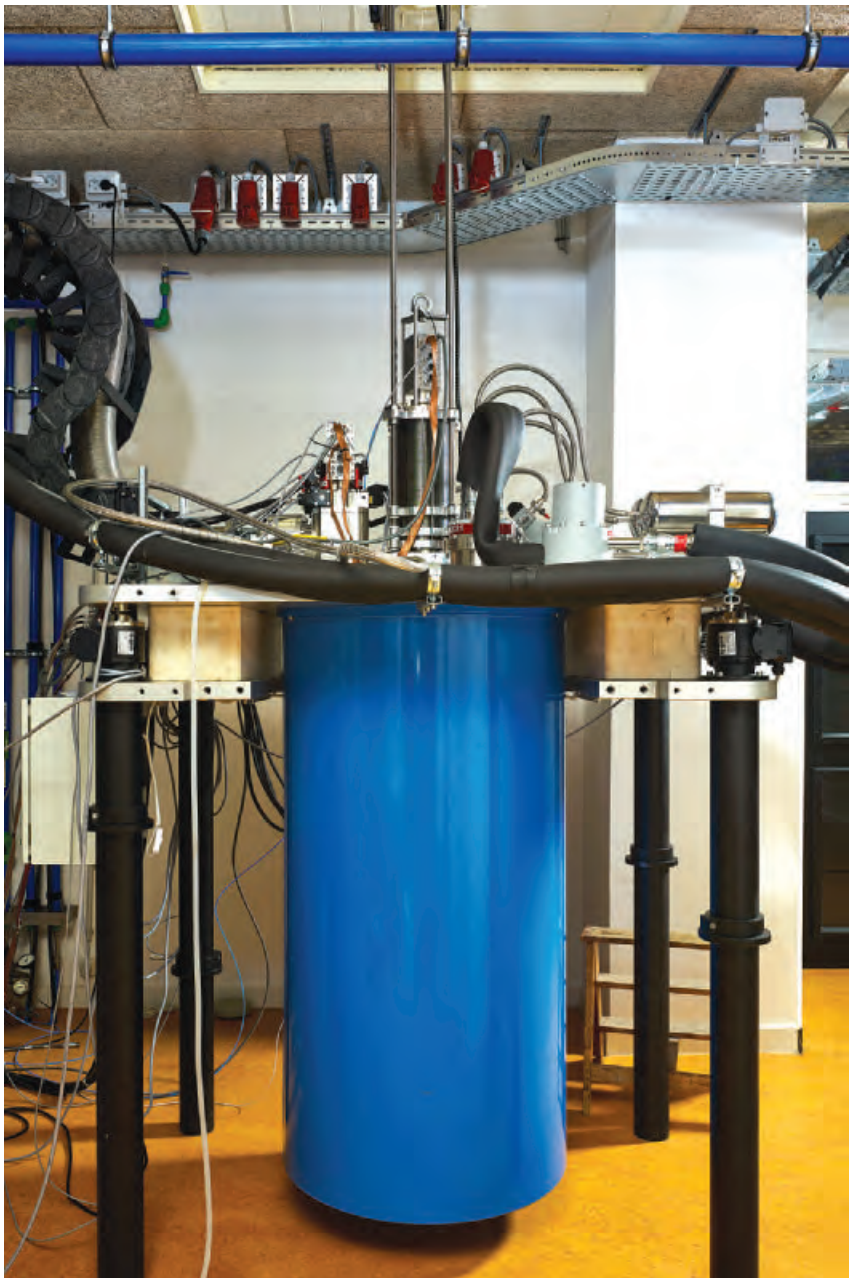
10大突破性科技（下）

翻譯／ Aurore Liang

實用量子電腦

包括 Google、Intel 在內等幾組研究團隊的進展顯示，能力超越以往想像的電腦終於快成真了。

撰文／亞斯卡利安（Russ Juskalian）



這個藍色冰箱把溫度降到剛好超過絕對零度，使量子實驗得以在內部的微小晶片上進行。

荷蘭 QuTech 研究中心負責全球最先進量子運算的實驗室，但看起來倒像在測試空調系統。位於台夫特科技大學（Delft University of Technology）應用科學樓安靜一角的實驗室裡，空無一人，纏繞在幾個三足和四足藍色大圓柱體四周，錯綜複雜的絕緣管、電線、控制器材，發出嗡嗡作響的共振波，彷彿遭到成群電子紡織娘入侵。

在這些基本上是增壓冰箱的藍色圓柱體中，奇怪的量子力學事件正在發生，奈米線、半導體、超導體在比絕對零度高一點點的溫度相遇，此時，在物理學的極限下，固體材料產生所謂的準粒子，準粒子的特性使他們有作為量子電腦關鍵組件的潛力，尤其這間實驗室已在實現量子電腦上取得重大進展，未來幾年內，或許加密技術、材料科學、

本刊取得美國麻省理工學院 Technology Review 期刊圖文授權
Technology Review, Published by MIT. TECHNOLOGY REVIEW internet URL: www.technologyreview.com
MIT Technology Review

突破性科技

能製造出穩定的量子電腦基本單位「量子位元」。

重要性

量子電腦能以指數級的速度，跑人工智慧程式和處理複雜的模擬及排程問題，甚至可以創造出無法破解的加密。

主要研發團隊或人員

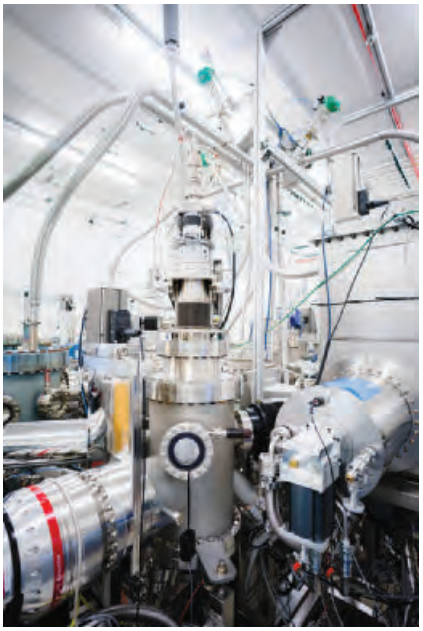
-QuTech
-Intel
-Microsoft
-Google
-IBM

上市時間

四到五年

量子電腦是什麼？

量子運算的核心是量子位元（qubit），一種類似電腦中以電晶體代表 0 和 1 的基本資訊單位。量子位元有兩個獨特的特性：可以同時表示 1 和 0，且能透過量子糾纏的現象影響其他的量子位元，如此一來，量子電腦進行特定類型的計算時，能走捷徑求出正確答案，因此比傳統電腦更強大。



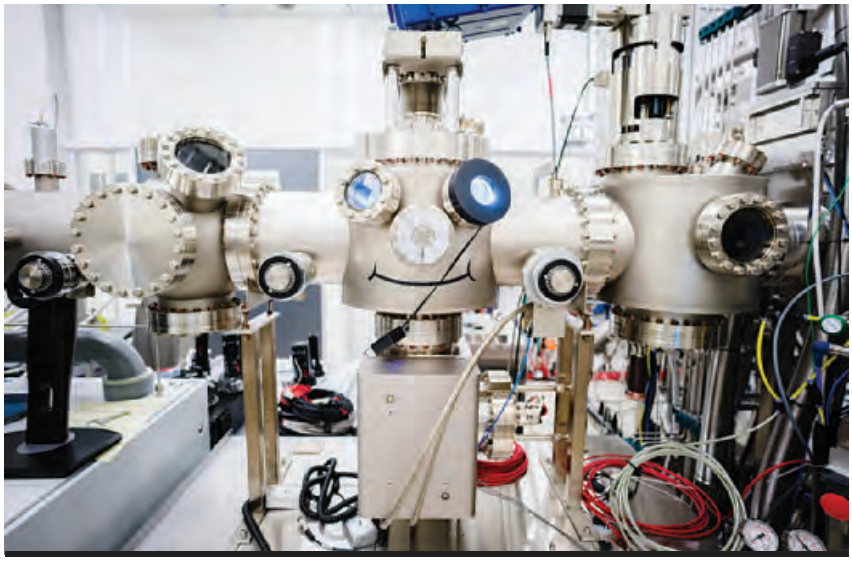
台夫特科技大學進行實驗。

醫藥研究、人工智慧都將因量子電腦而改寫。

量子運算年年都在 10 大突破性科技候選行列，結論卻也年年不變：為時尚早。事實上，量子位元和量子電腦多年來幾乎都停留在紙上談兵，只有薄弱的實驗能證明他們的可行性。（有段時間，加拿大公司 D-Wave 推出一種使用所謂量子退火技術的機器，這家公司把他稱為量子電腦，但有人質疑這項技術，頂多只能用於非常有限的運算組合，且與傳統電腦相比，在速度上不占優勢。）不過，今年，有些以往的理論設計正在打造實體中，此外，今年的新發展還包括 Google、IBM、Intel、微軟等公司投入資金，研究開發微電子、複雜電路、控制軟體等實際打造量子電腦所需的技術。

台夫特計畫的主持人是最近剛接受微軟聘任的考恩霍文教授（Leo Kouwenhoven），這項計畫的目的是克服打造量子電腦長久的障礙：量子位元（量子訊息的基本單位）很容易受到雜訊干擾而出錯，量子位元有用的前提，是必須達到量子疊加（Superposition，類似同時處於兩種不同物理狀態的性質）和糾纏（Entanglement，量子位元成對鏈接的現象，此時即使兩者實際上分開，但其中一個發生變化，另一個會立刻受到連帶影響），這兩種微妙的狀態條件很容易被振動或起伏的電場等極為輕微的干擾所破壞。

各界長期以來不斷努力克服這道難關，寄望打造出量子電腦，可以解決當今最強大的電腦也解不出的



以往的理論設計正在打造實體中。

問題，如今考恩霍文領導的團隊相信，他們所創造的量子位元本質穩固，像繩結般牢靠，考恩霍文說明：「這個繩結，不論怎麼扭轉拉扯也解不開，資訊不會改變。」穩定性高，研究人員才能大幅降低糾錯所須的運算能力，進而提高量子電腦的效能。

考恩霍文的工作必須要操控一些性質獨特，直到 2012 年才被發現的準粒子，這還只是幾個令人印象深刻的步驟之一，在同一間實驗室，接受 Intel 贊助的凡德西朋（Lieven Vandersypen）正示範如何在傳統矽晶圓上製造量子電路。

未來，量子電腦特別適合用於因式分解龐大數字（因此可以輕鬆破解當今許多加密技術，甚或可以提供難以破解的替代法），解決複雜的優化問題，執行機器學習運算法，甚至出現目前仍沒人料想得到的應用程式。

不過，我們即將可能會更清楚量子電腦的用途，研究人員目前為止已打造出可完全編程的五量子位元量子電腦，和較不穩固的 10 到 20 量子位元測試系統，兩種的功能都不太多，但 Google 的量子運算計畫主持人諾文（Harmut Neven）表示，他的團隊可望在一年內達成打造出 49 量子位元系統的目標。目標設定在 50 個量子位元並非偶然，這稱為量子優勢的門檻，超過這個位元數，傳統超級電腦就無法應付模擬量子電腦所需的記憶體和通訊頻成長，換言之，5 到 20 量子位元量子電腦能做的事，頂尖的超級電腦系統目前都能達成，但到了 50 量子位元左右，在物理上就不可能了。

所有接受採訪的學界和企業界量子研究者都認為，量子電腦在 30 到 100 個量子位元間，尤其是穩定度足以長時間執行各種運算的量子位元數，開始具有商業價值。此外，未來兩到五年，這樣的系統就可能上市。到最後，預計會出現 10 萬量子位元的系統，當模型準確度因此能達到分子級時，可能發現新的材料和藥物，對材料、化學、醫藥等產業帶來重大變革，那麼，連可用來做什麼都難以臆測的 100 萬個量子位元系統呢？諾文認為「未來 10 年內就可能出現」，就不難想像出來了。

扭轉癱瘓

科學界在利用大腦植入技術，重建因脊髓損傷而失去的行動能力上，取得重大進展。

撰文／羅格拉多（Antonio Regalado）

庫汀（Grégoire Courtine）腦中閃過「走啊，前進！」這個念頭。

這位法國神經科學家當時正在觀察一隻在跑步機上使勁弓背的獼猴，這隻動物的脊髓被庫汀的團隊用刀片從中切斷，右腿癱瘓，為了證明他能恢復這隻猴子的行走能力，庫汀和同事在猴子的頭骨下方安裝了一個緊貼運動皮層的記錄裝置，並在脊髓受損處下方縫上一個彈性電極墊，兩個電子設備以無線通訊連結。

實驗結果：系統讀取到猴子想要移動的念頭後，隨即以電刺激脈衝形式傳送到脊椎，很快地，猴子的右腿開始移動、伸長、彎曲、伸長、彎曲、蹣跚前進，任教於瑞士洛桑聯邦理工學院（École Polytechnique Fédérale de Lausanne.）的庫汀興奮地回憶道：「猴子腦子動了一下，接著，他開始行走！」

近年來，藉由大腦植入物與機器的組合，已有實驗動物和少數人成功以思想控制電腦游標或機械手臂，目前人員正朝著能一勞永逸地扭轉癱瘓的研究方向，邁出意義重大的下一步，他們將大腦解讀技術直接以無線方式連接到身體上的電刺激器，創造出庫汀所稱的「神經旁路」，讓四肢能夠再次受大腦指揮動作。

在克利夫蘭的凱斯西儲大學，一名四肢癱瘓，頭肩以外完全喪失行動能力的中年人，同意讓醫生將兩個與庫汀在猴子實驗中用的同型紀錄器植入大腦，在兩個比郵票小的矽膠製紀錄器上布滿 100 根細如髮絲的金屬探針，能「聽」見神經元

在靈長類大腦矽膠模型上展示的植入物。

突破性科技

以大腦身體間的無線電子介面代替受傷的神經系統。

重要性

每年有成千上萬的人因傷癱瘓。

主要研發團隊或人員

- 洛桑聯邦理工學院（École Polytechnique Fédérale de Lausanne）
- 哈佛大學維斯生物神經工程中心（Wyss Center for Bio and Neuroengineering）
- 匹茲堡大學（University of Pittsburgh）
- 凱斯西儲大學（Case Western Reserve University）

上市時間

10 到 15 年

發射出的命令。

為了完成旁路，由克希（Robert Kirsch）和阿吉柏耶（Bolu Ajiboye）領導的凱斯西儲大學團隊，將超過 16 枚細小的電極置入病患手臂和手掌的肌肉中，在實驗的紀錄影像中，可以看到這名志願者在彈簧扶手的幫忙下，緩緩抬起手臂，並用意志控制手掌開合，患者甚至把插著吸管的杯子端到唇邊，不靠這套系統，這些動作他沒一項做得到。

坐在自己手上一整天試試，便能稍

庫汀拿著腦脊介面的兩個主要構件。

布滿電極的大腦閱讀晶片特寫。

模擬脊髓用的彈性電極。

放在頭骨上的無線神經通訊裝置模型。

神經旁路的里程碑

1961 年

醫生兼發明家豪斯（William F. House）測試第一副可重建聽力的人工耳蝸，至今共有超過 25 萬人受惠於這項裝置。

1998 年

醫生在一名無法開口說話的癱瘓患者腦中安裝一個電極，患者可透過電極與電腦溝通。

2008 年

一隻猴子的大腦訊號經由網際網路從美國發送到日本，成功指揮機器人在跑步機上行走。

2013 年

Second Sight 公司的「仿生眼」獲美國主管機關核准上市，這項技術使用縫入視網膜的晶片，取代受傷的感光細胞。

2014-2015 年

俄亥俄州的醫生開始努力讓兩名癱瘓男性的手臂「重新動起來」，兩名患者的思想各自傳遞到自己手臂上的電極，控制手掌開合。

2016 年

28 歲的科普蘭（Nathan Copeland）裝了機器人手掌，經由大腦植入物操縱，讓他「感覺得到」手指，歐巴馬任內參觀匹茲堡一所實驗室時，科普蘭曾和總統擊拳致意。

微了解到脊髓損傷後有多難受，沒辦法抓自己的鼻子或摸孩子的頭，庫汀用戲劇化的誇張動作，伸手拿起一只紅色的濃縮咖啡杯，端到嘴邊，說：「但若有這個，你的生活便不一樣了。」

凱斯的實驗成果（已於 2017 年 3 月 28 日發表在國際知名醫學期刊《刺胳針（The Lancet）》），只是將電子植入技術運用在重建感官和能力的各種研究之一，除了治療癱瘓外，科學家希望利用所謂的神經修復術，將晶片植入眼睛，讓失明患者重見光明，或藉以喚回阿茲海默症患者失去的記憶。

他們知道這項研究行得通，以耳蝸植入物為例，訊號經過麥克風直接中繼到聽覺神經，繞過內耳與聽覺無關的部分，聽障兒第一次聽到媽媽聲音時睜大眼的影片，網路上每個月都要瘋傳一波，接受這項治療的聽障患者已超過 25 萬人。

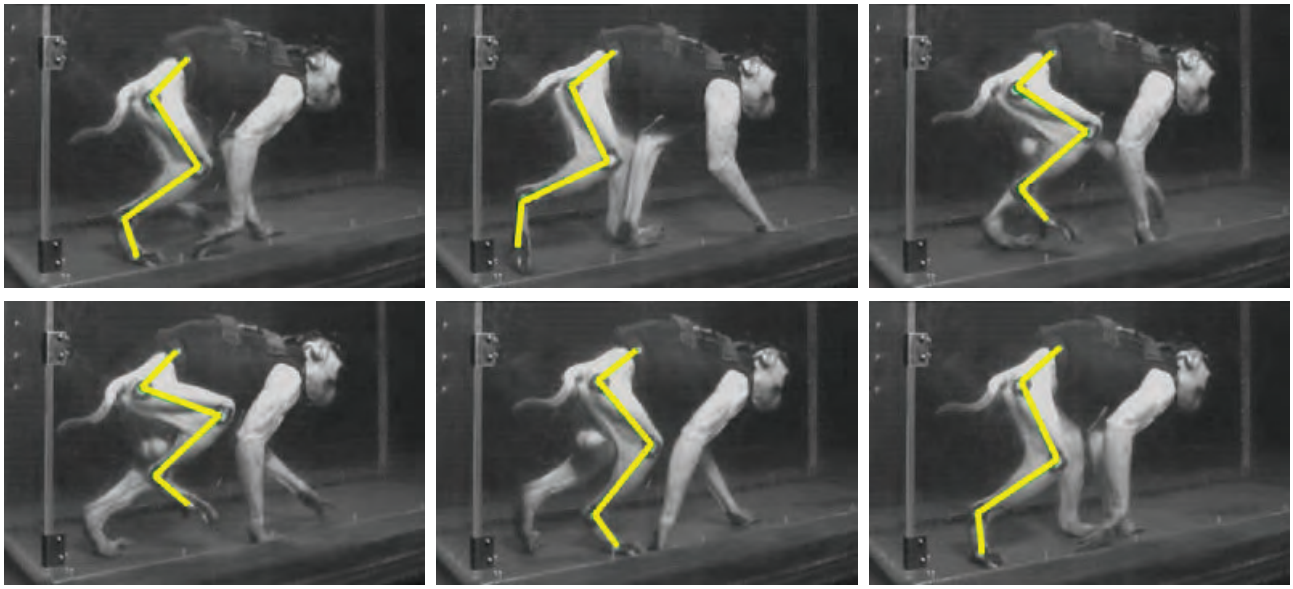
但要讓神經義肢對癱瘓患者變得有用，一向困難得多。1998 年，首次有患者靠腦中探針讓電腦游標在螢幕上移動，這項技術和其他好幾種驚人的腦控技術，一直未獲廣泛的實際使用，因為這項技術太激烈，太複雜，還出不了實驗室，庫汀驚嘆：「20 年的研究，臨床上卻什麼也沒有！」他把頭髮往後撥，接著說：「我們不斷向極限延伸，但重要的問題是這整個領域最後到底會不會推出任何產品？」

庫汀的實驗室位於日內瓦一座玻璃帷幕大樓中，同棟還有由瑞士億萬富翁魏斯（Hansjörg Wyss）投入一億美元成立的研究中心，專門鑽研如何克服脊髓旁路等神經技術的技術障礙，這座研究中心從醫療設備製造商和瑞士錶廠延攬專家，並設有無塵室，將金線列印到可以像人體一樣伸縮的橡膠電極上。

中心主任多諾霍（John Donoghue）來自美國，是美國開發大腦植入物的先驅，他兩年前遷居日內瓦，為打造出商業上可行的系統，目前正努力網羅優秀的神經科學家、技術專家、臨床醫生等技術資源和人才加入。

多諾霍的首要工作之一是「神經通訊（neurocomm）」，這種超小型無線裝置可以跟電腦網路用一樣快的速度，從大腦收集訊息，多諾霍稱之為「腦子裡的收音機」，他說這是「全世界最複雜的大腦通訊器。」目前的原型大小如火柴盒，是以生物相容的鈦與片狀藍寶石所製成，庫汀在猴子實驗中用的是較早期較大的版本。

多諾霍表示，即使神經旁路極端複雜，進展又極其緩慢，但為了翹首盼望的患者，值得全力以赴，他說：「去問問患者，想不想要手部能動？他們想要恢復原本的生活，他們想要重新動起來。」



洛桑聯邦理工學院研究人員製作的影片中，可看到一隻脊髓受損導致右腿癱瘓的猴子，重獲行走能力。

物聯網的殭屍網路

對居家裝置互相連線的無止無盡追求，正帶來危險的副作用，而且只會愈來愈糟。

撰文／施奈爾（Bruce Schneier）

殭屍網路的存在至少已有 10 年，早在 2000 年，駭客就曾透過網路入侵電腦，統一操縱大量遭感染的電腦執行各式各樣任務，例如，挾殭屍網路加總的強大運算能力，發動分散式拒絕服務攻擊，製造龐大流量癱瘓特定網站。

然而，隨著網路攝影機、數位錄影機等各種便宜的「物聯網」小工具愈來愈多，這個問題也日愈嚴重，這些裝置通常很少或根本沒有安全防護可言，因此駭客不費吹灰之力就能加以接管，要架構大型殭屍網路，一次癱瘓許多網站，比以往任何時候都更簡單。

去年 10 月，一個由 10 萬個受感染裝置組成的殭屍網路，造成網際網路基礎設施商戴恩（Dyn）的部分服務斷線，戴恩遭攻擊後，服務中斷並引發連鎖效應，甚至造成 Twitter、Netflix 等大型網站無法開啟，未來必然會有更多的攻擊：攻擊戴恩的殭屍網路是透過一款稱為 Mirai 的免費開放式惡意軟體指揮，受感染的電腦會高度自動化協作。

最佳防護之道是所有上網裝置都只使用安全的軟體，從根本防止殭

突破性科技

惡意軟體入侵控制網路攝影機、錄影機等消費裝置，引發大規模網路中斷。

重要性

使用這個軟體的殭屍網路正在造成愈來愈大，愈來愈難遏止的網路癱瘓。

主要研發團隊或人員

- 寫出 Mirai 殭屍網路軟體的人
- 任何把低安全性設備連上網使用的人，包括各位在內？

上市時間

現在

屍網路形成，但短期內這顯然無法實現，物聯網裝置設計時未考慮到安全性，通常連安裝補丁都沒辦法，例如，受 Mirai 感染的裝置已經成為殭屍網路的一部分，除非淘汰不再使用，否則未來永遠都受到控制，淪陷裝置的數量在未來幾年將呈級數增加，殭屍網路只會變得更大更強。

駭客使用殭屍網路的用途可多著了。

有人用殭屍網路騙取點擊數，點擊詐欺這種技倆是要欺騙廣告主，讓他們以為有人點擊或瀏覽他們的廣告，點擊詐欺的手段很多，但在自己的網頁嵌入 Google 廣告可算其中最簡單的一招，Google 廣告會根據網站點擊人數，支付費用給網站所有人，駭客只要指揮殭屍網路上的所有電腦，一再重複訪問特定網頁並點擊廣告，只要點、點、點，錢就輕鬆入袋！若讓駭客找出更多能在線上指揮殭屍網路從大企業吸金的手法，未來或許會看到整個網路廣告模式崩潰。

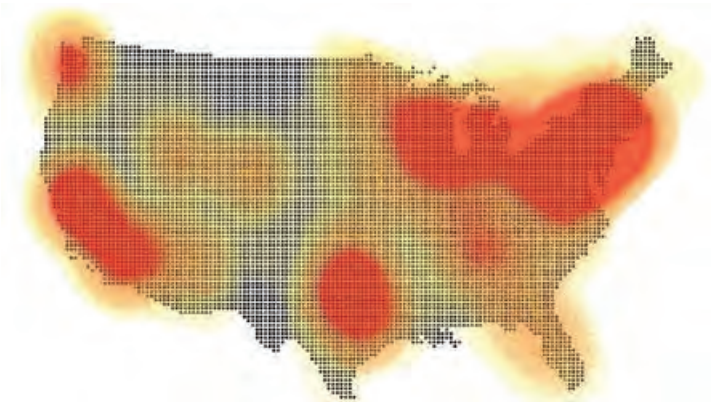
同樣地，殭屍網路可以用來逃過垃圾郵件過濾器，過濾垃圾郵件的方法之一，是找出哪些電腦在一口氣發送出成百上千萬封電子郵件，殭屍網路也可以用來加速破解密碼，侵入網路帳號，挖比特幣，以及任何需要應用到大型電腦網路的事，犯罪集團租用要按使用時間計費，這就是殭屍網路是門大生意的原因。

其中，最常成為頭條新聞的殭屍網路行動是「阻斷服務攻擊（DoS）」，雖然戴恩的加害者似乎是一群憤怒的駭客，但其他為求財動手的團體，則是把這樣的攻擊當作勒索的辦法，政治團體用阻斷服務攻擊，來讓他們討厭的網站閉嘴，這種攻擊肯定會在未來任何網路戰爭中成為戰術。

一旦知道某個殭屍網路的存在，就可以攻擊他的指令及控制系統，以往殭屍網路較少見時，這種策略還有用，但隨著殭屍網路愈來愈常見，這種見招拆招的手法會愈來愈沒效，個人也可以保護自己避免受到殭屍網路影響，例如，有幾家公司便提供拒絕服務攻擊的防護，然而實際防護力的高低，則取決於攻擊的嚴重程度和服務的類型。

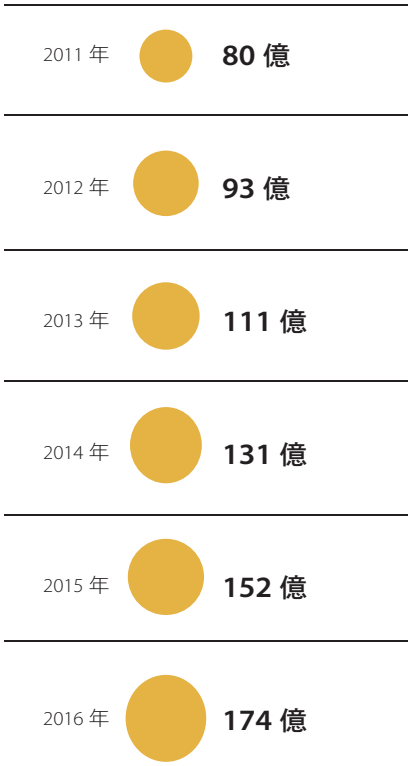
但整體而言，情勢對攻擊者有利。像戴恩這樣的攻擊事件，接下來一年將會更多。

淪陷裝置的數量在未來幾年將呈級數增加，殭屍網路只會變得更大更強。



2016 年 10 月 21 日戴恩遭拒絕服務攻擊而造成網路中斷範圍示意圖，戴恩的經營業務是管理將終端用戶連上網站的域名服務器。

全球「可上網」裝置的數量



資料來源：IHS MARKIT

施奈爾（Bruce Schneier）為現任 IBM Resilient 技術長，擁有 13 本加密和資訊安全相關著作。

Copyright©2017, Technology Review,All Rights Reserved.