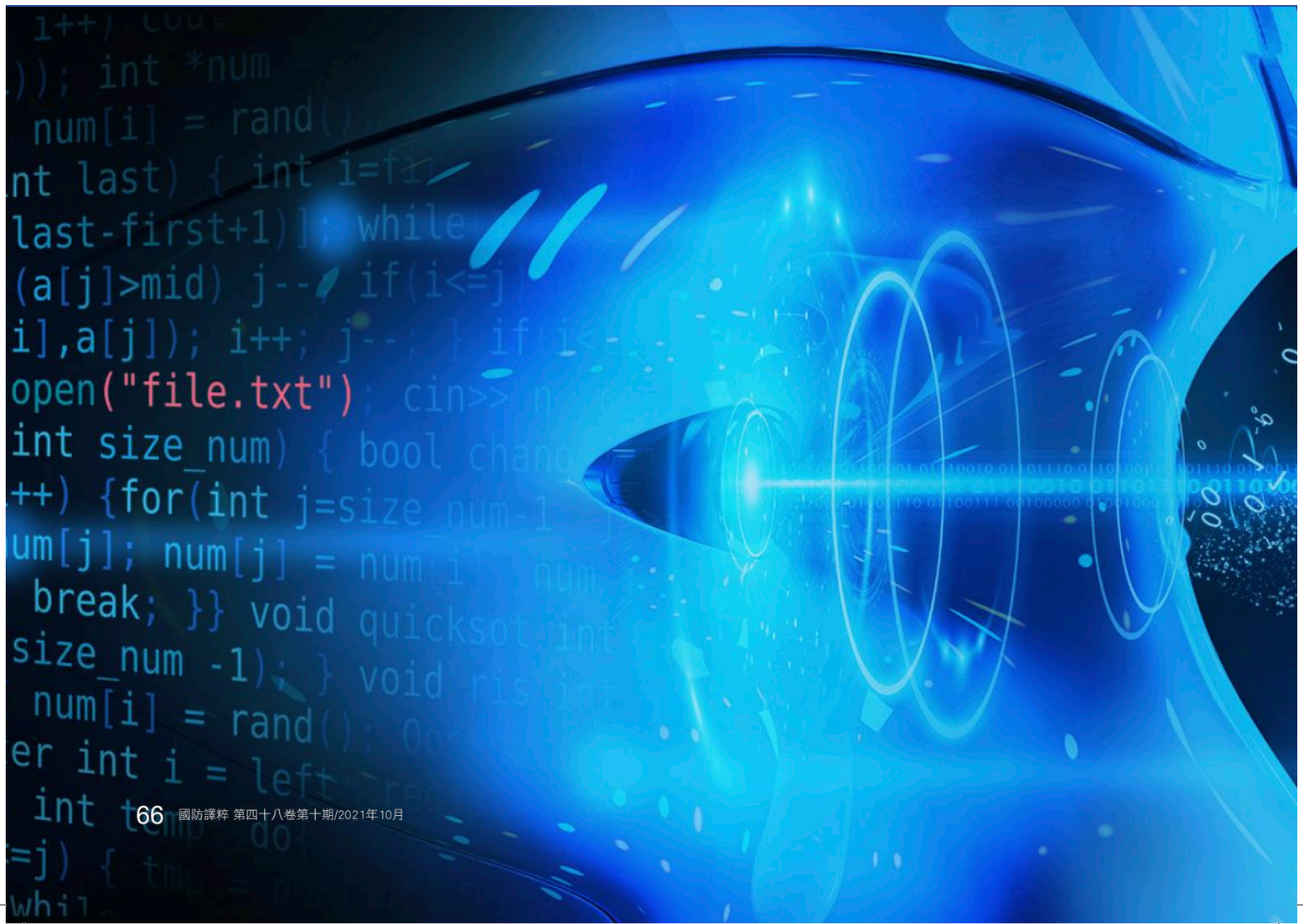
● 作者/Sam J. Tangredi ● 譯者/李永悌 ● 審者/馬浩翔

當孫子兵法碰上人工智慧

Sun Tzu Versus AI: Why Artificial Intelligence Can Fail in Great Power Conflict

取材/2021年5月美國海軍學會月刊(*Proceedings*, May/2021)

孫子有云：「兵者，詭道也。」商用人工智慧往往無法克服資料訛騙的問題，故本文主張應將資源投注於能解決此問題的感測器，並重新以軍用標準重整軍中的人工智慧，以符實需。



在五角大廈，目前人工智慧（Artificial Intelligence, AI)的前景，有如第二次世界大戰期間，後勤對美海軍艦隊司令暨美海軍軍令部部長金恩(Ernest King)上將般重要。據聞金恩曾在第二次世界大戰初期說過：「我不知道(美陸軍參謀長)馬歇爾(上將)說的『後勤』是什麼，不過海軍也需要它。」[1]受到政壇與企業界領袖思維所影響，近期美國防部官員似乎咸認(或至少在言語上強調)人工智慧將為戰爭帶來澈底與歷史性的改變。即便上述人士並不瞭解人工智慧的能力與限制，但仍要求「多多益善」。

儘管此種以擴大人工智慧軍事運用當作資訊管理手段的作法值得讚許，然而若因而認為人工智慧將改變遊戲規則則相當危險，因為這將使美國國防部無法認清事實，亦即與過去相比，當前戰爭中資訊與欺敵間的角力並未有澈底、必然或性質上的差異。人工智慧也許速度較快，或許是以電腦語言0與1進行，甚或涉及巨幅增加的原始資料；但致勝的最重要關鍵依舊是資訊有效性，而非處理資訊的手段。

這也就是為何美軍投資軍事人工智慧能力的心態操之過急──加上技術專家、軍事

「轉型主義者」或滿懷希望的投資人過度炒作的推波助瀾下——恐將招致失敗的原因。美國國防部必須認清，作為軍事資訊處理工具的人工智慧，只不過是資料世界中被過度放大的一角。即便美軍準則對此已有見解，但人工智慧既未改變戰爭的特徵，也未改變戰爭的本質。假設人工智慧確實能改變戰爭，而且主要係出自國防領導高層的意圖，則美國的投資與國防將面臨風險，尤其當美國國防部仰賴商用人工智慧時更是如此。

戰爭特質與商用人工智慧

的確，鑑於美軍部隊充斥著大量作戰與戰術資訊，投資人工智慧相當合理。資料似乎無所不在。如欲理解由作戰人員透過數位系統蒐集並且數量不斷激增的資料，那麼擁有能更迅速編輯、儲存與分類資訊的方法，就顯得至關重要。惟各類資料的重要性不盡相同，更重要的是其中大多是無關、無用、不完整或虛假的資料。此外，由於美國的安全環境係採潛在大國衝突——更恰當的術語應為「大型體制衝突」(Great Systems Conflict)——的形式架構，因此蒐集到的假資料將與日俱增。[2] 在此必須強調：假資料只會愈來愈多——並以類似日漸充斥在社群媒體的即時意見、推文與陰謀論等形式存在。

以上對美國國防部與人工智慧發展而言都是重要課題。企業界使用的人工智慧——特別是與網路產生資料有關者——在設計時多半未考量防範蓄意欺騙。然而倘若潛在客戶或許就其欲購買之產品或服務蓄意欺騙供應商，則整個人工智慧輔助行銷模式將隨之崩潰。假設供應鏈中的公司就零件規格欺騙組裝廠商，則該供應鏈將無法正常運作。若資料為假，人工智慧將不再是行銷或生產的商用資產——而是負債。商用人工智慧要發揮正常功能，必須假設其不受訛騙。

相較之下，無須再次閱讀中國戰略家孫子的兵法，就能知道此種情況在戰爭中絕不可能發生。因為「兵者，詭道也」，這句話經常被奉為孫子思想的主軸。

關於人工智慧是否將改變戰爭本質與特性的問題一直爭論不休——甚至最高延燒至國防部長層級。[3] 若戰爭本質是使對手屈服於我方意志的暴力(此為多數爭論者所認同的觀點)，則人工智慧無法改變此種定義。若戰爭的特性如孫子所言為欺敵，則人工智慧亦同樣無法加以改變。此外，自海格(Chuck Hagel)、卡特(Ashton Carter)以至於馬提斯(James Mattis)等歷任國防部長，皆依靠商用人工智慧作為軍事人工智慧決策輔助系統的最終基礎，惟其無法在目前發展狀態下改變戰爭的特性(欺騙)，且該特性與其用途彼此違悖。[4]

美國國防部在有關人工智慧發展的論述中，一直嚴重低估與經常忽視欺敵之效。惟近期的情報先進研究計畫活動(Intelligence Advanced Research Programs Activity)已著手研究欺敵與人工智慧間的關係。[5] 目前欺敵主題已逐漸納入美國國防部的內部討論，惟欺敵一詞往往仍無法連結人工智慧的論述。[6]

為避免錯誤投資、過度期待與期望落空時造成大眾無可避免的希望破滅，美國國防部必須承認，大部分商用人工智慧設計不僅未注意戰爭特質，也未將欺敵視為環境要素。將人工智慧納

人工智慧演算法只是統計分析程式，因此蒐集資料的感測器才是比演算法本身更為重要的投資。諸如中國共產黨等專制政權早已深諳此道，這也就是為何中共欲建立一套每十人就至少有一架國家監視攝影機監控的網路。
(Source: ALAMY)

入行政與保修功能以外之軍事用途，所需要的時間、研究與財政資源，遠比許多專家和支持者所能理解得更多。美國防部切勿在欺敵與人工智慧等課題上自欺欺人。

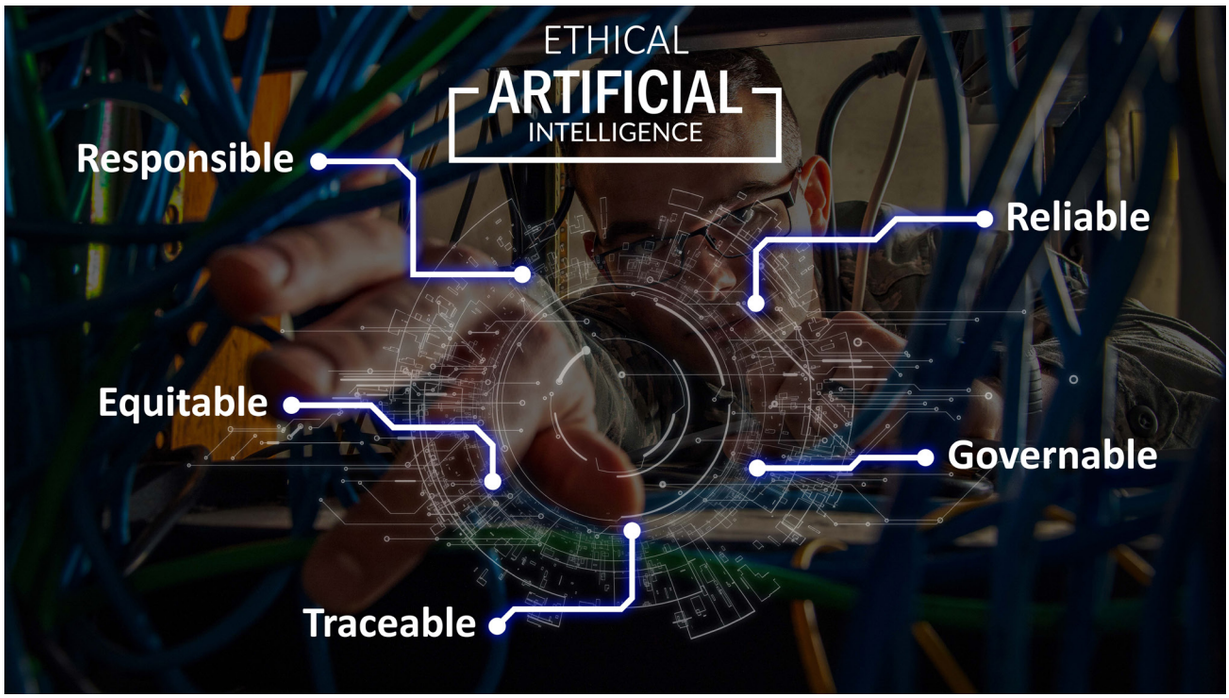
欺騙人工智慧演算法易如反掌

為何要對欺敵有所警覺？因為若無可資證明的正確資訊，人工智慧將極易受到欺騙。讀者可在家自行嘗試與驗證以下作法。

首先前往您已註冊過的購物網站，接著登入，並開始點選您不感興趣的銷售貨品。更有趣的是，選擇一項你從未參與過的運動──或許以網球為例。再點選球拍、網球、球衣或相關用品。該公司──以及其他購買您個人資料庫的公司──的行銷演算法會將個人資料迅速調整為包含網球。此時您得忍受收到網球用品廣告的困擾，不過只要透過網路瀏覽器明智查看部分與網球有關的網站後，即便您從未拿過球拍，數位世界也會將您視為網球選手。此時您的數位資料也已遭篡改。此舉不保證閣下將收到邀請加入本地網球俱樂部的電子郵件，不過隨著所謂的人工智慧在網路上日益普及，甚至比目前更無所不在，您或許會真的會收到邀請。因為根據演算法，閣下就是位網球選手。

這對國家安全領域亦有同樣影響──而且向來都是如此。敵人遭到挺進、佯攻、假行動、假報告、謠言、能力公開展示等類似手段欺騙的例子已不勝枚舉。這不僅是戰時反映的問題；承平時期的計畫與分析往往也會受誤導。直到冷戰結束後方得以窺探部分蘇聯檔案，在此之前美國就未曾注意到前蘇聯領導人對核子嚇阻與戰爭可能性的看法有多麼不同。[7]

這代表什麼？這代表人工智慧演算法只是統計分析程式。從獲得角度觀之，這意味著感測器才是比演算法(人工智慧)本身更重要的投資。諸如中國共產黨等專制政權早已深諳此道，這也就是為何──隨著以人工智慧推動的社會信用系統發



近期欺敵與人工智慧間之關聯，在美國防部引起眾多討論。(Source: DoD)

展一中共欲建立一套每十人就至少有一架國家監視攝影機監控(共有超過14億人民)的網路。[8] 人工智慧是否將使中共(遺憾的是，這是在民主國家發展的商用人工智慧協助下)有能力將中國大陸變得更加專制？[9] 確實如此；但若沒有這些攝影機，就無法達成目的。在沒有感測器確認資訊有效性的情況下──例如偵測到您已親身踏上網球場──人工智慧提出之建議仍不如人類判斷。

沒有資料，人工智慧將無用武之地

所謂的人工智慧與一般認知的智力無關。它只是比較高階的運算，能迅速串聯大量資料，並已證實能模擬兩種人類的特性：語音及視覺識別，而兩者都需要大量資料。這些能力以統計方法為基礎，比對傳入資訊與大量訓練資料，直到二進位電子計算的1與0認為近乎吻合。甲骨文(Oracle)公司某資深副總裁，將人工智慧定義為「教導軟體根據過往資料進行決策的統計技術。」[10] 部分由這些技術所產生的演算法可追溯至1890年代，當時統計技術才剛開始應用在商業領域。

機器學習與大數據是從統計技術中「創造」出人工智慧的兩項要素。在此過程中，機器學習實際上就是程式設計。而大數據則是被處理的資訊。這些術語可能會讓人看不清機器學習不具意義，且人工智慧若無正確可用資訊將無法發揮作用的事實。因此，俄羅斯萬年總統普丁有名言提到「人工智慧就是未來……而成為此領域的領導者，就能統治世界」，就並非正確說法。[11] 事

實上，政治軍事決策的主導者擁有的並非「最佳人工智慧」，而是在所有其他權力要素相對均等條件下，擁有最正確、最有意義且毫無虛假的資料。

沒有正確資料，最佳演算法或人工智慧機器將落得一無是處。因此，美國國防部欲將經費投資在任何特定人工智慧解決方案以前，應先考慮以下三個重要問題。首先，在競爭環境中是否有系統可以仰賴的資料？其次，人工智慧系統在僅有不完整或部分資料正確時，可否提供合理的決策協助？最後，人工智慧系統能否能預判與辨識出虛假資料？

簡言之，問題出在現有之商用人工智慧系統於發展時並未考量上述問題。

為資料而戰

冷戰(美國最後一段大型體制競爭)期間，蘇聯海軍元帥高希科夫(Sergey G. Gorshkov)將敵對行動前的行動與機動，諸如資訊蒐集與處理等，稱為「為第一擊而戰」(Struggle for the First Salvo)。在此觀點中，擁有最正確資訊的部隊與能先發制人打出第一擊者，將會獲得勝利。已故美海軍戰術權威休斯上校(Wayne Hughes)則將此優勢稱為「有效先制攻擊」(Attacking Effectively First)。[12]

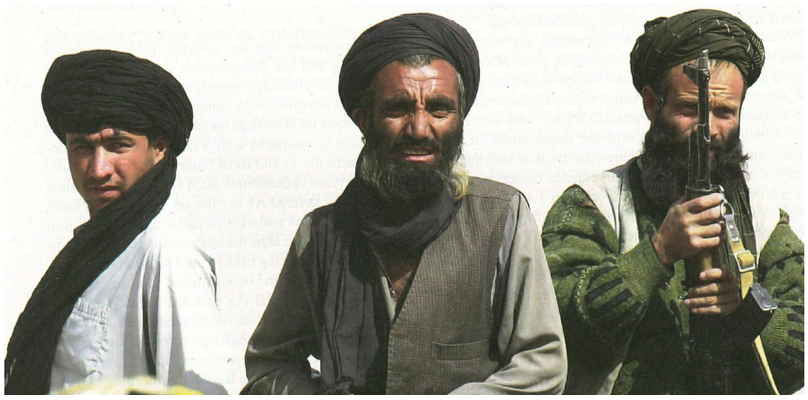
欲遂行有效先制攻擊，必須比敵人更迅速、更正確處理正確資訊。惟此處須再次強調，資訊正確性只是基本要求。人工智慧本身可作為判斷正確性的工具，惟前提是系統能知道所有蒐集到的資訊(不僅是特定資料)都有可能遭竄改。

冷戰期間，對於敵人特性、能力與意圖進行欺騙的可能性一直存有爭議。部分分析師主張，蘇聯擁有美國未能察覺的廣大戰略欺敵系統(其他人則認為這些分析師偏執妄想)。無論是何種情況，鮮少有人主張蘇聯並未三不五時在作戰層級做到成功欺敵。這是一場「貓捉老鼠」的比賽，而且追捕者與躲藏者能力幾乎可說是旗鼓相當。

儘管對此事實僅有口惠而無作為，但自冷戰結束後美國在其所選擇進行的衝突中，皆未在作戰層級棋逢對手。自沙漠風暴作戰行動展開後，美軍部隊比敵人擁有之更大優勢，在於可用且絕大部分正確的資訊，因此很少有人認真看待戰略或作戰層級欺敵的可能性。由於欺敵仍是戰爭戰術層級的明顯特性，因此戰術欺敵被視為可行作法。儘管如此，藉由增加感測器數量來蒐集更多資訊，仍被視為破除欺敵可能性的可行解決方案。

感測器能力與能量的提升，已到了讓部分軍事將領以為「迷霧已經解除」的境界。然而尚未被強調的是，這些敵人──無論是海珊主政的伊拉克、塔利班(Taliban)、米洛塞維奇(Slobodan Milošević)主政的塞爾維亞、或格達費(Muammar Qaddafi)統治的利比亞──在作戰層級的貓捉老鼠競賽中，完全不是美國對手。他們沒有欺騙美國感測器網路的能力。

儘管「戰爭迷霧已完全消除」的觀點在2000年代初期已不再具有吸引力，但大肆宣傳人工智慧卻有可能讓此觀點死灰復燃。從近期經驗中獲得的結論是，所有對欺敵的潛在關注，皆已消失在國防決策的背景中──同時人工智慧在軍事運用



自冷戰以來，如塔利班等諸多美國敵人在技術上未能趕上美國，也缺乏欺騙美國感測器網路的能力。惟若與中共或俄羅斯發生衝突，情況將有所不同。
(Source: San J. Tangredi)

的潛力上變得十分明顯。因此，美國國防部對於有大量資訊可用而甘之如飴的態度，恰好合乎美國科技業假設資訊的正確性與生俱來的看法。商用人工智慧在蒐集愈來愈多資訊，以及在運用更深入、複雜的演算法時，會假設自己不受欺騙。

惟在大型體系衝突下的未來安全環境中，此種假設是否正確？絕對不是。即便對人工智慧發展抱持樂觀態度，美國潛在敵人──中共及普丁領導的俄羅斯──擁有欺敵能力，將使美國自冷戰以來曾遭遇的所有欺敵活動相形見絀。此外，兩者的人工智慧系統發展皆已能與美國並駕齊驅，是有能力控制商用人工智慧發展的陰謀與反情報政權，亦已深諳人工智慧的弱點。兩者將惡意軟體植入美國商用人工智慧(質言之，即是商業界開發的軍事人工智慧應用)的能力確實相當驚人。

為正確資訊而戰，在大型體系競爭中將變得更形困難。軍事人工智慧必須據此作為立足的基本原則。

攸關未來的是資訊──而非人工智慧

為能成功管理軍事人工智慧的發展，美國國防部必須瞭解欺敵是必要的考量因素，而人工智慧必須一開始即為此目的而設計。

為能使軍事人工智慧維持合乎實際的期待，美國國防部必須謹記，未來效能所仰賴的是資訊，而不是處理資訊的人工智慧。人工智慧有助提升資訊處理速度──但卻不見得能讓資訊更為正確。感測器比運算系統更重要。沒有正確的資訊，人工智慧系統產生的將只是虛假資料。

自冷戰結束後，美國聯合部隊更加仰賴與沉溺在從戰爭與干預行動中所獲得的寶貴資訊，這已構成戰略問題。未來美軍部隊在大型體系競爭中獲得的正確資訊，將遠比後冷戰環境下獲得的還要少。人工智慧演算法無法減緩這項趨勢。為了反制欺騙，對人工智慧的投資必須能配合或不超過對感測器能量的投資。

美國作家布蘭德(Steward Brand)在1984年舉行的駭客大會中，首度提出「資訊渴望自由」的真知灼見，隨後在科技業領袖的一再鼓吹下，這句話幾乎已成為代表人工智慧潛力的神聖口號。惟布蘭德並未提到的是「資訊渴望真實」。

「自由」資訊就是真實資訊的假設，或許能建立如亞馬遜(Amazon)一般成功的行銷巨

人，也能建構出和馬奇諾防線(Maginot Line)一樣成功的軍事人工智慧巨龍。欲實現此目標，美國國防部必須更審慎規劃軍事人工智慧(與感測器)投資，同時在戰略上更對人工智慧在大型體制衝突中的可靠性存疑。

作者簡介

Sam J. Tangredi為美海軍備役上校，擔任羅德島州新港美海軍戰爭學院萊多斯(Leidos)未來戰爭研究首席暨未來戰爭研究院主任。

Reprint from *Proceedings* with permission.

註釋

1. 這段常被重複引述的話已難以確定其來源，故往往被認爲「出自某參謀軍官」。包括美海軍補給系統指揮部近期發表的《後勤語錄》(Logistics Quotations)中亦引用了這段話。見www.au.af.mil/au/awc/awcgate/navy/log_quotes_navsup.pdf。
2. 該詞取自丹恰克(Chris C. Demchak)博士的演說，Grace Hopper Chair of Cyber Conflict at the U.S. Naval War College.
3. Aaron Mehta, "Al Makes Mattis Question 'Fundamental' Belief about War," *Defense News*, 17 February 2018, defensenews.com/intel-geoint/2018/02/17/ai-makes-mattis-question-fundamental-beliefs-about-war/.
4. John Markoff, "Pentagon Turns to Silicon Valley for Edge in Artificial Intelligence," *The New York Times*, 11 May 2016, nytimes.com/2016/05/12/technology/artificial-intelligence-as-the-pentagons-latest-weapon.html.
5. Zigfried Hampel-Arias and John Speed Myers, "What Al Can and Cannot Do for the Intelligence Community," *Defense One*, 5 January 2021, defenseone.com/ideas/2021/01/what-ai-can-and-cannot-do-intelligence-community/171195/.
6. 爲防範外部攻擊，美國國防先進研究計畫局(DARPA)啓動了避免機器學習系統受到「難以察覺擾亂」的計畫，命名爲人工智慧反欺騙健全性保證(Guaranteeing Al Robustness against Deception, GARD)計畫。惟其與反制作戰環境下的大規模欺敵並不相同。見darpa.mil/program/guaranteeing-ai-robustness-against-deception。
7. A major theme of Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington, KY: University Press of Kentucky, 2001).
8. Frank Hersey, "China to-Have 626 Million Surveillance Cameras within 3 Years," *Technode*, 22 November 2017, technode.com/2017/11/22/china-to have-626-million-surveillance-cameras-within-3-years/; Anna Mitchell and Larry Diamond, "China's Surveillance State Should Scare Everyone," *The Atlantic*, 2 February 2018, theatlantic.com/international/archive/2018/02/china-surveillance/552203/.
9. April Glaser, "How Apple and Amazon Are Aiding Chinese Censors," *Slate*, 2 August 2017, slate.com/technology/2017/08/apple-and-amazon-are-helping-china-censor-the-internet.html; Glaser, "Is a Tech Company Ever Neutral?" *Slate*, 11 October 2019, slate.com/technology/2019/10/apple-chinese-government-microsoft-amazon-ice.html.
10. Aaron Ricardela, "Best Way to Realize Al Benefits: Don't Shoot the Moon," *Forbes*, 2 October 2019, forbes.com/sits/oracle/2019/10/02/best-way-to-realize-ai-benefits-dont-shoot-the-moon/. The quote is by Clive Swan.
11. "Whoever Leads in Al Will Rule the World': Putin to Russian Children on Knowledge Day," *RT* [*Russia Today*], 1 September 2017, rt.com/news/401731-ai-rule-world-putin/.
12. CAPT Wayne P. Hughes Jr., USN (Ret.), and RADM Robert Girrier, USN (Ret.), *Fleet Tactics and Naval Operations*, 3rd ed. (Annapolis, MD: Naval Institute Press, 2018), 40-44.