從預警情報分析探討「社會網路組織分析法」之運用－以恐怖主義活動爲案例

汪毓瑋

中央警察大學教授兼通識教育中心主任

摘要：防範恐怖主義活動有賴於預警情報之掌握與分析，而欲掌握預警情報，其戰略包括了如何更佳的定義問題、如何增加資訊蒐集之途徑及發現細節之適當層次；此外分析過程中還必須處理不確定性與克服慣有思考，才能在預警之概念下找出不同之行動方向，與避免會產生震驚結果之不知覺的先期預設。而對於更複雜的、屬於非線性動態系統範疇之恐怖主義活動，要獲得事先防範之預警情報，惟有透過可進行連接節點之社會網路組織分析法才可能較佳的進行。

關鍵詞：預警情報，社會網路組織分析法、恐怖主義活動

綱要：

壹、　前言

反恐已是目前各國安全工作之重點，且恐怖主義組織之發展已走向串聯之地區性組織與鬆散之結構，且進行打擊之手段已更趨多樣化，並欲尋求任何可能攻擊之目標，此種威脅所引發的思考是 21 世紀的國家安全挑戰與以往已有完全不同的特徵，因此相對的也必須有與 20 世紀完全不同的工具、技術、資源與知識才能加以有效遏阻。

情報部門面對此種威脅，在蒐情與研析方面之工作必須不斷的精進，才能及時提供事先加以防範之「預警情報」。也由於恐怖主義活動是一種特殊的、非典型的行爲，需要連接不同的分析團體與資料庫，並從大量與不同之資料中，將可能代表潛在風險之不確定與不清楚之指標結合起來，才能偵測與避免恐怖份子之攻擊，因此「社會網路組織分析法」已漸成爲有效之運用工具。

本文之舖陳，是先從「預警情報」之作用談起，強調須經由事先徵候之發掘才能有效找出因應威脅之機會，而此有賴於預警分析能力之發展；且其運作之有效與否，端視是否能夠正確處理不確定性與克服慣有之思考。進而論及處理非線性且具動態特質之恐怖活動，惟有透過「社會網路組織分析法」之經由關係資料的萃取，並進行連接節點之分析，且須克服資料不完整與掌握動態變化之困難，

才能比較有效的因應來自恐怖活動的威脅。

貳、 預警情報

資訊時代，由於科技發展已侵入我們生活的每個領域，因此應將注意力集中於在此脈絡下如何獲得正確的資訊，並以正確的方式來加以利用。而從國家安全的角度言，這個資訊就是情報。且雖然在目前資料盈塞的「全球化」世界，資訊較以往更容易獲得，但是關鍵在於應該從「質」而非「量」的要求上，將資訊變成有效的情報。因此要控制資訊使其被使用者所用，卻不是使用者受困於數量龐大的資訊，以致於在面對威脅時無法有效解讀。而預警情報之功能就是在資訊超載之環境下，如何事先藉由發掘各種與威脅有關之初起徵候，並經由分析過程而認清威脅，進而找出機會之有效方法。

一、分析威脅與機會

威脅與機會有同樣的特徵，兩者都代表了合理、明確的事件將可能發生，且需要決策者採取行動以避免威脅或利用機會。而雖然比較上可以容易的定義威脅與機會，但是要把它們找出來、分析與避免或加以利用，卻相對的困難。此可從物理學與數學上之定律，證明出要做出長期之預測是非常困難的。

例如物理學上之「海森伯格不確定原則」（Heisinberg Uncertainty Principle），該原則認爲位置與動量雖可加以測量，但由於兩者是相互影響的，因此不可能同時得出精確值；換言之，你可知道在那裏有什麼東西，或是知道它是如何快速的移動，但是你不可能對兩者同時加以精確的掌握。又如近期之數學研究顯示，許多過程、特別是複雜與大型的過程，對於微量之改變都非常敏感，此種現象稱之爲「基於初始條件之敏感」（sensitive dependence to initial conditions），意即在實體之間的最輕微的不同、或是認爲實體將會如何行事，在每一段時間、或是經過一段時間之變化，都可能導致判斷錯誤。

然而藉由情報分析至少可篩選由正式或非正式管道湧入之大量資訊，且使其有意義，而將「資訊超載」（information overload）之負面現象減少；且藉由分析，在某種程度上仍可提供及時之預警，並經由持續追踪問題而掌握其持續變化；進而提出短期之預測，或找出要做出如此預測之額外資源，換言之，越困難的問題越需要涉及有用之科技及每日之追踪，分析人員必須對問題有其獨到之敏感度，且建議決策者那些問題可以有效的處理，那些問題不能；並要決定可能性之範疇，因爲任何問題均有其歷史源由，如果仔細檢證應該可以定出特定問題之可能脈絡，若一旦掌握此脈絡，要預測最可能之結果就相對的成爲可能。[1]

二、發展預警分析能力

經由分析以提供預警情報之思考戰略，包括了如何更佳的定義問題、如何增加資訊蒐集之途徑及發現細節之適當層次。要更佳的定義問題，就要避免「鏡射」（mirror imaging）之錯誤，亦即不要認知對手也與你有同樣的想法。而要改變鏡

[1] Kristan J. Wheaton , The Warning Solution : Intelligence Analysis in The Age of Information Overload (Fairfax , Virginia : AFCEA International Press , 2001) , PP.17-20.

射之想法就要根本改變對資訊之態度。一般有兩種可能之策略，第一、避免錯誤與無用之資訊；第二、要去除已根深蒂固之既定「公式」的思考。

但也要注意兩種發展，第一、你的某項認知是基於一些事實，但是你也發現有些可作爲依據之事實，但是它們可能彼此不相關或是與問題無關，因此事實上至少存有兩個情勢發展之推論。然而我們經常會依熟悉之行事準則或思考去行事，但是涉及到危機或是機會之情勢，卻經常是你所不熟悉的。第二、儘可能精確的定義問題，也就是如何能更縮小問題之範圍而更聚焦，且要以中性之名詞來定義問題，並避免以「是」或「不是」等性質之固定一種答案來定義問題，而要從各種可能之合理角度來建構問題。

就資訊蒐集之途徑言，有各種不同之資訊開發途徑可加以努力，但是要注意的是當已成功開發某些資訊來源後，經過一段時間之運作，資訊會如洪水般不斷的湧來，因而不再是資訊不夠而是要解決「資訊超載」的問題，因此必須進行有用資訊篩選之細緻化工作，才能產生作爲預警情報基礎之有用資訊。

就發掘細節之適當層次言，事實上要定義出細節之適當層次是有困難的，第一、它是取決於問題，而問題可以定義爲戰略、行動與戰術三個層次，戰略問題是大圖像的問題，欲解決這類型之問題是依賴於從一個部門到另一個部門資源之根本轉變；行動問題是在戰略問題之下的大範圍的問題，例如總統要型塑其新的外交政策，這很明顯是有全球意含的戰略問題，但是這個政策在亞洲或是南美洲如何能有效之履行，就是行動問題；戰術問題是僅衝擊到涉及戰略問題之小部分要素之問題，例如此新的外交政策如何可能改變台灣與美國公司間之關係，就是戰術問題。因此，欲發掘適當之細節，完全是依賴於你如何去定位且以什麼樣的立場去思考，例如總統、部長等立場去思考此問題之層次。第二、資料之細緻化過程對於某一個問題是有意義的，但是對另一個問題可能就是浪費時間。第三、要同時擁有問題三個層次之視野，才能在自己定位之問題層次上正確的處理問題。例如在行動層次上工作就不能失掉戰略層次之問題，且問題的最初指標是來自於戰術來源，三者是相互影響的。

此外，在進行預警情報分析前之首要工作，就是針對分析要項先進行自我評估，這些分析要項包括了政治、經濟、歷史、地緣、文化、宗教、軍事、科學與變遷等。而每次要掌握問題時，就使用這些分析要項當成一個「檢查清單」，藉此找出你可能的弱點，例如你可能專注於軍事而對經濟領域關注較少，此種情況就必須加以修補，而能對於各種分析要項採取比較平衡之途徑，才不致於失掉重要資訊。其次，應嘗試進行連接人與體制之分析架構，因爲與每一個問題有關之重要資訊，均可能是來自於不同領域之資訊，而必須連接以進行整合分析，例如政治、經濟、歷史、地緣、宗教、軍事與科技等，但是要注意避免陷入以往思考之窠臼而造成誤導。[2]

[2] Ibid , PP.49-55.

參、預警情報之運作

「九・一一事件」之發生，不論是美國的輿論、學界、政壇與聯邦國會議員們概均一致指責係情報單位之重大情報失敗，他們的簡單推論，就是「蓋達組織」的威脅早已有之，且蒐集到之情報亦加以證明，但是政府卻不重視而故意忽略，或是錯誤的分析及錯誤的使用。例如在 2004 年 4 月 10 日被迫公布之 2001 年 8 月 6 日向布希總統提報的「總統每日簡報」（PDB）之標題，就已明確表明「賓拉登決定要攻擊美國」（Bin Ladin Determined to Strike in US）；[3]又如白宮前反恐事務之總統顧問克拉克（Richard A. Clarke）在其《反擊一切敵人》之專書中亦有如此之看法。[4]

然就情報之完整性言，情報本來就是藉由拼湊而欲達成一個較完整之圖像，而有其不完整性；它的蒐情目標也經常是難以捉摸的；且恐怖份子經常會藉由封鎖資訊而使對手無法瞭解真實情況之「否認」（denial）技術，與藉由某些措施而使對手誤信某些事情是真的之「欺騙」（deception）技術，以混淆情報之精確性，[5]而使蒐情者與分析者陷入模棱兩可與不確定之狀態；加諸恐怖組織不同於一般犯罪組織而難以滲透，[6]因此僅從「震驚」結果來指責情報失敗，可能是不公平的。[7]但是從預警情報之角度檢討，對於「九・一一事件」所應記取之教訓，應是整個情報圈缺乏對於如何維持一個有利於針對廣範圍國家安全威脅之情報蒐集、與因之據以進行分析之堅強且適當資源之關注。

且由於目前已被視爲恐怖組織代表之蓋達組織（Al Qaeda），其發展已傾向於非中心化組織、更彈性之運作方式，及藉由各種組織性犯罪手段，與透過更多有掩護身份之非政府組織等多元之管道，去籌募資金，因此必須要利用互補、協作、競爭性分析與分工。因爲沒有必要且也不可能每一個人均能很好的掌握每一件事，也不能設想那一個情報單位對於所有議題均能做出同樣高品質之判斷，因此我們的判斷不應該是基於「多數部門相信」就作出來的，而是基於對問題「最可信知識」來作出的。也因此所需要的是可以進行比較與可有專業水平的學者與專家，以提供更多的資訊與可被思考的觀點，也由於這麼多不同層面之努力，所有對於恐怖主義組織運作之預警情報需求，才能經由情報圈不同專家的整合來達成。

在從事預警情報之前，情報圈要能自我檢測工作表現，特別是針對分析產品

---

[3] “Bin Ladin Determined To Strike in US “, President’s Daily Brief , 6 August , 2001 . http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB116/pdb8-6-2001.pdf

[4] Richard A. Clarke , Against All Enemies : Inside America’s War on Terror (New York : RAC Enterprises , INC . , 2004) , PP.1-34, 227-247 .

[5] Roy Godson and James J. Wirtz ed., Strategic Denial and Deception : The Twenty-First Century Challenge (New Brunswick , NJ : Transaction ,2002) , PP1-2 .

[6] James F. Hoge , Jr., and Gideon Rose ed., How Did This Happen? Terrorism and the New War (New York : Public Affairs , 2001) ,P.160 .

[7] Stephane Lefebvre , “A Look at Intelligence Analysis “, International Journal of Intelligence and Counterintelligence , Vol. 17 , No. 2 , April/June 2004 , PP.231-232.

的品質與可用性，亦即對於恐怖組織運作之判斷，要經由不斷循環之嚴格的「事後檢討分析」（post-mortem analysis），來發現什麼做對了、什麼做錯了。如果發現做錯了，則要檢討爲什麼會做錯？才能確保不會再犯同樣的錯誤。也需要有「替代性判斷」（alternative judgements），才能確保我們真的做對了。此外，對恐怖組織運作之預警情資要及時送給正確的人，而一個簡單但重要的指導原則就是將情資的來源、方法和內容分開來，如此在最低的機密層級下，內容就可以廣泛、且很容易的分享。而要能運作，蒐情者必須要有很清楚的方法去顯示機密等級，如此可信的資訊與友善使用之程序，就可提供情治人員防範蓋達組織發動攻擊之額外資訊。[8]

一、 處理不確定性

傳統之預警情報分析，其組成首先是經由對描述情境之資訊的評估，然後預測其未來之發展。[9]然情報分析並不是尋求以任何一種精確之措施來預測未來，而是在預警之概念下找出不同之行動方向，例如最危險的、最可能的及最不可能的方向，[10]而其過程中首要處理的就是「不確定性」。

不確定概念是由資訊鴻溝，可能之欺騙，與單一之脈絡混合而成的，且「不確定」是情報的重要特徵，但是它可以藉由使用邏輯、相關之方法、分析技術、與更佳的蒐情來努力克服，且其中最重要之關鍵就是要對政策消費者「透明化」其判斷，而使其有信心採用經由分析而做出之預警情報。

而一般處理不確定性或是模稜兩可資料有兩個辦法，一是建立標準，情報分析者可根據五個關鍵之行動標準去建立其判斷，即藉由使用比例、更佳的可能性、在那裏是可能的、及避免過度聲稱其判斷之必然性；清楚說明其假設與判斷；發展與探討「可取代之未來」（alternative futures），亦即較少可能性之情節如果發生的話，也可能激烈的改變判斷；允許對於預測或詮釋之異議，且當可能對議題造成重大後果之資訊鴻溝存在時，要清楚說明情報圈不知道之事項。[11]

其中，假設是根據「預先警戒原則」（precautionary principle）而做出的，即當什麼時候某種行動會升高危及人類健康或是環境之威脅，且既使一些因果關係並不是充分的科學性建立，也必須採取預先警戒之措施，[12]此原則也導致了採取

---

[8] Collin Powell , “ Powell Says Strong National Intelligence Director Essential “ , International Information Programs of Department of State , 13 September , 2004 . http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2004&m=September&x=20040913181047adynned7.096499e-02&t=livefeeds/wf-latest.html

[9] Andrew Ilachinski , Land Warfare and Complexity , Part II : An Assessment of the Applicability of Nonlinear Dynamics and Complex Systems Theory to the Study of Land Warfare (Alexandria , VA : Center for Naval Analyses , CRM 96-68 , 1996) , P.58.

[10] Lodh K. Johnson , “ A Framework for a Theory of Strategic Intelligence “ , the 43rd Annual Convention of the International Studies Association (New Orleans , LA) , 23-27 March , 2002 . P. 12 .

[11] US General Accounting Office , “ Foreign Missile Threats : Analytic Soundness of Certain National Intelligence Estimates “ , NSIAD-96-225 , August 1996 , P.2. Joseph S. Nye , Jr. , “ Peering into the Future “ , Foreign Affairs , Vol. 73 , No. 4 , 1994 , P. 82. Stephane Lefebvre , op. cit., P.247.

[12] D. Appell , “ The New Uncertainty Principle “ , Scientific American , Vol.284 , No. 1 , January 2001 , P.18.

「先期作爲」（preemptive actions）之可能性與合理藉口。另一是進行「不同分析」（disparity analysis），即進行對於從事同樣項目分析之不同分析者間之分析與判斷的比較，而找出不同之背景與觀點。藉由此兩個辦法以找出鴻溝、錯誤與分歧。[13]

二、 克服慣有思考

慣有思考（mindset）的簡單定義，就是人類檢視世界所產生的一系列預期。且這些預期的產生，是基於過去的事件是如何發生的，是從重要國際現象間之關係、是關於一個國家其傳統上是如何行事等去做出結論。因此，當新的事件發生，只要是符合過去所堅信模式之有關資料，就會被接受且視爲有價值；若這些資料是和過去所預期相衝突的，就不會被接受。[14]

然就恐怖主義之威脅言，其目的就是要造成「震驚」之效果才能達成其宣傳之訴求目的，換言之，只有不被預期才會獲得如此結果。而此可證之於「九・一一事件」之所以事前未被預警的部份原因，就是情報分析人員在慣有思考下，認爲恐怖份子不會對美國本土發生攻擊之既定預設。事實上，此亦凸出了從事預警情報分析過程中，若沒有「想像」比沒有資訊更危險之事實，因此預警情報要能發揮作用，就必須先克服慣有思考。

克服慣有思考以提升預警能力之技巧有很多，例如可以經由「轉換性分析」（Linchpin analysis）之五項步驟，第一、找出可能決定結果的重要不確定要素或是關鍵性變數；第二、找出關鍵部份如何運作之工作性假設；第三、增進可信之證據與理由以支持工作性假設；第四、處理任何會造成工作性假設不能信任的指標；第五、檢討什麼樣的激烈事件可能會反轉預期結果。[15]此外，尚可運用「取代性分析」（Alternative Analysis）之途徑，其範疇包括了「關鍵假設之檢證」（Key Assumptions Check）、「戴維斯倡言」（Devill’s Advocacy）、「體制內、外比較分析」（Team A/Team B）、「假想敵分析」（Red Cell Analysis）、「偶發之假如…分析」（Contingency What If Analysis）、「高衝擊/低度可能性分析」（High Impact/Low Probability Analysis）、「模擬分析」（Scenario Analysis）等，而各有其作用。[16]

肆、社會網路組織分析法

欲進行對恐怖主義活動之預警情報分析常有其困難，因爲恐怖份子的行爲是處於純粹的混沌（chaos）與完全的決定性範疇，代表的是一種非線性的動態系統；其行爲模式雖展現爲規則性、但是卻非定期性的，換言之，在地區上是隨意的、但是在全球上是可被清楚定義。且分析恐怖主義、特別是目前蓋達組織之發展與運作模式，不像是分析中國海軍力量或是東南亞政治體系，這些分析是基於

[13] Stephane Lefebvre , op. cit., P.246-248.

[14] Roger Z. George , “Fixing the problem of Analytical Ming-Sets : Alternative Analysis” , International Journal of Intelligence and Counterintelligence ,Vol. 17 , No.3 , July-September ,2004 , PP.386-387.

[15] Jack Davis , “Changes in Analytic Tradecraft in CIA’s Directorate of Intelligence “, Product Evaluation Staff/Directorate of Intelligence , April 1995 , P.8.

[16] Roger Z. George , op. cit., PP.393-398.

已有完善定義之指標與資料來源。然而恐怖主義分析之資訊結構，卻是高度的破碎、缺乏良好定義之連結、及經常伴隨著欺騙，且要從少量片斷之資訊推論恐怖分子特定之戰略與計畫，要從表面上不同之要素中發現共同之線索，且不像恐怖分子只需要單一之弱點來加以利用，分析者卻要思考所有潛在之可能弱點。[17]

也由於恐怖分子易於躲藏且利用每個機會進行欺騙，其組織又難以滲透，加諸分析者不熟悉恐怖分子之語言與文化，亦無法有效掌握其企圖與能力，因此面臨的是高度的不確定性與資訊之缺乏。而發展所需要之專家又緩不濟急，致分析者需要從不完整之證據中抽離出其「意義」，使用既有之知識、經驗、專家與洞見，以補充缺乏證據與一直存在之模棱兩可的分析困難，[18]且其中最大之困難就是如何能夠事先比較具體的發掘恐怖分子欲進行攻擊之人、地、時與方法等之問題，亦即必須事先找出恐怖份子個別與群體間之關連與如何進行互動之模式，才有可能進行事先預警免於攻擊之發生，而社會網路組織分析（Social Network Analysis）應是可加以運用之方法。

該法是聚焦於如何去發掘未經揭露之人員互動之模式，是假定社會結構可以經由運動與接觸來明顯的加以說明，且這些互動不是隨機任意的、而是有概固定模式的。因爲，我們可以經由極小的「節點」（dots）來加以觀察，然後可以發現這些節點不是隨機任意的互動，有的是經常接觸、有的是偶而接觸、且有的是從未接觸。且相信一個人如何行動，是與更大之社會連接網相互聯結的。此種分析方法是由以數字、名詞加以組織之正式理論來引導，其中包括了組織理論、混沌理論等；且是進行經驗性資料之系統性分析。而其涵蓋面經常涉及到的是組織間之接觸（interorganisational networks）、組織內之接觸（intraorganisatonal networks）及又可區分爲正式與非正式組織內之接觸。[19]

一、以弋爾（Ted Robert Gurr）分析法爲基礎

是一種對恐怖主義研究之戰略分析途徑，而能協助分析者在不同之脈絡與層次上安置其問題。其後，「國防情報學院」（Defense Intelligence College）亦以此途徑爲基礎，提出《反恐怖主義情報分析方向》（Counterterrorism Analysis Course）之套案，其內容包括了事件前指標、資料庫設計與發展，分析工具，時間與事件圖表及案例研究等。但是此途徑仍未能解答人、地、時與方法等類型之問題，而是置焦點於減少資訊之鴻溝，提供充分有附加價值之材料，以協助政策規畫者尋求解決恐怖主義之方案。[20]

其研究設計是由五個層次構成之分析架構，分別是全球、國家、組織、事

---

[17] Jeffrey A. Lsaacson and Kevin M. O’ Connell , “ Beyond Sharing Intelligence , We Must Generate Knowledge “ , Rand Review , Vol.26 , No. 2, Summer 2002 , P. 49 .

[18] Lowell E. Jacoby , “ Information Sharing of Terrorism-Related Data “ , Statement for the Record before the Joint Intelligence Committee of the U. S. Senate and U. S. House of Representatives Investigating the Events Leading to the Attacks of 11 September 2001 , Public Hearing (Washington , DC: 1 October 2002) , P.3.

[19] John Scott , Social Network Analysis : A Handbook (London : SAGE Publications , 2001) ,PP.1-5.

[20] “Introduction To Terrorist Intelligence Analysis” , Defense Intelligence College . http://www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm

件與個人，每一個層次均有自己之一組研究問題與方法。在全球層次上，從時間、空間與戰術之角度檢視趨勢，擴散之過程，及恐怖主義是國家間衝突自然生長出來的，且提出地緣之趨勢分析是適當的方法。在國家層次上，檢證那個地方之恐怖主義最佔優勢，恐怖分子活動之趨勢與擴散模式，國家打擊恐怖主義之政策，引起恐怖主義之政治脈絡，及恐怖主義運動之衝擊，在此層面分析之主要目標是找出恐怖主義之原因。在恐怖主義組織層次上，檢視其社會/經濟起源，意識型態，組織，國際之聯結及其興衰。在事件分析之層次上，強調要研究攻擊目標之弱點，事件之結果，談判策略，與媒體之效果。在個人之分析層次上，注意甄補與訓練，動機，與恐怖活動對人質之衝擊。[21]

二、建構與分析「連接節點」

（一）關係資料之萃取

「九·一一事件」發生後所引起的質疑，就是爲什麼美國政府不能夠做到「連接節點」（connect the dots），亦即挑選與組合不同之片斷資訊，而產生對威脅之普遍性瞭解，[22]進而將相關資訊整合起來並事先提出防止攻擊之預警。研究之起步經常是提問「誰認識誰」？「那些個人與組織彼此互動，且如何進行」？分析之目的是要找出誰是主要的行爲者，以及他會採取什麼樣的立場與行動，所強調的是對「關係資料」（relational data）之分析。

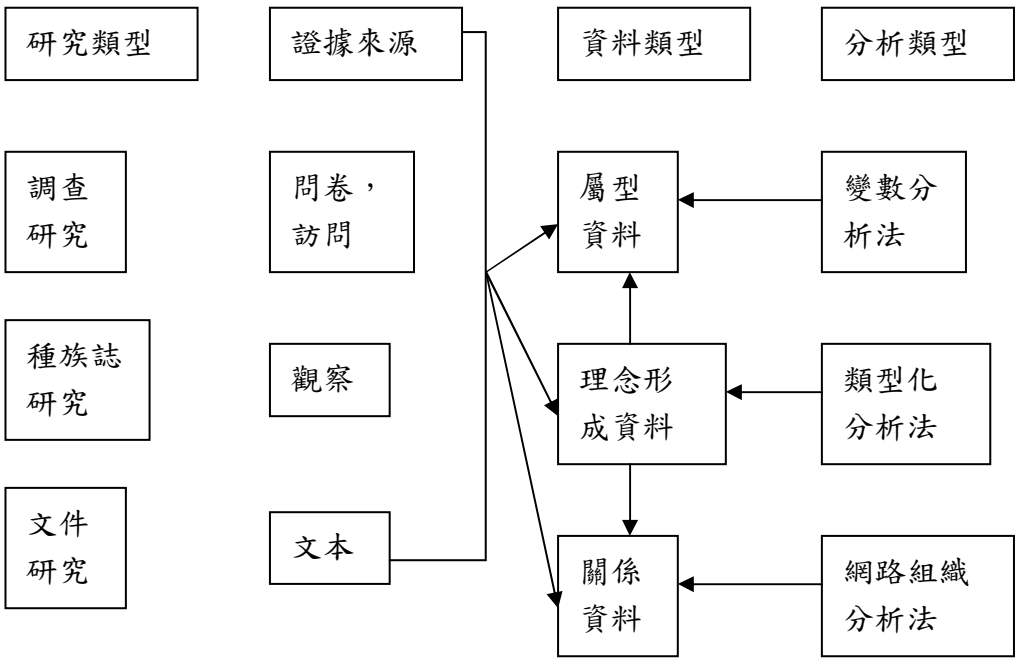
本質上，社會科學的資料與自然科學的物理資料不同，是基於文化價值與符號，是經由意義、動機、定義與類型化且透過詮釋而形成。一般有三種資料類型，即「屬型資料」（Attribute data），是關於個人或團體之態度、意見與行爲之資料；是經由調查與訪問來加以蒐集；而與其相應之方法是「變數分析法」（variable analysis），例如測量收入、職業與教育等。「關係資料」，是關於個人或團體之接觸、關係與連接等，而不是以獨立之個人或團體之屬性爲主之資料；關係指是連接之個別系統，注意的是連接成組之個別關係而成爲一個更大之關係體系；而與其相應之方法就是「網路組織分析法」。「理念形成資料」（Ideational data），是用來描述意義、動機、定義與類型化本身；而與其相應之方法是「類型化分析法」（typological analysis）。而在同一個調查研究之過程當中，此三種類型之資料經常是作爲整體分析不可分割的部分，如下圖。[23]

---

[21] Ted Robert Gurr , “Methodologies and Data for the Analysis of Oppositional Terrorism “, Symposium on International Terrorism（Washington , DC）, Defense Intelligence College , 2-3 December 1985 .

[22] John Hollywood , Diane Snyder , Kenneth McKay , and John Boon , “Out of the Ordinary : Finding Hidden Threats by Analyzing Unusual Behavior “, Rand Corporation , 2004 , P.iii.

[23] John Scott , Social Network Analysis : A Handbook (London : SAGE Publications , 2001) ,PP.1-5.



（圖示係源於 Social Network Analysis : A Handbook 之資料）

情報部門之功能在於能夠找出與追踪恐怖份子與其它的犯罪活動等，然情報單位所獲得的大量資訊，不是僅靠人力就可充分分析，必須藉由資訊技術以發現與瞭解新的與之前已獲得資訊間之重要連接，才可能完成分析並得出結論。所需要的就是在大量資料中，可顯示已發生或是將要發生之模式。如此大量的資料在本質上就是一種關係形式，換言之是儲藏在關係的資料庫中，且可預期在短期的未來會大量的增加。因此需要可以協助分析者對於關係資料可加以發現與說明證據之技術，也可以透過電腦而藉由特殊設計之檢索系統來加以輔助。[24]

而目前至少有三個不同之技術可以用來協助分析關係資料，第一、對於已知模式之資料，要發現其相吻合之處。困難的是當資料龐大，或是因爲不當的蒐集與處理致資料有遺漏之錯誤，或是當實體有意去欺騙或隱藏其行動時其適用性就可能受到影響，例如已知的洗錢模式可以用此種方法加以處理。第二、要發現與已知模式資料不相符之異例，這是基於去找出有那些事情是不符合規範之理念，而不論是否企圖加以隱藏，我們均可以發現事情的真實本質。一般言，此方面努力之企圖也會由於阻礙發現符合已知模式的同樣議題而更惡化，例如這些技術可用於進行犯罪調查但亦須考量賄賂與犯罪活動結合之情況。第三、發現新的模式，至少有兩種形式，即一種是以「社會網路組織分析法」去分析所關切人員之互動類型與頻率，以分辨出追尋共同目標團體之行動；另一種是「資料採礦」(Date

[24] 例如已被使用之「多條件反恐信息交換系統」來進行比對檢索。若以「九・一一事件」之嫌疑犯爲例，該等劫機者似應滿足以下條件，即此人在事件發生前近一兩年才來到美國，有宗教背景、並應有銀行戶頭、借貸情形、電話帳單、水電費帳單與駕照等各種記錄，將這些資料輸入數據庫中進行檢索比對，而逐步找出嫌疑犯。楊晴川，「是誰第一個鎖定”九・11”疑凶」，中國國防報，2004 年 12 月 9 日。

mining），以發現新的指標模式而能找出不能直接觀察之有興趣的事件，這些技術可以用來發現秘密組織或是新的保險詐欺形式。[25]

（二）克服資料不完整與掌握動態之情勢

社會網路組織分析對反恐怖主義之貢獻，是能夠經由結構性之關係資料畫出恐怖份子團體中看不見的動態。例如經由每日對恐怖份子之監偵與嫌疑犯的接觸就能顯示環繞其周圍的網路組織，而能找出、或增加更多之節點與連接。一旦直接的連接被找出來，則其中的關鍵人物就可凸顯出來。[26]然而使用網路組織分析法仍須克服三項問題，第一、不完全性，調查者仍會有未發現之「節點」與「連接」；第二、模糊不清的界限，很難去決定到底誰應該包含在網路內，誰不應該包含在網路內；第三、動態，這些網路組織不是靜態，他們總是在改變。此外，既使使用更複雜的方法，例如測量恐怖份子網路組織之關係力量，可能也無法產生有用之網路圖形。其原因之一係許多決恐怖份子關係之要素是「之前的連接」，通常經過一段短時間後，此網路組織就會變得鬆散。[27]

（三）連結節點之具體步驟

要綜合片斷資訊以瞭解威脅是非常困難的挑戰，因爲此分析過程不但需要從大量的資料中加以搜尋有關之資料，且分析要能直接指出相關之重要發現外；亦可能由於對一些優先資料處理之常態途徑，亦即經常會將焦點集中於尋找與之前攻擊類似之模式，却錯失了顯示下一個截然不同攻擊之資料；且會面臨不確定、混亂的資料，及時間與情勢之壓力，而導致分析者經常在不確定之情況下作出結論；且現存對於分享與連接資訊之法律、技術程序與文化障礙，又進一步使得這些挑戰更趨複雜化。[28]

也由於要解決欲進行「連接節點」但所擁有資料相較國土安全環境現實爲少之困難下，應有之「六步程序」認知就是首先、分析者要有假如一切均是「正常」的情況下，即要定義現狀，則所面臨之環境將是什麼情況。其原因就是我們經常不可能對於所有之「非常態」加以預測，但相對容易的是可以「描述現狀」做爲起點，進而論證此現狀如何會改變；其次、要找出一組所觀察到且與環境有關之量化與質化之「換算法」（metrics），特別是關於是否現實環境與所期盼的是相一致的。第三、要觀察與環境有關之一連串測量資料。當然分析者不可能檢證所有之觀察資料，但是可以「掃瞄」所有與現狀不同之「例外的」與「非典型」之訊號。[29] 第四、一旦發現此例外的行爲，分析者就可尋求支撐性之資料（supporting

---

[25] SRI ," Link Analysis Workbench" , Air Force Research Laboratory , September 2004 , PP.1-2.

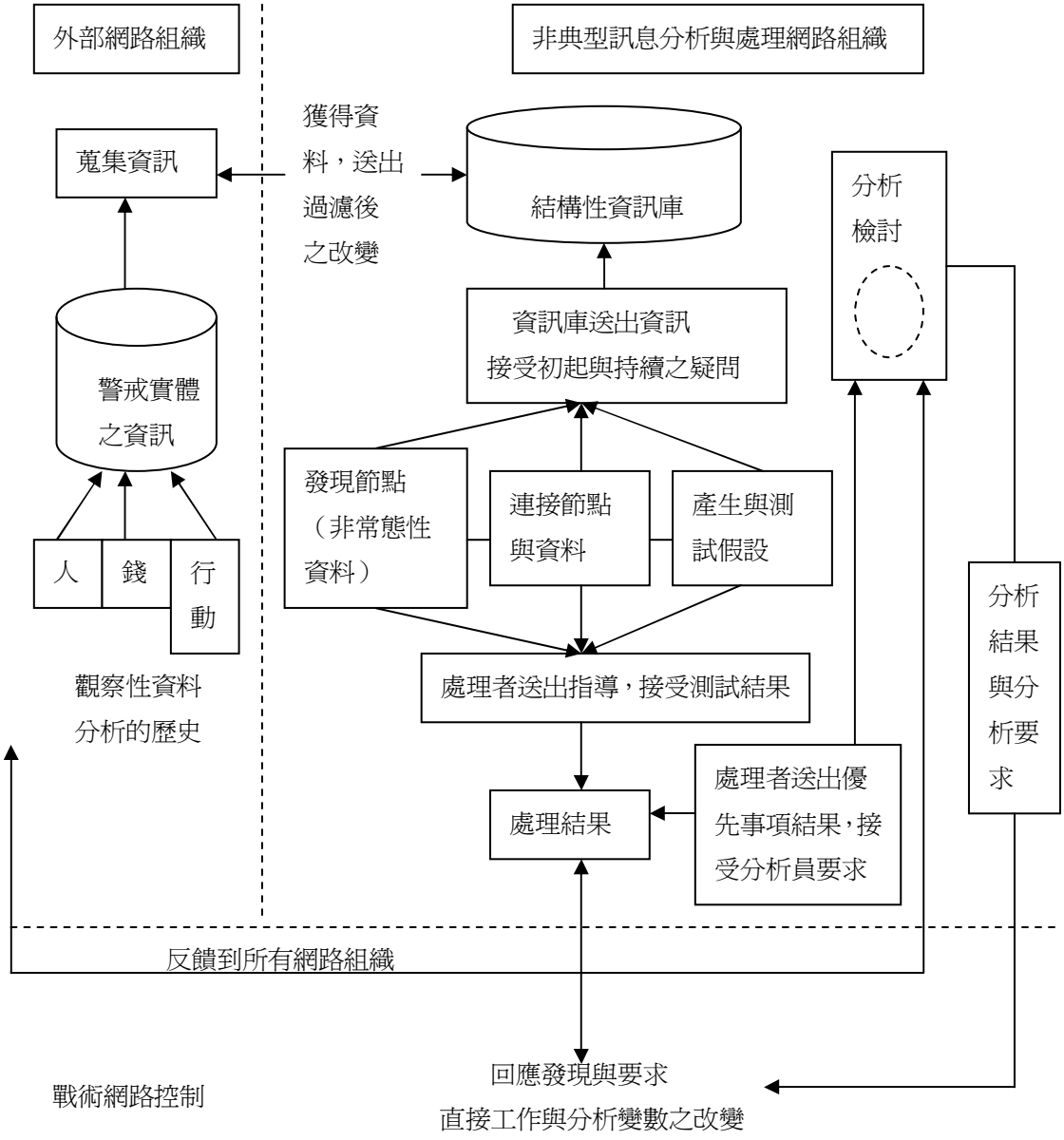
[26] Philip Vos Fellman and Roxana Wright , "Modeling Terrorist Networks-Complex Systems at the Mid-Range " , http://www.psych.lse.ac.uk/complexity/Conference/FellmanWright.pdf.

[27] Philip Vos Fellman and Roxana Wright , "Modeling Terrorist Networks-Complex Systems at the Mid-Range " , http://www.psych.lse.ac.uk/complexity/Conference/FellmanWright.pdf.

[28] John Hollywood , Diane Snyder , Kenneth McKay , and John Boon , "Out of the Ordinary : Finding Hidden Threats by Analyzing Unusual Behavior " , Rand Corporation , 2004 , PP.xv-xvi

[29] 此訊號之範圍從對環境完全瞭解其變化到整個未知之全部現象，例如我們不可能檢證所有與環境有關之非典型行爲，若真如此又會遭受到「資料超載」（data overload）之問題，因此所需要關注的是手邊現有並與此工作有關之「相關行爲」，其作法係若要找出對某一主題樂園之潛在威脅，很顯有許多遊客可能是涉及此不正常行爲卻不可能加以一一篩選，但可藉由一些「觀察

data），亦即能夠標示所觀察到的訊號是真實的現象且不是「傳言」（noise）。第五、若能發現支撐性資料，就要進一步尋求可說明此現象之相關資訊，然後發展與測試能說明此現象意義之假設。第六、一旦瞭解此現象，且找出了危險的指標，則分析者就可以使用這些具「啓發性」之情資與判斷，去避免或是減輕威脅。但要注意的是此過程不是「單線式」的，應該是經由反覆的、測試與學習的多元階段過程、是依於分析者在每一個階段對於現象之學習中來達成，換言之，要採行的是「依賴脈絡分析」（context-dependent analysis）之途徑。[30]有關運作之示意圖如下：



（圖示係源於 Out of the Ordinary : Finding Hidden Threats by Analyzing Unusual Behavior 專文之資料）

若以國家安全情報部門實際進行反恐之作爲爲例，第一、要從一組甚至多組

名單」進行進出旅行團之過濾等。

[30] John Hollywood , Diane Snyder , Kenneth McKay , and John Boon , "Out of the Ordinary : Finding Hidden Threats by Analyzing Unusual Behavior " , Rand Corporation , 2004 , PP.xvi-xvii.

之外在資料庫蒐集資訊，亦即結合情報與政府部門之資料庫與公開來源資料，且所有的資訊大部份均是符合「警戒實體」（watched entities），其中包括了已涉嫌對關鍵基礎設施結構且已被商業過程所監偵的相關之恐怖主義攻擊或行動有關之人員、地點、事態與籌措經費等活動資料。[31]這些基本資訊可以進一步由「先例設定現象」（precedent-setting phenomena）資料、關於非對稱性威脅的非常態行為之嫌疑資料的自願提供來加以支撐。[32]而藉由此種對於「警戒實體」之直接觀察並整合已參與觀察之「後設資料」（metadata），就能建立一個「結構性資訊庫」。

第二、基於此結構性資訊庫，監偵人員要自動的、不斷的過濾資訊，以找出非常態之訊號。這些訊號可能是單一的觀察，例如是非常大量的金融轉帳；或是重大的趨勢，例如在過去一個月內增加了 75%之轉帳記錄等。這些訊號就變成了「節點」，而對於這些非典型資訊之分析與處理可以用來支撐必要之監偵過濾，其步驟是從簡單之少量資料評估，即經常是由分析員生產；到複雜的評估數以萬計資料之演算，即經常是中樞神經網路（neural networks）的混合人員與機器之統計技術來加以完成。

第三、一旦此「節點」被找出來，下一步就是要找出與此節點有關之資訊。因此分析員要能夠發現新的與現存節點間之關係，亦要不斷進行「檢討過去」（backsweeping）之過程，以找出先前不顯著但卻與目前節點有關之資料。這些相關資料大部份應是來自於「結構性資訊庫」，但也可能是來自於情報圈之資料庫與商業性資料庫，例如商業與金融之交易情形等，而發現這些資訊將有助於決定非常態性現象之範圍與提供可協助說明之脈絡。

第四、一旦這些「節點」被連接起來，則分析員可以經由設定之假設去建立對於這些連結節點可能之詮釋，且進而建立協同之測同之測試計畫以決定這些假設之正確與否。而進行分析之主要目標，就是評估出那些現象應該在未來調查中給予優先之關切。結果，這些「假設」經常不能符合某種之特定推論，但是卻已達到提醒此現象是如此的不尋常、且可能有特定的懷疑特徵，並應進行測試監督，以決定該現象是否值得進一步調查或是不需要過度解讀。

第五、前述這些過程的結果，必須要優先加以處理。而產生的最優先結果要立即送交關鍵的分析員手中。此步驟之重要功能，是可減少潛在的、大量的非常態的發現，如此分析員才可以集中注意於僅是與此節點有重大相關之發現。

第六、要注意進行相關觀察之蒐情者與分析員之間的協同作為是非常重要的，因為可提醒不同的分析員所找尋的是同樣的資訊而能加以合作，且提供彼此間的溝通管道而能減少錯誤。因此分析員對於採取何種行動負有主要的責任，才能有效回應不尋常的現象並將分析洞見落實於蒐情。[33]此種找出「節點」與進行分析之過程，亦可簡化為如下簡表：

---

[31] 這些商業過程包括了國際商業活動；核子能源；危險材料；及含陸、海、空運之國際運輸等。

[32] 例如在「九・一一事件」攻擊之前，美國聯調局之官員可能提供其對於一些飛行學校之嫌疑人的懷疑資訊。

[33] John Hollywood , Diane Snyder , Kenneth McKay , and John Boon , “Out of the Ordinary : Finding Hidden Threats by Analyzing Unusual Behavior “ , Rand Corporation , 2004 , PP. xvii-xxii.

過程	應從事之工作與注意事項
第一階段	1、置焦點於已關注且有嫌疑的資訊；但亦要有開放的彈性，才能篩選必要特定資訊之資料庫並接納「所有來源」之非典型行爲資訊。 2、不要再進行對大量資料庫之「資料採礦」作爲，或是進行對於一般處理資料的蒐集，以避免「資料超載」的困擾。
第二階段	1、要尋求「非常態」之訊息，才能偵測到廣範圍之威脅行爲。 2、不能僅注意事先決定之模式，因爲有效訊息經常是與現存已有的模式分離的。
第三階段	1、發現「節點」，尋求相關資訊與生產假設。 2、運用的是「脈絡分析」，才能使資料在現存知識的脈絡中加以分析。
第四階段	藉由對於不尋常訊息之競爭性假設的生產與測試，以處理「不確定性」，且有助避免對於現象之不成熟接受或是詮釋。
第五階段	1、協同不同部門人員之努力，以連接節點。 2、要注意的不僅是非常態資料，且要進行的是對資料之非常態分析。

（本表係參考 Out of the Ordinary : Finding Hidden Threats by Analyzing Unusual Behavior 專文之資料，而由作者整理）

若經由此種連結節點之方法進行對於 1993 年「世貿中心」爆炸案之研究，可發現在爆炸案之後，雖然主要策畫者猶塞夫（Ramzi Yousef）逃走，但是聯調局找到其他的參與者，且經由調查線索，發現此行動是有國際關聯性。再經由其它幾個重要之「節點」，例如 1993 年早期全球性陰謀之線索；片斷之情報資料；1995 年 Bojinka 之事件；密告者之線索；1998 年東非爆炸案；2000 年 1 月恐怖分子在馬來西亞之會面；2000 年 10 月對美國船艦之攻擊；及「九・一一事件」後所獲取之線索，加以綜整以勾勒出網路節點再加以連結與分析，最後就明顯展現出此行動是與賓拉登和蓋達組織有關聯。[34]

伍、結論

打擊恐怖主義活動，絕不能忽視預測性與戰術性情報之需求，亦即完善預警情報作爲已是維護國家安全之情報部門的首要努力目標。但在從事預警情報分析之過程中，會面臨許多困難，例如情報之不確定性、不完整性，恐怖份子也會利用否認與欺騙等謀略作爲而導誤情報之研判，且預警標準之建立不易等均是無法完全解決之問題。然而仍可嘗試藉由一些符合科學之方法來加以運用，目的就是希望藉由關係資料所建構之連接分析、事件指標之建構與檢證，以達成某種程度之預判基礎，並嘗試較完整之解答人、地、時與方法等類型之問題，進而能夠據以提出預警情報以達成事先防範攻擊之目標。

社會網路組織分析法就是能強化預警情報分析的有用方法之一，其目的是要加強預測之能力，經由正確的詮釋社會網路組織，以協助在社會網路組織內對個人或組織之行爲及決策之預測。特別是若具有對個人行爲之瞭解與預測的能力，就能夠評估行動之特定方向。換言之，社會網路組織分析是連結節點之數學分析方法，若能有效的連接多組節點就能浮現出整個組織之網路架構；而一旦有了網路組織圖，就可使用社會網路組織母體來找出整個網路或部分路線及判斷出可能

[34] “How Al Qaeda's global network slowly came into focus for U.S. intelligence (1993-2001) “, Frontline . http://www.pbs.org/wgbh/pages/frontline/shows/knew/etc/connect.html

之行動，亦即會比較容易的提出恐怖分子將採行攻擊之人、地、時、目標與方法等之戰術預警情報。且透過此種方法及所建立之「關係資料庫」，經由長期之累積與修正，將能建立與不斷更新恐怖份子之「預警名單」，則其所能發揮之預警功能也會逐漸提升而能強化長期對恐怖活動監控與預先防阻之效。