



科技武器

WEAPON

● 作者/John Antal ● 譯者/王建基 ● 審者/楊宗興

軍事雲端運用發展

Leveraging the Military Cloud

取材/2016年4月德國軍事科技月刊(*Military Technology*, April/2016)

本文旨在探討雲端電腦之運作情形，以及諸如即將問世的物聯網、流運算、同態加密等新興科技的最新發展，這些都將會在不久後對資訊取得，以及作戰方式造成澈底的衝擊。



2015年11月，美陸軍綠扁帽部隊於密西西比州美里迪安海軍航空基地(Meridian Naval Air Station)實施之「南方打擊」(Southern Strike)16號演習中，執行非戰鬥撤離課目。取自軍事雲之資訊，能強化圖中這位戰士的戰場覺知。(Source: USAF/Christopher S. Muncy)

當今資訊系統不斷演進，並逐步獲得士兵階層所需之分析大數據(big data)運算能力。大數據是一個正在演變中的名詞，在於描述經電腦分析，發現態樣、趨勢與關聯性的極大數據組，尤其是人類的行為與互動——要提供這種數據給士兵絕非易事，因為電腦基礎設施十分昂貴、雜亂數據散得到處都是，而且網路安全始終面臨著威脅。

取得複雜資訊的便利性，得以強化狀況覺知並加速決策作業程序。簡言之，在今日之作戰武器中，資訊和炸彈一樣重要。要在戰場中任何地方及時獲得安全且精確之資訊，乃是當前資訊系統的一大挑戰。在時間不斷流逝之際，士兵所要的是迅速、可靠又安全的運算系統。

「雲端運算」(cloud computing)便是提供此一能力的保證，而且其所具備的能力遠超過人們想像，但仍須克服諸多窒礙因素方能為之。

人人都該擁有

雲端運算早已問世多年，但這個名詞一直到十年前才開始

火紅，並成為一種強行行銷的工具。每個人都應該在雲端存有自己的數據，就算是渠等根本不清楚雲端在哪、甚麼是雲端。簡言之，雲端運算就是對數據的儲存與取用，以及位於雲端(而不是電腦硬碟)的程式。所以，雲端運算也可稱為「網際網路運算」(Internet Computing)，但最通俗的名稱就是稱作「雲端」。其概念就是透過在雲端的遠端伺服器網際網路來儲存、管理及處理數據，而不是在本地儲存設備(例如你的電腦硬碟機)儲存資訊及程式。這可讓使用者只要付費就能獲得運算能力、數據儲存及其他服務，一如繳費就能享受水電等公共服務。

雲端揮別傳統「垂直式」(stove-pipe)運算方式，進一步邁向分散式系統，同時也由於其不須另行設置、維持及更新基礎設施就能分享資源，進而能節省金錢。在小型行動裝置能從網際網路獲得全部的雲端運算能力之際，大型電腦硬碟機再也沒有需求必要，運算成本也因此降低。2015年，雲端運算技術以一種商業創新力量的

型態崛起。《財星雜誌》(Fortune)全球100大公司，如「亞馬遜」(Amazon)、「阿里巴巴集團」(Alibaba Group)、「臉書」(Facebook)、「谷歌」(Google)及「國際商業機器」(IBM)等，刻正努力想方設法在雲端運算方面取得領先地位，並且從市值10億美元的市場中獲利。軍方也趕上此一潮流，而且對雲端的使用需求不斷成長。目前有多種能應用在所有軍、民雲的雲端運算型式，這些不同的「雲」可分成公共雲、私有雲、混合雲及社區雲。

安全等級最低的公共雲

公共雲(public cloud)對公眾開放，其安全等級最低，但最適合商業界，許多政府機關也加以運用，以提供低成本的電腦服務。過去十年，就有許多企業提供極其多樣能力之雲端服務。公共雲的實例之一，就是「亞馬遜網路服務系統」(Amazon Web Service)，該系統是一種無所不包且不斷演進的一種雲端運算平臺，由亞馬遜公司所創設，於2006年開始對外服務，為各個網站提供線上能力。



公共雲能為企業界提供即時且價廉之虛擬基礎設施，提供毋需硬體之運算能力。

適用軍方的私有雲

私有雲(private cloud)不對公眾開放，可提供一個更安全的環境，其通常受防火牆保護，並由資

訊科技專業人員管理。私有雲之所以適合軍方，是因為能夠提供最高程度的安全性，但同時在建置、維持及操作成本上，也會比從現有公共雲購買服務的成本更高。美「陸軍分散式通用地面系統」(Distributed Common Ground System-Army, DCGS-A)第三版(代號「格力芬」[Griffin])，就是私

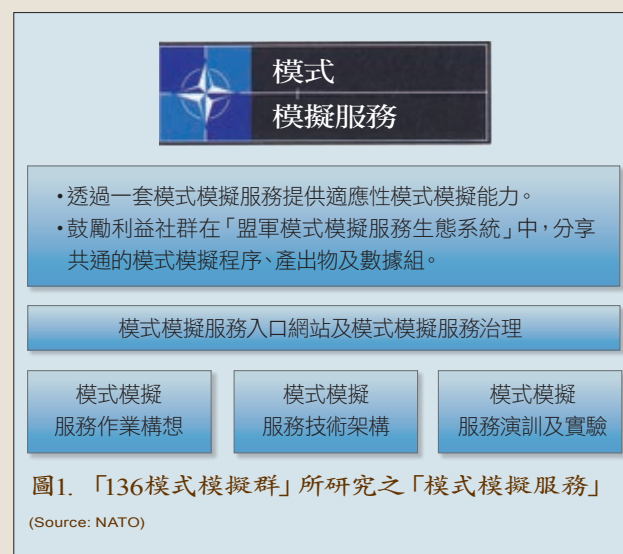
轉向新典範——模式模擬服務

北約甫於2016年2月發布的雲端運算政策，樹立了北約應遵循雲端運算之原則。此一結合模式模擬及取自雲端運算概念的產物稱為「模式模擬服務」(M&S as a Service, MSaaS)，是實現下一代模擬環境的一種相當可行方式。

就很大的程度而言，未來軍事訓練、分析與決策能力將由模式模擬提供。目前的兩個主要障礙為成本與可取用性：硬體、軟體及個人執行與運用模式模擬，都需要大量的時間與成本。此外，由於不確定的效度與臨時性處理所造成的有限信度，仍然是個問題。

模式模擬產出物對北約及軍事組織而言具高度價值，同時模式模擬產出物、數據與過程均能大量提供使用者便於取用亦十分重要。因此，在模式模擬產出物能被諸多使用者基於個人目的即時且自行取用之處，就需要新問世的「模式模擬生態系統」。這種「做為服務」的典範必須能隨時支援獨立運用，並且將多種模擬與真實系統融入一套統一的模擬環境之中。

鑒於諸多因素，以服務為本的方式咸認是實現未來模式模擬生態系統最佳方式。以服務為本的方式，以及取自雲端運算的各種概念之結合體，稱為「模式模擬服務」。最初北約「131模式模擬群」(Modeling & Simulation Group 131)，是在北約的背景下定義「模式模擬服務」，並且由於優異的工作績效，於2015年獲頒「北約科技組織」科學成就獎。



嗣後，北約「136模式模擬群」(模式模擬服務：快速部署具作業互通性且可靠模擬環境)於2014年成立，該群係一為期3年的研究任務編組，負責調查、提出及評估模式模擬服務之各項標準、協議、結構、執行成果及成本效益分析。

專案組織架構

本專案旨在定義未來的「聯盟模式模擬服務生態系統」(Allied M&S as a Service Ecosystem)，其目的在於透過持久性及臨時性模擬支援，提升北約作戰效能與效率。為達此一目的，136模式模擬群針對四大

人軍事雲的一個實例，該系統早先曾在阿富汗部署，是美陸軍第一套運用於戰鬥的戰術雲運算節點。

此一系統係專為提供地面士兵即時資訊而設計，例如運用

可預測出最可能遭遇非制式爆炸裝置路線的歷史資訊、全動態無人飛行載具影像，以及和雲端運算的直接鏈結——但該系統對使用者並不友善，有若干潛在問題尚待改進。北大西

洋公約組織(NATO，下稱北約)刻正跨出引進私有雲的第一步，藉由在歐洲投資發展一套名為「提供基礎架構的雲端服務」(infrastructure as a service, IaaS)之私有雲，作為其整體資

面向進行調查(參閱圖1)：

- 模式模擬服務作戰構想係由136模式模擬群所發展，是將模擬能力全面融入北約各項作戰任務與活動，俾最大程度提升北約的效能與效率。先前已經說明將模擬與北約全般任務與活動全面整合的益處。此外，模式模擬服務作戰構想，也對於持久性與臨時性模式模擬生態系統服務應如何有章法地加以落實加以定義，俾建構一種永續能力。
- 136模式模擬群的模式模擬服務技術架構，旨在對未來模式模擬服務生態系統之架構與技術細節做出規範。為使服務範圍儘量擴及最大，當前商業發展成果，以及現行各項標準與工具均將予以採用。根據北約資訊與通信科技政策，未來模式模擬生態系統係由各項模式模擬服務所構成，並在雲端進行配置與管理。模式模擬服務將在執行模擬作業之前提供，以大幅提升模式作業效能，並使模擬作業具備彈性且具備可量測性。
- 136模式模擬群研究任務編組不僅發展理論性構想，亦負責執行各項模式模擬服務演習與實驗，以評估所提構想並展示其作業能力。
- 模式模擬服務的入口網站，可提供知識管理能力，並做為探索、取用及管理模式模擬服務的單一窗口。136模式模擬群亦提出操作、維保，以及發展未來盟軍模式模擬服務生態系統的治理政策。

現況及後續作為

136模式模擬群目前已從16國及6個北約機構，網羅70餘位技術專家與作業人員。在136模式模擬群的固有基礎上，此一研究任務編組刻正接續奠定落實盟軍模式模擬服務生態系統的技術與組織基礎。考量未來所需，模式模擬服務的初期成果，將由「盟軍轉型司令部」(Allied Command Transformation, ACT)移交給「北約指揮管制通信委員會」(NATO C3 Board, NC3B)。關鍵成果均已於「北約電腦輔助演訓論壇」(NATO CAX Forum)、「模擬作業互通標準組織」(Simulation Interoperability Standard Organization, SISO)活動，以及各種國際與各國會議中提出。

136模式模擬群將於2017年底解編前，發展出「模式模擬服務」構想，並加以持續發展。初期經過深入研究的模式模擬服務為「合成環境服務」(Synthetic Environment Service)、「路徑規劃服務」(Route Planning Service)，以及「電腦輔助演訓報告產出服務」(CAX Report Generation Service)。此外，模式模擬服務的所有成員，亦將全力投入各項實驗活動與評估作業。

作者簡介

齊格飛 (Robert Siegfried) 博士係北約 136 模式模擬群共同主席、資訊科技 / 模式模擬專案高級顧問，以及阿迪透納公司 (aditerna，該公司係提供該範疇之特別服務與諮詢) 常務董事。



2014年，北約在斯洛維尼亞(Slovenia)波斯托伊納(Postojna)所舉行之「即刻反應」(Immediate Respond)演習中，美陸軍一等兵奎尼(Hannah Quaney)與科羅拉多州陸軍國民兵共同參與一項訓練課目，該演習旨在建立北約、克羅埃西亞及其區域夥伴國家間的作業互通性。(Source: John Antal)

訊科技及作為的一部份。盟軍轉型統帥(Supreme Allied Commander Transformation, SACT)梅西爾(Dennis Mercier)上將在2015年宣示道，「戰鬥系統的未來不是飛機。這是一套具備雲端身分證的指管通資情監偵(系統)，以及有人或無人駕駛平臺。北約將有能力與此一系統鏈結。北約須有能力建置未來的戰鬥系統，但是現在就要著手進行。」

這是北約邁向軍事雲端運算的第一步，該案預計劃將投資7,700萬美元，並且耗時十年完成。

物聯網的衝擊

至2020年前後，很可能還要更早，「物聯網」(Internet of Things)即可運作。這絕非科幻小說

情節，而是當前科技演進的必然結果。物聯網係由網路連接、具備各種嵌入式感測器的物體(諸如商用電子儀器、穿戴式裝置、環境感測器，以及安全監視裝備等)所組成。這些感測器能夠傳遞資訊數據，而這些數據能運用於多項行動，同時感測器亦具備記錄、評估與傳送指令等功能。就軍事武器系統而言，這可能包括開始及完成整個目標標定(發現、定位、追蹤、鎖定、接戰、評估)程序的感測器。透過從配備感測器的裝置向雲端自動地提供更多資訊，「物聯網」將能夠強化雲端功能。在

「物聯網」中，幾乎所有的裝置感測器都將能與其他感測器及雲端通聯，而「物聯網」的降臨，必將改變吾人生活與作戰方式。

如同之前的科技一般，各種新詞彙刻正發展當

社群雲

「社群雲」(Community Cloud)可以是性質相似實體間所安排之共享主機之公共、私人或混合性質的架構。銀行及合資企業通常在社群雲中運作。社群雲組織可分攤雲端主機成本及共用相似層級的安全度。社群雲可由內部自行管理，或由第三方提供者為之。就軍事運用上來說，多國軍事雲系統可能採用適切之社群雲架構。

中，俾用於描述雲端「物聯網」的衝擊。其中一個就是「霧運算」(fog computing)——意指當今雲端無所不在，不止在雲端的虛擬電腦系統，更擴展到極限，可與所有鏈結的裝置通聯。

「霧運算」一詞係「思科公司」(Cisco)首創之一種新典範，旨在支持無線數據傳輸，以協助在「物聯網」中遍布的裝置與雲端無縫整合。

「流運算」的衝擊

雲端雖然能使任何裝置隨時取得資訊，但是無法協助將資訊從裝置傳至雲端。這就是「流運算」(Liquid Computing)所需之處，而流運算一詞，只是一種譬喻資訊從一個裝置流向另一者的詞彙。流運算的基本概念，就是各項運算行動，不只數據，也應能輕易地在各裝置之間流動。流運算具備使各種不同裝置之數據及應用程式保持一致與最新的能力，舉例來說，其能讓使用者離開辦公室時停止在桌上型電腦的作業，然後在到達別處後，以平板電腦接續處理未完的工作。

諸如「安卓」(Android)或iOS

混合雲

「混合雲」(Hybrid Cloud)就是運用公共雲及私人雲服務的雲端架構。在此一混合設計下，日常及非機敏性的運算在公共雲中進行，而另一個由資訊科技部門所管理的私人雲，則可提供公共雲所欠缺的安全服務。這使得使用者能提高其能量，並為必須予以加密的數據，提供更高的安全程度。比起公共雲，「混合雲」架構能為軍事作戰提供更高的彈性、可量測性及安全性。今天，有許多組織也使用「混合雲」處理「大數據」。「大數據」對當今情報作戰十分重要，而「混合雲」對軍事雲作業則是重大需求。

智慧手機等諸多運算裝置的封閉系統架構，難以將運算活動從某一平臺轉至另一平臺。

蘋果公司(Apple)透過讓使用者能夠將文件完整地從iPhone傳至iPad再到iMac桌上型電腦，在其封閉系統架構取得領先地位。谷歌公司的「酷睿」(Chrome)瀏覽系統，還有微軟公司(Microsoft)在其Window10系統亦如法炮製。在「物聯網」問世後，個人使用的運算入口(智慧型手機、平板電腦、手提電腦或桌上型電腦)在各種具備互通聯能力裝置相互鏈結所構成的網絡中，將成為一種感測器。這種「雲」能在各個載臺之間實現流運算，推動封閉架構系統設計，開創更好的共享環境。

今天，官兵們已有太多的小應用程式可以用來執行有效管理。然而一個如智慧型手機般的單一雲入口(cloud portal)，乃是大多數官兵最想要的，而流運算就能提供更多助益俾加速數據共享、檢視並縮短數據與使用者之間的距離。

強化加密的衝擊

雖然雲端的益處十分明顯，但是安全仍十分重要，而且是邁向「軍事雲」的一大障礙。「國防先進研究計畫局」(DARPA)及其他機構刻正發展一套方式，以「同態加密」(homomorphic encryption, HE)的形式，為「軍事雲」提供安全保障。追溯希臘文根源，homomorphic這個字可概略翻譯成



「同樣形式」。同態加密可使運算以密文進行，並進而產生加密的運算結果，一經解密，即能與明文運算結果一致。這種加密形式提供了一種在雲端加密資訊的方式，但直到最近，加密運算仍會嚴重遲滯運算過程，使其仍難以導入實際運用。但在大量資金投入實用性同態加密後，這種狀況刻正改變中。2011年，「伽羅華公司」(Galois)獲得國防先進研究計畫局一紙價值490萬美元的合約，發展一套包括同態加密在內的演算法，使雲端更加安全。2013年，國際商業機器公司獲得了一項全同態加密專利。美國國防部在「聯邦風險及授權管理計畫」(Federal Risk and Authorization Management Program)下，刻正將雲端運算安全需求予以標準化。鑑於對雲端加密的需求日增，政府及軍方均十分重視並投入資金，以解決雲端加密問題。

策進方向

2015年12月9日，梅西爾宣告道，「未來指管就是提供確保永久戰略覺知，還有及時決策之各項能力……此一系統無疑地將採用雲端架構形式，因此其建構將需要北約與那些具備繁複架構、大數據管理或人工智慧等所需知識的廠商更為緊密合作。」

正如梅西爾所指，雲端可提供軍事部隊向後方強大虛擬運算能力取得資訊的能力，而此一能力僅需使用諸如連接網路的平板電腦或智慧型手機等小型裝置，即可在受保護的環境中安全無虞地作業。

雖然雲端對軍事作戰之助益甚廣，但是仍有



雲端將「垂直式」(stove-pipe)運算能力轉化為分散式系統並能節省經費，因其毋須建立、維持及更新架構即能分享資源。(Source: John Antal)

許多工作尚待完成，方能為官兵建構一個無縫且有效的雲端工具。物聯網、流運算及同態加密的發展，將可能加速雲端的實用價值。當這些科技成熟後、還有更多的自動系統在空中、陸上及海上部署時，戰場中各個相互鏈結的感測器數量勢必增加。將這些所有感測器與軍事雲相鏈結必然具有重大意義。不久後，每位配備連網行動裝置的官兵，將能與具備分享大數據能力的軍事雲構連。運用雲端科技興起及增強戰力科技的力量，將澈底改變一切事物，尤其是作戰。

作者簡介

John Antal係美陸軍退役上校。其為軍事事務專家，並且自2007年起擔任《德國軍事科技月刊》特派員迄今。

Reprint from *Military Technology* with permission.