

● 作者/Cortney Weinbaum and John N.T. Shanahan ● 譯者/李永悌 ● 審者/黃依歆

資料驅動時代下的情報作為

Intelligence in a Data-Driven Age

取材/2018年第三季美國聯合部隊季刊(*Joint Force Quarterly*, 3rd Quarter/2018)

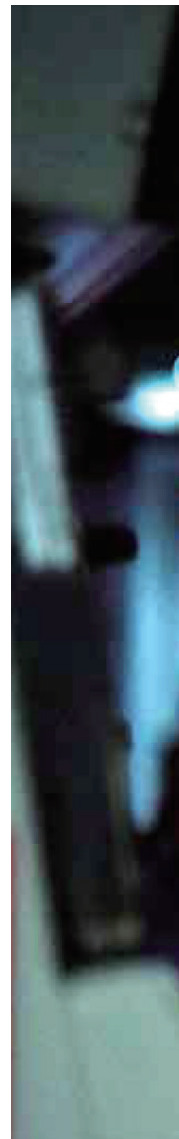
人工智慧與機器學習有助於增進未來情報分析效能，並提升競爭與時間的優勢，以獲得更多的勝算。數位轉型、有組織的多領域資料整合及演算法戰，將成為美國情報體系維持長期競爭優勢的要務。

在可預見的未來，美國無法偵測或反制的武器與戰術恐將造成戰爭的開端。現代的彈道飛彈需花費數十分鐘橫渡海洋，但未來的極音速武器卻可能僅需數分鐘即可完成。城鎮戰可能發生於高度連結的城市，這些地方的上空感測器價值有限，而無所不在的地面感測器卻承載過量資料，以致分析人員無法應用。在網路領域，當操作人員偵測到「武器發射」時，整批武器可能早已飛抵目標並達成所望效果。對衛星攻擊、經濟攻擊及祕密影響活動等，皆可能在無聲無息下發生，得知時早已為時已晚。

資料的向量、容量、快速、多樣性與無所不在，逐漸擾亂國家安全政策、作戰行動與情報的傳統工具與方法。擾亂的範圍只會擴大且加速。在「資訊就是力量」的口號影響下，社會已創造出能產生大量結構化與非結構資料的科技，其規模大到足以癱瘓以往的分析式諜報技術(analytic tradecraft)與模式認可(pattern rec-

ognition)。美國國防創新委員會(U.S. Defense Innovation Board)在2017年1月公開說明會提出的建議中，主張凡能蒐集或組織最多有關自己與敵人的資料者，將保有科技優勢。¹ 未能將資料視為戰略資產者，將拱手讓出寶貴的時間與空間給競爭對手或敵人。

美國情報體系，包括國防情報部門，面臨十分艱鉅的挑戰(容量與速度)，以及不斷增加的資料複雜度(多樣性與真實性)。在獲得、管理、關聯、融合，以及分析跨部會、盟國與夥伴不斷增加的大量資料時，美國情報體系備受挑戰。根據美國的經驗，情報體系產生資料時的格式差異，造成系統互不相容或無法進入，亦缺乏標準化的結構與全面共識的本體論。此情況導致所蒐集的情報有以下風險：未能有效利用、不夠即時、錯失跡象與警告，以及與決策無關。結果導致無法融合資料，及早在情報循環中產生多重來源情報，也無法盡可能接近蒐集點。分析人員被賦予過於困難、繁雜的任務且有過多障礙



尚待克服，導致無法提供決策者與作戰人員即時相關的分析判斷，或可採取行動的情報。

這些挑戰應透過以下方式解決：

- 引進可剖析資料、從資料中學習及據此反應的機器學習演算法。
- 鼓勵情報專業人員的創造力與深入思考。
- 設計有助於人機諜報技術成長的政策、資訊科技、敏捷

採購與安全環境。

這些問題無法在任何機構、計畫或情報領域內解決。美國已體認到以開創性方式適應此一新環境的迫切需求，其中必須包含用能掌控並了解大數據的系統與機器，進而提升情報體系的科技與作業優勢精進人機之間與機器之間的協同合作，因此分析人員得以充分利用時間，解決最棘手的問題。

同時，機器學習的「黑盒子」依舊有著無法預知後果的嚴重問題，其解決方案可能超出人類操作者的理解範圍。人工智慧系統已自行創造出人類程式設計師無法解讀的語言，² 並自行學習運用人類並未教導且無法理解的戰術進行遊戲。³ 在國家安全體系中，這些影響的後果仍然不明、多數未經驗證與探究。

2016年3月24日，美海軍飛彈驅逐艦墨菲號(USS *Michael Murphy*)士兵於珍珠港參與美海軍研究辦公室(Office of Naval Research)所展示的全新改良式訓練，其結合了軟體與兵棋推演技術，能協助海軍部隊發展各式任務與作戰行動的戰略。

(Source: USN/John F. Williams)

未來戰場空間

未來戰場空間的構成不僅包含船艦、戰車、飛彈與衛星，還包括演算法、網絡與感測網。在歷史上前所未見的是，未來戰爭將在衛星系統、電網、通信網路及運輸系統等軍用與民用的基礎設施，以及在人類網絡內進行。電子與人類戰場皆極易遭受敵方演算法的操控。

在電子環境中，演算法已用於監視與持續掌控關鍵基礎設施(電力、水力、食物、金融、通信……)。俄羅斯與中共已表露興趣，並有意在美國測試這些系統的能力與弱點，美國情報機構必須能融合跨多重來源的資料，方可了解敵方的活動和預期目標。

為擾亂人類網絡，美國聯邦人事管理局經安全查核的政府員工個資遭竊的案例，其所提供的豐富資料可供敵人針對單一軍事領導人或決策者打造祕密影響行動。⁴ 若這些資料與竊取自易速傳真(Equifax)公司的財務資料、雅虎(Yahoo!)網站的電子郵件紀錄、偉彭(Anthem)健康保險公司的醫療資訊及其他來源的資料相結合，演算法將可針對美國創造出高度精密且個人化的祕密影響行動。在一般行動上，北大西洋公約組織軍事部隊近期指出，其官兵的電話在軍事演訓期間遭俄羅



在電子環境中，演算法已用於監視與持續掌控關鍵基礎設施。

(Source: USAF/Andy M. Kin)

斯駭客入侵，據北約官員表示，其目的在「獲得作戰資訊、評估部隊實力與威嚇士兵」。⁵

能融合來自不同資料集的巨量資料並提供有意義的答案，正是人工智慧與機器學習的存在意義。只要商業界

能找到可用資料來預測消費者可能購買何種廠牌汽車或牙刷的方法，廠商就能辨識出用戶的偏好和弱點，就像情報官期待在個人心理檔案找到的資訊一樣。

美國處於容許對手加速竊取競爭優勢的風險之中。中共已制定人工智慧國家戰略，並承諾於未來五年投資數十億美元於人工智慧科技。⁶ 中共研究人員發表的人工智慧期刊論文量亦超過美國，⁷ 而共軍的戰略專家正準備應付未來人類無法跟上戰場決策節奏的世界。⁸

美國近期公布的《國家安全戰略》與《國防戰略報告》，皆提到人工智慧與自主功能對國家安全與作戰的重要性。⁹ 惟除了2016年「美國國家人工智慧研發戰略計畫」(多聚焦於研發)之外，美國還沒有全面性的人工智慧戰略。

字母公司(Alphabet，谷歌的母公司)前執行董事長暨美國國防創新諮詢委員會(Defense In-

novation Advisory Board)主席施密特(Eric Schmidt)提及中共相較於美國在人工智慧方面的進展：「2020年，中共將迎頭趕上；2025年，則將超越美國；到了2030年，中共將主導這項產業。」¹⁰

令人憂心的情報失誤

未來的諜報技術將仰賴存取資料、依據資料塑造正確的企業架構，以及發展人工智慧導向能力，並藉由透過人機與機器之間協同來大幅加速對資料的情境化理解，以及增進能在海量資料中找尋正確方向的分析專業。美國情報體系需要發展存取、管理與分析資料的諜報技術與方法論，包括機器智慧的結構化分析技術及分析式諜報技術標準。新技術的演進速度已超出美國國防部及情報體系能有效實行、訓練與運用該技術的能力。

美國國防情報部門內部對搜集器與感測器的投資，產生比以往許多類型的感測器有蒐集更多資料的能力。美國國防部對無人系統的計畫中囊括數千種無人空中、海上與地面系統

的說明，惟並未描述如何分析蒐集自這些系統所蒐集的資料以創造價值。¹¹ 除此之外，還包括太空系統與可公開獲得的非機密系統。情報蒐集的增加，甚至是來自絕對機密等級的精良感測器，並不一定等於擁有更多更好的情報或方針，尤其在面對實力匹敵者之時，他們可能同樣擅於適應資訊環境。

美國國防部由沙納翰(Shanahan)中將主導的「專家計畫」(Project Maven)，目標在克服人類情報分析員無法有效處理各領域大量且種類各異的情蒐問題，該窘境稱之為「成功災難」(success catastrophe)。¹² 「專家計畫」作為起點與開創計畫，前美國國防部副部長沃克(Robert Work)要求該計畫團隊找出人工智慧與電腦觀點的解決方案，俾加強、擴大與自動化無人空中系統全動態影像的運用。

當前情報實務係自跨領域(跨情報)的大型資料集中擷取出有價值的資訊，就像大海撈針，這導致大量蒐集與儲存情資，最終意圖將全部有價值情資一網打盡。而在日益邁入資料導向的時代，從大批彙總資料(例如

時間性與地理性的行為模式)中得出有價值情資的機會愈來愈大。如此將產生出乎意料的困境，因為資料過多恐造成人類無法有效搜尋有價值情資，而且也無足夠可用資料能產生並證實有用的情報。

接著就是一旦在獲得情報後該如何處置的問題。美軍各軍種刻正發展與獲得的戰鬥系統較以往需要更多的資料與情報，而情報任務資訊必須在獲得週期中盡早置入這些系統，且要能經常性快速更新，俾運用於作戰、可用資料結構，以及戰鬥系統可處理的機密等級當中。¹³ 在政策領域也一樣，由於機密情報的傳遞速度過慢或機密等級太高而無法使用，決策者日漸仰賴非機密的公開來源資訊。¹⁴

美空軍退役上校波伊德(John Boyd)在其開創性的「觀察、指導、決心、執行」(observe, orient, decide, and act, OODA)循環研究中，強調運用敵人無法理解的作戰節奏或使其跟不上作戰步調的重要性。在敵人的「觀察、指導、決心、執行」循環內運作，有助於透過迷惑或蒙



在演算法的新戰爭型態下，作戰人員將會視過去有數分鐘決策時間為一種奢侈。(Source: USAF/Zach Anderson)

敵對手的心理圖像來達成這些目標，如此一來，敵人即無法體會與應付周遭發生的事。在今日節奏快速且不斷變化的資料導向時代，資訊主宰(information dominance)或資訊優勢(information superiority)等詞彙仍為天馬行空的想像；反之，時間優勢(temporal advantage)可能是最好的結果。惟若美軍作戰人員能保持在敵方的「觀察、指導、決心、執行」循環之內，同時以富有想像力的方式運用資料去扭曲敵人的方向，如此亦足以佔得上風。

人工智慧與機器學習可於資料抵達時即時理解資料、評估選項、於數毫秒內發起行動與有所作為，透過「觀察、指導、決心、執行」循環各個步驟提供加速決策的機會。此類決策包括在人類操作員有時間讀取警示之前回應指示與警告，或於預定的核定參數之內展開反應。機器學習可提供縮短「觀察、指導、決心、執行」循環前兩個階段的新契機，並大幅增加人類加速決策與採取行動

的潛力。

美軍未來極可能面對「演算法對抗演算法」之戰，不禁令人感慨二十一世紀的作戰人員是否會將數分鐘的決策時間視為一種過去的奢侈。

解決方案近在眼前

情報機構能夠也應該投資跨領域、跨計畫與跨學門的機器學習能力，並要求情報官充分發揮這些能力。任何仍在艙間、專屬資料庫以及演算法無法觸及的機密領域所傳遞的資料，都需要由情報官進行人工整合，如此將延遲情報評估，並產生受保護的泡沫資料，而情報官無法查看此種資料，導致無法將所有的情資來源應用於分析問題。此情況對「知之必要」(need to know)概念形成威脅，並將迫使情報蒐集與分析部門(包含反情報與保防官同僚)將內部與外部威脅等而視之。資料保護政策可授權演算法存取人類分析員無法了解的資料欄位，如此可能需要決定對機器要有何種程度的信任，以及如何審核當機器工作時來自敵人造成與自然發生的漏洞。

為達到相關目標，美國應考慮進行以下數種行動。首先，尋找任何情報問題的答案時，應以每個分析員都需要所有潛在相關資料為前提，資料應來自每一筆可能的來源。¹⁵ 這代表必須在傳統的演繹(尋找已知的未知數)與歸納(透過合成發現未知的未知數)分析方法之間取得不同的平衡。這也需要有不同的情報蒐集方法，因為所有資料在蒐集許久後仍可能有關聯性，並應能在可得的檔案庫自由存取；此作法程序將大幅取決於資料集是否包含美國的個人與其他受保護實體的資

料，同時資料控制與資料品質保證將是基本功能。

機器學習與人工智慧的廣泛整合，將使因資料遭到竄改或操縱而產生的欺騙有機可乘。反制人工智慧(Counter-AI)將逐漸盛行，同時影響行動將呈現有待摸索的新面向，需重新強調攻勢與守勢的認知導向行動。情報分析員必須接受訓練，

學習如何看穿敵人意圖竄改或操縱資料之想法，包括了解如何運用人工智慧獲得最大優勢，以避免更精密的影響行動所造成的後果。

其次，不應將資料視為資訊科技問題；換言之，應以資訊科技系統所解決的作業問題去建構資訊科技系統。如此一來必須從封閉、專屬的架構與令

人無法接受的缺乏資料標準，轉變為開放式架構與敏捷方法學(Agile Methodology，開放式架構與快速短暫採用新科技與應用程式)，所有分析人員皆可隨時查詢與取用任何來源的任何資料。更常見的是將演算法移往資料，而非試圖將資料移往演算法。全球雲端解決方案(global cloud solution)對於人



2018年4月5日，美陸軍第10山地師第1旅級戰鬥部隊第6野戰砲兵團第3營士兵於鼓堡(Fort Drum)任務訓練中心瀏覽新式徒步精確射擊(Precision Fires-Dismounted)系統，包括以智慧型手機觀看無人飛行載具之直播全動態影像、3D數位地圖，以及發送精確目標座標等功能。(Source: US Army/James Avery)

工智慧各方面的整合而言，是至關重要且最為適用的方法，這方案不是只提供資料儲存或搜尋之用，更要掌握資料存取，才能提供機器學習與人機協同。因此，快速的資料存取需要有效的資料管理，而這需要有各式新技能與專業知識，諸如資料架構師與資料科學家。跨所有安全領域的網絡存取、所有相關類型資料之存取，以及顛覆性科技的敏捷整合，是實現與維持決策優勢的關鍵。

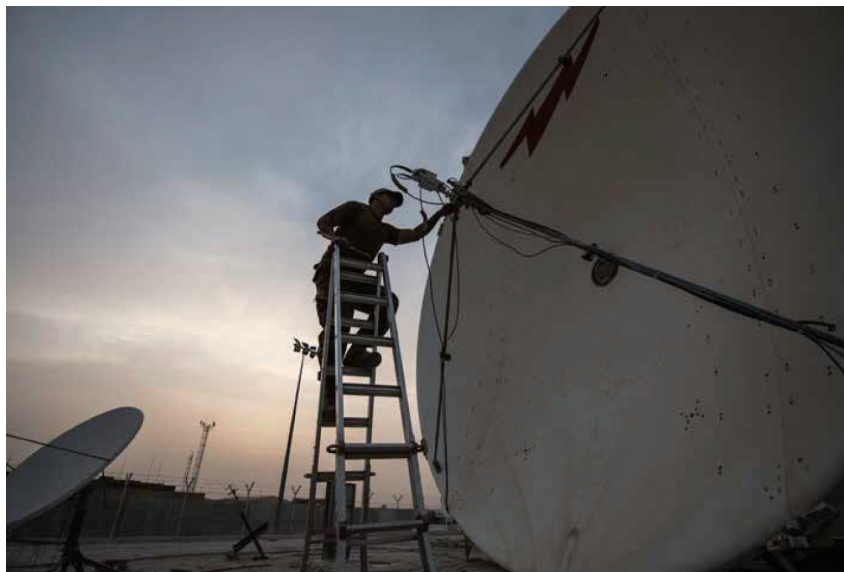
第三，公開可得與公開來源資訊將構成情報知識的根基。如此必須從最高機密情報絕對

正確的假設，大幅改變為接受並整合非傳統與非機密情資來源。自其他情報領域精心蒐集的情資，將可強化基礎情報，並填補現有的知識缺口。當機密等級不再是資訊具有情報價值的要件時，這將顛覆了六十年以來的傳統模式，並挑戰了「情報」的基本概念。¹⁶

第四，從工業時代的生產線處理與利用單一資料蒐集流的聯合分析團隊，轉變為資訊時代的企業經營模式，由部分分析人員進行多來源(multi-source)與全來源(all-source)的關聯與融合，並與盟軍、國家與

國際夥伴完全整合。儘管情報資料的分層是不錯的開始，但仍然不足。我們必須充份理解人類與人工智慧系統，才能賦予決策時間與空間。這項原則也引發了與未來全分析團隊廣度與深度平衡的更大問題。訓練必須更強調分析時的綜合研判與創造能力。

最後，上述解決方案需要革新美國情報體系對人力資本、預算編列、獲得、研究發展的生命週期。由於雇用與安全查核程序長達兩年或更久，導致各機構任用的是兩年前(在資料導向時代中算長了)名列前茅的員工，而在職業生涯中期雇用方面，職務要求在政府單位任職的經驗，要高於商業與學術領域的科學、科技與分析經驗。¹⁷在最好的情況下，美國國防部與情報體系在四年期的計畫預算執行(Planning, Programming, Budgeting, and Execution)程序內產出多年預算策略時一直備受挑戰，同時在目前長期持續撥款決議案(chronic continuing resolution)的氛圍中，產生預算策略只是期望，不會經常發生。各情報機構屢屢試圖利用一小



2018年3月30日，參與沉默哨兵行動(Operation Silent Sentry)的美空軍第379作戰支援中隊士兵於卡達烏代德空軍基地(Al Udeid Air Base)執行衛星天線保養，以維護關鍵衛星通信鏈路正常運作。(Source: US Air National Guard/Phil Speck)

部分的預算與「創新辦公室」制定創新的採購改革，惟這些解決方案擴及國家或軍事情報計畫時卻停滯不前。

改變美國情報體系的傳統採購程序，必須有一批訓練有素並擁有資源的合約官來澈底改革訂約程序，重新聚焦於品質、結果與產生關聯的速度，而非默許最低價、技術上尚可接受的合約。¹⁸採用敏捷方法學將促使科技開發、執行與精進的步伐更加迅速。最後，這些改革每一項都能創造出能讓研發部門蓬勃發展的環境，不論是在情報體系各機構或各軍種內。研發組織需要最傑出的技術人員，負責在情蒐人員、分析人員與產業供應商之間建立合作夥伴關係，而他們需要合約官積極主動的支援與有效的預算環境才能成功，最終將創造出備便人工智慧的典型作戰文化。

結論

本文至少提出了一項美國應規劃解決的致命弱點：過分仰賴科技。即使在自主式系統時代，戰爭仍將由人類戮力進行。若美國對抗的是在阿富汗山區或非洲叢林等技術落後的敵人，作戰人員與情報官將面對過份依賴需要大量資料的系統風險，抑或在勢均力敵的情況下，美國敵人有一天將能找出並利用美軍技術漏洞，使美軍作戰人員失去判斷力，或以全新且有創意的方式運用資料對抗美國。鑑於這兩種情況，美國將持續重視通過低技術測試且可靠的情報分析人員與作戰人員，他們要具備諜報技術與解決方案的專長。

最佳的情報分析源自藝術與科學的正確結合。今日的情報藝術可能與兩千年前並無差異。然而

現在不同的是，我們必須能讓以資料為重心的諜報技術科學變得更快更好。分析人員必須具備所有工具，才能處理大量資訊，使其能填補情報缺口，並能受惠於資料迅速獲得所產生的更佳行動結果。

人工智慧與機器學習將有助於增進未來情報分析人員團隊的效能，提高獲取與維持競爭或時間優勢的勝算。數位轉型、有組織的多領域資料整合，以及演算法戰，將成為情報部門維持長期競爭優勢角色的重心。這是戰略上的創新，也是戰術或分析層級的創新。兩者必須同時具備，但如此仍然不足。

美國情報體系即將面對人工智慧與機器學習的重大決定。儘管在十六年來不斷反恐與戡亂行動中尚存在缺失，美國情報體系仍打造出一支經驗豐富、受過實戰訓練的分析人員團隊，在世界上實不多見。美國情報體系最強大的潛在不對稱優勢仍為其快速理解資料，並保持在敵人的「觀察、指導、決心、執行」循環內的能力。美國與其敵人們是否會將機器的效能放慢至人類思考的速度，俾在此循環中維持人類的存在？或者各國是否將追求人工智慧並發揮其最大潛力，深怕若未達成將讓敵人佔得先機？現在已是美國情報體系決定如何回答這些問題的時候了。

作者簡介

Cortney Weinbaum係蘭德公司管理科學家。

John N.T. “Jack” Shanahan中將係國防部情報副部長辦公室國防情報(作戰支援)主任。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. “Defense Innovation Board Holds Public Meeting,” *DOD News*, video, 1:54:30, October 24, 2017, available at <www.defense.gov/Videos/videoId/560180/#DVIDSVideoPlayer1133>. Emphasis added.
2. Mark Wilson, “AI Is Inventing Languages Humans Can’t Understand. Should We Stop It?” *Co. Design*, July 14, 2017, available at <www.fastcodesign.com/90132632/ai-is-inventing-its-own-perfect-languages-should-we-stop-it>.
3. Larry Greenemeier, “AI versus AI: Self-Taught AlphaGo Zero Vanquishes Its Predecessor,” *Scientific American*, October 18, 2017, available at <www.scientificamerican.com/article/ai-versus-ai-self-taught-alphago-zero-vanquishes-its-predecessor/>.
4. Sina Beaghley, Joshua Mendelsohn, and David Stebbins, “What Is the Adversary Likely to Do with the Clearance Records for 20 Million Americans?” *Inside Sources*, January 19, 2017, available at <www.insidesources.com/adversary-likely-clearance-records-20-million-americans/>.
5. Thomas Grove, Julian E. Barnes, and Drew Hinshaw, “Russia Targets NATO Soldier Smartphones, Western Officials Say,” *Wall Street Journal*, October 4, 2017, available at <www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402>.
6. Graham Webster et al., “China’s Plan to ‘Lead’ in AI: Purpose, Prospects, and Problems,” *New America*, August 1, 2017, available at <www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/>.
7. “China May Match or Beat America in AI,” *The Economist*, July 15, 2017, available at <www.economist.com/news/business/21725018-its-deep-pool-data-may-let-it-lead-artificial-intelligence-china-may-match-or-beat-america>.
8. Elsa B. Kania, “Artificial Intelligence and Chinese Power,” *Foreign Affairs*, December 5, 2017, available at <www.foreignaffairs.com/articles/china/2017-12-05/artificial-intelligence-and-chinese-power>.
9. *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), available at <www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>; *Summary of the National Defense Strategy: Sharpening the American Military’s Competitive Edge* (Washington, DC: Department of Defense, 2018), available at <www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
10. Patrick Tucker, “China Will Surpass U.S. in AI Around 2025, Says Google’s Eric Schmidt,” *Defense One*, November 1, 2017, available at <www.defenseone.com/technology/2017/11/google-chief-china-will-surpass-us-ai-around-2025/142214/>.
11. *Unmanned Systems Integrated Roadmap FY2013–2038* (Washington, DC: Department of Defense, 2013), available at <<http://archive.defense.gov/pubs/DOD-USRM-2013.pdf>>.
12. Cheryl Pellerin, “Project Maven to Deploy Computer Algorithms to War Zone by Year’s End,” *DOD News*, July 21, 2017, available at <www.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/>.
13. *Unmanned Systems Integrated Roadmap FY2013–2038*.
14. Derek Grossman, “Keeping Up with the Policymakers: The Unclassified Tearline,” *War on the Rocks*, July 28, 2016, available at <<https://warontherocks.com/2016/07/keeping-up-with-the-policymakers-the-unclassified-tearline/>>.
15. *The 9/11 Commission Report* (Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004), available at <www.9-11commission.gov/>.
16. Rich Girven, Sina Beaghley, and Cortney Weinbaum, “A New Paradigm for Secrecy,” *U.S. News & World Report*, October 13, 2015, available at <www.usnews.com/opinion/blogs/world-report/2015/10/13/defining-a-new-paradigm-for-government-secrecy>.
17. Lindy Kyzer, “Top Secret Clearance Processing Times Lengthen, Secret Times Improve,” *ClearanceJobs.com*, November 1, 2017, available at <<https://news.clearance-jobs.com/2017/11/01/top-secret-clearance-processing-times-lengthen-secret-times-improve/>>.
18. Scott R. Calisti, “Lowest Price Technically Acceptable: Why All the Debate?” *Defense AT&L*, March–April 2015, available at <<http://dau.dodlive.mil/2015/03/01/lowest-price-technically-acceptable-why-all-the-debate/>>.