

Chapter

1

導 論

Introduction

未來將由智慧數據驅動。

如今，要忽視人工智慧（AI）領域的這股熱潮確實困難，甚至是不可能的。

當您正在閱讀第一章時，可能已經感覺到內容有些陳舊了——這正顯示該領域發展的速度之快。當我正在打字撰寫本文的同時，Apple 剛剛結束了 2024 年的 Apple 全球開發者大會（WWDC），在這場活動中，他們以「Apple Intelligence」和 Siri 全新升級，重返生態系統，正式回應生成式 AI 的熱潮。就在前一個月，OpenAI 發佈了春季更新，推出了最新的 GPT-4o，它已經遠遠超越了該團隊在 2022 年底推出並讓全世界為之瘋狂的 ChatGPT 初版。同時，Google 也在 2024 年 Google I/O 大會上宣布對搜尋功能進行一項根本性的變革，這不僅將改變推動該公司達到今日地位的廣告模式，也將為我們所見所聞和閱讀的內容帶來一個截然不同的未來。關於這部分，將在後續章節進一步說明。

然而，儘管人工智慧近年來被大肆炒作，但人工智慧其實並不是什麼新鮮事。事實上，這個概念早在 1950 年代中期就已經出現。此外，傳統金融機構和成熟的金融科技公司也早已開始運用人工智慧一段時間了。在本書第一章中，我們將帶你回顧人工智慧的發展歷史，以及它是如何融入我們的日常生活中。

❖ 什麼是人工智慧？

「人工智慧」（Artificial Intelligence）這個詞，是由美國科學家約翰·麥卡錫（John McCarthy）於 1955 年首次提出的¹。用最簡單的方式來說，人工智慧是指一系列技術，它能讓機器執行過去必須由人類完成的複雜任務，同時它能夠在極短的時間內處理大量資料，遠比人類手動處理所需的時間更少。

經濟合作暨發展組織（OECD）已更新人工智慧的定義，以反映近期生成式 AI 的發展。最新定義如下：「人工智慧系統是一種以機器為基礎的系統，能夠根據明確或隱含的目標，從接收到的『輸入（input）』中推理出如何產生『輸出（output）』，例如預測、內容、推薦或決策，進而影響實體或虛擬環境。不同的 AI 系統在部署後，具有不同程度的自主性與適應性。」²

人工智慧在我們現代生活中的廣泛應用，正是這項技術價值的最佳體現。從我們早上醒來查看電子郵件或新聞推播的那一刻起，到離開家門，應對交通狀況的過程，AI 都在後台默默的運作，或作為我們的輔助駕駛（co-pilot），與我們並肩而行。隨著科技不斷進步，未來我們很可能會看到更多全新的應用與科技的出現。

這不僅是銀行業的重要時刻，更是整個社會的關鍵時刻。這並非因為我們應該擔心人工智慧超越人類，而是因為過去和現在的挑戰，例如具有偏見的數據和高昂的營運成本，可能會影響技術發展的軌跡、誰將從中受益，以及它是否會使我們的社會更加團結或進一步分化。

❖ 人工智慧簡史

首先，讓我們把時間倒轉回 1942 年。

當時，一位名叫艾薩克·阿西莫夫（Isaac Asimov）的美國作家，在《驚奇科幻雜誌》（Astounding Fiction）上發表了一篇名為「轉圈圈」〈Runaround〉的短篇小說，並首次提出了著名的機器人三大法則³。這些法則旨在讓機器人遵守，以防止對其人類創造者造成傷害。第一法則、機器人不得傷害人類，或袖手旁觀坐視人類受到傷害；第二法則、除非違背第一法則，機器人必須服從人類的命令；第三法則、在不違背第一及第二法則的情況下，機器人必須保護自己的生存。

接著在 1950 年，英國數學家暨電腦科學家艾倫・圖靈（Alan Turing）提出了一個「模仿遊戲」，用來判斷機器是否具備思考能力。這個遊戲，也就是後來廣為人知的圖靈測試（Turing Test），是由一位遠端的人類提問者向一台電腦和一位真人分別提出一系列問題，根據他們的回答，來判斷哪一位是人、哪一位是機器。如果提問者無法準確分辨出誰是人、誰是機器，就表示該機器具備了類似人類的思考或對話能力。

圖靈當時還預測，在接下來的五十年內，電腦將能夠擅長這項模仿遊戲，以至於一般的提問者在問答五分鐘之後，能夠辨識機器與人類的正確率將不會超過 70%。⁴ 不過，我想我們可以合理地說，西元 2000 年早已過去，而我們至今仍未真正看到一台能夠像圖靈當初預測那樣會「思考」的機器。

❖ 人工智慧的黃金時代

在圖靈測試預測之後，隨之而來的是一陣熱情與希望——這段時期被稱為人工智慧的黃金時代。這個時期始於 1956 年，當時約翰・麥卡錫（John McCarthy）在達特茅斯大學的一場夏季會議上首次提出了「人工智慧」這個術語。在此期間取得的一些進展包括：

- ◆ Shakey 機器人——第一個能夠透過感知周圍環境而自主移動的行動機器人。由當時的史丹福研究院（SRI，當時稱為史丹福研究所）於 1966 年至 1972 年間開發。Shakey 的人工智慧生態系統由多個關鍵組件構成，包括電視攝影機和光學測距儀（電腦視覺）、天線無線電連接（通訊系統）、碰撞感測器（導航系統）以及用來推動物體的推桿⁵。它的分層軟體架構是第一次在機器人領域中被使用，並且與其他技術生

態系統結合，這使得 Shakey 成為未來世代具備人工智慧能力機器人的系統模型。

- ◆ SHRDLU——一個用來理解自然語言的程式。由 Terry Winograd 於 1968 年至 1970 年間在麻省理工學院人工智慧實驗室編寫，能夠與使用者進行簡單的對話，並在桌上移動彩色方塊。⁶它最初的成功激發一系列將人工智慧商業化的努力。

事實上，這個領域充滿如此多的期待，以至於麻省理工學院資訊科學與人工智慧實驗室兩位創辦人之一的馬文·閔斯基（Marvin Minsky）在 1970 年預測，在三到八年內就會出現具備一般人類智力的機器。

❖ 第一次人工智慧寒冬

然而，在一連串未能成功將人工智慧應用於現實世界場景所導致的失望之後，現實情況終於浮現。與現今的人工智慧不同，當時能取得的資料非常有限，運算成本高昂，更不用說，當時的運算能力根本不足以創造或解決任何實用的問題。我們將在本書第四章進一步探討其中一些因素，因為成本仍然是人工智慧普及與規模化的最大限制之一，並將影響誰能取得這項技術以及這項技術最終將造福誰。

俗話說：「能做不代表應該做。」一項科技若要被廣泛採用，必須能展現真正的價值並解決實際的問題。

1973 年，劍橋大學的教授詹姆斯·萊特希爾爵士（Professor Sir James Lighthill）指出，「通用機器人是一個海市蜃樓」，這標誌著人工智慧冬天正式到來的歷史時刻。⁷

當時認為能在如此短的時間內就實現人類水平的智能，實際上是不切實際的期待。事實上，美國哲學家約翰・希爾（John Searle）在 1980 年發表的論文《心靈、大腦與程式》（Minds, Brains, and Programs）中提出了「中文房間論證」，以此說明人工智慧確實是「人工」的。⁸ 這個論證指出，僅僅因為電腦程式能透過操作中文字符來模擬智慧，並不代表它真正理解這些字符的含義，因為對機器而言，這些字符本身並沒有任何意義。

人們對人工智慧的關注與資金逐漸減緩，第一次人工智慧寒冬正式到來。

❖ 人工智慧的繁榮時期

然而，這波低潮並未持續太久。從 1980 年代開始，企業開始採用專家系統（expert system）——這些程式透過專家知識，並運用一連串「如果……那麼……」的規則，模仿人類專家的決策過程來回答問題或解決問題。由於具有商業價值的潛力，人工智慧再度受到關注，並開始聚焦於知識工程（knowledge engineering）領域。XCON（也稱為 R1）是卡內基美隆大學的約翰・麥克德莫特（John McDermott）為迪吉多公司（DEC）開發基於規則的系統，用以協助 DEC 的 VAX-11/780 系統之訂購，以確保按訂單配置了正確的零組件。約翰在 1980 年的論文中所發表的評論，似乎預示了未來 AI 在商業上的應用前景：「它所產出的配置始終是合適的，而且提供給實際組裝系統技術人員的資訊，比人類所能產生的還要更詳細。」（McDermott, 1980）⁹

另一項重要的發展出現在 1984 年，道格拉斯・雷納特（Douglas Lenat）發起了一個名為 CYC 的專案，他稱之為「本體工程」（ontological engineering）¹⁰。他主張，讓電腦程式擁有常識的唯一方法，就是將所有事實與知識匯入程式中，使其能夠進行處理與閱讀，最終理解人類概念所蘊含的意義。他表示：「可以把這想像成數千萬關於世界運作方式的經驗法則，而這些法則幾乎從未被明確傳達過。不過，除了這些隱含規則之外，常識系統還需要能從這些規則和其他明確陳述中做出正確的推論。」（Lenat, 2020）。¹¹

到了 1980 年代中期，人工智慧又開始出現另一種新興的發展路徑。由澳裔美籍科學家羅德尼・布魯克斯（Rodney Brooks）在麻省理工學院人工智慧實驗室（MIT AI Laboratory）提出的新人工智慧（nouvelle AI），不再依賴事先設定好的規則與邏輯，而是透過感應器和與外界互動進行學習，與傳統人工智慧形成對比。¹²

❖ 第二次人工智慧寒冬

隨著人工智慧熱潮的升溫，外界期待科技所承諾能達成的成果卻最終並未實現。1982 年，日本政府啟動了為期 10 年、總投資達 4 億美元的第五代電腦計畫（FGCP：Fifth Generation Computer Project），旨在資助專家系統並開發具備推理能力的電腦，但該計畫最終在 1992 年宣告結束。¹³ 不幸的是，這項努力並未帶來研究人員所期望的突破，反而證明了這是一個過於雄心勃勃且成本過高的計畫。當時，專家系統需要龐大的資料量才能運作，而儲存空間依然非常昂貴。

商業界對於人工智慧的關注再度減弱，資金也隨之縮減，標誌著第二次人工智慧寒冬短暫來臨。

❖ 人工智慧的現代化時代

1990 年代到 2000 年代初期，科技快速發展，為我們今日所處的世界奠定了基礎。1991 年，英國科學家提姆・伯納斯・李（Tim Berners-Lee）發表了全球第一個網頁（<http://info.cern.ch>）。1993 年，馬克・安德森（Marc Andreessen）推出了 Mosaic，這是第一個圖形化網頁瀏覽器。1992 年，英國軟體架構師尼爾・帕普沃斯（Neil Papworth）從電腦向同事理查・賈維斯（Richard Jarvis）發送了全球第一則簡訊（SMS，short message service），但直到 1999 年，簡訊才能在多個行動網路間相互傳送。¹⁴1995 年，亞馬遜推出線上書店。1998 年，賴瑞・佩奇（Larry Page）和謝爾蓋・布林（Sergey Brin）創辦了 Google，並迅速成為網路上最具主導地位的搜尋引擎。2004 年，Facebook 正式上線。

我們所熟知的資訊交流方式，從此被永遠改變。隨著世界變得越來越互相聯結，電腦的速度與運算能力也不斷提升。透過網路與各種連網裝置所產生的資料爆炸性成長，為模型訓練提供了必要的輸入來源。隨著機器學習相關領域持續取得進展，人工智慧的熱潮也慢慢回歸。

1997 年，IBM 開發的西洋棋程式「深藍」（Deep Blue）擊敗了世界冠軍加里・卡斯帕羅夫（Garry Kasparov），成為史上第一個打敗現任西洋棋世界冠軍的電腦程式。2002 年，掃地機器人 Roomba 誕生。2005 年，自駕車與機器人 STANLEY 贏得了 DARPA 大挑戰賽（DARPA Grand Challenge，譯註：DARPA Grand Challenger 是由美國國防高等研究計畫署（DARPA）於 2004 年首次舉辦的自駕車競賽，旨在推動無人車輛技術的發展）。

歡迎來到現代人工智慧的現代化時代。

❖ 機器學習的崛起

2011 年，IBM 的 Watson 深度問答系統（Watson DeepQA）參加了知名電視益智節目《Jeopardy! 》（危險邊緣），並創下歷史紀錄，擊敗了兩位最具代表性的冠軍——布萊德·魯特（Brad Rutter）和肯·詹寧斯（Ken Jennings）。¹⁵ Watson 以 IBM 創辦人湯瑪斯·華生（Thomas J. Watson Sr.）命名，是一套能理解自然語言問題並直接給出答案的問答系統，代表了語音技術領域的一大突破。隨後，各式各樣的語音助理接連問世並快速進入市場，包括：Siri（2010 年）、Amazon Alexa（2014 年）、Microsoft Cortana（2014 年）、Google Assistant（2016 年）、Alice（2017 年）。

人工智慧開始悄悄走入我們的日常生活，隨時隨地都能看見它的身影。

2014 年，Google 以 4 億英鎊收購了位於英國、專注於深度強化學習（結合深度學習與強化學習技術）的 AI 公司 DeepMind。2015 年，DeepMind 開發的 AlphaGo 擊敗了曾經榮膺三屆歐洲圍棋冠軍樊麾，這項成就震驚了世界。隔年（2016 年），AlphaGo 更擊敗了來自南韓、擁有 18 項世界冠軍頭銜、被譽為十年來最強棋手的李世乭。這場世紀對決吸引了全球超過 2 億觀眾觀看。¹⁶

❖ 人工智慧豐盛的時代

直到近年為止，影像標註（image annotation）通常都仰賴人工完成，是建立機器學習訓練資料的重要步驟。透過學習這些已標註的範例，機器才能對未曾見過的樣本進行預測。然而，處理龐大數據分類的

挑戰十分巨大，整個過程極為耗時且成本高昂，要訓練出能處理多項任務的模型更是困難重重。

此外，這類資料標註作業也引發了倫理爭議，因為它們經常仰賴來自弱勢族群或邊緣社群的低廉勞力。麻省理工學院科技評論（MIT Technology Review）的一個專題報導，將這類剝削性行為稱為「人工智慧殖民主義」（AI Colonialism），引發社會關注。¹⁷

自我監督式學習（Self-Supervised Learning）於 2017 年左右興起，這種全新的學習模式讓模型能夠利用資料的一部分來預測另一部分，省去了過去大量仰賴人工標註的瓶頸。透過大量、多元且未標註的資料進行訓練，人工智慧模型得以更有效率地擴展，並在實際應用中展現更優異的表現。

大量高品質的資料、運算能力強大的硬體，以及先進的演算法，共同構成了推動人工智慧發展的三大支柱。2022 年底，ChatGPT 橫空出世，席捲全球。自此，我們見證了一波又一波的生成式 AI 工具與應用，涵蓋文字、影像與影片的生成，包括：Claude（Anthropic）、Copilot（Microsoft）、Dall-E（OpenAI）、Gemini（Google）、HeyGen、Imagine（Meta）、MidJourney、Sora（OpenAI）、Stable Diffusion DreamStudio 以及眾多其他應用模型。這些僅僅是目前主流的幾個代表性模型而已。這個生態系發展之快速，甚至在我完成本書手稿之前，又將有全新一代功能更強大的工具問世。

支撐這一波生成式 AI 工具的正是基礎模型（Foundation Models），其中包括像 GPT-4 和 LLaMA 這類大型語言模型（LLMs），它們都是透過龐大資料量訓練而成。資料經常被比喻為「新石油」或「氧氣」，而「運算能力」（Compute）也被稱為「新石油」的原因，在於這些模

型的運作極度依賴運算資源，且成本高昂。根據 2024 年人工智慧指數報告（Artificial Intelligence Index Report 2024），OpenAI 訓練 GPT-4 所需的運算成本高達 7,800 萬美元，而 Google 訓練 Gemini Ultra 的成本更高，達到 1 億 9,100 萬美元。

在這場新一輪的科技淘金熱中，創投、科技專家、創業家與大型企業紛紛投入，試圖搶占這個具有顛覆性潛力的科技並佔一席之地，各國政府也正積極投入，力求在這場全球競賽中取得領先地位。雖然過去人工智慧寒冬時期所面臨的資料不足與運算能力不足等挑戰已經不再是問題，但若要真正釋放這項科技的潛力，我們仍需克服諸多困難。除了高昂的模型訓練與再訓練成本外，環境影響也成為日益嚴峻的議題，而且不僅限於碳排放。隨著 AI 發展與應用加速，能源消耗與冷卻用水需求持續攀升，資料中心的擴建需求也隨之增加。例如，加州大學河濱分校電機與電腦工程副教授 Shaolei Ren 的研究指出，Google 的資料中心在 2022 年的用水量相較 2021 年增加了 20%，而 Microsoft 的用水量更成長了 34%。¹⁸ 此外，根據國際能源署（IEA）在《2024 年電力市場報告》中預測，資料中心的總電力消耗將從 2022 年的 460 太瓦時（TWh），到 2026 年超過 1,000TWh，幾乎是日本全國用電量的規模。雖然目前難以精確量化 AI 單獨造成的環境足跡，但這些預測凸顯了尋求更節能解決方案的迫切性。AI 的進步不應以我們唯一的家園「地球」做為代價。

我們將在本書後續章節中進一步探討隱私與資料所有權、倫理與負責任的人工智慧、治理機制，以及社會經濟與環境影響等相關議題（見圖 1.1）。