CLTC
Center for Long-Term Cybersecurity
UC Berkeley

CNA
ANALYSIS & SOLUTIONS

2025年網路安全展望
見解和發現

Cybersecurity Futures 2025
Insights and Findings

台灣資通安全研究與教學中心 TWISC@AS　譯

原文序

《2025 年網路安全展望》是加州大學柏克萊分校長期網路安全研究中心（Center for Long-Term Cybersecurity, CLTC）與美國海軍分析中心公共研究所（CAN’s Institute for Public Research）長期合作的計畫，並由世界經濟論壇的全球網路安全未來委員會及其網路安全中心協助完成。

報告簡述了計畫的過程和進展，並總結 2018 年在全球舉辦各次工作坊的觀點，還包括工作坊中作為討論基礎的四種情景。同時，在計畫網站（cyberfutures2025.org）上提供關於計畫的介紹以及四個情境的影片，也提供了互動式的工具，以啟發使用者形成策略性決策。我們希望這份報告和所附的多媒體內容能夠讓相關領域之讀者獲益，讓其組織機構更有預見性、更積極主動，最終更妥善應對各種新興的網路安全挑戰。當您與這些想法有相關見解，歡迎提供回饋意見。

感謝世界經濟論壇及其網路安全中心的全程合作。也要感謝支援這項工作的組織，包括 HP、Symantec、Qualcomm、CyberCube 以及工作坊的各協辦方。尤其感謝眾多同事，為情境的建立提供了意見和建議，還要感謝來自業界、政府和參與全球網路安全未來委員會的民間團體，他們對我們的工作坊做出了貢獻，並協助凝聚出重要的見解。

Steven Weber
Professor, UC Berkeley School of Information
Director, Center for Long-Term Cybersecurity

David Kaufman
Vice President and Director
Dawn Thomas
Associate Director
CNA Institute for Public Research

Alan Cohn
Partner, Steptoe & Johnson LLP
Adjunct Professor, Georgetown University Law Center
Co-Chair, World Economic Forum Global Future Council on Cybersecurity (2016-2018)

目錄

摘要

背景和概述

當技術與人為因素相互交錯將產生高度的不確定性，這是長久以來對於數位時代的看法，而這種不確定性相對於防禦者和保護者而言，更有利於網路攻擊者，使網路安全專業人員處於結構性劣勢。

展望未來，人與數位技術的交匯處，現今所使用的安全技術，與浮現在將來決策框架中的種種網路安全議題和挑戰，兩者之間將產生隔閡。為了填補這個缺口，我們制定了一套具前瞻性的網路安全情境，在政府、產業和公民社會面臨即將發生的網路安全挑戰之前，激發民眾展開迫切的討論。《2025年網路安全展望》的基礎理念是：如果能夠預測網路安全挑戰將如何演變，瞭解各地的政府、企業和社會如何看待這些挑戰，我們就能優化決策者的佈署，減少阻力並創造合作的機會。僅粗略地瞭解目前網路安全政策和策略架構是不足的，因此，《2025年網路安全展望》試圖為未來實務和戰術推動的高層次概念和策略提供藍圖。

階段 1：制定《2025年網路安全展望》情境

在計畫的第一階段，我們制定了一套情境，粗略地描繪2025年「網路安全展望」可能的發展。這四種情境是專為啟發世界各地的不同觀點而設計，旨在強調如何對未來的目標與價值之間進行取捨，並聚焦在重要與可行的網路安全議題上，同時也挑戰現有的信念。

《2025年網路安全展望》的情境不是對未來的預測，而是合乎邏輯的描述，講述2025年來自技術、經濟、人類行為、企業策略、政府政策、社會和道德層面等的變革力量，會如何重疊並結合起來，製造出各種與現今不同的網路安全問題。這些問題涵蓋更多層面的參與者，有更大的利害關係，擁有不同的技術基礎，並以一種新穎的方式觸及人類的核心價值觀。此四種情境詳參後述。

階段 2：國際工作坊

2018年5月至10月間，我們在帕羅奧圖（Palo Alto）、慕尼黑（Munich）、新加坡（Singapore）、香港、莫斯科（Moscow）、日內瓦

（Geneva）和華盛頓特區（Washington, DC）各舉辦了一場工作坊，並邀請政府、企業、公民社會、學術界和其他領域人士參與。由於各工作坊間觀點與反應的比較也是重要的直接成果，為了產生可比較的觀點與反應，每個工作坊都採取相同的運作模式。

雖然這四種情境在 2025 年不見得會「實現」，但屆時的網路安全領域中，將很可能涵蓋這些情境中的眾多議題和挑戰；理解世界各地的反應有助於制定前瞻性的研究和政策方向，同時讓這些研究和政策更強韌、更理智、更務實，並能更廣泛地適用於所有國家和地區。

階段 3：產生見解

我們從 7 次工作坊中形成了一系列摘要見解。這些見解具有明顯的侷限，其中最重要的影響是使用廣域地理標籤代表某個工作坊的成果；例如，將慕尼黑工作坊的成果標示為「歐洲」（有來自歐洲各國、機構和領域的代表），但它不等同在全歐洲舉辦工作坊，也不是從歐洲各國或各地區所區分出的不同意見，所以地理標籤就像不完美的代理或像邊緣模糊的「雲」[1]。另一個侷限是近因偏誤（recency bias）[2]，工作坊的參與者是人，人會依據當時心中最重要和最緊迫的事情判斷未來情境，我們設計的工作坊能夠儘可能地減少這類偏差，但無法完全去除。

雖然有所侷限，我們認為下列的初步見解至少在方向是正確的，因此在策略規劃和未來決策中值得被關注。進一步，我們提供三個整體觀察與五個新的前景來重新建構決策環境。

整體觀察

值得注意的是，數位技術和安全的論述現在已經被深度「國有化」，並且

---

[1] 譯者註：以地理標籤區分工作坊的成果，並不能真正代表或代理該地區的意見，甚至無法呈現意見的分布，特別是本計畫僅舉辦七個工作坊，更無法呈現全球的意見，就如同飄浮在空中的雲，雖然邊緣可見但事實上模糊而不穩定。就像慕尼黑工作坊的結果因為有來自歐洲各國的人士參與，所以不能代表慕尼黑的意見，也因為樣本代表性不足，所以不能代表全歐洲的意見。

[2] 又稱近因效應，指人們在判斷事物發展趨勢時，會認為未來事件將會和近期體驗高度類似，因而造成預期上的偏誤。這還是一種普遍的心理學特徵。

在我們的情景中變得更明顯。在「自由與開放的網際網路」的論述下，政府不應對網際網路進行過多干預，三年前仍有說服力，但這種天真的意識形態，基本上已經不復存在；現在「數據國家主義（data nationalism）[3]」已經是既定事實，此論點聚焦於實現國家權力目標的技術。此一轉變在歷史上雖然很常見，但對於網際網路和數位經濟而言卻是明顯的阻礙。

由於「網路規範」的模糊論述，讓人們對網路安全產生強烈的幻滅感。世界各地的工作坊參與者很難具體定義網路規範，也很難闡明對於規範的討論將如何引導（而非遵循）新的網路行為。

人們對於數位技術可以改善人類體驗的深刻期待，可能會消失在新興的場景中。第一代數位技術伴隨著（可能過度樂觀的）理想主義，包括財富創造、安全、效率、和平、幸福等等，這些期待難免會隨著時間而調整。但是如果鐘擺朝向風險和威脅的那端擺動得太快、太遠（現在看來似乎如此），社會就有可能忽視這些技術經過妥善管理與保護時帶來的巨大效益。

新的前景

1. 過去 20 年，政府和企業的「中庸之道」是以柔性監管和不需許可的創新當作共同打造數位經濟的基礎，但這種做法不一定能持續。工作坊中，參與者並未試著維持「除非新技術被證明具危險性，企業得自由發展與佈署新技術」的模式，因為他們看不見此模式有效提高數位安全的可能性。打破這個模式的想法，即使僅是期望，也是政經環境中的顯著改變，我們可期待新的監管制度中將會出現各種不同管制方法的實驗；儘管這些實驗將強化政府的角色，但全球的數位環境也將變得愈來愈多樣化。

   這引發了一個簡單的問題：如果（必定）發生問題時，誰應該帶頭糾正錯誤？帕羅奧圖的答案是「一定是大公司，因為他們有能力處理」。慕尼黑的答案是「歐洲缺乏公司，且我們不相信政府會有所反應，所以需要公民社會運動」。新加坡的回答更溫和：「應該不會發生那麼大的錯誤，但如果發生，政府會是最後的救星」。這些答案的發展在根本上有著明顯的牴

---

[3] 參照資料在地化，指企業打算在某國提供服務時，該國會要求企業必須將該國的用戶資料儲存在該國境內，或不得任意傳輸至該國境外。

觸。

2. 數位地緣政治不只是單純地疊加在傳統地緣政治中，數位化正在創造新參與者之間的新聯盟，而不限於是國家之間。目前許多人仍然認為「沒有人會真的因為網路攻擊開戰，如果真的開戰，那網路攻擊也不會是唯一的原因」。我們的工作坊結果顯示這種想法難以為繼。聯盟正在重組：例如關於歐洲網路攻擊起因的爭論，對美國國安局與對 APT-2 等團體的關注是相同的。半官方組織和犯罪組織扮演的角色開始與大公司和政府的角色有等同的影響力：將其稱為「非國家角色」以暗示其為次級地緣政治地位是錯誤的。現在，「大公司和政府」同樣普遍被視為是政治程序中近乎平等的參與者。像丹麥等國家已經設立正式的技術部門大使，更多國家將比照辦理。新技術的出現可能會徹底改變地緣政治的角力抗衡（例如量子運算），加速與數位利益相關的聯盟重組，而且在新的聯盟中，企業的地位可能會與國家一樣重要。對於哪些行為構成犯罪活動，以及什麼人或組織是「罪犯」，也將出現新的定義。由於這些定義各地有所不同，數位犯罪分子在全球市場上套利的機會將會增加。

3. 數位化所引發的就業替代和不平等，將不僅僅是壓力的源頭，所產生的力量會對勞動市場和政治帶來根本性的崩潰和失敗。社會資本和更廣泛的社會適應力，將是引導社會度過自動化和機器人衝擊勞動市場後，再達成均衡的關鍵資產。

   國家和地區在此方面的定位大相徑庭，例如，基於相信「許多亞洲國家在面對類似挑戰時，已證明具有適應力和凝聚力」，亞洲人似乎對社會能夠承受這些變化有著更高的信心。然而，大眾也日益發現，大多數國家的經濟成長和發展軌跡越來越不確定。美國和歐洲的民粹主義運動部分顯示出，社會的壓力來自於大眾對「市場和政治的複合體，能確保數位技術效益可以幫助弱勢」缺乏信心。後工業時代開發中國家的成功故事（利用低工資製造業累積的資本，發展高附加價值產業）現已不復存在，而後期的開發中國家，要在「以資料和機器學習為主的全球經濟」中取得成功，路徑尚不明確。在世界部分地區，尤其是美國和歐洲等先進國家，窘迫和流

離失所的勞工或（大多被授權或委任）技術精英勞工所造成的跨國流動正在萌芽，這將成為安全議題中一個新的重要成分。

4. 如今，最大的中介平台[4]在各地都屬於非常獨特的類別，其與政府、消費者和社會的關係需要特殊評估、關注甚或監督。一個重要的觀察是，雖然許多平台已經或即將具有全球性，但有關其社會和經濟後果的討論，仍停留在國家或地區性層面。如今獨占或寡占已成為全球對於未來市場的假設，歐洲人最為強調其負面影響；在亞洲，重點在平台所建構的說詞，以及嘗試評估該說詞「真實性」的行動對社會資本和凝聚力影響程度；美國一直致力於讓消費者獲益的市場競爭政策，對於美籍平台公司如何影響美國以外的社會和經濟，幾乎看不到（也不關心）。

   儘管運算架構（computing architecture）的變化會推動變革，但在 2025 年情境中，這些當代的觀察仍保持高度說服力。顯而易見的是，競爭政策和網路安全政策在許多方面正在趨同，這一趨勢也將各國競爭政策發展途徑的差異納入安全領域之中。

5. 網路安全領域的挑戰，從保護網路和資料庫不受主權或犯罪者侵害，正轉變成保護其免受不當操縱。暴力攻擊仍是重要議題，但是攻擊的複雜度將上升，並且採取更隱蔽的管道，例如對抗性的機器學習（adversarial machine learning）、精巧的深度偽造（deep fake），或簡單改變訓練資料以誤導演算法。這將加速網路安全成為更具科學意義領域的趨勢，但也將對已經承受巨大壓力的資安人員帶來更多的負擔。亞洲比其他地方更重視「大規模的社會適應力計畫」這種應對措施；在美國，消費者和使用者大多數仍然處於被動狀態，「將其教育成為更精明的資訊消費者是可能的」這個概念仍然僅處於萌芽階段。或許將更多的負擔交給具有人工智慧的自動化系統是另一種可靠的方式，這樣的方式與人類決策應維持那些角色和控制存在本質上的差異。

階段 4：下一步是什麼？

根據這些觀察結果，我們認為在未來幾年，政府和民間制定資安策略的決

---

[4] 譯者註：如 uber 或 Airbnb。

策高層，除個別處理下列問題外，也應相互合作。雖然這些不是特定產業或國家在執行層面上的問題，但其答案和假說應能在快速發展的環境中，為打造更加穩健的營運計畫提供參考。

- 新的非法網路黑市在哪裡發展？市場上交易的是什麼？
- 罪犯的定義是什麼？這些定義之間，可供套利的差異是什麼？
- 有哪些新的地緣政治聯盟成形與出現？我們如何理解國家和社會內部利益分化所造成的細微差別？這些細微差別將會影響這些聯盟所採取的方向。
- 不同的社會能夠吸收多少因數位化所加劇並（或）誘發的不平等？以什麼樣的速率進行？
- 哪裡有先發優勢？技術方面如此，但政策方面亦同嗎？
- 什麼特質會使社會對數位操縱（digital manipulation）具有抵抗力和復原力？如果員工、消費者和公民需要在 2025 年的網路安全領域中成為較不被動的角色，他們需要獲得哪些新的能力，及如何獲得這些能力？

解決上述問題應該是各國公私部門的管理高層、董事會和政府機構在 2019 年應該關注的重點。

情境說明

情境 1：量子運算的飛躍

2025 年，首批達成量子運算實用化的國家，近年來致力於建構一項不擴散機制，以維持這項技術所產生的經濟、戰略和軍事優勢。但競爭落後的其他國家（甚至大城市），拒絕以限制發展為代價，來換取由少數供應者所提供的不完整量子服務，反而轉為試圖追求「量子自治（quantum autonomy）」。技術發展幾乎加速到無視道德，經濟和其他社會政治問題，量子運算擴散到販毒集團和其他犯罪網路所組成的「全球化犯罪（deviant globalization）」領域。最後，針對政府的不擴散協議，其利益不夠誘人且威脅也不夠可怕，因此在上世代對抑制核武器擴散多少會起作用的模式，但在量子時代卻失敗了。2025 年，以美國和中國為首的國家開始設想，他們的下一步行動是否最好扭轉方向，加速向其各自的盟友推廣量子運算，以對抗量子運算在犯罪領域中的擴散。

情境 2：新的彈性空間

如今隨著安全數位技術、物聯網（Internet of Things，IoT）技術和大規模機器學習（machine learning, ML）技術的不斷發展，將混亂的人類行為透過精確的指標及預測式演算法加以理解並預測，但這是個有毒的聖杯。產生這個現象的根本原因，是人類與社會生活失去了「彈性空間（wiggle room）」。2020 年代，社會面臨與過去數個世紀截然不同的問題：以往人類對世界的瞭解不夠多，在不準確中掙扎；而如今人類對世界瞭解得過多、過於精確。安全性已經提高到一定程度，許多重要數位系統具有極高的可信度，而這也產生新的難題：高度精確的認知剝奪了讓社會和經濟生活易於管理的潤滑劑。當人無法忽視令人不安的事實，或無法達成可行的模糊協定，或者大家都明知對某些「事件」無法達成共識時，便會開始尋找新的彈性空間。他們會以操縱身分或利用多重、可變的身分來找出彈性空間。巧妙引入有益的不確定性和重新創造彈性空間的做法，符合新出現的安全疑慮和各國間持續變化的競爭態勢。

情境 3：Barlow 的復仇

隨著數位安全在 2010 年底急劇惡化，世界各地的企業和個人逐漸共同意識到，過去十年那種由政府、企業、工程標準機構等所拼湊出的規範，已經無法規範現今的數位社會。雖然大家一致認為部份的措施、零星的改革和微小的修

改並不可行，但對於如何全面重新制訂規則，也存在重大的分歧，導致兩條截然不同的道路。在部份國家，政府基本上已不對網路進行干預，而交由大型企業來管理。這如同 1996 年 John Perry Barlow「網路空間獨立宣言」的諷刺版。而在其他國家採取了相反的做法，擁抱全面的網際網路國家主義（internet nationalism），將數位力量直接視為國家權力的來源和目標。在 2025 年，兩個幾乎存在於不同面向，並可以被明顯區別的模式間，其重疊與交錯正激發出最具挑戰性的緊張關係，但也出現了驚人的相似之處。

情境 4：相信我們

2010 年代後期的數位風險，將網際網路經濟推向崩潰邊緣，促使企業採取重大安全措施，將安全功能轉移到人工智慧（AI）網狀網路（mesh network）—「SafetyNet」，此網路能夠在迴圈中偵測異常和入侵並修補系統，而不需要人工干預。當 AI 網路幫助經濟擺脫了困境，並使在數位生活獲得穩定感的同時，人們對 AI 可能會破壞勞動市場的隱憂逐漸浮出水面。儘管「SafetyNet」在許多方面風險相對較低，但新型態漏洞的出現，使得 AI 本身的安全性一直受到質疑。2025 年，大多數人覺得數位環境是支離破碎的空間：一個是不安全和不可靠的網際網路，另一個是高度安全但不斷受到監控及由演算法組成和保護的「SafetyNet」。當機構將自己的活動限縮在兩種環境之一時，可以鬆一口氣。但是許多人都在懷疑，對他們而言重要的真實特質（他們認為值得保護的價值觀），是否在前進的過程中已被踐踏了。

量子運算的飛躍

2025 年，首批達成量子運算實用化的國家，近年來致力於建構一項不擴散機制，以維持這項技術所產生的經濟、戰略和軍事優勢。但競爭落後的其他國家（甚至大城市），拒絕以限制發展為代價，來換取由少數供應者所提供的不完整量子服務，反而轉為試圖追求「量子自治（quantum autonomy）」。技術發展幾乎加速到無視道德，經濟和其他社會政治問題，量子運算擴散到販毒集團和其他犯罪網路所組成的「全球化犯罪（deviant globalization）」領域。最後，針對政府的不擴散協議，其利益不夠誘人且威脅也不夠可怕，因此在上世代對抑制核武器擴散多少會起作用的模式，但在量子時代卻失敗了。2025 年，以美國和中國為首的國家開始設想，他們的下一步行動是否最好扭轉方向，加速向其各自的盟友推廣量子運算，以對抗量子運算在犯罪領域中的擴散。

2018 年，一系列秘密行動將美國量子運算研究完全納入國防部的職權範圍，美國政府著迷於量子運算技術在軍事上應用，特別是破解傳統加密技術的能力，排擠該技術應用於其他潛在領域，並成為研究工作的重點；經由與國會合作通過大量研究預算，以及極為嚴格的出口管制措施，激起了商業界和學術研究團體的反對意見，直到他們看到可供於增加研究能量的龐大政府預算和國防資源。對部分人而言，這是與惡魔的交易；但是，給參與者足夠的經費，及加上違背政策時將面臨的法律責任，這幾乎是一筆無法抗拒的交易。

2020 年，美國國防部宣布已經打造出具備量子運算能力的電腦，政府保留了最初的設備，同時為與國防相關應用的學術研究提供了有限的使用機會。民間部門也推出量子電腦，但是其大部分運算活動都是機密的，令人懷疑美國情報和國防部門正利用大部分運算能力來破解現有的加密通訊。美國政府對民間部門的量子運算產品和服務實施了嚴格的控制，讓民間部門最初推出的量子即服務（quantum-as-a-service）受限於官僚程序的泥沼，五眼聯盟[5]國家的政府是少數例外，這更加深大眾對其主要應用的疑慮。

監控能力自然有其回報，美國及其盟友在國內外宣布了一系列對抗極端主

---

[5] 是由澳洲聯邦、加拿大、紐西蘭、大不列顛暨北愛爾蘭聯合王國（英國）和美利堅合眾國（美國）等五國組成的情報共享聯盟。

義威脅、瓦解恐怖組織和滲透外國情報行動方面的重大突破。解密似乎給了量子技術參與者一個很大的優勢，量子人工智慧（Quantum-enabled artificial intelligence）也促進了網路安全能力的重大改進，為政府與私人所受到的網路攻擊提供靈活的防禦，可以對攻擊者做出近即時（near-real time）的反應，並幾乎能夠立即用攻擊者混淆代碼的固有方式進行追蹤，將尋找網路攻擊起源的長期挑戰趨近精確科學。

使用量子運算破解加密和進行監控的正當程序還不夠紮實。美國的政策決定機構仍然深陷於有關《外國情報監視法》（FISA）和政府主導駭客行為的辯論中，尚未準備好應對技術領域重大轉變帶來的法規和道德問題。外國政府認為具有新型量子運算能力的美國情報機構無所不知，並因此開始回歸到使用更古老、更缺乏效率的通訊方式，他們常對量子運算進行分析與預測情報領域的成效感到驚訝；而大型的全球毒品和走私集團更加驚恐，同時受創於獲利大幅下滑。

對商用量子運算的嚴格控管在市場上引發長期抗議，但國防和情報界堅守嚴格控管的立場。儘管如此，缺乏更廣泛的市場參與，凸顯量子領域的先行者困境：對進一步研究的缺乏，限制了美國可為量子電腦開發的應用程式。對使用的嚴格控管，導致程式設計語言和硬體架構的擴展比預期慢得多。當商業和研究部門談論使用受限所產生的機會成本時，國防界卻著眼於這些核心知識基礎必須被保護，正如同核能技術的發展受原子彈歷史所限制，讓大眾也對量子運算越來越懷疑。

與此同時，因為限制協議的逐漸失效，歐洲對量子運算的投資在接下來幾年會加倍成長。一個法德聯合財團很快宣布其具有量子運算的能力，並且（諷刺的是）向歐盟成員國政府提供有限的服務，以回應歐盟對量子商用化的限制。2022 年，據稱中國也開發了一部可運作的量子電腦，並提供國營公司（受到嚴密監控的）使用。由於美國和歐洲的私人企業擔心中國同行的競爭，立刻要求使用下一級的運算能力，但商業利益再次無法凌駕國防和情報部門所認為的國安需要。

類似 1970 年代的不結盟運動[6]，由印度領導並聯合其他部分國家，在國際場合上呼籲量子技術是人類的共同資產，不能以規範為由進行保密，不能被個別國家擁有或用於軍事目的。令人驚訝的是，全球有許多大型的城市也加入了這一行列。當多倫多-首爾-約翰尼斯堡（Toronto-Seoul-Johannesburg, TSJ）投入追求量子能力，同時承諾對全球開放並應用在人道主義和衛生時，使得這個運動非常的前衛。

量子運算強權國則聯合起來對抗這項運動。2023 年，中國、美國、英國、法國和德國制定了一項正式的聯合不擴散協議。該協議允許在國際上銷售量子運算服務，但應限制在不具情報或軍事價值的應用上。基礎技術禁止出口，且具備量子運算能力的國家，同意共同偵測網路上未經授權的量子運算活動。

這項量子不擴散條約（Quantum Non-Proliferation Treaty, QNPT）提案，出於全球公共利益向其他國家提議，量子運算強權國在特定情況下似已準備好與 TSJ 等城市聯盟進行交易。他們在還沒詳細討論之前，就決定不要將交易擴展到非法領域及犯罪網路。有傳言稱，提華納（Tijuana）、西納洛亞（Sinaloa）和華雷斯（Juárez）[7]集團（縮寫剛好也叫 TSJ）也聯合起來，以竊取資訊、劫持網路等手段來獲得量子技術，甚至在未報導的事件中，綁架 QNPT 成員國在外旅行的科學家。

量子運算用於商業和人道主義的前景，被國防和情報目的破壞。金融服務業願意花錢在特定應用中，獲得量子電腦的運算效率，但對於將研究資料暴露在量子技術下，醫療保健等產業並不感興趣，因為擔心政府會從中得知其他資訊。

加州柏克萊（Berkeley, California）宣布成為「自由量子區」。一些學術研究團體持續強烈反對政府資助的國防研究，但是這些努力和以前一樣都失敗了。

2023 年，有無量子運算能力國家間的分裂，已成為主要國際聯盟的最顯著

---

[6] 不結盟運動（Non-Aligned Movement）：擁有 120 個成員國和 17 個觀察員國的鬆散國際組織。它成立於冷戰時期，其成員國奉行獨立自主的外交政策，不與美蘇兩個超級大國中的任何一個結盟。

[7] 提華納、西納洛亞和華雷斯均為墨西哥的城市。

特徵。最終，QNPR[8]提供有限的量子運算當成「胡蘿蔔」並不吸引人：應用程式和服務太有限，且很少有國家願意冒險讓外國政府（甚至盟友）取得他們的運算活動。同時，非法的量子地下市場依然蓬勃發展，也許有部分國家在這些活動中與販毒集團結盟，儘管沒有人能肯定，但有明確的證據顯示，有空殼組織、人頭和斷點在進行掩飾。

似乎具備量子運算能力的國家忽略了一項事實：這種技術能夠而且將比核武器技術擴散的更快、更廣泛，犯罪分子和販毒集團會堅持不懈追求量子技術。因此，不擴散機制其實並不管用。對於國家來說制裁看似合理，但沒有人準備好要開戰來阻止量子技術的傳播，即使很清楚開戰的對象。

量子運算用於商業和人道主義的前景，被國防和情報目的破壞

2024 年底，俄羅斯宣布打造出量子電腦。這是以從販毒集團竊取的工程細節為基礎嗎？技術看起來非常相似。

之後，儘管美國和歐盟威脅要實施嚴厲制裁，俄羅斯還是簽署了一項公開協定，向伊朗和印度公布了該技術的細節，使伊朗與沙烏地阿拉伯、印度與巴基斯坦的關係更加緊張。這兩個國家都向美國呼籲，讓他們同樣「武裝」這項技術，以重建量子運算力量的平衡；有傳言稱，萬一美國不接受，他們將向中國發出類似的呼籲。與此同時，俄羅斯與以色列及日本簽署了相同的技術共享協議，這兩個國家也曾經向美國提出呼籲，但遭到拒絕。

壓垮 QNPT 的最後一根稻草發生在 2025 年，多倫多-首爾-約翰尼斯堡聯盟宣布跨越量子運算門檻，打造出的量子電腦比任何國家所持有的都更為先進。不擴散機制已經失敗，而「越多越好」這種相反論點逐漸獲得廣泛認同。一種共識正在形成，真正「控制」這項技術的方法是開放給每個人使用，並將重點重新聚焦在商業和人道主義上，同時讓國防和情報部門建立國家間的威懾平衡

部分最先進的量子運算應用出現在全球地下經濟中，例如量子暗網

對大多數人來說，密碼學仍停留在失效狀態，但是日益普及的後量子密碼學已經開始在商業上產生更多的需求。美國已經開始讓部分量子大型供應商私

---

[8] 譯者註：原文中的 QNPR 似應為 QNPT。

有化並解除對其的管制，試圖在成長的、全球的量子經濟中重新獲得競爭優勢。但是部分最先進的量子運算應用出現在全球地下經濟中，例如量子暗網，對合法企業和多國政府而言這種網路的能見度和使用是有限的。量子運算能力在那裡用來強化人口或器官販賣、非法藥物和非法虛擬實境體驗的供應鏈，及珍稀動物和失竊藝術品的非法交易。

量子運算更為廣闊的前景可能在2030年後實現，但這部分發展已被命運多舛的不擴散計畫大幅推遲。量子運算尚未洗去早期被國防壟斷的公眾印象，這已成為大國和其他國家間另個爭論源頭。也許最有趣的是，在2025年，量子運算被視為推動「網路化城市概念從抽象理論走向現實」的技術突破。對於非法全球化者而言它也已成為增長的主要引擎，其利潤助長了超出合法用途、完全不受監管且無情競爭的商業活動。

新的彈性空間

如今隨著安全數位技術、物聯網（Internet of Things, IoT）技術和大規模機器學習（machine learning, ML）技術的不斷發展，將混亂的人類行為透過精確的指標及預測式演算法加以理解並預測，但在很多方面卻是有害的。產生這個現象的根本原因，是人類與社會生活失去了「彈性空間（wiggle room）」。2020 年代，社會面臨與過去數個世紀截然不同的問題：以往人類對世界的瞭解不夠多，在不準確中掙扎；而如今人類對世界瞭解得過多、過於精確。安全性已經提高到一定程度，許多重要數位系統具有極高的可信度，而這也產生新的難題：高度精確的認知剝奪了讓社會和經濟生活易於管理的潤滑劑。當人無法忽視令人不安的事實，或無法達成可行的模糊協定，或者大家都明知對某些「事件」無法達成共識時，便會開始尋找新的彈性空間。他們會以操縱身分或利用多重、可變的身分來找出彈性空間。巧妙引入有益的不確定性和重新創造彈性空間的做法，與新安全疑慮的浮現及各國間持續變化競爭的態勢相符。

「精確知識問題」開始以非常平凡的方式出現，儘管對於財產受到威脅的人來說，這似乎並不平凡。2020 年，加州波托拉谷（Portola Valley）完成感測器系統「毯子（blanket）」的部署，每一條街道和每一處地產都密集安裝含 GPS 功能的感測器，以測量溫度、水流、聲音、氣壓和其他環境品質，成為了世界上最智慧的城市。

這是一項技術奇蹟，也完全就是一場社會災難。過去長期相安無事的鄰居，開始為越界幾公分的樹枝而爭吵；該市有一半的房屋超過合法地界，現在必須重新丈量；貓狗侵犯他人住家範圍的活動，包含時間和地理資訊，被記錄下來，鄰居們會互相傳送清理資訊（和帳單）；大聲的音樂和看足球賽時的歡呼聲，所造成的噪音污染成為一種可以精確衡量的無妄之災；草坪灑水噴頭必須由極昂貴的系統取代，這些系統可調整噴灑角度和強度，以免在強風下噴灑超出邊界。

矽谷（Silicon Valley）之外的媒體對上述事件諷刺地表示，這是富人及其「第一世界」才有的極端荒謬問題，但對於波托拉谷的法院、警察局和行政機關來說，案件量在一年內增加了 10 倍，這不是件有趣的事。大眾此時才驚覺到，不知道鄰居在做什麼是維持日常生活的必要條件。全球最智慧的城市現在

變成了世界上最多爭議的城市，也是世界上最不快樂的城市之一。

經濟學者對寇斯定理（Coase theorem）[9]中的某部分很感興趣：在產權清晰、交易成本較低之下，所有這些糾紛都可以由一方向對方支付款項而達到妥善解決。依此原則，部署人工智慧系統（品牌名稱為 Coase.ai）能夠減少這些情況下投入的人力，並在爭議各方之間建立更好的平衡。但除了經濟學者外，幾乎沒有人認為這是個好方法，因為捲入糾紛的人並不會對效率經濟平衡感到興趣。他們想要的是公平、透明和道歉，有時則是對自己內心深處的不滿進行報復，這些更多是情緒上的不滿而非物質或金錢。

全球最智慧的城市現在變成了世界上最多爭議的城市，也是世界上最不快樂的城市之一。

一些規模較大的邊境市場 [10]也出現了類似議題，經濟學家 Hernando De Soto 把這種新型感測器系統當成科技銀彈，並在聖保羅（São Paulo）、拉哥斯（Lagos）和馬尼拉（Manila）附近的貧民窟建立明確的產權。建立房地產等實體資產的所有權，例如家庭實際所有且法律可交易或抵押的土地，是實現資本積累和經濟成長的手段，感測器系統透過建立產權邊界和使用細分圖等方式在此取得成功。但事實證明，De Soto 所謂的「資本之謎」根本就是人類的情感之謎：幾十年來默默分享資源的鄰居，現在為了誰「擁有」什麼而激烈鬥爭，這是因為輸贏的情緒感受而不只是資本的因素，而本應利用這些精確資料裁決糾紛的地方機構，現在卻完全不知所措。

發生在波托拉谷和聖保羅的事態，以更大規模及更嚴重的後果，在國家間的衝突中出現。最開始是在邊境地區，例如阿克賽欽（Aksai Chin），中國和印度在此已存在數十年的領土爭議；新的衝突也出現在衣索比亞和厄利垂亞之間的未定邊界、約旦河西岸、薩哈拉沙漠的邊緣；更為極端的是，隨著北極海冰的融化，北極海底礦藏的歸屬也引發了新的爭端。如今再也無法避免「誰擁

---

[9] 寇斯定理：描述一個經濟體系內部的資源配置與產出，在外部性存在的情形下，其經濟效率所可能受到的影響。

[10] 邊境市場（frontier markets）：或稱新領域市場，泛指在市場規模、政治風險、金融基礎建設、法規環境、對外國投資人開放度等方面都有許多可改進空間，也遜於新興市場的國家，但邊境市場的經濟一般而言都擁有高度成長率。

有什麼或邊界在何處」等爭議，因為產權方面不再有任何模糊性來緩和爭端。

現在此類伴隨政治和情感因素的爭端，均演變成對主權的直接挑戰。當日本清楚得知位於中國的燃煤電廠「偷」走了國民多少年的健康生活；當德州的一個城市清楚知道他們為非法移民提供基本服務花費了多少成本；當墨西哥北部的一個城市精確計算出邊境另一邊的工廠向地下水源傾倒污染物所帶來的管理成本是多少；關於這些問題，國際政治領域尚未做好準備，似乎沒有任何條約、協定、合約或交易能夠因應。

「合理推諉（plausible deniability）[11]」曾被視為無賴在政治和外交上的最後避難所，許多觀察人士認為，誠實、責任和高效將是未來的發展方向——屆時假新聞不可能再出現，因為每則政治廣告和外交訊息都帶有準確、加密和安全的相關資訊能夠準確地證明它的來源、出處和時間。而事實證明，這些期望就像波托拉谷的「智慧城市」計畫一樣天真。

在宏觀層面，人類事務中最重要驅動力的假設，也存在同樣的錯誤。在政治、外交甚至商業領域，大多數的爭端其實並不涉及經濟成本和利益的分配，因此這些爭端無法以寇斯定理中的和平談判和利益均衡解決。這些爭端關乎地位、威望和情感的力量，存在於人類的下視丘（hypothalamus）中[12]。因此大眾找到了一種不同的方式，為事務處置帶來一定的彈性空間。完善外部環境資訊的「解決方案」，是環境中加入不完美的行為者資訊。在實務中，這代表個人為自己創造了多重或可變的身分。在2010年代，這聽起來很可怕（因為大多與犯罪分子和「身分盜竊」有關），但在2020年代，這已經成為許多人所想要的，並於能負擔時即可達成。

完善外部環境資訊的「解決方案」，是環境中加入不完美的行為者資訊

網際網路和數位世界是最容易做到這一點的地方，從一開始就是如此，就像著名的《紐約客（the New Yorker）》漫畫所作出的深刻描述：「在網際網

---

[11] 是中央情報局（CIA）在20世紀60年代初創造的詞彙，用來描述高級官員隱瞞信息的情況，以便中央情報局非法或不受歡迎的活動，被公眾所知的情況下，保護他們免受影響。

[12] 譯者註：下視丘的腺體調節體溫、血糖、電解質平衡、脂肪代謝、攝食習慣、睡眠、性行為、情緒、荷爾蒙的製作及自律神經系統；作者應該是指人類並非透過理性的方式來處理這些爭端。

路上，沒有人知道你是一隻狗」。2000 年代，在擁有網際網路的國家，青少年能用網路作的事，已經遠遠超出過往青少年的標準：在生活的各層面嘗試使用不同的身分。2010 年代後期，地區衝突和水資源短缺等問題迫使眾多移民和難民跨越國界，他們發現擁有多重「真實」身分是生存的必要部分。在自由社會中，族群民族主義（ethnic nationalism）的抬頭也帶來了類似的壓力，迫使人在不同的環境下改變自己。

身分資訊公司很快就發現，生物識別技術、三要素認證和 DNA「指紋」等技術，將為合法和非法獲利提供機會。人權團體重提 Adolfo Kaminsky 的故事：在第二次世界大戰中，他偽造文件讓人改變身分，在職業生涯中拯救了成千上萬人的生命。所謂的 Kaminskers（效法 Kaminsky 的人）以偽造身分為難民開發了一系列新的數位產品；他們使用設計軟體和工業 3D 列印機等現有商用技術，研發出能以假亂真的身分證件，並接受全球的捐款以支應這項工作。對此，政府的應對策略則是提高對蛋白質「指紋」（proteomic “finger prints”）技術的投入，但這只是貓抓老鼠的下一個階段，幾個月後，Kaminskers 也找到了合成的方法。

2025 年，無論合法與非法，多重或可變身分的市場極為龐大：情報機構和犯罪網路購買了大量「拋棄式身分（burner identities）」，以用於單次使用後拋棄；有錢人會購買備用的身分資訊，以備不時之需。世界各地有數量驚人的「正常人」在使用多重身分，以制衡外在超精確資料所帶來的負面影響。

民眾在這些可變的身分中發現新的社交潤滑劑。在許多方面，相較於外在不完善資訊，可變身分更難控制和管理，因為身分與人緊密連結，此種連結也反映出人類深層的恐懼和欲望。

雖然這最初是合約和協議的問題，但現在已成為許多人的哲學和宗教信仰問題。我是誰？意識或靈魂在哪裡？對每個人來說，現在的數位世界讓這些問題都變得非常真實和具體。現在 Walt Whitman 的「Song of Myself」在世界上被廣為傳誦：

“Do I contradict myself? Very well then, I contradict myself. (I am large, I contain multitudes.)”

這句話已成為時代的圭臬。但是，政治和經濟組織從未了解管理 Whitman 式現實（Whitman-esque reality）代表什麼。買房子的「我」和投票、登機、開立銀行帳戶或登記結婚的「我」是同一個人嗎？如果答案是「部分相同」呢？如果答案不重要呢？如果答案每天都在變呢？在 2025 年，這些問題才開始浮現，更不要說解決了。

我們必須從慘痛的教訓中瞭解到，以技術實現高度透明的動機並不是為了理解行為的細節，細節不重要，重要的是要深刻理解人類的意圖，而這也正是它嚴重挫敗的原因所在。擁有準確資訊的專業或業餘觀察者，可以定義和驗證他們想要的所有細節，但無助於理解他人或自己內心深處的意圖與目標。

正因不精確和不確定性所提供的彈性空間，幾個世紀以來，讓個人的社會生活可以維持。以往為了實現更高的目標，人們會設法忽視和容忍以避免爭端。以往人們可以決定那些敏感議題（包括性別和種族差異）的可能已知「事實」社會大眾最好不要知道，或至少在大眾知道時，清楚要採取什麼行動。以往人們能以洩漏文件、傳送行為的微妙訊號、透過微笑或眨眼來確認我們都理解了某些東西，無須明示而實際面臨後果。

民眾再也無法做到與上述相同的事情。機器對機器的協議和合約現在（在經濟意義上）是「完美的」，而涉及人類時，身分議題則成為主要的缺陷，但同時也是現代社會中最重要的社交潤滑劑。這表示要解決以下挑戰：什麼程度的身分不精確是可行的，而什麼程度會是「不良行為者」的操縱攻擊。至目前為止，還沒有人知道如何回答，因為這個問題至少部分涉及了人類內心的意圖。

Barlow 的復仇

隨著數位安全在2010年底急劇惡化，世界各地的企業和個人逐漸共同意識到，過去十年那種由政府、企業、工程標準機構等所拼湊出的規範，已經無法規範現今的數位社會。雖然大家一致認為部份的措施、零星的改革和微小的修改並不可行，但對於如何全面重新制訂規則，也存在重大的分歧，導致兩條截然不同的道路。在部份國家，政府基本上已不對網路進行干預，而交由大型企業來管理。這如同 1996 年 John Perry Barlow「網路空間獨立宣言」的諷刺版。而在其他國家採取了相反的做法，擁抱全面的網際網路國家主義（internet nationalism），將數位力量直接視為國家權力的來源和目標。在2025年，兩個幾乎存在於不同面向，並可以被明顯區別的模式間，其重疊與交錯正激發出最具挑戰性的緊張關係，但也出現了驚人的相似之處。

建立網際網路社會的時機還能再推遲嗎？這是網際網路協會（Internet Society）於 2020 年 12 月在巴林的麥納瑪（Manama）所舉行的多方利害關係人會議上，所有與會代表都在思考的問題。會議的共識是不要再對網際網路抱持美好的想像，更精確地來說，假裝它是美好的，這樣的想像做為數位世界的特徵，已經持續至本世紀的第二個十年。2020 年是 Homebrew Computer Club 成立 45 周年，也是 TCP/IP 成為 ARPANET 唯一核准的通訊協定 38 周年，但即便經過這麼長的時間，這些也未成為網際網路「制憲會議」的真正推動力，而是2019年的事件超過公眾容忍極限這件事情，成為真正的推動力，也致使網際網路時代的古老神話再也無法維繫。

關於成長的好消息是：2019 年，全球市值最大的 11 家公司，首次全部由數位技術公司包辦（6 家美國公司、4 家中國公司和 1 家韓國公司上榜），中國電子商務占零售產業銷售額的比例飆升至 50%以上（在美國，這一比例達到25%），全球網際網路普及率達到75%。但2019年也是數位安全崩潰的一年，網際網路被廣泛認為在商業、言論和社交互動上，是不及格的基礎設施。不僅僅是危險、困難、有風險或有害的，而是失敗。不僅是單一事件（網路「珍珠港」事件、對全球銀行的攻擊事件或選舉操弄事件）推動了這共識信念，而是資料洩露、網路攻擊、資訊操弄和可疑權利主張的頻率穩步上升，侵蝕了人們的信任。由歐洲消費者首先展開為期一天的 Facebook 抵制活動，導致全球流

量下降了 70%，基本上讓此平台呈現癱瘓狀態，此事件成為了里程碑；此活動在全球迅速蔓延，引發對其他數位平台和政府數位服務為期一天的抵制。

消費者對隱私、監視以及「您應該擁有自己的資料」等不切實際且複雜的論述現在被擱置，改為更簡單的宣示：對數位世界的信任徹底瓦解。如果數位社會要有所進展，則對於廣泛存在的安全議題，必須有一些重要、可見甚至革命性的作為。

對數位世界的信任徹底瓦解。如果數位社會要有所進展，則對於廣泛存在的安全議題，必須有一些重要、可見甚至革命性的作為。

Barlow 在 1996 年指出，工業時代的政府看起來像是「疲憊的鋼鐵巨人」，試圖管理一個不停想掙脫其掌控的數位世界。畢竟，19 和 20 世紀政府組織的設計，如 Max Weber 的主張，是以掌握細節和可預測的過程來尋求控制；然而大規模的資訊網路過於複雜和動態，無法以這種方式來掌控。

這一點在迅速惡化的公部門網路安全中變得非常明顯，而各國政府已經對這種失衡感到極度厭倦。在 2025 年，政府是數位世界的溫和監管者和寬容裁判的樂觀想法（提供足夠的資源以供發展，而不妨礙民營部門的創新），已經不再適用；提及官僚控制對數位網路的態度時，結論是「要就玩真的，不然就不要做」。換言之，各國政府面臨著一個嚴峻的選擇，要不就完全退出，要不就回歸強而有力的主權控制。過去 30 年以來，多數政府試圖占據的模糊地帶已不復存在，因為公民、企業和政府機構已經放棄這種態度。

這個認知開啟數位世界真正的制憲時刻（constitutive moment）[13]，社會必須做出真正的選擇，決定朝著哪個方向發展，要不朝著 Barlow 的願景發展，要不就是朝向西伐利亞（Westphalian）式 [14]的控管，而有一些選擇令人非常意外。

第一個意外是，歐盟迅速而明確地轉向 Barlow 的做法。在 2010 年末，歐洲各國政府曾試圖更密切地監管資料的使用，但面臨著一個重大而令人意外的

---

[13] 憲政時刻（constitutional moment）語出美國憲法學者 Bruce Ackerman，是 1990 年代針對美國憲政所提出的「民主二元」（dualist democracy）反思。

[14] 西伐利亞主權體系，即每個主權國家對其領土和國內事務擁有主權，排除所有外部勢力侵擾，不干涉別國內政的原則，每個國家在國際法中是平等的，是國際法的建立基礎。

兩難處境：公民和服務提供者都不希望政府干預。歐洲「一般資料保護規則」（General Data Protection Regulation；GDPR）在 2020 年的重大失敗顯示，根據模糊、不確定的隱私偏好進行監管是行不通的。於隱私問題上達成最低可行共識的努力，不僅在全球層面以失敗告終，甚至在國家層級也失敗了。歐盟各國公民對 GDPR 的強烈反對，瓦解政府聲稱保護其公民並加強社會秩序此一「執法權」的道德論述，因為公民拒絕 GDPR 模稜兩可規定的施行。民眾常說想要更多的隱私，但歐洲人在市場上的行為卻並非如此。

歐盟的隱私現在完全由企業而非政府定義，實質上，大公司的服務條款已成為商業和言論的社會合約。許多政府，尤其是在布魯塞爾（Brussels）的歐盟政府，都悄悄地鬆了一口氣，他們可以拋棄這些燙手山芋，將其從立法和監管議程中刪除。此外，由於 2025 年有 90%的公部門機構在商業雲端服務上運作其數位系統，因此這些服務條款現在同樣是政府與公民之間的合約。此模式運作良好，尤其在容許資料的使用以換取有價值的服務，因為公民已經理解、預期和接受這些服務條款。

美國轉向 Barlow 做法的主要原因與核心安全有關，其監管機構開始瞭解，對安全所制定的監管規定越多，就越鼓勵單一文化，也就越有效地為攻擊者提供指引，因為每項監管規定都成為攻擊的藍圖，而且攻擊技術在加解密的戰爭中是勝利的一方。2019 年，當部份安全通訊平台被要求開啟後門時，結果與反對者所預測的完全一致：使用者轉向了美國以外更安全的其他平台；雖然競爭仍在繼續，但數字和經濟形勢最終都與聯邦政府背道而馳，而國安局的預算也達到上限。

2020 年，美國戲劇性的轉向放鬆管制。大公司對撤回監管感到欣慰，因為他們覺得在法遵方面投入太多成本，但在解決真正的安全問題上卻做得不夠，雖然這論點肯定出於私利，但同時也存在部分的真實性。領先的公司開始在內部和彼此之間，圍繞安全議題建立起競爭文化。各公司嘗試了一段時間的「主動防禦」，但由於對風險來源的信心不足，很快導致彼此的互相攻擊。最終，這些公司落入恐怖平衡，到了 2022 年，「主動防禦」措施已很少見。在瞭解了這些界限之後，出現的是一場競爭；企業必須選擇自己的「最佳」安全層級，而市場有效地出現區隔；部分公司將「以客戶為中心的安全」設在更高的級

別，使得市場對他們的服務需求更大；許多公司在減少內部威脅方面投入了大量資金，由於對環境的控制最為有力而取得良好的成果。

許多觀察家並不意外，中國以完全相反的方向，朝著西伐利亞體系重新確立控制權前進。作為數位技術民族主義的藍圖，中國2016年的《網絡安全法》僅是個開始，到了2019年，對外國產品的日益不信任，推動了「中國優先」的技術和數位供應鏈、虛擬貨幣和數據流。網路武器和機器學習式的自主武器，已成為中國軍事投資和部署的最新領域。與政府監控計畫相關的社會信用體系，已發展到可監督民眾大部分日常生活。在北京和其他主要城市，大多數人的聲音淹沒了反對派，他們享受著快速的經濟成長，同時對西方的遭遇感到幸災樂禍。

如今中國的表現證明，確實有可能將主權、非民主控制下的快速經濟成長和技術創新結合起來。

其他國家在未來幾年面對Barlow或西伐利亞策略時將會如何選擇，印度的軌跡可能是最重要的參考信號。印度喧囂的政治經濟延伸到數位世界，似乎無法控制而註定要採用Barlow的方法…直到2021年，印度電網遭遇大規模網路攻擊，導致主要系統連續數日關閉並造成數千人死亡，這一事件的發生徹底改變了爭論方向。到2022年，印度正朝著西伐利亞綜合體的方向發展，以中國為範本並盡最大努力做好部署工作。印度的一些大公司和許多成熟的數位公民都想抵制這種發展趨勢，但在現實中他們已經失去信譽，且大多數的印度人認為，這些企業和數位公民，並未在有機會時為數位世界提供社會秩序。

2025年，仍有大大小小的國家處於觀望狀態，但從雅加達、拉哥斯和聖保羅等地的角度來看，選擇立場的時間已經不多了。其實，數位世界已經巴爾幹化（Balkanized）[15]，而且有著更為複雜的地理環境。一些「區域」受到商業提供者服務條款的管理和約束，而這些超越國界和不存在自然地理限制的狀態是20世紀的遺跡；其他地區則是由明確的國家邊界所劃分，國家主權於此的權力運作，相較於實際的國家邊界，更為嚴格、更有效率且更具控制力。

---

[15] 巴爾幹化是一個地緣政治學術語，其定義為一個國家或政區分裂成多個互相敵對的國家或政區的過程。

Barlow 世界在某些方面的表現令人稱奇。2010 年代後期經歷受政府控制的威脅，促使網際網路社群更積極建立社會合約，而非如 1996 年般輕率地假設在「自然的自我組織程序」中，會順理成章地產生可運作的社會，這正是維基百科（Wikipedia）和一些開源社群等指標範例的基礎所在。因此當政府收手，數位社會已準備好迎接其憲政時刻。作為這種成熟的指標範例，平台公司和公民協商了新的資料契約，讓個人資料的使用和定價，在每個人都能理解的單頁協議中，明確且透明的呈現。此時，網際網路使用者不再被政府保護或被公司欺騙，認為他們可以無需付出任何代價而免費獲得所有數位資源。

西伐利亞世界則以不同的方式運作；它不太符合憲政精神，而更符合傳統的力量式平衡。威懾看似限制主要的跨境數位衝突，然而它也允許持續、緩慢的智慧財產權竊取，對資料庫和金融系統的輕微攻擊，以及其他低程度衝突，這些衝突不斷提醒著次要層面存在的不安全因素。國家範圍內的物聯網系統代表過去的多邊貿易機制正在消失，因為大多數交易商品現在都支援物聯網。2002 年[16]，北京宣布中國道路上只可行駛中國自製的車輛，而韓國對國內交通實行同樣的限制，這些事實就清楚表明了這一點。2024 年，約旦和卡達指控以色列使用網路武器侵犯綠線（the Green Line）[17]，並透過關閉競爭性的網際網路伺服器和網站來有效擴大以色列的邊界。由加拿大和瑞士領導的大量談判，化解了這場特殊的危機，每個人都確信在可預見的未來會有類似的危機，但沒有人能確定這些恐怖平衡將會發展到何種程度。

在實體和數位層面上，當需要同時面對 Barlow 和西伐利亞兩種世界時，出現許多難題。這兩種集團在推動與控制的驅動力存在本質的差異，兩者之間的摩擦表現在經濟、政治、哲學領域中，甚至在軍事領域。例如，有雄心的全球平台公司面臨著一個極其尷尬的局面，他們已經獲得了在 Barlow 地區建立起自有政治經濟的極大自由，但同時他們必須在西伐利亞地區建立國家規定的半官方結構。在這兩個地區之間的技術、資料、甚至人員的轉移過程需要大量交易成本，且大多情況下完全不值得嘗試。

---

[16] 譯者註：原文中 2002 年應為誤植，可能是 2020 年或 2022 年。

[17] 第一次以阿戰爭後，於 1949 年達成停火協議所劃定的暫時邊界線。

在實體和數位層面上，當需要同時面對 Barlow 和西伐利亞兩種世界時，出現許多難題。

每個系統都會針對其他系統探測弱點和漏洞，但這是個複雜而模糊的賽局，其中風險通常大於潛在的利益。如同冷戰初期，存在著激烈的哲學和意識形態競爭，在這種競爭中，每個系統都宣稱另一個系統註定要遭到歷史淘汰。但是這些論述忽視了明顯的事實，亦即兩種截然不同的集團，至少就目前而言，在許多方面（尤其是安全）都運作得比 2019 年全球網路混亂時來得好。

這種意識形態競爭的一個主要諷刺，是雙方在重要性的考量上，工程和經濟的需要均勝過了言論及溝通。Barlow 認為，在網際網路時代，「任何人、任何地方」都能夠表達信念，而不用擔心被強迫保持沉默或順從。實際上，Barlow 地區的私人社會秩序，至少與西伐利亞地區政府定義的社會秩序一樣具有強制性。無論身在何處，經濟成長和數位安全都是相輔相成，以至於鮮少有政府或大公司會採取行動，維持多元化意見是值得為之奮鬥和犧牲的公共利益此種概念，他們最終都只希望「剛好夠」。在 Barlow 世界，任何人都可以進入任何領域，但是要留在裡面必須遵守規則（服務條款），這並非私刑正義（vigilante justice），但那些背離的人將面臨社會孤立。

在西伐利亞世界，政府提供具有足夠吸引力的消遣（例如沉浸式 VR 遊戲），來消耗大部分破壞性的政治能量。利用預測性話語分析策略（甚至有傳言稱是思想策略），對公開演講進行即時或甚至超越即時的監控。違規者不會被逮捕、監禁或遭受酷刑，他們只是失去「正常」生活所需要的數位服務，如銀行、醫療和通訊。在西伐利亞地區異議分子實際存在，他們可以自由在街上行走，但在數位空間中，他們與其他異議份子或可被說服的對象被完全隔離開來，也因此變得無能為力。

2025 年的全球網際網路，已經變得非常像一群小鎮，相當安全且大致上墨守成規，基本上不關心其他地方會發生什麼事。

相信我們

2010 年代後期的數位風險，將網際網路經濟推向崩潰邊緣，促使企業採取重大安全措施，將安全功能轉移到人工智慧網狀網路─「SafetyNet」，此網路能夠在迴圈中偵測異常和入侵並修補系統，而不需要人工干預。當 AI 網路幫助經濟擺脫了困境，並使在數位生活獲得穩定感的同時，人們對 AI 可能會破壞勞動市場的隱憂逐漸浮出水面。儘管「SafetyNet」在許多方面風險相對較低，但新型態漏洞的出現，使得 AI 本身的安全性一直受到質疑。2025 年，大多數人覺得數位環境是支離破碎的空間：一個是不安全和不可靠的網際網路，另一個是高度安全但不斷受到監控及由演算法組成和保護的「SafetyNet」。當機構將自己的活動限縮在兩種環境之一時，可以鬆一口氣。但是許多人都在懷疑，對他們而言重要的真實特質（他們認為值得保護的價值觀），是否在前進的過程中已被踐踏了。

精通電腦的罪犯能夠從數位系統中竊取敏感資訊，已經不是什麼新聞；2017 年，多起備受矚目的攻擊事件，如 Mirai Botnet、WannaCry、Petya，都再次明確顯示，網際網路可能是各種活動的危險場所；2018 年，隨著嵌入式硬體漏洞成為明顯的攻擊點，民眾對網路連線技術的信任持續下滑，並假設遲早會有一個發生「大事件」的轉捩點出現。每個人似乎都在等待那一刻，看它將如何定義更廣泛的網路安全議題。

然而，大眾輿論中的轉捩點並沒有到來。一個根本原因是數位攻擊持續騷擾政府和公司，而非一般人。2018 年，大多數國家的網際網路一般使用者和數位消費者，都沒有經歷過夠大的、重要的個人負面影響。重辦信用卡是小麻煩，而身分盜竊則麻煩一點，但都不是很大的危機。假新聞、資料操縱及對基礎設施攻擊的威脅，仍然抽象的或是有點距離的問題，這是其他人需要擔心的議題。對採取深度行動的需求並沒有那麼廣泛，也沒有政府、技術專家、企業和民間社群提升危機意識（或部分人所謂的製造恐懼）以促成改變。就像史達林對死亡的名言，一份被盜的資料記錄可能是一場悲劇，但是 8700 萬份被盜的資料記錄就只是統計資料，這些都太抽象而不具體，並無法改變大眾的觀點。

直到 2019 年，一個跨國犯罪組織肆無忌憚地宣布，已發現容器軟體（container software）中存在零日漏洞（zero-day vulnerability），可以大規模

存取個人電子郵件帳戶。駭客公開了 11,000 個隨機 Gmail 帳戶的完整電子郵件歷史記錄，揭露了大量隱藏的事件、不可告人的懷孕訊息、金融騙局和其他醜陋的個人資訊和祕密，並威脅要按順序公布其他 Gmail 帳戶的完整歷史記錄（週一公布 A、週二公布 B 等等）。由於是公開敲詐勒索，整個事件給人的感覺不同，犯罪分子對他們所處的境況非常有信心以至於毫無掩飾。他們在世界各地的主要報紙，刊登整版廣告提出贖金要求；一些受害者支付贖金，而拒付贖金的人發現，他們的銀行和醫療資料，依駭客所說的精確時間表被公布出來。

現在這種威脅已攤在陽光下，並在正常人的生活中如影隨形，而大眾的反應是緊急且有組織地退出敏感交易的線上系統。在主要醫療機構取得紙本病歷的排隊時間，拉長到好幾個小時；銀行重新開放了關閉的櫃檯；傳真機從倉庫中被取出。傳統媒體意識到有機會奪回一些市場支配力，因此增強了此核心論點上的聲量：網際網路上的任何東西都能且將被用來對付使用者。突然之間，任何捍衛網際網路自由的人都可能會遭到網路霸凌而噤聲。

容器軟體供應商（尤其是在美國和中國）試圖反擊，阿里巴巴、Amazon、Docker 和 Google 聯合發布由公司認證的軟體更新（並得到美國和中國相關政府機構的認可），以防止在接下來的六個月內遭到未經授權的存取。但是，儘管在技術上合理，恢復信心的善意努力在壓力下並未堅持下去。2020 年初，Snapchat 遭到一個熱門第三方驗證應用程式中發現的新漏洞所攻擊，犯罪分子利用電腦視覺技術進行偵測，並張貼出含有數千張裸照的可搜尋資料庫的連結。雖然身分驗證程式漏洞與容器軟體缺陷並無直接關係，但大眾認為沒有差異，他們只覺得又一個重要的承諾破滅了。沒有任何制度性的保證可以彌補大範圍攻擊向量，政府迴避任何進一步的努力來增強大眾對私人解決方案的信心。2020 年底，相較於 2018 年，網際網路已經變得有些黯淡，這並非大規模的關閉：線上遊戲繼續激增，因為玩家並不在意遊戲結果是否公開；紀錄健身資料和類似資料的網站也是如此，因為大眾把精力集中在他們真正想要保護，並認為能夠保護的少數事情上。在網際網路上的被動觀看活動持續成長，包含電影、YouTube 和其他媒體；色情網站的存取頻率較低，因為這些網站的造訪記錄會首先公布給造訪者的家人，然後向大眾公開。

在這波事件的轉向中，令人驚訝的是，在某種程度上引起更大範圍的社會文化運動，此運動旨在抗議數位經濟所致的非數位影響。例如在美國和歐洲，人口向密集城市中心轉移的趨勢開始改變，大眾在城鎮中看見新的商業契機，這些城鎮缺乏網路商業機會而需要實體商店。加州的貝克斯菲爾德（Bakersfield）、英國的赫爾（Hull）和德國的德勒斯登（Dresden）是 2021 年人口成長最快的三個城市。

但是研究界並沒有失去信心，而且有很好的理由：柏克萊大學、麻省理工學院和卡內基梅隆大學安全實驗室內的人工智慧平台，在分析能力、自我導向反應和發展自身學習機制方面超越了所有人的期待。當學者們爭論 AI 是否真的具有資格被稱為「泛用智慧」的時候，2021 年公開的測試版中，其快速的學習能力以及「學習如何更快學習的能力」震驚了世界。這款 AI 在 2022 年以開源形式公開發布，一夜之間，它就從技術上的新奇變成了歷史上重要的熱門軟體。

網際網路平台的大型公司抓住這個機會，將本身的產品建立在此開源 AI 系統上，而不是強化產品本身，以一種能重新贏得市場的方式，將可行的安全性恢復到其產品和系統中。原始軟體中安全面向的部分，目前在 AI 的支援上有著最為迫切的需求。2022 年，暱稱為「sAIfety」的資訊安全 AI，已被世界的主要網路公司所安裝，並且安全專家宣布了為企業部署提供服務的計劃。但為了能夠更快得學習，AI 對知識有高度渴求，因此，幾個月後大眾就清楚認識到，讓 AI 在許多服務上分別運作並不是最佳選擇。

隨著大型科技公司制定出一系列標準，允許去中心化網狀網路的 AI，可以共同觀察彼此的服務活動，這前景顯得樂觀。此架構支援在服務之間快速分享訊號，並形成一種行為資訊的結構，在這行為資訊的結構下，可逐漸識別不良行為者、標記遭利用的漏洞，以及不需人工介入即可進行系統修補。Facebook、Google、Amazon 和 Microsoft 幾家公司聯合宣布將推出網狀網路，為其他採用者打開了存取巨大智慧訊號流（intelligent signal stream）的大門。隨著網路的擴大，人工智慧網路的誤報率大幅下降，Google 宣布帳戶遭竊情形減少 90%；美國各大銀行也自豪地宣稱身分盜竊減少了 95%；在 2023 年，FBI 利用安全 AI 網路所提供的新電子證據，成功起訴了網路罪犯。

之後，支付公司 Stripe 抓住了創造市場的機會。Stripe 援引 AI 網路在許多主要平台上的成功，宣布對於任何不符合 AI 新安全標準的客戶，將停止付款程序。接下來，Stripe 推出了一項認證業務，對服務中進行觀測的 AI 配置進行稽核，並向符合標準者頒發電子證書，亦即信任標章─「SafetyNet」。Visa、MasterCard 和中國銀聯等其它支付公司也很快跟進採用同樣的標準。

這款 AI 在 2022 年以開源形式公開發布，一夜之間，它就從技術上的新奇變成了歷史上重要的熱門軟體。

2023 年競爭已全面展開，世界各地的公司在其網路和服務上，實行以 AI 作為驅動力的資訊安全。SafetyNet 的稽核不僅關注是否遵守部署 AI 的步驟，也重視是否遵循 AI 提出的建議和修補。傳輸層安全性協定（TLS）[18]、多重身分驗證和其他被普遍接受的安全性技術，被採用的比率急劇上升，但真正重要的是人工智慧系統。Amazon、阿里巴巴、AWS 和 Google 都提供代管的 AI 安全服務，即使再小的企業也有機會獲得 SafetyNet 的信任標章。銀行和醫療記錄轉向 SafetyNet 聯盟的服務商，敏感的個人通訊也是如此。專家們對網路互動信心的恢復而歡欣鼓舞，認為 2020 年代初期離線運動是一種短暫的干擾，同時這個例外反證一條規律：數位永遠是贏家。

AI 在打擊網路犯罪方面的成功，也為該技術的其他許多應用鋪平了道路，這些應用不僅獲得接受，而且受到高度期待。在企業內部配備 AI 數位助理，去除了傳統的網際網路干擾，使得經濟生產力大幅提高，而這種技術幫助員工專注於「最重要的事情」。大多數人並不認為 AI 主宰了他們的觀點，或以企業的視角來篩選資訊，而認為這種技術確實有用，是豐富日常生活的助手。例如在日本，公營的養老院將 AI 整合到公寓中，該系統在使用者看來就像是老朋友，或患者家屬推薦的其他熟悉人物；AI 能夠記住每個人的偏好和行為，並提供持續的反應和鼓勵，這是人類照護員無法達成的；這個計畫從各個方面來看都很成功：患者的幸福感和身體健康指標都有所改善。2024 年，一家總部位於肯亞的資產管理公司宣布，該公司完全不依賴人類員工運作了 6 個月，而這段時間

---

[18] 傳輸層安全性協定（Transport Layer Security；TLS）及其前身安全通訊協定（Secure Sockets Layer；SSL）是一種安全協定，目的是為網際網路通訊提供安全及資料完整性保障。

的業績超過了美國所有大型共同基金。舊金山（San Francisco）一家日間照護公司宣布，計畫開發一種 AI 看護服務，而早期的試辦結果顯示，這是彌補學齡前教育預算和人力不足的有效解決方案。

但我們也要看到黑暗的一面，學術研究人員逐漸發現，使用者對數位助手的本質感到困惑：他們有知覺嗎？他們有生命嗎？有意識嗎？這些有沒有關係？據說與個人使用 AI 相關的疾病，包括社交退縮、依賴和性方面的強迫症。到 2022 年，AI 抗拒者（在 2020 年被視為懷舊浪漫主義者）已開始在全球擁有大量擁護者，一些人擔心，將與 AI 的無機互動視為理想，會削弱我們對不完美人際關係的感知，無論是在情感、知識還是生理領域；其他人則擔心，對 AI 的癡迷正取代與上帝建立關係的時間。還有一些人擔心，依賴 AI 作為所有問題的解決之道，會危及人類的自立能力；更讓人擔心的是，那些曾經被認為是邊緣的、哲學的，或抽象思想家的杞人憂天，正在成為對數位技術焦慮的主流。

學術研究人員逐漸發現，使用者對數位助手的本質感到困惑：他們有知覺嗎？他們有生命嗎？有意識嗎？這些有沒有關係？

「這一切代表什麼?」這個哲學問題對部分人產生了重大影響，但安全方面的改善帶來了不可否認的經濟效益，2023 年在 AI 的引領下，網路經濟重回正軌。

但不久，一個更具毀滅性的打擊擊中了 SafetyNet。大眾開始看到政府利用新的 AI 系統來獲取（不公平的？）優勢，降低大眾對該技術的信心，並且削弱了該系統的價值。2023 年末，在柏林一宗針對網路罪犯的重大案件中由 AI 自行說明，大眾對 SafetyNet 就被告詳細資訊的了解程度，及起訴書中這項具有科幻本質卻又平凡地出現的指控感到震驚。且 SafetyNet 更早前已預測，這名罪犯之後從事網路犯罪的可能性為 99%，並要求法院在犯罪前實施懲罰。

上述事件看似僅為《關鍵報告（Minority Report）》式科幻小說，但當 AI 本身不再繼續將演算過程保密，而將透明性作為其法律策略的一部分時，卻產生極大的煽動性及情緒性。對許多人來說，這更像是一種操弄，而非真的讓人安心：我們為什麼要相信 AI 會說出關於它自己的真相，以便讓你放心？尤其是機器也在告訴你，它確切知道你想聽到的是什麼！

大眾對這個轉變迅速產生了強烈的反對，要求知道企業和政府如何使用從 SafetyNet 取得的資料。AI 再次準備好回答所有這些問題，並以完全透明的方式解釋自己。它認為自己沒有什麼可隱瞞的；對人類而言，它愈透明，就愈快了解如何以人類無法表達的方式為人類服務─至少 AI 是這樣說的。

美國的民眾試圖向 AI 解釋，他們不要 AI 自我解釋─大多數人無法理解 AI 的自我解釋。諷刺的是，美國民眾希望政府來做解釋，而中國人似乎也希望如此。幾乎所有人現在都同意使用「紅旗規則」，要求 AI 的互動必須用紅旗標示，以向人類清楚說明電話另一端的聲音（或文章、影片的作者）其實是機器而不是人。但是可以信任 AI 能把自己貼上 AI 的標籤嗎？誰可以被信任來做這件事？如何驗證？

在對人類使用者究竟想獲得什麼有更多瞭解及時間允許下，SafetyNet 也許能夠通過這些障礙。但是它沒有得到這個機會，因為出現新型且由政府主導的網路攻擊，其利用系統中 AI 無法識別和修補的漏洞以進行攻擊。

2024 年初，俄羅斯情報部門的一次大規模洩露事件顯示，該國的情報總局（GRU）已獲得對數百萬個 AI 應用程式的廣泛控制（包括 SafetyNet 的骨幹），並利用這些 AI 應用程式在前蘇聯的衛星國家引發社會動盪，例如，在捷克引發了反斯洛伐克情緒。美國當局的調查表明，AI 操控與即將舉行的總統選舉之資訊安全有關，美國國會迅速採取行動，通過了影響重大的「外國人工智慧標記法（FAIFA）」，強制將使用外國資料或系統的 AI 必須標記為非人類。

「紅旗」概念發展為人類共同傳統理念，還是一年前的事，它可以幫助世界各地的人管理其與機器的關係，但現在已經變為其他目的。它已成為政府推動科技國家主義進程（techno-nationalist agenda）的一部分，試圖用來將外國 AI 拒之門外。

不出所料，俄羅斯政府採取報復行動，並透露美國國安局一直在利用 SafetyNet 中不同的漏洞，對外國人採取針對性的暗殺行動。最令人不安的是，似乎美國國安局使用這種方法改變數位助理產生的資訊，以提供危險的駕駛指示、不準確的醫療建議，或教唆目標採取自殺行動。

大眾不信任 AI 並非因為不理解，而是確實瞭解它的強大。

2025 年似乎存在兩個網際網路：一個是受 AI 保護的 SafetyNet，在這種網路中，至少不會發生的身分盜竊、欺詐和資料洩露等低等級的傷害。另一個是不安全、經常受到破壞的網路，這種網路只有一些不太重要的資訊。但是，SafetyNet 卻被政府（尤其是情報機構）的某些行為所破壞。儘管不信任這兩類網路的原因有所不同，但其影響程度大致相同。大眾不信任 AI 並非因為不理解，而是確實瞭解它的強大。大眾也不信任由人類決策支配的機構，因為 AI 已經揭露相當多握有權力之人的基本動機和意圖。皮尤研究中心（Pew Research Center）於 2025 年 1 月進行的一項調查顯示，全球公眾輿論認為，在兩種網際網路環境間的選擇，並不是在「安全」和「不安全」之間選擇，而是選擇以誰作為對手。

本報告中譯本，特別感謝 2020 年 3 月間，李育杰執行長率領 TWISC 訪問美國加州柏克萊大學長期網路安全研究中心時之提議，以及該中心 Ann Cleaveland 主任之翻譯授權。

TWSC