

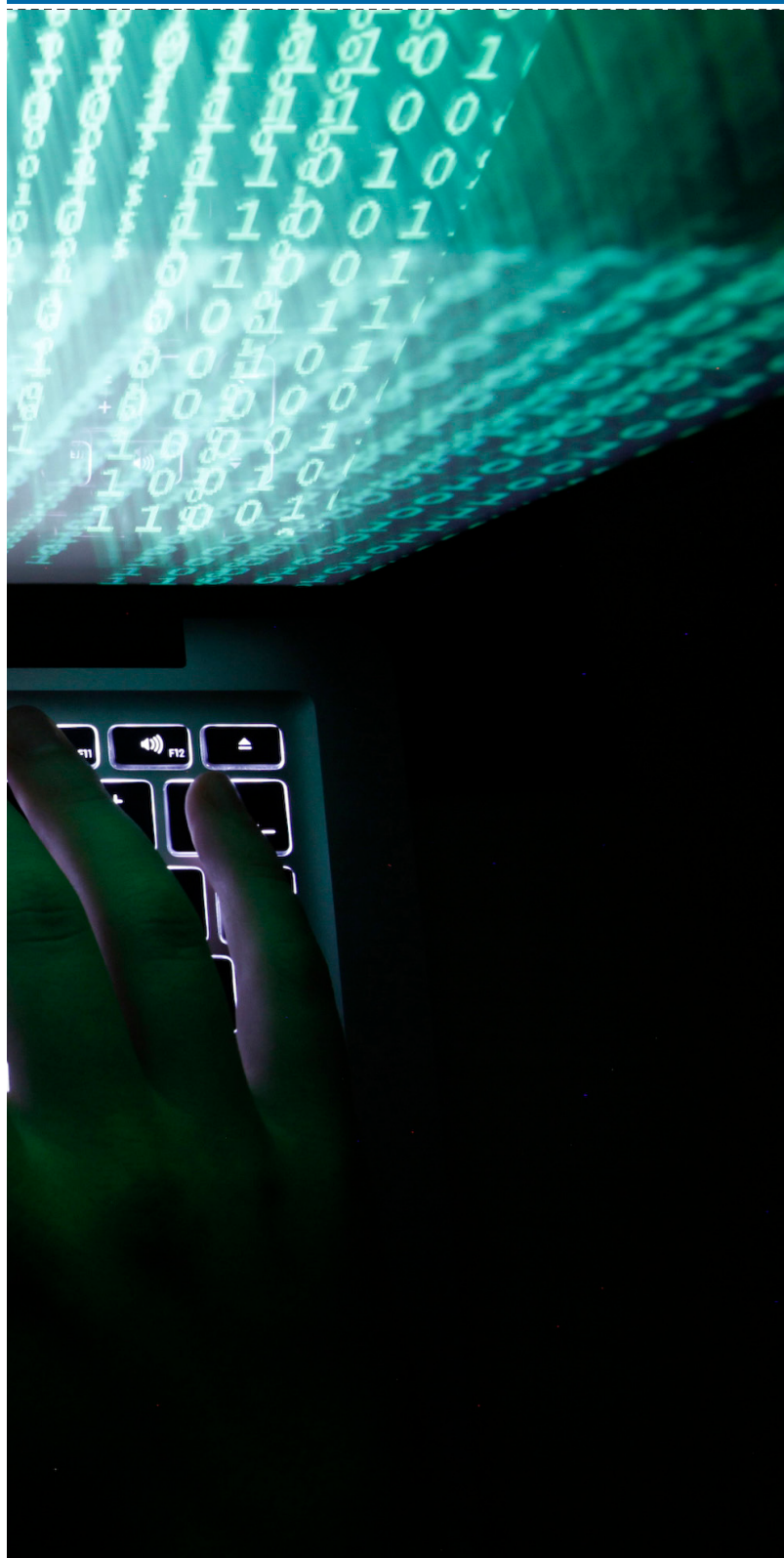
● 作者/Greg Hadley ● 譯者/趙炳強 ● 審者/馬浩翔

防範駭客入侵供應鏈

Hacking the Supply Chain

取材/2021年12月美國空軍月刊(*Air Force Magazine*, December/2021)

網際網路的快速發展，讓許多新式電子設備乃至於武器，均已數位化並且具備聯網功能，然而這也為競爭者提供一個低成本卻高成效的攻擊蹊徑，資安防護與應變作為已成為美國國防部刻不容緩的新作戰領域。



(Source: Reuters/達志)

2021年4月，時任美國國防部「作戰測試與評估辦公室」(Operational Test and Evaluation)代理主任的歐圖爾(Raymond D. O' Toole Jr.)博士，在「參議院軍事委員會戰備小組」(Senate Armed Services Readiness Subcommittee)作證時投下了一枚震撼彈。

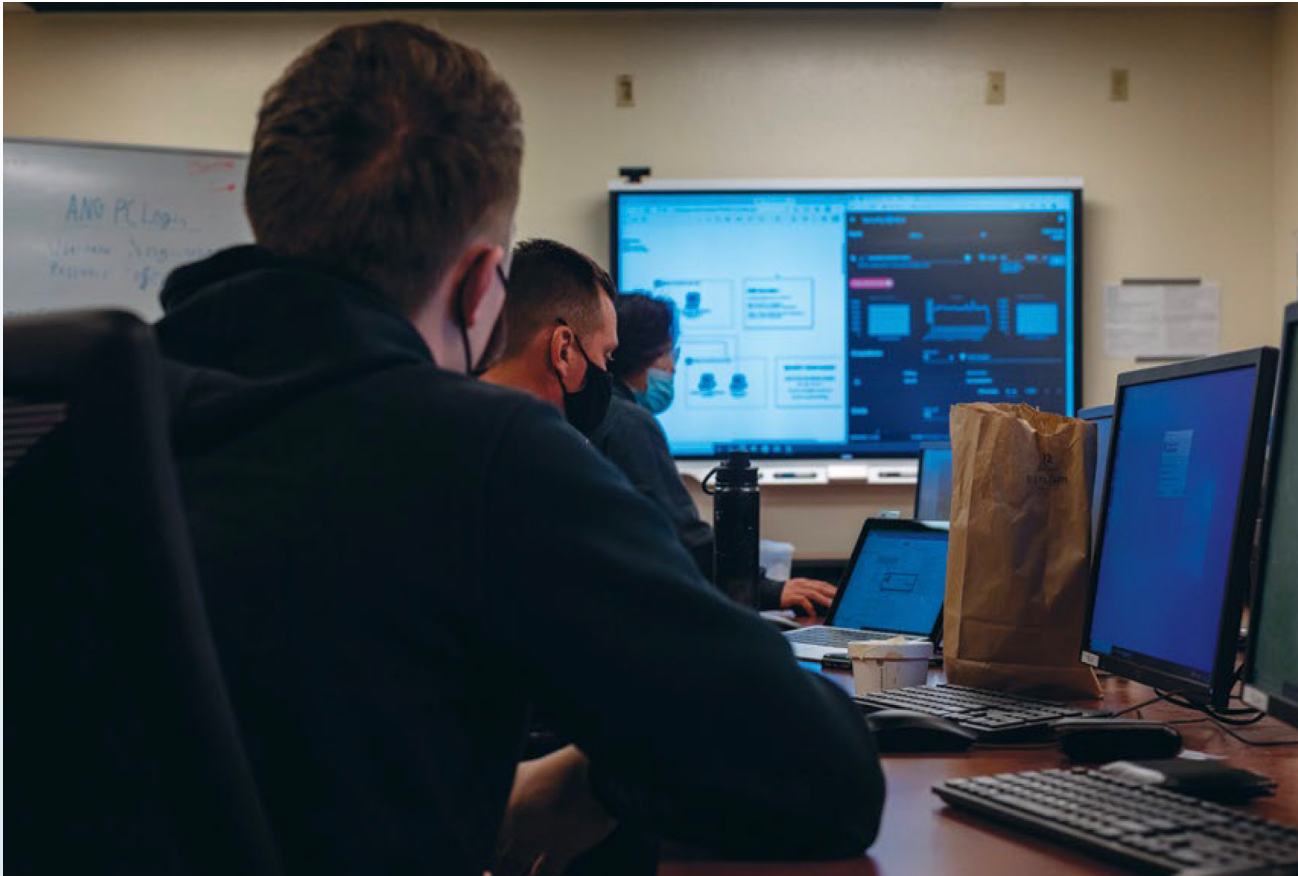
歐圖爾表示，「正如委員會所知，網路安全是最普遍存在的威脅媒介，而國防部在這方面基本上做得只能說差強人意……在2020年作戰測試與評估辦公室主任評估計畫中，幾乎沒有一個計畫能夠抵禦相關網路威脅」。

小組副主席，同時也是共和黨阿拉斯加州參議員的蘇利文(Dan Sullivan)很快感受到事態嚴重性，他說，「我們的對手經常收看我們的聽證，但此刻我卻希望他們漏看了這一場。只是我們到底要怎麼做才能彌補這些缺陷呢……這真的很讓人意外，也很讓人擔心」。

六個月後，小組主席民主黨參議員凱恩(Tim Kaine)在質詢拜登政府提名的作戰測試與評估辦公室主任格爾廷(Nickolas Guertin)時回憶起此事件。

凱恩談到他對歐圖爾的反應時表示，「參議員蘇利文和我看著彼此然後說，『這場聽證是公開的嗎？』而證人歐圖爾博士則說，『我已經在另一場公開聽證上證實此點』，但這實在讓我們感到相當困擾」。

國防部面對的網路挑戰相當艱鉅。系統愈



第152通訊分隊與內華達大學雷諾分校(University of Nevada, Reno) 網路研究社的「紅隊」(Red Team)，在內華達大學網路安全中心共同實施網路安全技能訓練。(Source: USAF/Thomas Cox)

加依賴軟體程式碼，而其中大部分包含開放原始碼元件。依賴雲端系統託管資料庫與電腦工作負載的程度愈來愈高，也增加國防部被攻擊的可能性和範圍。防止駭客入侵國防部網路的傳統網路防禦措施，已被為保護網路內部資料所建構的新戰略所取代，而這就是駭客所樂見的。

有些人認為主要挑戰是培養更具備網路能力的人才，這也正是歐圖爾所建議；格爾廷表示，這個問題中更重要的是，從一開始就該將網路安全整合到系統開發過程中。真實情況則是，在一個

日益緊密連結的世界中，每套武器系統都是網路目標。

威脅概述

早在2013年1月，國防科學委員會(Defense Science Board)工作小組提出的《韌性軍事系統和進階網路威脅》(*Resilient Military Systems and the Advanced Cyber Threat*)報告中便已提出警告，認為對手可以利用網路漏洞進行以下攻擊：

- 削弱及切斷通訊

- 操縱及破壞資料
- 致使武器失效
- (甚至可能)摧毀武器或系統

中共、俄羅斯、伊朗和北韓都認為網路提供了一個機會，可以做為美國的國防弱點，以對抗美國在軍事技術方面的優勢。該報告稱，對基礎設施和部隊進行大規模攻擊，可能「逐漸造成許多人喪失生命和對國家的控制，並產生攸關存亡的後果」該報告補充道，若要發動如此攻擊，「必須有一個既具備能力，也有意圖發動攻擊的對手」。

科欽(Klon Kitchen)是美國企業研究所(American Enterprise Institute)的資深研究員，曾致力創立美國網路空間日晷委員會(U.S. Cyberspace Solarium Commission)，他說今天不難想像哪些對手可能有如此能耐。他表示：「中國……有能力、有意圖，也曾經展示過運用供應鏈的能力來取得資訊、洩露資料，並且安插爾後可以為己所用的漏洞」。

博斯艾倫公司(Booz Allen)副總裁，身兼定位、導航和定時

(Positioning, Navigation, and Timing)業務負責人柯金斯(Kevin Coggins)表示，網路漏洞不僅會影響電腦世界，也威脅著現實世界。

柯金斯說，「這聽起來很科幻，但你真的可以透過網路阻止事態運作……人們過去不會考慮武器系統網路安全，因為你只看到武器系統的作為，某物擊中目標並炸毀建築物、某物飛過空中、某物繞行地球……但那些物體(也都是)電腦。這些物體的每一個核心中都有著一臺電腦，也有資訊不斷進出。這就說明它有許多面向會遭到攻擊，而這足以開始讓大家思考網路安全」。

正如空軍前參謀長古德芬(David L. Goldfein)上將所言，F-35便是一臺「剛好會飛的電腦」。現代數位武器透過網路與太空中的感測器連結通訊鏈路。古氏的多領域指管願景，也正是國防部現在稱為「聯合全領域指揮管制」(JADC2)的指管機制，而正如空軍前籌獲業務部門主管羅柏(Will Roper)所言，實際上是一套「軍事物聯網」。

問題是，並未有防駭客系統存在。如果可建造，就可受破壞。十年前，伊朗的網路戰部隊因控制一架美國RQ-170無人偵察機而聲名大噪。該事件凸顯此類系統具有之潛在漏洞，以及無須動用世界大國技術就能完成開發這種能力的事實。與此同時，中共和俄羅斯已經磨練出自身網路技能，並且滲透到美國政府和產業網路，洩露數量未知的資料，而更提高資訊戰的風險。

Dynetics Aerospace的國防與民用領域技術長佛格提(Kevin Fogarty)表示，「顯而易見的是，軍方正在走向伯仲同儕競爭(Near-Peer Competition)的轉變中……但我們已經在網路領域持續這種競爭一段時間，遠比在動能武器領域經歷的時間要來得更久……因此，當動能武器能力也要開始走向如此競爭模式時，便須瞭解自己與對手的網路能力態勢。然後必須瞭解這些因素對現有老舊系統，以及正在籌獲的新系統造成之影響。任何存在網路上事物，那怕只是動用到一個位元或是位元組，都會是網路目標」。



美空軍第 60 通訊中隊網路傳輸系統技術士迪雅絲(Stephanie Dias)中士，在加州曲維斯空軍基地(Travis)設定網路交換器。軍方過去重點放在保護網路，但最近的戰略則傾向於保護儲存和透過網路傳輸的資料。(Source: USAF/Alexander Merchak)

保護供應鏈

網路漏洞始於開發階段。新美國安全中心(Center for a New American Security)「技術與國家安全計畫」(Technology and National Security Program)資深研究員布蘭特(Laura Brent)說：「如果你能竊取武器系統的整套計畫，潛在漏洞顯然就會增加」。

保護合約商的網路確實是第一道防線。「網路安全成熟度模型認證」(Cybersecurity Maturity Model Certification)替合約商建立網路安全標準和訓練，這是好的第一步。然而，保護包括在海外製造的電腦晶片和次組件的數位供應鏈，卻完

全是另外一回事。

具有美國國家安全局背景的博斯艾倫公司負責人懷特(Ann White)指出，「大多數晶片已不再於美國製造……因此，我們正在研究如何識別在製造過程以及與供應鏈相關的漏洞，還有如何排除這些漏洞」。

這些零件大部分是在臺灣、中國大陸和韓國製造；中國大陸製造的零組件疑慮特別高。

有關中國大陸在供應鏈中角色的具體漏洞是機密，但這種威脅造成的影響相當明確。

科欽說，「試想，如果(中國大陸)進入晶片供應鏈，然後透過關閉軍機導航系統……或者如果可

以破壞海上通訊能力，甚至以限制我們任何平臺內基本系統電源等方式進行破壞」。

在最近的SolarWinds駭客攻擊中，俄羅斯得以入侵數百家公司和聯邦機構，包括美國國防部以及發現破壞活動的網路安全專家火眼公司(FireEye)。駭客入侵SolarWinds系統，然後等待時機，運用長期戰略透過將惡意軟體附加到合法更新來加以散播，然後慢慢散播至SolarWinds的客戶。

即使國防部能夠保護合約商的資訊科技系統並確保供應鏈安全，但這種相當複雜的攻擊也很難被發現。

懷特表示，「使用者便是一個漏洞……而這取決於使用者與系統的互動方式」。

點按電子郵件或網站上的詐騙連結、下載同事(或貌似同事)分享的檔案，或者進行任何人在正常上班日都可能遇到的其他例行公事，都可能導致意外觸發網路攻擊。

惡意軟體一旦入侵系統，便能洩露或操縱資料，導致系統產生不良結果、當機或甚至故障。柯金斯說，「如果你癱瘓掉

無人機、飛彈上的處理器，或衛星上的感測器，也沒有人可以按下重設按鈕……而且如果並未針對這種狀況設計復原機制，就沒救了。在重設和復原前，它就只是塊廢鐵」。

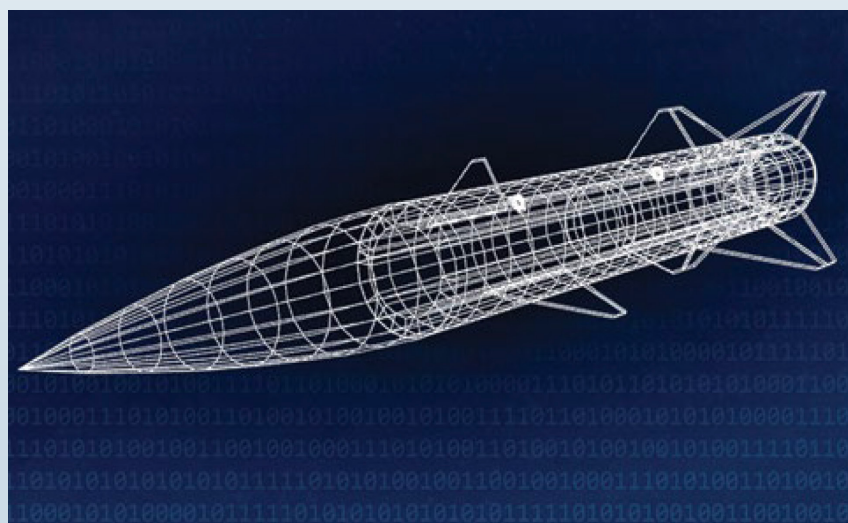
用以滲透和破壞伊朗鈾濃縮工廠的「震網」(Stuxnet)蠕蟲攻擊，導致該廠離心機發生故障並實際啟動自毀程序。這起事件通常被認為是以色列和美國合作的結果，也是目前已知最早直接影響現實世界的電腦病毒案例之一。

科欽說，「相當類似的事件可以在許多系統中做到……我的意思是，你可以關閉冷卻系統，

因此這些不同平臺中依賴該冷卻系統的其他一切機械，都可能因此過熱並停止運作……如果你擁有這種存取權限，基本上不乏可以作怪的方法」。

現下努力

美國政府問責署(Government Accountability Office，下稱「問責署」)於1997年首次將網路安全定位為高風險。如今，雖然整體網路安全性已較以往更為強大且有效，但駭客可接觸的系統範圍卻呈指數級增長。問責署在2021年的報告中表揚空軍的武器系統網路韌性辦公室(Cyber Resiliency Office for



數位分身為系統在各方面提供一種虛擬測試平臺，讓工程師能夠想像武器在輸入資料產生變化時的狀況，包括是否導入不良資料或惡意軟體。

(Source: USAF/Chris Quinlan and John James)



F-35A不僅是一架戰鬥機，也是一套飛行感測器與資料中心，能夠累積並分享大量資料，並且由數百萬個須從全球供應鏈購得之零件所組成。

(Source: USAF/Andrew Sarver)

Weapon Systems)，該部門針對如何定義籌獲系統的網路安全需求，以及如何將其納入合約等事宜，給予適合全軍參考的指導。

美空軍的《系統安全工程網路指南》(System Security Engineering Cyber Guidebook)整合網路安全至開發過程中，採用類似於「敏捷軟體開發」(Agile Software Development)中使用的「DevSecOps」(開發[Development]、安全[Security]和作業[Operation])思維。在此方法中，開發人員、安全專家和作業人員都在新系統上平行作業，而非承接作業。佛格提說，而且軟

體和硬體中網路安全方法交叉運用，也不應在此打住。

佛格提說，「『零信任』(Zero Trust)一詞不僅適用於你的個人電腦網路，也須套用在我們的武器系統架構……因此確實須審視那些結構、制定指導方針，並且確保我們將這些結構從資訊科技領域正確轉化為網路實體武器系統」。

柯金斯說，資訊科技領域應該延續至武器系統網路防禦的另一種方法「反覆更新」，也就是網路安全永遠不會被認為是完善或完備。

「(舉例來說)，這不僅僅只是『向我提出一支iPhone需求，然

後我會為你生出一支iPhone，送到你手上』而是『為我建構一種可以不斷升級的能力，並且可以不斷跟上威脅速度』；隨著威脅變化，能力轉型也相當容易……從歷史上看來，我們還未能設計出可更新或容易更改的武器系統」。

與問責署一樣，柯金斯也特別提到空軍在這方面的努力，他特別讚揚「一號平臺」(Platform One)，這是一個用在軟體的DevSecOps的平臺，專為強化防禦威脅能力所設計，同時針對不同程式仍保有彈性。

懷特補充道，從硬體來看，「數位分身」也可以增強網路安全。她說，在開發和測試階段使用武器系統的虛擬複本，可以讓各機構與合約商「模擬攻擊、模擬緩解措施，然後評估其成效」。

整體而言，增加測試向來是國會試圖解決問題的核心部分；2021年的《國防授權法》(National Defense Authorization Act)要求國防部長制定政策，定期測試主要武器系統的網路漏洞，而立法機關也已提供資金給相關實驗計畫，這些

計畫將用在培育具有網路能力的人才；一如歐圖爾所說，也就是國防部需要的人才。

然而，即便有籌獲需求、反覆更新和增加測試等作為，威脅仍然如此廣泛、普遍，以至於布倫特警告，「重要的是要意識到，無論是網路還是其他方面，都可能無法做到百分之百安全性……那麼，在允許實現關鍵任務功能的同時，可接受風險程度有多少？」

風險評估和彈性

考量國防部與空軍所面臨的現實，例如預算有限，以及在不同時期設計、建造的老舊系統，如何決定可接受的網路安全風險程度尤其重要。

懷特說，「我認為我們有許多系統都有類似假設……資訊科技系統需要網路安全，但這些具備微控制器及處理器的系統，並未連接到網際網路，因此不須考量網路安全」。

而在不同時期如此思維所衍生出的風險並沒有那麼大。佛格提說，這些系統是「煙囪式(Stove-Piped)……擁有自家指揮和控制系統……你可以保護系統，也可以選擇不加以保護，但對手無法進行很多橫向動作」。¹

現在，「聯合全領域指揮管制」試圖以前所未見的方式連接感測器和系統，布蘭特說，「你的強大與否取決於你最薄弱的環節……」。即便是在考量網路安全情況下所開發的系統，也可能因為連接到安全性較低的系統而受到損害。修復那些安全性較低的系統，也不像快速軟體更新那麼簡單。

柯金斯說，「我們很難將修補程式在舊系統上

執行，因為在這些系統上執行修補程式十分困難……系統可能必須回到原廠才能讓人員進行相關操作。在新做法中，你能在野戰層級完成這些作業，並且節省大量時間和金錢。我們目前正在嘗試更新許多舊系統，而發布一套修補程式可能須耗時五年」。

隨著時間推移，目前正在開發一款考量到安全性的系統，在這些領域中進行更嚴格測試，並且能夠接收反覆更新。此系統將會取代舊有系統，但這可能需要數年時間；與此同時，仍有一些方法可以彌補這些差距。

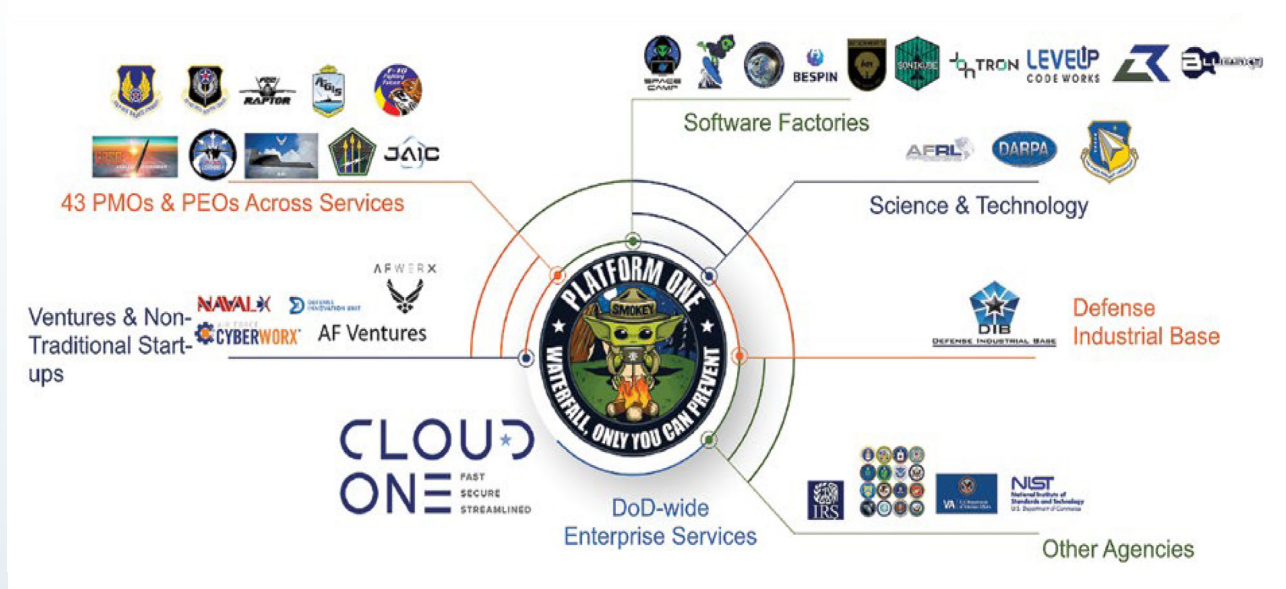
懷特說，一方面來看，「並非必須修復每個漏洞，如果這並未……對作戰產生影響，或者產生影響的可能性非常低，那就沒有必要修復。修復那些我們認為對手知道，且易受影響、易於執行，並且能取得高作戰成效的漏洞即可」。

柯金斯補充說，解決此問題甚至能不涉及軟體修補程式的部署。有時就像訓練人員操作武器系統一樣簡單。

「有一個很好的例子，有些他們不會注意到的衛星遙測資料，而這些遙測資料已經穩定傳輸了20年……我們使用全球定位系統已經很久了。但現在有些在遙測資料上的指標，顯示出可能已經發生某種攻擊，而你身為操作者可以偵測到這類問題，然後立即採取行動」。

在此例中，衛星的網路安全措施並未能阻止攻擊；但問題並不只是成功或失敗那麼簡單。

布蘭特說，「我認為我們經常以二進位方式處理其中一些挑戰，而這在某種程度上是否有效……答案是，即使當下並未奏效，系統能夠恢復



「一號平臺」透過各家工廠(如Kessel Run、Kobayashi Maru、SpaceCAMP和Unified Platform) 匯集來自美空軍的頂尖人才。它現在是美國國防部DevSecOps的官方企業服務團隊。(Source:USAF)

運作的時間和彈性程度又是如何？」

不僅系統必須具備韌性，即便在環境不理想的情況下，操作者也必須能夠使用該系統；佛格提說，「這不只是知道如何操作系統而已，你也必須知道如何在敵人積極攻擊狀態下使用系統」。

有多位專家表示，這說明國防部更須持續發展工作團隊，讓這些人才除專精於專業領域之外，也必須全面掌握數位技術。隨著武器系統本身變得愈加數位化，如此能力將會相當必要。

懷特表示，「網路安全不僅侷限在電腦領域……時至今日，就連我家門鈴裡也有電腦……室內燈具也是由電腦控制。隨著一切都與電腦有關，我們就必須更深入思考這些需求，在這些電腦都成為敵人的攻擊範圍時，對我們的意義又是什麼，以及我們如何針對這些攻擊發展強化措施並降低風險」。

作者簡介

Greg Hadley畢業於聖母大學(University of Notre Dame)，曾在州政府(南卡羅萊納州哥倫比亞)和網路媒體公司中任職。

Reprinted by permission from *Air Force Magazine*, published by the Air Force Association.

註釋

1. 「橫向動作」(Lateral movement)是攻擊者在破壞端點後使用的一種技術，用於拓展對組織中其他主機或應用程式的存取能力。橫向動作有助於攻擊者在網路中保持其耐久性，並更接近有價值的資產，還可以讓攻擊者控制管理員的機器以及相關權限和資料。