

網絡軍團招兵買馬 無人機橫行無忌

美「寒戰」炮火禍全球

德國柏林圍牆1989年倒下，宣告冷戰（Cold War）時期結束；美國2001年起發動全球反恐戰爭，戰火至今亦已漸減。美國總統奧巴馬宣稱「戰爭洪潮已退」，卻將矛頭指向崛起中的中國，把這個經濟增長是美國4倍、預計2017年甚至可超越美國成為最大經濟體的國家設為假想敵。專家指，世界已進入全新的「寒戰」（Cool War）時代。 ■香港文匯報記者 余家昌、陳國麟

「寒戰」一詞最先由權威雜誌《外交政策》行政總裁兼特約編輯羅特科普夫提出，用以形容「因為經常涉及攻擊策略，故較『冷戰』暖一點，但又未至於動武互損的『熱戰』」的戰爭。同時，寒戰另一定義是因為此類戰爭往往動用全球最尖端、最酷（Cool）的科技，與冷戰相比，更大程度改變人類戰爭模式。

可癱瘓電網 無交戰守則

剛卸任的美國前防長帕內塔去年10月坦言，網絡世界將成為下一個「珍珠港」。他表示，具敵意的國家或極端分子可透過發動網絡攻擊，令載有致命化學品的火車出軌、污染主要城市水源或癱瘓全國供電網，威脅不容忽視。奧巴馬上月国情咨文將網絡戰列作重點，五角大樓更計劃網戰人手由900人增至4,500人。

美國為了打擊伊朗核計劃，於2009年起先發制人，使用「震網」（Stuxnet）病毒攻擊伊朗地下核設施，於翌年摧毀近千座離心機。前中情局（CIA）局長海登形容，網絡攻擊是「全新、未被使用過的兵器」，將徹底改變戰爭本質，堪比當年投落日本長崎和廣島的原子彈。專家指，網絡攻擊並不如路上交通或國際金融等有明確守則和規條，帶來嚴重後果的危險性遠超以往的武器。

濫用新兵器樹敵 勢遭報復

此外，能夠殺敵於千里之外的無人偵察機，也是另一種足以改變戰爭模式的兵器。據估計，美軍無人機自2008年迄今擊殺逾3,000人，當中無辜被殺平民多達400人。白宮聲稱，無人機殺害平民數目較少，較傳統兵器「人道」。但華府顧問厄爾曼指出，無人機不僅造成平民死傷，亦會激起受襲地區對美國的更強敵意，令美國四處樹敵。

前特種部隊指揮官麥克里斯特爾坦言，出動無人機對美軍而言，只是按幾個按鈕，但被炸一方經歷卻如同戰爭，美國必須慎防濫用，否則勢將遭到報復性攻擊。

學者福山：國際格局恐大亂

1990年代以《歷史之終結與最後一人》一書成名的日裔美國作家弗朗西斯·福山指出，寒戰基本概念在於美國希望從前線抽身的同時，憑藉無人機及網絡攻擊等新世代遙距武器繼續發揮影響。他警告，寒戰或漸漸成為美國孤立主義的掩飾，一旦以美國作靠山的盟國發現美方支援不再可靠，恐引發連鎖反應，國際格局或大亂。

電腦病毒盛行 多國納作戰武器



網絡武器近年迅速發展，至今已有近160個國家參與網絡間諜計劃，美、俄、印、英、日等國軍隊更將電腦病毒正式列入作戰武器。

美：重點提高攻擊能力

美國國防部前年宣布斥5億美元（約39億港元）研製網絡攻擊武器，以應對日益增強的網絡戰威脅。國

防部先進研究項目署（DARPA）主任杜根當時指出，為使敏感的電腦系統免受攻擊，當局需要「更多更好的選擇」，必須在進攻和防禦工具兩個方面投資，並將重點研究如何提高網絡攻擊能力。

英：擲77億增網絡防禦

2010年美國和以色列「震網」病毒攻擊伊朗離心機，令英國意識到網絡防禦的緊迫性，除加緊研製網絡武器，更追加6.5億英鎊（約77億港元）用於網絡防禦與安全。有英國高官指，儘管網絡武器不會取代傳統武器，但將會成為國家軍火庫的一部分，是英國首次承認網絡武器研發計劃。

日：力爭制網權

日本不甘在「制網權」上落後，早已加緊構建「網戰部隊」，秘密研製網絡武器多年，包括具備攻擊能力的電腦病毒。《讀賣新聞》稱，這種武器可反向探知外部網絡攻擊的直接攻擊源，還可順藤摸瓜，直搗將攻擊源電腦作為「跳板」加以操控的「後台」電腦。

全球最著名的其中一次網絡戰，是美國對伊朗納坦茲核電站發動的「震網」（Stuxnet）病毒攻擊。2010年春，此病毒控制了該國離心機操作電腦的運行，並篡改監控錄像畫面，導致約1,000部離心機報廢，約佔全部的1/5，使伊朗鉅額濃縮能力倒退數年。

「震網」是首個專門攻擊物理世界基礎的蠕蟲病毒，包含空前複雜的惡意代碼，主要通過「U盤」和區域網絡進行傳播，只要目標電腦使用微軟操作系統，病毒便會偽裝成「RealTek」與「JMicron」兩大公司的數碼簽名，順利繞過安全檢測，自動尋找及

「震網」襲伊核設施 美以幕後黑手

攻擊工業控制系統軟件，甚至使設備失控自毀，而工作人員卻毫不知情。

毀離心機 核計劃倒退兩年

「震網」還能自我複製，並將副本通過網絡傳輸，任何個人電腦只要和中毒電腦相連，就會自動傳播給其他相連電腦，造成連鎖反應，最後癱瘓整個網絡。由於此病毒相當複雜，程式設計員需很了解工業生產過程及基建，背後有一支非常



■伊朗總統內賈德巡視納坦茲核設施。資料圖片

美軍4大網戰武器

電腦病毒	電子生物
●包括「邏輯炸彈」、「軟件嗅探」、「蠕蟲」等破壞性病毒。 ●可通過網絡攻擊，癱瘓敵方指揮系統，也可實施單系統攻擊，破壞獨立作戰平台。 ●平時潛伏在電腦或武器系統，到預定時間突然爆發，毀掉所有數據，或阻止彈頭爆炸。	●能否噬電腦電子零件，並使電子線路絕緣，像微生物吞噬垃圾和廢料一樣。 ●對作戰人員產生電子生物干擾，破壞其戰鬥力。 ●美國國防部研製「神經電子」武器，可令電腦和雷達屏幕產生不易覺察的閃動，使操作員神經性頭痛，視覺細胞受損。
電磁脈衝	電腦黑客
●坦克、艦艇、導彈以及電腦裝備發射帶病毒的電磁波，可使電腦程序錯亂或刪除，武器無法正常工作。	●專家將美國一架無人機改造，能從空中展開網絡攻擊、監控手機及破解手機PIN碼，藉此竊聽電話，甚至假冒手機訊號發射塔。



■美國加緊組建網戰部隊。圖為美國空軍網絡指揮中心。資料圖片

戰爭的「文明外衣」

李鍾洲

戰爭形態隨人類社會發展而演進，傳統戰爭講求殺敵佔地，到了上世紀美蘇冷戰則訴諸核威懾，避免真正開打。進入「寒戰」時代，電腦病毒、電磁脈衝武器和無人機等高科技兵器大行其道，標榜有效打擊並盡量減低人命傷亡，向來野蠻血腥的戰爭似乎披上一層文明的外衣。

傳統戰爭是浩大的政治和軍事工程，入侵者再強大也好，都要千方百計想個冠冕堂皇的理由，為敵方羅織各種罪名，為宣戰合理化，接着就是繁複的動員、軍需運輸和後勤任務，而寒戰幾乎完全顛覆過往戰爭的概念，衝擊舊有的外交、國際法和主權觀。

以網絡戰為例，無需正式宣戰就可施襲，亦沒所謂前線，不見領土被侵、不聞半響槍聲、嗅不到一絲硝煙味，戰爭可能早已降臨。兩國網絡部隊躲在秘密作戰室，指揮最先進的電腦病毒，在虛擬世界你攻我守，但與此同時，兩國仍維持正常外交和經貿來往，普羅大眾仍蒙在鼓裡，彷彿一切相安無事。

出動無人機「反恐」，亦是另一種廉價的戰爭手段。軍官安坐控制室，遙控無人機轟炸目標人物，如玩電腦射擊遊戲。這與在陣地冒槍林彈雨作戰相比，兩者對戰爭、對生命價值的體驗不會一樣。

美國內戰南方軍的羅伯特·李將軍曾慨嘆：「幸好戰爭如此駭人，否則我們會打到樂此不疲。」當寒戰打得如此便宜方便、如此「文明」；當指控某方開戰，就如向賽車手開起違罰單般可笑，戰爭還算什麼，和平還算什麼？也許，只有在網絡戰癱瘓社會運作，在濫用無人機而招血腥報復之時，人們才會反思，戰爭的文明外衣只是一件國王的新衣。

筆走波瀾

安坐辦公室殺敵 「感覺很不真實」

美國空軍機師斯科特曾駕駛F-16戰機飛過伊拉克上空，現在他卻只需安坐紐約州的空軍基地，單憑操作桿和幾個按鈕，便能指示「死神」無人機於千里之外殺敵。談到外界將操控無人機比擬作電子遊戲，斯科特強烈否認，強調所有無人機操控員都明白，每一下按鈕可能奪走的都是實實在在的生命。



斯科特的日常生活與一般上班族似乎無分別——早上從家中出發上班，閒時帶孩子上學或參加學校活動。他坦言，坐在舒適的座椅發動戰爭的感覺很不真實，但每次向目標發炮時，都會令他汗毛直豎，儼如親身駕駛戰機殺敵一樣。

「我對敵人沒任何感情」

斯科特指出，無人機操控小組通常會透過鏡頭觀察目標一段長時間，制訂計劃後才實行攻擊，並非如外界所言般濫轟亂炸。他稱自己通常會等待目標離開家人和孩子時才發動攻擊，且每次按鍵前均要調整心情：「我對敵人沒任何感情。我被委派任務，然後執行。」

睹血腥影像 難釋懷

無人機上的高解像鏡頭容許操控員目視攻擊成果，傳送回來的影像通常都非常血腥。斯科特指出，影像通常是目標被炸得支離破碎，但亦見過誤炸時被波及的兒童或美軍屍體呈現在屏幕上。他表示：「我不斷告訴自己『擊殺目標有重要原因』，但對那些鏡頭卻永遠無法忘懷。」

傳染性極強的病毒，是網絡戰最重要及最具代表性的武器之一。普通病毒一旦放出去，傳染範圍和破壞效果有多大、流行時間有多長，病毒製造者多數沒把握。病毒武器則不同，它須盡量做到只針對敵對國家電腦和網絡，不能波及其他無關國家甚至本國，否則導致敵我雙輸，或損害中立國家利益，引來輿論譴責。

病毒武器如同導彈，有精確目標定位和識別能力，可藉其他電腦和網絡傳播，但只破壞特定範圍的目標。它還有遙控功能，一旦戰事結束或在特殊需要時可自毀。病毒武器另一特徵，是擁有極強傳染能力，可在不同操作系統之間傳染，除了微軟視窗系統，Unix、Linux等亦難倖免。它還可跨硬件平台傳染，普通電腦、智能手機、平板電腦和工程電腦等「一網打盡」。

手機板電腦無倖免 病毒武器易傳染