南一 資訊科技

2-3 人工智慧與未來挑戰

人工智慧是一個正在迅速發展的領域，它讓機器可以像人類一樣學習和做出決策，這也帶來了一些重要的議題。

智慧王

什麼是人工智慧？

人工智慧（Artificial Intelligence，簡稱AI）是由「人工」所創造的「智慧」。而「智慧」這個詞指的是具備一系列特定能力，包括：邏輯思考、抽象思維、預測與規劃、理解複雜概念、現象和語言以及學習和解決問題等。目前我們已經能使機器展現出「類似擁有智慧」的行為，而這些機器只能在執行特定任務時表現出一定程度的智能，因此也稱為「弱人工智慧（Weak AI）」。

T8小教室#1 AI到底是什麼? 人類會被取代嗎?

智慧王

機器學習

最初，科學家為解決電腦面對的問題，創建了許多演算法撰寫程式；後來需要靠許多小程式彼此互相合作，才能完成，這就是AI 最早的雛型。
經由演算法撰寫的程式，通常只能處理固定情境的問題，且無法隨著環境不同採用更適當的策略當引進了人類學習的模式，加上大數據資料的出現，讓人工智慧的發展進入機器也能模仿人類的學習能力，現在一般大眾所說的人工智慧，常指的就是機器學習(Machine Learning)。

【CloudMile 科技情報站 EP.1】AI 是什麼？淺談人工智慧｜ 機器學習 V.S 深度學習

人工智慧的發展歷史

南一資訊科技

1950年代
圖靈測試
Turing Test

運用機器來測試是否具有如人類智慧的概念，是由艾倫． 圖靈(AlanTuring)所提倡的。

1956年代
達特茅斯會議
Dartmouth Workshop

達特茅斯會議被視為人工智慧領域的起源之一，會議的成果包括正式命名，藉由電腦與演算法的進步，從此揭開序幕。

1970年代
專家系統
Expert System

由於電腦硬體的加速發展，處理資料的能力提升，催生了足以處理知識與資料的專家系統，其目標是在模擬人類專家在特定領域中的知識和決策能力。

1990年代
大數據時代
機器學習

隨著網際網路的普及，網路上充滿了可供人工智慧訓練和應用的大數據。這一發展推動了機器學習開始發揮其真正的潛力。

2010年代
深度學習

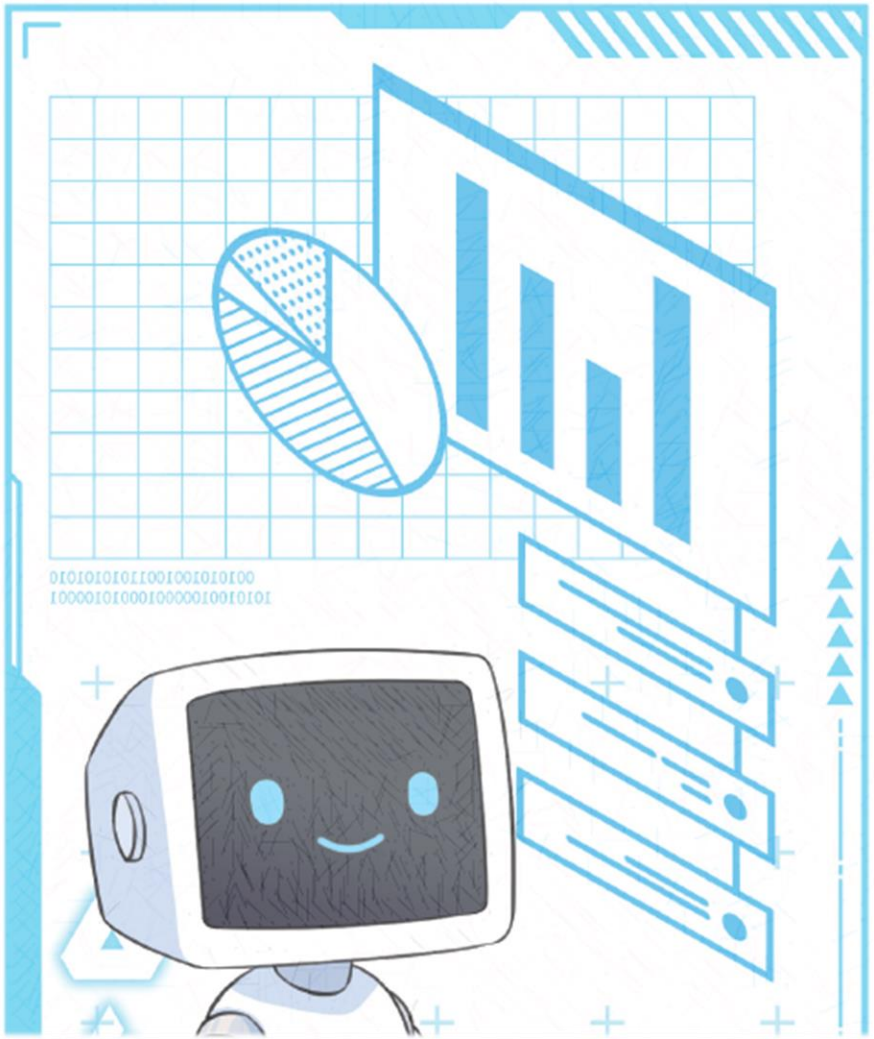
善於處理感知類型資料與學習的深度學習問世，電腦處理視覺與聽覺等相關資料的能力突飛猛進，因而取得了突破進展。

2023-未來
生成式AI

生成式人工智能（Generative AI）領域正在快速的發展，主要特點是可以產生文字、圖像、音樂等，而不僅僅是處理和分析資料。

智慧王

大數據(Big Data)

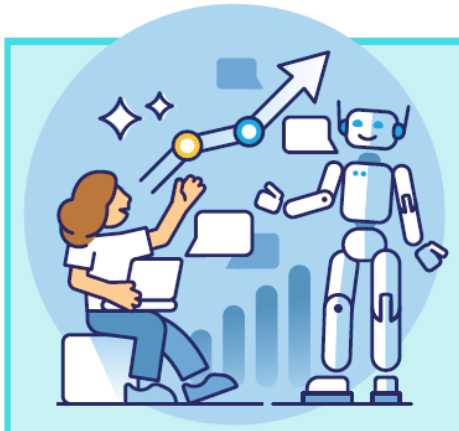
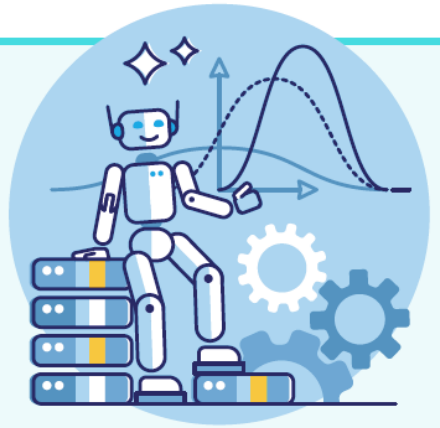
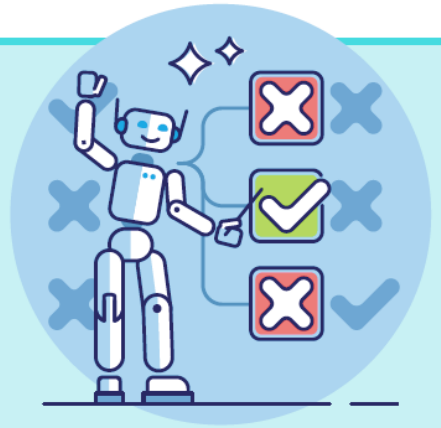
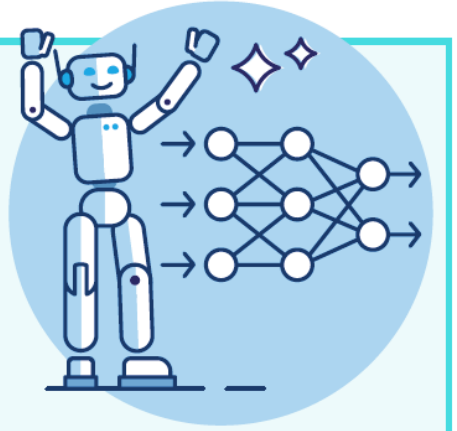


大數據是指規模龐大且多樣化的資料集合，包含了各種來源的資料，這些資料對於機器學習非常重要，因為機器學習演算法需要大量的資料來訓練模型，使得電腦能夠自動從數據中學習模式和規律。

Machine learning methods.

二 機器學習的方式

機器學習的方法主要可分為監督式學習(Supervised Learning)、非監督式學習(Unsupervised Learning)、強化學習(Reinforcement Learning)及深度學習(Deep Learning)，這些機器學習的方法各有其適用的解決問題類型。

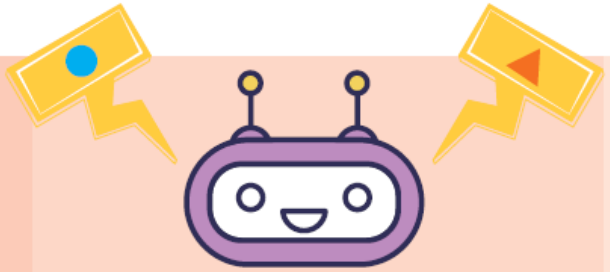
			
監督式學習 Supervised Learning	非監督式學習 Unsupervised Learning	強化學習 Reinforcement Learning	深度學習 Deep Learning
用以解決分類、預測的問題；有標準答案。	用以解決分群的問題；沒有標準答案。	用以解決控制的問題或取得最優解。	用以解決複雜的問題，利用多層次的神經網絡處理和學習資料模仿人類大腦結構。

1 監督式學習

監督式學習的運作方式較直觀，就像是教電腦如何做事情的過程，我們告訴電腦要學習的東西，然後告訴它哪些是對的，哪些是錯的，通過這樣的訓練，電腦可以學會如何正確的做事情。

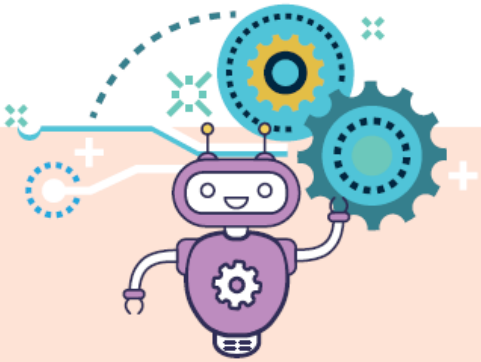
標註 (Label)

如果我們想讓電腦學習分類三角形及圓形，需要先正確標註它們的圖片。



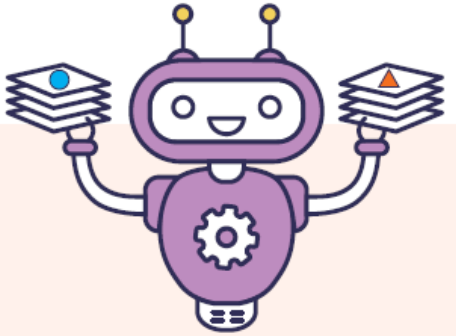
特徵 (Feature)

將圖片輸入到電腦，讓電腦以演算法自行歸納這些輸入資料的特徵。



模型 (Model)

電腦完成設定的訓練回合後會建立模型。

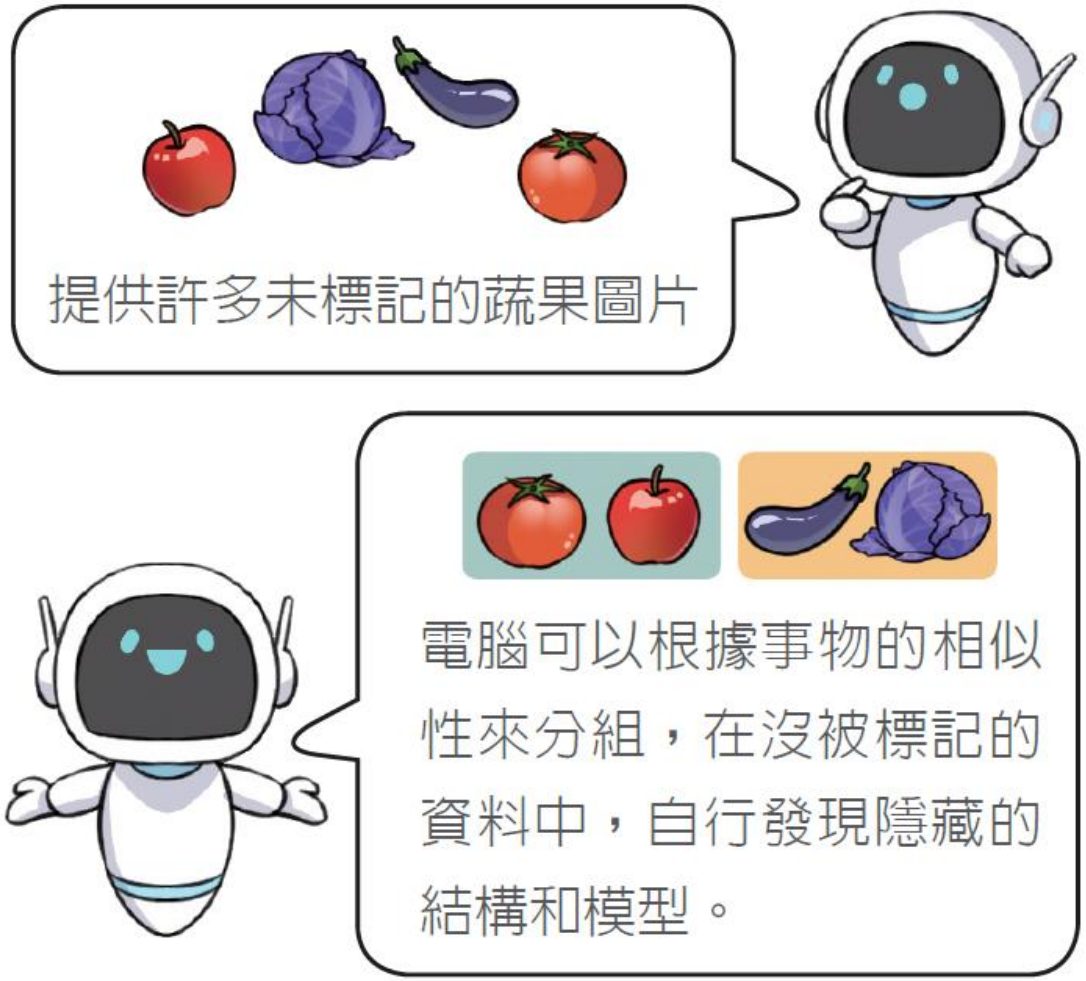


測試 (Test)

若這個模型能通過其它辨識圖形的測試，電腦使用它時，就能擁有識別三角形和圓形圖片的能力。

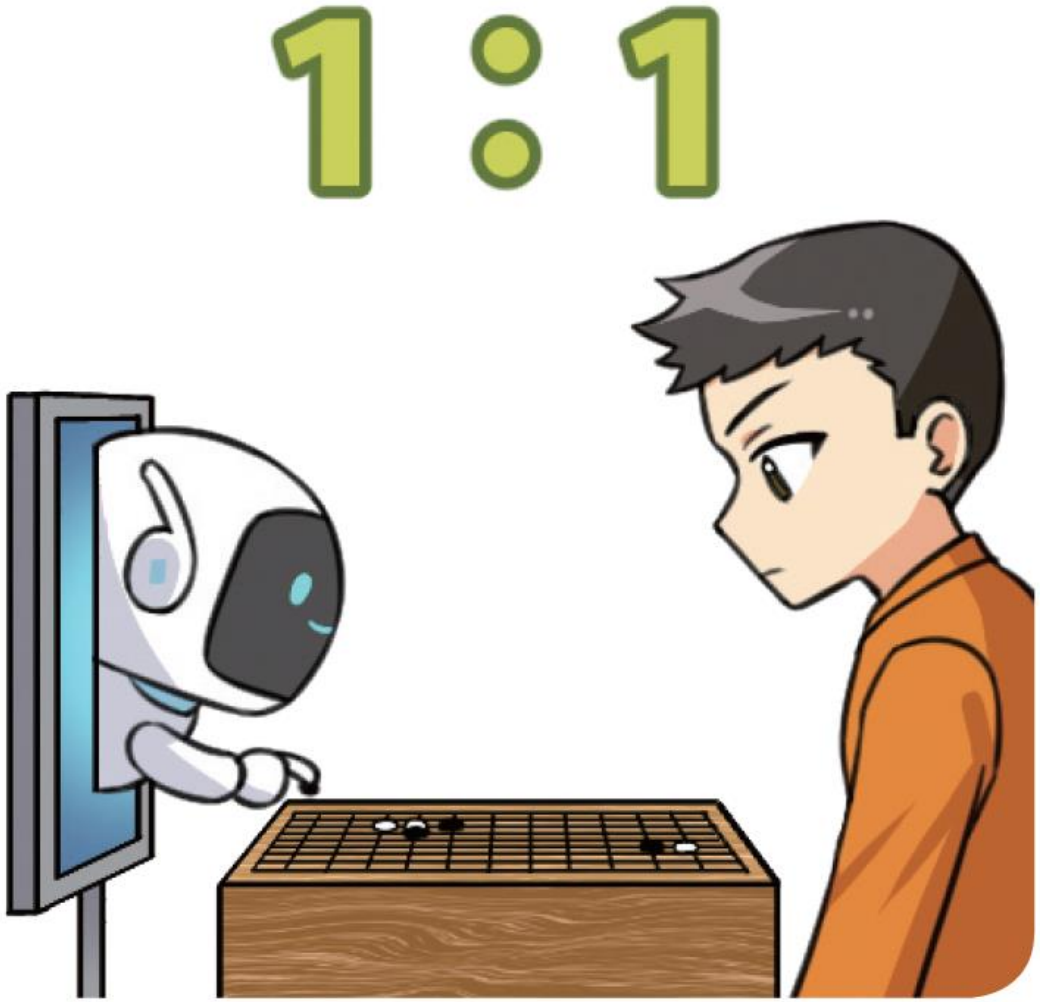
2 非監督式學習

非監督式學習是在沒有標記過的訓練資料中，電腦能自動對資料進行分類或分群。一般在處理問題時，並不容易取得具完整標記的資料，當不知如何分類資料，或是需要電腦從資料中自行尋找相同的模型時，非監督式學習將可以提供很大的幫助。



3 強化學習

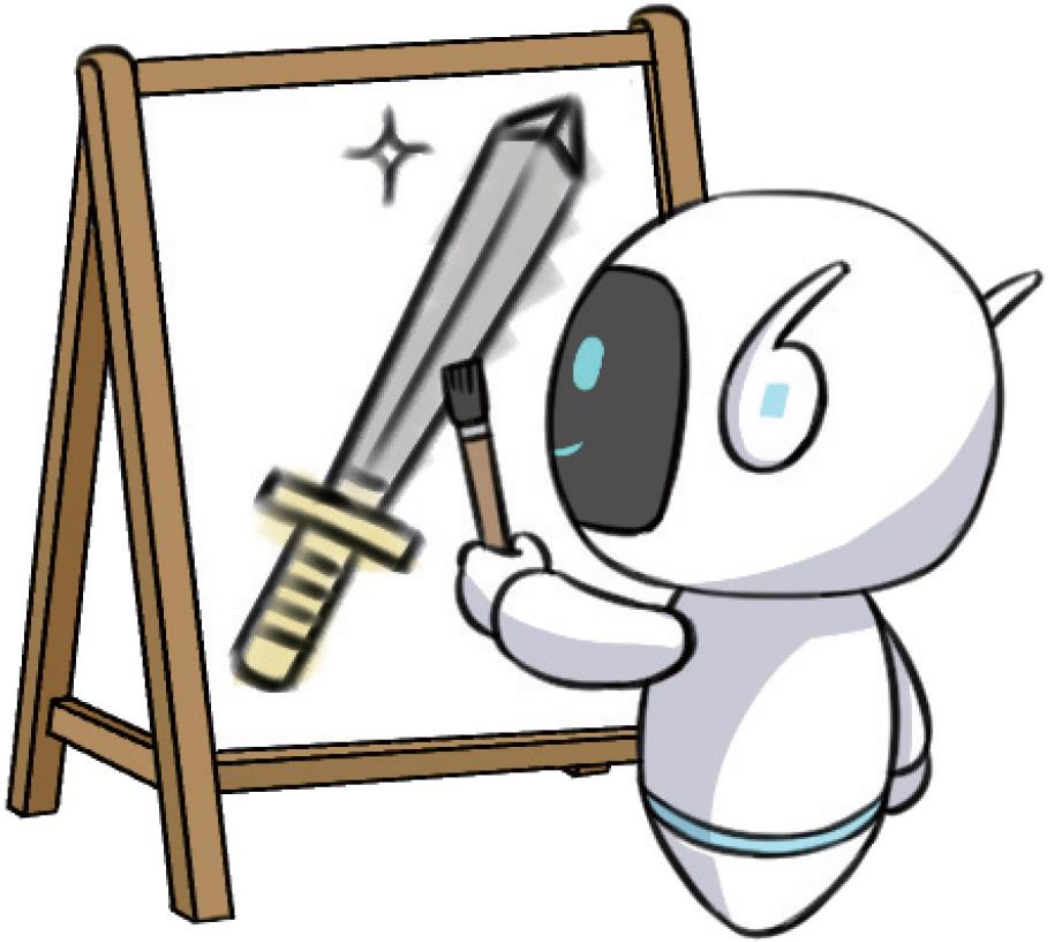
強化式學習是電腦自動依據每次行為結果再重複學習的方法。它可以訓練電腦做出決策，以實現最佳結果。強化式學習源自心理學行為學派的學習觀點，認為學習是刺激與環境互動的結果，完成目標的動作會得到增強，偏離目標的動作則被忽略。這種嘗試錯誤的學習方法，能使電腦在沒有人為干預、沒有明確指令下，就能夠做出一系列的決策。



強化式學習經常被應用在下棋或遊戲。

4 深度學習

深度學習是一種以類神經網路為架構的演算法，可指導電腦以類似人腦學習的方式來處理資料。深度學習中的形容詞「深度」是指使用多層類神經網路。在傳統的機器學習中，資料特徵通常是由人為標記產生出來的，需要經過專家對資料進行許多的分析及研究，才能產生出有用、效果良好的特徵。深度學習則具有自動抽取特徵的能力。



生成式AI 就是深度學習的一種。

AI that protect ocean.

二 保護海洋的AI

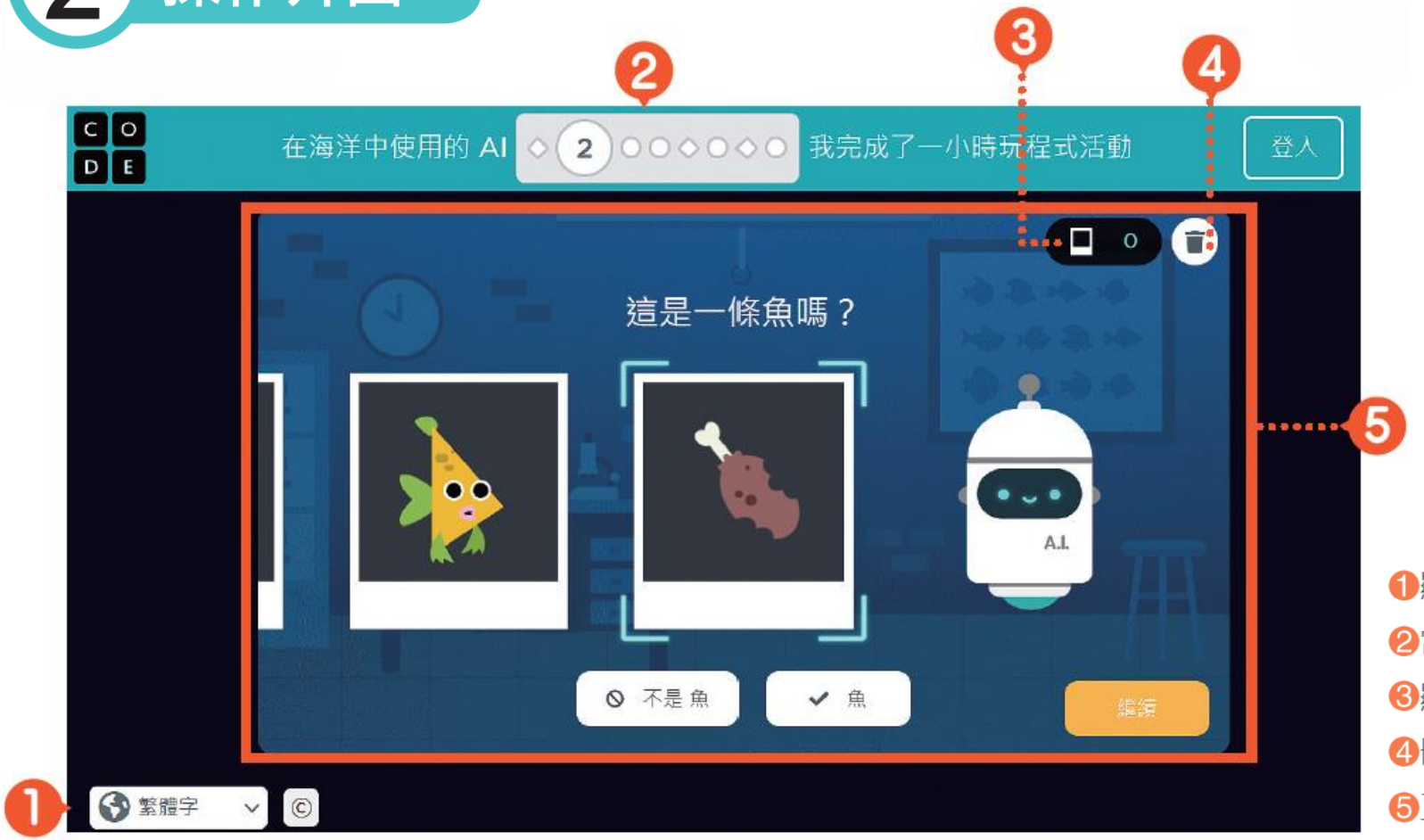
全球每年約有數億磅的垃圾流入海洋，隨著科技的發展，人類應用AI偵測辨別及清除海洋垃圾的技術越趨成熟，AI 藉由大量的資料學習辨識以及蒐集不同的海洋垃圾，以減輕塑膠垃圾對海洋造成的生態汙染，我們一起來了解機器是如何透過學習，解決海洋垃圾的問題。

南一 資訊科技

1 登入 AI for Oceans

輸入網址：http://video.nani.com.tw/oceangame

2 操作介面



❶顯示語言：預設為英文，可改為「繁體中文」顯示。

❷當前學習進度。

❸顯示目前已訓練的圖片張數。

❹刪除訓練資料：會歸零當前進度已訓練的資料。

❺互動學習主要操作介面。

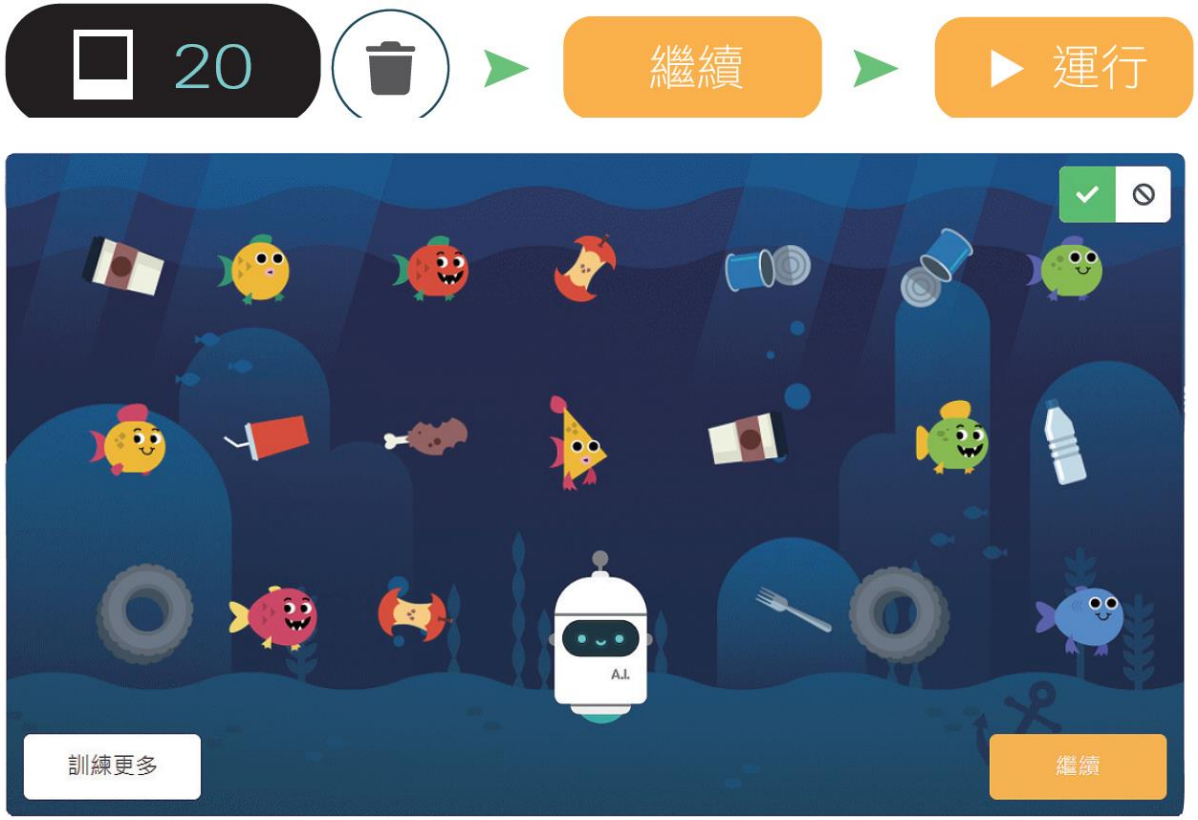
3 訓練 AI

以滑鼠點選【魚】或【不是魚】按鈕，告訴 AI 機器人這張圖片的正確答案，這個動作稱之為標註 (label)，是監督式學習的關鍵動作，目的是讓機器人知道答案，並能從中提取具有辨識度的重要特徵。

AI 會從你的錯誤中學習，如果你做了「錯誤」的選擇，AI 機器人就會跟你犯一樣的錯誤喔！

4 測試 AI

當測試的圖片到達「20」張時，請點選右下角「繼續」，並點選「運行」，運行過程可以看到機器辨識每張圖片的結果，請在機器辨識20 張測試圖片後，點選【繼續】，可得到整體辨識結果，看看AI機器人辨識的結果如何呢？



想一想

當訓練的圖片很少時，會發生什麼事呢？

牛刀小試

表示 AI 辨識為「魚」的圖片。

表示 AI 辨識為「不是魚」的圖片。

(1) 利用 5 張圖片訓練 AI，完成訓練後，使用 20 張圖片測試 AI。

✓ AI 辨識為魚的垃圾有 ___ 張；⊘ AI 辨識為垃圾的魚有 ___ 張。

(2) 利用 10 張圖片訓練 AI，完成訓練後，使用 20 張圖片測試 AI。

✓ AI 辨識為魚的垃圾有 ___ 張；⊘ AI 辨識為垃圾的魚有 ___ 張。

(3) 利用 25 張圖片訓練 AI，完成訓練後，使用 20 張圖片測試 AI。

✓ AI 辨識為魚的垃圾有 ___ 張；⊘ AI 辨識為垃圾的魚有 ___ 張。

(4) 以上 AI 辨識垃圾和魚，發生錯誤次數最低的訓練是第 ____ 次。

(5) 若要提高電腦正確辨識垃圾和魚的成功率，我可以怎麼做？

牛刀小試

在頁面上方可以看到活動的進度，請點選「◇○○ 4 ◇○◇○ (進度 4) 訓練 AI 來清潔海洋」，依據提示完成活動並回答問題。

(1) 分別利用 5 張以及 25 張圖片訓練 AI，並使用 20 張圖片測試 AI。

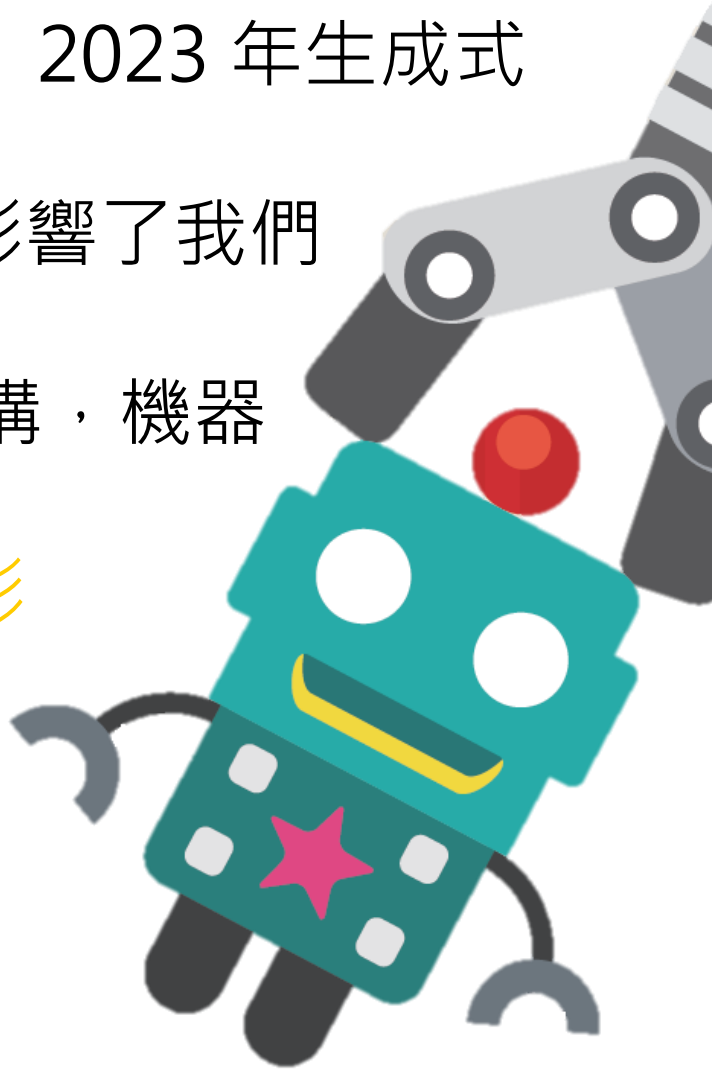
請問哪一個訓練出現辨識海洋生物錯誤的次數最低，為什麼？

(2) 如果「不小心」將其中幾張是海洋生物的圖片點錯了，變成「垃圾」，會發生什麼事？要怎麼做才能更正呢？

Applications of artificial intelligence.

二 人工智慧的應用

人工智慧(AI) 已經成為現代潮流發展的一個關鍵詞， 2023 年生成式AI蓬勃發展，不僅在科技界引起廣泛討論，也深刻影響了我們與世界互動的方式。生成式AI 是基於深度學習的架構，機器透過大量資料的學習，模仿人類感知的能力，關於影像辨識、語音辨識、自然語言處理、圖像生成等應用也跟著不斷推陳出新。



1 影像辨識— Quick, Draw

網址：http://video.nani.com.tw/qdraw

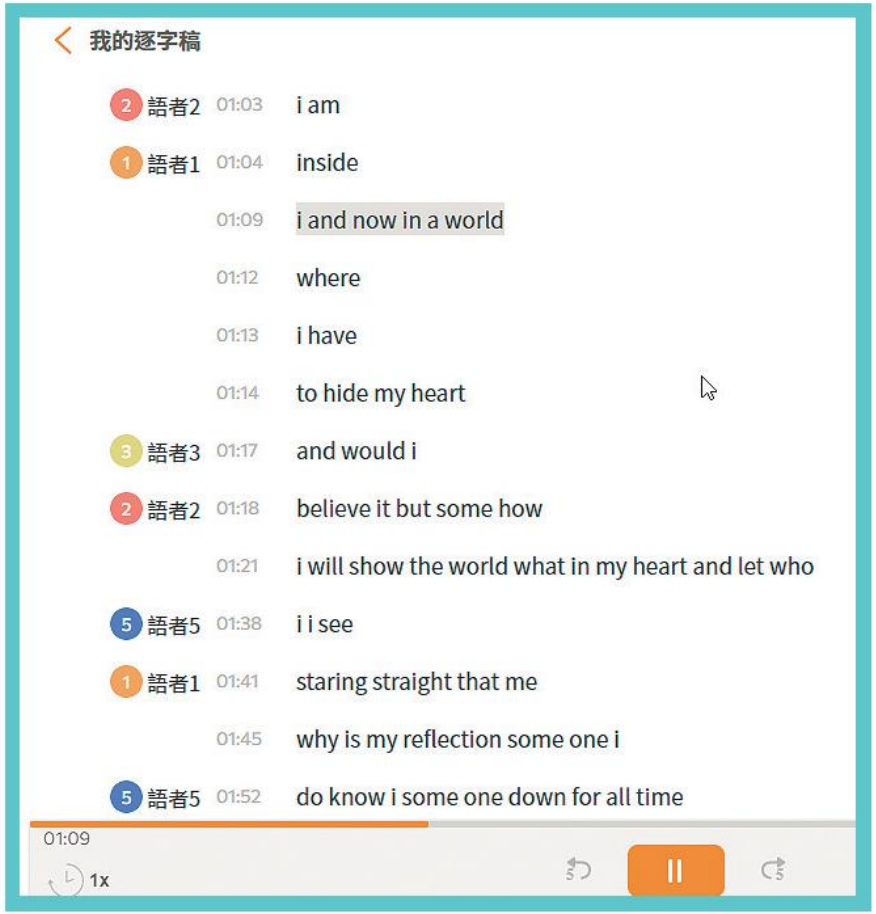
是由Google 開發的遊戲，這款遊戲挑戰你在20秒內繪畫特定物體，而AI 將竭盡全力猜測你所畫的是什麼，在這個遊戲中，影像辨識技術扮演了關鍵角色，當你開始畫一個物體時，你的筆劃將即時被傳送到Google 的伺服器，而AI 通過比對你的筆劃與已知物體的筆劃模式，並參考龐大的數據庫，試圖猜測出你所畫的是什麼物體。

Quick Draw 畫面

2 語音辨識—雅婷逐字稿

網址：http://video.nani.com.tw/yating

是一個嶄新的語音辨識應用，系統通過分析聲音波形、音調和音頻特徵，將語音準確轉錄成文字。這一過程需要使用大量的資料，用以訓練語音辨識模型，從而提高辨識準確性，除了可以使用麥克風語音輸入辨識，也可以上傳影音檔或 Youtube 連結辨識。



雅婷逐字稿畫面

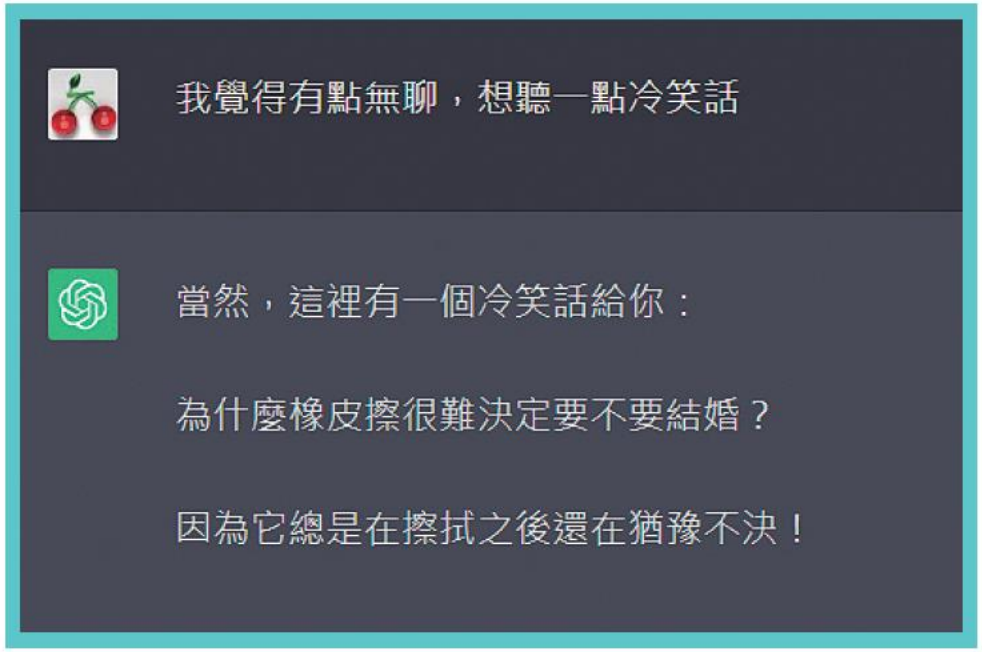
牛刀小試

請動手玩玩看「Quick, Draw ！」以及「雅婷逐字稿」，並說說看你對這兩種技術的印象如何？它們的準確性如何？

3 自然語言處理— ChatGPT

網址：http://video.nani.com.tw/cgpt

是一個以自然語言為基礎的對話模型，它可以理解和生成文字，並被設計用於進行與人類自然而流暢的對話，以回答問題、提供信息，或參與對話交流。



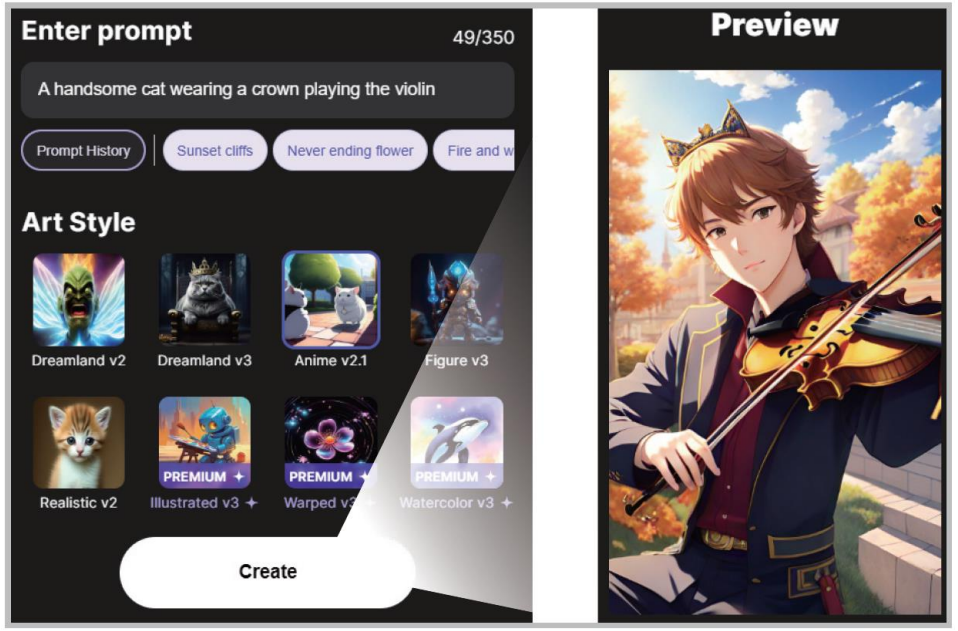
ChatGPT 畫面

自然語言(Natural Language) 是人類日常生活中使用的語言，通常指的是人們用來溝通、表達思想和交流信息的語言。例如：中文、英文。

4 圖像生成— Dream by WOMBO

網址： http://video.nani.com.tw/dai

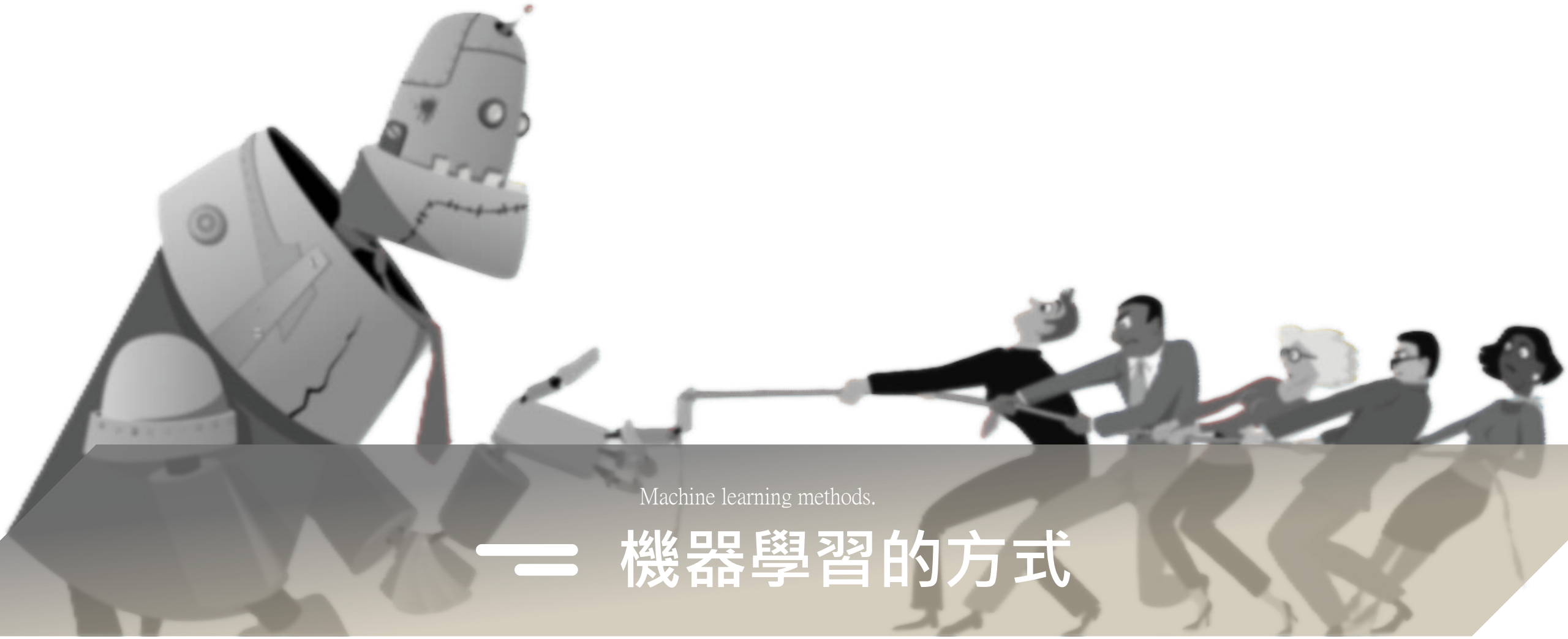
是一個利用AI 生成圖像的工具，可以通過文字描述或概念，選擇圖片風格後，讓AI生成符合描述的藝術圖像。



Dream by WOMBO 畫面

牛刀小試

請動手玩玩看「ChatGPT」以及「Dream by WOMBO」，並說說看你對這兩種技術的印象如何？它們有什麼優缺點？



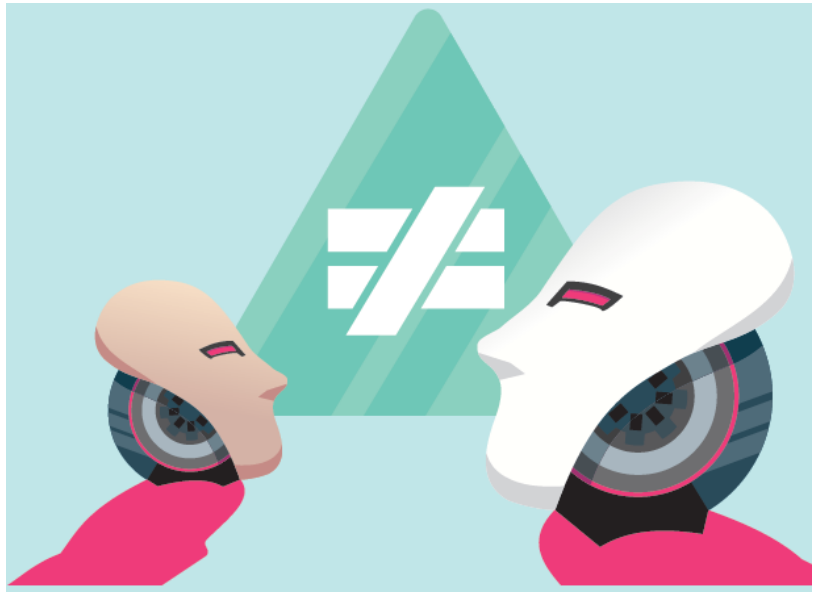
Machine learning methods.

二 機器學習的方式

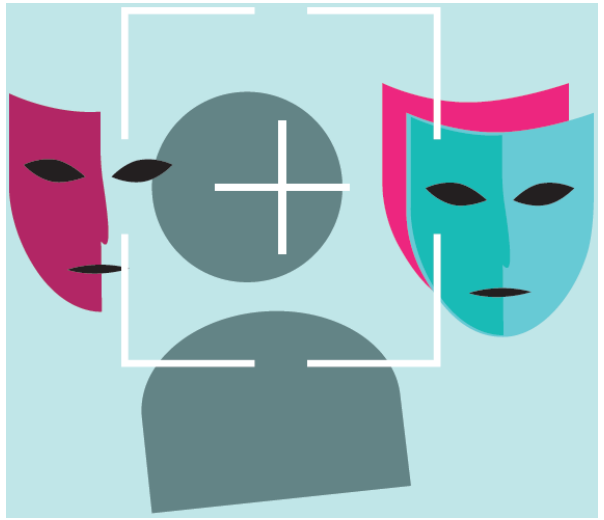
人工智慧可以提高我們工作上的效率，其技術將被廣泛應用於各個領域，例如：家居、交通、醫療、金融、教育等，並推動這些領域的轉型升級。然而AI 提供更多的創新機會和可能性的同時，也引發許多挑戰。

1 偏見

機器學習常會伴隨人類的價值觀，例如：監督式學習中，電腦的訓練受到人類提供的資訊影響，如果標註本身帶有偏見(Bias)，那麼模型也可能學到這些偏見，進而在預測時產生偏見。

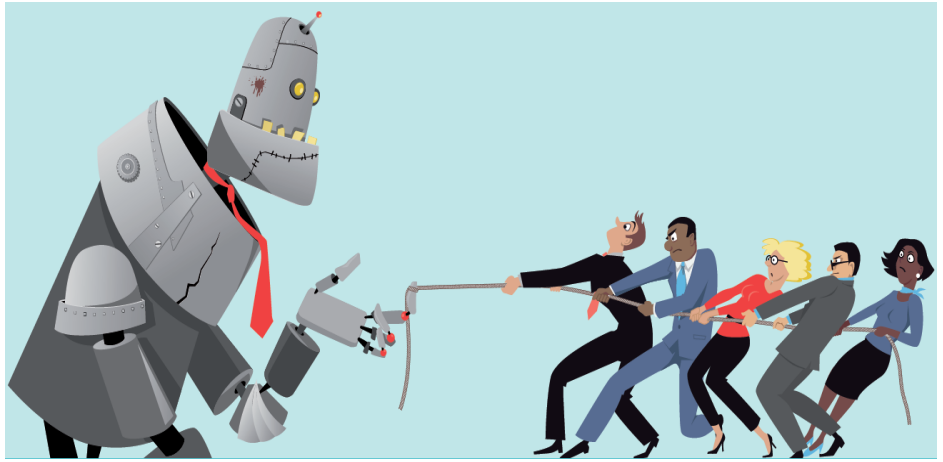


2 濫用



透過人工智慧技術，可以輕鬆地製造虛假的影片或影像，使其看起來極為真實，例如：深偽技術（Deepfake），這可能導致誤導、欺騙和詐騙，並對個人隱私構成潛在威脅。

3 誤判



AI 在做出決策或預測時，可能因為訓練資料不足、訓練過程不完善或演算法的限制等出現判斷錯誤的情況，對個人、組織甚至社會造成影響。

想一想

在自動化和智能化的環境下，如果人工智慧系統被駭客攻擊，可能會對社會造成嚴重的影響。你能想像有哪些潛在的攻擊手法？應該如何加強防禦措施，以降低這些風險？

病毒攻擊AI化!衍生「勒索洗錢產業鏈」 台灣企業成國際駭客肥羊｜十點不一樣20230923 @TVBSNEWS01