作者/James M. Davitch　譯者/黃國賢　審者/黃依歆

公開來源情資的分析與規劃

Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data

取材/2017年第4季美國聯合部隊季刊(*Joint Force Quarterly*, 4th Quarter/2017)

情報界偏重機密情資的窠臼，助長了情資獨有的僵化思考。相對地，以公開來源取得敵方訊息，據以進行預測性分析，將能強化情報專業，針對即將來臨的衝突提供即時之徵候與預警。

在多年耗費鉅資於情監偵系統情蒐能力之後，情報界如今同樣投注於提升情報分析的科技。[1] 然而，若不能體認公開來源情資(open source information)持續攀升的價值，則情報界將難以了解此等投資的實質回饋。

本文旨在探討當代情報界的源起，及其傾向於仰賴非公開來源的機密資料。接下來說明應如何運用公開來源情資，並提出將之視為未來早期徵候與預警的新思維，最後則是向情報界提出精進作為與可行步驟，意即運用公開來源情資強化軍事情報部隊。

掌握公開來源資料的分析潛力，而非嚴密防護機密情資外洩，正是情報專家所面對的「大數據」挑戰。公開來源情資有可能是敵方在第一時間釋出敵意的徵候，亦即美國國防部所稱未來可能的威脅環境。[2] 但情報界官僚體系仍維持一貫的封鎖模式，僅侷限於機密來源。

祕密的文化

珍珠港奇襲事件及美陸軍與海軍情報機構間各自分權獨立的隔閡，導致許多人認為美國極易遭受不可預期的打擊。鑑此，杜魯門總統決定整

2016年12月16日，位於新墨西哥州霍洛曼空軍基地(Holloman AFB)的MQ-9死神無人機。(Source: USAF/J.M. Eddins, Jr.)

合情報任務，希望藉此辨識外國進犯意圖的初期徵候與預警。1947年中央情報局於焉誕生，其設置目標就是要成為阻卻未來突襲事件的主要防線。[3] 以下簡介1947至1990年間，情報作業在工業時代的運作模式。

當時情報界關注重點僅限縮於蘇聯的發展動向與能力，導致「國家情報」成為情蒐與回報的主要特色。然而蘇聯係一複雜的目標，能夠蒐集到的情資亦相當稀少。但對今日全球化、相互連結與依賴的地緣政治環境來說，相同的情報問題「較不複雜」。[4] 蘇聯時期封閉的社會及高明的反情報架構，使得發展昂貴的感測器與平臺成為必要，所以才能在拒止環境中藉由高度探索能力，從撲朔迷離之中一窺全般堂奧。[5] 誠如屈福登(Gregory Treverton)所言，「冷戰最高峰時期的氛圍，是強烈主張密切鎖定蘇聯相關情報，將刺探敵方祕密列為最高優先，尤其是那些透過衛星及其他科技蒐集而來的祕密情資。」[6]

日本偷襲珍珠港事件是美國遭受不可預期打擊的歷史著名案例之一。
(Source: Wiki)

冷戰期間情報的主要服務對象是總統及美國國家安全會議，因為若美國發生另一起奇襲事件，總統就會成為眾矢之的。客製化的感測器材與載臺是為了能夠精確計算出蘇聯的飛機、船艦及其他軍事裝備數量。當時對情報界而言，公開來源的訊息大多會被視為由蘇聯高層向大眾釋出的官方訊息與宣傳，而這些訊息也被認為能提供總統掌握敵方領導階層的想法。[7] 然而，情報界的計畫與預算卻著重於精良的情蒐系統。

情報界之所以會聚焦於機密來源情報，主要是基於因應「國家情報優先架構」(National In-

telligence Priorities Framework, NIPF)所列舉的情蒐順序。國家情報優先架構旨在作為高階政策官員制定「重大利益」優先議題的工具，並提供給情報部門據以憑辦。[8] 問題是情報部門的既有工具都以機密資料為主，因此為了符合國家情報優先架構，便只能以現有的資源與方法，畢竟其已經冷戰「證實」為致勝之道。這點使採購與發展新式感測器與載臺以產製更多的機密資訊成為必然結果。情報界因應情報問題的方式，主要仰賴機密來源的價值。[9]

打破窠臼並不容易，但情報界如果想要採取更積極的態度，就非得這麼做不可。阻礙這項目標的因素包括組織的惰性；不敢嘗試未經測試的替代方法；無論多麼不切實際，卻仍滿足於回答較簡單的問題。在危機真正發生之前，龐大的組織鮮少願意對改革做出回應，相反地大家只想依循既定例行模式與簡單的標準作業程序。[10] 依照目前情蒐作業的主流架構，情報專業人員必然持續在組織中停滯不前，因為他們只會進行嘉士特(Ronald Garst)所定義之「敘事性分析」(descriptive analysis)。[11] 舉例而言，分析部門總是例行性描述何事、何時、何地，卻因此忽略了預測性分析。[12] 無獨有偶，美國情報感測器在提供支援敘事性情報分析的數據上表現得相當優異。但情報界也因此變得裹足不前，並且無法解答決策高層通常較有興趣的事：接下來「將會發生何事」，以及原因為何。康納曼(Daniel Kahneman)將該趨勢連結至「替代探索法」(substitution heuristic)，亦即藉由評估相關且較易處理的問題，簡化困難的工作。[13]

仰賴機密來源的祕密資料會傾向量化情報問題的答案，例如任務的數目及蒐集與處理過的影像數量。這些資料可以在數字上輕易完成蒐集與加總，但卻轉移了質化指標的調查需求，但這些工作反而可能決定情報作業程序是否能夠有意義地解決根本的情報問題。[14] 因此，原本的問題是「美國的情蒐作業狀況是否有助於更了解敵方？」接著轉變為，「情監偵系統出動多少架次用於支援領導階層設定的優先項目？」

值得關注的是，儘管公開來源能提供很大的用處，但它們並非解決所有情報問題的萬靈丹。每一種情況都有必要檢視其根本特性。但因為早已習慣於自動忽略，而無法得到公開來源的潛在價值，充其量就是失去創意性的解決方案。然而最糟的狀況，則是象徵情報界將會錯失未來衝突的重大徵候與預警，同時因應全球地緣動態變化，預先做好面對緊急複雜情勢的準備。[15]

911攻擊事件提供了一種動力，將公開來源情資的價值主張推向前線，使其所具備的能力由強化傳統情報作為的形態，明確且迅速地轉變為反恐任務。然而，直到大數據的速度、多樣與大量等特性，隨著社群媒體蓬勃發展愈發明顯，才使更多公開來源的分析資料得以真正取代機密來源。如今情報部門有可能會把公開來源當作情蒐程序的起點，同時運用機密資料來強化非機密來源，進而顛覆以往的作業型態。

情報不只侷限於祕密

前中情局長海登(Michael Hayden)向美國外交關係協會(Council on Foreign Relations)形容情報

前中情局長海登曾形容情報交易為一場拼圖遊戲，這也意味著吾人需拼湊所有片段的情資。(Source: Wiki)

交易為一種拼圖遊戲。[16] 這項隱喻令人相信所有的片段都在等著我們加以拼湊。不幸地，這樣的想法通常會被解讀為需要更多情蒐感測器，反而提高了機密情資的獨占性。如此一來，機密情蒐是否為一窺探真相的窗口，就會持續存疑而爭論不休。尤有甚者，此舉所產生的結果是要求尋求與創造更多的資料，徒增研析作為的負擔。最終結果，祕密情報的獨占性就會變成研析的基礎，導致限縮甚或排除具有創新性的思維。[17]

關於情報問題，特別是那些即將發生戰爭之模糊徵兆，比謎題更令人費解。奧科特(Anthony Olcott)指出，就算不是不可能，此種神祕問題也很難獲得妥善的解決，「無論你以機密手段或其他方法蒐集到多少情資。」[18] 嘗試回答神祕事物通常涉及不確定、懷疑及認知不和諧，而這些大多是我們想要避免的事。但是抱持懷疑並處理各種可能性卻有其必要，因為情報問題本身鮮少存在容易、明確及有事實根據的答案。唯一可以確定的是，情報的神祕感是一種持續存在的不確定性，而這種不確定性並非單純投入更多監視感測器就能緩解。

泰洛克(Philip Tetlock)曾描述確定性所產生的誘惑，他表示確定性「滿足大腦對於秩序的渴望，產出井然有序的解釋，提出完善解決之道。」[19] 康納曼則提出警告，聲稱過度信任此種確定性會導致：「高度信心的聲明顯示某人在心中已建構了一個合乎邏輯的故事，但並不

表示這個故事就是真的。」[20] 當蒐集到愈來愈多證據，甚至出自機密來源時，有時候確實可以減輕疑問的程度，儘管這不代表疑問已解決。但如果僅將證據的範圍指向排他性的機敏情資，並宣稱已找出真相，就會像盲人試圖描述彩虹顏色般可笑。[21]

儘管有些謎團確實需要借助機密「片段」來拼湊，但運用公開來源情資則愈來愈能幫助吾人深入理解神祕，並能回答具體且清晰的問題。公開來源可以協助了解國家武器研發時程之突破性進展，該資訊過去得靠諜報工作或科技感測器方能取得。例如「中共最新一代地對空飛彈的射程範圍及速度為何？」此類問題如今已可透過公開來源獲得解答。[22] 奧科特在闡述商業及公部門如何運用公開來源時，提及富爾德(Leonard Fuld)所稱情報的基本規則：「凡金錢交易之處，即資訊交換之所在。」[23]

鑑於未來的情報問題終將較像「神祕」而非「祕密」，分析人員需採用更多創意性與批判性思考，並較以往運用更多元的情資。

如此一來，以往慣用機密情蒐「蒐集──處理──分析」傳統模式的分析人員，腦力負擔將更加沉重。情報界直覺地接受機密資料所提交的答案，正是康納曼所稱我們「1號系統」的回應，一種「自動且快速」的思考模式，僅有很少或是連心智活動都沒有。[24] 康納曼把這種模式和「2號系統」相較，此系統「將專注力置於需慎思的心智活動上。」[25] 隱晦的神祕通常未能提供即時答案，因此產生了不確定性，而為了解答這些神祕所需要的創意性思考，正是「2號系統」的範疇。

情報界對機密情資的重視最終可能阻礙創造性思考。取得機密情資的管道，通常伴隨著聲望流傳與知道的必要性限制，這點「促進了區分—簡化—待處理議題的觀點。」[26] 柯比爾(Josh Kerbel)指出冷戰期間「『情報界』對於好的情資相對擁有獨占權」，但卻「持續使分析人員混淆情資的獨有性與決策者的實用性。」[27] 在冷戰期間，高價值的情資通常具技術性與時效性，主要透過通信及電訊傳遞。情報專業人員通常會將此等資料視為情蒐目標「可偵測到的印記」。此種可探測到的特徵在冷戰時期轉瞬即逝，如今在資訊時代則是爆炸性地充斥各處。

穿戴式科技及物聯網提供精準的個人地理定位，並且將個人過去的隱私細節連結至網際網路的公開架構之下。另外，此種情資並不需要透過高空感測器或地下諜報活動祕密地取得。事實上，網路上的個人「自願地」公開自身資料於公開場域中。誠如屈福登所言，在資訊時代中，「蒐集情資已經不是太大的問題了，而查證的方法也不會只有一種。」[28] 公開來源環境能夠探測到敵方的訊息，而這在資訊時代來臨之前根本無法想像。

公開來源資料的匯流，包含快速成長的社群媒體平臺，只會成為未來更不可或缺的資訊來源。柯比爾指出，「情報界必須克服其不切實際的想法，認為自己的附加價值大多來自只有自己可以接觸的機密情資。」[29] 許多公開來源的社群媒體公司都是價值連城的企業，例如：2010

年成立的Instagram為成長最快的社群媒體平臺，2016年已達3億用戶。[30] 羅斯(Alec Ross)指出，「如今有將近160億個連上網際網路的裝置。從現在算起的四年內，該數字將會攀升至400億。」[31]

儘管這些公開能取得的資訊已經存在，公開來源作為一種情報的形式，仍然較少受到情報領域重視。屈福登批判該現象，「如今的情報……擁有大量資訊……而且公認具有可信度，已經不再如情資匱乏的年代大多仰賴衛星或間諜。」[32] 唾手可得的情資如今不僅是具有價值的補充資料，更能重新定義徵候與預警，同時應作為未來情報研析的基礎。就本質而言，不應該是公開來源去強化祕密情資，而是應該反過來才對。此舉可能產生效益，為當前與未來混沌不明的作戰環境爭取不可或缺的預警訊息。

徵候與預警：「混合戰」中的公開來源資訊

2014年夏季，「親俄分離主義者」在東烏克蘭出沒。莫斯科一再否認其正規部隊在烏克蘭領土範圍從事軍事行動，但社群媒體卻狠狠打臉俄羅斯政府。俄軍年輕士兵「自拍」上傳

2015年9月27日，北卡羅來納州布拉格堡(Fort Bragg)的美軍第82空降師跟義大利維辰札福爾格(Folgore)空降旅的官兵，在16.1網路整合評估驗證作業中，於墨西哥州白沙太空港演練聯合強制進入作戰。(Source: US Army/Aura E. Sklenicka)

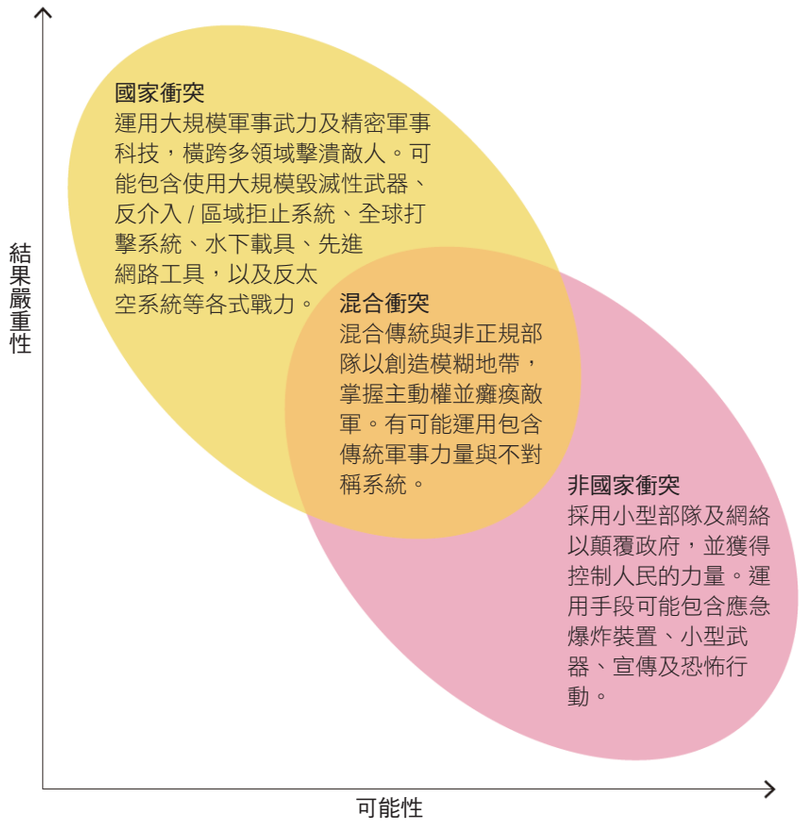
到Instagram，但他們可能事先未料到相關數據透露渠等位於烏克蘭境內的地理位置。他們也提供了強力的證據，顯示俄國共謀參與飛彈擊落馬來西亞航空MH17客機事件。[33] 初期報導迅速從公開來源的管道傳入，包含上傳至推特及Instagram的照片，以及大量的YouTube影片。[34] 此種形式的線索本身並未構成「最終成品」，但可用於指引傳統情監偵的情蒐資產，以查核這些公開來源線索。

儘管相關證據排山倒海而來，俄羅斯國防機構竟然仍將責任推給烏克蘭部隊。[35] 俄羅斯總統普丁抓住機會打贏了宣傳戰，他振振有詞地表示這種狀況原本可以避免，「假如基輔當初沒有對親俄分離分子再度採取軍事行動的話。」[36] 這些混合傳統及非傳統事件的高密度公共關係活動，將成為美軍未來最有可能面對，同時也是最危險的衝突場景。

前參謀首長聯席會議主席鄧普西(Martin Dempsey)上將針對此種資訊作戰提出適切的定義(亦概述於2015年美國國家軍事戰略，詳見圖表)：「國家及非國家行為者聯手運用廣泛的武器來達成共同目標，一如吾人在東烏克蘭所見。」[37] 他接著表示，「混合衝突增加了模糊的狀況、複雜的決策，同時也會拖累有效的回應協調工作。」[38]

部分人士主張，發生在烏克蘭的混合戰概念，不過就是傳統技術與程序的延伸罷了。[39] 無論如何定義，我們觀察的重點在於這是未來衝突最有可能出現的場景，因為得以讓敵人運用孫子所提出的建言：避實擊虛。美軍擁有壓倒性的強大傳統軍力。但當敵人發動假資訊戰，並採用非正規軍事力量時，就能讓情勢低於衝突門檻，避免美國發揮其傳統的軍力優勢。誠如部分人士已注意到的，此類混合戰的戰略能夠「在某國了解衝突已開始前就癱瘓某國」，而且還能成功「在北約各

圖表：衝突之進程



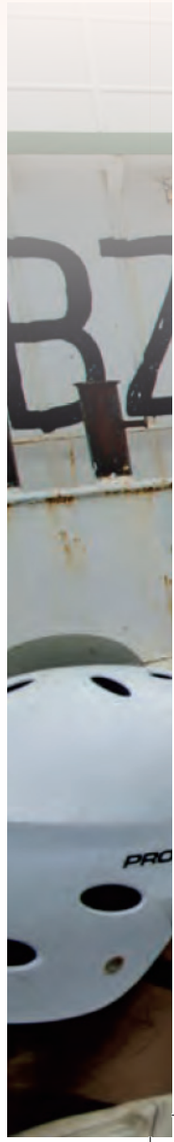
國察覺及反應前暗中進行。」

此種未來衝突的形態將不僅限於美國在歐亞大陸的敵人。白邦瑞(Michael Pillsbury)描述中共可能採用某種稱為「超限戰」(unrestricted warfare)的軍事準則，[40] 其在各方面都與資訊作戰相似。[41] 在此區域內，其中一項高危險性的可能行動方案，是中共運用「平民」漁船遂行軍事行動，意在鞏固其領土宣示之目的。此類行動並非無先例可循。小規模的「漁船事件」可能讓情勢演變為海上緊張對峙。這些都讓中共一方面貌似推託毫不知情，一方面讓事件保持在衝突邊緣，刺激美軍介入更深。

正如派弗(Steven Pifer)2015年在美國參議院聽證上所言，非正規武力預示著更大規模的傳統行動，將成為未來交鋒的範例。[42] 前美國歐洲司令部司令布里德洛夫(Philip Breedlove)上將亦表達同樣的關切，強調北約必須準備好回應「看不出屬於哪個主權國家軍徽的特種部隊越過邊界滋生事端」，且後者最終目的是顛覆國家。[43] 然而，情報界所運用的傳統徵候與預警技術、情監偵系統，長久以來都著重於大型軍事部隊的部署。如此作法的風險在於易錯失早期線索，使原本可以先發制人的機會跟著流失。

美國國防部長辦公室所追求的「第三次抵銷戰略」在於威懾潛在敵人，使其莫敢輕舉妄動。為達成此目標，情報界的目標應該針對即將發生的衝突提供最適時的徵候與預警，以避免美國遭遇偽稱自身為非戰鬥身分實體時，陷入決策癱瘓現象。另一個次要目標則是提供決策者確切的證據來反制侵略者的宣傳攻勢。而未來最適合該任務的工具將不會是那些原本用來反制蘇聯戰車的傳統情蒐載臺；而是那些來自公開來源的情資。冷戰時期的戰術、技術與程序無助於辨認「小綠人」(little green men，編按：出現於2014年烏克蘭危機中身分不明的士兵，身著綠軍服並攜行俄國武器裝備，被認為與俄軍有關)、無害的漁船，抑或支援他們的資金、武器與領導幹部。鑑此，改變情報界運作的方式有其必要。改變可循序漸進，藉由能在公開來源情報上增加更多細節線索的祕密搜尋感測器，擴大發展公開來源情資。

誠如第三次抵銷戰略所示，在全新的公開來源資訊環境中，人機協作被賦予相當重要的使命，尤其在人工智慧方面更是如此。儘管社群媒體平臺如臉書、Instagram及推特在全世界廣泛流行，某些國家仍主要在國內使用特定社群媒體，如接觸(VKontakte)與QQ空間分別是俄國及中共最受歡迎的社群媒體網站。分析人員必須對此有所認知，不僅要能解讀外國語言，還要將目標的社會文化差異納入考量。自動機器翻譯工具的能力正在快速提升，對上述兩者皆能提供助益。2014年5月，微軟公司展示了一種電腦程式，能即時翻譯口語文字。[44] 納捷法巴德(Maryam Najafabadi)等人描述機器翻譯應用程式所具備的「深度學習」能力時，提及Google的演算法工具「word2vec」能夠在巨量詞語當中，快速學習其中複雜關聯性。[45] 由於運用所謂的「詞向量」(word vectors)，這套語言翻譯工具因此能分辨詞語的細微差異與脈絡關係，而



非僅止於字面直譯。社群媒體公司所發展的人工智慧翻譯工具能夠打破語言的權威結構。機器的強化能力將讓我們不只聽懂人說的話，更能聽懂其所欲傳達的意涵。

改革建議

主要變革應集中於軍事情報專業人員思考問題的方式。吾人有必要改變文化上的思維，意即至少要將機密性資訊與公開取得資訊這兩者的重要性同等視之。對軍方而言，變革應從入門的教育與訓練場合做起。下一代情報專業人員的成長環境充斥著科技及社群媒體，對這些「數位住民」而言，突破陳舊思維的窠臼並非難事。然而，機密來源的誘惑力依然會存在。情報訓練必須能夠配合下一代人員的習性，尋求公開來源的管道。

此外，未來美國將需要訓練其空軍官兵運用手邊工具，並鼓勵他們追求創新思維，期能從公

2016年11月29日，在美海軍驅逐艦桑普森號(USS *Sampson*)之大洋洲海上安全方案任務中，美官兵及海岸防衛隊太平洋執法分隊人員正在接近一艘中共漁船。(Source: USN/Bryan Jackson)

開來源資料當中進行最佳的情蒐與研析。特定的研析訓練應包含重新描述問題、因果流路圖、加權排序、反向思考，以及其他許多在瓊斯(Morgan Jones)所著《思考的工具》(*The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*)一書中所提及的技巧。

教導空軍官兵應用大量湧入資料的分析技巧，其重要性不論怎麼強調都不為過。首先，這些技巧允許分析人員公開透明地向他人「展示成果」。其次，這些技巧可以教導精準的語言，迫使分析員正確地界定問題框架，以確保提出的問題能夠找到答案，而不是開放各自解讀。最後，這些技巧可以防止軍事情報分析人員陷入康納曼的「1號系統」陷阱中。人類本能傾向第一時間抓住貌似有理的解釋，這點對任何人而言都是個挑戰，特別對相關情報專業人員來說，在面對有時間限制之軍事行動下壓力會更大。

位居領導階層的幹部往往會尋求跟自己原本觀點相符的資料。一般而言，這點在軍事行動中意味著長官偏好機密情資，而公開來源情資則是較乏人問津。[46] 破除此種確認偏誤(confirmation bias)的方法便是運用原有的研析技能。隨著這些技能及知識的妥善運用，情報界將得以向決策者做出更好的回應，而非將時間與精力浪費在範圍有限卻很平庸的成果上，無止境地尋求拼圖的碎片。

如果情報界要認真看待發展批判性思考的技能，正確的途徑便是正視這些分析技巧，嘗試運用經過證實的科學方法。泰洛克指出，「情報界的預測人員從未做系統性評估」，以確認渠等研析預測是否精準。[47] 要是情報界這麼做，其實花費成本會遠比投入情監偵系統的飛行與維護成本來得低。如此以公開來源為基礎的試驗成果，能夠提供有價值、低成本的情資，對未來計畫作為及預算決策都相當有利。

但吾人又該如何看待「老派」的情報分析呢？在資訊時代之前出生的人可能不太喜歡公開來源資料，較傾向傳統情蒐來源。然而與其忍受時間的緩慢推移，還要等到下一代晉升至領導階層，具前瞻性思考的軍事分析人員現在就必須打破機密分級固定模式的窠臼。他們必須了解公開來源與導引情蒐的關聯性，而不是本末倒置。此外，分析人員必須自己「願意」採行這種新模式。但該怎麼做呢？

美國情報高等研究計畫署(Intelligence Advanced Research Projects Activity, IARPA)是國家情報總監(Director of National Intelligence)的支持計畫機構之一，該辦公室邀請情報界各方參與者進行預測競賽。其中有一項名為「神準判斷」(Good Judgment Project)的衍生計畫，邀集國防部內外人士自由參與。2011年，美國情報高等研究計畫署舉辦首屆錦標賽，藉以探索群眾外包情報的潛力。參賽者針對真實世界的事件進行預測，隨後得以判定渠等預測準確性。或許「神準判斷」最有趣之處在於，那些能接觸機敏限制性資訊的參賽者，相對於無法接觸者而言，完全沒有任何優勢。事實上，結果恰恰相反，可能因為機密情資的文化偏差而使這些人未能做出更全面性的預測。在一篇《華盛頓郵報》的評論文章中詳述了該競賽的結果。伊格納提斯(David Ignatius)

明確指出，那些「沒有管道」接觸機敏情資的參賽者，「比起情報界有權閱讀攔截資訊及其他祕密資料的分析人員表現得更好，較平均成績高出了30%。」[48] 他接著表示，「國家安全局的論點顯然是資料愈多愈好……但此種對信號的熱烈追求毫無明智的判斷可言。」[49]

正如美軍強力要求體能訓練最終必須納入常規性測驗，國防部也應定期舉辦「認知的體能訓練」錦標賽。從各種不同的「神準判斷」競賽結果中可得知，「精確預測是有可能的，只要能在制度上獎勵精確預測——而非那些標新立異的解釋，或是忠於黨派的決策。」[50] 換言之，諸如此類的競賽可以培育兼具創新與批判性思考，同時磨練並提升個人的專業技能。尤有甚者，競賽可以讓他們發展與提出問題，這些問題可以進一步加以回應、評量且得分。競賽活動對軍方而言並不陌生。數十年來，美空軍戰鬥機飛行員都會跟其他中隊進行「射火雞」(turkey shoot)的對抗訓練。勝出一方可接受表揚並獲得同儕的認可。國防部有必要舉辦以公開來源為主的情監偵「射火雞」對抗競賽，邀請參與者運用公開來源資訊做出屬於自己的結論，並且授權機構接受這些個人的報告，並允許積極的專業人士拿出最佳本事，展現他們的超高研析本領。

個人及單位之間的競爭能夠激勵動機，同時進一步培育優質情報專業。而且基於「神準判斷」競賽的結果，吾人可以預期那些不信任公開來源者的態度應該會有所改變。至少，參賽者可以從中學習到，機密來源的重要性相較於吾人以嚴謹態度研析，顯得微不足道。

成功的契機

未來若要成功偵測到可能引發衝突之模糊線索，將要透過具創意之持續問題分析流程，並能夠提出有效之解決方案。支撐這些方案的資料將愈發仰賴那些唾手可得，卻在傳統上遭汙名化之公開來源。但誠如曾參與「持久自由作戰行動」(Operation Enduring Freedom)的前資深情報員所言，「情報界的標準行動模式相當重視機密，但很遺憾地對任務的成效卻沒那麼在意。」[51] 個人必須跳脫機密分級固定模式的架構，並專注於最能夠幫助達成任務的情資。

機器在分析的過程中可扮演協助的角色，但無法取代這個過程。「機器在『模仿人類的意涵』上可以做得更好，因此可以對人類的行為做出更好的預測」，[52] 不過泰洛克主張模仿人類意涵與破解意涵的原始意圖有很大差別，他結論道，「這裡始終有人類判斷的一席之地。」[53] 為達此目標，吾人必須將人類的心智投注於研析訓練，並以公開可取得的資訊為基礎進行預測工作。投資於提升創新思維及靈活運用公開來源資料，終能協助領導階層制定決策，並能讓情報界在未來擁有強勁之相對優勢。

作者簡介

James M. Davitch 中校係美空軍全球打擊司令部情報作戰處處長，該司令部位於路易斯安那州巴克斯德空軍基地(Barksdale AFB)。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. 筆者預感謝下列人員： Colonel Jeffrey Donnithorne, Dr. Jon Kimminau, Dr. Lisa Costa, Dr. Robert Norton, Mr. Josh Kerbel, Lieutenant Colonel Robert Folker, and Majors Kyle Bressette and Seth Gilpin for their thoughtful comments and suggestions. 文中茗有疏漏，全由筆者負責 See also Adam Lowther and John Farrell, "From the Air," *Air & Space Power Journal* 26, no. 4 (2012), 61–102.
2. Marcus Weisgerber, "Dempsey's Final Instruction to the Pentagon: Prepare for a Long War," *Defense One*, July 1, 2015, available at <www.defenseone.com/management/2015/07/dempseys-final-instruction-pentagon-prepare-long-war/116761/>.
3. Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, RAND Studies in Policy Analysis (New York: Cambridge University Press, 2003).
4. Josh Kerbel, "The U.S. Intelligence Community's Creativity Challenge," *National Interest*, October 13, 2014, available at <http://nationalinterest.org/feature/the-us-intelligence-communitys-creativity-challenge-11451>.
5. Robert Baer, *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism* (New York: Crown, 2002); see also Bruno Tertrais, review of *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*, by David E. Hoffman, *Survival* 52, no. 1 (2010), 220.
6. Treverton.
7. Anthony Olcott, *Open Source Intelligence in a Networked World* (New York: Bloomsbury Intelligence Studies, 2012), chap. 6.
8. Ibid., chap. 4.
9. 此過程的問題在於欠缺準據以判定情監偵的成效。文職與軍事管理人員情蒐要項之優先次序，係依據國家層級的「國家情報優先架構」及在此架構下以命令爲導向的情報需求，並基於情報所需排定優先次序據以支援任務。量化的測量諸如任務的數量或情蒐及處理過之影像數量，通常用來代替測量值以評估成效是否符合情蒐要項優先次序。這些資料可以在數字上輕易完成蒐集與加總，但卻轉移了質化指標的調查需求，但這些工作反而可能決定情報作業程序是否能夠有意義地解決根本的情報問題。此外，亦述及批判性分析問題及策劃創意性解決方案之不足。Lieutenant Colonel David Vernal, Air War College student, interview by the author, November 15, 2015.
10. Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999).
11. Ronald D. Garst, "Fundamentals of Intelligence Analysis," in *Intelligence Analysis: ANA630*, vol. 1 (Washington, DC: Joint Military Intelligence College, 2000), 18–28.
12. 「描述性分析」重點爲何人、何事、何處等問題，其與「預測性分析」的差異在於後者很難用陳述事實的方式表達，因此衍生更多認知上的壓力。處理「將會發生何事」的預測性問題迫使分析人員承受更多風險，必須在充滿不確定狀態下做出主觀的判斷。此外，這些開放式問題必須以一定範圍的各種可能性來回答，而這些問題通常也同樣有各種主觀的可能性。
13. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2013).
14. Vernal, interview, November 15, 2015.
15. Kerbel.
16. Remarks by Central Intelligence Agency Director Michael Hayden, Council on Foreign Relations, Washington, DC, September 7, 2007, available at <www.cia.gov/news-information/speeches-testimony/2007/general-haydens-remarks-at-the-council-on-foreign-relations.html>.
17. 在2016年空軍戰爭學院的研究中，斯東(Adam Stone)中校驗證到空軍未能享有批判性思考(critical thinking)帶來的好處。針對「空軍未來作戰概念」驗證批判性思考者與追蹤批判性思考技能指標之目標，斯東執行了一項量化批判性思考的研究計畫。他以空軍指揮參謀學院、高級航太研究學院，以及空軍戰爭學院的專業軍事教育學員爲樣本。他的(統計上具意義)統計結果顯示，「相較於同等學歷者，空軍指參學院及空軍戰爭學院的軍官在批判性思考上的技能低於平均值。」參見Adam J. Stone, *Critical Thinking Skills of U.S. Air Force Senior and Intermediate Developmental Education Students*(Maxwell Air Force Base, AL: Air War College, 2016).
18. Olcott, chap. 4.
19. Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Crown, 2015).
20. Kahneman.
21. 奈伊(Joseph Nye)指出，冷戰之後外交政策分析家面臨的挑戰如同抽象事物般神祕，這不是快速回答或簡單分析就能解決的。參見Joseph S. Nye, "Peering into the Fu-

ture," *Foreign Affairs* 73, no. 4 (1994), 82–93。另一方面，祕密本身是定義過的問題，較能透過諜報工作或技術手段解答。祕密有助於滿足看似具事實根據的答案與敘事性分析。然而，隨著未來愈來愈多的資料得以公開取得，適當於公開來源情資環境中應用人機協作，或許得以產出過去僅能靠機密性感測器才能取得的資訊。

22. 這點在筆者與奧本大學(Auburn University)的諾頓(Robert Norton)博士進行訪談後獲得進一步支持。諾頓描述如何透過掌握敵國的研發時程，監控外國武器製造的潛力。他強調國外大學發表研究成果於科技期刊的需求，如同美國高等教育機構的作爲。在科技發展的相關資訊中，經常可以觀察到建構緩慢，卻迅速消失的現象，這或許代表某國的研究已到達適當階段，開始過渡到操作測試及評估階段。
23. Olcott, chap. 4.
24. Kahneman.
25. Ibid.
26. Josh Kerbel, "The U.S. Intelligence Community Wants Disruptive Change as Long as It's Not Disruptive," *War on the Rocks*, January 20, 2016, available at <http://warontherocks.com/2016/01/the-u-s-intelligence-community-wants-disruptive-change-as-long-as-its-notdisruptive/>.
27. Ibid.
28. Treverton, 9.
29. Ibid.
30. Matthew Harris, "Marketing with Instagram, the Fastest Growing Social Platform!" *The Medium Well*, February 19, 2016, available at <http://mediumwell.com/marketing-instagram/>.
31. Alec Ross, "Industries of the Future," Carnegie Council podcast, March 10, 2016.
32. Treverton, 6.
33. Ralph S. Clem, "MH17 Three Years Later: What Have We Learned," *War on the Rocks*, July 18, 2017, available at <https://warontherocks.com/2017/07/mh17-three-years-later-whathave-we-learned/>.
34. "What We Know So Far About the Passenger Jet Shot Down in Ukraine," *Foreign Policy*, July 17, 2014, available at <http://foreignpolicy.com/2014/07/17/what-weknow-so-far-about-the-passenger-jet-shot-downin-ukraine/>.
35. Ibid.
36. Ibid.
37. Weisgerber.
38. Ibid.
39. Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016, available at <http://warontherocks.com/2016/03/russian-hybrid-warfareand-other-dark-arts/>.
40. Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt, 2015).
41. 在找出不對稱方式以對抗較強大傳統敵人這一點上，確實是符合的
42. Steven Pifer, "Russian Aggression Against Ukraine, and the West's Policy Response," testimony before the U.S. Senate Foreign Relations Committee, Washington, DC, March 4, 2015, available at <www.brookings.edu/testimonies/russian-aggression-against-ukraine-and-thewests-policy-response-2/>.
43. "NATO Flexes Its Muscle Memory," *The Economist*, August 30, 2014, available at <www.economist.com/news/international/21614166-russias-aggression-ukraine-has-made-natos-summit-wales-most-important>; Dan Gonzales and Sarah Harting, "Exposing Russia's CovertActions," *U.S. News & World Report*, April 29, 2014.
44. "Rise of the Machines," *The Economist*, May 9, 2015, 18–21.
45. Maryam M. Najafabadi et al., "Deep Learning Applications and Challenges in Big Data Analytics," *Journal of Big Data* 2, no. 1 (2015), 1–21.
46. Kahneman.
47. Tetlock and Gardner.
48. David Ignatius, "More Chatter Than Needed," *Washington Post*, November 1, 2013.
49. Ibid.
50. Angela Chen, "Seeing into the Future," *Chronicle of Higher Education*, October 5, 2015, available at <www.chronicle.com/article/Philip-Tetlock-s-Tomorrows/233507>.
51. Michael Flynn, Matthew Pottinger, and Paul Batchelor, "Fixing Intel in Afghanistan," *Marine Corps Gazette* 94, no. 4 (2010), 62–67.
52. Tetlock and Gardner.
53. Ibid.