漫談網路戰爭

doi:10.29752/NST.201102.0013

新社會政策, (14), 2011

作者/Author： 張國城

頁數/Page： 59-61

出版日期/Publication Date：2011/02

漫談網路戰爭

張國城
台北醫學大學助理教授

網路戰爭是現在新興的戰爭型態。《時代》雜誌2009年11月18日報道，中國不斷而且更多地滲透美國網路、竊取機密，並可能在戰爭爆發時進行電子攻擊。台灣國家安全局局長蔡得勝在2010年11月也在立法院指出，該局網站從1到10月，每分鐘被駭客攻擊11.56次，每個月被攻擊將近50萬次。蔡得勝表示，侵擾來源的主要位置，以台灣304萬次最高，佔了60%，不過，網軍的攻擊方式通常會透過第三地迂迴的進攻，中國大陸是主要攻擊來源。[1]顯然，某些國家已經把網路攻擊作爲一種戰爭工具，讓網際網路變成了戰場。

本文將就以下幾個方向來進行討論：

一、 網路戰爭的可能性

二、 網路戰爭的危險性

三、 網路戰爭的迷思

四、 小結

一、 網路戰爭的可能性

網路戰爭的可能性在於：

(一) 現代世界太依賴網路，包括軍事領域

網路24小時開放，又能快速傳送大量文字、圖像、聲音與視頻資料，且跨國運作，同時和傳統通訊手段、儲存資訊的手段相比，在成本上大爲儉省，這都是人類不斷加深依賴網路的重要原因。現代世界對網路的依賴是人盡皆知的，金融、貿易和通訊領域幾乎已經完全依賴網路，如果網路受損或中斷，交易無法進行，則引起的衝擊非同小可。甚至比實體經濟建設的攻擊和摧毀還要大。

在軍事上，網路即時通訊和同步通訊的功能讓各載台將能夠高效連結，讓指揮管制的層級能夠扁平化，又能快速傳遞命令與計畫，所以成爲現代軍事事務革命的主要象徵和依據。美海軍在1997年4月提出「網路中心戰」(Network Central Warfare,NCW)概念，就是通過全球資訊網路，將分散配置的作戰要素集成爲網路化的作戰指揮體系、作戰力量體系和作戰保障體系，實現各作戰要素間對戰場態勢感知共用，最大限度地把資訊優勢轉變爲決策優勢和行動優勢，充分發揮整體作戰效能。[2]如今NCW已經成爲美軍的主要作戰準則，並且實際運用到阿富汗和伊拉克戰爭中。

(二) 網路戰爭不必像傳統軍備那樣投資巨大

若只是想在網路上攻擊敵人，不需要如傳統作戰那樣組建龐大的部隊，也不需要龐大的後勤支援體系，更不須花費龐大資源和成本實施訓練。且相關從事網路戰爭的部隊和網路上的軍事行動在訓練和計畫階段容易保持隱密。

(三) 網路戰爭暫時不至於引起全面性的衝突和對抗

目前雖然尚未正式爆發網路戰爭，但是有不少國家已經遭受大規模的網路攻擊。最近的一次是2010年11月23日，愛沙尼亞出現網際網路癱瘓，全國範圍內廣泛應用的網際網路身份確認系統停止運行，使需要通過該服務系統進行身份確認的金融和法律等方面的活動受到嚴重影響。但是目前各國還沒因爲遭受網路攻擊而發動軍事報復的前例，因爲在很多狀態下，網路攻擊難以找到「兇手」，也因此不會引起大規模的衝突。

(四) 網路戰爭被弱小一方視為是有效的戰爭工具

數年前曾有一本書名爲「超限戰」，引起眾多討論。有人就指出軍事弱勢的國家可

1.http://www.voafanti.com/gate/big5/www.voanews.com/chinese/news/20101116-TAIWAN-NSB-WEBSITE-ATTACKED-CHINESE-HACKERS-108418544.html
2.http://news.xinhuanet.com/mil/2008-03/25/content_7855919_1.htm

以利用駭客、病毒等方式對先進國家的軍民網路發動攻擊，形成典型的「超限戰」。

(五) 網路戰爭缺乏有效的國際法規範

國際法對於戰爭的規範以不得攻擊平民和非軍事目標爲主，但是網路戰爭很明顯地經常是以非軍事目標爲主。而且許多網路駭客是平民，除非透過所在國家的國內法，否則無法予以制裁。在許多狀況下更難以確定網路戰爭的發動者來自於哪一國，是個人行爲還是由官方所指使，是純粹好玩還是別有目的。如此都讓國際間制定一定的國際法原則用以約束網路攻擊有相當大的難度。

二、 網路戰爭的危險性

(一) 網路戰爭有可能造成社會機能的嚴重失靈或癱瘓

網路戰爭可能以入侵和干擾一些機構的網站與伺服器的運作（比如非法遙距控制、盜取洩漏資料、散播電腦病毒、發放垃圾訊息或假訊息、癱瘓服務等）來進行，藉以威脅該機構和有關人員，甚至配合其他的宣傳、心理作爲來行動，使目標者之利益和聲譽蒙受損失。這種損害可能難以估計，甚至超過有形的軍事攻擊。因爲有形的軍事攻擊事先必有一定的徵兆，同時現代軍事發展的態勢已經可以讓戰爭及其附帶的損害盡量遠離平民。這不僅僅是人道及政治因素，而是現代化精密武器越來越昂貴，沒有必要浪費軍事價值太低的平民身上。但是網路戰爭首當其衝的受害者可能是平民和民用設施。 結果是社會機能的嚴重失靈和癱瘓，損害可能大於固定資產的損失。

目前中東地區任何國家若有一油田遭攻擊破壞，損失可能是以數十億美元計算，但若該國的外匯交易系統遭人攻擊或破壞，引起的連鎖反應損失可能是以數百億美元計算，同時會直接波動到世界的其他地區。

(二) 網路戰爭有可能擴大戰爭的危險

因爲網路戰爭的型態之一是散播假訊息，因此在劍拔弩張的雙方，可能強化誤解而增加戰爭的危險。若一國的軍事資訊和通訊系統遭網路戰爭破壞限於盲目，很可能會被理解爲是假想敵即將發動戰爭的徵兆，因此可能引發防衛反應而眞的讓事態惡化爲戰爭。

三、 有關於網路戰爭的迷思

(一) 網路戰爭的體系日益複雜，不只是三兩名駭客可以解決

雖然在網路上攻擊敵人不需要組建龐大的部隊，購買大批戰車、飛機和軍艦，相對也不需要龐大的後勤支援體系，但是美軍NCW體系經過幾年的發展，還是一個規模極其龐大的巨系統，從資訊化作戰中資訊的獲取、傳遞、處理、利用等環節來看，其核心系統作要由戰場感知、資料鏈、資訊傳輸、敵我識別、導航定位、電視會議、數位地理、類比仿眞、資料庫等九大系統構成。目前各國都發現若要和美軍協同作戰或是抗衡美軍，不建立起以上的各個系統恐怕是不行的。因此多半仿照美軍的概念進行，依次建構以上的各個系統。所以單靠幾名駭客就能癱瘓他國網路的小說或電影情節然可能性不是完全爲零，但成眞的可能性將越來越低。

(二) 網路戰爭仍須其他戰爭形式予以配合

癱瘓敵國網路當然可能造成嚴重的混亂與損失，但若沒有其他的戰爭形式配合，還是不太可能逼使一個國家放棄既有的政治與戰略目標。而有形的軍事力量也不會因爲網路戰爭化爲烏有，只是效能和戰力會減低，但若攻擊的一方沒有足夠的實體軍事力量趁著受攻擊的一方在混亂和失序之中發動攻擊，則充其量僅能發揮恐嚇的效果。

(三) 網路戰爭暫時難以改變現實國際社會中的力量對比態勢

雖然軍事弱勢的一方有利用網路戰爭有效打擊較強對手的可能。但是許多軍事強國同時也是網路強國，一些弱勢國家所能採用的手段強勢國家一樣可以採用以反制。以中國而言，被認爲是許多網路駭客攻擊的策源地，問題是中國自己的經濟和社會運作也越

來越依賴網路，若大舉進攻他國網站，別國也可以用類似手段實施報復。

小結

如何防止網路戰爭的損害，是各國未來國家安全和軍事建設的重要課題。在這方面有一些值得注意的方向：

(一) 網際網路並不是「公有的」，而是一個多數爲私人擁有之電腦網路的網路；很多也經由政府單位或私人部門的合作來完成。許多掀起網路戰爭的駭客也是透過私人部門的電腦和網路伺服器，攻擊的也是民間目標，因此國安和軍事單位應該更廣泛地與民間部門結合，尤其是經營電腦網路的網際網路服務提供者，他們可以在辨識被病毒感染的電腦和偵測病毒攻擊上負起更重要的責任。

(二) 運用各種防禦手段，包括強化對電腦加密，實體隔離等，防止敵方（或駭客）進行電腦滲透來竊取電腦情報使「駭客」無計可施。

(三) 認清網路戰爭仍然有其侷限性，不必過度誇大其威脅，或是因噎廢食，自我減緩資訊化、網路化的腳步。因爲網路的特性對於軍事戰力的發揮具有無比的重要性。

(四) 平時應該建立「資料庫」的概念，對於發生過的網路攻擊詳加紀錄，作爲爾後因應的參考，並可由敵方對我方的網路攻擊方式中研擬精進我方的網路攻擊能力。美軍用於資訊化作戰的資料庫規模就龐大。目前已建立了各種大型資料庫1000多個。在伊拉克戰爭中，美軍所應用的資料庫存儲了多達70萬億位元組的資料資訊，其資料量是當今世界最大的圖書館——美國國會圖書館的3倍。

只有正確理解加上充分準備，方能使我們在網路戰爭中的損失降到最低，進而掌握主動，成爲贏家。■