



Inspired by Stephanie Franziska Scholz's cover of *The Economist* - 3/19/2020

後疫情時代網路安全的未來

The Post-Pandemic Future of Cybersecurity

台灣資通安全研究與教學中心 TWISC@AS 譯

後疫情時代網路安全的未來¹

Published in CLTC Bulletin·Aug 25 2020

An Imperfect Patchwork	4
Party Like It's 1999 (or The Roaring 20s)	7
Analog Investment	10
Global Singapore	12

¹ 原文網址:

<https://medium.com/cltc-bulletin/the-post-pandemic-future-of-cybersecurity-7956c6c1292f>

後疫情時代網路安全的未來

Charles Kapelke

數位安全如同生活中許多層面，對比於 2020 年疫情危機，產生了重大或根本的轉變。我們現在如何開始為新世界將出現的新興挑戰和機會做好準備？



自成立以來，加州大學伯克萊分校長期網路安全研究中心 (CLTC) 透過全面性的思考，未來 (或更確切地說，多種可能的未來) 所塑造各種人類-科技互動過程將以何種形式衝擊網路安全，作為形成研究計畫的依據。

當 CLTC 於 2015 年成立時，我們使用一種稱為情境規劃的正式流程，以發展出展望 2020 年的敘述。當我們預見到許多趨勢時，或許錯過了一些，這些初始情境幫助我們預測出，如強大的預測演算法、物聯網及數據市場擴展等趨勢。大約四年後，我們發展了一系列用以展望 2025 年的新情境，評估強大的人工智慧、量子技術和無處不在的感測器等新興技術之潛在影響。

現在，在 COVID-19 大流行的前幾個月 (及其造成的社會、政治和經濟動盪) 中，CLTC 的團隊成員為 2025 年制定了一套新的情境。在 CLTC 主任 (faculty director) Steven Weber 的帶領下，CLTC 團隊發展出「關鍵不確定性」亦即可變的驅動因素，這些因素在形塑後疫情世界具有決定性意義。我們使用結構化的情境規劃流程，考慮各種力量 (社會、技術、經濟、環境、政治和軍事) 的碰撞，如何在未來五年內重塑我們的世界。

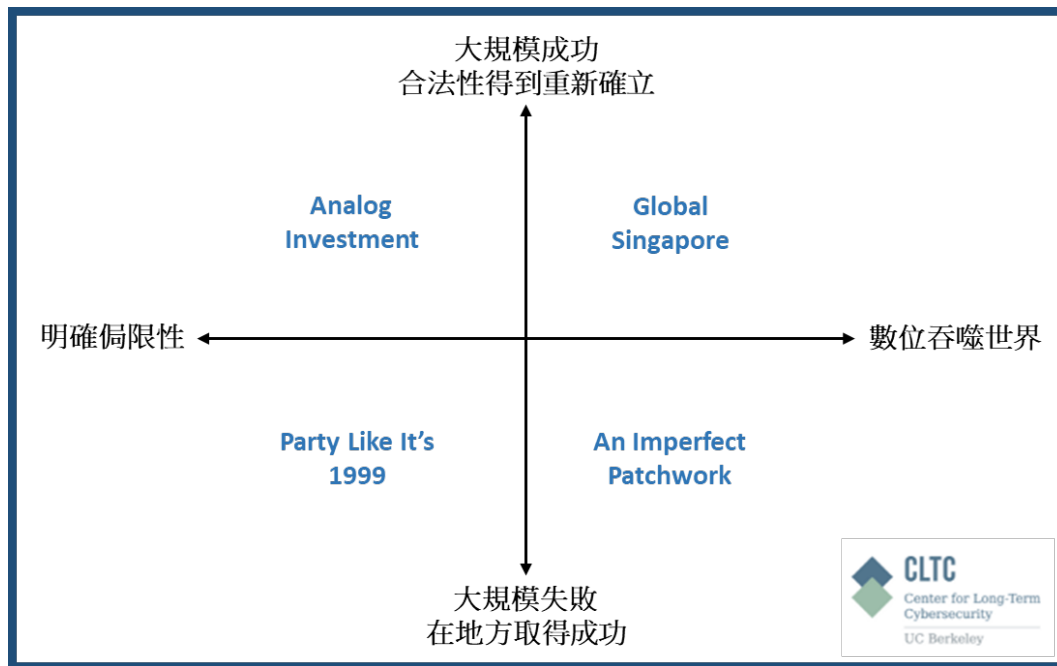
由於僅聚焦在我們最了解的國家 - 美國，這項工作在某種程度上受到限制；因為這裡的見解，部分是由前述的焦點所形塑，所以如果將此見解推廣到其他地區，則應將其視為初始假設。

我們首先提出一個明確、至關重要卻被忽視的問題：經過數月被迫使用線上會議後，疫情過後技術的使用是否會衰退？還是我們將會進一步融入虛擬領域？

當 COVID 追蹤應用程式出現後，人們是否會願意為了更好的公共衛生而犧牲隱私權，使得新的監視時代來臨？疫情是否會導致全球合作的增加？或因零和心態作祟，致使民族主義和其他狹隘的利益引發進一步分裂？疫情會如何改變大眾對氣候變遷的態度或當地社區的角色？與我們的研究最相關的是，這些轉變將如何共同塑造數位安全的未來？更廣泛地說，人類與科技間的關係？

最終，我們聚焦於兩個可變關鍵因素的交點，這似乎掌握了許多可能定義未來幾年的重大議題。第一個因素涉及數位科技是否（以及如何）繼續主導我們的生活。在光譜的一端是「數位吞噬世界」，因為科技運行良好，我們進一步沉浸其中並將生活轉移到線上空間。在另一端是「明確侷限性」 - 社會將數位科技的迷戀，限制在生活中真正造成改善的地方，而在物理世界的其餘特定領域，數位化的限制變得極度明顯。

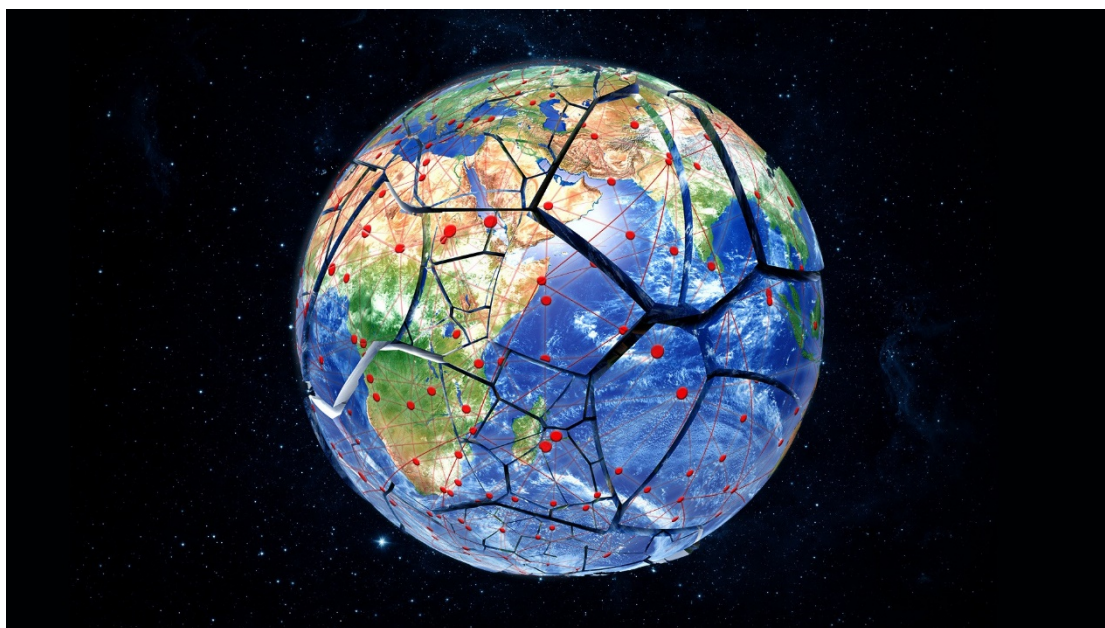
第二個因素相對於美國和世界各地的國家政府在推動社會發展方面，是否（以及如何）建立並保持強大的作用（「大規模成功，合法性得到重新確立」），或中央政府的衰落，讓地方政府自我發展（「大規模失敗，在地方取得成功」）。



這些情境基於兩個因素：數位科技是否（以及如何）將繼續主導我們的生活；以及各國政府在推動社會前進方面，是否（以及如何）建立和保持強大的作用。

當然，從這兩個關鍵不確定性的相互作用中，所出現的敘述都不可能是「正確的」。這些情境不是要進行預測，而是要產生假說。因此，最好將這些故事作為啟發，以幫助我們更清晰地思考可能發生的情況。與往常相同，我們的目標是運用長期的思維來闡明這個問題：**如果這個未來真的實現，我們會想在 2020 年致力於哪些網路安全議題？**如果這些假說令人信服，那麼決策就很清楚：讓我們現在就著手解決這些問題。

An Imperfect Patchwork



疫情導致的衰退下，各國政府面臨預算緊縮，以及處理漸趨科技化社會²的能力不足。朝向數位社會的轉變仍持續進行，但並非全無不利之處。學校使用線上教學、醫護人員轉變為遠距醫療，但造成品質的下降。在不同地區中，方法和標準的差異導致效率低下。

Sammy Patel 醫師每天對 40 至 50 名患者實施「診治」，從毒橡木疹到流行性感冒，均在他位於內布拉斯加州奧馬哈的起居室。Patel 是 21 世紀的「鄉村醫生」，透過操縱手機上的鏡頭，利用 Zoom 提供諮詢服務對患者進行相關指導。

「最難的部分是需要看病人背部時，沒有人可以協助病患。」Patel 如此說「借助現行的個人診斷工具，我無需到場就可以治療約 75% 的患者。醫療品質可能不如往常，但很方便。」

Patel 醫生的遠距醫療，是過去五年這個世界如何「虛擬化」的一個例子，這一切在 2020 年的 COVID-19 疫情中加速轉變，從大學到火人祭(Burning Man)³都被迫轉移到線上舉行，但這樣的轉變速度可能快到難以掌控。

即使在 2022 年「完全控制」冠狀病毒後，民眾還是選擇留在室內並避開公

² 科技化社會(technology-based society)：透過社群媒體、網路等機能，取代傳統社會互動方式所構成的社會型態。

³ 火人祭是一年一度在美國內華達州的黑石沙漠舉辦的活動，九天的活動開始於美國勞動節前一個星期六，結束於美國勞工節當天。

共場所，大部分的原因是民眾懷疑政府的能力。商用不動產的價格已經崩潰，從橋牌俱樂部到保齡球等社交活動主要透過數位化進行。全國各地數百所私立學校都放棄了實體課程，與此同時，法定必須接納所有學生的公立學校則一直在努力適應：K-12 考試成績在 2024 年跌至歷史最低點，專家將此責任歸咎於數位教學。

數位化的需求極大，因為網路世界比以往任何時候都更加支離破碎。疫情導致的衰退下，政府協調基本服務的能力有限，對於技術（以及大多數其他領域）的監管薄弱，導致有關隱私和數據保護的規則混亂不堪。儘管主要數位平台在建立標準方面做出了最大努力，但眾多的差異導致效率低下。美國各州試圖獨自管理日益活躍的線上世界，但這通常導致困惑和混亂；例如在 2024 年初，由於數位識別系統不相容，新墨西哥州的州際卡車司機被亞利桑那州拒絕進入。

許多企業在準備就緒前就被迫使用線上系統，以至於未能建立穩固的安全性，更不用說維持了。勒索軟體和其他攻擊已成為「正常」生活的一部分。亞馬遜在 2023 年的資安事件 - 當公司 100 億美元的虛擬貨幣神秘消失時 - 突顯了治理支離破碎、毫無規則的網際網路所面臨的挑戰。當駭客主義者發布了數十次《Fortune 500》董事會會議的視頻時，這不僅震驚了股市，而且引發了新問題，在於有關科技巨頭保護最重要消費者的能力。

將 5G 整合到物聯網 (IoT) 中，可提高供應鏈效率。但它導致了無數不安全的端點，而強烈擔憂是否造成「積勞成疾(death from a thousand cuts.)」的後果。在被譽為「LAN 的復仇」(或區域網路)中，許多社群已經放棄了基於雲端的解決方案，轉而運營自己的網路以求可更好地自保。

這些碎片化的主要好處是，儘管數位「輕罪」正在上升，但有系統的災難性網路攻擊風險已降低。對民族國家的攻擊已相對不重要，因為後果不再嚴重，除了少數幾個積極防禦的著名目標以外；但對大多數用戶而言，安全性卻進一步受到侵蝕，物理和數位世界的犯罪率都在上升。

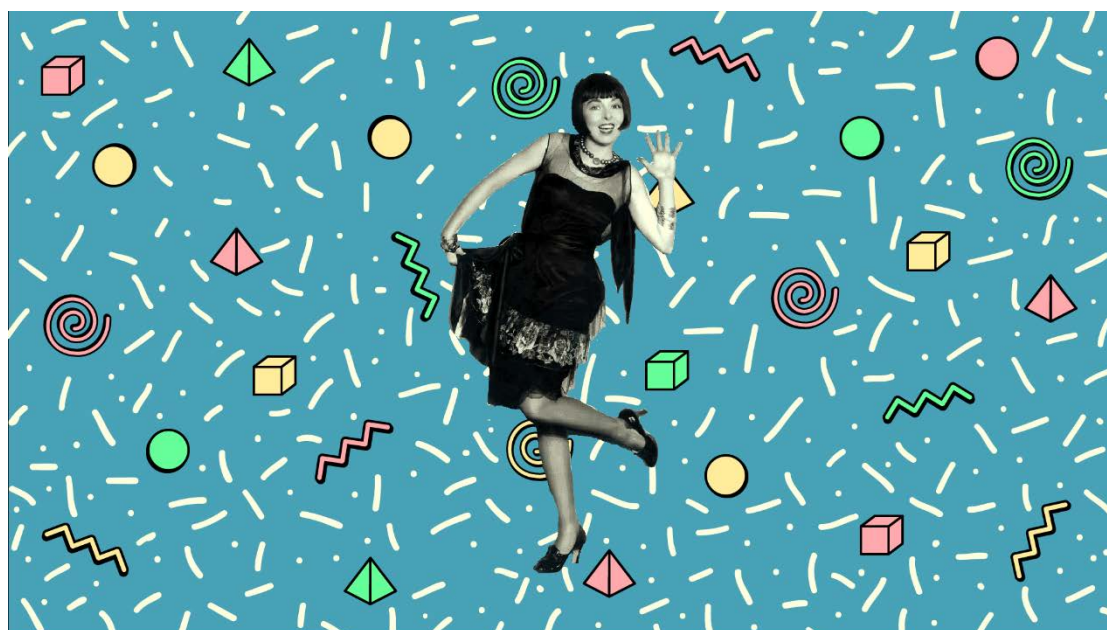
「他們曾經說過『我們是生命共同體』，但是現在聽起來很傻。」前酒保 Martha Johnston 說，他目前在網路進行調製雞尾酒的線上課程。「現在，現在全靠 Nextdoor 了解發生了什麼事，躲起來、保持門上鎖以及確保密碼夠安全。」

如果這個未來真的實現，我們會想在 2020 年致力於哪些網路安全議題？

如果這個未來真的實現，或可建立一套共同指標，來評估升級和/或降級的風險與效果，並反映到各種經濟部門和其他人類活動，以便隨時根據標準化的成

本效益分析，決定是否將特定活動網路化。在某些情況下，經過風險調整後，感染 COVID 的負擔可能比網路化的負擔更可接受。2020 年夏季，在學校是否開放的決定中，即因缺乏這一指標而產生困擾。

Party Like It's 1999 (or The Roaring 20s)



經過幾個月僅能使用 Zoom 與其他線上互動的隔離，隨著疫情的消退，社會立即衝出了數位領域，人們急切地回到了現場活動和面對面的互動中。各國政府已進一步陷入功能失調的境地，面對數位世界的疲憊和幻滅，社區和公司不得不獨自面對網路安全和其他挑戰。

自世界屈服於 COVID-19 以來已經過去了五年，儘管這種病毒可能已得到控制，但全球經濟仍處於衰退之中。諷刺的是，實體零售再次飆升，大型購物中心再度風靡，而像 Amazon.com 這樣的數位巨頭經歷了股價暴跌。

「五年前飛漲的數位業務一直努力從泡沫中復甦。」 Kitari Investment Group 的投資分析師 Jorge Padrio 說，「疫情將顧客推到了他們不真正想要的地方，因此他們一有機會就逃走了。」

起初，自然環境也有所好轉，因為 2020-2022 年間碳排放量急劇減少；但隨工業復甦和汽車使用回到原來的狀態，污染也逐漸回升。「有幾個月裡，我們可以在公寓裡聽到外面的鳥叫聲，」加州爾灣 (Irvine, California) 的屋主 Heather Jones 說。「確實有這樣的感覺，就像是，實際上這就是應該的樣子。」

疫情引發 Zoom 的使用和網路外送宅配的激增，暴露了全數位生活(all-digital life)的嚴格限制；隔離帶來的疲憊及對科技感到精疲力盡，美國人在有機會的瞬間，便回到面對面的互動。與「慢食」運動類似，「慢科技(slow tech)」運動導致數位設備的使用急遽減少。2022 年，# LookUp 主題標籤在 Twitter 上出現短暫的

流行，隨後傳達以下訊息：「拋棄手機，重新加入身邊的現實世界」，使社交媒體本身吸引力下降。紐約和其他市區的一些酒吧和餐館已開始提供「養機場(phone checks)⁴」，以幫助客人放下電話。串流視訊的收視率直線下降，但體育賽事和百老匯表演的入場人數空前地高。Hipster Weekly 的時尚專欄作家 Melanie Matthews 說：「一直在看手機真是粗鄙。」

對虛擬生活的強烈反對部分是由於有消息顯示，Facebook 正在將用戶的隱私資訊儲存在世界各地的伺服器中，包括在那些政府主張有權存取其境內儲存資料的國家中。「Zoombombing⁵是一回事，但故意拿這麼多的個資去冒險，則是另一個層次的問題。」Neptune 數位安全公司的安全分析師 Moisha Yldirim 說，「人們意識到自己所有的簡訊，家庭照片和其他數據可能會在任何地方出現，而且可能已經發生了，這真的讓他們感到毛骨悚然。」

疫情也暴露聯邦政府無力保護美國人的生活；在第三波疫情後，國會陷入僵局，並將問題留給州和地方政府自行解決；導致在資料洩露和勒索軟體攻擊持續不斷時，在應對網路安全等需要共同承擔的挑戰上，各地政府間的對策顯得雜亂無章。

於此同時「技術革命」停滯不前，備受吹捧的 VR、5G 和「物聯網」等技術沒有想像中火熱，原因在於人們對過去一直使用的行動裝置感到滿意。

人們一直致力於「security by design」，但因缺乏明確且有效的標準和法規(及缺乏積極的政府作為後盾)，網路仍像以往一樣脆弱。在 2023 年的「Big Breaches」，不僅 Vanguard 公司和 Schwab 公司，網路罪犯更從公共退休基金掠奪了數十億美元的退休儲蓄，進一步削弱了社會大眾的信任。

「人們不再專注於他們使用的科技裝置，並願意接受隱私的喪失(甚至偶發的身份盜用)，以換取無須面對問題。」Gorman Research 的安全分析師 Vanessa Brown 說，「實際上，技術永遠不會消失，但是缺乏關注意義安全標準已經過時了。」

由於對政府進行救援的信任度降低，社群組織已變得至關重要；美國國內和國際的非政府組織，填補各種社會服務的缺口。「DIY」是當今的口頭禪，儘管教

⁴ 部隊中保管個人手機的櫃子之暱稱。

⁵ 有心人士試圖登入未設密碼的會議，或是利用漏洞找尋 ID 進入 Zoom 會議，輕者單純偷聽、惡作劇，重者甚至用色情、仇恨言論干擾會議的行為。

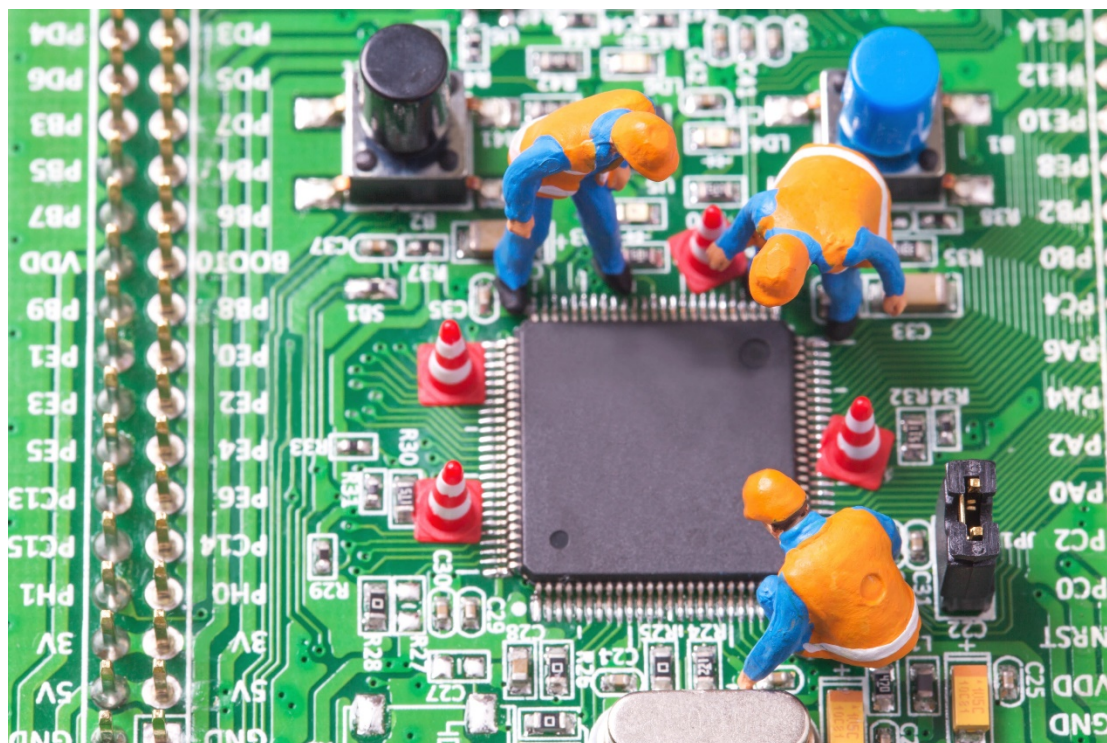
室中對科技的抵制日益增強，但美國教師聯合會還是批准了一項網路安全課程，旨在將學生培養為「足以自我保護數位安全和隱私的公民」。

「網路安全專業人員，很難掌握不斷湧現然後消失的無數平台、標準和技術。」Padrio 說「我們應該做更多的工作，來鼓勵通用、強大、開源的安全和加密標準；我們還需要繼續對民眾(包括最年輕的一代)，進行安全和隱私保護的基礎教育；如同回到原點，世界就像還在 1999 年而非 2025 年。」

如果這個未來真的實現，我們會想在 2020 年致力於哪些網路安全議題？

如果這種未來得以實現，我們或許會希望，科技巨頭被允許比現在更強大，只要他們在安全方面投入更大比例的資源和精力。對比較小、安全性較低的開放市場，更安全的寡占市場可能是更好的結果，尤其是，在政府根本無法或不願意，去塑造和監管具多數小型參與者市場的情況。

Analog Investment



美國聯邦政府在推動經濟復甦上扮演決定性角色，主要聚焦於創造就業機會和建立傳統基礎設施。全球經濟復甦並進入了繁榮的新時代，當許多主要製造商以機器人代替人類後，緊接而來的是對 AI 的強烈反對，並使得數位科技的發展明顯放緩。

當我們慶祝「康復日」四周年之際，當 COVID-19 疫苗向公眾釋出時，有必要去理解美國的今天與 2020 年疫情爆發時有何不同。

最令人驚訝的是，如何恢復對積極、稱職的中央政府之尊重；隨著不同國家在控制疫情上的不同經歷（從日本和韓國這樣的贏家，到巴西和美國這樣的失敗者），使人們重新意識到，只有高水準的政府才能大規模統籌提供公共服務。在華盛頓特區(Washington, DC)，由前述而產生的妥協精神導致改革的開始，在五年前幾乎所有人都認為這不可能。「說真的，我們在那個階段別無選擇。」政治顧問公司 Greenblatt & Walsh 的分析師 Victor Hruska 說。「誰知道非得要一場全球性的疫情和經濟崩潰，才能讓政府採取一致行動？」

許多專家指出，總統大規模的「返璞歸真」基礎設施支出計畫，相對於傳統需求如橋樑、住宅和道路等，更少花費在「智慧」系統。這項 21 世紀的「新政」使成千上萬的美國人重返工作崗位，而且許多新工作集中在智慧能源和氣候變遷

應對（例如野火撲滅，太陽能發電廠）。

大量的基礎設施投資，伴隨對科技工具和系統依賴的顯著降低。疫情後的失業潮使勞動力變得便宜，麥當勞、溫蒂和其他連鎖店因開設「非接觸式」餐館，降低了對廚師和店員的需求，因而受到強烈反對。在一定程度複雜的環境中，人工智慧系統以次優的方式（有時甚至是滑稽的方式）執行。在長達一周的新 5G 網路中斷及一系列網路攻擊，使十餘家標普 500 公司暫停兩個交易日後，大眾基本上決定了他們的「新」世界，應該建立在經過驗證的舊技術上。

這產生了必要的政治動機令國會通過 2023 年《數位基礎設施法案》，這是有史以來首部具有實效的國家隱私和「資料權利」法規，其結果之一導致科技巨頭及其資料被重新指定為「關鍵基礎設施」。同時，社群和工會等都抵制建立大規模「智慧城市」基礎設施的呼籲，而對遠距學習的強烈反對，導致地方教育單位投資於建築物、教師和員工，而非更多的線上教學能力；美國到 2025 年時，小學教師的人均比超過以往任何時候。

網路安全也發生了令人驚訝的轉變；一方面，隨著新系統的部署變慢，攻擊表面⁶維持某種程度的穩定。但是過時、不應於 2025 年仍繼續使用，卻因大量而無法更新的物聯網設備（尤其是工業設備），造成了巨大挑戰。「物聯網設備已成為『棕地』⁷資產，因為沒有任何投資來進行必要的軟硬體更新，以確保其安全。」TechnologyServes 的總裁 Jody McGovern 這麼說。

聯邦和州政府現在是科技解決方案（包括網路安全服務和產品）的最大買家，因為他們已學會非常有效的使用科技，以提高服務效率。人才已從矽谷（Silicon Valley）和奧斯丁（Austin）等私人技術中心，轉移到華盛頓特區及利潤較高的政府契約。

「相較於購買最新版本的 AI，城市在尋找和修復坑洞方面投入了更多的資金。」美國城市地區協會（The Association of American Urban Areas）主任 Susan Binghamton 說。「而且有些城市已經悄悄地在其 IT 預算中增加了『贖金』作為執行成本，老化的基礎設施不單純是搖搖欲墜的橋樑，而是沒有人願意投資必要的

⁶ 攻擊表面（The attack surface）：也稱攻擊面、攻擊層面，它是指軟體環境中可以被未授權用戶（攻擊者）輸入或提取資料而受到攻擊的點位。

⁷ 棕地（brownfield）：以前的工業或商業場所，將來的使用會受到實際或想像的環境污染而影響。

升級以確保數位系統安全。」

如果這個未來真的實現，我們會想在 2020 年致力於哪些網路安全議題？

如果這種未來得以實現，我們可能希望在單純的「阻截和擒抱」網路安全議題上花費更多的時間和精力，例如網路釣魚攻擊、勒索軟體和針對廉價 IoT 設備所進行的暴力密碼攻擊。大部分花費在對抗性機器學習等前瞻議題上的精力，在這個世界上幾乎沒有實際價值，而以簡單的方式改變用戶慣行，這種網路安全行為干預措施將更為重要。

Global Singapore



新冠病毒疫情席捲全球五年後，實體世界看起來與 2019 年極為相似，但支撐每個人生活的數位基礎設施已經有了巨大進步。美國在數位科技上投資了數兆美元，並在 COVID-19 疫情下，加速數位轉型以改善經濟狀況。為了安全和效率，公民（有時不情願地）犧牲了一些自由和很多隱私。

到 2020 年末，美國已成為公認 COVID-19 疫情的全球震央；每個美國人的週遭都有被感染的人，以及在經濟衰退時失業的人。但當美國動盪時，其他眾多國家主要透過先進數位科技指導，進行大規模、由中央政府統籌的政策，設法在 2021 年初限制了病毒傳播，並將生活的大部份恢復正常。感測器資料（來自手機、搜索引擎、地圖應用程序和交通模式，加上先進的 AI 模型）的廣泛使用，有助於決定公共衛生資源的分配。現在「監視」一詞具有不同的含義，相較於 2020 年初負面的「監視資本主義」，它在公共衛生中的用法更加正面。

漸漸地，美國政府不協調的政策變得無法自圓其說。很明顯，需要進行重大的轉變，並且在政治光譜的兩端都需要更多的支持，以採取以資料為導向、果斷的聯邦政府應變。白宮任命了科技專家、科學家和公衛專家，並給了他們「不計代價」的授權，以便應對疫情和在 2021 年初振興經濟。政府強迫科技巨頭通過集中式資料庫協調資料共享，並開發了簡化足跡追蹤的新方法，作為以資料為依據的公衛措施其一，使得冠狀病毒疫情在短短一年時間內得到了有效遏制。

這種動員的成功，甚至給了美國公眾中的懷疑論者也留下深刻印象，同時讓決策者更敢於「優化」美國人生活的其他方面。隱私權的倡導者自然對侵犯公民自由持反對態度，但是在極短時間內就公衛和經濟方面的巨大進步，使得對隱私權侵害的假設如同螳臂擋車。現在，90%的公眾贊成政府對冠狀病毒疫情的應變措施，只有 5%的人認為在自由權上所付出的代價過高。

政治上的成功及合法性不再受到質疑鼓舞了政治人物，他們試圖將資料導向的政策制定和科技的基礎設施，擴展到美國人生活的許多領域。新加坡式的技術官僚成為廣泛的效仿對象，2021 年下半年，國會通過了一系列名為 GovNet 2021 的法案，該法案在數位工具、科技領域、網路安全及其他領域投資數億美元，以進行公共服務的全面升級，例如公共交通與警力。該項目的範圍、規模和預算都超過了「新政」，官員們再次依靠研究人員、技術人員、計算機科學家和網路安全專家的專業知識，並結合科技倫理學家，以決定如何負責地管理新的數位基礎設施。

如今，大規模投資已大致獲得回報，先進的數位技術已緊密整合到公共基礎設施中。美國有著驚人的高效率，隨著首次提供線上投票，2024 年總統大選成為了歷史性的時刻。50%的美國人選擇線上投票，據統計證明，選民欺詐的發生率低於現場投票的發生率，這在很大程度上歸功於國家龐大的網路安全預算。

這項網路安全投資至關重要，因為攻擊面的擴大速度，比疫情前任何人所預見的都要快得多。對於科技巨頭共享資料的擔憂減少了，但因單點故障⁸造成的影響越來越大，人們更加擔心針對國家基礎設施的攻擊越來越容易發生（儘管不清楚是否有人真的知道這些單點故障在哪裡）。

結果上來說，對自由和個人隱私遭侵犯的焦慮，已成為人們在有餘力時沉迷

⁸ 單點故障 (points of failure)：指系統中一旦失效，就會讓整個系統無法運作的部分，換句話說，單點故障即會整體故障。

的奢侈品。令公民自由主義者恐懼的是，雖然有公眾異議和社會運動被鎮壓的謠言，但大多數民眾已開始妥協。這是因為，人們很容易想起在 2020 年所遭受的創傷和不安全感，對健康、經濟和社會心理安全的渴望，已經遠超過對隱私權的關注（而在許多公民眼中，隱私權僅是想像中的問題）。

「政府現在可以存取空前數量的、集中化的資料，雖然現在政府告訴我們資料被負責任的管理，但並不能保證資料現在真的，或在將來會得到負責任的管理」電子自由基金會的政策專家 Kristen Hyde 說。「美國公眾需要透過各種方式思考，我們的資訊生態系可能受到損害，而我們卻視而不見，且在發生問題時，任何（解決問題的）模型或框架都沒有。」

如果這個未來真的實現，我們會想在 2020 年致力於哪些網路安全議題？

如果這種未來得以實現，我們可能希望我們已經開發並廣泛傳播了一種更加緊密的、完整的觀點，和一組清楚闡明監視與隱私間的細微關係，和二者間折衷方案的模型。如果這被視為二元選擇，並且被大規模的公衛和經濟災難所決定，在零和的傾向性下，2020 年最壞情況是隱私權的概念將失去作用。我們可能還希望獲得更多的研究和結論，以了解在個資上——一般情況與感受下理解為「棘輪效應（ratchet effect）」——如何改變：一旦超出個人的控制範圍，是否有辦法證明其「落日⁹」，或是否有辦法把個資取回來？

CLTC 的團隊成員通過腦力激盪和情境發想產生了這篇文章，Kayla Brown 是《Global Singapore》段落的主要作者。我們歡迎您對這些情境提供回饋，請將任何想法、評論或問題寄到 cltc@berkeley.edu。

本報告中譯本於 2020 年 10 月，經 CLTC 中心 Ann Cleaveland 主任之翻譯授權。

⁹ 棘輪效應：人為過程一旦發生特定情況，逆轉的能力就受到限制。

¹⁰ 譯者註：指個資在一段期間後，自動被刪除。

TW/SC