



● 作者/Rick Adams ● 譯者/周茂林 ● 審者/黃依歆

需才孔亟：迎戰網路攻擊

Help Wanted: Cyber Pros

取材/2018年4月德國軍事科技月刊(*Military Technology*, April/2018)

面對新科技與社群媒體普及的便利，
洩漏軍事情資可能構成的風險也同時隱藏巨大威脅。
為此，各國刻正網羅網路專才，卻面臨人才短缺與資源不足的問題，
如何前瞻考量未來情勢，打造軍事作戰全方位實力，
乃軍隊之重要議題。

英國風險評估公司巨鴻集團營運長惠廷所提及的「虛擬網路助理」工具，具備「類似狙擊手焦點射擊」的功能。(Source: Rick Adams)



FOCUS

專題報導

凡「跑」過必留下痕跡！這是一個社群媒體「武器化」的時代。有關在線上洩漏個資的議題，我們自己有時反而是最大的風險源頭。

2017年11月，舊金山一家新創公司「史托瓦」(Strava，瑞典文原意是「奮鬥」)推出運動路徑「全球熱區圖」，蒐集了過去數年間從Fitbit、Jawbone、Vivofit等個人運動穿戴裝置下載的3兆個全球定位系統位置數據。儘管該應用程式具備新穎的優勢，卻是潛在軍事禍患的淵藪。

20歲的澳洲國立大學學生魯瑟(Nathan Ruser)專攻國際安全，任職於甫成立兩年的「聯合衝突分析協會」(Institute of United Conflict Analy-

sis)。他觀察到最受歡迎的慢跑路徑或單車動線——呈現於明亮的螢光透明地圖——不僅可能暴露了坐落於阿富汗、伊拉克、索馬利亞、尼日及其他偏遠地區的軍事基地位置(儘管訊息也可能來自他處)，更有可能曝光非值勤軍人所青睞的運動路線。美軍在阿富汗坎達哈(Kandahar)基地外的「狙擊手巷道」(sniper alley)即為一例。

以上所述不僅是美軍的問題。俄羅斯在敘利亞的主要基地赫梅明(Khmeimim)，因為可能的巡邏路線遭到標示而相當顯目；英軍福克蘭群島蒙普列仁(Mount Pleasant)空軍基地則因為附近流行的游泳地點而顯得特別突出。

從個人運動穿戴裝置下載的全球定位系統位置數據中可發現，受歡迎的慢跑路徑或單車路線，可能會暴露軍事基地位置與人員運動習慣，而成為軍事禍患的淵藪。(Source:國防譯粹編輯室)



上述資訊都是恐怖分子、擄人勒贖集團、潛行跟監者的重要情資。加州網路安全漏洞評估公司蟲夥(Bugcrowd)創辦人、董事長兼技術長艾力斯(Casey Ellis)曾表示，「人們設計軟體時都是考量正常使用的情境，不會想到被人濫用的可能性。」

美國國防部長馬提斯(Jim Mattis)已下令評估該狀況，五角大廈也發表聲明，指出「我們嚴正面對類似事件，並刻正評估情勢，決定是否需要進一步的訓練或指導，以及發展出其他政策，以持續確保美國海內外國防人員的安全。」兩年前，美海軍與陸戰隊批准使用穿戴式健身追蹤器，還透過各項先導計畫鼓勵官兵使用。但是，類似的追蹤裝置現在可能要與卡巴斯基實驗室(Kaspersky Lab)的軟體(總部位於俄羅斯的一家電腦安全公司)、大疆創新公司空拍機Phantom(總部位於中國大陸)一樣，必須停止使用了。

美國西點軍校「陸軍網路研究所」(Army Cyber Institute)所長霍爾(Andrew Hall)上校表示，「我們開始檢視過去為消費者和顧客群簡化系統、讓事情更有效率的作法。然後我們發現效率是一項弱點，會遭到不當利用。」

網路攻擊頻仍

網路攻擊的節奏逐漸加速。美國網路司令部司令兼國家安全局局長羅哲斯(Michael S. Rogers)上將即表示，「在我任職於網路司令部期間，幾乎每天世界上都會發生至少一樁重大網路安全事件。」羅哲斯針對新設「網路任務部隊」(cyber mission force)預算需求案出席美國眾議院軍事委



「蟲夥」創辦人艾力斯曾說過：「人們設計軟體時，都是考量正常使用的情境，不會想到有被人濫用的可能性。」(Source: Wiki)

員會新興威脅與能力小組委員會時強調，「我們承受著日趨多元的先進科技威脅，而且敵軍技術更為複雜，手段更為精準。」

美空軍近期估計，其空中暨地面電腦系統網絡每日要因應超過100萬次的網路攻擊。

例如，F-35戰機被人稱為「具有翅膀的大型電腦」，某次其細部示意圖遭駭客攻擊後，經查攻擊檔案來自於一家未具名的澳洲國防廠商，該



FOCUS

專題報導

公司曾參與F-35戰機的研發計畫。

又如，美國國家安全局在羅哲斯任內開發的「永恆藍」(EternalBlue)程式，於2017年4月遭一群自稱「影子掮客」(Shadow Brokers)的駭客入侵，後者利用「永恆藍」竊取了數十億筆加密虛擬貨幣(cryptocurrency)，牽連至少150個國家，導致超過30萬臺電腦系統當機。以上攻擊於2018年1月另以「挖礦」

(WannaMine)的網路蠕蟲捲土重來，據傳各公司須加裝某種新一代的防毒軟體，以偵測並防堵病毒，而這種作法「不是不可能，只是有其困難度」。

另外，北韓駭客據稱已經自孟加拉、厄瓜多、波蘭與越南網路銀行竊取了將近1億美元，以維持西方國家多項制裁下的北韓經濟。

根據日本情報通信研究機構(National Institute of Informa-

tion and Communications Technology)的統計，日本網路系統於2016年遭受1,280億次的網路攻擊，目標主要為連上物聯網(IoT)的裝置，其中最大宗攻擊者據信來自中共。

同樣地，根據英國國家網路安全中心(National Cyber Security Centre, NCSC)主任馬丁(Ciaran Martin)的說法，英國國家網路安全中心自2016年成立以來，已封鎖「數千萬次」的網



2017年發生的NotPetya網路攻擊事件，使「默客」製藥大廠銷售額損失上億美元，另再耗費鉅資更新其資訊基礎設施。(Source: Merck UG Office)

路攻擊行動。

勒索病毒(鎖住使用者的電腦系統,直到付出贖金)攻擊在一年內激增167倍,損失達數百萬美元。受災戶包括馬士基(Maersk)航運公司(耗資2億美元重新安裝4萬5,000臺個人電腦和4,000臺伺服器)和聯邦快遞(損失3億美元)。

2017年發生NotPetya網路攻擊事件,使默克(Merck)製藥大廠銷售額損失1億3,500萬美元,另再花費1億7,500萬美元更新其資訊基礎設施。據估病毒勒索事件的受害者高達90%來自健康照護產業,單在美國境內就損失26億美元。

耶路撒冷企業夥伴(Jerusalem Venture Partners)董事長馬格利特(Erel Margalit)以科技企業家身分提出警告,網路駭客除了詐取金錢外,「還有可能已在製藥過程中變更化學配方……這已造成歐洲的網路災難。」

馬格利特同時強調,「多次演習顯示歐洲仍有65座核能設施易受攻擊,這些地點可能遭到足以引起嚴重事件之駭客攻擊。」馬格利特聲稱伊朗培養了

「一支駭客軍隊」遊走於各國境內。「伊朗核武威脅是個未來議題,但是伊朗網路威脅是當前立即的挑戰。」

以色列國防軍退役上將卡羅(Ariel Karo)目前任職於曾研發「鐵穹」(Iron Dome)飛彈防禦系統的拉斐爾(Rafael)公司。他近期提出「網路鐘罩」(Cyber-Dome)建議,指出拉斐爾公司的部分專業領域在應付「全天候攻擊之環境」。

事實上,馬提斯認為伊朗為中東穩定與否「最重大的挑戰」。馬提斯認為「伊朗與其鄰國競爭,堅守影響力之弧與維持動盪情勢,爭奪區域霸權,達成目標的作法則是利用國家支持的恐怖活動、擴充代理人網絡,以及發展飛彈計畫。」馬提斯表示,「無可否認地,美國國土已不再是庇護所。無論是攻擊市民的恐怖分子,還是針對個人、商業、政府基礎設施的惡意網路活動,或是政治與資訊顛覆,美國都已成為目標。」

馬提斯認為,「這股前仆後繼的新科技發展驅力,不僅以較低的門檻擴充了參與者,而且不斷加速進展中」,因此,

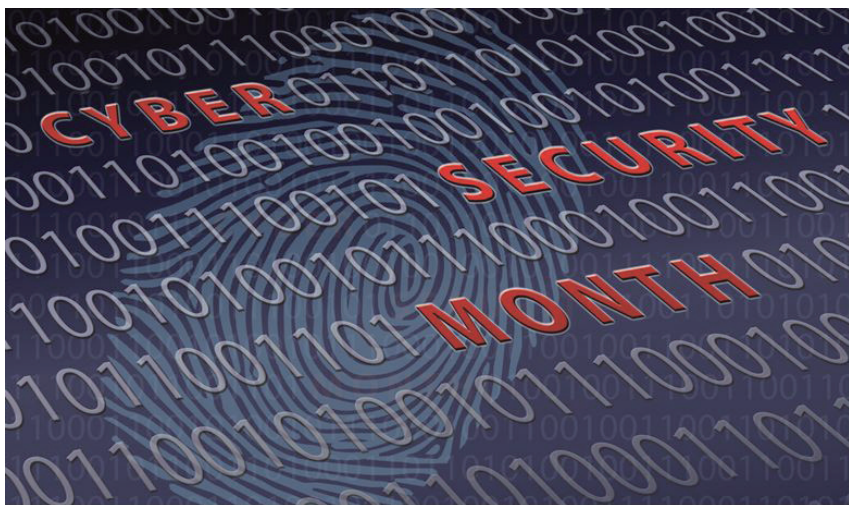
「美國將投資於網路防禦,提升彈性,並廣續整合網路各項能力,打造軍事作戰全方位的實力。」

亟需網路專才

歐巴馬政府時期的國防部部長卡特(Ash Carter)曾表示對網路司令部反制伊斯蘭國的實效「非常失望」。卡特寫道,美軍針對伊斯蘭國的攻勢網路作戰,「從未真正產生任何有效的網路武器或技術。」

全世界各國政府現階段正競相發展各項網路能力,期能跟上「暗網」(Dark Web)駭客的水準,不管這批駭客是敵對國家、非國家行為者或是網路罪犯。而這在公私部門創造了約150萬到180萬個網路安全相關職缺。

美國國防部希望按照羅哲斯的構想,在2018年9月成立一支為數6,200員的強力「網路任務部隊」。這支部隊包括:13個國家任務單位,以捍衛美國與其利益,阻絕網路攻擊;68個網路防護單位,以維護美國國防部按優先排序的各個網路系統;27個戰鬥任務單位,期以統一的網路空間作戰效力,支援作戰



世界各國政府現階段正競相發展各項網路能力，期能跟上「暗網」駭客的水準。(Source: Wiki)

司令部；以及25個支援單位，為上述國家和戰鬥任務單位提供分析支援和計畫作為。

在此必須指出的是，美國國家安全局在過去三年裡，由於不斷遭控逾越職權，加上內部組織重整，不但飽受士氣下滑之苦，而且導致上百位的程式設計師、工程師、資料科學家離職。國家安全局前資深研究員威廉斯(Ellison Anne Williams)表示，「局內正大量流失極為優質的技術人才。它失去了一流的、最睿智的幕僚群，堪稱是嚴重的打擊。」威廉斯於2016年離職，自創資料安全公司英服爾(Enveil)，隨後僱用了10位當年的老同事。

美陸軍為了扭轉這批人才朝民間企業外流的趨勢，提供了網路專業人士一筆4萬美元的留營獎金，並擬定直接任用計畫。

黑箱物料(Darkmatter)是位於阿布達比的一家成立三年的網路安全公司，成員650人，許多主管都來自西方國家晶片大廠英特爾(Intel)和電信元件供應商黑莓(Blackberry)。由於黑箱物料公司是由阿拉伯聯合大公國行動電話企業阿百奈(Faisal al-Bannai)創立，該公司訂單的主要來源為該國政府，例如國家電子安全局(National Electronic Security Authority)。

目前芬蘭國防軍設下的可行

目標，是在2024年前維持200多位的網路安全專業人士員額，並規定這些人須為芬蘭公民。芬蘭國防軍不僅要和國內民間公司競求網路人才，另一挑戰則是來自全歐洲計約20萬個新釋出的網路職缺。但是芬蘭國防軍司令部司令漢斯凱寧(Mikko Heiskanen)表示，「我們沒有辦法滿足一流人才開出來的薪資，他們要求的條件高於我們預算允許的好幾倍，換句話說，我們不盡然會得到想要的專才，但必須滿足於能得到的人才。」

漢斯凱寧的說法在於吸引不同類型的駭客能夠「為軍方工作，在其他崗位上，一個人侵入電腦系統和修改資料是違法的，但卻在我們這裡能合法進行，例如駭入電腦系統及竄改資料。」

歷經2007年拆除戰爭銅像引起的網路攻擊後，愛沙尼亞(全國總人口約130萬)這個小國已經轉型為全球最先進的數位化社會之一，同時也是北約「網路合作防衛卓越中心」(Cooperative Cyber Defence Centre of Excellence)的據點。其中，「愛

沙尼亞防衛聯盟網路防護單位」(Cyber Defence Unit of the Estonian Defence League)是一個成立於1918年的革命團體，據傳受到美國革命戰爭義勇兵之感召而發起，該團體目前是由一批非政府部門、從事網路安全工作的民眾組成，任務聚焦於維繫該國的線上生態、分享網路安全相關知識、強化公私部門的合作關係，以及進行危機管理以保護關鍵基礎設施。愛沙尼亞前總統烏爾維斯(Toomas Hendrik Ilves)對此表示，「國家在私部門的人才濟濟，政府部門會以愛國為名，每週一次提供這些人工作的機會。」

2017年12月25日，越南人民軍宣布成立的47特遣隊(Task Force 47)或許是最雄心勃勃的網軍計畫：作法是從部隊裡選訓1萬名以上的軍人，以抵制越南政府聲稱「和平革命」的殘餘分子、異議人士在網路上所散布的「錯誤觀點」(例如西方政治理念和生活型態)。反越南政權勢力察覺到近乎半數的越南人民使用臉書後，正透過社群媒體宣揚反政府的訴求。越南人民軍則是以「網路群集」(swarm the web)戰術進行反制，作法是開設臉書專頁宣揚政府政策並抹黑對手——與西方政治活動如出一轍。

機器和機器的對決

傳統耗時的工作技巧，已導致網路人才短缺的問題更形嚴峻。英國風險評估公司巨鴻(Titania Group)集團營運長惠廷(Nicolas Whiting)表示，「資安官絕大部分的心力都花在逐條分析和稽查工作，幾乎沒有時間因應更策略性和關鍵性的任務」，她進一步指出，「有些研發人員已經開始在

篩檢工具上加入組態分析元件，然而這些元件仍不夠精密」，她將組態分析比擬為「野戰軍砲擊自身前方陣地以尋找防禦弱點。篩檢軟體產生的偽陽性存在和篩檢結果的確認，不斷消磨已筋疲力竭的網路團隊。」

惠廷青睞的途徑是使用先進的組態分析工具，又稱虛擬網路助理，「類似狙擊手的焦點射擊」，自動化組態稽核複製「人工測試員的稽核技術，再以超越人為能力的速度和範圍，來強化單位的防火牆和網路裝置。這項技術可在數秒之間逐條稽核200項系統，也就是說數分鐘之內即可完成所有軍事基地網路的稽核，該過程若由人工處理需耗時數週。」

不幸的是，吾人的敵手也同樣針對自動化工具和人工智慧技術進行武器化。西點軍校的霍爾認為敵人正從事「威脅鑄造」實驗，他描述為一種「建構式思考未來十年威脅形態的途徑。」例如，駭客可能控制無人駕駛車輛，然後駛入群眾之中。

誠如西點軍校電腦暨網路科學教授索必斯柯(Edward Sobieski)博士告訴學生的，「我不需要一支機器人兵團，我只打算利用你手中的東西。」

只要我們的機器人慢跑時，能關上它們的「Fit-bit」運動手環。

作者簡介

Rick Adams係航空訓練、系統模擬、安全及多項領域專家。他目前是《德國軍事科技月刊》定期撰稿者，具有三十多年的知名企業與出版商經驗。

Reprint from *Military Technology* with permission.