進行主題的分析與探討，並透過智慧型的分析方法建構特定領域的知識結構與關聯，將能有效呈現該領域之潛在發展重點，以輔助

情蒐及學研單位相關人員，在數量龐大的網路公開資訊中，快速且精確的發掘隱含知識與事件發展的趨向。

一般來說，處理大量文件分析有兩種方式：(1)群集分析（clustering analysis），其目標在藉由群聚相似的資料樣態而降低資料量；(2)投影分析（projection analysis），主要係以降低資料維度為目的。而自組織映射圖（self-organizing map; SOM）則是兼顧群集及投影特色的分析方式（Yen & Wu 2008）。SOM 係由赫爾辛基大學 Kohonen 教授於 1982 年所提出，經常用來提供視覺化的文件分析與處理。然而，SOM 只能呈現出單一層級的結果，無法展現出文件間階層性的關係（Vicente & Vellido 2004）；故學者 Dittenbach, Rauber, and Merkl（2002）提出增長階層式自組織映射圖（growing hierarchical self-organizing map; GHSOM）的方法，以增加縱向層級式的知識結構。目前 GHSOM 文件分析方法已應用於多個領域（陳文華等 2004； 姜國輝 & 楊喻翔 2012； Shih et al. 2008； Yang et al. 2011），唯在網路作戰安全與管理領域的相關研究卻是付之闕如。

面對中國「網軍」強大的威脅，目前我方由國安會負責協調行政院技服中心、科技部與國防部三方進行網路安全之整體規劃；其中國軍在國防轉型、軍務革新與資訊戰力等各方面，均依據相關計畫逐步推展，以因應網際時代作戰之需求。然而，國家在擬定各項組織變革、戰略方向及攻防策略等政策時，除參考世界主要軍事強國外，往往最有效的方式即「以敵為師」。因此我們更應藉由瞭解中國大陸發展網路作戰現況及趨勢，擬定我方在網路作戰安全及管理上對應之方針。

本研究即以「網路作戰」為主題進行樣本文件蒐集，透過文字探勘技術及 GHSOM 方法，建構詞彙分群結果，並分析網路作戰安全與管理之實務意涵。研究成果不僅可觀察中國大陸學者對於網路作戰議題的整體性策略思維，亦可做為我國政府在規劃網路作戰安全與管理相關事務之參照。

貳、文獻探討

一、網路作戰

美國國防大學 Libicki 教授（1995）將資訊戰區分 7 種類型：指揮管制戰、情資戰、電子戰、心理戰、駭客戰、經濟資訊戰與網路戰。湯添福（2009）整理美國空軍頒布的資訊作戰準則（Air Force, 2005），將資訊作戰區分為影響作戰、網路作戰及電子作戰三大類型，其主要在取得資訊優勢，以爭取戰爭最後勝利。網路戰是資訊戰的特殊形式，乃在網路空間進行一系列的襲擾、竄改、竊取、監視與破壞的作戰行動。網際空間相較於傳統的陸地、空中、海上和太空等區域，被定義為第五類戰場空間（Cornish et al. 2010）。與傳統戰爭相比，網路戰具有突然性、隱蔽性、不對稱性和代價低、參與性強等特點（李承禹 2007）。

網路作戰係於網際空間中運用多類型的攻防資訊及電腦網路技術，以取代實體作戰的手段（Nicholson et al. 2012）。許多學者已提出網路作戰的重要特性，其中呂登明（2004）認為網路作戰具有空間的無限性、力量的廣泛性、手段的知識性、時間的連續性、過程的突變性及效率的高效性等特質。與傳統作戰方式相較，梁華傑（2008）則認為網路戰攻防具有「無平、戰時之分」、「無地域疆界侷限」、「全時域攻防」、「無年齡限制的網路戰士」及「戰略/戰術/戰技多層次融合」等特性。而 Cornish et al.（2010）則提出形成網際軍事戰略的數項特性：第一、網路作戰促使網攻者不需要透過實體的武裝衝突即可達成其軍事及戰略之目標；第二、網際網路提供給小型網攻者非對稱式的戰力空間；第三、使用偽冒 IP 位址、境外服務器及假名，網攻者可以在一個給定的時間內完全匿名並不受到任何懲治；第四、網際空間不容易區分軍事或民間、實體或邏輯、國家或非國家的界限；第五、網路作戰被認為是一個新的、但非完全獨立的多邊戰場組件；第六、網際空間的作戰概念更可能以脅迫及對抗等形式發生於企業組織中。故網路作戰乃屬於現今資訊科技發展下的攻防型態及概念，對於國家政府及企業組織均具有資訊安全及管理上的重大意涵。

由上述網路作戰特性中，可以知道作戰型態的複雜性及作戰方式的多元性。近二十年來，因應網路科技的不斷發展，國際之間在網際空間的攻防與對抗從未停止。2007 年 9 月，以色列進行果園作戰（operation orchard）行動，利用電腦網路，將特殊程式植入敘利亞防空雷達系統，並使其癱瘓無法發揮制空的作用（簡華慶 2012）；2007 年 4 月愛沙尼亞因蘇俄時代紀念銅像遷移之爭議，造成國會、政府部門、銀行、媒體等網站受到大規模攻擊，而導致全國性民生活動之癱瘓。2013 年 3 月南韓遭受最大規模網路戰爭攻擊，造成韓國境內多家金融、保險、媒體、電信等機構硬碟毀損或電腦當機。經官方調查此次攻擊係北韓歷經 8 個月的精心策畫，不斷的透過各種手法來蒐集、掃描、偵測、入侵南韓目標企業，然後伺機發動總攻擊（張景皓 2013）。2013 年 5 月，我方屏東琉球籍漁船廣大興號在台菲經濟重疊海域遭菲律賓船隻掃射，造成我方船員洪石成身亡。此次事件立刻引發台菲之間的駭客大戰，分別癱瘓兩國政府多個官方網站。而中國大陸是投入網路作戰資源及發展網路作戰組織最積極的國家，歷年來疑似由中國大陸所發起的諸多網路駭客事件（如表 1），都證明了其以國家力量支援網際空間作戰策略的具體行動。

表 1：疑似與中國大陸相關的網路攻擊事件彙整

時間	網路戰名稱	緣由	受駭國家/對象
2001	衛國網絡戰	美軍機於海南島附近海域與中國戰機發生擦撞事件	美國/政府、企業網站
2003	驟雨計畫（Titan Rain）	中國大陸有目的性的駭客組織連續、長期性的入侵美國重要網站	美國/政府、軍火商、科研院等網站
2006	藏獨監控	由中共科技部指導成立海外藏獨網路監控站相關系統	西藏/各地流亡政府、海外支持藏獨團體網站
2009	鬼網（Ghost Net）	加拿大蒙克國際研究中心發現一個龐大的電腦間諜系統，企圖滲入全球政府和私人企業網站	全球（包括台灣）/政府和私人企業網站
2009	極光行動（Aurora）	由於中共對於言論自由的箝制，故中國針對逾 20 家國際型企業發動「精心策劃且目標明確」的攻擊	美國/ Google、Adobe、Juniper 等多家民間企業
2014	公投駭客行動	針對壹集團支持香港民眾爭取普選投票及挺佔中行動，中國大陸駭客發動多起癱瘓攻擊	香港/蘋果日報、壹週刊等相關企業的網站及 APP

資料來源：彙整自蕭懷湘（2010）、簡華慶（2012）及網路資料

美軍網路作戰涵蓋五大策略：(1)透過組織、訓練及設備使國防部在網際空間發揮最大作戰潛力；(2)以創新的防禦理念來保護國防部的網路系統；(3)聯合其他政府部門及民間機構，建立全政府體系的網路安全策略；(4)與國際合作夥伴建立聯合防禦網路；(5)運用國家創造力，動員特殊網路力量及創新技術來進行防禦（DoD, U.S. 2012）。其作戰內涵包括「網路攻擊」、「網路防禦」及「網路戰支援」三部份（Air Force, 2005），與 Armistead（2010）將電腦網路作戰區分為攻勢、守勢與支援三類型的概念相同。其中網路攻擊係運用指管、電子、網路及實體作戰等型式，進行利用、混淆與破壞敵方之各種資訊、資訊流、資訊系統與基礎設備所採取之癱瘓作為。而網路防禦意指為了保護己方的資訊系統及相關設施免遭敵方的欺騙與破壞，其防護方法包括以指管通訊、電子作戰、資訊網路等安全防護與資訊戰力恢復等型式來進行。網路戰支援則是作戰行動負責人（或指揮官），以搜尋、辨識、定位等方式來弱化敵方區域資源，進而威脅敵方未來的作戰行動。網路戰支援則提供決策者直接涉及網絡戰行動所需的資訊，相關資料可用來製作情報，或提供針對電子或破壞性的攻擊（湯添福 2009）。

二、網路作戰安全與管理

1991 年波灣戰爭美軍以網路科技為輔，快速擊敗伊拉克，突顯科技作戰的優勢；2001 年 911 事件衝擊民眾對國家領土安全防護的認知，加速美國對於中東國家相關組織及全球社群網站的監控，前一小節也揭露全球網路戰爭的諸多真實案例。由這些事例的影響得知，軍事武力不再是威脅國家安全的唯一來源，網際空間戰場的影響擴及國家主權、政治制度、金融秩序及訊息安全，其威脅更甚於實體作戰。正如美國國家安全戰略白皮書所述，網際安全是一種對於國家安全、公共安全及經濟發展最嚴重的威脅與挑戰（DoD, U.S. 2012）。網際空間威脅不受國家邊界的限制，也沒有實體組織可以單獨偵防，在國防及民生等各項基礎建設均逐步與網際網路連結的情況下，即使國家處於非戰爭狀態，在政治與組織戰略競逐中，網際空間也被視為一種前線戰場（Choo 2011）及作戰武器（Liles 2007）。故不管是國家或企業，若敵方發動跨國網路間諜活動或跨組織的商情竊取事件，對於仰賴資通科技的國家政府與企業組織，均面臨資訊安全與管理上的衝擊及挑戰。

國與國之間的網路衝突或競爭中，不管是防衛受到網路攻擊的目標，或是阻止他國干涉本國內政，網際空間中的主權爭議目前還是取決於關鍵技術的發展（梁德昭等 2012）。根據美國在 2011 年 5 月以全球戰略的全新思維，對外公布「網路空間國際戰略」報告，其中包括 7 項關鍵戰略競逐領域：作業系統、搜尋引擎、通訊裝備基礎設施、雲端運算、治理論壇、密碼體系及網際網路協定第六版（IPv6），並宣告將整合外交、軍事、法律及經濟等力量，採取「勸阻」及「威懾」的防衛策略。國家網路安全戰略（National Cyber Security Strategy; NCSS）是一個協助政府管理網路安全風險的重要指標，歐洲的網路與資訊安全組織（European Network and Information Security Agency; ENISA）制定國家網路安全戰略的具體行動，主要提升關鍵基礎建設及網路安全與回應能力，報告中提供 20 項具體行動描述網路安全策略的建立與執行，並建議國家能與其他國家的公私部門合作（Falessi et al. 2012）。而 Luiijf, Besseling and de Graaf（2013）針對多個國家的網路安全戰略進行比較分析後，發現在經濟、國安與軍事防禦等方面出發點的不同，將造成網路安全戰略策訂方法的歧異，因此各國在網路競合的關係上，是非常複雜且不穩定的。因此，如何制定全球性的網路安全戰略，已是世界各國在防範其重要基礎建設與關鍵資訊系統上的主要管理政策。俄羅斯以「網路軍控」來對應美國網路戰能力的發展，英國則倡議「網路主權」意識，日本強調「資訊安全是綜合安保體系的核心」，南韓成立「網路空間司令部」，我方則將資通安全列為國家安全的重要課題。

中國大陸已蒐整網際攻擊手法與技術等資訊，並藉由駭客技術人才訓練處所

及行政機構的設立，加快具資訊安全防護與網路創新能力的網路精英培訓，以保護該國國家安全和維護人民利益（蕭懷湘 2010；陳巍 2010），反觀我方在網路作戰人才培育及資訊作戰模擬場域的投資則是有所不足。簡華慶（2012）認為網路作戰策略除了要制定網路資訊管控流程外，更需強化人員的教育訓練，才可避免因資訊安全漏洞肇生的網路入侵事件，並有效維護網際空間的國家主權。然而，當主權國家的資訊安全與網路空間受制於其他國家的通資基礎設備，或是跨國企業網路公司產品，則其即可透過衛星、網路和通訊等相關系統來竊取國安機密與商業情資，造成無法預知的損失。故網際空間之防護除了要採行適當及足夠的技術安全措施外，更要從安全政策、管理、法律、教育、組織、人力、國際合作等各方面，以全方位及全新的觀點推動（何全德 2013）。

三、自組織映射分群法

自組織映射圖（self-organizing map, SOM）是由赫爾辛基大學的 Kohonen 教授（1982）所提出的類神經網路分群法，其構想係從物以類聚的概念來整合具有相似功能的資料節點（unit），進而形成視覺化的叢集關係。SOM 係以維度縮減的技術，將高維度的輸入向量，依據相似度映射至二維平面圖形的輸出節點上，以建立主題群集，並呈現視覺化的領域知識關聯（Börner et al. 2003）。 學者林頌堅（2010）彙整多位學者觀點，提出 SOM 的數項特性：(1)在忽略某些較不重要資訊的前提下，進行特徵相近文件的節點映射，將在有限空間內表現出極大量的資料項目；(2)以非監督式方法為訓練基礎的 SOM，將在該映射圖形中保留資料項目在原維度環境下的特徵、結構與關係；(3)SOM 可整合多個不同資訊類別（如關鍵字、作者等）來建置特徵向量，以進行聚合訓練及建構映射結果；(4)與多維尺度法 MDS（multidimensional scaling）相較，SOM 所需要的計算資源較少，且圖形呈現的一致性較高，當增加新文件時，不必重新訓練即可映射至視覺化的圖形結構。

許多學者已透過 SOM 的分群技術，探索不同資訊應用（如檢索服務、主題瀏覽、文字探勘等）及特定知識領域（如科技研究、資訊傳播等）的發展（林頌堅 2010）。此外，部份學者也針對產業或社會現象進行分析與探索，例如：簡禎富、李培瑞與彭誠湧（2003）使用半導體製程晶圓測試參數的多維度資料，以自我組織映射圖網路演算法將資料分群，發現隱藏於半導體製程資料中的樣型與良率間的關聯性，可迅速有效地察覺可能導致製程異常的原因。施東河與黃于爵（2003）則利用類神經網路中的 SOM 網路架構，提出一套具有學習能力的網站入侵偵測系統，來偵測惡意電子郵件。

然而，SOM 的運作具有二項限制因素（Dittenbach et al. 2002; Vicente & Vellido 2004）：第一、SOM 圖形拓撲的大小固定，且需於訓練前設定，無法自動學習以

致不容易找到適當的群數；第二、SOM 平面圖形不易處理龐大的輸入資料，且無法表現資料間的層級關係。也就是說，當輸入資料量過大，由於拓撲大小固定，會造成單一輸出節點所涵蓋的輸入向量過多，且由於無法延伸擴展，故呈現於 SOM 的資料項目將過於雜亂。因應以上 SOM 的功能缺失，Dittenbach et al.（2002）提出了增長階層式自組織映射圖（growing hierarchical self-organizing map; GHSOM）的想法。GHSOM 為 SOM 架構的延伸，呈現具層次性的映射結構，且每個層級均由數個獨立的 SOM 結果所構成，這些層級的拓樸結構可依據資料相依關係而有所變化；亦即 GHSOM 涵蓋水平拓樸增長及垂直層級增長的概念，是一種動態但不破壞原有學習機制的演算模式，其二維平面 SOM 與多維階層 GHSOM 的架構關係詳如圖 1 所示。

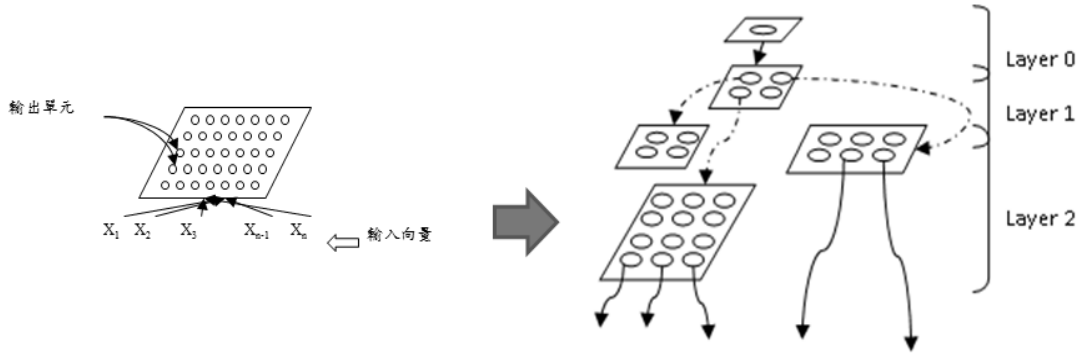

圖 1：從二維平面 SOM 到多維階層 GHSOM 的架構關係

目前 GHSOM 的相關研究與應用非常多元，包括研究主題挖掘、產業管理分析、資訊網路探索及特定領域應用等。在研究主題挖掘部分，楊喻翔與釋惠敏（2011）探討 1952 至 2009 年 SCIE 及 SSCI 中與安寧療護相關研究文獻的生產力分析，並利用 GHSOM 呈現安寧療護文獻中重要研究主題及概念交涉關係；姜國輝與楊喻翔（2012）以 GHSOM 分析出「利他」文獻中歷年重要研究主題及相關概念的交互關係，除提供學者深入瞭解利他研究的範疇與學科關係，更能快速聚焦及掌握利他主題中的研究概念。在產業管理分析部分，戴元峰、吳騏與薛義誠（2013）透過文字探勘技術及 GHSOM 群聚分析方法，將「國際科技政策觀測系統」中以文字型式呈現之文件資料，轉換為以圖像型式呈現的「科技訊息分群圖譜」，有助於提升決策者迅速瞭解國際科技政策發展概況的需求，強化系統的環境監視功能。陳文華、施人英與吳壽山（2004）以台塑集團王永慶先生為對象，運用 GHSOM 輔助建構管理者的知識地圖，從功能層次的觀點，獲得不錯的分群

效果，可明確地將集團創辦人之企業精神顯示於知識地圖中。

在資訊網路探索部分，Shi et al.（2012）提出一個智慧型的網路流量識別方法，採用 GHSOM 來訓練網路封包的屬性（如時戳、來源和目的 IP 等），以應用於網路封包探索之研究；Ibrahim（2010）則利用 GHSOM 創建 Misuse 入侵偵測系統，可以分析已知或未知網路攻擊。而在特定領域應用部分，Ortiz et al.（2013）提出一個運用醫療核磁共振成影像系統（MRI）判斷的分割方法，並使用 GHSOM 和多目標的特徵選擇為基礎，優化分割過程的性能；Shih et al.（2008）則以證券暨期貨市場的法律問題為目標，建構一個以內容為基礎且易於操作的法律知識地圖。

參、研究方法與架構

本研究提出之架構係以群集探勘概念為基礎所進行的流程設計，主要區分為三階段：資料蒐集、詞彙處理及群集分析。資料蒐集階段以中國知網（CNKI）平台之期刊全文數據庫（China Journal Full-text Database; CJFD）為來源，針對論文中包括「網路作戰」主題的文件進行資料蒐整，以建立分析文件庫；詞彙處理階段包括文件斷詞、詞性標註、同義詞（贅詞）處理、特徵詞計算、文件向量關係計算等步驟；群集分析階段則以 GHSOM 的方法進行詞彙分群，瞭解網路作戰主題發展的類別層面，並進行成果分析。研究架構如圖 2 所示，各階段的執行步驟說明如後。

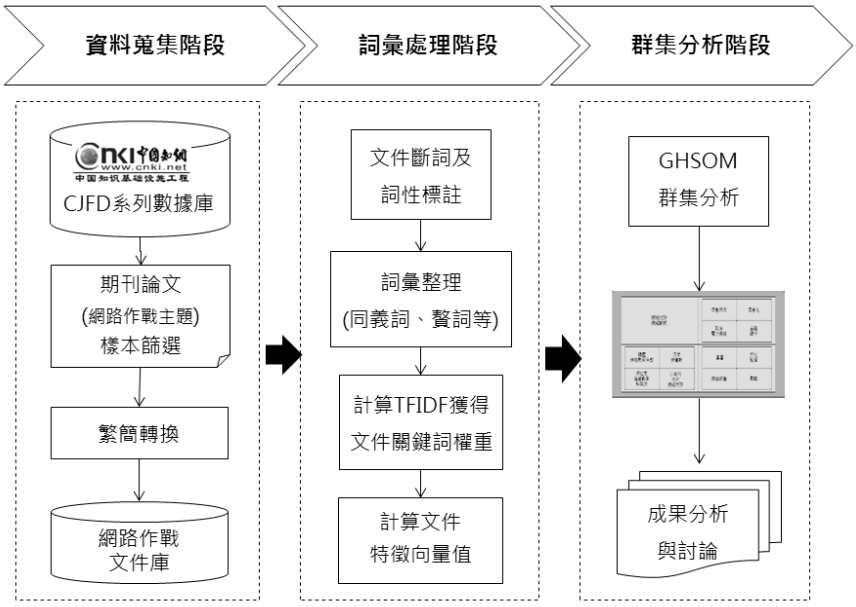

圖 2：研究架構圖

一、資料蒐集階段

本研究自中國期刊全文數據庫中蒐整 2000 至 2010 年期間的相關文件，並以兩類條件進行文件篩選：(1)標題與關鍵詞中含有「網路（絡）戰」、「網路（絡）作戰」的字詞；(2)摘要文字中包括網路（絡）戰、網路（絡）攻擊、網路（絡）防禦、網路（絡）作戰等詞彙。符合條件之蒐整文件共計 2,387 篇，扣除部分無法下載及具機敏性的文件，確認可用文章樣本為 1,358 篇。接著以共享軟體採批次方式將下載檔案轉換成純文字檔，並以人工方式進行相關錯誤檢視與修正。而相關文件處理部分則另以共享軟體將字形由簡體字轉換為繁體字後，儲存於文件庫中，以利後續斷詞整理及成果分析作業。

二、詞彙處理階段

本階段包括中文斷詞、詞性標註與篩選、同義詞/相似詞/贅詞等比較、特徵詞權重計算與篩選等事宜。本研究採用中研院研發之中文斷詞系統 CKIP（chinese knowledge information processing）進行詞彙分割與詞性標註，而 CKIP 可提供使用者依需求自建特定領域專屬詞庫，以獲得精準之斷詞結果；惟近年來有關網路作戰方面並未建有專業詞庫，因此本研究詞彙的斷詞與詞性標註係以兩次詞庫比對的方式來進行詞彙擷取之工作。

首先以樣本文件中各篇文章的關鍵詞為主要詞彙，經人工篩選及專家研判後獲得具有特殊涵義的專有詞彙或術語，將其匯入專屬詞庫以提供未來斷詞處理時的參照；接著即以 CKIP 進行全文文件之詞彙辨識及標註。考量詞彙術語的特性與系統計算的負荷量，本研究僅擷取名詞詞性的詞彙進行分析。經相關程序處理後，取得全部名詞數計有 34,416 個詞彙。

為增加詞彙與主題的關聯性，本研究除使用 N-Gram 方法進行詞彙合併（例如：「高科技」+「作戰」=「高科技作戰」），並驗證其組合的正確性外，也針對部分同義詞（例如：日誌 vs. 日志）、相似詞（例如：電腦病毒 vs. 計算機病毒）、中英譯詞（例如：SQL 注入式攻擊 vs. SQL Injection）及無意義詞（例如：編號、獅子、當天）等語意不清詞彙，以自訂規則或人工檢視方式予以刪除或合併；經處理後之詞彙數為 1,070 個。

而在進行詞彙探勘群集分析之前，必須瞭解關鍵詞彙在文件中的重要程度，使其具有能夠代表文件的特徵。TF-IDF（term frequency - inverse document frequency）是經常使用於資訊檢索領域中的權重計算方法（Salton 1986），主要係指詞彙的重要性會與其在文章中出現的詞頻 tf 成正比，但會與其在其它文章中出現的頻率 idf 成反比。將 tf 值和 idf 值相乘，可以更加突顯詞彙的代表性。相關公式說明如下：

$$w_i(d) = tf_i(d) \times \log\left(\frac{N}{df_i}\right) \quad (1)$$

其中 w_i（d）：詞彙 k_i 在文件 d 中的權重；tf_i（d）：詞彙 k_i 在文件 d_j 中的詞頻；

N：文件集中所有文件總數；df_i：文件集中出現詞彙 k_i 的文件數

為了選出更具代表性的詞彙方能適當反應文章內容，我們將所有詞彙的權重排序，保留權重較重之詞彙換算為矩陣向量，以做為 GHSOM 分群計算之輸入值。本研究以 Java 開發工具程式，設計 TFIDF 詞彙計算及權重排序之模式，依據權重的門檻值，本研究選取前 400 筆權重較高之詞彙為特徵向量值，以利後續分析。

三、群集分析階段

GHSOM 方法採用平均量化誤差（mean quantization error, mqe）來控制映射圖的增長過程，可節省 SOM 需事先定義矩陣大小的麻煩，並大幅提升群集的效率。本研究參酌 Kohonen（1997）、Dittenbach et al.（2002）、陳文華等（2004）、Shih et al.（2008）、姜國輝與楊喻翔（2012）等學者之建議，綜整 GHSOM 學習演算流程說明如下：

（一）初始化階段

1. 給定 GHSOM 初始化參數

   包括學習率（learning rate）、鄰近範圍（neighborhood range）、初始映射圖大小（initial map size）、水平擴展停止準則（growing-stopping criterion）、階層增長停止準則（hierarchical stopping criterion）、標籤最大值（maximum number of labels），標籤門檻值（label threshold）等參數。

2. 虛擬第 0 層權重向量（m_0），計算其平均量化誤差（mqe_0）

   假設存在僅由一個節點（unit）組成的虛擬層（layer 0），該層之權重向量（m_0）以所有輸入向量的平均值做為初始值，並計算其平均量化誤差（mqe_0）。

3. 平均量化誤差 mqe 計算公式

   某處理節點 i 的平均量化誤差為其權重向量（m_i）與所有對應至該節點的輸入向量集合（C_i）之間的平均歐氏距離（euclidean distance），其計算公式如式(2)所示。其中 x_j 表示輸入資料向量，C_i 為 x_j 對應到節點 i 的子集合，n_{ci} 則為該子集合的樣本數。

$$mqe_i = \frac{1}{n_{C_i}} \cdot \sum_{x_j \in C_i} \left\| m_i - x_j \right\|,\ n_{C_i} = \left| C_i \right| \tag{2}$$

4. 設定第一層初始映射圖大小

以自組織學習的最小映射圖來設定第一層（layer 1）初始映射圖大小，例如：預設以 2×2 的基本單位來建構 SOM 初始圖形。

（二）學習及成長階段

1. 評估目前層級的映射品質

經固定學習次數後，分析所有節點的 mqe，其中擁有最大 mqe 值的節點被選為誤差節點 e（公式如(3)），地圖會在此誤差節點與其最不相似的鄰居節點之間插入一個新的節點（列或欄），而此新的處理節點之權重向量則被初始化為鄰居的平均值。

$$e = \arg\max_i \left\{ \frac{1}{n_{C_i}} \cdot \sum_{x_j \in C_i} \left\| m_i - x_j \right\| \right\},\ n_{C_i} = \left| C_i \right| \tag{3}$$

2. 計算目前映射圖的 MQE 值

每個映射圖的 MQE 代表所有對應至集合 U 量化誤差的平均值，如公式(4)，其中 m 表示目前的 SOM 映射圖，n_u 表示所有在 U 集合的數量。

$$MQE_m = \frac{1}{n_u} \cdot \sum_{i \in U} mqe_i, n_u = \left| U \right| \tag{4}$$

3. 映射圖擴展階段

若成長過程中的 MQE 達到地圖所對應到上一層節點 mqe_u 值的特定比例 τ_1（如公式(5)）時，則停止映射圖的學習。其中擴展參數 τ_1 之目的為映射圖大小的控制。τ_1 愈大則 MQE_m 容忍度愈大，學習時間較短；反之，τ_1 愈小，則 MQE_m 容忍度愈小，學習時間則愈長。

$$MQE_m < \tau_1 \cdot mqe_u \tag{5}$$

（三）映射圖階層增長階段

若各節點平均量化誤差（mqe_i）在目前層皆小於在第 0 層某特定比例 τ_2 時（終止準則如公式(6)），則不需再往下一階層增長。其中階層增長參數 τ_2 之目的是輸入資料品質的控制。τ_2 愈小表示愈容易往下層細分。

$$mqe_i < \tau_2 \cdot mqe_0 \tag{6}$$

（四）學習循環階段

整個學習流程反覆進行步驟（二）及（三），直至滿足公式(5)及(6)為止。

本研究使用 Matlab 套裝工具，以選取的權重詞彙為輸入向量，並經試誤及參數調適後律訂 τ_1(=0.95)與 τ_2(=0.001)值，其餘初始參數則使用系統預設值。同時以上述學習流程為分群方法，期望獲得符合研究所需目的之分群結果。

將 GHSOM 群集演算完成之詞彙分群階層圖，以美軍網路作戰定義（網路攻擊、網路防禦、網路戰支援）為基礎進行歸納分析，取得中國網路作戰發展現況及趨勢重要議題，即可提供瞭解網路作戰安全與管理發展的重要參考。

肆、研究成果

一、主題分析與討論

本研究將 1358 篇文章中具代表性的 400 個詞彙，以 GHSOM 演算方法進行分群後，系統產出所有詞之分群階層圖（如圖 3），歸納出 4 層，共 191 個區塊。

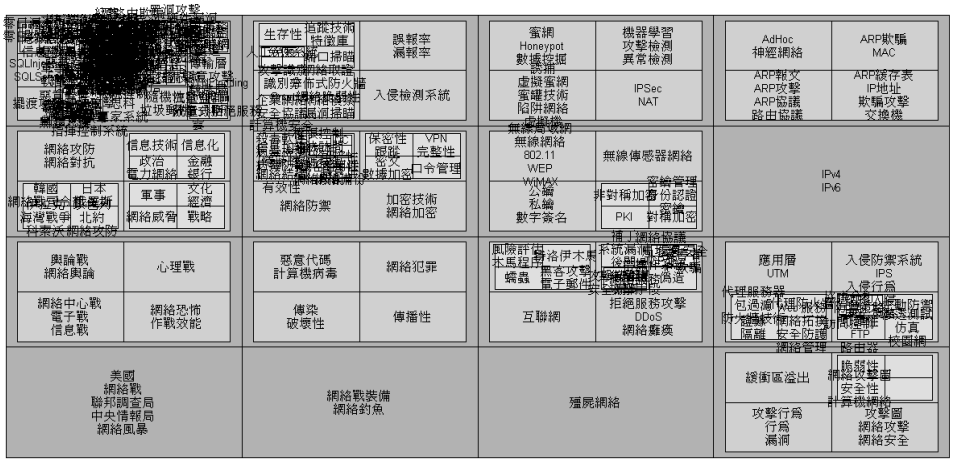

圖 3：GHSOM 分群階層圖

為利後續分析識別，本研究參照姜國輝與楊喻翔（2012）的層級關係為命名的原則，將群集成果以(1)、(1.1)、(1.1.1)等方式呈現其層級性的關係（如圖 4），其中第一階層共分為 16 個區塊，其中區塊顏色愈深者代表愈上層，本研究之分群

結果層級數最高為第 4 層。

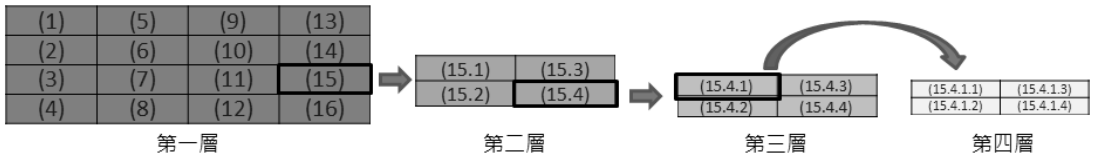

圖 4：分群階層命名範例

藉由 GHSOM 所生成之各區分群階層圖，呈現出中國大陸 2000-2010 年於網路作戰的發展目標及重要主題，並依美軍網路作戰定義將其分別歸屬於網路攻擊、網路防禦與網路戰支援三類。相關分群結果、議題命名、詞彙及層級數等資料彙整如表 2。

第一層集群分類共有 16 個區塊，其中除(4)、(8)、(12)、(14)無第二層子區塊；(1)網路攻擊技術的第二層有 15 個子區塊外，其餘皆為 4 個子區塊，故總計第二層共有 59 個區塊；第三層及第四層分別有 94 及 22 個區塊，每個區塊代表該分群計算結果的代表詞彙集合。從第一層結果可以觀察其分佈領域涵蓋電腦網路攻擊、欺敵、破壞、電子戰、作戰安全與心理作戰等，有些區塊因為包含的代表詞彙數太多，無法分析其整體概念趨向，利用 GHSOM 的特性可將深度階層分類表達出來，重新劃分子群並進一步觀察及研討其代表意涵，讓研究人員得以知道哪些詞彙在網路作戰文獻中具有重要研究概念，以利聚焦分析。

表 2：GHSOM 分群結果彙整表

分群命名	重要議題	美軍定義分類	總詞彙數	層級數
(1)*	網路攻擊技術	網路攻擊	175	4
(2)*	網路作戰案例與影響	網路戰支援	25	3
(3)	網路作戰方法與效益	網路戰支援	8	2
(4)	網路戰發展機構	網路戰支援	5	1
(5)	入侵偵測安全管理	網路防禦	23	4
(6)	網路防禦策略與技術	網路防禦	35	4
(7)	網路犯罪與病毒傳播	網路攻擊	6	2
(8)	網路釣魚技術	網路攻擊	2	1
(9)	誘捕技術發展	網路戰支援	15	2
(10)	無線網路安全技術與管理	網路戰支援	15	3

分群命名	重要議題	美軍定義分類	總詞彙數	層級數
(11)	網際網路攻擊威脅	網路攻擊	30	4
(12)	僵屍網路技術	網路攻擊	1	1
(13)	ARP 協定安全	網路攻擊	12	2
(14)	IP 基礎建設與發展	網路戰支援	2	1
(15)*	網路整合與主動防禦	網路防禦	33	4
(16)	系統漏洞與網路安全	網路防禦	12	3

*為列入後續說明之範例群集

上表為網路作戰安全與管理所呈現各面向的重要議題，為便於分析群集之結果，以下就美軍定義的網路作戰分類中，分別挑選層級數較高，且具代表性的重要群集為例，包括(1)網路攻擊技術：網路攻擊、(2)網路作戰案例與影響：網路戰支援及(15)網路整合與主動防禦：網路防禦等三項，進行成果分析與說明。為簡化說明層級性的成果，僅於分群(1)呈現階層式之架構範例及相關說明，其餘範例則不進行延伸性的成果討論。

分群(1)：網路攻擊技術

本分群階層為層級數最深，且詞彙數最多的一個群集，其分群結果如圖 5 所示。共計區分為 15 個區塊，其中有 13 個區塊與網路攻擊類型、方式、系統等概念具相關性，且其又涵蓋多項與網路攻擊技術、管理有關之代表性詞彙。因此定義分群(1)為「網路攻擊技術」，係屬於美軍定義分類中的網路攻擊類別。

經彙整分析中國大陸網路作戰攻擊手法，研判對岸具有規劃、情報蒐集與攻擊目標的能力，其利用監聽、掃瞄及社交工程等的手法以截獲資訊。在代表詞彙集群中可以發現(1.10)利用嗅探技術於網路或資料庫等進行資訊的蒐集，(1.6)出現多種社群媒體與 web 社交工程手段進行監聽，此外也出現網軍、解放軍等字彙群集，故可得知中國大陸已於 2000-2010 年間成立具規模之網軍組織進行公開的情資蒐集。在以密碼破解直接入侵目標的網攻手法中，(1.11)集群中涵蓋加解密演算法與認證技術的概念。而利用漏洞、惡意程式碼與後門程式間接入侵目標，可在(1.2)SQL Injection、(1.5)惡意程序、網頁掛馬、軟件安全與(1.3)擺渡攻擊群集詞彙中反映出其意涵。電腦網路攻擊行為主要為擾亂、阻絕、降低或摧毀電腦網路中的資訊或網路環境，以便利用惡意程式碼、病毒或阻絕服務來破壞資訊設施，因此代表詞彙從(1.7)淹沒攻擊、(1.10)泛洪攻擊的資源消耗，於(1.15)的分佈式拒絕服務、Smurf 等，都依駭客手法及趨勢採取混合攻擊方式以奪取制網權。

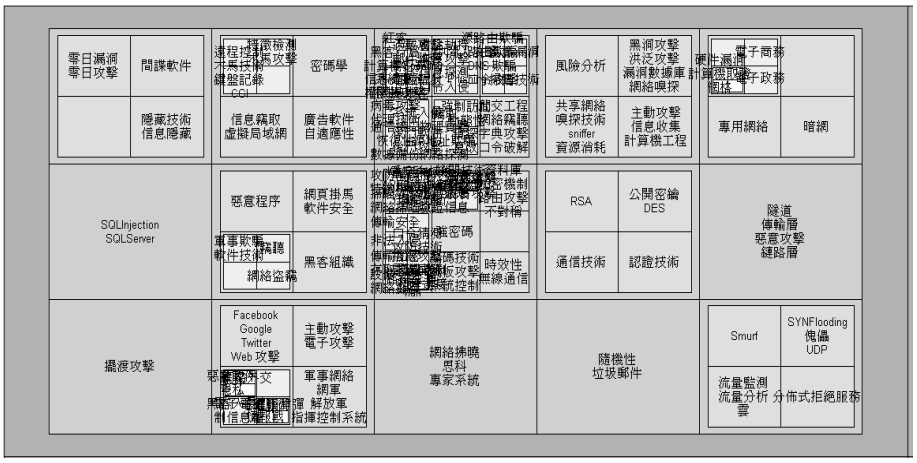

圖 5：「網路攻擊技術」映射圖

若以層級概念細分，可觀察出更為深入的訊息。圖 5 群集中以(1.7)及(1.8)兩個區塊的詞彙數最多且聚合最為密集，故以圖 6 展現其次層結構與詞彙群集關係之範例，以說明其群集階層之特性。

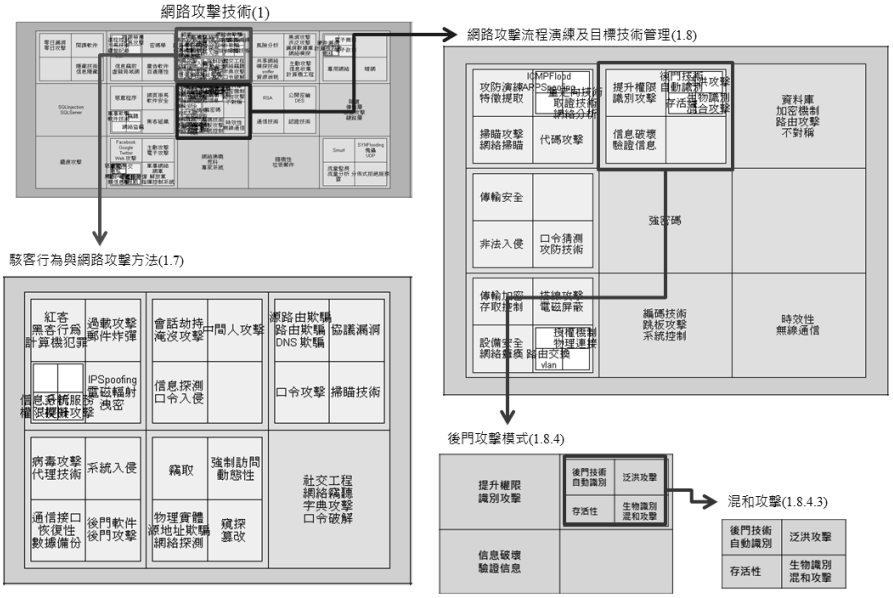

圖 6：「網路攻擊技術」的階層增長映射結構圖（範例）

階層(1.7)之 SOM 平面包括六個區塊，其概念涵蓋傳統攻擊手法（例如：郵件炸彈、病毒攻擊、字典攻擊）、欺騙方式（例如：路由欺騙、源地址欺騙、DNS 欺

騙）、駭客行為（例如：計算機犯罪、信息探測、竊取、窺探、篡改）等，故此部分命名為「駭客行為與網路攻擊方法」。階層(1.8)包括八個有意義之區塊，其概念涵蓋網路攻擊流程（例如：網路掃描、特徵提取、自動識別、提升權限、網絡癱瘓）、存取控制與加密（例如：加密機制、傳輸加密、強密碼、授權機制、驗證信息）及攻防技術與管理（例如：攻防演練、混和攻擊、傳輸安全、設備安全），故此階層區塊命名為「網路攻擊流程演練及目標技術管理」。階層(1.8.4)包括三個區塊，具備「後門攻擊模式」之意涵，主要透過各種混和攻擊技術入侵後門，以進行資訊破壞及提升權限。階層(1.8.4.3)則更為強調後門技術與識別技術之運用，取得系統掌控權後，甚至可發動泛洪攻擊。每一個不同層級的 SOM 平面均代表網路作戰概念中安全與管理的特殊意涵，其餘概念之延伸則可以類似的方法進行彙總論證。

整體來說，中國大陸已具備網路作戰武器研發、部署及作戰能力，置重點於網路攻擊技術提升、專屬網路安全防禦、情報網之整合等，達成制信息權的目標。

分群(2)：網路作戰案例與影響

本詞彙分群共有三個層級，主要代表詞彙為網絡攻防、網絡對抗、電力網絡、海灣戰爭、軍事、戰略等名詞，因此將此分群定義為「網路作戰案例與影響」（如圖 7），係屬美軍定義分類中的網路戰支援。

集群(2.1)揭露網路攻防及對抗在網際空間中的重要概念。傳統網路作戰多僅限於商（家）用電腦相關設備之影響；然而，網路作戰攻防目標並不限於軍事設施，若許多民生設施的破壞造成經濟數據、能源供應或心理恐慌等各面向的威脅，亦會造成極大的影響。網路作戰是網際空間的競逐，不受國家地域邊界的限制，網路作戰的目標可能影響政治、軍事、文化、經濟等各面向的參與人員，透過資訊交流將思想、概念、政策或方向，以直接或間接方式影響、操縱甚至控制國際政治輿論關係、社會民生活動或民眾事件觀感，故集群(2.3)與(2.4)已呈現出網路對抗的戰爭中，對於和民眾生活息息相關的政治、文化、經濟金融、銀行及電力網絡等的關連性，已漸趨密切與重要。例如：2007 年愛沙尼亞因為遷移二戰中陣亡的蘇軍紀念碑，引起俄羅斯及親俄民眾的強烈不滿，從當年 4 月底開始，整個愛沙尼亞網路遭到大規模的組織性攻擊，該國政府無力防禦，不得已情況下切斷全國與國際網路的連線，將該國隔離于全球網路之外，因此造成該國在民生活動及經濟金融的全面癱瘓。

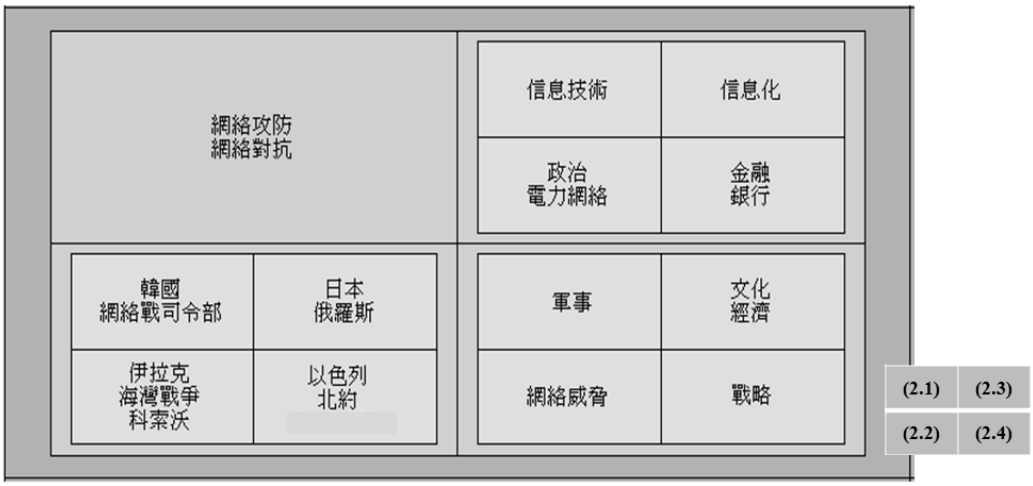

圖 7：「網路作戰案例與影響」映射圖

在現代化戰爭中已將網路作戰對抗及實戰納入其軍事行動中，目標可能是軍事通信、情報、後勤、作戰的軍事基礎建設，甚至是電信、運輸、能源、財政與供應鏈等民間基礎建設，例如：1991 年的波灣戰爭，美國派遣特工人員在伊拉克新購買的印表機晶片中嵌入病毒，致使伊拉克防空體系中的預警和 C3I 系統癱瘓；1999 年科索沃戰爭，北約入侵南聯盟系統竊取軍事情報，南聯盟軍方則在網上搜索所有參與對其空襲的北約武器裝備的資訊，為其反空襲作戰提供了有力支援，而北約部分電腦的軟、硬體已經遭到來自南聯盟的電腦病毒的重創。由本分群詞彙結果(2.2)得知中國大陸藉由波斯灣戰爭及科索沃戰爭等著名戰役與事件，學習多國資訊技術運用於軍事行動的方法，並蒐集各國軍事力量投入網路作戰的發展現況，以瞭解未來戰爭的制網權對國家政、經、軍、心等各重要層面之影響。

整體來說，集群(2)顯示中國大陸於電腦網路攻防或對抗中，不僅從多國案例中探索作戰規劃及實施手段，瞭解網路作戰在軍事戰略、政經文化等各方面的影響，同時也積極蒐整網路作戰對於公共或民生基礎建設的威脅與破壞。

分群(15)：網路整合與主動防禦

本詞彙分群共有 4 個層級，33 個關鍵詞彙。主要代表詞彙為網路管理、安全防護、入侵防禦系統、防火牆、防禦策略、滲透測試等名詞，因此將此分群定義為「網路整合與主動防禦」（如圖 8），並將其歸屬於美軍定義分類中的網路防禦概念。

在網路防禦策略部份，中國大陸近年的研究涵蓋互聯網（網際網路）、區域網路及專有網路部份，而其研究範疇及重點則是以建立資訊處理系統而採取的技

術安全防護，並以實現電子資訊的保密性、完整性、可用性和可控性為防禦主軸。此群集的詞彙集合，整體而言包括預防、控制、偵測及紀錄四項構面。集群(15.1)代表詞彙為應用層及 UTM（unified threat management），其概念呈現為整合式的威脅管理模式，顯示中國大陸除以基本的防火牆來過濾特定 IP 及通訊埠外，也在網路協定應用層導入 UTM 來進行資訊安全防護，以防止漏洞攻擊和掃描攻擊。集群(15.3)得知中國大陸在網路管理架構，係採用入侵防護系統（intrusion prevention system; IPS）防堵攻擊者的入侵行為，以提早偵測出漏洞攻擊、掃瞄、惡意程式碼的破壞行為和阻絕服務等攻擊。

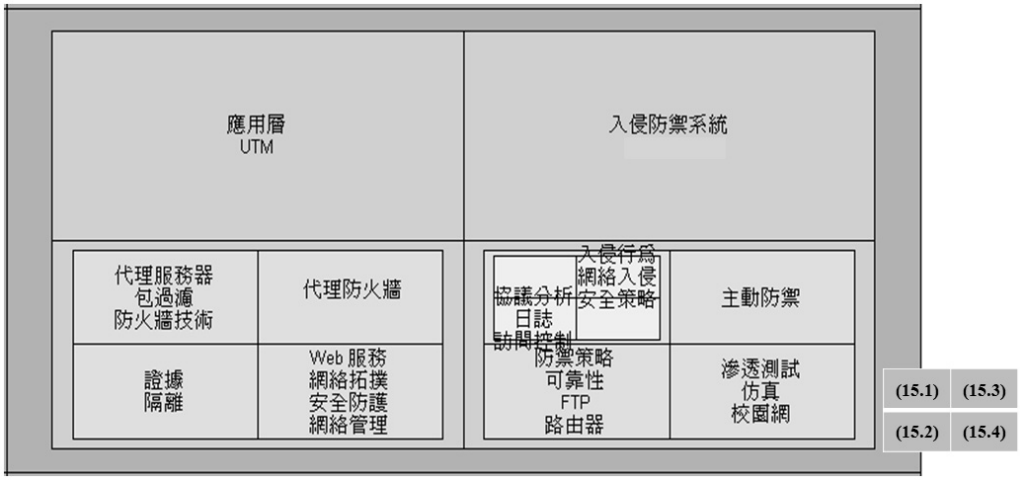

圖 8：「網路整合與主動防禦」映射圖

在集群(15.2)中，除網路管理、安全防護與網絡拓樸等詞彙彰顯了管理政策與作業流程的要求外，也建置代理防火牆與代理服務器，來提高網路作戰中實體位址的安全性，另外輔以證據、隔離等鑑識技術的發展。集群(15.4)代表詞彙中除強調主動防禦的戰略目標，組織的網路環境透過滲透與仿真校園網測試，能夠即時修補未知漏洞，以獲得高強度的網路作戰防護能力。此外，(15.4.1)則強調網路入侵的訪問控制及安全策略，以及入侵行為後的日誌分析，可強化防禦策略的完整性。

整體而言，集群(15)的詞彙整合縱深防禦的概念，企圖以多層次、多手段的全面性防護策略來進行各項網路作戰防禦作為。

二、綜合討論

本研究羅蒐中國大陸 2000-2010 年網路作戰公開文獻資料，利用文字探勘與增

長階層式自組織映射圖等技術，將詞彙分群後獲得「網路攻擊技術」、「入侵偵測安全管理」、「網路防禦策略與技術」、「網路作戰方法與效益」等 16 個網路作戰重要議題，分析不同層級主題之內涵，並闡述相關現況及趨勢。依據詞彙群集之成果，發現中國大陸在網路攻擊的著墨更甚於防禦的概念，同時對於資安的基礎建設或相關技術亦非常重視。針對中國大陸網路作戰安全與管理之發展內涵與方向，提出下列數點綜合說明：

（一）網路攻擊方法的多元，造成網安對抗技術的不斷升級

網路資訊攻擊技術日新月異，包括以網路癱瘓為作戰主軸的分散式阻絕服務攻擊、監控及擷取網路通信過程中訊息的中間人攻擊、以社交工程為基準的網路釣魚攻擊、利用資料庫設計弱點所進行的資料隱碼攻擊等，多至數十項不同的網攻手法，每一項均會造成受害端不同程度的損失。目前來看，惡意程式的數量將持續增加，各種變異手法亦將不斷演變升級；木馬攻擊的佈建方式將更加隱蔽及具有欺騙性，以誘騙主要攻擊之目標。目前中國大陸網路攻擊技術不僅增加在目標性攻擊（targeted attacks）與進階持續性滲透攻擊（advanced persistent threat; APT）的頻率及複雜度，同時在攻擊目標時還強調攻擊前之佈建（社交工程、網路釣魚、僵屍網路），並藉由網軍及民間駭客組織隨科技演進不斷研發反偵測技術之惡意軟體，於境外採各種手法混合運用以實施練兵及攻擊作為。

（二）國家層級對於網路作戰的重視，造就全國網軍組織及駭客產業的發展

為達成「高科技條件下的局部戰爭」之戰略指導，中國大陸除將仿效美國擴編網軍等相關組織、強化人才之培養及增編預算外，持續應用網路戰手段影響其戰略或政治目標。而國家也間接鼓勵駭客地下產業的發展，使專業駭客透過網路釣魚、攻擊勒索、網絡刷票、個人隱私竊取等易於獲利的攻擊方式，對許多國際型商業網站發動攻擊；同時也透過阻絕服務、殭屍網路、零日攻擊等易於癱瘓網路運作的方式，針對特定國家發動相關攻擊。此外，由近期發生的許多個資外洩、販售及網際惡意勒索的網安事件來看，利用資訊能力與網路技術來竊取、癱瘓、破壞，甚至進行犯罪的網路攻擊者所形成的駭客經濟，將成為另一波駭客產業發展的契機。

（三）以「理論為基，實務為本」之概念，強化主動式防禦機制之設計

防禦是網路作戰層級中最重要的工作（Williams 2011）。中國大陸近年來在網安防禦方面的研究，除強調以隱蔽及加密為核心的理論基礎及技術發展外，也積極開發防範入侵的各項技術與能量。故不僅成立屬於共軍系統的網軍部隊、基地及研究中心，亦積極整合民間學研機構（如中國科學院）與行政系統（如科技部），分別針對資訊安全領域中的各項基礎技術，投入大量的人力及相關資源進行研發，成果展現於密碼技術的成熟與蓬勃。此外，相關科研單位亦積極投入智慧型

技術（如機器學習、資料探勘、免疫系統）於入侵防護之應用，主動發掘潛在之漏洞與風險，並以縱深防禦之架構佈建完整性的防護體系。

（四）網安基礎建設及先進關鍵技術之籌獲，確保國家網路安全攻防能量

為使資訊軟、硬體設備及技術不受制於他國，中國大陸除著重於各項網路基礎環境（例如：IPv6、無線傳感器等）與技術（例如：加密、認證、PKI 等）之研討，同時也著手開發或採購相關關鍵技術及設備（例如：作業系統、網路設備、防毒軟體等），除可確保該國重要網通安全外，另可於量產後銷售至全世界，遂行其網路作戰之目的。

（五）網路作戰趨勢與新興威脅

探勘資料中已出現電力網路的攻擊對象，顯示網路安全形勢日益嚴峻，對公共網絡安全運行帶來嚴重影響；針對全球網際網路基礎建設和金融、證券、稅務、交通、海關、工業、能源、科技等重點行業的聯網資訊系統之探測、滲透和攻擊將逐漸增多，亦已成為對岸積極研擬控制的目標。此外，由於無線與移動性裝置的普及，行動網路的安全問題受到重視，因此移動性的網際空間成為網路作戰攻防作業中，另一波新興的網際戰場。

美國一直都是中國大陸在經貿、政治及軍事等各方面的假想敵，在網路作戰發展上亦然。中國大陸從經濟崛起後，積極佈建其於網路作戰之攻防能量，以期達成網路強國的戰略部署，並成為網際空間之霸權國家。故在各式國際間之衝突，均可見其以國家力量或駭客組織進行情蒐、監控、癱瘓及破壞等作為，企圖影響他國政府或企業之正常營運，遂行其國家政策或網路戰略之目標。

伍、結論與建議

網路作戰係以網際網路為戰場空間，並於該空間進行網路攻擊、防禦及支援的新興作戰思維，是國家整體資訊作戰中極重要的一環。然而，在行動通訊、社群媒體、雲端運算、巨量資料、物聯網等資訊技術快速發展的推播下，網際空間已經成為政府運作、企業生存與個人生活不可或缺的數位虛擬世界。而各式的網際威脅也與日俱增，意即使用者在網際之間可能遭遇的安全及管理問題將更為複雜。

自 2001 年迄今，世界各國在網際空間中的作戰從不曾間斷，台灣更是中國大陸駭客首要的練兵場域，不僅影響軍事策略的佈建，也影響社會及國家安全的整體面向。作戰方式從無差別的惡意程式散佈，到聚焦於資料竊取對象的進階持續性滲透攻擊，不同的網路作戰手段形塑不同的攻防思維。中國大陸至今已具有一定規模之網路攻防能量，對於全球企業，甚至各國政府均可能造成重要情資竊取

及系統癱瘓之事件，此為我們應警覺與高度關注之處。網路攻防的發起端可能涵蓋國家、公部門、學研機構、網路公民等不同層級，攻擊的路徑可能以借道多國伺服器、潛伏民間資訊設備端、儲存於全新資網通設備等方式，而攻擊的目標不僅是國家政府部門，亦包括特定的財經機構、媒體、公共設施及民間企業等。由此可知，網際戰爭具備複雜性及不可避免性，縱使兩國之間檯面上和平相處，交流頻繁，但國際間的網路戰爭將永不會停止。網際威脅是今日國家安全中最重要的議題，當國家政經發展、軍事組織及整個社會對於網路的依賴性愈大，網路作戰攻防、安全與管理等議題就愈顯重要，並應列為國家安全整體規劃的一部分。

本研究以詞彙探勘與分群技術來探討中國大陸網路作戰的發展，並建構具層級性的議題連結關係。透過實證探索之流程設計與成果討論，本研究除以軍事觀點切入網路作戰之主軸及建構層級式分群概念外，同時也探討相關網路作戰內涵對於國家安全政策與一般性企業組織之影響。故本論文研究成果不僅可從客觀的角度瞭解對岸學者於網路作戰議題的整體觀點，也可做為我方政府在軍事或民間發展網路作戰安全與管理相關事務之借鏡。

依據研究成果之特性，提出相關建議說明如下：

一、深植網安防駭素養，推動全民網路防禦作戰思維

網際威脅來源多樣，網安問題影響深遠，任何個人或電腦端的弱點突破，可能就造成企業組織，甚或國家層級資訊網路的大災難。故應育網安概念於日常活動之中，以深植網安防駭素養於自我認知及理解之下。因此，建議仿全民國防之概念，定期向全國電腦網路使用者推廣基本的網安認知及建立防護能量，甚至可仿全民英檢方式舉辦網路安全能力檢定，各政府機關或企業組織可依據自己產業之特性，決定員工的網安能力層級，讓全民網戰暨防駭的思維深植於工作及生活之中。

二、設計全國性網安聯防機制，落實網路攻防人才培育

目前行政院資通安全技術服務中心已將全國區分為五大區域聯防中心，分別負責維護與處理區域政府組織之資安事件。然而，相關聯防架構多為政府機構間之橫向聯繫，對於各層級的深化與民間企業之連結關係則較為不足。故應從全國觀點建構重要部會及相關產業的網路安全防禦作為，強化網路端、系統端到用戶端的作戰防禦縱深，建立「多層次防護、及時性管控」之資安防護網，以提升全國性的防禦能量。資訊網路安全不分平/戰時，我方應隨時掌握最新威脅情資及網通技術、適時調校設備部署、持續強化安全管控，重點置於防制惡意之網路入侵、破壞、封鎖、竊取等行為，以維資訊網路安全。

此外，網路戰力除植基於國家的軟、硬體實力外，更要重視作戰攻防人才的籌獲及培育。相較於對岸將網路作戰組織深植於學校及民間產業，我方在作戰組織編成上仍欠缺機動性及整合性。故建議以「推廣教育普及化」、「專業技能深入化」及「人才培育長期性」三項準則進行網戰教育訓練及人才培育之規劃與開發；其中推廣教育為建立網安防駭素養的一環，專業技能則可透過學研單位及民間駭客團體的整合，深化網路攻防人才之養成，並提供長期性的技能深化，以培育並建構未來軍/民聯合網路作戰之人力資源。

三、提升民生暨公共設施系統於網際網路環境運作之安全性

網路作戰目標不限於軍事機構及設施，若民生基礎建設遭到破壞將造成經濟數據、能源供應或心理恐慌等各面向的威脅。SCADA（supervisory control and data acquisition）係指以電腦設備為基的民生基礎建設關鍵系統（如電力、給水、石油、化工等領域），它可以對現場的營運設備，提供監視、控制，資訊蒐集及參數調節等功能。目前 SCADA 系統與網際網路連結的比例已逐年增加，且已發現存在若干網安漏洞，嚴重威脅公共設施運行之安全。故 SCADA 系統近年來已成為駭客攻擊的目標，同時在網路戰爭相關論述中，鏈結至 SCADA 系統以造成民生基礎建設的破壞及威脅也愈來愈明顯（Nicholson et al. 2012），甚至有學者認為真實的網路作戰是從此類威脅被發現後才真正開始（Chen 2010）。

目前我方政府已積極關注此類攻擊事件及影響，本研究建議行政院組織專案小組，針對國內各項大型公共設施系統進行診斷及評估；以技術面掃瞄並偵測系統可能存在之威脅，適時修補防護；同時以政策面規範該類系統連網的具體流程及防禦作為，以降低網路作戰安全與管理之風險。

四、強化資訊安全管理能量，形塑組織網路安全文化

依據英國政府近年的調查報告顯示，企業於網路損失的型態區分為智財權、工業間諜、勒索、竊取及客戶資料外洩，受害最嚴重的產業則包括生技製藥與電子資訊等。近年來，由於個資法的影響，許多企業組織面臨資安管理的多重挑戰。企業除遵循標準建構組織的資訊安全管理制度（information security management system; ISMS）外，也應針對個資條例所衍生的各項風險來建構資料防護機制。此外，因應網站被破壞及癱瘓的事件不斷在網路攻防過程中發生，建立緊急復原流程及相關防制能量就非常重要，同時也要強化企業演練的機制。

資訊及網路安全係每一個組織成員的責任，故必須深耕於組織文化之中。資訊安全文化係指組織成員所共享的資訊安全態度、價值、規範及實務，以支援所有組織活動，建立內外部參與者之間的信任（蘇建源等 2010）。網路安全文化受

到教育宣導及規範懲處之內外在激勵的影響，故需從持續性的教育訓練及明確的標準規範來強化組織成員對於網路安全的重視，進而形成組織的網安文化。透過該項文化的養成，確保組織成員具備網路防禦之意識及能量。

五、擴編網路作戰組織，建構平/戰時網路攻防作戰策略轉換及協同演習機制

國防安全為國土安全的第一線，國軍落實「網路作戰安全」就是確保國土安全的基本要求。目前國軍網路作戰之攻防整備與演練，係由參謀本部轄下的資電作戰指揮部負責（簡華慶 2012），加上國安與情報等相關單位定期的滲透及情蒐，並適時與行政院技服中心、科技部等單位協調運作，形成國家層級的網路攻防架構。然而，網際空間之對抗作戰需要具備資網專業及作戰策略等能力的人才及民間各項網路基礎環境的支援，故為確保我方的網路攻防作戰優勢，應探究民間資訊運作設施與相關安全防護能量於平時與戰時（緊急狀況）納入國家整體網路作戰攻防作為之可行性與具體作法，同時訂定相關執行規範與建立可行之運作機制，達成「平時維運，戰時管控」的目標。

因此，除需由政府適時成立或擴編相關機構外，亦應納編民間駭客組織，輔以產、官、學、研各界之整合能量，來建構網路作戰協同演訓架構及流程，將網路攻防能量深植於軍方與民間的合作，期望加速平/戰時網路作戰策略轉換的模式，以對抗或反制他國網軍之攻擊。

六、參照對岸網戰佈建及相關作為，建構網際空間指管能力

網路作戰在攻防兩大面向的各項資源投入具極大差異。攻擊面向著眼於非對稱式的能力結構，網際空間存在多樣的網攻方法及工具，且需要的知識技能要求亦不高，即可達成基本的攻擊；反之，防禦面向則需要多區域、多層次的人力、財務及軟硬體設備的投資，方可達到基本之防護能量。故防禦代價及成本均遠高於攻擊面向的投資。以敵為師，參照對岸網戰發展之重點及相關作為，來思考我方網路戰力的佈建，可聚焦重點投資之攻防內容。

網路作戰的精神在於攻防之間的賽局對抗，防禦雖為抗衡敵方網路攻擊的首要工作，但若僅採取消極或被動的防禦作為，或關閉對外網路的連線，不僅無法達成防護之目的，也容易造成戰場氣勢的衰落。因此，我方除應強化重點防禦之能量外，亦應參酌世界先進國家或中國大陸在網路攻擊方面的手段與方法，以「寓防於攻」的網路作戰概念，發揮以小搏大的不對稱作戰能力。此外，網際空間既然為軍事作戰之新興戰場，正規部隊作戰指揮官就必須了解網際攻防之特性，具備網際空間指管能力，同時針對敵方的各式攻防作為能夠通盤理解，才能於網際

空間中穩佔制敵先機。

綜上所述，網際空間沒有絕對性的安全，尤其在具有意圖式的作戰思維概念下，安全威脅無所不在。特別在政府開放資料（open data）風潮盛行之際，如何確保國家機敏資訊的安全性及洩漏風險，是我們必須積極重視的問題。因此，在不同面向均應考量網路作戰潛在之意涵及影響，除充分了解網路作戰安全架構下的威脅來源、發生機率與衝擊程度，同時建構以多面向縱深防禦觀點為基礎的網路作戰安全與管理架構，劃分全國性網路安全區域，建立網安訊息預警、防護、偵測、危機處理、災難復原，甚至適度回擊的網路攻防程序。

當今資訊社會的運作核心是電腦及資料交換的網路環境，世界各國持續發展資訊技術，並針對傳統工作模式進行改革。不論民間或軍方，亦不論平時或戰時。中國大陸近年來的政經環境與軍事作為等發展，屢屢受到世界各國所關注，尤其是植基於網路作戰的不對稱戰爭形態，勢必為其重要的國家作戰手段。

本研究建構網路作戰安全與管理主題的分析模式及實證探索流程，相關成果亦融入實務觀點來討論不同類別及層級中所呈現之意涵，同時提出多項具體發展建議。對於中國大陸在網際空間中的作戰安全與管理各項議題的瞭解，應具有其價值性。在此建議幾點未來值得進一步探討的方向：

1. 以本研究為基礎來擴增網路作戰相關詞彙，並延伸至國際性的網路作戰議題，探討不同國家在網戰策略思維上的差異性。
2. 本研究僅蒐整 2000-2010 年期間的資料，各項群集分析的成果係為整體性之觀察，並未探討不同時間區段或特定事件發生後之議題轉換與趨勢分析。未來除可持續蒐整跨類型的相關資料外，亦可嘗試建構不同時間週期的主題探索及相關趨勢。
3. 由於雲端運算環境、物聯網、巨量資料分析等技術的發展，未來網際空間的複雜性及資安要求勢必持續增加。因此，網路作戰策略發展及攻防技能的養成亦可能形成新興的作戰觀點，值得進行深入探究與分析。

誌謝

感謝兩位匿名審查委員的諸多寶貴意見，使本論文之內容更臻完善；本研究承蒙行政院國家科學委員會專案經費支持（計畫編號：NSC 98-2410-H-606-006-MY2 & NSC 102-2410-H-606-007），謹致謝忱。

參考文獻

Brett, T.W.（2011），『網際空間作戰的十大論點』，*國防譯粹*，第三十八卷，第八期，頁 4-17。

Magnuson, S.（2006），『網路戰：美國國防部憂心其網路漏洞』（宋家駒譯），*國防譯粹*，第三十三卷，第十二期，頁 25-28。

何全德（2013），『從虛擬國境防護趨勢看政府資通安全策進方向』，*資訊安全通訊*，第十九卷，第二期，頁 40-52。

吳嘉龍（2013），『網路科技發展與資訊安全管理研究探討』，*危機管理學刊*，第十卷，第二期，頁 79-86。

呂登明（2004），*信息化戰爭與信息化軍隊*，解放軍版社，北京。

李承禹（2007），『中國網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用』，*復興崗學報*，第九十期，頁 245-264。

林頌堅（2010），『利用自組織映射圖技術的研究主題視覺呈現及其在資訊傳播學領域的應用』，*圖書資訊學研究*，第五卷，第一期，頁 23-49。

姜國輝、楊喻翔（2012），『應用增長層級式自我組織映射圖於歷年研究主題圖之呈現』，*圖書資訊學研究*，第六卷，第二期，頁 1-35。

施東河、黃于爵（2003），『網站入侵偵測系統之分析與研究』，*中華民國資訊管理學報*，第九卷，第二期，頁 183-214。

張景皓（2013），韓國爆發史上最大駭客攻擊：下午 2 點硬碟自動銷燬，iThome 網站，http://www.ithome.com.tw/node/79400（存取日期 2014/06/30）。

梁華傑（2008），『網路戰資訊安全探討與省思』，*國防雜誌*，第二十三卷，第二期，頁 103-120。

梁德昭、朱志平、林凱薰（2012），『國家主權延伸至網路空間之討論』，*前瞻科技與管理*，第二卷，第二期，頁 1-14。

陳文華、施人英、吳壽山（2004），『探討文字採掘技術在管理者知識地圖之應用』，*中山管理評論*， 第十二卷，特刊，頁 35-64。

陳巍（2010），『黑客攻擊的防範措施和黑客技術應用的思考』，*湖南科技學院學報*，第三十一卷，第七期，頁 79-81。

湯添福（2009），『中共信息戰之研究』，未出版碩士論文，國立中山大學中國與亞太區域研究所，高雄市。

新華網（2010），英國智庫稱未來戰爭將從大規模網路攻擊開始，http://mil.eastday.com/m/20100208/u1a5009305.html，（存取日期 2014/06/30）

楊喻翔、釋惠敏（2011），『安寧療護文獻之計量研究：1952-2009』，*安寧療護雜誌*，第十六卷，第一期，頁 42-61。

蕭懷湘（2010），『中共培育網路對抗人才之規劃及展望』，*前瞻科技與管理*，特刊，頁 105-120。

戴元峰、吳騏、薛義誠（2013），『「科技訊息分群圖譜」導入政府決策支援系統之應用』，*公共行政學報*，第四十四卷，頁 113-160。

簡華慶（2012），『網路資訊戰所扮演角色及因應策略之研究』，*國防雜誌*，第二十七卷，第一期，頁 122-138。

簡禎富、李培瑞、彭誠湧（2003），『半導體製程資料特徵萃取與資料挖礦之研究』，*中華民國資訊管理學報*，第十卷，第一期，頁 63-84。

蘇建源、江琬琯、阮金聲（2010），『資訊安全政策實施對資訊安全文化與資訊安全有效性影響之研究』，*資訊管理學報*，第十七卷，第四期，頁 61-87。

翟文中（2003），『公開資訊在情報研析之價值』，*國防雜誌*，第二十三卷，第一期，頁 126-134。

Air Force, U.S. (2005), *Information Operations*, Washington DC: Department of the Air Force Doctrine Document 2-5, USA.

Armistead, L. (2010). *Information operations matters: Best practices.* Potomac Books, Inc., USA.

Börner, K., Chen, C. and Boyack, K.W. (2003), 'Visualizing knowledge domains', *Annual review of information science and technology*, Vol. 37, No 1, pp. 179-255.

Choo, K.K.R. (2011), 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, Vol. 30, No. 8, pp. 719-731.

Chen, T. (2010), 'Stuxnet, the real start of cyber warfare?', *IEEE Network*, Vol. 24, No. 6, pp. 2-3.

Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2010), *On Cyber Warfare*, Chatham House, London, UK.

Dittenbach, M., Rauber, A. and Merkl, D. (2002), 'Uncovering hierarchical structure in data using the growing hierarchical self-organizing map'. *Neurocomputing*, Vol. 48, No. 1, pp. 199-216.

DoD, U.S. (2012), Department of Defense Strategy for Operating in Cyberspace, http://www.defense.gov/news/d20110714cyber.pdf（存取日期 2014/06/30）

Falessi, N., Gavrila, R., Klejnstrup, M.R. and Moulinos, K. (2012), *National cybersecurity strategies: practical guide on development and execution*, European Network and Information Security Agency (ENISA), EU.

Ibrahim, L.M. (2010), 'Artificial neural network for misuse detection', *Journal of Communication and Computer*, Vol. 7, No. 6, pp. 38-48.

Kohonen, T. (1982), 'Self-organized formation of topologically correct feature maps', *Biological Cybernetics*, Vol. 43, No. 1, pp. 59-69 .

Kohonen, T. (1997), *Self-organizing Map*, Springer Verlag, Berlin, Germany.

Libicki, M.C. (1995), *What Is Information Warfare?* , National Defense University Press, Washington, D.C., USA.

Liles, S. (2007), 'Cyber warfare compared to fourth and fifth generation warfare as applied to the Internet', *Proceedings of the IEEE International Symposium on Technology & Society (ISTAS 2007)*, Las Vegas, NV, June 1-2, pp. 1-3.

Luiijf, E., Besseling, K. and de Graaf, P. (2013), 'Nineteen national cyber security strategies', *International Journal of Critical Infrastructures*, Vol. 9, No. 1, pp. 3-31.

Nicholson, A., Webber, S., Dyer, S., Patel, T. and Janicke, H. (2012), 'SCADA security in the light of Cyber-Warfare', *Computers and Security*, Vol. 31, No. 4, pp. 418-436.

Ortiz, A., Górriz, J. M., Ramírez, J. and Salas-González, D. (2013), 'Improving MRI segmentation with probabilistic GHSOM and multiobjective optimization', *Neurocomputing*, Vol. 114, pp. 118-131.

Pattie, M. (1994), 'Agents that Reduce Work and Information Overload', *Communications ACM*, Vol. 37, No. 7, pp. 30-40.

Salton, G. and McGill, M.J. (1986), *Introduction to Modern Information Retrieval*, New York: McGraw-Hill, NY, USA.

Shi, H., Hamagami, T., Xu, H., Yu, P. and Wu, Y. (2012), 'A method for classifying packets into network flows based on GHSOM', *Mobile Networks and Applications*, Vol. 17, No. 6, pp. 730-739.

Shih, J.Y., Chang, Y.J. and Chen, W.H. (2008), 'Using GHSOM to construct legal maps for Taiwan's securities and futures markets', *Expert Systems with Applications,* Vol. 34, No. 2, pp. 850-858.

Vicente, D. and Vellido, A. (2004), 'Review of hierarchical models for data clustering and visualization.', in Raúl Giráldez, José C. Riquelme and Jesús S. Aguilar-Ruiz (Eds), *Tendencias de la Minería de Datos en España.*, Red Española de Minería de Datos., Española, USA.

Williams, B.T. (2011), 'Ten propositions regarding cyberspace operations', *Joint Force Quarterly*, Vol. 61, pp. 11-17.

Yang, Y.H., Bhikshu, H. and Tsaih, R.H. (2011), 'The topic analysis of hospice care research using co-word analysis and GHSOM', *Intelligent Computing and Information Science*, Vol. 134, pp. 459-465.

Yen, G.G. and Wu, Z. (2008), 'Ranked centroid projection: a data visualization approach with self-organizing maps', *IEEE Transactions on Neural Networks*, Vol. 19, No. 2, pp. 245-259.