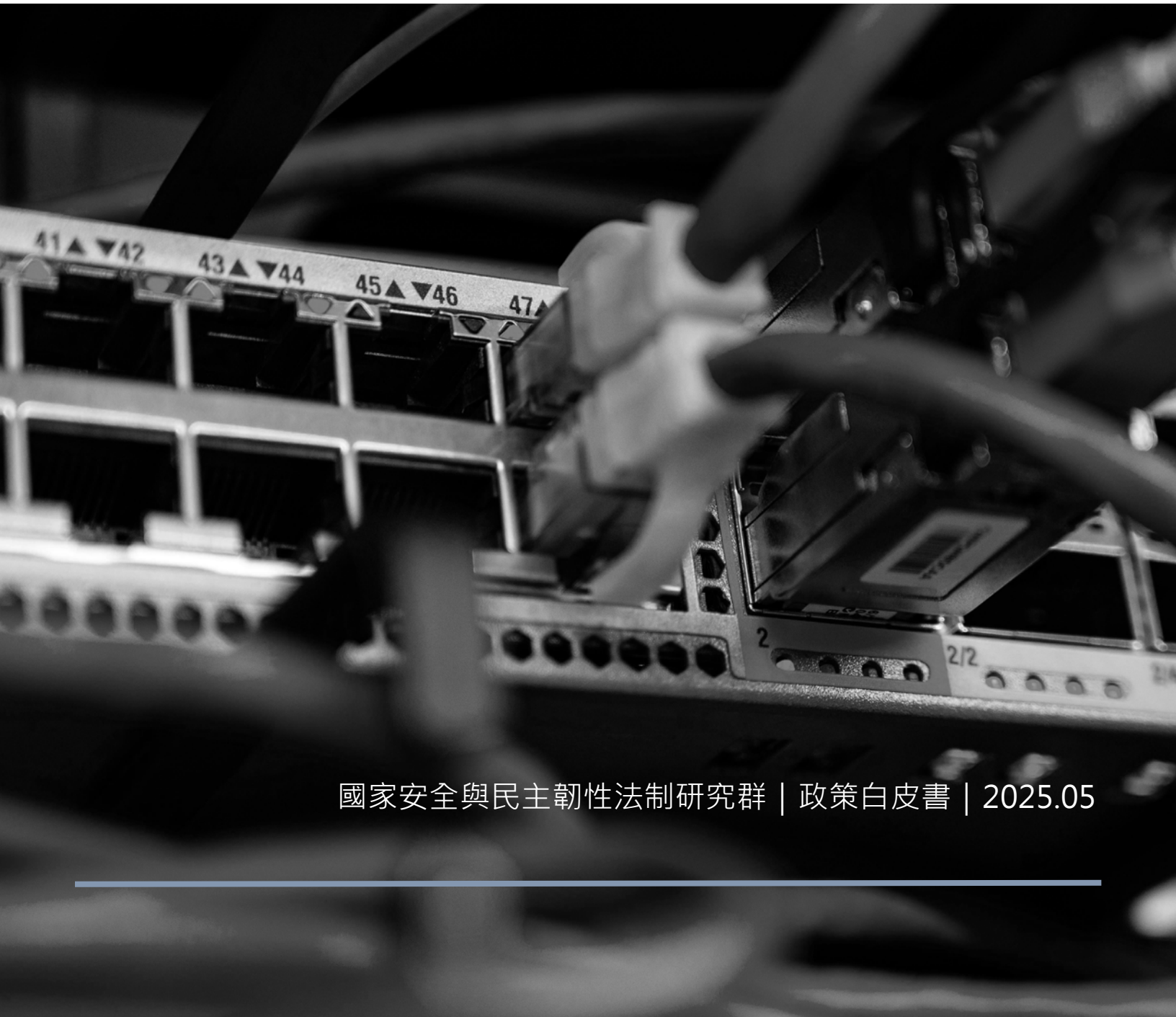
建構網路攻擊於戰爭法的適用與其交戰規則之制定

黃居正 教授

國立清華大學科技法律研究所



國家安全與民主韌性法制研究群｜政策白皮書｜2025.05

摘要

本篇探討網路攻擊在當代戰爭中的角色與其於戰爭法下的適用性，並主張需制定相關的交戰規則。文中指出，網路攻擊已成為威脅國家安全的重要手段，其性質跨越國界、具高隱蔽性與雙重用途，與傳統武力形式大不相同。然而，現行國際法與聯合國憲章主要針對傳統物理戰爭設計，對網路戰的規範存在明顯不足。

文中分析了「網路交戰人員」與私人網路安全公司的角色，指出這些人員在缺乏明確指揮關係下，可能造成國家責任的逃避。進一步闡述，儘管網路戰可能未造成直接物理破壞，其對國家安全與基礎設施之影響，足以構成實質的交戰理由。

因此，筆者建議應將戰爭法中的四項核心原則——比例、必要、區別與人道——延伸適用至網路戰。並透過科學矩陣檢視不同網路攻擊特徵對原則適用性的影響，以制定具體可行的網路交戰規則，確保新型戰爭形態亦能受到國際人道法的規範與約束。

國安風險辨識與風險分析

1. 網路攻擊與網路戰

「網路攻擊（cyber attack）」是指「涉及國家安全利益並牽涉國際關係之網路攻擊行為」。「網路間諜」行為，則視其入侵程度、目的及標的，是意圖探知與國防、國安相關之國家防禦能力與戰略布局等，或僅只是於本國經濟秩序的違反，例如未經授權查看或複製商業機密。個案是否構成網路攻擊，而得據以採取拒止甚至回擊等措施，須就其事實判斷。

前白宮網路安全顧問 Richard Clarke 曾將「網路戰（cyber war）」定義為：「一國為造成損害或破壞，侵入另一國電腦網路系統的行為」，將「網路戰」等同傳統戰爭中的「侵略」行為。其侵略方式是敵方透過網路系統，以我方電腦網路系統或關鍵基礎設施為攻擊目標，加以破壞或致生損害，獲致瓦解我方抵禦能力之目的。

聯合國憲章第 2 條第 4 款規定的武力不行使原則，係著眼過去歷史列強間的大規模戰爭（full-scale），其並未預想規範如網路戰此種「微型戰爭」，故在「武力使用」、「武器」與「動武」之定義，可能因此型態而受有限制。此外，由「非國家行動者」參與之資訊戰、網路戰是否為憲章限制武力使用的規範對象亦不無疑問。

2. 網路交戰人員與私人網路安全公司

「網路交戰人員（cyber-combatants）」，是指在非常規的網路戰中，由攻擊方實施網路攻擊獲致如常規戰爭般的破壞力戰果與附隨損害的交戰人員。相較在人類戰爭史慣常作為補充人力、與普通士兵相似的「僱傭軍」，網路交戰人員與從事網路服務的私人網路安全公司（Private Cybersecurity Firms, PCSFs），更趨近現代區域性衝突中為避免適用戰爭法，以契約締結等方式參與特定國家軍事行動之人員組成的「私人軍事公司（Private Military Companies, PMCs）」。

不論是受國家僱用參與特定的武裝行動的 PMCs，或為國家從事網路攻擊防禦行為的 PCSFs，皆對其僱員之監督管理保有相當獨立性，導致國家於 PMCs、PCSFs 直接指揮監督淡化（甚者僅受約款拘束，不存在指揮監督關係）。此結果導致當 PMCs、PCSFs 行為違反國際強行法（如侵犯人權）時，國家可能因此脫免其責任，為現行國際法的灰色地帶。

3. 適用戰爭法規範網路攻擊行為之可能

古典戰爭法的規範目的，是在限制國族國家過度擴張之主權行為。受戰爭法規範的戰爭目的須包含相當主權元素，例如：領土性（地域性）、主權動機，及國族國家之治理體系相關的武（暴）力行為。「領土性」要素，係為解決雙方領土爭端；「主權動機」是建立於國家對其領土與國內事務享有絕對主權原則，得排除外部勢力的侵擾，不受他國之干涉；「國族國家之治理體系相關的武（暴）力行為」，著眼於軍事武力之保有與主權絕對間的歷史關係，認為國家享有使用武力一絕對專屬的權能。

然網路攻擊不必然涉及領土完整性或管轄絕對性，其爭端原因也不絕對明確，其活動本質不具有屬地性。此外，網路行動的技術本質是跨越邊界的，難以確定其主權管轄之界限；網路基礎設施的營運與維護具有高度隱匿性與移動性，許多國家更須高度倚賴私人所提供之網路基礎設施營運，亦難以確認其所在主權領域。縱有客觀物理接觸（例如：海底光纖電纜），一國也未必享有絕對排他的管轄。

相較古典戰爭以實體軍事設施作為攻擊、脅迫之目標，網路戰可能是以交易秩序破壞作為目的，常以被攻擊國關鍵基礎設施為標的，連帶造成經濟上的脅迫（economic coercion）。縱使其造成的損害結果與常規戰爭損害相當，國際法院過去的裁判實務並不認為純粹經濟上的脅迫（如貿易制裁、禁運、拒絕融資、貸款等可能損其經濟力之行為）屬於武力行使。網路戰是否因此就不構成武力行使，致不能以之合法行使自衛權？

1999 年美國國防部（DoD）出版論文「對於資訊行動之國際法議題之評估（An Assessment of International Legal Issues in Information Operations）」指出，即使被攻擊的系統並非機密軍事後勤系統，也可能嚴重威脅國家安全。例如破壞管理軍事燃料、備品、運輸、部隊動員或醫療用品的電腦化系統數據。其認為，即使沒有造成物理傷害、破壞、網路攻擊事件亦可能構成重大的「交戰理由（casus belli）」。DoD 承認戰爭法如何適用於網路行動迄今未得出好的解答，但 2015 年 DoD 戰爭法手冊第 16 章「網路行動（Cyber Operations）」依舊載明戰爭法應適用於網路，並將隨網路能力發展及各國對應其發展反應決定其觀點。

4. 制定網路攻擊交戰規則之可能

戰爭法的四個核心原則：以戰略目的而非個別戰術行為判斷的「比例原則（proportionality）」；僅於軍事需求條件下，方允許破壞或扣押一般市民財產設施的「必要原則（necessity）」；區分交戰與非交戰人員、軍事目標與受保護的財產或場所的「區別原則（discrimination）」；禁止以殘酷手段，製造與軍事目標無關、不成比例的傷害或痛苦之「人道原則（humanity）」，其射程當然及於供交戰人員作為戰場指引的「交戰規則（Rules of Engagement, ROE）」，確保交戰人員不至於因戰場的慘烈狀態失去理智過度行使武力。

由於網路戰非常規武力行為，具高度技術特徵、相當大的變異性，為便利其與戰爭法原則間錯綜複雜之適用，學說將網路戰歸納出八項特徵，其包含：具物理性、可見破壞效果的「動力學（kinetics）」、表彰攻擊者身分之「可識別性（visibility）」、具脅迫性，相同行為致不同結果的「可變性（mutability）」、涉及身分與授權之「偽裝狀態（masquerade）」、網攻武器的「軍民通用性」或「雙重用途（dual-use）」、關於網路空間控制之「分區（partition）和篡奪性」、因人為設計本質缺陷，在行動中被動改變的「不確定性（instability）」與著重物理特性的「迫近性（intimacy）」。

因應策略的政策建議

A. 1.建構適用網路攻擊行為之戰爭法規範

使用網路作戰，只是軍事技術的演進形式，因為在基礎設施大比例倚賴自動化控制的今日，對其進行網路攻擊，仍可能造成範圍與規模幾與常規戰爭結果無異的物理、動能傷害，故不能使其脫免戰爭法規範。

B. 2.將戰爭法規範原則納入網路戰之交戰規則制定（參表一）

（1）動力學特徵：必要、區別、比例與人道原則皆可正常適用。

（2）可識別性：由於判斷武力行使之存在與否，是以敵方具有機密性之戰略或戰術為核心而具有隱密性，故四個原則不一定可被適用。

（3）可變性：人道及必要原則難以應用，但可規範適用比例與區分原則。例如以錯誤格式代碼干擾敵方通訊，考慮其向平民援助的必要設施運作（醫院、儲水設施、電力系統），其行為應受規制。

（4）偽裝狀態：必要與區別原則應被適用，須藉由區別原則避免網路攻擊行動擴散至非軍事用途目標（儘管判別因身分轉換性高而非常困難）。

（5）軍民通用：難以適用。

（6）分區和篡奪性：應適用區別、比例與必要原則，避免在控制的網路空間對平民、未捲入衝突的其他國家造成不當傷害。

（7）不確定性：適用區別、比例原則。

（8）迫近性：行為參與者須了解其伺服器或網路活動影響之物理位置所在，避免比例、必要與區別原則的違反。

表一、網路戰之交戰規則的科學矩陣

	必要原則	區別原則	比例原則	人道原則
動力學特徵	是	是	是	是
可識別性	否	否	否	否
可變性	否	是	否	否
偽裝狀態	是	是	否	否
軍民通用	否	否	否	可能
分區和篡奪性	是	是	是	否
不確定性	否	是	是	否
迫近性	是	是	是	否