

校友作品

洪瑞浩(控制61)：AI風險與預防機制的再思

2023-12-14



近年來人工智慧 (AI) 的發展日新月異，不僅大大增加了人們生活的便利性，一步步提升生產力，促進經濟發展；人類也很有機會能藉由更多的AI創新科技來分析大數據、了解變化趨勢並且提供可靠的預測，協助解決地球氣候變遷和生態崩潰的危機。然而，不受控制的AI發展也可能帶來各種難以控制的威脅和風險，需要我們及早認識並預作防範。

已經發生、正在形成或未來可能出現的AI風險有那些呢？以下舉出幾個大項依序說明：

- 自動化取代人力：功能強大的AI不僅逐漸取代例行性、重複和可預測的勞動工作（生產製造、物流運輸、行政文書等），目前甚至對於需要專業知識的創意工作者（如程式設計、作曲、論文、律師、代書或法律文件的撰寫等）也構成了威脅。這些正大量流失工作機會所造成的大規模結構性失業、更嚴重的貧窮危機和可能引發的社會動亂需要正視並預作防範。
- 資源消耗大對環境不利：AI從晶片、伺服器到數據中心都需要消耗大量的電力和水等資源，發散更多的廢氣和污染物，影響環境。
- 深偽技術的安全威脅：利用AI技術製作偽造錄音、錄影、假訊息、或提供偽造的假證據、製造病毒等來進行破壞、詐欺、煽動顛覆，未來更將層出不窮，令人防不勝防。
- 隱私權保障：政府和企業數位化數據的大量蒐集和儲存（包括金融信用、人臉辨識和網路個資等），由於資安漏洞經常被有心人士駭入濫用、讓一般民眾的隱私權失去保護，可能導致個人或組織的權益受損。
- AI演算法的偏誤：AI演算法可能於學習設計時就針對性別、人種、階級等帶有偏見，也可能邏輯有誤；若使用這些AI程式進行資格分級篩選、信用評估、或績效考核等決策應用，很可能失去透明性和公平性，損害部分弱勢族群的正常權益。
- 不受約束的AI致命武器：無人機、殺手機器人或自駕戰鬥機等AI操控的武器已經逐漸出現於如俄烏戰爭等局部戰場；未來若遭野心國家或恐怖分子，不受武器公約規範而大規模使用，這些更精準並可以大量使用的致命武器，對人類是否會形成類似核武或生化武器、新一波的毀滅性浩劫？
- 不受人類控制的超級AI：未來是否會出現比人類聰明、完全不受控制的超級人工智慧，形成對人類文明和生存的威脅，目前仍然眾說紛紜；但未來發生的可能性，仍然讓許多科學家和有識之士憂心不已。

針對以上的AI風險，個人、企業、政府和國際組織可以採行什麼預防和監管措施呢？綜合專家學者的看法，筆者提出下列的建議：

- 個人：謹慎管理個資，不為小利隨意提供不明機構使用。對充斥網路的訊息必須進行客觀的判斷小心求證，堅持同理心和正直良善的倫理道德信念，不輕信謠言隨波逐流。避免工作被取代，平時培養創新思考和靈活應變的能力，努力提升領導、溝通和自我管理能力。
- 企業：秉持環保愛地球、善盡社會責任和完善的治理信念，積極整合資源並培育AI人才來發展並且控管管險；推動自動化但同時謹慎應運用創新科技來創造新的工作機會；AI設計納入道德倫理規範和公平平等的價值觀；對於AI所提供的資訊不是照單全收、必須輔助進行客觀專業的判斷；完善資安防護以保障客戶的隱私；持續發展更省電產品以減少對環境的不利影響；遵守國際公約，避免涉入致命AI武器的研發製造，減少對人類生命的威脅。
- 政府與國際機構：各國政府必須充分掌握全球AI技術與法規制定的趨勢，持續配合國內發展需求打造有利的發展環境；面對自動化形成的失業潮應盡早建構可以保障全民的社會福利安全網，並且提供失業人士新技能再教育的機會；對深偽技術的濫用、隱私權保護和資安維護必須制定嚴謹的管理規範和法律規定。各國政府和聯合國等國際組織必須通力合作，及時制定AI武器和超級人工智慧的研發、擴散和管制公約，有效約束未來不受控制的AI研發或大規模AI致命武器的使用。

上一篇: 田銘茗(電工78)：連方格循環五四三



NYCU 陽明交大



Facebook

NYCU 陽明交大



官網

NYCU 陽明交大



Instagram



NYCU 陽明交大



twitter

Join DrayTek, Vigor your life

居精品翹楚, 易世界潮流
網通用的精質生



Email: nctu.yosheng.editor@gmail.com
電話: 886-3-5712121#51472
地址: 新竹市大學路1001號浩然圖書館

