作者/Tim Mahon　譯者/黃文啟　審者/劉宗翰

21世紀的網路威脅及因應之道：以北約組織為例

Cyber-the 21st Century Threats

取材/2015年5月德國軍事科技月刊(*Military Technology*, May/2015)

面對網路威脅不斷擴大，北約組織正在策擬各項整體網路防衛政策，並希冀結合產、官、學界網路資源，以強化北約各國的整體網路安全。

當2001年9月美國世貿大樓和五角大廈遭到攻擊時，全球僅有5億人口使用網際網路(約占當時全球人口的8%)。時至今日，全球網際網路使用者已接近30億人，超過全球人口的40%。從當時到今日，一系列的社會與商業攻擊事件都是透過網路領域發動(有些是實體，有些則是虛擬攻擊)，人們愈來愈憂慮下一個「重大變數」(Big One)，可能是國家支持或犯罪團體發動的網路恐怖主義，而此種恐怖攻擊所造成的災難性後果，可能將耗時數週、數月、甚或數年才能真正復原。

就最基本的層面而言，網路威脅所衍生的顧慮，會使那些把自己當成目標之對象，被迫採取惱人的反應措施。例如，早在2006年，美國太空總署已發現本身在利用電子郵件執行工作或資訊分享時受到限制。由於擔心電子郵件的附檔可能內含諸如電腦病毒、惡意程式或電腦蠕蟲等有害軟體，於是該機關立即對任何帶有附檔的電子郵件進行封鎖。此舉對於太空總署的工作人員以及必須經常與該署人員連絡的人士造成極大負擔，迫使這些人必須尋找其他可規避此一做法的替代方案，才能分享大容量的資訊、報告和分析。該個案足以凸顯潛在網路戰所存在之嚴重議題，因為不論是北約組織的計畫人員或其他網路存在弱點的各國政府安全機關幕僚，都不容忽視這個問題。網路攻擊不見得一定具有明顯的軍事本質，才能讓人感受到其威力。事實上，網路攻擊甚至根本毋須真正發生，只要簡單威脅就可能產生災難性後果，遭鎖定機關便會被迫採取預防性或先制性行動。

網路是一個全新且多變的領域，而對其安全的威脅必然會演化。(Source: Tim Mahon)

2007年，就在愛沙尼亞政府與俄羅斯發生爭端不久之後，隨即發生了震驚全球的外國駭客癱瘓該國政府與政論網路事件，讓整個歐洲響起了警鐘，包含瑞典、英國和西班牙等國，都了解到事情的嚴重性，立即策擬並公布一系列有效的策略，以反制網路威脅。2008年，在美國總統大選的高潮時刻，共和黨與民主黨的資料庫也同樣遭到境外駭客入侵，不僅嚴重損及整個民主程序的嚴整性，更讓所有安全主管機關大感震驚。同年稍後，喬治亞共和國自己認定安全無虞的政府網路，也在俄羅斯採取軍事行動的同時，遭到駭客入侵，甚至因為網路戰的跡象一直存在，導致喬治亞遭受到前所有未有的政治壓力。

2011年初，由於多個加拿大政府網站遭到攻擊，迫使該國主要經濟機關必須將網際網路連結關閉多日。這次事件表面上雖不算什麼大事，但實際影響的絕非只是暫時無法傳送簡訊或使用社群媒體而已。其真正受影響者為一般大眾日常活動中所牽涉日益龐大事務的決策流程與電子資料傳輸遭到癱瘓和損害，包含經濟、商務、財務、政治與社會等面向。即便只是決策過程的一時耽誤，如果同一時間證券市場、能源交易網或電子稅務申報系統遭到攻擊，那就可能造成資料遺失、漫長的訴訟或重大財務損失的嚴重後果。這正是網路戰如此惡質、影響如此深遠的原因所在。就涉及的對象而言，此種威脅正以指數方式快速擴大。具有敵意的他國政府與軍隊，當然是網路威脅的來源，但不斷出現的各類型極端團體，由於其目的在顛覆社會與政治體制，且精於運用各種網路領域資源，以支持並執行其計畫，因此威脅涵蓋範圍已經是十年前人們完全無法想像的程度。不僅如此，受重大網路犯罪日益嚴重的影響所及，已使美國聯邦調查局將其視為是「美國今日所面對的最重大威脅，」因此今日人們所面對的情況與北約組織、各國政府及其他組織團體相當，只要認定自身有弱點，就必須尋找其他執行工作的替代方式。

網路潛在威脅加劇已迫使各國紛紛採取措施以確保網路安全。

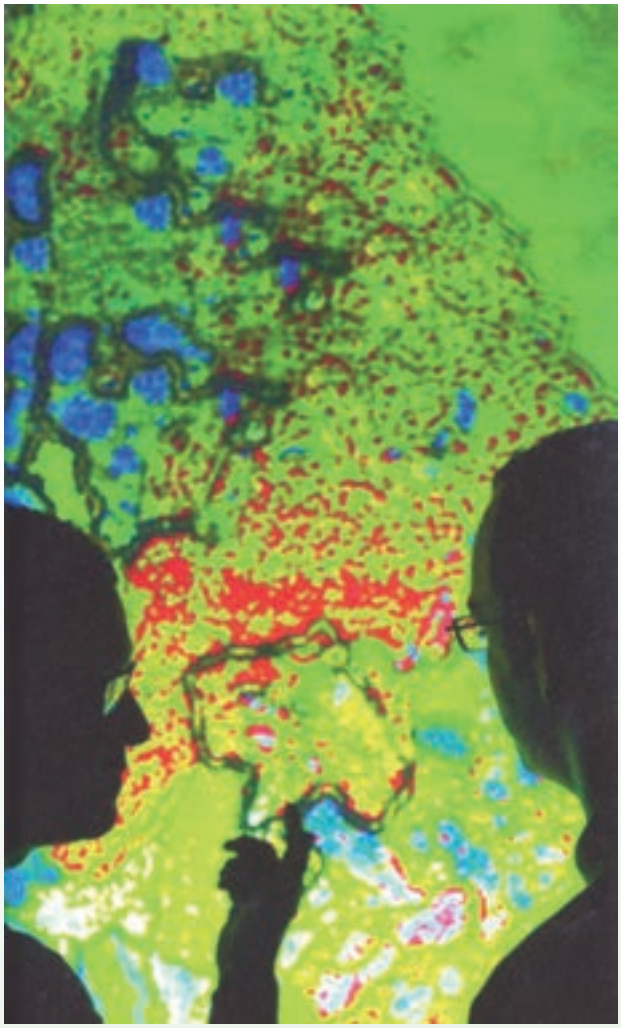
複雜、耗資且無止境的問題

讓整個問題變得更為複雜的原因是，網路戰雖為一種相當新的概念，卻無法以一種明確而細緻的解決方案，便能清楚加以區隔的可辨別性威脅。儘管網路具有獨特特徵，卻往往和更傳統與常規的攻擊方式同時發生，使潛在的敵對勢力獲得了另一種新能力。到目前為止極少的證據顯示，有任何國家已經將網際網路與既有攻擊計畫成功地結合，但這並不代表此種計畫作為尚未獲得突破性進展。

電腦科技幾乎已成為所有現代化武器系統不可或缺的一環。削弱武器系統作用的關鍵要素是，降低任何防衛措施的潛在效能。甚至於更有效的方式，當屬削弱維繫現代軍事行動的任何或所有功能的效用：亦即通信網路、戰略狀況覺知、後勤支援、運輸、飛航管理、衛星監視系統等，只要能損害或破壞上述任何一項要件的功能，就可以讓規劃最完美的防衛戰略完全癱瘓。如果所有網路行動方案同步執行，搭配協同性但不必然是大規模的傳統突襲、入侵或直接對抗手段，可以想見將有何等的災難性結果。

網路戰的入門成本非常低。網路攻擊所造成的後果往往超出人們所能想像的程度，但是所需的基本能力卻只要一小群擁有專業技術能力的個人，加上極少量的裝備和可靠之寬頻電腦通信即可。此種不成比例的效果，讓許多小國、潛在敵手和非國家行為者趨之若鶩，因為其只需運用極為廉價的投資，即可造成最大的破壞效果。

低門檻的網路戰已成為敵人對付北約最常採取之不對稱作為。



網路武器在今日世界極易取得與擴散。網路犯案者包含追求聲望的個人、政治活動分子、犯罪組織和政府支持的網路諜報活動，或是具意識型態動機的恐怖分子。這些人偏好破壞或動搖一國的安全與基礎建設、經濟和社會等。(Source: RUAG)

因應多變威脅之政策

上述各項議題已促使北約組織開始發展網路政策，運用整個盟國在各方面的資源，以反制各種既有與潛在之網路攻擊。由英國的例子即可看出，單一國家遭遇問題的嚴重程度，該國政府的加密通信網路，在2012年的時候平均每90秒即遭到攻擊一次：全年度總共遭到40萬次的網路入侵、攻擊或破壞行動。

北約所核定的第一份網路防衛政策於2008年1月公布，時間就在愛沙尼亞遭到網路攻擊後不久(此事件是主要促成原因)。然而，由於網路威脅演變快速，這項政策在之後已經過多次修訂與補充。北約組織在2014年9月的威爾斯高峰會(Wales Summit)後公布了一項極重要的政策聲明，明確將網路防衛列為北約集體防衛核心任務的重要環節。不僅如此，該項政策對於未來軍事與執法行動具有重大影響的原因在於，其確認國際法(和北約組織責任)對於網路領域的適用性等同於其他實體領域。最後，在針對反制無形但極為實際之網路攻擊威脅方面，北約組織所採取的最重要作為是致力強化與業界的網路安全合作。

值得一提的是，該峰會聲明內容使用「共同合作」(collaboration)一詞其實具有相當的針對性。透過此種針對性的文字使用，讓北約的企圖與訴求清楚表達，完全不帶模糊空間，該項政策聲明凸顯了北約必須採取更密切與更深層次的作為，以結合軍事、政府和業界資源的重要性，俾利以更為協同與快速的方式，運用一切「最頂尖」的防護手段，彌補北約組織在數位領域的能力落差。

回到政策本身，同樣值得注意的是，當前所實施的北約組織網路政策係著眼於對有效防衛的演變及執行層面產生影響等涵蓋範圍相當廣泛的議題。簡化網路防衛政策治理是一重要議題，須網羅大量才智之士、財務與實體資源，同時

因而引起額外的關注與議題，就此而言，在愛沙尼亞首都塔林成立的「卓越合作網路防衛中心」(Cooperative Cyber Defence Centre of Excellence, CCDCOE)正持續扮演要角。

首要必須提及的是，北約組織目前的重點在於防護與確保自身的通信網路，這也是理所當然的作為。確保涵蓋全北約組織之某項軍事基礎建設的安全，顯然是其所應採取之初期步驟的優先事項，尤其是諸如防空等範疇，不僅是北約集體防衛的重要支柱，隨著空中指管系統在未來數年將涵蓋整個歐洲地區，其重要性與日俱增，優先順序更是不在話下。在北約採取的網路防衛作為中，相當程度的重點係在於確保網路防衛與整體作戰計畫作為緊密整合，包含將民防緊急應變計畫整合於其他非軍事但網路防衛存在關鍵弱點的政府機關等，就算不是最主要，但也不容忽視的議題。

北約組織已採取諸般手段整合各國所擁有的網路防衛資源。

團結組織，分散威脅

然而，北約組織網路政策也闡明，保護全北約共用網路固然為優先工作，但每一個會員國都有責任針對自身實體與數位資產建立、發展與維持一套強固的網路防衛戰略。就這方面而言，並非所有國家都具有同樣的條件。某些國家仍然難以讓全政府與全民都能體認到潛在威脅之實際本質，其他國家則缺乏科技或人力資源，無法制定「專屬」(stand-alone)之策略。

某些個案的問題已演變成北約組織的一項難題，因為各會員國所擁有之諸如通信網路或數據分析中心等資產，係北約組織戰略能力的重大環節──隨著舊式防衛系統提升整合至現代化系統中所帶來的更廣泛戰略影響，此一議題將產生日益嚴重的弱點──而其中一大重點便是空中指管系統。耗資21億歐元建構一套整體防空與彈道飛彈防禦系統，是一項值得肯定且至關重要的計畫，但這套涵蓋全歐的系統卻可能因為網路事件而嚴重削弱其效能──即使是最單純型態的事件。

因此，北約組織網路政策的重要面向之一，便是提供國家層級的教育與援助，旨在確保各會員會都能建立可靠、強固的網路防衛支援政策。發展共同標準、確認關鍵弱點、建立例行性監視、監督與分析程序、發展並執行適切與相關演習，以及發展原則、標準和機制，使各會員國均能保護自身國家資產，並有效地貢獻集體網路防衛作為等，這都已成為北約的關鍵性議題。

因此網路防衛已成為「北約防衛計畫作業流程」(NATO Defence Planning Process, NDPP)不可或缺的一環，其使全北約組織可在能力發展方面採取共同做法。建立能力發展方面的相互支持目標領域，同時確保各項發展作為都能跟上日益擴大威脅範圍內作戰與科技面向之快速變化，已成為北約明智、效能導向政策的關鍵要素。

儘管「北約電腦事故反應能力」(NATO Computer Incident Response Capability, NCIRC)已能提供泛北約組織反制網路攻擊的適切等級處置能力，但該組織仍持續完成其他方案，運用各種共通能力來建立強固、反覆性與集體防衛平臺。

上圖/網路領域獨特之處在於低門檻導致權力分散。透過網路空間將訊息傳達至全球，遠比大型船隻橫跨海洋更廉價、更快速。(Source: Tim Mahon)

下圖/2014年6月3日在愛沙尼亞首都塔林所舉行的北約「和平與安全科學」(Science for Peace and Security, SPS)資訊日中，愛沙尼亞的國防投資次長兼代理國防規劃次長帕那米(Ingvar Pärnamäe)特別強調愛沙尼亞特殊歷史經驗的影響和在網路防衛的國際角色：「網路防衛和新興安全挑戰對於北約組織有極爲重要的政治性影響，需要各會員國更密切合作，方能建立一個更爲鞏固的同盟。」(Source: Tim Mahon)

儘管北約組織推動的「巧防衛」(Smart Defence)政策受到廣泛討論與報導，但仍有部分人士批評北約缺乏全面性整合作為，未能採取嚴謹做法以確保明智的集體發展能力與武獲政策。然而，就網路而言，各界仍然高度肯定北約組織在相互支援有關活動方面所採取的「整合所有環節」作為。依據「巧防衛」政策，北約組織已經推動多項旨在改善網路防衛能力的計畫。這些計畫包含針對協調各國技術與能力發展計畫的「多國網路防衛能力發展」(Multinational Cyber Defence Capability Development, MN CD)專案；針對各國迫切需要的「多國網路防衛教育訓練」(Multinational Cyber Defence Education and Training, MN CD E&T)專案；以及為使政府與業界密切合作，提供快速與有效反制電腦入侵與攻擊知識庫所需之「惡意程式資訊分享平臺」(Malware Information Sharing Platform, MISP)。

建立全面性的網路安全覺知是未來各國必須致力推動的方向。

教育、覺知與資訊傳播的關鍵性

如前文所述，某些國家目前所遭遇的挑戰之一，便是如何確保全國上下均擁有充分且不斷進步的威脅認知水準──包含政府所屬機關和公共監督機構，以利政府相關活動能獲得支持和相關的經費。就此一範疇而言，卓越合作網路防衛中心所擁有的能力及其推動相關活動，將具有絕對的關鍵性。

卓越合作網路防衛中心是北約組織在網路領

域中公認最首要的研究與訓練機構。因此，該中心幾乎就是當前網路防衛戰的最前線，負責提供北約組織及所有會員國廣泛項目之教育、諮詢和研發服務，包含支援與安排整個北約組織日益增加的網路相關演訓活動，其中每年的「網路聯盟演習」(Cyber Coalition Exercise)可能是這些作為中最具指標性之項目。

然而，卓越合作網路防衛中心並非解決教育與強化覺知需求的唯一機構。設於義大利拉提納(Latina)的「北約通信暨資訊系統學校」(NATO Communications and Information Systems School, NCISS)，長期以來也扮演卓越中心的角色，負責提供北約大多數通信與資訊系統之操作與維修訓練——事實上，該校近年來亦提供非北約會員的國家各種技術訓練。北約通信暨資訊系統學校未來將利用該校遷移至葡萄牙的機會，重新規劃其服務項目，將網路防衛議題列為更主要的重點項目，除了專門提供操作與維修訓練服務外，也將致力各項提升覺知的專案。

今日負責解決網路問題的安全專家們，對於此種新科技的全般影響了解程度，正如同當年核子專家們在首次核子試爆後數年的情況一般。

(Source: Tim Mahon)

在操作訓練層次上，北約組織所屬司令部與機關也運用本身的各種能力，重新著重於網路戰相關議題。例如，位於挪威斯塔凡格(Stavanger)的「聯合作戰中心」(Joint Warfare Centre)就是專門負責提供三星、四星上將司令及其所屬幕僚建構性訓練的主要機關。運用模擬工具、實兵演訓，以及廣泛「建構性」或「兵棋推演」設施，高階司令及其支援單位能運用、預演、實作和評判各項戰術與程序。今日所有北約的主要演習都會包含社群媒體網路項目，納入測驗與訓練各級指揮官的作戰環境。例如，聯合作戰中心發展出一套等同臉書和推特的模擬演訓系統，定期在訓練想定中導入不確定與擾亂因素，使指揮官的計畫作為受到無預警輿論事件和刻意顛覆的考驗。導入無預警的網路狀況，是針對維持與改善作戰整備的關鍵項目——還有什麼例子會比在演訓中加入完全不預期且具有潛在毀滅性的狀況，更有助於讓人們了解某些能力對於戰備的破壞效果呢？

北約總部和所屬機關與設施

所構成的複雜、多面向架構，正在運用當前各地方不同的能力提供協助，使對抗網路戰的強固防護網能不斷進步。德國奧柏安梅高(Oberammergau)的北約學校，提供北約部隊教育訓練，將各種網路防衛原則應用到既有及未來可能變化的各種政策、作戰、戰略和準則。在羅馬的「北約防衛學院」(NATO Defence College)也提供支援性環境，將網路議題對領導統御思想與戰略思維的影響融入其教育文化內容。

集體性作為

北約組織不可且不應認為自己可以單槍匹馬解決網路安全問題。歷史教會世人，當面對潛在的毀滅性威脅時，社會各階層應團結在政府的領導下，採取今日我們名之為「國家總動員」(whole of nation)的處置方式。確保充分網路防衛手段的必要處置方法亦復如此。否則，人們必然會面對一個截然不同的結果，因為若無法採取「國家總動員」作為，這些所謂必要防護手段在受到考驗時，就不太可能達到充分的效果。

創新作為多半來自業界。這並不代表政府就無法創新──但發明的泉源和針對問題解決能力發展革命性與革新性的做法，經常都是來自業界所屬組織。掌握此種能力，針對似乎愈來愈難以駕馭的問題，找出極新且可能更具無比效率的解決方案，是一個需要政府與業界建立更密切合作關係才能找到答案的問題。

北約組織的網路政策已確認業界為網路空間之要角，且要完全感謝業界在此一領域所提供的關鍵科技專業本質與創新。「北約企業網路夥伴關係」(NATO Industry Cyber Partnership, NICP)專案之目的在於，培養與促進北約組織與業界之間的志願性交往。面對軍文機關間日益模糊的界線，該專案企圖以既有基礎建設和非正式關係為基礎，創造軍文合作的新穎與精巧做法，俾利充分運用諸如各國「電腦緊急應變小組」(Computer Emergency Response Team, CERT)等既有設施，同時確保未來組織架構能符合不斷變化的集體性、強固性與有效的網路防衛需求。

網路戰已不再只是科幻小說的情節而是具體存在之嚴重威脅。

常言道，國防如同一張保單。如同所有保單一般，國防這張保單亦有其保費，且其額度會隨風險環境變化而調整。一個精明的車主必然會確保其車輛保險盡可能涵蓋各種實質和潛在的威脅，同時管理不太可能發生之威脅，俾降低保險成本。吾人的問題(抑或北約組織的問題)在於，網路戰已不再是一種神秘威脅，大部分只存在科幻小說家或陰謀論者的心中。它是一個千真萬確的威脅。在美國，針對政府或民間網路用來使社會運行無礙之關鍵應用軟體所發動的攻擊，平均每2秒就會發生一次。要研擬有效防衛措施來對抗那些潛在的網路攻擊，將需要軍方、政府和業界建立前所未有的密切合作。

作者簡介

Tim Mahon係德國軍事科技月刊常駐倫敦特派員。

Reprint from *Military Technology* with permission.