作者/Jane Harman　譯者/鄭麗園　審者/郭啟銘

美國情報界應與時俱進

Disrupting The Intelligence Community: America's Spy Agencies Need An Upgrade

取材/2015年3-4月外交事務雙月刊 (*Foreign Affairs*, March-April/2015)

近年來，情報獲取的程序因科技發展而澈底改變，大眾愈來愈重視數位資料保密，但美國政府機密卻被公布在網路上。美國的情報部門需要升級，以因應新時代的挑戰。

美國中情局局長布瑞南打算澈底重組該局，以面對未來挑戰。
(Source: AP/達志)

40年前，在水門案醜聞事件發生後不久，邱吉委員會(Church Committee)澈底調查美國情報組織所使用的手段。上次美國情報機構因應911恐怖攻擊後所進行的重大重新編組，距今也已經過了十年。這兩項努力都帶來一系列的改革，其中包含設立參議院與眾議院情報委員會、通過「外國情報監視法」(Foreign Intelligence Surveillance Act, FISA)，以及採用筆者在國會協助引導通過的「情報改革及恐怖主義防制法」(Intelligence Reform and Terrorism Prevention Act)。

新挑戰的出現再度引爆倡議改變的聲浪。美國政府最近承認的無人飛機計畫、美國國家安全局(National Security Agency)承包商史諾登(Edward Snowden)洩露該局的監視活動，以及參議院情報委員會最近針對中央情報局(Central Intelligence Agency, CIA, 簡稱中情局)拘禁和質詢手段所提的報告，都使大眾對政府權力過度伸張感到緊張。在此同時，一些出奇不意的發展，都讓美國官員遭受意外打擊。敘利亞政府的解體、波士頓馬拉松爆炸案、伊拉克和大敘利亞伊斯蘭國(Islamic State of Iraq and al-Sham, ISIS)的猛然竄起、以及美國電腦網路遭受系統化的駭客攻擊，這些事件都讓華府顯得措手不及。2014年11月，《華盛頓郵報》(*The Washington Post*)報導，中情局局長布瑞南(John Brennan)正考量澈底重組該局：將行動及分析兩個部門整合成為「混合單位」(hybrid units)，以因應某些特定地區與威脅。該報消息來源形容此計畫為「中情局有史以來相當具企圖心的改革計畫。」

但把折疊式躺椅重新排列這樣的重組方式，並不足以讓情報體系面對未來的挑戰。華府必須跳脫傳統智慧，考慮另類的未來前景。試著想像這樣的情況：十年後的今天，中情局的主要任務將會是祕密行動，這是中情局可以為美國安全做出獨特而寶貴貢獻的領域。美國國家安全局方面則不再收集個人資料，因為私部門的公司有足夠的資源從事同樣的任務。而傳統的諜報——利用間諜蒐集人工情報——將變得遠遜於開放來源(open-source)的情報，尤其是從社群媒體蒐集而來的情報。在這每種狀況下，改變都會迅速到來。因此與其緩慢而蹣跚地適應，該是接受現實並正面應對的時間了。

准許無人飛機攻擊

自從2001年美國布希總統(George W. Bush)宣布「反恐戰爭」起，中情局消滅恐怖分子的手法愈來愈高段。中情局執行「目標狙殺」(targeted killings)的才能，卻讓中情局朗里總部(Langley)內外的不少人士感到不安。2014年11月，前中情局準軍事官員阿克曼(Elliot Ackerman)在《紐約客》(*The New Yorker*)雜誌中寫到，「我的同事們內心所存在的不安，並不源於(目標狙殺)本身……這個不安之所以存在，乃是因為這讓人覺得我們正在大規模執行一項我們曾宣誓不會做的事。我們多數人都覺得我們彷彿正在違背第12333號行政命令。」

該命令係由雷根總統(Ronald Reagan) 於1981年發布，以回應邱吉委員會針對非法國內監視以及狙殺外國領袖的計謀所做的廣泛調查發現。該命令嚴禁美國政府規劃或執行暗殺。但當目標是恐怖分子時，政府的律師並不認為「暗殺」(assassination)和「目標狙殺」是同義字，這是在華府與蓋

達組織(al Qaeda)衝突開始之前就有的差異。1983年美國駐黎巴嫩大使館爆炸案後，也曾引起對目標狙殺議題的類似關注。以那次事件來看，誠如華盛頓郵報記者平可斯(Walter Pincus)之後所寫的報導表示，中情局在商討後「與國會的監督委員會達成了一項非正式的共識：如果一項祕密行動得知一名恐怖分子在其公寓中規劃如何炸掉一棟建築物，他就必須被拘留。但如果該恐怖分子被發現且知悉正在前往炸毀一棟建築物的途中……如果沒有其他阻止他的方式，則可以狙殺。」且該行政命令指出，情報體系負責執行「特殊活動」以確保國家安全，而無人飛機計畫就被歸類在此範疇之內。

即使如此，資深官員持續地對中情局日益增長的準軍事角色感到不安，就連布瑞南本人都於2013年2月的同意權聽證會中，描述這些行為已經與中情局傳統上專注於間諜業務「脫軌」。其實在布瑞南接掌中情局沒多久後，白宮似乎準備好將所有無人飛機作戰計畫轉至五角大廈，因為國防部也有自己的無人飛機計畫。但是這個舉動從未發生，部分原因是因為將軍們的阻撓，另一部分則是因為國會無法繞過內部委員會的流言蜚語。其實，最重要的一個關鍵，是中情局的績效斐然。誠如赫希(Michael Hirsh)2014年2月在《國家雜誌》(*National Journal*)中提到，專家們認定中情局「在精準鎖定狙殺行動上，就是比軍方高明得多——特別重要的是，中情局能保證他們要抓的壞人是真正的壞人。」

雖然找不到任何公開的資料來比較中情局與五角大廈的無人戰機計畫，但在資深的決策官員眼中，中情局的表現可圈可點。2013年12月一架五角大廈的無人飛機出擊時，據報誤擊了包括無辜的葉門婚禮賓客在內的一個車隊。在那之前的數月，加州民主黨參議員范士丹(Dianne Feinstein)時任參議院情報委員會主委，就稱讚中情局的「耐心以及審慎」，同時關切「軍方的計畫表現沒那麼好。」

反對將無人飛機計畫留在中情局的人則辯稱，中情局的主要任務應是從事諜報行動(espionage)而非祕密行動(covert action)。他們的辯論基礎是，長期而言，國防部沒有理由不發展執行機密無人飛機攻擊的專業和其他可對外否認的行動任務。將所有的無人飛機作戰從中情局轉至五角大廈也完全合法，總統可以撰寫命令明日立即授權。

跟著錢流，就能導出一項基本事實：中情局的優勢是在準軍事層面上。

然而，真正的問題在於，中情局的核心任務——發展人工情報——愈來愈難落實。某些程度來說，這是中情局成員的屬性所造成的。雖然近來中情局招攬成員的人才庫較昔日寬廣得多(過去有種流行說法是，中情局吸收的成員大都是白人、男性、耶魯大學畢業)，但是政府的身家安檢系統(clearance system)仍排斥很多合格的申請者——雖然這些人擁有關鍵語言能力並對文化透澈理解——卻會因為有個祖母住在巴格達或有個舅舅在突尼斯(Tunis)而被刷掉。想要滲透到中東的部落或非國家組織本身已經很困難了，缺乏熟悉阿拉伯習俗或精通多種阿拉伯方言的人才，只會

使任務更加艱難危險。

另一個讓人工情報搜集愈來愈困難的原因是美國趨於明顯的政治文化。在恐怖分子團體內培養線民(更別說派人臥底)是件風險極大的事。無論情報員有多勇敢或有多願意為國服務，情報官員現在必須在一個勸阻承擔風險的政治環境中運作，因為美國民眾對美國人士的傷亡反應強烈——這個現象在2012年位於利比亞班加西(Benghazi)的美國基地遭攻擊案後更為明顯，當時共有兩名外交人員及兩名安全人員喪命。當然，這種政治限制及對風險的排斥也會影響美軍。這部分解釋了為何很多美國決策者對於派兵進入伊斯蘭國(ISIS)作戰的想法較為冷淡。諷刺的是，有效的空中攻擊仰賴精準的目標標定，而那卻需要有人在地面搜集情報，那份工作本身就會使得美國人員暴露在原本採取空戰所欲避免的那種威脅中。

美國民眾的爭議也危及到人工情報的另一個來源：審訊。參議院情報委員會針對布希時代的審訊及拘禁計畫所做的多年詳細調查更是火上添油，該報告不但質疑這些所謂的強化審訊技術的合法性，也質疑它們的效率。(2003年筆者以國會議員身分寫信給時任中情局總顧問穆勒[Scott Muller]，質疑該計畫的政策指導原則，也要求中情局不要銷毀這些審訊影片。) 目前，歐巴馬總統雖然試圖關閉位於古巴的關達納摩灣(Guantánamo Bay)拘禁中心，將恐怖分子嫌犯轉移到美國本土的監獄計畫持續受阻，因為國會反對在美國開庭審判。即使如此，拘禁中心所關的人數已從2003年的600多人降至今日撰稿時的127人。眼下大家都盯著下任美國國防部長，看他如何在歐巴馬任期結束前完成這個任務。

如果這些趨勢持續下去，中情局將更難像過去那樣搜集人工情報。那麼情報界該如何因應呢？他們可以將收集人工情報的任務外包給較不排斥風險且在文化上較合適的外國友善情報單位，例如以色列、約旦及英國的單位。中情局也可以將其人工情報搜集聚焦於只直接支援祕密行動。中情局亦可繼續改善它的身家安全調查程序，使之容易些，比方說如果單位亟需某些人的專業特長，可以給予臨時或有限制性的權限。

但在今日的環境中，中情局主要的附加價值可從其財務方面反映出來。根據一份被洩露、並刊載於《華盛頓郵報》的2013年情報體系機密預算，祕密行動計畫的經費撥付(26億美元)超出了人工情報的經費撥付(23億美元)。跟著錢流，就能導出一項基本事實：中情局的優勢是在準軍事(paramilitary)層面上。

數據雷區

中情局並非唯一面對挑戰的情報機構。在史諾登洩密案後，媒體紛紛描繪美國國家安全局為一個全能的強勢機構，對個人的數據資料有無止境的胃口，且在取得上並沒太多障礙。在一個刻正進行中的辯論裡，公民自由倡議者曾對抗過主張國家安全為主的鷹派，雙方都有個有缺陷的假設：國家安全局的競爭優勢是在數據的大量搜集整合。

事實上，國家安全局所布下的數位天羅地網，從來沒有像其最

強烈批評者所愛影射的那樣全面，且國會在2008年修訂了外國情報監視法，以確保該局的數據收集是受「外國情報監視法庭」(Foreign Intelligence Surveillance Court) 的詳細限制及審查。此外，有關進一步限制國家安全局計畫的新建議正日益高漲，而美國的高科技公司正在採取愈來愈多引人注目的舉動，來保護他們的客戶資料。

處於數位權力的平衡時代，美國情報界需要爭取矽谷私部門的信任與支持，將隱私與國家安全變成正和博奕。

的確，國家安全局的未來將會受到其與矽谷的關係所形塑，一種比什麼都重要的關係──那就是該局正在迅速地成為矽谷的小夥伴關係。人們可以懷疑高科技公司因國家安全局的監控措施而起之憤怒的真實性──例如，臉書(Facebook)公司據說儲存了其每月十多億活躍用戶的拍位元組(petabytes)資料，其聯合創辦人祖克伯格(Mark Zuckerberg) 卻對大量數據收集的想法感到驚訝。但矽谷的反應起了作用，其結果變成一場加密的短程賽車競賽，而這使得高層政府官員感到恐慌。蘋果、臉書及谷歌等公司，捨棄在政府有壓倒性優勢的法庭去辯論監控政策，而改在網路空間上回應。為了滿足全球客戶群對嚴格隱私保護的期望，他們開發了將客戶數據加以嚴密保管的技術能力。

蘋果公司現在於公司網站上增加了一個「政府資訊要求」的網頁，此頁不是有關他們如何愉快地遵守政府要求。它明確寫道：「我們對於客戶隱私的承諾不會因政府資訊要求而停止。」蘋果的

為滿足客戶群對嚴格隱私保護的期望，臉書等社群媒體公司開發了嚴密保管數據的技術能力。(Source: AP/達志)

iPhone手機如果安裝最新的iOS8作業系統，能將其數據進行加密且隱藏於密碼後，套句蘋果自己的話說，「蘋果在技術上無法回應政府對數據提取的搜索令。」谷歌也如法炮製，在他們的Android手機內加入類似功能。其他機構都感受了這種漣漪效果。2014年10月，聯邦調查局(FBI)局長科米(James Comey)說，該局「正掙扎著去……維持(其)能力，以實際搜集其被授權搜集的通信數據。」

多年來，公部門和私部門之間的科技能力出現愈來愈大的差距。像美國中情局一樣，國家安全局都碰到招聘人才的問題。該機構站在隱私代溝的對立面；他們也沒有希望可像臉書等企業提供超高薪資，甚至於連他們的實習生都比不上。身家安全審核制度使事情變得更糟，以是否抽過大麻和非法下載音樂等問題，來折磨應徵者。國家安全局有些聘僱方法已有改善，但沒有人預期在爭奪頂尖人才的競賽中，該機構在未來能很快地贏過科技公司。

從長遠來看，華府無法在數位競爭上贏過矽谷。現在既然政府對私部門的需要，遠大於私部門對政府的需要，最重要的任務就是重建二者之間的信任。國家安全局誠然可以尋找方法來解決科技公司的防禦，但任何拙劣的企圖將帶來很高的政治代價。可取代的做法是，該機構在需要資料時，需要不斷透過正當管道遞送搜集令，遵守既定的法律程序，並努力說服公眾他們對隱私的尊重。隨著像臉書及谷歌等公司愈來愈深切地融入全球通信基礎設施——兩家公司據報導正在研究向發展中國家提供網路服務——他們可能會在開放來源的數據收集上成為政府的夥伴。這項共同努力，如果還能依據外國情報監視法，並且適切地對公眾說明，那將是一個低成本情報收集的金礦。但情報界需要向私部門做一個更聰明、更尊重的宣導，亦即認識到權力的數位平衡。其目標應該是將隱私和安全性轉變成正和博弈(positive-sum game)：以保證更加兼顧二者。

如此一來，國家安全局還可以扮演什麼角色？它的首要任務應該是情報加密、密碼破解和網路作戰。華府仍需要有能力滲透他國的加密網路，並且防止其敵人、敵對國家及非國家的相同作為。雖然國家安全局已在此領域證實其能力，它需要將重點聚焦於與那些優秀的中共、北韓、俄羅斯及非國家駭客齊頭並進。

今天，所謂的「浸派對」(dip party)，就是那種間諜趁著喝雞尾酒時竊聽的做法，早已過時了。

一目了然

網際網路公司的興起動力，已與另一股顛覆情報世界的力量平行：開放來源的資訊急速增加。在冷戰期間，沒有什麼能夠與一位完美安插的間諜或一間被完全竊聽的臥室價值相匹配。今天，所謂的「浸派對」(dip party)，就是那種間諜趁著喝雞尾酒時竊聽的做法，早已過時了。那是因為決策者所尋求的大部分資訊在很大程度上已不再是祕密。雖然複雜的諜報技術在某些情況下仍然有用——高階的網路攻擊有賴對人類、人的習慣及其使用軟體的熟悉瞭解——中情局不需要在俄羅斯農業部安排一名幹員，以瞭解烏克蘭的事態發展。事實

上，社群媒體已提供了一些從當地取得的最佳報導，讓旁觀者隨著事件的發展，即時同步上傳照片及影片。情報機構需要善用科技革命，科技革命讓突尼西亞水果販引爆「阿拉伯之春」(Arab Spring)，也讓伊斯蘭國(ISIS)利用張貼野蠻影片以吸引成千上萬追隨者，更讓美國國務院開始擁抱「推特」(Twitter)。

既然每個智慧型手機用戶都是情報的潛在收集者，則關鍵在於有技巧地整理數據。雖然沒有結構性障礙阻止美國情報界將此數據整理工作做好，但情報界仍然存有近乎精英主義的強烈偏見，反對使用免費即可獲得的資訊。他們的偏好經常是監聽恐怖分子的電話，以及派送間諜衛星去搜索隱藏的訓練營，而不是去讀某位19歲的聖戰士在「推特」社交網路上的留言。不過，處在一個網路激進的時代，教義或信仰的灌輸經常發生在明顯可見之處。

隨著情報界遠離傳統的諜報活動，轉向開放來源分析後，間諜業務中相當重要而恆久的問題將成為眾所關注的中心：如何保護分析，使之不因政策喜好而出現偏見。2004年的情報改革之所以被提出，有很大部分係因情報過程嚴重出錯，導致美國在2003 年入侵伊拉克，以及2001年911攻擊之前的不作為。決策者過去確實想要——如今仍然想要——確保國家永遠不會再面對類似的失敗。

美國國會2004年頒布的改革，對該時期而言是正確的，但如今情勢已發生轉變。當一個人擴展情報基礎，將那些任何人透過公開管道可廣泛獲得的大量原始資訊囊括進來後，在眾多分析師能呈現更大的圖像之前，個人的數據資料會有無數種方式讓決策者形成偏見。當然，一直都有讓偏見滲入簡報過程的方法：例如著眼於特定政策規定所製作的分析，或者透過持續不斷地針對尚未向總統徵詢過的單一主題進行簡報。開放來源的資訊會使問題變得更糟，但無論重新編組或政治上的改變都不能使問題消失。人們將偏見帶到他們所做的所有事情上，最終，情報的好壞與分析者本身相關。

此一基本事實不會很快獲得改變，不過其他很多事情則會。套用一句為「網路空間」(cyberspace)這個字彙命名的小說家吉卜生(William Gibson)所說的話：「未來已然在這裡了——只是分布得太不均勻。」塑造情報界的趨勢是可以察覺的：在預算上、在組織結構圖表上、在戰區裡。決策者卻遲遲沒有注意到，因為他們的注意力總是從一個危機跳到下一個危機。但是如果華府希望獲得領先地位，並防範未來的問題於未然，那就需要改變。誠如跟過去一樣，人員的素質不是問題，美國的分析師和官員持續以勇氣及卓越精神服務國家。真正的挑戰在於這個系統的適應力不如其所面對的敵人，且受限於傳統邏輯思維的束縛。

作者簡介

Jane Harman係「伍德羅威爾遜國際學者中心」(Woodrow Wilson International Center for Scholars) 主任、主席及執行長。她曾任九屆加州的眾議員。2002年至2006年期間，她是美國眾議院情報委員會的最資深民主黨員(ranking Democrat)。