美中網電間諜戰發展情勢研析

曾復生 博士
國家政策研究基金會國安組顧問

一、 前言

2021 年 2 月 23 日，美國國會參議院情報委員會針對「太陽風事件」，邀請政府官員與產業代表舉行聽證會，並要求行政部門積極應對中俄等國「網電間諜戰」威脅。此前，美國務院亦曾經於 1 月下旬宣布，拜登政府將採用「更全面、更系統性」的作法，解決美國網電資通內容與技術，遭受中國竊取與盜用的問題。

美中「網電間諜戰」隱藏在國安、外交、國防、科技與財經等部門，以及網資通電作戰部隊和非官方民間公司組織中，並透過電腦網路的連結，可以在世界上各個角落，進行「灰色地帶」作戰而不易被察覺。這種「巧戰而屈人之兵」作戰型態，已經對美中關鍵科技與重要基礎設施、軍事電腦網路通訊與電磁頻譜，以及政府人事、財經、金融、科研機構造成安全威脅，同時也為國際關係帶來新議題與挑戰。

「網電間諜戰」能量是建立「不對稱戰力優勢」重要環節，內涵包括「制科技權」、「制資訊權」、「制電磁權」、「制密碼權」與「制標準權」等，並以「國際封鎖」、「間諜謀略」、「衛星對抗」、「資訊對抗」、「通信對抗」、「電子對抗」，以及「網路對抗」為主要作戰形式。當前，美中角力至少有 9 個關鍵戰略高地，包括高階半導體晶片設計與製造、作業系統、搜尋引擎、通信裝備基礎設施、海底光纖電纜、雲端運算、治理論壇、密碼體系，以及網際網路新協定等。

電腦網路本身就是一種武器與戰場，前線已無所不在，奪取戰場控制權將不只是導彈、飛彈和士兵，還包括高科技能量、電腦網路、數位通訊、電磁頻譜，以及標準規則話語權。同時，美中在國家安全戰略架構中，將「網電間諜戰」視為關鍵作戰領域，並成為戰略競爭決勝點之一。2020 年 10 月下旬，中共 19 屆 5 中全會通過《十四五規劃》，特別強調科技自主，準備在「關鍵核心技術取得重大突破」，就是體認到中國支撐「網電間諜戰」等科技，多數採用美國研發技術與

軟硬體設備，一旦關係生變爆發科技戰時，中國科技能量將受制於人，因此必須落實關鍵技術自主創新，以鞏固「網電間諜戰」能量基礎。

2020 年 10 月間，美國國家安全局與網路作戰指揮部發出警告，中國政府的駭客正對美國國防電腦網路體系，發動「網電間諜戰」威脅行為，呼籲相關單位提高警覺，並要求北京當局應有所收斂。同時，華府智庫「大西洋理事會」研究報告指出，中國的「戰略支援部隊」將發動「網軍」攻勢，意圖掌握「國際話語權」，散播貶抑民主價值訊息，干擾美國總統大選。此前，美國防部於 9 月 1 日發布《2020 年中國軍力報告》，特別關切中國太空衛星、網路與人工智慧，以及資通電等聯合作戰能量，並認為共軍「戰略支援部隊」的「網電間諜戰」能量，將攸關主控戰場管理的成敗，影響美中在西太平洋軍力消長，並衝擊台海和平穩定與台灣安全環境。

近年來，美國府會共同認為中國網路間諜，大量竊取美國大企業數據與研發成果，讓美國企業總計損失超過 6000 億美元。不過，美國國安局也曾駭入中國通訊設備商華為總裁任正非的電郵，以調查華為公司與共軍關係，還曾竊聽胡錦濤電話。「中國國家互聯網信息辦公室」更指出，「史諾登事件」揭露美國才是世界上最大網路竊密者，也是攻擊中國網路的頭號威脅。此外，中國國務院機構曾經發表「美國全球監聽行動記錄」，認為美國長期監聽中國等多個國家，危害全球網路與通訊安全，並要求美國就監聽行動提出解釋。

2020 年 10 月，美國國防部發布《電磁頻譜優勢戰略》，結合美軍參聯會於 5 月發布的《聯合電磁頻譜作戰》條令，成為美軍發展「網電間諜戰」能量的指導綱領。此前，美國國防部曾經於 2011 年發佈「網路作戰戰略」、2013 年發佈《電磁頻譜戰略》、2017 年發佈《電子戰戰略》，以及 2018 年版《國防戰略》等，除明確要求五角大廈將網路與電磁頻譜視同作戰領域，並對來自其他國家的網路駭客攻擊與電磁頻譜干擾，認定為已構成戰爭行為，決定比照陸、海、空三軍，從被動防禦轉為主動攻擊，以因應日益升高的網路與電磁頻譜安全威脅，同時計劃與民間企業及美國盟邦，共同合作發展網路與電磁頻譜作戰能量。

美國戰略圈認為，中國的「戰略支援部隊」正在想方設法，癱瘓或者嚴重破壞美國的基礎設施，例如電力網、金融交易網、供水系統，以及飛航管制系統等，需要透過網路進入的設施，而這些基礎設施正是美國經濟的中樞，突顯「網電間諜戰」也是一場進行中的經濟戰。美國前國安顧問瓊斯於

2020 年 10 月 19 日，亦在「大西洋理事會」強調，中國的網路破壞行為給美國傷害最深的，就是經濟領域的網路間諜活動，而這些間諜活動包括，竊取國家機密、竊取私人企業商業機密、盜取知識產權和工業技術機密，以及竊取談判策略等。

整體而言，面對美中「網電間諜戰」交鋒新形勢，未來的戰略競逐中電腦網路與電磁頻譜，本身就是一種武器與戰場，前線無所不在，奪取戰場控制權將不只是導彈、飛彈和士兵，還包括電腦網路、數位通訊與電磁頻譜。美中戰略互疑情勢若繼續惡化，台灣採取「友美和中」平衡策略，恐將會面臨被迫選邊壓力與困局。印太地區受制於美中關係格局，也將隨著兩國交鋒強度變化起伏。當前，美中仍積極發展「網電間諜戰」能量，並持續相互較勁，意味一場看不到煙硝的「超限戰」角力，正方興未艾。

二、美中「網電間諜戰」短兵相接

2015 年間，美中曾經同意設立一個「網路安全工作小組」，希望能夠透過國際間網路安全合作，讓網路空間順暢便利互惠，並避免雙方誤解與誤判，破壞網路空間和平使用。當時的拜登副總統就強調，網電安全對每一個人都有影響，對航空飛機，鐵路運輸，甚至是水壩的水流，電力輸送，金融行業，銀行保險每一筆交易也都有影響，因此，保護人民，保護其權利和基礎建設，對每一個國家都有利益。

2020 年間，全球有五百億筆資料在網電空間流傳，並透過網電空間交換、彙整與獲取。各種重要資訊在彈指之間，即迅速傳遞於網電空間，大幅增加滲透破壞，以及蒐情機會，不但容易肇生資訊安全危機，也將損及國家安全與利益。尤其在雲端運算、社群網站、大數據與人工智慧、互動網站等蓬勃發展下，資訊與電磁頻譜安全問題，對國防安全、金融、基礎建設等方面造成的威脅，將更為明顯。同時，許多主權國家的資訊與網電安全，更將受制於位在其他國家的網路、通訊與電磁頻譜設施，甚至被跨國企業網電資訊公司所掌握，因此也形成國際關係的新挑戰。

世界主要國家為防範重要基礎建設資訊系統，遭遇敵國破壞與入侵，無不制定「網路安全戰略」，採取「攻守一體」的策略措施。美國總統川普就曾經在 2018 年發佈《美國網路安全戰略》，將網路空間與電磁頻譜能力列為最優先發展、重

點保障的六大軍力之一。2020 年 10 月，美國防部為發展聯合全域作戰數據優勢，發布《國防部資料戰略》（DoD Data Strategy），提出 8 項指導原則，建構 4 個基本能力，達成 7 大數據目標，運用網路聯結打造國防部成為「以數據為中心的機構」，發揮聯戰優勢與效率。美國陸戰隊作戰發展司令部更強調，網路作戰與防衛能力越來越重要，美軍必須持續投資開發，因為現今的所有戰力都離不開網路，不論是戰場情偵、目標鎖定，或是聯合作戰都需要運用網路。

中國自 1985 年就開始發展網路與電磁頻譜能量，近年則積極實施「寬帶中國」戰略，到 2020 年已基本覆蓋所有農村；同時，中國透過互聯網架設國際交流橋樑，並推進「數位中國建設」，展開「互聯網+行動計劃」，運用網路發展創新事業；此外，中國與世界各國合作遏制資訊技術濫用，反對網路攻擊與軍備競賽，並堅持多邊參與原則，共同制定國際網路治理規則。

當前，中國發展「網電間諜戰」能量，主要項目包括：透過電腦網路攻擊，來完成長距離的攻擊破壞任務，運用電腦網路攻擊癱瘓對手國重要經濟活動能量，達到警告嚇阻的效果，運用電腦網路瓦解對手國 C4ISR 系統，運用電腦網路攻擊發揮「先發制人」威懾效果，結合電腦網路和電子戰特種部隊奇襲能量，達到心理威懾目標，並迫使對手國接受政治談判條件，運用電腦網路攻擊破壞後勤補給系統，以及運用電腦網路攻擊癱瘓對手國金融、電力運輸與通訊系統等。

美中兩國積極發展「網電間諜戰」能量，不強調大規模殺傷而重視體系癱瘓；交戰方式由接觸轉向非接觸作戰；行動模式從線性向非線性轉變；兵力組成由規模組合轉為效能融合；作戰指揮從預先計劃變成同步指揮。這種作戰方式，基本上是貫徹「巧戰而屈人之兵」用兵思想，以「不對稱戰力」創造有利態勢，減少附帶傷亡數量，並迫使對手國快速進入政治談判階段，接受其所提出的政治條件。

近年來，美中相互指控對方發動「網電間諜戰」攻擊，已讓兩國陷入「修昔底德陷阱」風險升高。2021 年 1 月拜登新政府上台後，是否會重新恢復「美中網路安全工作小組」運作，讓兩國的「網電間諜戰」降溫，仍有待觀察。

三、「網電間諜戰」角力場域

美中兩國在國家安全戰略架構中，已經將「網電間諜戰」視為新戰場，意味爭奪網路空間與電磁頻譜「控制權」勢在必行。2015 年間，中共中央成立「網路

安全和信息化領導小組」，由習近平領軍，顯示中共高層已將網路安全及發展，提升為國家安全戰略一環。習近平特別強調，「沒有網路安全，就沒有國家安全；沒有信息化，就沒有現代化」。美國總統川普亦於 2018 年發布的《美國網路安全戰略》，亦將網電作戰能力列為最優先發展軍力。

「網電間諜戰」至少有 9 個關鍵戰略高地，包括高階半導體晶片設計與製造、作業系統、搜尋引擎、通信裝備基礎設施、海底光纖電纜、雲端運算、治理論壇、密碼體系，以及網際網路協定第六版（Internet Protocol Version 6, IPv6）等。現階段，全球高階半導體晶片設計、製造技術，以及生產設備與關鍵原材料，主要還是掌控在美國政府與美資跨國企業手中，美國政府可以運用「出口許可管制」，以及司法「長臂管轄權」，對中國祭出「雙斷」措施，延阻或癱瘓中國發展「網電間諜戰」能量，並讓中國面臨高科技被「卡脖子」難題。

其次，美國的微軟 Windows 作業系統全球市佔率高達 80%以上，而 Linux 作業系統只有 1%；另在行動作業系統領域，美國公司「谷歌安卓」（Google Android）佔全球市場 40%以上。從國家安全角度，即使美國政府無法直接控制世界上大多數桌上型電腦，以及行動裝置的動力驅動軟體，但網路作業系統的軟體優勢，仍掌握在美國公司手中。

搜尋引擎是「網電間諜戰」的第 3 個戰略高地。雖然作業系統決定了電腦系統的技術特性，但搜尋引擎卻能對觀念造成巨大影響。美國公司谷歌在搜尋引擎的全球市場佔有率達 80％以上，其藉由優異的性能來吸引使用者，並自然形成議題設定與偏好形塑的力量。美中兩國在搜尋引擎戰略高地的爭奪戰早已開打。北京當局於 2010 年把谷歌逼出大陸，隨後，中國經營的搜尋引擎「百度」（Baidu），實際上成為中國大陸 9 億網民的唯一選擇。

「網電間諜戰」第 4 個戰略高地是通訊裝備基礎設施，美國在此領域具有主導地位，幾乎所有網際網路的資訊流量，都通過美國公司的通信裝備基礎設施。前中情局長哈斯斐表示，「由於全球電傳通信的特性，我們在這個領域擁有極大的主場優勢，而且有必要善用此優勢」。不過，近年來中國方面積極創建通信裝備骨幹，並運用華為公司拓展中東歐與南歐、東南亞、中東及非洲的市場，以降低其資訊流量通過美國基礎設施的需求。近年，華為意圖運用成本優勢發展全球 5G 網通設備，主導新一代行動通訊與物聯網，已經遭遇到美國全球性封殺行動。

第 5 個「網電間諜戰」高地是海底光纖電纜。現今 406 條海底光纖電纜承載全球 95%訊息數據流量，構成國際互聯網主幹，其間中資「華為海洋」鋪設了 105 條光纖電纜，是全球第 4 大海底光纖電纜業者。由於海底光纖電纜的鋪設與維護建設，涉及深海作業光纖傳輸等尖端技術，同時業者亦擁有切斷、干擾，或監控海纜通訊的能量與優勢，讓美國推動全球「乾淨網路」計畫面臨考驗，也讓中國在此戰略高地取得可觀籌碼。

第 6 個「網電間諜戰」高地是雲端運算。通信裝備基礎設施主要在保持對全球通信路徑的影響力，而雲端運算則是擁有網路上，集中處理及儲存資訊趨勢的影響力。隨著雲端運算服務市場的成長，越來越多資料將會流經美中兩國所擁有的基礎設施，使其成為網路空間戰略競逐焦點，並直接衝擊國家安全結構與內容。

第 7 個戰略高地是治理論壇。全球網路空間治理論壇由許多利害關係人組成集團，共同決定網際網路空間的通信標準，例如「電機電子工程師學會」（IEEE）、「國際電信聯盟」（ITU）、「全球資訊網聯盟」（WWWC）等組織，在形塑網路領域特性上，均扮演不可或缺的角色。目前，美中兩國均積極參與網路治理機構制定方針與標準，並競爭主導優勢地位，為發展「網電間諜戰」能量鋪路。

第 8 個「網電間諜戰」角力高地是密碼體系。密碼體系的數學基礎提供網際空間安全根基。如果保護資料安全的方法出問題，則網際網路的整個經濟引擎可能一夕崩壞。美國政府在密碼體系領域扮演重要角色，但密碼體系也代表「網電間諜戰」中的軟實力要素，因為政府無法對其本身以外的網路發號施令，然而，國家標準技術協會所制定開放、具競爭性的標準程序，有助於吸引重視安全的民營公司並壯大美國主導的密碼體系。

「網電間諜戰」的第 9 個戰略高地，是與「網際網路基本路由協定」（the fundamental routing protocol of the internet）有關的網際網路新協定。目前北京當局已決定在新一代網際網路架構中，採用新標準的大型計劃；同時中國有超過 9 億網際網路使用者，且其經濟仍在成長中，故有潛力對網際網路新協定、其硬體設備執行面與治理論壇發揮極大影響力。美國政府也正採取積極作為，協助美國企業克服採用新版協定的財務障礙，並避免喪失其對網際網路重要領域優勢地位，讓「網電間諜戰」能量受限。

網路競合是國際關係的重大課題，其中包括美中兩強的競合本質，同時也將

影響兩國戰略競逐動向。目前，美中仍依照各自的國家安全戰略，積極設立專責的網路戰機構，並規劃在 9 大「網電間諜戰」角力高地，強化本國的核心競爭力與綜合實力。2020 年 10 月下旬，中共 19 屆 5 中全會通過《十四五規劃》，特別強調「科技自主」，必須在「關鍵核心技術取得重大突破」，就是體認到中國目前所使用的高科技，多數採用美國政府與企業研發的技術。當美中科技戰爆發時，中國明顯受制於人並被「卡脖子」。因此，中國必須加速落實關鍵技術自主創新，做為鞏固「網電間諜戰」能量基礎，才可能在美中大國競爭格局爭取優勢。

四、「網電間諜戰」安全措施

2018 年的《美國國防戰略》特別提出「前沿防禦」概念，要求網路作戰指揮部在對手到達美國前，盡可能在美國以外的網路中接近對手，並展開行動將威脅化解與排除。2020 年美國總統大選期間，美國特別部署「情況監視+信息共享+直接行動」的網電安全機制，防範中國、俄羅斯與伊朗等國，發動「網電間諜戰」干擾破壞選舉，甚至對選舉結果造成不當影響。同時，美國正積極立法限制政府採購中國網通產品。2020 年 7 月，美國與澳洲兩國防長還在華府發表聯合聲明，強調美澳將增加網電領域納入共同防禦的項目與內容，無論是美國或澳洲單方面受到網電攻擊，兩國將同步採取防禦行動，以應對中國發展「網電間諜戰」新威脅。

美國戰略情報圈主流意見認為，網電攻擊和網路間諜活動，已經取代恐怖主義成為美國的頭號安全威脅。目前，美國採取的具體反制行動包括，成立 40 支網電作戰部隊，其中有 13 支專責網電攻擊任務，以發揮網電先制攻擊的效果。美國家安全局長兼網路作戰指揮部司令中曾根表示，網路攻擊已被列為全球首要安全威脅，美國將推動訊息安全分享機制，強化基礎網路設施維護，以及減少經貿科技機密遭竊等相關應對措施。

另，美國防部要求「先進研究計劃署」（DARPA），發展網路安全 X 計劃（Plan X），保障敏感電腦網路不受攻擊，並加強研究網路攻擊能力，以處理「特定軍事需求」。今後，美國與其他國家發生軍事衝突時，第一波攻擊者將不再由戰斧巡弋飛彈或隱形轟炸機擔綱，而是由坐在美國本土的「網軍」，以各種程式、網路病毒或蠕蟲發動攻擊，癱瘓對手的公開網路，甚至以駭客方式，攻入對手的保密網路，破壞對手指管通情監偵系統，或者從內部摧毀發電廠和通訊等重要基礎設施。

中國執行「網電間諜戰」任務的主要機構包括：（一）戰略支援部隊負責電腦網路運作、電子反制能量、組建國防信息化保障任務，以及執行戰場網路情報蒐集等；（二）在 5 大戰區設置戰區聯合作戰指揮部，並成立信息對抗中心，負責電子對抗及網路信息體系的防護；（三）大陸軍事科學院及國防大學則是負責研發各種「網電間諜戰」的作戰指導與準則，並積極培育訓練各項執行任務的軍官和士兵。此外，大陸可以運用「網電間諜戰」工具包括：駭客、電腦程式病毒、硬體設備破壞、內部滲透破壞攻擊，以及電磁脈衝攻擊等。至於執行任務的平台則包括：電腦、全球網路連線，以及有能力的操作人員。對於大陸軍事科學院及國防大學而言，其當前最重要的任務之一，就是要訓練出能夠成功執行任務的「網電間諜戰」軍官與士兵。

為防範國家重要基礎建設資訊系統遭敵破壞與入侵，世界各國無不制定「網路安全國家戰略」，其目的即為預防遭受網路攻擊，同時為了在「網電間諜戰」中成為贏家，多數國家正積極強化網電作戰能量。目前，美國為防範重要基礎建設資訊系統，遭遇敵國破壞與入侵，已經制定「網路安全戰略」，採取「攻守一體」的策略措施。

美國總統歐巴馬與川普曾經先後頒佈「制裁網路駭客」行政命令，授權政府機構對威脅美國外交政策、國家安全，或經濟穩定的境外駭客，包括國家、組織，或個人，實施制裁，凍結其資產、禁止進行金融交易、禁止入境，也不能與美國公民及公司進行商業往來。歐巴馬與川普都表示，網路攻擊威脅是美國經濟與國家安全最嚴重挑戰，美國政府將透過外交、貿易和執法等各種手段，打擊針對美國的惡意網攻行為。

前國安局長李翔宙表示，「未來戰爭型態是坐在家裡打」，而且網路威脅來自四面八方。美中情局就在 2015 年 3 月成立「數位創新處」，應對瞬息萬變的網路攻擊威脅。俄羅斯發動對烏克蘭軍事行動，並成功併吞克里米亞，就曾經先期部署「靈蛇」間諜軟體，蟄伏在烏國重要系統中，採取「零時差」網路戰，並在烏克蘭國防部內下達相互矛盾命令，讓前線指揮官不知所措。

美國國安局曾對伊朗濃縮鈾工廠發動網路攻擊，延緩該國核武計劃。網路駭客鎖定跨國公司防毒軟體供應商，利用上傳應徵履歷機會，將擁有「零時差」攻擊能力含毒軟體，潛入該公司電腦系統，當跨國公司採用該公司防毒軟體時，等

於讓放毒的網路駭客取得「零時差」攻擊或竊密金鑰匙。另俄羅斯防毒軟體商卡巴斯基指出，美國已研發出在硬碟內暗藏監控軟體，使美國安局能監偵全球半數以上電腦。

美中兩國曾經為加強網路安全合作，避免網路攻擊造成無可彌補傷害，2015年9月習近平赴美國是訪問時，將網路安全列為重要議題；兩國執法部門也都成立「網路安全工作小組」，共同研究應對網路恐怖攻擊；此外，各國間也正積極運用多邊機制，制定網路安全行為準則，規範國際網路行為。不過，美中自2018年貿易戰開打後，兩國戰略競爭領域不斷擴大，並進入短兵相接的「網電間諜戰」，讓先前的合作關係停擺。同時，網路黑暗面中的國家利益競逐、恐怖組織為達目的不擇手段擊行為，以及商業競爭網路間諜活動等，亦越演越烈，而且威脅與破壞程度既深又廣。

五、結語

「網電間諜戰」是整體綜合國力的展現，包涵國家戰略與軍事科技能量；同時也是一把「雙刃劍」，一旦運用網電部隊進攻別國的網路與電磁頻譜，導致網路與電訊癱瘓，而本國的網路與資通電能量作用也將急劇下降，因為國際間的網路與電磁頻譜安全必須靠合作，才能提升網路與資通電的便利性與使用價值。

不過，美中近年互視彼此為競爭對手與威脅，並相互發動「網電間諜戰」，已經讓雙方都造成嚴重損失。美國總統拜登表示，美國網電領域的安全威脅正在增加，並要求北京當局在網電領域遵守國際準則。習近平相對也提出建議，希望雙方能夠制定限制「網電間諜戰」的「接戰準則」（codes of engagement），並進一步探討維護網電安全國家責任內容。

在資訊科技設備精進的時代，「資訊戰」、「網路戰」與「電子戰」已為各國重視，重要資訊在彈指之間，即迅速傳遞於網路空間與電磁頻譜，大幅增加滲透破壞，以及蒐情機會，不但容易肇生資訊安全危機，也將損及國家安全與利益。目前，雲端運算、社群網站、互動網站蓬勃發展，網電安全問題對國家安全、金融、基礎建設等方面造成的威脅，將更為明顯。為防範國家重要基礎建設資訊系統遭敵破壞與入侵，世界各國無不制定「網路安全戰略」，其目的即為預防遭受網路攻擊，同時為了在「網電間諜戰」中成為贏家，多數國家都傾向強化網電作戰能量。

台灣與美國在網電安全領域有密切合作關係。當美中在網電空間交鋒加劇情勢下，台灣除了因應市場結構轉變新挑戰，也將面臨網電產業發展與網電安全新威脅。因此，台灣宜從國家安全與產業發展層面，規劃務實策略應對。首先，政府應先發佈「國家網電安全戰略」，明確台灣發展網電安全戰略目標，以及指導維護安全策略原則；其次，政府應主導結合半導體與資通電科技產業，積極在「網電間諜戰」關鍵戰略高地，發展台灣的能量與角色；最後，政府應加強國人的網電安全意識，防範國家重要基礎設施、關鍵資訊與電磁頻譜，受到敵國「網電間諜戰」威脅，以維護國家安全。

(本專欄文章作者意見不代表論壇立場)