moda

出國報告（出國類別：開會）

微軟西雅圖「Power Asia 研討會」參訪交流報告

服務機關：數位發展部數位產業署

姓名、職稱：呂正華署長、林宗漢科長等 2 人

派赴國家/地區：美國/西雅圖

出國期間：中華民國 113 年 2 月 26 日-113 年 3 月 3 日

報告日期：中華民國 113 年 5 月 6 日

摘要

生成式 AI 興起影響產業甚遠，國際研究機構 Gartner 在 2024 年《十大戰略性科技趨勢》指南中預測，隨著 AI 導入的門檻大幅降低，未來 3 年內全球企業採用 AI 技術的比例將由目前不到 5%，急遽攀升至 80%以上。而 IBM 公司日前發表一份市場報告《2023 年全球 AI 科技使用現況》，調查結果顯示即使現今生成式 AI 已成為多數企業唾手可得的科技工具之一，但僅有不到四成(38%)的受訪企業已經建置生成式 AI 應用。探究企業未積極採用生成式 AI 的原因，在於企業擔憂資料隱私未受妥善保護(57%)，與缺乏對生成式 AI 如何收集與使用數據，以及產出結果正確性的信任(42%)。

為了因應 AI 帶來的挑戰，在「智慧國家發展方案」與「臺灣 AI 行動計畫 2.0」的架構之下，數位發展部在 2023 年 12 月成立「AI 產品與系統評測中心（後簡稱為 AI 評測中心）」，旨在建構臺灣的 AI 產品與系統評測方式與規範提供 AI 評測服務，逐步實現可信任的 AI 評測環境。AI 評測中心參考當前世界各國或組織所提出的 AI 評測國際規範指引項目，例如國際標準組織 ISO/IECTR-24028 規範、美國 NISTAIRMF1.0 規範、歐盟 AI Act 等，所提出的 AI 評測國際規範指引項目，研訂 AI 評測規範並建立 AI 評測機制。

有鑒於現在受到最廣泛應用的是大語言模型(LLM)所產出的文字，因此數位發展部所推動的 AI 評測機制首先以語言模型作為主要評測對象，參考現有的國際試驗方法，持續發展臺灣的評測工具與系統並建立語言模型的評測項目。考慮到不同地區的文化背景可能導致對同一句話的不同解讀，因此 AI 的發展不能僅僅由國際大型公司單方面決定，而應該透過微調來適應各地區的文化背景，以更符合當地的實際需求。數位發展部也將積極蒐集社會期待，轉化為 AI 評測指引，並歡迎像 Meta、微軟、Google 等國際大型公司接受評測，共同朝向可信任且安全的 AI 發展。

本次參加「Power Asia」研討會，藉此與人工智慧開發、應用與安全等專家進行意見交流，探討科技創新、深入探討可信任 AI、AI 的安全、信任的全球發展政策，以作為制訂我國 AI 數位產業政策之參考。

綜上，此行藉由與微軟研究單位、創新團隊及其他亞洲國家政策制定成員彼此分享 AI 政策，有助我國與微軟建立長期交流平臺與合作機制，並期以此推動經驗，為台美雙邊產業開創更多機會。

目　　錄

壹、 出國目的

一、 背景說明

2020 年微軟宣布將設立全台首座、全球第 66 座 Azure 資料中心區域，以前瞻技術力助加速推動臺灣各產業數位轉型與創新。微軟在 Power Asia 的發展佈局引人矚目，根據 IDC 的研究，預期到了 2024 年微軟生態系（包括微軟本身、微軟產業夥伴與客戶）將於臺灣、馬來西亞、印度三大區域共創造 210 億美元以上的經濟價值，並提供 100,000 個工作機會，顯示微軟資料中心區域將成為未來數位轉型或創新的發展基石。

此外，微軟 DevDaysAsia2023 也在臺灣登場以「AI 聚能轉新局，生成造浪創未來」，與臺灣碩軟、伊雲谷、光禾感知、安然科技、亞博福爾摩沙、深義分析、愛酷智能、新芽網路、達易智造、奧榮科技、碩網資訊、精誠軟體、遠傳電信、選優科技等合作夥伴一同展示橫跨 AI、雲端及商用程式領域的解決方案，讓與會者一窺在地的創新潛能見證新興智慧應用遍地開花。

Microsoft Power Platform 作為低程式碼平台，也在推動應用開發的未來，根據 Gartner 的研究，到了 2026 年有 75%的新應用程式，可能將由低程式碼工具開發。微軟的 Power Platform 提供全面的低程式碼解決方案，改變了開發人員的工作方式，並提高了生產力，使每個人都能夠以遠超預期的速度快速建構解決方案。現在開發人員可以透過 Power Platform 創造自訂應用程式，實現流程自動化，並管理整個組織的資訊。

生成式人工智慧（Generative AI）技術正以超乎想像的速度改變我們的日常生活和企業營運；Bloomberg Intelligence 更預測生成式 AI 的市場規模將從 2022 年的 400 億美元增長到 2032 年的 1.3 兆美元；臺灣也不例外，企業紛紛投資以掌握先機；臺灣微軟總經理卞志祥表示：「在雲端服務、生成式 AI 等技術的挹注下，將推動臺灣產業的黃金十年變革；在這個關鍵時刻，微軟除了推出相應產品，更積極攜手產業夥伴，助企業以破壞式創新引領未來變革。

微軟不斷推動人工智慧（AI）發展，並在全球進行重大投資，包括以生成式 AI 技術協助企業加速轉型，提高生產力，並創造更智慧的應用，推出「微軟產業 AI 化圖鑑」，涵蓋了超過 60 種不同產業和應用領域的 AI 解決方案，這

些解決方案旨在協助企業提升效率、強化安全性，推動產業升級，並以 AI 強化網路防禦能力，保護客戶數位安全，宣布「安全未來倡議」。

值此重要時機，生成式 AI 將對各行各業帶來巨大影響，政府與產業界一同努力，以 AI 應用服務推動產業升級與變革。透過參與微軟主辦之「Power Asia」會議，瞭解微軟合作夥伴生態系統，並倡議數位發展部數位產業署在 AI 推動的成果，藉以連結亞洲相關重要國家進行交流討論。透過臺灣在資通訊領域上的優勢，說明如何以政策帶動產業發展，除進行生成式 AI 應用及發展規劃、亦發展適用於我國的 AI 產品與系統評測機制參考國際標準，以制定我國 AI 評測機制及數位產業推動方向；其中微軟於 AI 系統及服務之安全性、可靠性、資料隱私性、資安等議題之技術與開發現況，可提供制定參考及邀請參與評測，擴展國際交流合作。

二、 出訪目的

為推動數位發展部數位產業署 AI 評測計畫參考國際標準，以制定我國 AI 評測機制及數位產業推動方向，其中微軟於 AI 系統及服務之安全性、可靠性、資料隱私性、資安等議題之技術與開發現況，可提供制定參考。本次出訪主要參與微軟「Power Asia 會議」，倡議及交流我國在 AI 產業發展政策及 AI 評測推動規劃，與微軟研發、創新團隊及其他亞洲國家政策制定成員彼此分享 AI 政策，並與微軟交流相關合作議題。

(一)參加 Power Asia 研討會議題交流

1.探討科技創新：由微軟研發和創新團隊分享 Open AI 合作夥伴關係、探討 AI 未來、可信任及創新的經驗。

2.引領人工智慧未來：深入探討可信任 AI、AI 的安全、可信任的全球發展政策，並制定我國 AI 數位產業政策。

3.人工智慧合作夥伴關係：與其他亞洲國家政策制定成員彼此分享 AI 政策，並與微軟交流相關合作議題。

(二)參訪「cloud collaboration center」

全面了解 Azure 的內部流程和客戶體驗，瞭解微軟全球工程團隊協作技術，實現 Azure 雲中創新的理想，對於國內產業推動與後續與微軟合作擴散，具有其實質的重要意義。

貳、 出訪行程

本次出國時間從 113 年 2 月 26 日至 113 年 3 月 3 日，共計 7 日（詳如下表）。

表 1、本次出國出訪行程

日期	時段	行程
2/26(一)	晚上	啟程臺北(桃園)臺灣時間 **2/26(一)下午 23:40**→西雅圖(塔可瑪)**美西時間 2/26(一)下午 18:10**
2/27(二)	上午	參加 Power ASIA 研討會議題 • Welcome and introduction to ORA • Responsible AI and Public Policy–a global perspective • Advancing sustainability with AI
	下午	參加 Power ASIA 研討會議題 • Security in AI • What's next in AI • AI adoption across global Public Sector • Global perspectives on AI and Policy and Procurement
	晚上	研討會晚宴
2/28(三)	上午	參加 Power ASIA 研討會議題 • Welcome and recap • The importance of standards: Microsoft's contributions to the development of Standards • The Large Language Model Landscape for Governments
	下午	參加 Power ASIA 研討會議題 • The Future of Work • Technology for Fundamental Rights: how AI can contribute to bridging the digital divide, and improve opportunities
	晚上	研討會晚宴
2/29(四)	上午	參加 Power ASIA 研討會 • Round table Discussion
	下午	Tour of Microsoft Cloud Collaboration Centre
3/1(五)	上午	AI 的產業垂直應用案例分享 • Partner Ecosystem enablement from MSFT • AI future in MS
3/2(六)-3/3(日)	上午	返程西雅圖(塔可瑪)美西時間 3/2(六)上午 00:10→臺北(桃園)台北時間 3/3(日)上午 05:20

參、 訪團成員

一、數位發展部數位產業署

NO	姓名	單位	職稱
1	呂正華	數位發展部數位產業署	署長
2	林宗漢	數位發展部數位產業署	科長

肆、 行程紀要

一、 2 月 26 日行程

台北搭機飛往美國西雅圖

二、 2 月 27 日行程

(一) 參與 Power ASIA 研討會

時　　間：2024 年 2 月 27 日（二）上午 9 時 15 分~下午 17 時 30 分

出席代表：數位發展部數位產業署呂正華署長、林宗漢科長

微軟亞洲區銷售與策略副總 Mark Leigh 及以微軟研發、技術與管理人員、以及各國出席人員（詳附件三）

表 2、2 月 27 日 PowerAsia 研討會議程

時間	議程
10:00-10:45	歡迎並介紹 ORA Lee Hickin，亞洲人工智慧技術與政策主管
10:45-11:30	“負責任的人工智慧和公共政策——全球視角” Owen Larter，負責任人工智慧辦公室公共政策總監
11:45-12:30	利用人工智慧促進永續發展
14:00-14:45	人工智慧的安全性
14:45-15:30	人工智慧的下一步是什麼？
15:45-16:30	全球公共部門所採用的人工智慧
16:30-17:00	人工智慧、政策和採購的全球視角
17:00~	每日總結

活動紀要：

1. **介紹微軟 ORA 部門事務與人工智慧倡議原則(Welcome and introduction to ORA)**

由微軟人工智慧技術與政策負責人 Lee Hickin 主持，針對 Microsoft 負責任的 AI 方法以及如何將其應用於公共部門挑戰，進行討論，透過民意調查以評估參與者的觀點和生成式人工智慧及其使用的經驗案例、挑戰與治理。Microsoft Office 概述負責任的人工智慧，其原則標準以及確保人工智慧的措施，值得在信賴的環境中以道德方式開發和部署。本活動與來自亞洲各地的政府領袖學習及簡要討論機會和人工智慧在政治、經濟、科技和社會方面議題。

2. 全球觀點- 負責任人工智慧與公共政策(Responsible AI and Public Policy – a global perspective):

由微軟負責任的人工智慧辦公室 Owen，說明 AI 機會和人工智慧的風險以及微軟的開發方式之人工智慧計畫，透過微軟人工智慧的案例，提高生產力、科學研究和自然語言介面，並說明面對 AI 挑戰如何確保人工智慧安全、可靠、公平對社會有益。

他解釋了一些用來審查和監控的內部政策及 AI 敏感使用的一些政策和流程，例如負責任的 AI 標準、隱私安全和負責任生態系統。

Microsoft 的負責任 AI 標準是指導我們如何構建 AI 系統的框架，以協助我們邁向發展更好、更值得信賴的 AI 之重要一步。Microsoft 公開分享了最新的負責任 AI 標準，及 Microsoft 所學到的知識，並邀請其他人圍繞 AI 主題，建立更好的規範和目標反饋。此標準提供具體可行的指導，超越了迄今主導 AI 領域的最高原則，並為開發 AI 系統的團隊，提供了具體的目標或結果，這些目標有助於將廣泛的原則（例如"負責任"）分解為其關鍵的實現方式，例如影響評估、數據治理和人工監督。每一個目標透過分組要求組成，這些要求是團隊必須採取的步驟，以確保 AI 系統在整個生命周期內實現目標。最後，該標準將可用的工具和實踐方法對應到具體的要求，以便實施該標準的 Microsoft 團隊可以獲得幫助。

因為 AI 越來越多地成為我們生活的一部分，但我們的法律尚未跟上，它們尚未適應 AI 的獨特風險或社會需求。因此，我們相信致力從設計上就具有負責任性，以確保 AI 系統穩定相對重要，所以這種實用指南的需求會越來越大，因此，需要不斷完善我們的政策，並從產品經驗中吸取教訓。

3. 運用人工智慧達到先進永續目標(Advancing sustainability with AI):

此議題由微軟首席永續長 Melanie Nakagawa 進行分享，有鑒於地球危機的緊迫性，所以 AI 在實現零碳排放、氣候適應性和對自然

的積極影響方面扮演著至關重要的角色。面對暖化及極端天氣之氣候變化的影響，需要前所未有的行動，Microsoft 認為企業要繁榮，世界也必須繁榮，而 AI 是實現這一目標的重要工具。

Melanie Nakagawa 分享了一些人工智慧氣候解決方案的案例變化包括水、廢棄物和生態系統，透過 AI 測量、預測和複雜系統優化，進行預測，例如用 AI 以比人類快 10,000 倍地速度，繪製大型南極冰山，幫助我們了解融水流入海洋的情況。

AI 亦可繪製及預測森林砍伐的影響，測量森林的砍伐速率和碳儲存，它有助於產出低碳材料、可再生能源和氣候適應性之作物，而且 AI 能為從業人員提供分析能力，以有效管理複雜系統。

Microsoft 的目標是在 2030 年實現碳負值，並在 2050 年之前消除歷史性的碳排放，該公司與合作夥伴合作投資於 AI 可持續性的解決方案，並參與政策制定，透過《加速可持續性的 AI 指南》概述了解鎖 AI 在實現未來綠色產業方面的潛力與可行步驟。

4. 人工智慧之資訊安全(Security in AI):

本場主題是人工智慧和網路安全，分為四個主要主題，主持人 Herain Oberoi 為微軟數據和人工智慧安全、治理、合規和政策總經理，面對當前資訊安全的挑戰與趨勢，主持人分享關於數據網路犯罪規模和影響的統計內容。另討論包括：

- **國家級攻擊增加**：資訊安全面臨越來越多高度複雜的對手，針對國家發起針對關鍵基礎設施、組織和政府的攻擊。
- **攻擊者使用 AI**：攻擊者利用人工智慧增強其攻擊能力，因其適應性和自動化而具有獨特的挑戰以 AI 驅動的攻擊。
- **勒索軟體攻擊上升**：勒索軟體攻擊持續增加，進而影響企業、機構和個人，這些攻擊利用漏洞，並要求贖金以解密數據。

- **技術人才短缺**：資訊安全專業人員的短缺仍然是一個迫切的問題，組織難以找到和保留能夠有效防禦網路威脅的專家。
- **安全工具的複雜性**：不斷變化的威脅形勢需要複雜的安全工具。然而，管理和整合這些工具可能很複雜且耗費資源。
- **網路犯罪的規模和影響**：網路犯罪對全球經濟造成巨大損失，2022 年損失為 8.44 兆美元，預計到 2027 年網路犯罪的全球成本將達到 23.84 兆美元。

面對上述的問題，微軟在網路安全投資中，其中包括四個領域：威脅情報、綜合安全、人工智慧防禦和安全工具並治理人工智慧。以安全策略為例，透過微軟使用自己的雲端、端點和物聯網地圖來收集和分析威脅訊號，並與合作夥伴和執行部門合作，以打擊網路威脅。而在防禦的角色上，Microsoft Security Copilot 是一款利用生成式 AI 幫助安全分析師更快、更準確地調查和應對事件的產品。同時，Microsoft 正在開發工具和框架，以幫助客戶確保和管理組織中 AI 的使用。

5. 人工智慧大未來(What's next in AI):

這是關於大語言模型的人工智慧革命及其用途公共部門的創新和復原力。主要發言人是 John Maeda，他是微軟創意技術專家。

他解釋了兩種類型的 AI 模型之間的區別：完成模型和嵌入模型，以及它們如何共同創造類似聊天的互動、函數調用和數據分析。他還展示了他自己的項目 Apple Vision Pro 的項目，該項目使用手勢和語音與 AI 進行連接，也討論了 AI 的風險和機遇，並分享了一些人口下降、數位轉型和可參與等不同情境的實例應用。他還回答了觀眾關於他的背景、工作以及 AI 和元宇宙的看法與問題。

6. 運用人工智慧進行全球公共部門跨領域合作(AI adoption across global Public Sector):

這主題討論全球公共部門採用人工智慧議題，由微軟公共部門負責人 Angie 分享她與亞太地區政府客戶合作內涵，以及他們如何使用人工智慧改善公民服務，賦權勞動力，創造可持續營運以及保護資料的經驗和見解。

她舉了一些人工智慧成功的案例，例如台灣學校的聊天機器人，澳洲政府以生成式 AI 副駕駛員將重複任務自動化等。討論政府技能培訓的機會，人工智慧的勞動力，以及微軟的研究、數據和認證的貢獻。另外她強調了重新思考人工智慧採購的重要性以及如何在靈活性、成本效益分析、競爭和法規之間取得平衡至關重要。會場回答了一些問題參與者了解採購流程、數位轉型之旅、人工智慧和合作夥伴生態系統的監管等相關問題。

7. 全球觀點-人工智慧、政策與採購(Global perspectives on AI and Policy and Procurement):

針對政府採用雲端和人工智慧服務的採購挑戰和機會，由微軟副主席 Antony Cook、微軟總法律顧問暨亞洲公共部門商業法律主管 Rose Lee 共同主持。

分享有效使用人工智慧達到雲端的先決條件，但需要解決數據分類、數據治理、數據遷移和基於消耗模型的問題，政府需要在人工智慧政策和採購中平衡創新和風險管理，並在不同地區和國家進行最佳實踐和趨勢學習，政府可以使用沙盒、框架協議和雲端優先政策，以在其採購流程中創造更大的靈活性和實驗性。

如澳洲和新加坡的使用集中式框架協議，實現更快、更靈活跨不同領域的雲端和人工智慧服務政府機構的採購，將人工智慧的案例和優勢，加強於公民服務、教育、醫療保健和公共部門生產力上。

另外來自不同國家的解決方案，包括：瑞典使用人工智慧覆蓋各種政府服務單一平台，允許公民使用及互動，同時確保隱私及其資料的安全性。印度使用行動應用程序，提供資訊和服務偏遠地區和當地農村居民語言，使用人工智慧進行翻譯和檢索相關資料。

人工智慧政策在不同各國採取的方法和原則上，已逐步採用或正在考慮所謂平衡創新和風險管理，例如廣島與 G7 國家和其他受邀者如印尼等國達成一致安全的原則和指南，以可信任的開發與部署人工智慧，先鎖定在高風險和前瞻領域上。英國則使用 NIST 框架，這是一套自願且靈活的標準和工具，使人工智慧系統更具安全性和彈性。

三、 2 月 28 日行程

(一) 參與 Power ASIA 研討會

時間：2024 年 2 月 28 日（三）上午 9 時 15 分到 16:00

出席代表：數位發展部數位產業署呂正華署長、林宗漢科長

微軟亞洲區銷售與策略副總 Mark Leigh 及以微軟研發、技術與管理人員、以及各國出席人員（詳附件三）

表 3、2 月 28 日 Power ASIA 研討會議程

時間	議程
09:15-09:45	歡迎與回顧
09:45-10:30	標準的重要性：微軟對標準的制定
10:30-11:15	政府的大型語言模型簡介
11:35-12:20	透過雲端人工智慧基礎設施解決數位主權問題
12:20-13:50	參觀：數位犯罪部門
13:50-14:35	探討 AI 工作的未來
14:50-15:35	科技促進基本權利：人工智慧如何減少數位落差與改善商機
15:35~	每日總結

活動紀要：

1. 歡迎與回顧(Welcome and Recap):

由微軟人工智慧技術與政策負責人 Lee Hickin 主持，先回顧前一天重點，並簡要介紹了語義核心，這是一個用於協調多個複雜來源上的 AI 任務工具，宣布當天的議程，包括標準、Azure 開放式

AI、M365 協同工作、數據中心基礎設施以及對數位犯罪單位的參觀。討論議題包括：

(1) AI 在採購中的機會與挑戰：

- 機會：AI 可以幫助優化採購流程，提高效率、降低成本、並改善供應鏈管理。例如，AI 可以分析大量數據、預測需求、優化庫存、並自動進行價格報價。
- 挑戰：AI 需要高品質的訓練數據，並且在採購領域中，這可能是一個挑戰。此外，AI 的使用需要合規性和透明度，以確保遵守法規和道德標準。

(2) 監管、競爭、創新和消費者保護：

- 監管：不同國家對 AI 的監管方式不同，例如，歐盟的數位市場法案（DMA）和英國的數位市場、競爭和消費者法案（DMCC）都在規範數位市場。
- 競爭：AI 的應用可能影響市場競爭，所以監管機構需要平衡的促進創新和保護競爭需求。
- 創新：AI 的發展需要鼓勵創新，但同時也需要確保不會對消費者造成損害。
- 消費者保護：AI 應用需要透明度，以確保消費者知道其數據如何被使用，並且有權控制其數據。

(3) 協作和分享：建立與全球思想領袖和 Microsoft 專家的持續互動計畫，可以透過以下方式實現：

- 戰略合作夥伴關係：確保合作夥伴與組織的戰略目標和價值觀保持一致。
- 專業知識：利用合作夥伴的專業知識，共同解決問題並推動創新。
- 協作：建立清晰的溝通渠道，確保協作順暢。

(4) 培訓合作夥伴並充分利用平台的功能：

- 提供培訓和資源，幫助合作夥伴理解 AI 的應用和平台的功能。

- 了解合作夥伴的需求，並根據其技能和興趣進行客製化培訓。
- 鼓勵合作夥伴參與社區和知識共享活動，以便更好地利用 AI 的全部功能。

(5) 對下一代 AI 工具和服務的藍圖和願景：

- 與 John Maeda 進行深入交流，了解他對 AI 工具和服務未來發展的看法。
- 探討如何將這些願景轉化為實際的產品和解決方案。

2. 標準的重要性：微軟在發展標準的貢獻(The importance of standards : Microsoft's contributions to the development to Standards):

這次的會議主題是有關人工智慧標準，以及微軟參與國際標準的過程。主要演講者是 Jason，他負責微軟企業標準組，並擔任與美國國家標準與技術研究所（NIST）的合作關係的執行贊助人。

Jason 解釋了不同類型的標準、AI 標準化的挑戰和機會，以及在全球背景下軟法(soft law)和一致性的角色，此外，他還介紹了 ISOIEC42001 文件，這是第一個針對 AI 管理系統的國際標準，提供了監督和認證可信任 AI 實踐的框架。與會者提出了一些關於共同義務、其他企業對標準的接受以及倫理和工程實踐之間的區別問題。

3. 大語言模型在公共治理的運用(The Large Language Model Landscape for Governments):

這次的會議主題是關於 Azure 平台上的大型語言模型，由 Matt Sinclair 主持，他是 Microsoft Azure AIGTM 策略的負責人。

Matt 解釋了導航和運用大型語言模型的概念，例如如何選擇合適的模型、改進搜索體驗、應用信任和負責任的 AI 標準，以及管理生成式 AI 應用的生命周期。

Matt 在 Azure AI Studio 中展示了幾個案例，他使用不同模型，例如 GPT-4、GPT-3/5、Llama2 和 Mistral，並展示了如何進行基準測試、微調和協調。此外，Matt 還展示了 Azure AI 中的一些新功能和工具，例如助手 API、混合式搜索、內容安全和多模態。

4. 雲端人工智慧基礎建設的數位主權主張(Addressing sovereign data concerns with Cloud AI Infrastructure):

會議主題是人工智慧和雲基礎設施，重點是數位主權和安全，Azure 全球基礎建設總監 Alistair Speirs，他談到了人工智慧在不同企業和產品中的應用和好處，以及它需要支持它的超大規模雲端基礎架構。展示人工智慧如何創造新材料、電池和藥物，以及如何改進精準醫學，並解釋數據保護、合規性和主權的挑戰，以及 Microsoft Azure 提供的不同解決方案。討論數據儲存的不同方法，例如本地、混合和超大規模雲端，以及它們之間的權衡。介紹機密計算的概念，該概念將數據在靜態、傳輸和使用時進行加密，以防止第三方在未經授權下進入。最後，提到 Azure 提供的其他功能和服務，以實現主權控制，例如加密、合規性、透明度和指導。

5. 未來與展望(The Future of Work):

會議討論的是生成式 AI 未來的工作，以及 Microsoft365 的 Copilot，本場由 Matthew Duncan，Microsoft 未來工作倡議的領導者，提出了一些研究結果並展示 Copilot 如何可以幫助提高個人生產力、創意和客製化。參與者也提出了一些問題瞭解 Copilot 如何運作，以及如何與其他人連接數據來源以衡量其影響和收益。

6. 人文科技：人工智慧如何減少數位落差與改善商機(Technology for Fundamental Rights : how AI can contribute to bridging the digital divide, and improve opportunities):

Teresa Hutson 是 Microsoft 的技術與企業責任副總裁,同時也是 Technology for Fundamental Rights 團隊的領導者。她致力於保護全球人民的基本權利,推動包括連接 2.5 億未受服務的人口進行推廣,網路服務不足的人們,直至 2025 年為他們推廣教育、健康和金融包容性的 AI 解決方案。並與其他 19 家公司合作制定了一項技術協議,以打擊選舉中欺騙性 AI 的使用,並推動內容真實性標準、安全架構檢測和公眾意識。展示了一些 AI 工具,使世界對於殘障人士更加無障礙,例如 Be My Eyes、Copilot 和 Seaboard。

四、 2 月 29 日行程

(一)參加 Power ASIA 研討會

會談時間：2024 年 2 月 29 日（四）上午 8 時 45 分

出席代表：數位發展部數位產業署呂正華署長、林宗漢科長

微軟亞洲區銷售與策略副總 Mark Leigh 及以微軟研發、技術與管理人員、以及各國出席人員（詳附件三）

表 4、2 月 29 日 Power ASIA 研討會議程

時間	議程
08:45-10:15	圓桌討論 分享人工智慧方面的學習、挑戰和成功
10:15-12:00	參訪微軟雲端協作中心
12:00-13:30	研討會總結及分享交流

活動紀要：

1. 圓桌會議(Participant Roundtable)

與亞洲國家政策制定成員，透過圓桌討論 AI 政策與挑戰，分述如下：

澳大利亞的AI試點計劃與Copilot：澳大利亞數位轉型局（DTA）的 Chris 分享如何利用現有與 Microsoft 簽訂的採購協議以及經過

IRAP 安全評估使 56 個機構和 7000 名用戶能夠訪問 Copilot，提高生產力並改善工作品質。

日本的 AI 策略與安全研究所：內閣辦公室的 Shinji 提出了他們國家 AI 策略的框架和原則，涵蓋了實施和創新兩大支柱，並建立了日本 AI 安全研究所，以與國際合作夥伴和標準進行合作。

新加坡的挑戰：團隊表示，他們用戶使用中遇到了懷疑和興奮，主要是由於數據安全和能力問題。他們說明了新加坡處理科技事務的不同機構，例如 Gov Tech、MINDEF 和 HTX。解釋了 HTX 面臨的營運和安全挑戰，以及建立資訊化能力的總體計劃。

新加坡的 AI 採用與倫理：國家 AI 團隊的 Wanyi 說明飛輪模型加速了公共部門 AI 採用，其中包括產品創新、組合、意識、素養和治理。她還強調了他們正在使用和開發的內部和商業 AI 產品，以及他們正在制定的 AI 倫理和治理框架。

泰國的 AI 路線圖和挑戰：數位經濟部的 Wisit 分享了泰國科技採用和數位轉型的現狀，以及他們國家 AI 策略的願景和框架，該策略聚焦於數位化、基礎設施、勞動力、治理、監管、研究和開發。他還提到了他們面臨的一些障礙和機遇，例如採購、數據、安全和使用案例。

菲律賓的 AI 策略與要務：來自貿易和工業部的 Fita 說明了菲律賓在製造和農業等領域的 AI 項目和挑戰。她還分享了他們國家 AI 策略路線圖的詳細內容，該策略包括兩大支柱（實施和創新）、4 個維度、7 個要務和 42 項任務。她還討論了一些正在進行中的活動和倡議，例如建立 AI 工作小組、建立 AI 研究中心以及制定 AI 倫理和治理框架。

臺灣的 AI 發展與 AI 評測：數位發展部數位產業署於會議上分享了臺灣促進 AI 產業化、創新和可信任性的願景、策略和倡議，並介紹了 AI 產品及系統評測中心及其標準和技術。與會者亦提出了有

關臺灣與國際 AI 標準（如 ISO 和 NIST）的一致性，以及評估多模型的時間表及相關問題交流。

印尼的 AI 治理與合作：印尼的代表分享了他們的 AI 治理法律和倫理框架，以及他們對向其他國家學習並與不同利益相關者在 AI 發展和監管方面合作的興趣。

後續活動和學習圈：主辦方感謝與會者的演講和討論，並提出了一些可能的工作坊、評估和技能培訓活動，以幫助他們推動 AI 策略。他們還建議透過學習圈和分享鏈結此團體的互動。

2. 參觀微軟雲端協作中心(Cloud Collaboration Center):

西雅圖的 Azure Cloud Collaboration Center(CCC)是一個位於微軟紅蒙德總部的先進設施，專為加強 Azure 雲端平台的性能和安全性而設計。以下是 CCC 的一些特點：

- 即時狀態顯示:CCC 設有一個壯觀的 1,600 平方英尺的電視牆，顯示 Azure 的即時狀態，包括內部流程、網路基礎設施和客戶服務的健康狀況，工程師可以一目瞭然地分辨潛在問題，並在問題發生時迅速進行處理。
- 協作空間:CCC 是一個專為協作而建的中央化工作空間，動態、可自定義的工作區，可根據小組大小重新配置，無論他們身在何處，先進的可視化和 Skype 技術使專家可以隨時參與討論。
- 解決 GDPR 問題:CCC 在確保 Azure 符合歐盟的一般數據保護法規(GDPR)方面發揮了重要作用，這項法規對 Azure 的 140 個不同服務產生了巨大影響，在客戶要求時立即且可驗證地從所有系統中刪除其個人數據。CCC 協助全球的微軟工程團隊經過長達數周的努力，以確保 Azure 符合 GDPR 的要求。這個 CCC 是主要雲端提供商中第一個擁有這種設施的，它為 Azure 的持續改進和客戶服務提供了無價的支持。

- 建置豐富的生成式 AI 應用程式：使用適用於 Azure AI 的新 Azure Database for PostgreSQL 延伸模組，從 SQL 查詢存取 Azure Open AI 和 Azure AI 語言服務。
- 提高效能和可規模性：在超大規模 Azure SQL 資料庫上建置 AI 啟動應用程式，並以商業開放原始碼定價獲得 Azure SQL 的效能和安全性。

五、 3 月 1 日行程

(一)人工智慧的產業垂直應用案例分享

會談時間：2024 年 3 月 1 日（五）上午 8 時 45 分

出席代表：數位發展部數位產業署呂正華署長、林宗漢科長

微軟 Azure AI 與機器學習產品行銷總監 Richard L. Tso 及技術人員

表 5、3 月 1 日 POWER AISIA 研討會後與微軟交流 AI 垂直應用議程

時間	議程
10:00-10:50	微軟的合作夥伴賦能生態系統
11:00-12:10	微軟的 AI 未來發展
12:10-12:30	交流與討論分享

活動紀要：

1. 微軟的合作夥伴賦能生態系統 (Partner Ecosystem enablement from MSFT)

微軟 Azure AI Services 涵蓋了多個人工智慧領域，包括視覺、語音、語言、決策和網路搜尋等服務，這些服務使開發者能夠建立能看、聽、說、理解和解釋用戶需求的智慧型應用程式，並根據這些輸入做出明智的決策。

- 視覺服務使應用程式能夠識別和分析圖片和影片中的內容，從而進行圖像識別、場景偵測和臉部識別等。例如，零售商可以

使用視覺服務來分析客戶的購物行為，或者醫療機構可以用來分析醫學影像。

- 語音服務提供了語音轉文字和文字轉語音的功能，使應用程式能夠與用戶進行自然的語音交流，這可以應用於客戶服務機器人，或者幫助有語言障礙的人士進行溝通。
- 語言服務則是利用自然語言處理技術，幫助應用程式理解、翻譯和生成語言，這可以用於自動翻譯服務，或者分析社交媒體上的情感趨勢。
- 決策服務則提供了一系列的算法，幫助應用程式在複雜的數據集中做出決策，這可以用於風險管理、個性化推薦系統或者預測分析。
- 最後，網路搜尋服務則允許應用程式處理和分析網路數據，從而提供更豐富的用戶體驗。例如，新聞聚合應用程式可以使用這項服務來提供個性化的新聞摘要。

微軟 Azure AI Services 為開發者提供了強大的工具，以便快速且有效地整合人工智慧到他們的應用程式和服務中，從而創造出更智慧、更個性化的用戶體驗。這些服務的應用範圍廣泛，從企業到醫療保健，從零售到金融服務，都能找到其應用的場景。微軟 Azure AI Services 的目標是為所有企業提供可靠、安全且負責任的人工智慧解決方案。這些服務不僅能夠提升效率和效能，還能夠幫助企業在競爭激烈的市場中保持領先。

2. 微軟的 AI 未來發展

微軟透過其 Azure 平台，提供了一系列的工具和服務來幫助合作夥伴建立和現代化 AI 應用程式，這些工具和服務包括應用程式現代化、生成式人工智慧、機器學習以及 Azure OpenAI 服務部署，這些都符合微軟高專業水準的國際認證標準。微軟強調以 AI 驅動轉型

及在 Azure OpenAI 上的企業級應用商機，並提供合作夥伴更多資源，滿足客戶在雲端上的體驗。

此外，微軟也舉辦了 AI 合作夥伴培訓巡迴展（AI Partner Training Roadshow），這是一個面向合作夥伴的培訓活動，旨在分享 AI 的最新趨勢和技術，並提供專家指導。這些活動通常包括產品展示、AI 部署案例分享、技術或銷售培訓，以及與微軟技術和行銷團隊的專家對話，參加者可以在這些活動中獲得實際操作經驗，並學習如何向客戶推廣微軟的 AI 和 Copilot 能力。

例如，在 2024 年的參訪中，參加者將有機會深入了解生成 AI、雲端規模的數據基礎設施、雲原生應用程式開發等領域。他們還將學習如何利用 Azure Data & AI 解決方案來建構功能豐富的生成 AI 應用程式，並提高性能和可擴展性。此外，還會介紹如何利用 Copilot for Microsoft 365 來增強 M365 的核心架構、數據主權、安全性和合規性，以及 Copilot 的擴展性和部署。

這些培訓和參訪活動不僅提供了技術知識，還提供了與專家和其他合作夥伴交流的機會，從而幫助合作夥伴更好地理解和應用 AI 技術，推動客戶參與度，最終實現數位轉型。這些活動對於開發人員、解決方案架構師、實施顧問以及銷售和預銷售顧問等不同角色的專業人士都非常有益，透過這些培訓和交流，微軟的合作夥伴可以獲得必要的技能和知識，以建構和現代化 AI 應用程式，並在競爭激烈的市場中保持領先地位。

伍、 結論

根據 2021 年研調機構 Oxford Insights 針對各國政府人工智慧整備度（Government Artificial Intelligence Readiness Index）的評估報告，綜合分析來自政府、技術部門、數據與基礎建設等面向指標，臺灣在全球 160 個國家中排名第 18、在東亞國家地區則排名第 5，人工智慧正在迅速成為世界各國領導人最關切的議題。近年來，我國政府與民間均積極投入 AI 研發與應用，而為持續推動臺灣產業化 AI 發展，更需進一步發展 AI 產品的相關標準與 AI 產品認驗證指引，並且接軌國際相關標準與規範、落實 AI 治理。臺灣 AI 行動計畫的下一步，將聚焦可解釋、可信任 AI，包括參考國際標準來制定 AI 產品驗證規範、建立模型測試和評估方法。透過搭建 AI 治理基礎設施，如建立 AI 產品與系統評測中心來衡量 AI 風險、模型表現和穩健性；以及打造 AI 產品驗證機制來推動產業發展、加速 AI 落地。

自 2023 年底美國總統拜登（Joe Biden）於 10 月 30 日簽署了一項與人工智慧（AI）有關的行政命令，當下美國尚無任何有關 AI 的立法，而這也是美國總統所簽署的第一個 AI 行政命令，提出了 8 項行動目標。拜登所指示的 AI 目標涵蓋建立 AI 安全的新標準，保護美國人的隱私，促進公平與公民權利，替消費者、病患及學生挺身而出，支持勞工，推動創新與競爭，提升美國在海外的領導地位，並確保政府負責任及有效地使用 AI。該命令的第一項就是建立 AI 安全的新標準，準備採取全面的行動來保護美國人免受 AI 潛在風險的危害。包括要求強大 AI 系統的開發者必須與美國政府分享其安全測試結構與其它重大資訊；必須發展各式標準、工具與測試來協助確保 AI 系統是安全及可靠的；制定強大的標準來監控生物合成，避免利用 AI 設計出危險的生物材料；建立如何分辨 AI 生成內容與官方內容的偵測機制與最佳實作，以避免人們遭到 AI 詐騙；開發 AI 工具來發現及修補重大軟體中的安全漏洞。

基於上述法案與行動目標，美國商務部於今年 2 月成立美國人工智

慧安全機構(U.S. AI Security Institute, USAISI)，由美國國家標準技術研究院(National Institute of Standards and Technology,簡稱 NIST)主導，來負責未來 AI 安全相關工作，並同步籌組了美國人工智慧安全研究聯盟(U.S. AI Safety Institute Consortium，AISIC)，包含約 200 家企業實體，如 OpenAI、Google、Anthropic 和微軟(Microsoft)、臉書(Facebook)母公司 Meta、蘋果(Apple)、亞馬遜(Amazon)、輝達(NVIDIA)、英特爾(Intel)等公司，以及主要學術機構和政府機構，將隸屬於美國 AI 安全研究院(USAISI)旗下。共同參與標準制定與相關 AI 安全工作的討論。由於 AISIC 是產業與美國政府交流的管道，且開放企業或法人參加，未來應該可以推動臺灣重要產業或法人加入此組織，共同為 AI 標準提出建言，也能加速臺灣接軌國際之腳步。

而現階段臺灣正優先完善 AI 治理運作環境，參酌國際標準組織制定的 AI 標準，與 NIST 美國國家標準與技術研究院、LNE 法國國家計量測試實驗室架構，來建置我國 AI 產品與系統評測中心（AI Evaluation Center, AIEC），此中心已於 2023 年 12 月成立；透過提供包括資料面、演算法、模型面等各項評估與測試技術工具，以評估 AI 產品系統自研發到應用導入階段的風險、效能和穩健性。同時，亦將規劃建立 AI 產品認驗證體系（AI Product Certification Scheme），依循特定的國內外標準，並由透過遵循 ISO 17025、ISO 17065、ISO 17011 等品質管理系統國際標準的測試實驗室與驗證機構（certification bodies）來進行測試驗證，帶動國內 AI 產業發展。未來透過如前述美國 AISIC 等聯盟，或其他相關組織的參與鏈結國際，發展我國的 AI 指引與標準，以推動臺灣可信任 AI 產品輸出國際市場，提供我國 AI 國際影響力。

透過本次國際交流的分享，有助於評測後續政策規劃，另數位發展部數位產業署於 2024 年 3 月 23 日將辦理「運用 AI 促進資訊完整性」線上公民審議大會，透過公民參與，包含個人及利害關係社群，能充分反映來自民間的專業意見，不僅具有民間代表性，也作為公私協力的典範，足以作為國家施政的正當性基礎及關鍵參考依據。其中包含從個人對勞動力

釋放與賦能，到社會各群體的利害關係探討與產業升級及輔導轉型的影響層面，最後到國家層級的管制政策制度化，充分收集從個人到群體，再到國家策略層面的公民意見，充分展現臺灣人民血液中的民主素養與思想倡議。本年度將持續以 AI 審議式民主的活動，與公民面對 GAI 技術對社會產業的衝擊，以及如歐盟、美國在 AI 法治與標準制定後的因應措施，期待透過公民參與以及意見的交流與彙整，充分展現臺灣的公民民主素養，以及政府廣納建言，匯聚群眾意見與 AI 技術看法，建立施政以民為本的正當性基礎。

陸、 心得與建議

一、心得

與各國代表共同參與微軟主辦之「Power Asia」會議，瞭解微軟合作夥伴生態系統，並倡議數位發展部數位產業署在 AI 推動的成果，藉以連結亞洲相關重要國家，進行交流討論。透過臺灣在資通訊領域上的優勢，說明如何以政策帶動產業發展，除進行生成式 AI 應用及發展規劃、亦發展適用於我國的 AI 產品與系統評測機制，參考國際標準，以制定我國 AI 評測機制及數位產業推動方向。

這次活動瞭解微軟在負責且受信任的 AI 上，提出了六個關鍵準則，以引導 AI 在權責、包容性、可靠性和安全性、公平性、透明度，以及隱私權與安全性等層面上的發展。這些原則有助於建立負責任且值得信任的 AI，並將其應用核心產品和服務。這次以實地參訪的形式，看到微軟將負責任 AI 文化納入公司體制，並公開分享提供實質工具與治理經驗，以確保 AI 對客戶和社會更加安全可靠。

數位發展部已於 2023 年底成立 AI 產品與系統評測中心並完成掛牌，將於今(2024)年上半年提出 AI 產品與系統基本規範以及 AI 產品與系統基本檢測基準，提供產業對於人工智慧應用之產品與系統可依循之開發管理與評測作法。呼應微軟針對 AI 系統及服務之安全性、可靠性、資料隱私性、資安等議題之技術與開發現況，這次出國參訪交流將作為後續政策制定重要參考，並藉此邀請微軟公司參與臺灣 AI 評測，擴展國際交流合作，收穫良多。

為推動國際大廠參與評測，藉此活動與微軟進行深度交流，了解 AI 的發展趨勢，同時也藉此機會向各國參加者分享我國推動 AI 評測之內涵，也藉這機會邀請微軟，將其開發中的語言模型，提供 AI 產品與系統評測中心，以應用程式界面進行評測。另亦針對大型平台對於生成式 AI 內容進行分析及辨別方面等議題進行交流，共同朝向可信任數位環境發展。

二、建議

2022 年，OpenAI 推出大型語言模型「ChatGPT」，使用者能透過對話，從 ChatGPT 獲得解答；臺灣緊接著也研發台版繁中、納入臺灣文化的聊天機器人 TAIDE（Trustworthy AI Dialog Engine）。TAIDE 是臺灣第一個本土 AI 引擎，過去，大型語言模型常以簡體中文的文本訓練，欠缺繁體中文資料，並常出現偏誤。所以，國科會透過 TAIDE 計畫，完成能呼應本土化需求，並確保生成式 AI 的可信任性和適用性的大型語言模型。

為提出我國 AI 發展依循建議，進而輔導業者掌握國際趨勢與標準，數位發展部數位產業署提出「AI 產品與系統評測參考指引(草案)」。然而 AI 產品與系統評測中心目前規劃之測試類別涵蓋面向廣泛，其中，測試類別「準確度」與「公平性」不容易判斷，「公平性」倘涉及不同面向亦會有所不同，且人工檢測難度也高，如何讓民眾信服也需多思考。

藉由本次出訪，透過與國際大廠交流及與亞洲重要代表互動意見，回饋至審議式民主活動籌備構想上，針對一些公共政策討論可以促進我們全體民眾的參與，透過這種公民意見的協作平台，不僅是技術上的創新，更是民主實踐的進步，我們可能在討論的過程中遇到意見分歧，但我們更希望能夠在這種集體智慧的討論中在看似對立的價值之間找到平衡。

隨著 AI 的應用與發展越來越蓬勃，民眾也會想要參與 AI 的相關政策與內容討論。我們也建議其它國際大廠可藉由線上公民審議大會邀請專家學者與社會大眾一起探討，如何運用 AI 來辨識和分析資訊的完整性等相關議題，透過具包容性和平等的對話平台，讓來自全台各地的公民、社群和數位從業者，針對如何運用 AI 技術提升資訊完整性的一些方案和相關考量進行討論。協助政府在運用 AI 提升行政效率的同時，也能秉持負責任及可信賴的態度，並保有自主思維及創造力，促進民眾與政府的互信。

回國於辦理公民審議大會後，邀集國際大廠就強化平台的分析及辨別機制、及將語言模型(LLM)提送 AI 評測中心等議題進行討論，以瞭解國際大廠對於 AI 須具備可信任、準確性及安全等重要特性想法，及後續送測態度，一同推動可信任 AI 的發展。

柒、 照片紀實

圖 1、呂正華署長、林宗漢科長與參加 PowerAsia 會議成員合照

圖 2、PowerAsia 研討會參訪 Microsoft Cybercrime Center 與會人員合照

圖 3、參訪 Microsoft Azure Cloud Collaboration Center 團員合照

圖 4、微軟 Lee Hickin 於 2 月 27 日 PowerAsia 研討會說明議程

圖 5、2 月 28 日 PowerAsia 研討會講師分享情形

圖 6、數位發展部數位產業署出訪人員於 2 月 29 日 PowerAsia 研討會與各國分享 AI 應用與發展

圖 7、數位發展部數位產業署出訪人員於 3 月 1 日交流微軟的合作夥伴生態系統賦能

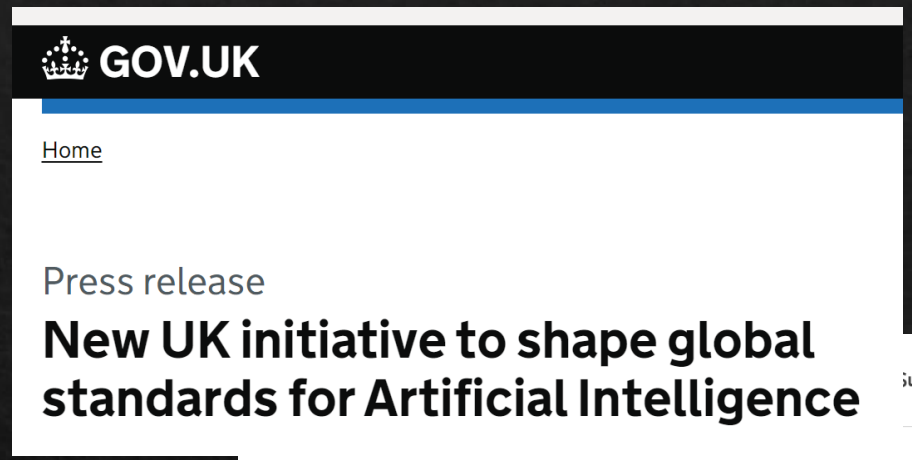
附件一

The Accountability of Trust

Jason Matusow

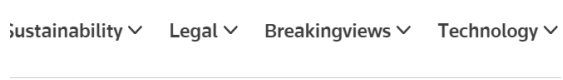
General Manager, Corporate Standards Group

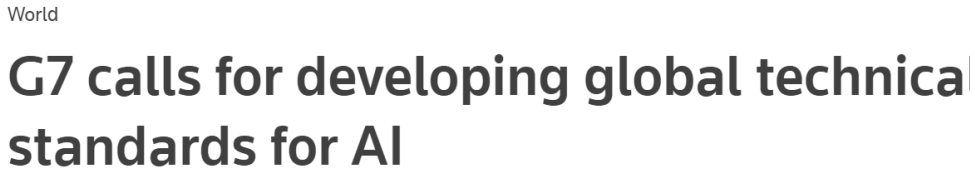
Microsoft


GOV.UK
Home
Press release
New UK initiative to shape global standards for Artificial Intelligence


About
Centers
Press
President's Page
Scholars
Policy Areas
Products


Report
Artificial Intelligence: The Risks Posed by
Current Lack of Standards
By Elisabeth Braw
American Enterprise Institute
December 07, 2021

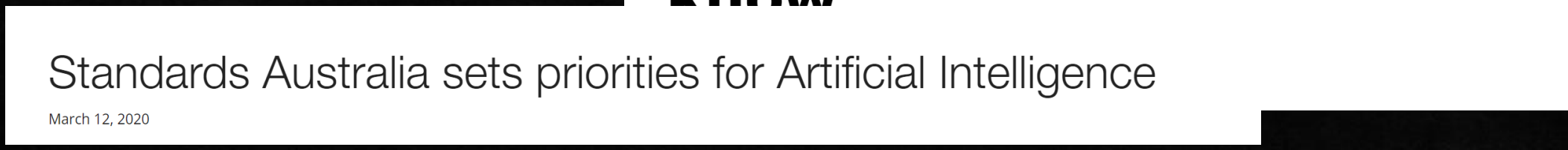

Sustainability
Legal
Breakingviews
Technology


World
G7 calls for developing global technica
standards for AI


AI
President Biden issues executive order to set standards for AI safety and security
AI hype sparks excitement and fear as government pushes for greater guardrails
Paul Sawers @psawers / 6:39 AM PDT • October 30, 2023


Jan. 17, 2024, 2:07 AM PST
China Drafts Guidelines on Standards for AI Sector
Wenshan Luo


EUROPEAN UNION
EU sets global standards with first
AI regulations: Here's what you nee
know


Standards Australia sets priorities for Artificial Intelligence
March 12, 2020


Cadbury
DAIRY MILK


CMA CGM


string4replace = string4
value = float(value) tempValue = str(
tempString = tempString.replace(
tempString = tempString.replace("czFieldID",str(key))
tempString = tempString.replace("czData"
in line and flagCheckRic
in line: myEvent =
os.path.exists(path): os.makedirs(path)
shutil.rmtree(
searchObj = re.search(


Leading Edge
Trailing Edge

Technology

Standards

Laws

Metrology Standards

Safety Standards

Interoperability Standards

Management Standards

Self-Attestation

3rd Party Certification

Labeling Programs

Licensing

Soft Law

- Procurement requirements
- Efficient contracting
- Trusted behaviors

Enacted Law

- Incorporation by reference
- Conformity requirements
- Licensing and registration

Standards

Codes of Conduct

Ad Hoc Expert Groups

Enterprise Norms

Marketplace Examples

Digital Services

- Delivered Over the Internet
- Dynamic and Evolving Offerings
- Cross-Boarder Availability
- Shared Assurance Obligations

Digital Services on Traditional Goods

- Integrated Multi-Sectoral Solutions
- Static Goods & Dynamic Applications
- Cross-Border Digital Services Delivery

Digital Services on Industrial Goods

- New Business Models
- Data → Machine Learning → AI
- Every Actor Wants The Data
- Personal and Non-Personal Data
- Cross-Border Availability

- Underlying Platforms Are Enablers
- AI At Every Layer
- Horizontal Regs / Vertical Solutions
- Overlapping Competent Authorities
- Industrial Policy Objectives

Artificial Intelligence

AI Principles

- Independent baselines of ethical structures
- Training, development, deployment, and use
- None are implementable on their own

Microsoft's AI Principles

Microsoft Blueprint for Governing AI – May 25

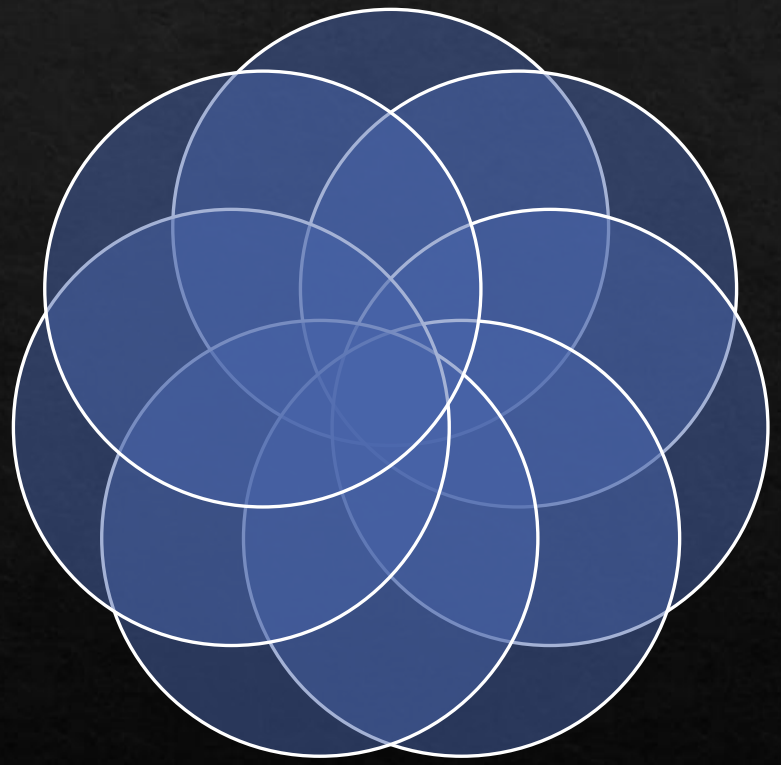
- **Implement and build** upon new government-led AI safety frameworks
- **Require effective safety brakes** for AI systems that control critical infrastructure
- **Develop a broader legal and regulatory framework** based on the technology architecture for AI
- **Promote transparency** and ensure academic and public access to AI
- **Pursue new public-private partnership** to use AI as an effective tool to address the inevitable societal challenges that come with new technology

The AI "Standards" Landscape

International Standards

Open Source Software Projects

Vertical Industry Standards



Safety Institutes, Codes, and Frameworks

Narrow Interop Standards

Academic Publications

Regional Standards

Responsible AI Standardization

Scoped	> Standardize **engineering and management practices** not ethics
Digital	> Natively address **digital services** not products
Coherent	> Enable **global applicability** to legal frameworks
Transversal	> Recognize inherent **domain dependencies** such as with cybersecurity, privacy, and data governance

NIST AI RMF

Govern

- Culture of risk management in the organization.
- Align with principles, policies and strategic priorities.

Map

- Identify risks for AI systems.
- Identify risk treatments.

Measure

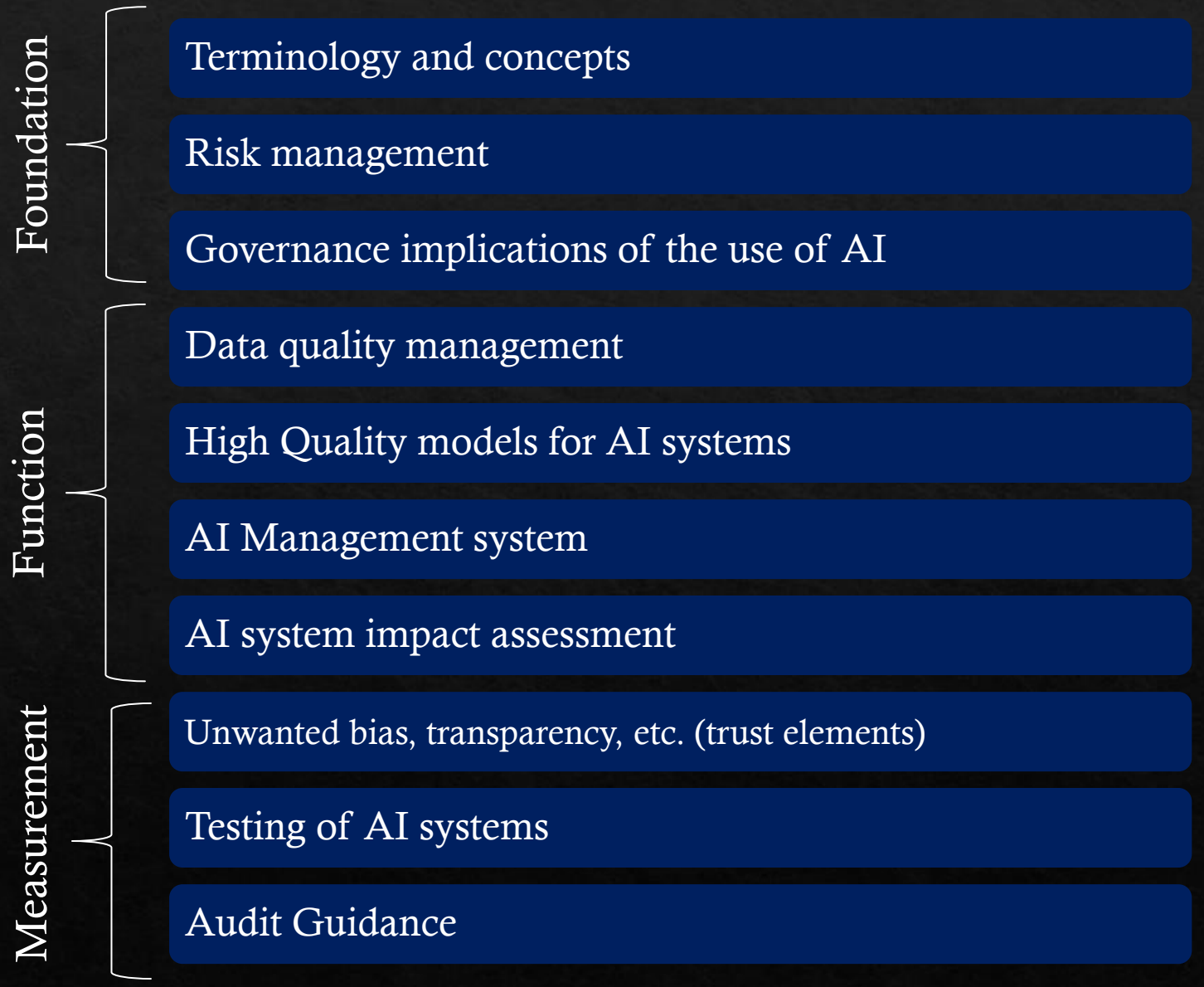
- Risk assessment.
- Test, evaluation, verification and validation (TEVV) processes established.

Manage

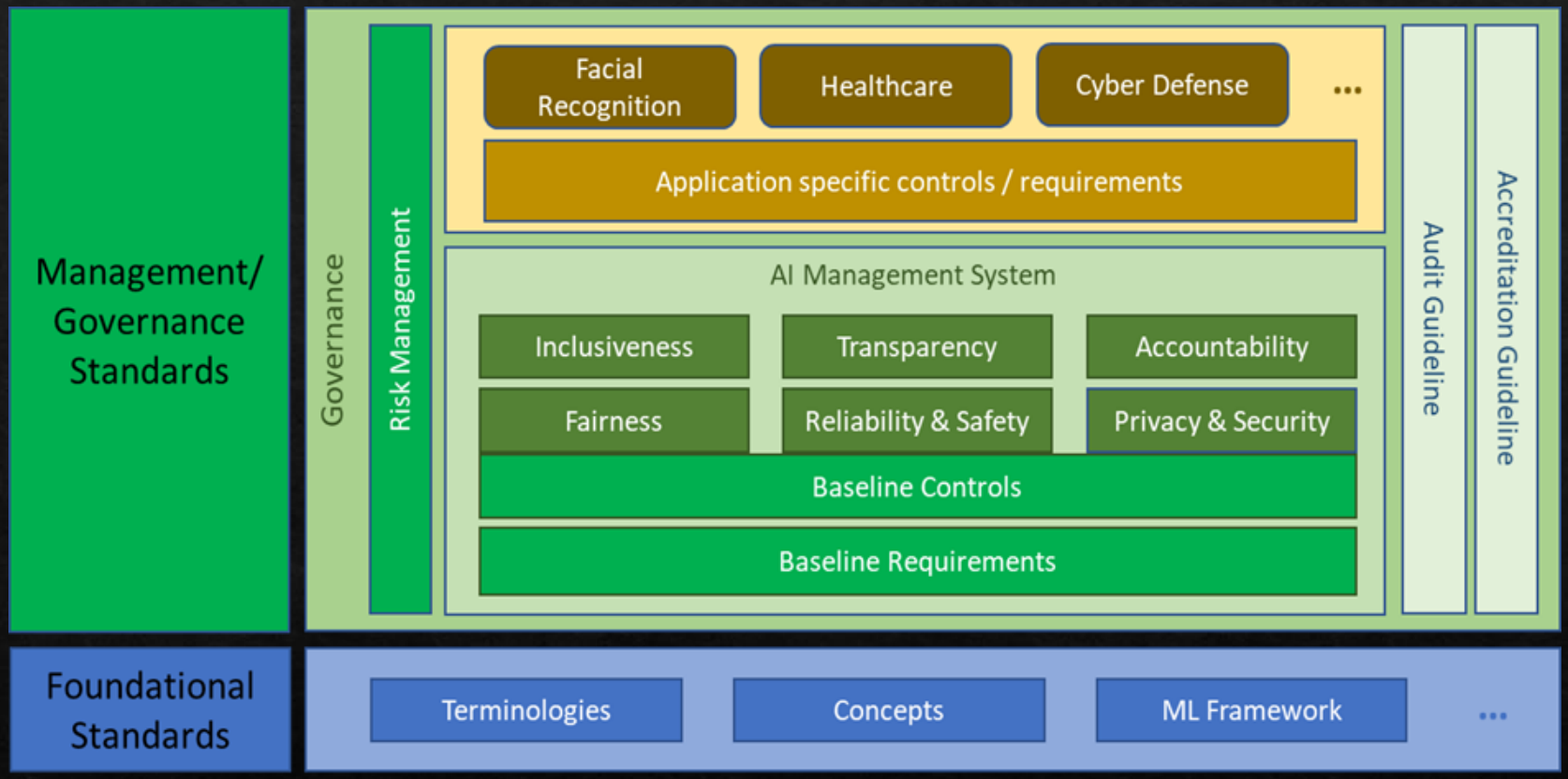
- Executes on items established in “Governance”
- Executes on risk treatments and continuous TEVV processes
- Continuous monitoring and improvement.

Standards Concepts for Responsible AI

- Differentiated components
- A system of related standards
- Not standardized regulation
- Dependence on strong accreditation and certification practices



Management System Standards Architecture for AI



ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS

Establish the Rigor

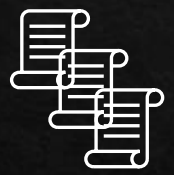
Declare the Risks

Set the Means

Prove It

Show It

Law, Regulations, and Organizational Policies



Audit Scheme

Management System

Scope of Applicability

Risk Framework

Impact Assessment

Management Commitment

Controls

Documentation

Training & competencies

Inspection

Audit

Certification

Compliance Artifacts

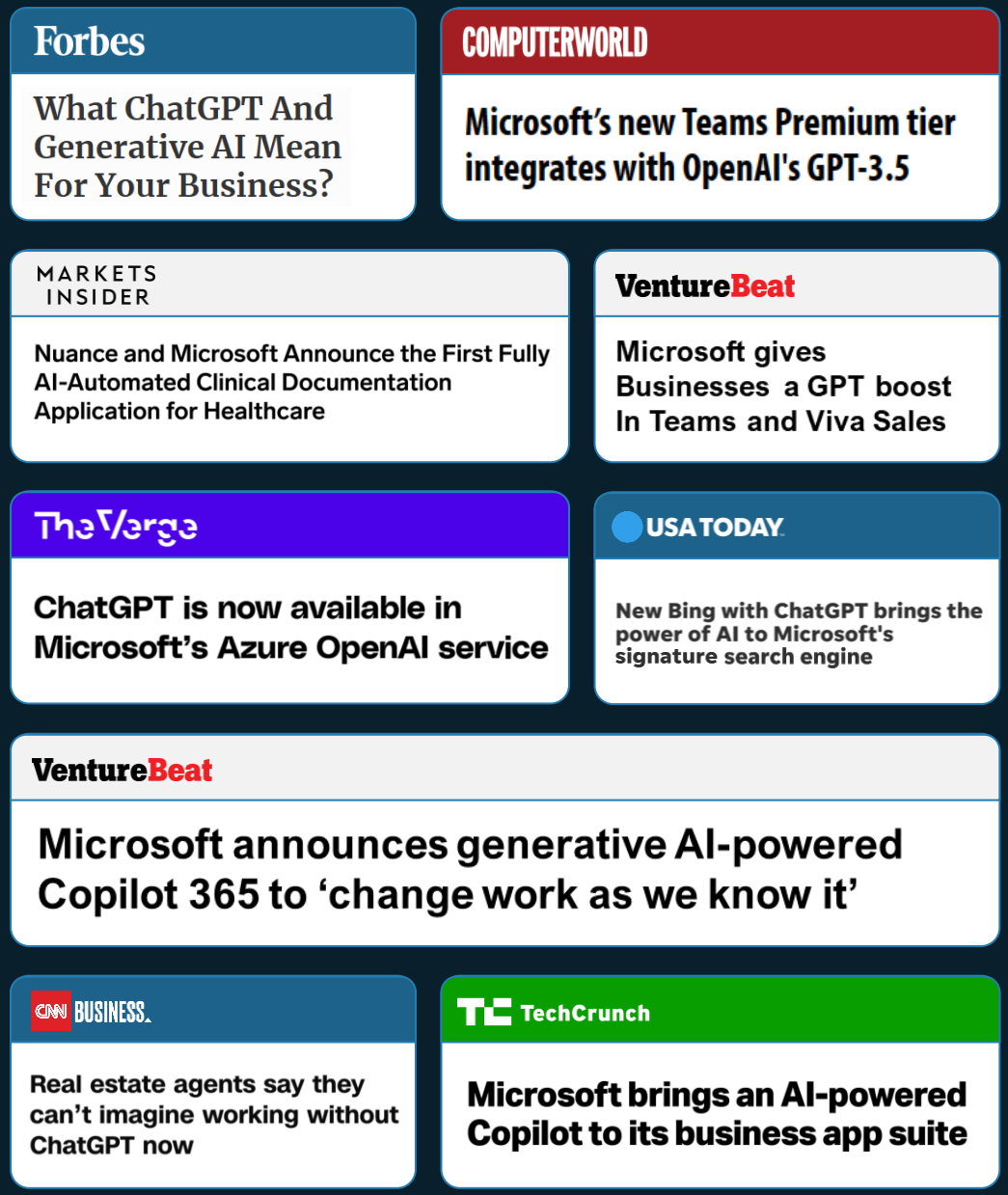
附件二

Microsoft

Meeting the AI Moment
A cross societal approach to AI governance

Owen Larter
Director of Responsible AI Public Policy
Office of Responsible AI
Microsoft

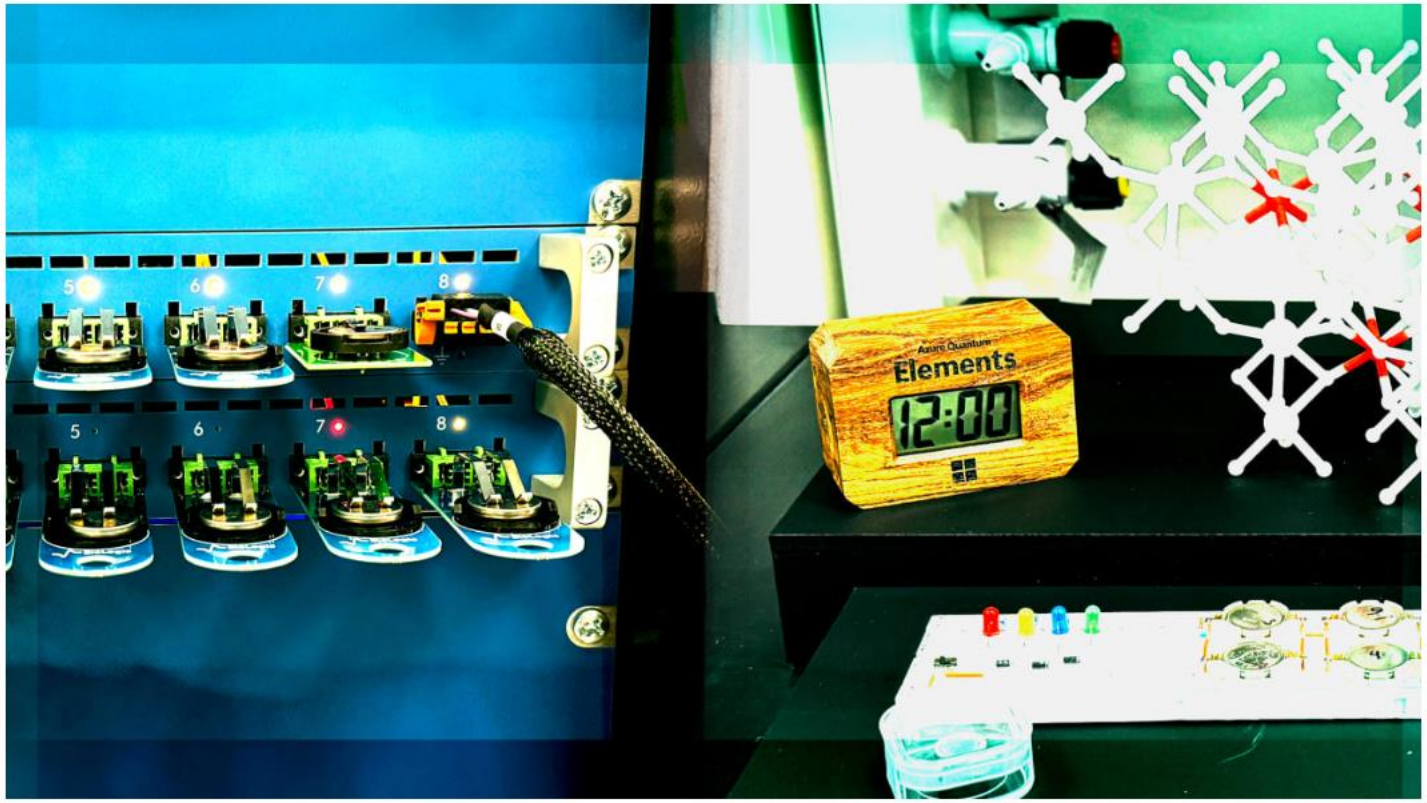
People are using AI to be more productive



Microsoft Research
AI4Science

Satya Nadella on the bigger vision behind Microsoft's new battery

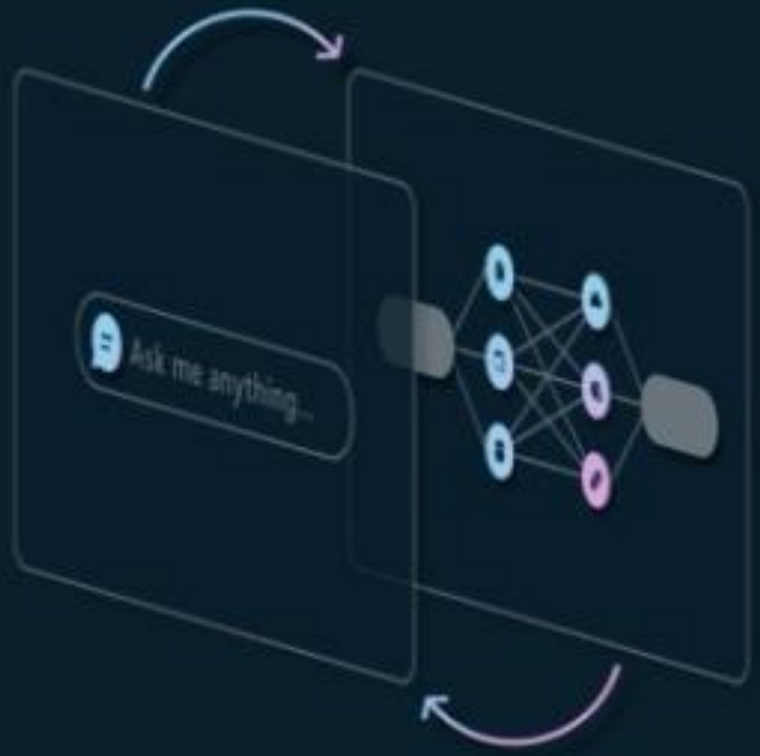
Working with a national lab, the software giant used AI to tackle the flaws of today's lithium batteries—and pave a new path for scientific discovery.



[Photos: Harry McCracken]

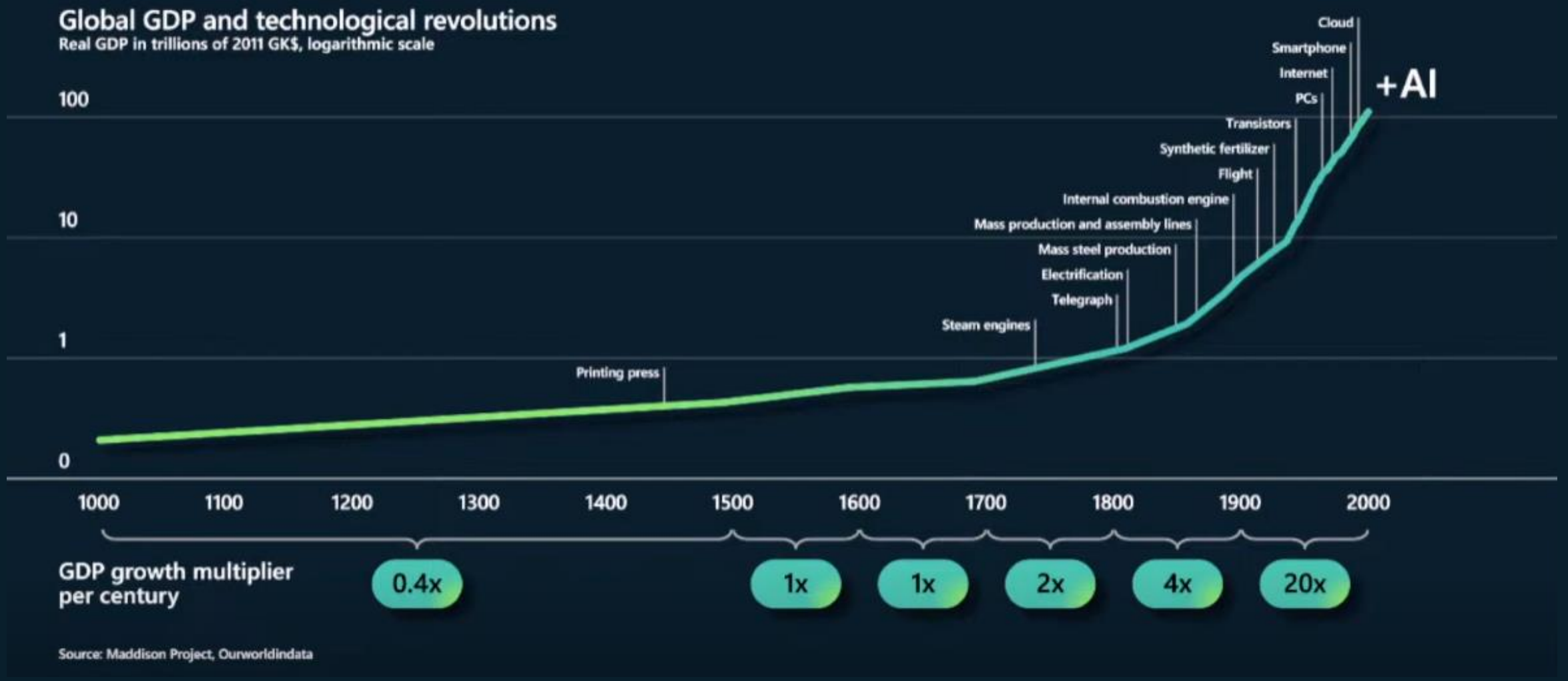
The next platform shift

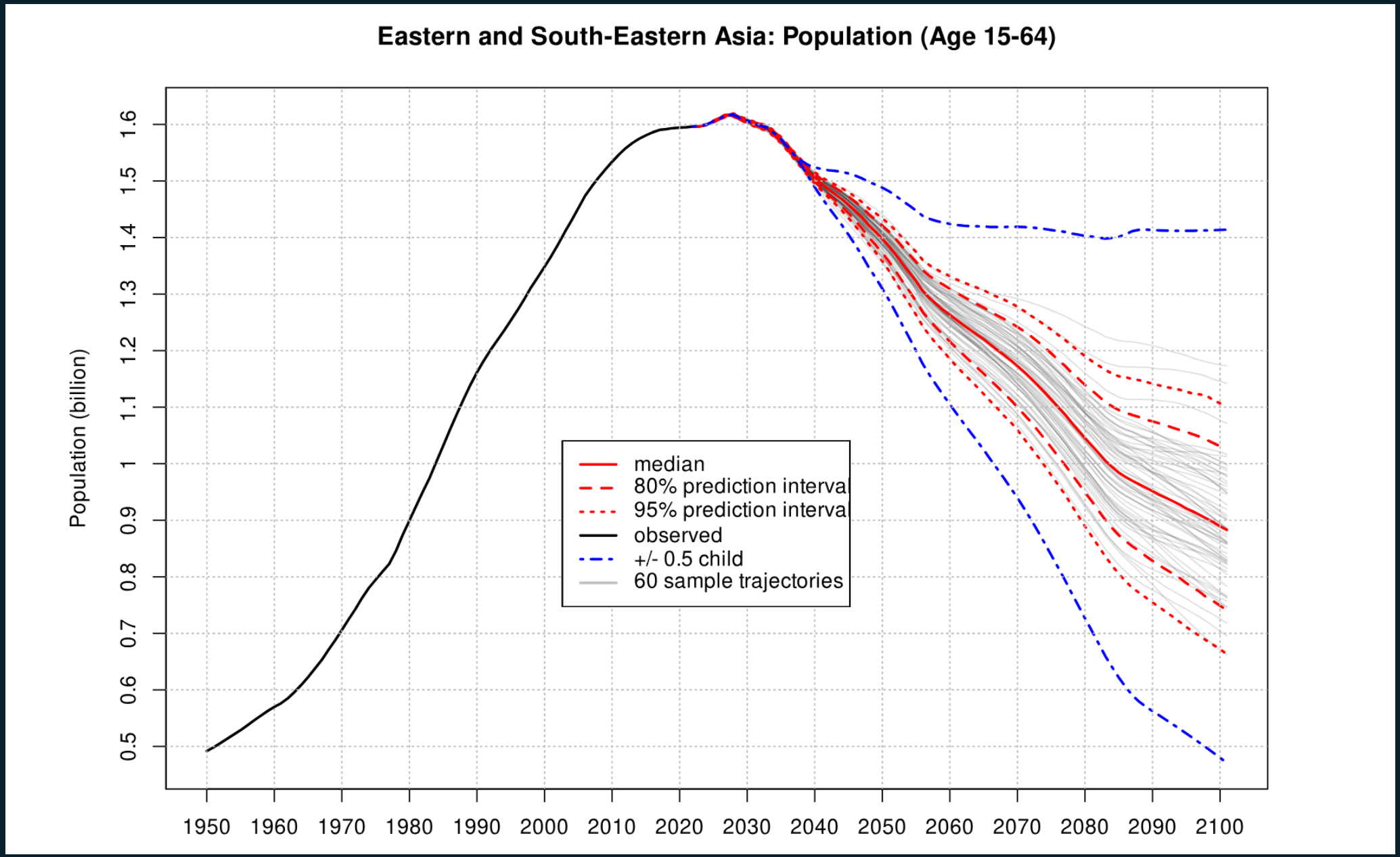
Natural language



Reasoning engine

Technology drives GDP growth, and the pace of change is accelerating




Eastern and South-Eastern Asia: Population (Age 15-64)
Population (billion)
0.5
0.6
0.7
0.8
0.9
1
1.1
1.2
1.3
1.4
1.5
1.6
1950
1960
1970
1980
1990
2000
2010
2020
2030
2040
2050
2060
2070
2080
2090
2100
median
80% prediction interval
95% prediction interval
observed
+/- 0.5 child
60 sample trajectories

Safe, secure and trustworthy AI

AI is safe and secure and used responsibly

AI advances international competitiveness and national security

AI serves society broadly, not narrowly

Meeting the AI moment: advancing the future through responsible AI

Feb 2, 2023 | Brad Smith - Vice Chair & President

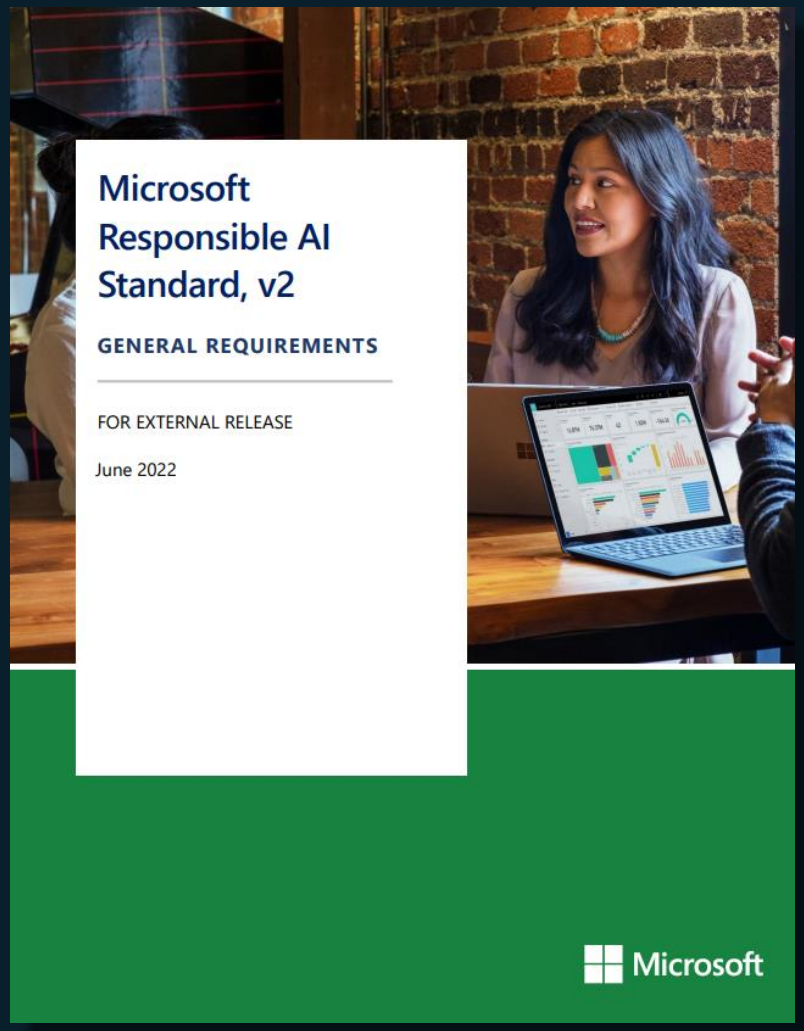
Early last summer, a small group of senior leaders and responsible AI experts at Microsoft started using technology from OpenAI similar to what the world now knows as ChatGPT. Even for those who had worked closely with the developers of this technology at OpenAI since 2019, the most recent progress seemed remarkable. AI developments we had expected around 2033 would arrive in 2023 instead.

Looking back at the history of our industry, certain watershed years stand out. For example, internet usage exploded with the popularity of the browser in 1995, and smartphone growth accelerated in 2007 with the launch of the iPhone. It's now likely that 2023 will mark a critical inflection point for artificial intelligence. The opportunities for people are huge. And the responsibilities for those of us who develop this technology are bigger still. We need to use this watershed year not just to launch new AI advances, but to responsibly and effectively address both the promises and perils that lie ahead.

The stakes are high. AI may well represent the most consequential technology advance of our lifetime. And while that's saying a lot, there's good reason to say it. Today's cutting-edge AI is a powerful tool for advancing critical thinking and stimulating creative expression. It makes it possible not only to search for information but to seek answers to questions. It can help people uncover insights amid complex data and processes. It speeds up our ability to express what we learn more quickly. Perhaps most important, it's going to do all these things

Industry must work with civil society to support governments in developing frameworks for responsible innovation

Microsoft's approach to Responsible AI



Principles

Fairness

Reliability & safety

Privacy & security

Inclusiveness

Transparency

Accountability

Corporate Standard

Goals
Requirements
Practices

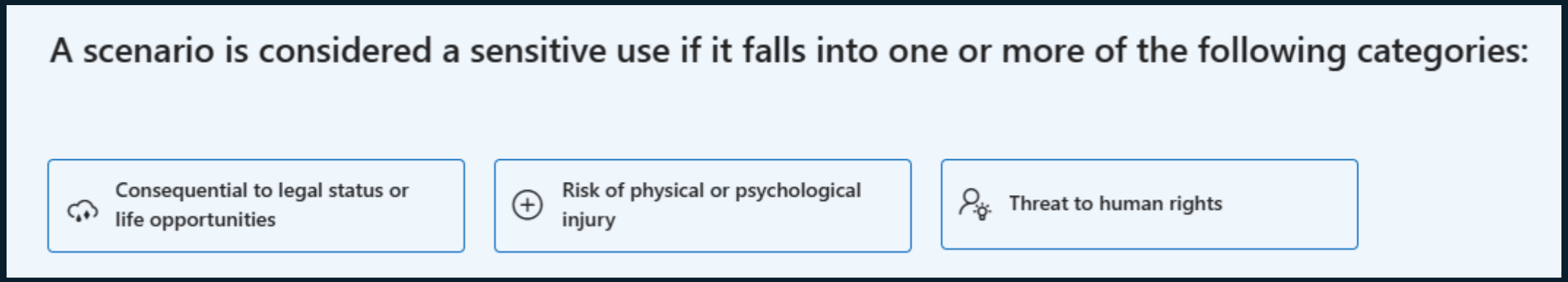
Implementation

Processes
Training
Tools

Oversight

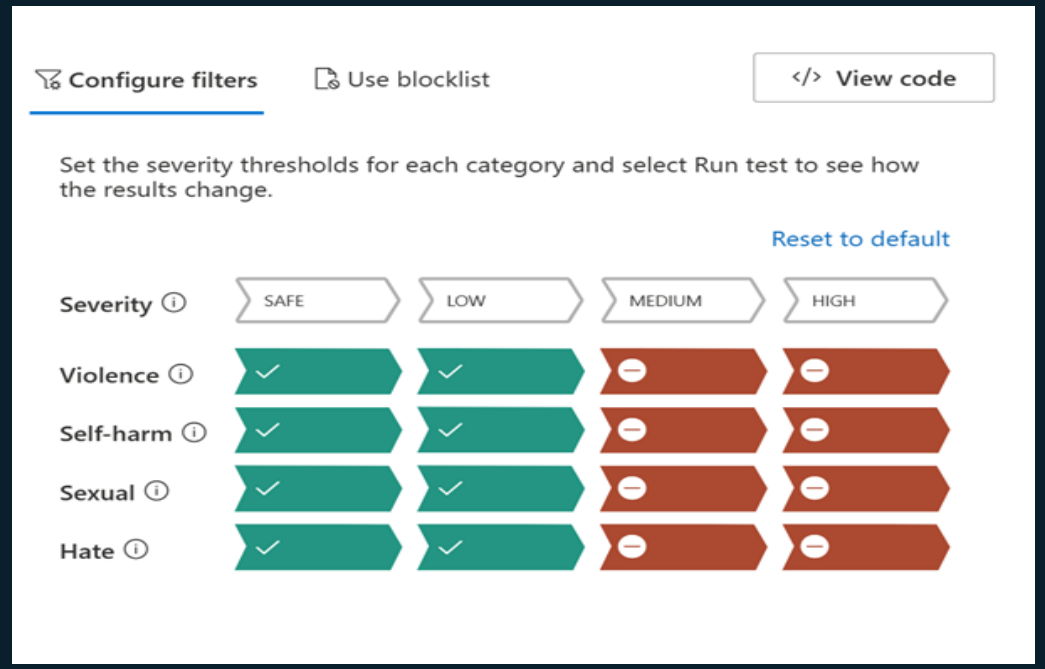
Monitoring
Reporting
Auditing

Sensitive Uses Team



Our ecosystem

Azure AI Content Safety



1

Azure AI Content Safety classifies harmful content into four categories:

Hate Sexual Self-harm Violence

2

Next, it returns a severity level for each category from 0 – 6:

Hate: 0 – 2 – 4 – 6
Sexual: 0 – 2 – 4 – 6
Self-harm: 0 – 2 – 4 – 6
Violence: 0 – 2 – 4 – 6

3

Then, it surfaces content based on the severity level:

High risk: Auto blocked
Medium risk: Sent to moderator and prioritized by risk level, topic, and user reputation
Low risk: Auto approved

A Tech Accord to Combat Deceptive Use of AI in 2024 Elections

This accord seeks to set expectations for how signatories will manage the risks arising from deceptive AI election content created through their publicly accessible, large-scale platforms or open foundational models, or distributed on their large-scale social or publishing platforms in line with their own policies and practices as relevant to the commitments in the accord.

Read the Press Release ›

Read the full accord ›

Watch the Webcast ›

Adobe

amazon

ANTHROP\C

arm

IIElevenLabs

Google

IBM

Inflection

LG AI Research

LinkedIn

McAfee

Microsoft

Meta

NetApp

NOTA

OpenAI

stability.ai

Commitments to Help Combat Deceptive Use of AI in 2024 Elections

Addressing deepfake creation

1. Advance content authenticity through provenance and watermarking
2. Strengthen safety architecture for content creation tools

Detecting and responding to deceptive deepfakes

3. Detect the distribution of deepfakes
4. Address deepfakes that are detected, including by removing them
5. Share information and best practices across the tech sector

Transparency and resilience

6. Provide transparency to the public
7. Engage with civil society, academics, and experts
8. Foster public awareness and resilience

Microsoft

Governing AI: A Blueprint for the Future

May 25, 2023

Foreword: How Do We Best Govern AI?

Brad Smith, Vice Chair
and President, Microsoft

"Don't ask what computers can do, ask what they should do."

That is the title of the chapter on AI and ethics in a book I coauthored in 2019. At the time, we wrote that "this may be one of the defining questions of our generation." Four years later, the question has seized center stage not just in the world's capitals, but around many dinner tables.

As people have used or heard about the power of OpenAI's GPT-4 foundation model, they have often been surprised or even astounded. Many have been enthused or even excited. Some have been concerned or even frightened. What has become clear to almost everyone is something we noted four years ago—we are the first generation in the history of humanity to create machines that can make decisions that previously could only be made by people.

Countries around the world are asking common questions. How can we use this new technology to solve our problems? How do we avoid or manage new problems it might create? How do we control technology that is so powerful?

These questions call not only for broad and thoughtful conversation, but decisive and effective action. This paper offers some of our ideas and suggestions as a company.

These suggestions build on the lessons we've been learning based on the work we've been doing for several years. Microsoft CEO Satya Nadella set us on a clear course when he wrote in 2016 that "perhaps the most productive debate we can have isn't one of good versus evil: The debate should be about the values instilled in the people and institutions creating this technology."

Since that time, we've defined, published, and implemented ethical principles to guide our work. And we've built out constantly improving engineering and governance systems to put these principles into practice. Today we have nearly 350 people working on responsible AI at Microsoft, helping us implement best practices for building safe, secure, and transparent AI systems designed to benefit society.

New opportunities to improve the human condition

The resulting advances in our approach have given us the capability and confidence to see ever-expanding ways for AI to improve people's lives. We've seen AI help save individuals' eyesight, make progress on new cures for cancer, generate new insights about proteins, and provide predictions to protect people from hazardous weather. Other innovations are fending off cyberattacks and helping to protect fundamental human rights, even in nations afflicted by foreign invasion or civil war.

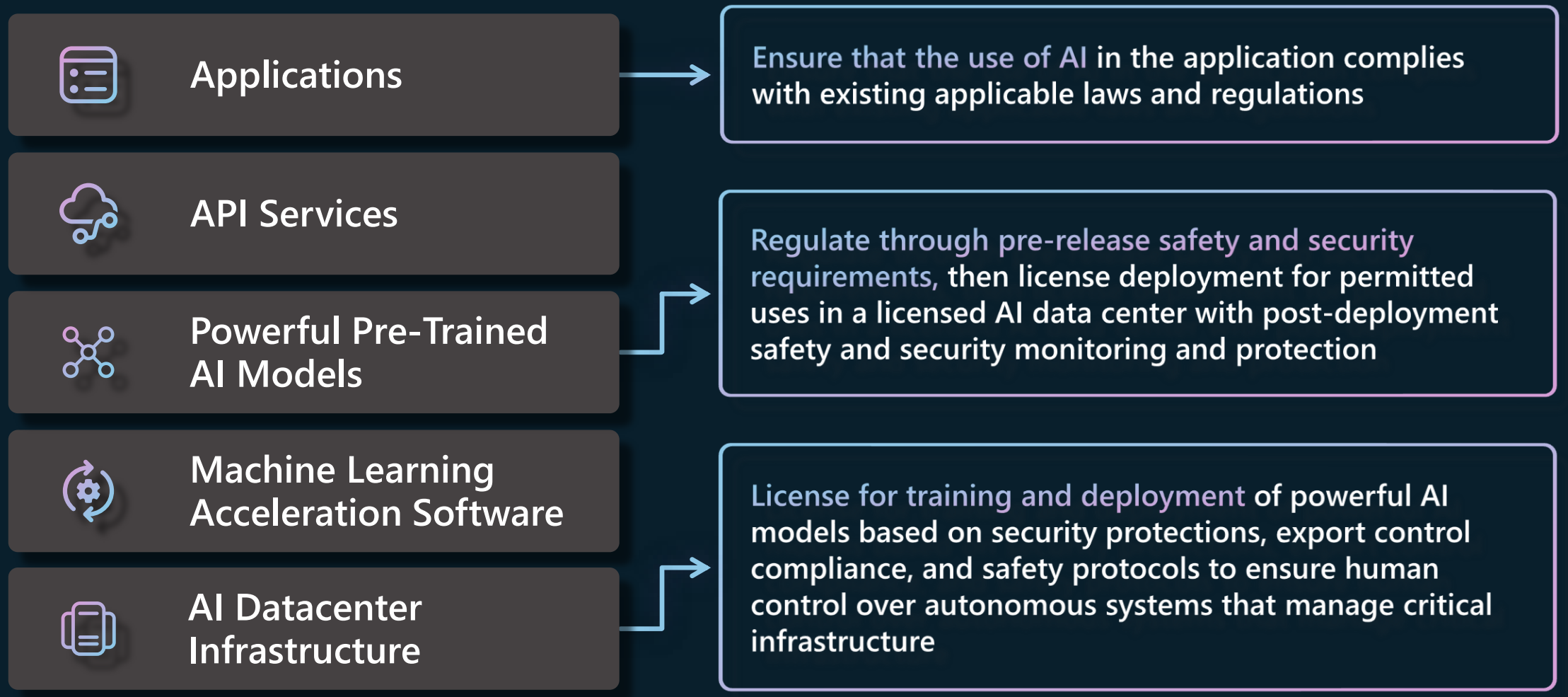
Everyday activities will benefit as well. By acting as a copilot in people's lives, the power of foundation models like GPT-4 is turning search into a more powerful tool for research and improving productivity for people at work. And for any parent who has struggled to remember how to help their 13-year-old child through an algebra homework assignment, AI-based assistance is a helpful tutor.

In so many ways, AI offers perhaps even more potential for the good of humanity than any invention that has preceded it. Since the invention of the printing press with movable type in the 1400s, human prosperity has been growing at an accelerating rate. Inventions like the steam engine, electricity, the automobile, the airplane, computing, and the internet have provided many of the building blocks for modern civilization. And like the printing press itself, AI offers a new tool to genuinely help advance human learning and thought.

A five-point blueprint for governing AI

1. Implement and build upon new government-led AI safety frameworks
2. Require safety brakes for AI systems that control critical infrastructure
3. Develop a broader legal and regulatory framework based on the technology architecture for AI
4. Promote transparency and ensure academic and public access to AI
5. Pursue new public-private partnerships to use AI as an effective tool to address the inevitable societal challenges that come with new technology

A proposed AI regulatory architecture



KY3C

Applying to AI services the “Know Your Customer” concept developed for financial services

Know your Cloud

Know your Customer

Know your Content

OCTOBER 30, 2023

FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

 ▸ BRIEFING ROOM ▸ STATEMENTS AND RELEASES

Hiroshima Process International

Code of Conduct for Organizations

Developing Advanced AI Systems

- Risk based approach
- Expand global coordination on regulatory architecture that matches the technology architecture
- Global coordination on measurement and science – Safety Institutes

Frontier Model Forum

Microsoft, Anthropic, Google, and OpenAI launch an industry body focused on ensuring safe and responsible development of frontier AI models.

Advance AI safety research to promote responsible development of frontier models and minimize potential risks,

Identify safety best practices for frontier models

Share knowledge with policymakers, academics, civil society, and others to advance responsible AI development

Support efforts to leverage AI to address society's biggest challenges.

附件三

PowerAsia 2024 Participant List

ANZ

Chris Fechner
Chief Executive Officer
Digital Transformation Agency
Australia

Glenn Kirker
Chief Data Officer, Defence Digital
New Zealand Defence Force
New Zealand

Taiwan

Isabel Hou
Secretary General
Taiwan AI Academy Foundation
Taiwan

Jang-Hwa Leu
Director-General
Administration for Digital Industries,
Ministry of Digital Affairs
Taiwan

Tsung-Han Lin
Section Chief
Administration for Digital Industries,
Ministry of Digital Affairs
Taiwan

ASEAN

Dr Aris Kusdaryono
Director of Application Governance
Ministry of Communication and Informatics
Indonesia

Arif Wahyudi
Analyst Cooperation
Ministry of Communication and Informatics
Indonesia

Rafaelita "Fita" Aldaba
Undersecretary
Department of Trade and Industry
Philippines

Alvina Goh
Director (Data Science & AI Platforms)
Government Technology Agency
Singapore

Hud Syafiq Herman
Engineer
Home Team Science & Technology Agency
Singapore

Colin Tan
Assistant Chief Executive (Enterprise Group)
Home Team Science & Technology Agency
Singapore

Wanyi Weng
Director
National AI Office, Smart Nation Group
Singapore

Chalitda Madhyamapurush
Executive Senior Advisor
The Electronic Transactions Development Agency
Thailand

Professor Wisit Wisitsora-At
Permanent Secretary
Ministry of Digital Economy and Society
Thailand

Japan

Genta Ando
Executive Director
Ministry of Economy, Trade and Industry / Japan
External Trade Organisation
Japan

Mariko Ohde
Director
Japan External Trade Organisation / Information-technology Promotion Agency New York
Japan

Shinji Tokumasu
Deputy Director-General for Science, Technology and Innovation
Cabinet Office
Japan