熱點聚焦

網路衝突及升級動能對現實環境與兩岸關係之衝擊

The Dynamics of Cyber Conflict, Escalation beyond the Cyber Realm and the Impact of Cross-Strait Relations

Tobias Burgers

Otto-Suhr-Institut, Free University of Berlin

過去 30 年間，數位科技在全球範圍內大規模普及。電腦與行動通訊設備的廣泛應用，以及網際網路中的各種智能服務已然無所不在。今日的人們幾乎已無法想像往昔沒有智慧型手機的時代。回顧歷史，在這波數位科技浪潮發展的前期，人們對於網路技術的重要性認識有限，對於新型數位科技在現實生活中的整合運用也所知不多。但情況在過去 20 年間有了很大的變化，資訊革命深刻影響了人類文明的各種層面，包含日常生活、溝通方式或對於安全問題的認知等，無論是個人或國家都需要努力適應。

對個別用戶來說，網路空間中的各種安全威脅如網路釣魚、駭客攻擊、惡意程式散播等已是十分常見的現象；對於國家與國際社會來說，出現於網路空間的新型安全威脅，或者結合運用網路技術的傳統威脅亦日益迫切，譬如大規模駭客攻擊、分散式阻斷服務攻擊（DDoS）、網路間諜，及利用網路技術對實體目標造成物理性傷害

等，都是當前國際間常出現的安全挑戰。

換言之，數位革命與其衍生的新型威脅態樣正漸進改變國際安全的性質。特別是網路空間已成為一個衝突頻仍的灰色領域，位處其中的國家與非國家行為體，基於獲取情報、利益或削弱對手等動機不斷相互摩擦乃至攻擊。談到網路安全時，我們必須瞭解此處的核心問題之一是威脅的不易確認性。在現實物理環境中的安全威脅通常是可以清楚辨認定性的，但在網路空間中很難做到這一點，主要原因是網路威脅的可見度薄弱，有時很難辨認網路惡意活動是否正在發生、危害程度強弱及行為者的真實意圖為何。進一步講，多數國家也尚未建立一套清晰的網路威脅評估標準：所謂的網路威脅究竟是指駭客入侵電腦系統？製作散播惡意軟體？還是破壞數據資料或特定目標？總之，在網路領域中確認威脅程度與威脅意圖是很困難的。

威脅與威脅感知在國際關係的傳統安全研究中扮演著舉足輕重的角色，也是主政者制訂安全政策的重要依據。一般來說，威脅感知的成立兼受客觀威脅狀態及主觀行為者認知的影響。相關問題在鮑德溫（David A. Baldwin,）等學者的研究中多有說明。但是，如上文所述，與傳統安全事務相比，在網路空間中感知威脅相對困難許多，部分是因為許多行為者對於這一新穎科技領域認識不足，部分則是受到客觀技術能力侷限。此外，許多在國際安全領域曾被普遍運用的傳統理論模型如威脅平衡和權力平衡等，在網路安全問題上也未必全然適用，這就導致研究者在探討如何處理相關網路威脅事態時不可避免地將遭遇許多困難。

讓情況更加複雜的另一項因素是網路空間中目前仍欠缺受到普遍承認的法規與行為準則。由於缺乏規範的引導，行為者無法辨識

自身或他者的行為是否逾越了紅線。這條紅線的模糊多變，也導致國家在規劃網路防務政策時不易確認行動的合理限度何在。

例如，使用物理性軍事手段回應網路攻擊曾在過往的討論中被各方認定極為不宜，但這一論調近期卻在美國的新版網路戰略中被公然提出；以色列政府也持類似論調，主張以傳統軍事攻擊報復哈馬斯（Hamas）等敵人的惡意網路活動。平心而論，這類作法固然可能產生更強烈的嚇阻效果，卻也不禁使人質疑威脅與反制手段之間的似有比例失衡之嫌。更甚者，許多行為者似乎有意挑戰國際社會對於網路威脅的容忍上限。近年的許多事例顯示網路威脅與衝突型態正在升高。早期的網路攻擊旨在獲取情報與數據資料，近期的許多網路攻擊卻以在現實環境中創造物理破壞效果為目標，例如震網病毒（Stuxnet）事件，和俄羅斯對烏克蘭電網及沙烏地阿拉伯化工廠電腦系統的攻擊等，都說明以數位手段破壞實體設施的作法不但可行，而且正越來越常見。

這些事例說明了網路領域中的「紅線」是多麼脆弱、規範準則有多麼模糊多變，而網路衝突的升級風險也將隨之加劇：由於不易確認網路攻擊或惡意活動發起者的真實意圖與全面危害程度，兼且考慮網路領域中的攻防成本差異巨大，國家在面臨重大網路威脅時，往往傾向從寬認定威脅嚴重性，設想最壞情況並以主動防禦（Active Defense）名義強勢反擊。

因此，我們可以說今日的網路空間是一個缺乏規範約束且威脅性亦被高估的高風險環境，發生在其中的衝突更可能外溢至網路以外的現實世界之中。為了理解網路衝突如何產生外溢升級效應，著名的核戰略學者凱恩（Herman Kahn）提出的戰爭升級理論或有重新詮釋的價值。該理論的升級階梯共有 37 個層次，從位於階梯頂端的

熱核大戰到位處階梯底部的輕微安全事件。在網路安全議題中應用這一理論模型有可能讓研究者更能瞭解網路衝突升級流程，及其如何導致國家間的關係惡化和傳統衝突事件發生。

網路衝突外溢至現實世界的情況很可能出現在未來的兩岸關係發展進程中。

例如，中國在處理兩岸事務或南海爭端等安全問題時，可能會透過網路途徑以切香腸策略（Strategy of Salami Slicing）的方式逐步加強對台灣施壓。鑑於台海兩岸的政治與安全互動過去幾年間已明顯惡化，如果台灣的民主進步黨在 2020 年 1 月大選後繼續執政，北京當局很可能擴大對台威嚇施壓。除了以軍機軍艦繞台的傳統作法外，網路攻擊也是其可能採用的手段。因此，台灣政府必須審慎思考如何應對來自對岸的網路威脅，包括有哪些防禦手段、有哪些可用於嚇阻的工具，以及如何操作才能在兩岸間成功建構一種能有效管控威脅的平衡互動框架。

（翻譯：張凱銘）