《台灣戰略研究》第二卷第一期
2026 年 1 月　33 頁～ 58 頁

Taiwan Strategic Studies, Vol.2 No.1
January 2026, pp.33-58
DOI: 10.30249/tss.202601_2(1).0002

網路敵意行動之國際法評價與臺灣因應策略

林昕璇 *

摘　要

資通訊技術的迅即發展，帶動網路空間已成為國際政治、經濟與軍事互動的重要場域。各國間透過網路手段進行間諜活動、認知作戰、基礎設施攻擊等「網路敵意行為」（hostile cyber activities）日益頻繁，對國家安全與民主制度構成重大威脅。由於網路攻擊具備匿名性、超地緣性與模糊性，國際法對於此類行為的規範與評價尚處於發展階段，故而對行為歸責與法律界定帶來挑戰。臺灣作為高度依賴資訊基礎設施的民主社會，面臨來自國際網路敵意行為的多重威脅，亟需建立符合國際法與本土需求之因應策略。政府已推動《國家資通安全戰略 2025》，強調「資安即國安」理念，並建立國家資安戰情協同應變中心，以及強化國家資通安全會報，提升整體資安韌性。本文乃從當前國際法秩序的視野，檢視直接和間接規範網路攻擊之國際法體系的現狀與侷限，提出建立涵蓋政治、法律、外交與技術層次的分層回應機制，強化歸責標準、公私協作、數位外交與立法改革，提升臺灣資安韌性、應變能力、法制基礎與國際合作能量等若干制度整備之規範性建議。

關鍵詞：網路攻擊、網路戰、國際法規範、數位韌性、網路駭客主義

* 國立成功大學政治學系副教授，美國維吉尼亞大學法學博士（S.J.D.）。
收件：2025 年 6 月 13 日；一修：2025 年 7 月 29 日；通過：2025 年 8 月 4 日；接受：2025 年 12 月 15 日。

International Legal Implications for Hostile Activities in Cyberspace and Taiwan's Response Strategies

Hsin-Hsuan Lin**

Abstract

The rapid development of information and communication technologies has transformed cyberspace into a critical arena for international political, economic, and military interactions. Hostile cyber activities—such as espionage, cognitive warfare, and attacks on critical infrastructure—have become increasingly frequent among states, posing significant threats to national security and democratic institutions. The regulation and evaluation of such activities under international law remain in a developmental stage, primarily guided by principles of the United Nations Charter, including the prohibition of the use of force, state sovereignty, non-intervention, and countermeasures. However, the anonymity, transboundary nature, and ambiguity of cyberattacks pose challenges to attribution and legal classification. As a highly digitized democratic society, Taiwan faces multifaceted threats from hostile international cyber activities and urgently needs a response strategy that aligns with both international legal standards and domestic needs. The government has launched the "National Cybersecurity Strategy 2025," emphasizing the concept of "cybersecurity as national security," and established a joint cyber defense system and a situational awareness and emergency response center to enhance overall cyber resilience. From the perspective of the evolving international legal order, this paper proposes a multi-layered response mechanism encompassing political, legal, diplomatic, and technical dimensions. It offers normative recommendations for institutional preparedness in Taiwan, including strengthening attribution standards, fostering public-private collaboration, advancing digital diplomacy, and reforming legislation to enhance cybersecurity resilience, responsiveness, legal infrastructure, and international cooperation capacity.

Keywords: cyberattacks, cyber warfare, international legal norms, digital resilience, hacktivism

** Associate Professor, Department of Political Science, National Cheng Kung University; S.J.D., University of Virginia School of Law. Email: hl3bu@virginia.edu

壹、研究緣起

數位依賴（digital dependencies）所引發的國家安全挑戰，已在國家治理、企業營運與個人生活等層面日益顯著，且三者之交織互動也牽動國際戰略布局的敏感神經。析言之，資通訊技術肇致的風險具有高度系統性，伴隨著數位資料的集中化儲存固然有助於電子化基礎建設的整合匯流，於此同時，卻也將各國的資通基礎建設和國家基礎建設暴露於跨境網路敵意活動之風險之下，隨之伴生的資訊外洩規模日益猖獗、損失難以估計。美國人事管理局（U.S. Office of Personnel Management）之資安事件，導致逾 2,200 萬筆聯邦雇員個資遭駭，顯示國家級資安體系的結構性脆弱（Citron & Eichensehr, 2025, pp. 49-50）。2021 年 Colonial Pipeline 遭駭事件造成美國東岸主要輸油管線停擺數日，進而引發「恐慌性搶購」，適足彰顯關鍵基礎設施網路安全與能源安全之間的高度聯動性（Citron & Eichensehr, 2025, p. 50）。無獨有偶，網路敵意行為殃及之私部門亦有日益增加之勢，2017 年信用評等機構 Equifax 遭受的資料外洩事件，波及近 1.48 億名美國公民，進一步凸顯私部門在個資治理上的法遵與風險控管不足（Citron & Eichensehr, 2025, p. 50）。此外，對數位紀錄與網路系統的高度依賴，使企業面臨日益頻繁且具有高度毀滅性的勒索軟體攻擊。2017 年，WannaCry 病毒影響了全球至少 150 個國家的數十萬臺電腦，WannaCry 惡意軟體阻止微軟的 Windows 作業系統啟動，並加密受影響電腦上儲存的所有資料。前揭諸項憑恃網路之跨國性、難以追索性的侵害事件涉及網路攻擊具備匿名性與模糊性等特質，不僅對行為歸責與法律界定帶來挑戰，更攸關國家安全與公共利益之保障，催動各國政府莫不重行檢視與強化關鍵基礎設施的資安法制架構與應變機制（Sigholm, 2013）。

臺灣作為高度依賴資訊基礎設施的民主社會，面臨來自國際網路敵意行為的多重威脅，亟需建立符合國際法與本土需求之因應策略。本文旨在探討數位依賴日益加深下所引發的國家安全挑戰，首先就網路敵意行為與駭客行動主義分別涉及之模糊邊界與治理困境，提出網路敵意行為之概念混淆與適用侷限所涉跨境性與模糊性的法律挑戰。第三部分檢視現行國際法規範，涵蓋直接與間接針對網路攻擊之規範框架對於網路攻擊的適用性與侷限性，同時延伸至現行國際法中國家責任與盡職調

查（due diligence）適用於網路攻擊所肇致之適用難題與解釋取向。本文續而聚焦國家安全威脅與數位依賴日益加劇的國家地緣政治下，三種當前國際社群因應網路攻擊因應模式：「保持沉默不歸咎」、「歸咎但保留法律立場」、「歸咎並尋求多邊聯合認定」，進而探討不同模式背後隱藏之國際法秩序博弈與臺灣政策選擇的啟示。最後聚焦於臺灣現況，提出整合法制建構與國際合作之多層次應對策略，以建立具韌性的數位安全治理架構。

貳、網路敵意行為與駭客行動主義：模糊邊界與治理困境

一、網路敵意行為之概念混淆與適用侷限

根據史丹佛大學國際安全與合作中心高級研究專家 Herbert Lin 的定義，其將網路攻擊視為「使用刻意地行動和操作來改變、破壞、欺騙、降級或摧毀敵方電腦系統或網路或資訊」，並將其等同於攻擊性網路行動（Lin, 2010, p. 63）。惟誠如網路法專家 Oona Hathaway 精闢地指出當前各國在處理非國家網路活動時亟需回應三個核心問題：首先是缺乏對關鍵概念的明確定義，如「武力使用」和「武裝攻擊」。其主張儘管現代網路攻擊日益頻繁，並可能造成癱瘓電網、防空系統甚至損害核設施等嚴重損害結果，但在國際法下，占據絕大宗的此類攻擊仍未達「武裝攻擊」的標準，難以直接適用戰爭法。蓋戰爭法原為明確軍事衝突而設計，網路攻擊的手段和效果與傳統戰爭差異極大，致令「網路戰爭」一詞在規範行概念界定上爭議不斷（林昕璇，2023，頁 102-107；Hathaway et al., 2012, pp. 881-882）。

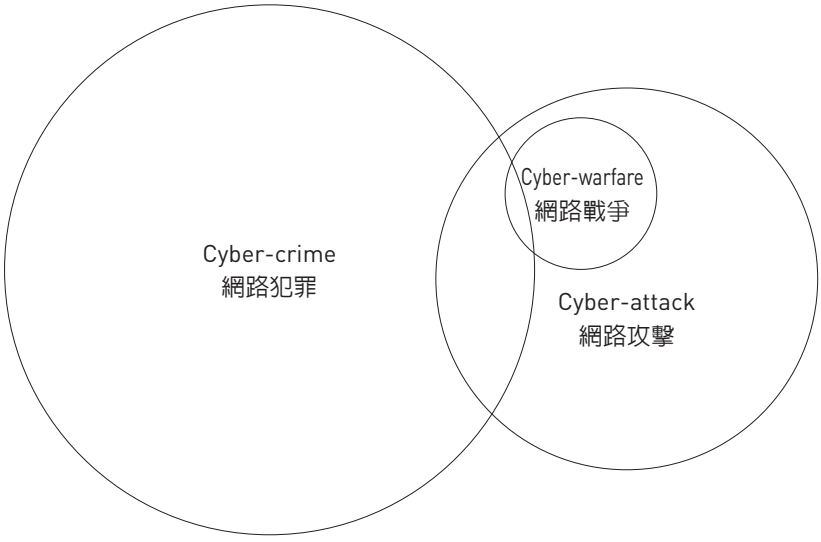
職此，區分網路攻擊的位階層級實有清楚釐清適用概念上的模糊性與混淆性的必要價值。進一步言，僅有構成「武裝攻擊」或發生於既有武裝衝突中的網路行動，方能納入戰爭法的適用範圍。其餘如間諜、滲透或政治破壞等，應由不干涉原則、國際刑法或國內法處理，而非一概視為戰爭行為。Oona Hathaway 等網路法專家更直言不諱地指出，當前必須擬定一部網路攻擊條約的首要任務，乃繫諸於建立一致性且可操作的定義，釐清「網路攻擊」（cyber-attack）、「網路犯罪」（cyber-crime）與「網路戰爭（cyber-warfare）」三者的界線。而前開三者定義不同之處，在於網

路攻擊僅指涉基於政治或國安目的蓄意削弱電腦網路功能的行為，網路犯罪則是非國家行為體或私部門組織違反刑法的電腦犯罪，而網路戰爭則需造成足以比擬武裝攻擊的人身或財產損害。這類定義不僅可作為各國立法基礎，也有助於建立跨國合作共識（Hathaway et al., 2012, p. 833），三者的關係可圖示如圖 1。

圖 1

網路犯罪、網路攻擊與網路戰的聯集關係圖

FIGURE 1: Relationship between cyber-actions



資料來源：作者重製自 "The law of cyber-attack," by O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, & J. Spiegel, 2012, *California Law Review*, 100(4), p. 833.

其次是歸因問題。Dennis Broeders、Els De Busser 和 Patryk Pawlak 指出，國際法並未提供具體規則說明何種證據足以歸因網路攻擊（Broeders et al., 2020, pp. 6-7）。特別是在國家與高級持續性威脅（advanced persistent threats, APTs）等代理組織之間建立證據聯繫更加困難，不啻彰顯國際法基本上忽略了此等模糊行為者作為國家力量延伸的現實（Katagiri, 2021, p. 3）。

不容忽視的是，現行國際法秩序未能充分維護網路空間和平的原因在於此等機制實無法有效規範非國家行為者（如個人駭客和科技公司）的行為。揆諸實際，

傳統國際法由政府官員制定，高度以國家為中心，與網路空間中非國家行為者占主導地位的現實不符。固然由北約合作網路防禦卓越中心邀集專家學者編纂的《適用於網路戰爭的塔林國際法手冊》（*Tallinn Manual on the International Law Applicable to Cyber Warfare, Tallinn Manual*, 以下簡稱塔林手冊）分別於 2013 年、2017 年輯錄出版成書，可謂國際法適用於網路空間討論的高峰，惟仍缺乏明確文獻和足夠的國際共識，凝聚據此確定各國真正接受這些規則作為管理網路行動的權威指南。

同時，國際法機構素來在懲罰非國家暴力行為方面普遍缺乏強制力的老病沉痾同樣也延伸至網路領域（Katagiri, 2021, p. 3）。在此等因國際社會現實導致的法律真空下，主要科技公司等私營部門則陸續填補此一領域的規範真空，利用其數位產品重塑規範，成為「規範企業家」（Katagiri, 2021, p. 3）。然而，該等企業干預這個場域的立法形成的結果亦導致各行為體之間缺乏協調，私部門利益與國家利益並不完全一致的弊端（Katagiri, 2021, p. 3）。此外，國際社會關於網路空間規範的討論高度不民主，主要由少數大國和積極的中等強國主導，而這些國家對應採用的規範存在重大分歧。國際法在應對這些挑戰時面臨嚴重缺乏的一致性、反覆性的國家實踐，可見一斑（Katagiri, 2021, p. 3）。

二、駭客行動主義者（hacktivists）之概念意涵

誠如上述，鑑諸網路空間中非國家行為者占主導地位的現實，實有必要就網路空間中的非國家行為者的組織型態與類型態樣予以系統性的分析（Sigholm, 2013）。職此，駭客行動主義者指涉利用網路進行政治或社會抗議，該等行為移離於時而合法，時而非法的灰色空間，並且背後多隱藏政治、軍事或商業目標。常見的行為包括：網頁篡改（defacement）、網路資源重導（redirects）、分散式阻斷服務攻擊（DDoS）、資訊竊取（data theft）等（Sigholm, 2013, p. 14）。往昔較為人所知、頗具代表性的駭客行動團體是「匿名者」（anonymous），他們發動過多起重大攻擊，如對山達基教會的戰爭、阿拉伯之春的支援行動等。這些行為主要是出於政治或社會立場，具有強烈的抗議性質。有學者將上述非國家行為體更系統化地賦予概念意涵與判斷基準（Sigholm, 2013, pp. 14-23），茲分述如下。

（一）駭客（hackers）

駭客乃指涉擁有高深技術知識的人，他們深入了解計算機硬體、軟體、操作系統及網路運作，並且能夠設計複雜的攻擊。根據動機和道德標準，駭客可分為三類（Sigholm, 2013, pp. 14-15）：

1. 黑帽駭客（black-hat hackers）：進行非法攻擊，通常以牟利為目的，無視法律後果。例如竊取信用卡信息或入侵企業系統。
2. 白帽駭客（white-hat hackers）：亦可稱為道德駭客，受雇於政府或企業，負責測試網路安全、修補漏洞，從而防止黑帽駭客的攻擊。
3. 灰帽駭客（grey-hat hackers）：介於黑帽與白帽之間，通常不以非法行為為主，但偶爾會進行一些未經授權的行為，如在未通報的情況下發現並修復漏洞。

（二）愛國駭客（patriot hackers）

愛國駭客的主要目的是協助本國政府，通過網路攻擊來支持或宣揚本國的政治利益，特別是在衝突或戰爭中。例如，中國的「紅客聯盟」曾發表愛國駭客宣言，並與其他駭客發動過「駭客戰爭」。俄羅斯的愛國駭客也在過去的數次戰爭中，發揮了重要作用，如在 2007 年愛沙尼亞 DDoS 攻擊、2008 年喬治亞網路戰等（Sigholm, 2013, pp. 16-17）。

（三）內部網路人員（cyber insiders）

內部網路人員是指擁有合法存取權限的人，他們因金錢、報復或個人動機背叛自己的公司或政府機構，進行資料竊取或內部攻擊。這些行為相對難以偵測，因為這些人擁有合法權限。例如，開發人員可能會在程式中植入後門，或者利用 USB 裝置竊取機密資料。最著名的案例是維基解密（WikiLeaks）事件（Sigholm, 2013, pp. 16-17）。

（四）網路恐怖分子（cyber terrorists）

網路恐怖分子利用網路技術發動攻擊，旨在達成政治或意識形態目標，並造成公眾恐慌。雖然專家對網路恐怖主義的威脅評價分歧，但如果網路攻擊成功，可能

對國家安全、經濟或公眾信任造成極大損害。網路恐怖攻擊的特點是具有高度隱蔽性與無國界的特徵（Sigholm, 2013, p. 18）。

（五）惡意軟體作者（malware authors）

惡意軟體作者專門開發用於惡意攻擊或犯罪活動的軟體，如病毒、木馬、勒索病毒等。他們的技術非常高超，並且擅長隱匿攻擊，避免被防毒軟體、間諜程式防護或垃圾郵件過濾技術發現（Sigholm, 2013, pp. 18-19）。

（六）網路詐騙者（cyber scammers）

網路詐騙者通過各種手段利用網路進行欺詐，目的是獲取受害者的金錢或敏感資訊。常見的詐騙手法包括：（1）隨機垃圾郵件詐騙：如假冒樂透獎金或高薪工作機會等。（2）網路釣魚（phishing）：發送假冒銀行或其他機構的電子郵件，誘騙受害者提供敏感資料。（3）標槍式網路釣魚（spear phishing）：更具針對性，利用社交工程技巧欺騙特定目標（Sigholm, 2013, p. 19）。

參、網路攻擊於國際法律體系之邊緣性及非拘束性

誠如前述，當前國際法上尚無一套全面性的國際法律架構能夠統一規範所有類型的網路攻擊，惟世界各地的多邊組織已開始透過零散的法律與政策措施，試圖遏制此一日益嚴重的安全威脅行動。本節簡要回顧由聯合國、北約、歐洲理事會、上海合作組織等機構發起的相關法律行動與制度。又此等國際規範體系基於系爭規約是否以網路攻擊行為直接規範客體，進而可分成「直接規範網路攻擊之國際法律體系」與「間接規範網路攻擊之國際法律體系」，茲解析如下。

一、直接規範網路攻擊之國際法律體系

（一）聯合國（United Nations）

聯合國在網路安全議題上的進展至今仍相對有限。儘管聯合國大會曾通過多項關於資訊安全的決議，惟核期性質多屬原則性聲明，未能落實化為具有強制規範

效力的具體遵循義務（Hathaway et al., 2012, pp. 860-861）。惟不容諱言的是聯合國大會允許所有會員國參與，係當前得以廣泛討論凝聚全球共識的超國界國際組織雖然其決議無法律拘束力，但具有象徵意義，可反映各國對網路安全政策的立場（Hathaway et al., 2012, pp. 860-861）。此外，大會亦可主導研究與設立專家小組，如 2004 年起運作的「政府專家小組」（Group of Governmental Experts, GGE），即已發表多份重要報告，扮演超國界組織引領未來制定規範前瞻視野的專家要角（Luzzatto, 2022, p. 266）。晚近值得注意的發展為 2015 年 GGE 發布之《關於從國際安全的角度看資訊和電信領域的發展政府專家組的報告》（*Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*），該份調查報告首度明確確認《聯合國憲章》適用於網路空間；要求國家不得蓄意損害他國關鍵基礎設施。國家應避免讓境內被用作發動惡意網路活動的平臺（Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015）。2021 年 GGE 報告《從國際安全角度促進網路空間負責任國家行為政府專家組的報告》（*Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*），重申 2015 年報告的原則與規範；強化對國際法適用的承認，尤其是《國際人道法》、《國際人權法》、《國家責任法》；呼籲各國建立國內政策協調機制與網路事件應變能力（Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2021）。

（二）北約（North Atlantic Treaty Organization, NATO）

迄至 2007 年愛沙尼亞遭大規模網路攻擊後，北約方才開始重視網路安全威脅。似顯示其缺乏明確的網路防禦原則與整體戰略。2008 年布加勒斯特高峰會（2008 Bucharest NATO summit）後，北約設立合作網路防禦卓越中心（Cooperative Cyber Defense Centre of Excellence），負責整合成員國能力與制定長期戰略（Hathaway et al., 2012, pp. 861-862）。2008 年在北約網路防禦卓越中心的邀集下組成北約國際專家小組（International Group of Experts），該小組編纂的《塔林手冊》被稱為「第一

部網路戰爭規範法典」（孫國祥，2015，頁 167-168）。塔林手冊的編纂小組成員中不乏同時具備學術與軍事背景的專家，集結多位編輯委員、法律專家、同行評審人員，以及所有技術顧問、紀錄員與專案協調與管理人員，多來自北約或各國軍方。因此，自其發起機構、人員組成與編撰過程來看，《塔林手冊》成書背後所匯集兼具學術、政治與軍事等多重背景的專家學者雖不乏軍事強權國家試圖領軍成為網路攻擊法制之規範制定者的意圖，惟囿於國際地緣政治，與取得等同國際法之拘束力仍有一定程度的落差（孫國祥，2015，頁 167-168）。

《塔林手冊》嗣後於 2017 年推出《塔林手冊 2.0》版，仍堪稱人類迄今為止最具系統性地針對網路戰制定規則的重要嘗試。新一代專家沿用原始《塔林手冊》的格式，制定了補充性規則，並將其與原有規則合併，形成了這部《塔林手冊 2.0：適用於網路行動的國際法》。因此，《塔林手冊 2.0》取代了初版手冊的地位。首先須明確理解，《塔林手冊 2.0》並非法定文件，而是兩次由獨立專家群以個人身分進行之研究工作的成果（Schmitt, 2017, pp. 2-3）。該手冊不代表北約合作網路防禦卓越中心或北約本身之立場，亦不反映任何觀察員所代表之組織或國家的官方立場乃手冊中一再強調者（Schmitt, 2017, pp. 2-3）。此外，本手冊所呈現之法律內容係反映截至 2016 年 6 月兩屆國際專家小組採認時之國際法狀態。同時序言中亦明揭本手冊之問世，實非「最佳實務」指引，亦非國際法「漸進式發展」之產物，更不帶有任何政策性或政治性立場（Schmitt, 2017, pp. 2-5）。換言之，《塔林手冊 2.0》意圖客觀呈現現行有效之法律（lex lata），因此兩屆專家小組均刻意避免納入任何屬於擬制法（lex ferenda）之主張（Schmitt, 2017, pp. 2-5）。目前，直接處理網路行動的條約極為有限，即使已有者，其涵蓋範圍亦相當狹隘。同時，鑒於國家網路行動多屬機密，且關於「法之意見」（opinio juris）之公開表示亦屬稀少，因此現階段尚難明確界定是否已存在具體之網路習慣國際法。然而，此一法律上的空缺並不代表網路行動處於無規範的真空狀態。

（三）歐洲理事會（Council of Europe）

與其他國際組織相比，歐洲理事會在網路安全領域起步最早、規範也最具體，2001 年通過的《布達佩斯網路犯罪公約》（*Cyber-Crime Convention*）是全球首部針

對網路與電腦犯罪的國際條約，旨在透過立法與合作建立保護社會的共同刑事政策，《布達佩斯網路犯罪公約》制定之網路犯罪及相關行為包括：垃圾郵件、駭客攻擊、病毒散布、色情內容、身分盜用、資料竊取、資料操控、勒索軟體、分散式阻斷服務攻擊、企業電子郵件詐騙、電子郵件偽造、銀行詐欺、社群媒體濫用，以及智慧財產權侵害等。公約也涵蓋關於網路霸凌、網路騷擾、「復仇式色情」以及「假新聞」散播等事件的通報（Nguyen & Golman, 2021）。

圍繞網路攻擊的規範性指針需迄至 2019 年，歐盟（European Union, EU）理事會通過《2019/796 號規章：關於針對威脅歐盟或其成員國的網路攻擊所採取的限制性措施》（*Council Regulation [EU] 2019/796 of 17 May 2019 Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States*），針對威脅歐盟或其成員國的網路攻擊採取限制性措施。復根據系爭規章第 1 條第 3 款明確列舉「網路攻擊」涵蓋：（1）存取資訊系統；（2）干擾資訊系統；（3）干擾資料；或（4）攔截資料。制裁可針對不僅已完成的行為，也包括未遂的行動。欲成為制裁對象，網路攻擊必須符合兩項要件：（1）該攻擊具有重大影響；（2）該攻擊對歐盟或其成員國構成外部威脅（Council Regulation 2019/796, 2019）。

而判斷網路攻擊是否具有重大影響，系爭規章第 2 條訂有明文，亦即可考慮一系列指標：（1）攻擊造成的範圍、規模、影響或干擾的嚴重性；（2）受影響的自然人或法人、實體或機構的數量；（3）涉及的成員國數量；（4）造成的經濟損失金額；（5）行動人為自己或他人獲取的經濟利益；（6）被竊取的資料量或資料外洩的規模；（7）所存取的商業機密資料的性質（Council Regulation 2019/796, 2019）。

前開歐盟《2019/796 號規章》針對網路攻擊所設的制裁框架雖具體且具前瞻性，然其在實務執行層面仍面臨若干挑戰。首先，對「重大影響」的認定雖列有多項指標，但多為質性標準，如「嚴重性」、「規模」與「經濟利益」，易生解釋空間，恐導致成員國間標準不一，進而影響制裁的一致性與可信度。其次，規章設下「外部威脅」作為制裁必要條件，意即若攻擊源自歐盟內部，即便造成重大破壞，亦僅得由各國依其國內法處理，此對跨境網路犯罪實際威脅之應對明顯不足。再者，未遂行為雖納入制裁範圍，理應強化預防效果，然於證據蒐集與行為定性上仍具高難度，在技術上支持法律上歸責一節，仍存在重重阻礙。

（四）上海合作組織（Shanghai Cooperation Organization, SCO）

上海合作組織是由中國、俄羅斯、哈薩克、吉爾吉斯、塔吉克與烏茲別克等國於 2001 年創立之區域性政府間安全合作組織。2009 年於葉卡捷琳堡簽署《上海合作組織成員國保障國際信息安全政府間合作協定》，序言開宗明義明揭：「上海合作組織成員國政府（以下簡稱「各方」）注意到構成全球信息空間的信息通信新技術和新手段在發展和應用方面取得巨大進步；對在民用和軍事領域將這些技術和手段用於與維護國際穩定和安全相悖目的所引起的威脅表示擔憂；認為國際信息安全作為國際安全體系中的一個關鍵因素具有重大意義；深信各方在國際信息安全問題上進一步加深信任、加強協作是當務之急，符合各方利益……」（上海合作組織成員國保障國際信息安全政府間合作協定，2009）。值得強調者，前揭合作協定中提出釐清自身對網路攻擊的定義範疇，較值得注意者，系爭協定第 2 條定義網路技術為「用於傳播破壞國家政治、經濟和社會制度以及精神文化環境的信息」亦納入規範的射程範疇。[1] 此等擴張性理解與西方價值觀與權利觀產生相當大的歧異，蓋西方權利保障式的論述立基於儘可能減少並避免限制政治異議表達的網路活動上加諸過度規範。與此相對地，上海合作組織的規範模式提供了另一種關於網路攻擊的規範觀點，惟於此同時亦凸顯出一個不容否認的事實，亦即全球在定義「網路攻擊」本質與可接受範圍時的重大分歧。析言之中國與傳統西方陣營事實上於是否將「政治顛覆性言論」視為網路攻擊，仍存在深刻價值分歧（Hathaway et al., 2012, p. 865）。

二、間接規範網路攻擊的國際法律體系

除前開專門特定以網路攻擊對規範對象之公約或協議，國際法中尚且另外設置雖非專為規範網路攻擊而設，惟可能因其所涵蓋的「手段」與「工具」被間接適用於特定類型的攻擊行為，從而導致網路攻擊的途徑或工具手段上涉及如以電信資通

[1] 根據《上海合作組織成員國保障國際信息安全政府間合作協定》第 2 條所界定之國際信息安全領域的主要威脅涵蓋如下：（1）信息武器的研製和使用，信息戰的準備和實施；（2）信息恐怖主義；（3）信息犯罪；（4）利用在信息空間的領先地位損害他國的利益和安全；（5）傳播破壞他國政治、經濟和社會制度以及精神文化環境的信息；（6）對全球和各國信息基礎設施安全穩定運行的自然和（或）人為威脅。

訊技術、航空或海洋領域所規範的傳輸技術、設施或活動，這些「手段導向」或「途徑導向」的網路攻擊則會納入射程範疇。整體而言，此類制度提供了一套零散且有限的工具，僅適用少部分藉由特定媒介執行的網路攻擊，無法全面涵蓋所有網路威脅。茲析述如下。

（一）電信法

首先，國際電信法可能適用於涉及國際電纜或無線電頻率通訊的網路攻擊，由聯合國轄下的國際電信聯盟（International Telecommunication Union, ITU）負責制定與管理。該組織旨在「透過高效率的電信服務，維護世界和平並促進所有國家的經濟與社會發展」。ITU 制定的規範包括具條約效力的管理規則與無線電規則，以及不具拘束力的電信標準，主要作用是協調成員國間無線頻譜與通訊資源的分配與使用（Hathaway et al., 2012, pp. 867-868）。

揆諸實際，《國際電信聯盟憲章》（*Constitution of the International Telecommunication Union*）並未直接定義或規範「網路攻擊」，但憲章第 1 條開宗明義宣示憲章之本旨為促進全球通信安全、國際合作；復憲章第 45 條規定有害干擾（harmful interference）之禁止：「所有電臺，無論其用途為何，均應以不對其他成員國、已認可的運營機構，或依《無線電規則》規定運作並從事無線電業務的其他合法授權運營機構之無線電服務或通信造成有害干擾的方式設立與運作」（Constitution of the International Telecommunication Union, 1992）。條文為數甚少，且多是例示性、外交呼籲式的政策指針，難謂構成國際間對資安與跨國電信保護的法律基礎。

（二）航空法（aviation law）

當網路攻擊干擾非軍用航空系統時，可能誘發三項主要的國際航空法規之適用：亦即 1944 年《國際民用航空公約》（*Convention on International Civil Aviation*, 因簽署地點位於美國芝加哥，又稱為《芝加哥公約》）、1971 年《蒙特婁公約》（Montreal Convention），以及 1988 年《蒙特婁機場暴力行為制止議定書》（*Montreal Convention for the Suppression of Unlawful Acts Against Civil Aviation*）。揆諸前揭三公約之規範意旨，若攻擊造成航空管制中斷、乘客名單或禁飛名單被篡改，即可能違反上

述法律。事實上，各該公約各有規範重點，首先，《芝加哥公約》建立了國際民航組織（International Civil Aviation Organization, ICAO），要求成員國對「民用航空航行安全給予應有關注」，並禁止任何干擾民航飛行的行為。雖然公約 1984 年修正案禁止使用武器攻擊民航機，但在戰爭或緊急狀況下，成員國可暫時中止其部分義務，只需通知理事會。《蒙特婁公約》則進一步明定，任何人若「故意且非法地」使航空器無法飛行，或「危及其在飛行中的安全」，例如破壞導航設施或干擾其運作，皆構成犯罪。因此，若網路攻擊影響飛航操作或空管系統，即屬此犯罪範疇（Hathaway et al., 2012, pp. 869-870）。

復次，《蒙特婁議定書》則擴展法律保護至機場設施。第二條指出，若某人故意使用裝置、物質或武器對機場人員施暴，或破壞設施與航空器、干擾機場服務，若足以危及安全，亦構成犯罪。此包括透過網路干擾乘客資訊、禁飛名單或整體機場資訊系統的行為。承上所述，國際法層次的航空法規並非為網路戰而設，卻已涵蓋多數針對民用航空安全的數位攻擊，為應對此類威脅提供一系列間接但有效的國際規範框架與管制途徑（Hathaway et al., 2012, pp. 869-870）。

（三）海洋法（law of the sea）

近年臺灣海纜斷纜事件層出不窮，引發外界關注。台灣網路資訊中心董事長黃勝雄表示，99% 網路頻寬都依賴海纜，可謂臺灣的「數位生命線」，乘載全球超過 95% 的數據傳輸，舉凡日常的語音通話、看串流影片至金融匯兌交易，以及國際貿易、軍事資訊等，均大幅仰賴海纜進行傳輸，乃各國重要關鍵基礎設施（黃浩珉，2025；蘇思云，2025）。就此涉及海域之國際規範而言，1982 年《聯合國海洋法公約》（*United Nations Convention on the Law of the Sea*, UNCLOS）雖未專門針對網路攻擊設立規範，但其中若干條文，特別是第 19 條、第 109 條與第 113 條，在某些情況下可能間接適用於海上網路攻擊行為。

1. 根據公約第 19 條，外國船隻享有「無害通過」權，但不得對沿海國的和平、良好秩序或安全構成威脅。條文列舉數項「非無害行為」，其中包括（a）對沿海國主權或政治獨立的武力威脅、（c）為損害國防而蒐集情報、（d）涉及國防的宣傳行動，以及（k）干擾通訊系統或其他設施。第（k）款尤其

與網路攻擊密切相關，暗示若在通過時干擾對方的通訊設施，即可能構成違法（United Nations Convention on the Law of the Sea, 1994, Article 19）。

2. 第 109 條則規定，各國應合作制止來自公海的未授權廣播，定義為「從船舶或設施向大眾傳送音訊或電視節目，違反國際規範者，但不包括求救訊號」。因此，若網路攻擊透過海上船舶侵入並發送違法訊號，可能構成此規範之違反（United Nations Convention on the Law of the Sea, 1994, Article 109）。
3. 第 113 條要求各國制定法律懲罰蓄意破壞海底電纜的行為，包括透過網路攻擊導致的損害。若攻擊涉及跨國海底電纜系統，行為即可能構成應受追究的國際不法行為（United Nations Convention on the Law of the Sea, 1994, Article 113）。

整體而言，海洋法雖非專為網路攻擊設計，但部分條文已能提供有限的法律依據以應對海上發動的數位威脅（Hathaway et al., 2012, pp. 872-873）。

三、國際案例分析：三種網路攻擊因應模式

在面對國家主導的網路攻擊時，受害國常採取三種策略，選擇的博弈背後往往牽涉深層的地緣政治考量。其一為「沉默與不歸咎策略」，如伊朗在 2008 年震網事件、以及沙烏地阿拉伯與卡達於 2012 至 2017 年間遭遇 Shamoon 攻擊時所採行，出於避免直接挑戰強權、維持區域穩定或避免引發報復行動的政治現實，選擇不公開指責攻擊國。第二為「歸咎但法律立場保留策略」，即國家雖政治上點名攻擊來源國，但刻意不明言是否違反國際法，保留外交協商與未來對抗的彈性，常見於與大國有經濟或軍事依存關係的國家。第三為「歸咎與多邊聯合認定策略」，如美國與歐洲盟邦對中國 APT 駭客或俄羅斯選舉干預的回應，透過跨國合作建立指控的可信度，強化集體回應，顯示出地緣聯盟在網路安全領域的重要性。這三種模式反映國家在高度敏感且具戰略意義的網路空間中，如何在法律、政治與地緣結構間尋求平衡（Sander, 2019, pp. 365-368）。

（一）沉默與不歸咎策略

2008 年伊朗的震網事件是歷史上首次確認由國家主導的網路攻擊之一。儘管該攻擊導致離心機出現異常運作，伊朗當時並未立即察覺是網路攻擊所致，也未公

開將攻擊歸咎於其他國家（Sander, 2019, pp. 365-368）。類似情況同樣出現在 2012 至 2017 年間的 Shamoon 攻擊中，沙烏地阿拉伯與卡達的能源部門及媒體機構遭受嚴重破壞，然而兩國政府迄今未公開指責任何國家或組織。這種策略可能出於政治考量，避免衝突升高，但同時也可能使攻擊者得以持續行動，缺乏必要的威懾效果，尚且可稱之為沉默與不歸咎策略（silence as pertaining to the what attribution question）（Sander, 2019, p. 365）。

（二）歸咎但法律立場保留策略

第二種網路攻擊因應模式，學者稱之為歸咎但法律立場保留策略—— "publicly attributing cyber attacks to other States whilst remaining silent about whether international law is applicable to the situation"，其具體事例為 2014 年，美國 Sony 影業遭駭客入侵，事件不僅造成巨額財產損失，隨之觸發對國家資訊安全的高度警覺。美國政府迅速公開指控北韓為幕後主使，並對相關個人及機構祭出制裁。然而，美國並未就該攻擊是否違反國際法發表明確法律意見。這反映出美國傾向將此類行為視為「具敵意的行為」而非明確的「武力使用」，進而保留政策與法律空間（Sander, 2019, p. 366）。

（三）歸咎與多邊聯合認定策略

最後一種的策略乃歸咎與多邊認定策略—— "publicly attributing them to another State and confirming that the pattern of operations constituted a violation of international law"（Sander, 2019, p. 367）。2017 年 WannaCry 勒索病毒在全球造成大規模癱瘓，英國、美國及其他五眼聯盟國家（包含加拿大、澳洲、紐西蘭）相繼公開指控北韓為攻擊主謀。該事件是跨國聯合歸咎的典型案例，不僅展現出網路安全合作的重要性，也強化了攻擊來源國的政治壓力。值得注意的是，科技企業如微軟也加入歸咎行列，顯示出民間力量在網路安全領域扮演日益關鍵的角色（Sander, 2019, pp. 366-368）。

綜合以上所述，當前國際社群對網路敵意行為的回應暨究責模式歸納如表 1。

表 1
網路攻擊各國歸咎策略歸納表

因應模式	具體事例	發動主體	有無科技企業介入
沉默與不歸咎策略	2008 年伊朗震網事件、2012-2017 年 Shamoon 攻擊	伊朗、沙烏地阿拉伯、卡達	無
歸咎但法律立場保留策略	2014 年索尼影業遭駭事件	美國	無
歸咎與多邊聯合認定策略	2017 年 WannaCry 勒索病毒事件	英國、美國、加拿大、澳洲、紐西蘭	有

四、國家責任與盡職調查之適用與解釋

（一）國家責任歸因的適用侷限與解釋取向

綜上以言，鑒於當前網路攻擊日益盛行管制不易，基於網路環境及互聯網技術有其直接歸因上的技術困難性，聯合國國際法委員會（The International Law Commission, ILC）2001 年通過的《關於國家不法行為責任的條款草案》（*Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, 以下簡稱《草案》）第 4 條至第 8 條明定國家行為的歸責原則。第 4 條確認，無論是行使立法、行政或司法等職能的任何國家機關，其行為均可歸責於國家；該等機關可包含具有此地位的個人或實體。第 5 條進一步擴張至非正式國家機關但依法受權行使政府權力的個人或實體，其在行使該等職權時所為行為亦可歸責於國家。第 6 條則處理跨國支配情形，即當一國機關受另一國控制並代表後者行使政府職能時，相關行為歸屬於支配國。第 7 條強調，即使行為者逾越職權或違背指示，只要其名義上仍為國家機關或授權者，行為仍視為國家行為。第 8 條則涵蓋非正式代理人，只要行為人實際受國家指揮、控制或指示，其行為亦可歸責於國家。整體而言，此部分規章明確釐清國家透過正式或非正式機構行為的歸責架構，實具有界定國際法上釐清國家責任的適用範圍之規範功能。

前揭《草案》規定可謂替國家機關的網路行動、他國機關的網路行動歸因與非國家行為體網路行動的責任確定揭示一可資參照的規範性指針。並且此歸因準則

也受到《塔林手冊 2.0》所部分承繼，舉例而言，《塔林手冊 2.0》第四章“Law of International Responsibility”一章中之規則 15 至 18 即直面網路行動歸責於國家的問題。根據前開規則，《塔林手冊 2.0》認為，地理因素在歸責問題上僅具有限的相關性。尤其當國家可能為了隱匿其行為，從其領土之外發動網路行動。例如，某國可指示（參見規則 17）位於他國的非國家行為者，將分布於多個國家的主機納入殭屍網路，並利用該殭屍網路攻擊受害國。此處的關鍵問題在於，該非國家行為者是否依據第一國的指示行事，而非其進行行動的地點。

如前揭手冊之規則 15 所述，網路行動發動之地，或殭屍電腦所在之國，僅因相關行為團體或殭屍電腦位於其境內，並不足以推定該國必然須對該行動負責。然而，若該領土國家未能對相關個人或網路基礎設施採取適當管控措施，則可能引發「應盡注意義務」問題。在此情況下，該發動網路行動之國家可能因自身未能採取必要補救措施而承擔國際責任，而非基於對該網路行動本身的歸責（朱玲玲，2019，頁 76），應予敘明。

（二）國家盡職調查義務之適用侷限

承上所述，於釐清網路行為與國家責任體系之關係後，需要續行處理的問題意識乃現行國際法體系是否足以規範跨國敵意行為？為何若干國家在既有國際法體系下仍選擇了歸咎但保留法律立場的譴責途徑？其具體成因實與網路敵意行動的本質與事實上對行為者進行歸屬判斷（factual attribution）上的困難使然。國際軍事法大儒 Michael N. Schmitt 即精闢地綜合國際法判決先例與《塔林手冊》對此一規範的詮釋後指出，部分國家對於將「應盡注意義務」（due diligence）原則適用於網路行為持保留態度，原因在於此舉將使其承擔相應的法律義務（Schmitt, 2015, pp. 71-72）。應盡注意義務源自「主權」原則。根據此原則，國家在其領土範圍內對各項事務與行為享有主權的同時，亦必然負有相應之法律責任（Schmitt, 2015, pp. 71-72）。

1941 年「煙塵事件仲裁案」（Trail Smelter Arbitration）中，國際仲裁法庭裁定，一國「於任何時候均有責任保護其他國家不受本國管轄範圍內個人所造成的損害行為」（Trail Smelter Arbitration, 1941）。嗣後於 1949 年，國際法院於其首案「科孚

海峽案」（Corfu Channel Case）中進一步指出：「每一國家皆有義務不得明知而容許其領土被用作從事侵害他國權利之行為」（Corfu Channel, 1949）。

然而，各界對於是否將此原則適用於網路空間持保留態度，亦屬情有可原，揆諸實際，某些國家的網路基礎設施經常被用來發動或協助對他國有害的網路行動，卻未涉及足以使該行為歸責於該國的任何國家行為（Schmitt, 2015, pp. 73-74）。再者，事實上對行為者進行歸屬判斷上的困難，會妨礙一國採取行動終止該等網路行動。此等顧慮在網路連結度高的國家尤其明顯，因為這些國家的惡意軟體感染率通常也最高。正因如此，這些國家的網路基礎設施極易受到惡意行為者的入侵，並被轉為殭屍網路（botnets），進而被用於對其他國家發動攻擊。換言之，這些國家恐將承擔最為沉重的「應盡注意義務」負擔（Schmitt, 2015, p. 74）。

肆、臺灣的網路攻擊風險與當前應對挑戰

臺灣因地緣政治敏感性長期處暴露於高度的資訊戰與網路攻擊風險之中。根據行政院發布之當前資安情勢分析，我國證券業遭 DDoS 攻擊、WannaCry 勒索病毒及遠東商銀 SWIFT 系統遭入侵事件，此外勒索軟體爆炸性成長、DDoS 攻擊遽增、組織型駭客猖獗，國內外資安威脅陡增（行政院資通安全處，2017）。目前，臺灣雖已建立《資通安全管理法》、設立國家資通安全研究院（National Institute of Cyber Security, NICS），政府已推動《國家資通安全戰略 2025》，強調「資安即國安」理念，並建立國家資安戰情協同應變中心，以及強化國家資通安全會報，提升整體資安韌性，惟仍面臨幾項來自制度面和執行面的多重挑戰，諸如歸責困難：臺灣缺乏足夠的技術與國際支援來進行攻擊來源溯源（attribution），導致難以對攻擊進行政治或法律回應，缺乏統一應對架構（目前資安事件的應變主要由各部會與民間單位個別處理）等。再者對於遭受的國家級攻擊是否屬於武力攻擊、是否適用國際法仍卻乏清楚立場，不啻加劇臺灣關鍵基礎設施遭受不預期威脅的突發性與脆弱性。根據本文前開分析，臺灣可從下列途徑強化網路攻擊應對策略。

一、建立分層回應模型

建立一套涵蓋政治、法律、外交與技術層次的「分層回應機制」，依據攻擊程度與來源可信度，分為低度、中度、高度危機應對模式。此一模式不僅需具備即時反應能力，更應融入「威脅中立性」、「內向聚焦」與「去政治化潛力」等韌性治理核心理念。

具體而言，在面對低度攻擊時，應以技術調查與快速修復為優先，並由國家資通安全研究院主導技術層面調查與系統恢復，同時持續監控相關威脅源頭是否擴大；由於此類攻擊未必能即時辨識來源，採取威脅中立（threat-neutral）手段，有助於提升整體資安結構對多樣威脅的普遍應對能力，例如資料備援、資訊同步與系統自動化回復。

當情勢升級為中度危機，則啟動政府跨部會協調與資訊發布機制，由國家資通安全研究院主導各部會資源調度與對外溝通。此階段強調「內向聚焦」（inward-focused），即此時與其對外歸責，毋寧應優先鞏固國內制度與資源整合，並聚焦於

圖 2
分層防禦機制示意圖

自我防禦能力的強化與社會秩序穩定。同時透過與民間企業、地方政府與公民社會的協作，強化各層級回應能量，提升整體國家韌性。

若攻擊明確可歸責於特定國家或組織，進入高度危機等級，則啟動外交與法律層面的反制機制。此時可由外交部發表聲明，提出國際訴求與尋求盟友支持，並由專業法律顧問團隊評估國際法之適用性與反制空間，例如援引《聯合國憲章》第51條自衛權原則，或參考《塔林手冊》提出國際法的回應策略與論述主張。

二、建立網路攻擊歸責標準與公開機制

建立網路攻擊歸責標準，例如攻擊工具特徵、指令與控制伺服器位置、語言指令特徵、攻擊歷史與目標一致性等。同時，建立公開歸責程序，在符合證據標準的情況下，由政府正式對外說明並發表政策立場，以建立國內外的信任。

本文分析三種主流網路攻擊歸責策略——「沉默與不歸咎」、「歸咎但保留法律立場」與「歸咎與多邊聯合認定」——之後，紆衡臺灣當前的國際地位、地緣政治處境、對外關係與資訊化戰爭所受威脅的型態，當前最適合臺灣採取的策略乃第二種：「歸咎但保留法律立場策略」。此一策略兼顧政治彈性、外交空間與國內外輿論管理，是在實力不對稱與國際承認受限下，相對穩健且具操作性的選項。

（一）政治與法律彈性兼具

首先，若直接採取「歸咎並訴諸國際法」的模式，網路攻擊歸責標準不明與國際法對於網路敵意行為意涵不清的基礎上，恐陷入更複雜的話語權競爭。相對而言，透過政治點名特定來源國，卻不立即啟動法律反制程序，可保留外交協商與未來回應的操作空間，同時對外表明立場、維護自身正當性與主權主張。

（二）因應地緣政治與軍事現實

考量臺灣長期面對的是來自中國的複合性灰色地帶作戰行為（如 APT 攻擊、假訊息滲透、供應鏈破壞等），直接採取「公開聯合歸責」可能引發對方更強烈的反制或侵擾行為，也可能致使第三方國家降低合作意願。因此，保留法律立場可作為一種戰略性模糊手段，減少地緣對抗的激化風險。在國內方面，透過有限度的公

開歸責，可回應社會對透明資訊的需求，強化民眾對政府的信任感；在國際方面，即使無法全面參與多邊安全合作機制，仍可藉由明確的政治語言與一致政策回應，建立臺灣在資安責任與規則遵守上的形象，促進理念相近國家的信任與合作意願。

（三）搭配公開歸責標準與程序建構，提升可信度

臺灣應通盤檢視現行既有法制，分別就電信資通訊技術、航空或海洋領域所規範的傳輸技術、設施或活動，這些「手段導向」或「途徑導向」的網路攻擊之法律意涵與違反後的制裁法律效果，形諸明文，建立一套制度化的歸責標準與公開機制，在對國際社群有限參或嗣後採多邊認定的情況下，也能以高度專業與透明的方式爭取國際輿論支持，彌補法律地位的弱勢。

三、明確國際法立場與解釋取向

總結上述討論，「歸咎但保留法律立場」策略提供了高度彈性與實務可行性，符合臺灣當前的國際角色與資安風險態勢。此策略既不會讓網路敵意行為無從究責，又不至於過度升高衝突風險，是臺灣在灰色地帶戰爭與認知作戰下穩健而務實的回應方式。搭配制度化歸責流程與跨部門協調機制，更能使此策略發揮最大效益。

其次，主管機關應針對網路攻擊是否構成「武力使用」或「武裝攻擊」提出法律見解，並釐清國際人道法、主權原則、禁干涉原則在網路領域的適用情境。同時，應修法擴大《資通安全管理法》適用範圍，涵蓋重要民間平臺（如社群媒體、雲端服務提供者）與跨境數據流通。而這類關鍵資訊基礎設施（critical information infrastructure, CII）所潛藏的弱點亦成為駭客或敵軍攻擊的目標。由於關鍵基礎設施具有相互依存的特性，部分關鍵基礎設施如果遭駭而失效，可能引發連鎖衝擊，造成系統性全面崩潰，不僅擾亂民眾生活秩序，也阻礙經濟發展，更可能危及國家安全。

在備受爭議的歸責議題上，若攻擊明確可歸責於特定國家或組織，則啟動外交與法律層面的反制機制，自不待言，而在非國家行為體涉嫌發動之攻擊之情境下，學者參考前揭國際法各項淵源與《塔林手冊》提出的判斷基準頗值參考，亦即當有害的網路活動可追溯至某政府的電腦時，除非該國能提出令人信服的解釋，證明該

電腦是被外部操控，否則該行動將被歸責於該國。而在當今網路行為也可能由非國家行為者（non-state actor）所發動之情境脈絡下，根據國際法，若非國家行為者的行動造成對他國的損害，僅在該行動可歸責於某一國家時，該國才須承擔國家責任（Couzigou, 2018, pp. 38-39）。

根據國際法，非國家行為者的網路行動可歸責於一國的情形，尤其包括下列三種情況：

第一，根據《國際不法行為國家責任草案》第 5 條關於行使政府權力要素的個人或實體之行為規定一節，系爭行動是由獲國家授權行使政府職權之個人或實體所為。例如，若國家授權某私人公司執行通常由政府行使的職權，並要求其執行網路行動，則該行為可歸責於該國（Couzigou, 2018, pp. 38-39）。

第二，當國家明確承認並採納某一網路行動為自身行為時，該行動亦視為該國之行為（Couzigou, 2018, pp. 38-39）。

第三種情況，也是最常見的一種，是行動實體係在一國的指示、指導或控制下執行行動。例如，當一國僱用某個人或某個組織來發動網路攻擊時在此情形中，該國對該行為的指導或控制程度必須是高度的，亦即，該國應對特定的網路行動具有實質上的指揮或控制。是否構成這種情形，應根據個案具體事實加以判斷（Couzigou, 2018, pp. 38-39）。[2]

伍、結論：以數位韌性為圭臬的中長程因應策略

資訊化戰爭已是各國莫不苦於應對之國家課題，隨著數位依賴的深化，臺灣所面對的網路安全挑戰日益嚴峻，卻無系統化、持續性的，以加強數位韌性為圭臬的中長程策略因應。其次，網路敵意行為跨越疆界、難以明確釐清歸責的特性，更突顯出現行國際法對於網路攻擊回應的制度性缺口。無論是國家行為者或非國家行為者，其交錯進行的網路行動，常在法律定義與實務操作上模糊不清，使得相關國際規範在適用上備受侷限。

[2] 參見國際法院 1986 年尼加拉瓜訴美國案（Nicaragua v. U.S.）乙案。Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), 1986 I.C.J. 14.

本文爬梳目前的國際法體系，發現當前國際法上對於網路攻擊之相關準繩雖涵蓋聯合國框架下的資訊安全決議與北約主導的《塔林手冊》，但整體而言，前者多屬原則性宣示，欠缺法律強制力；後者雖為西方主導的初步法制建構嘗試，卻亦未具國際法律地位，尚無法形成普遍約束力。此顯示國際社會雖已意識到網路安全的重要性，但實質法治建構仍處於初步階段。

面對此一局勢，國際社會主要採取三種因應模式，包括「保持沉默不歸咎」、「歸咎但保留法律立場」以及「歸咎並尋求多邊聯合認定」。這些模式反映出各國在國際法秩序博弈中的策略選擇，也揭示出在國際共識尚未形成之前，國家多傾向保留法律彈性以維持自身利益。承襲此一脈絡，本文主張臺灣採取多層次策略應對此一挑戰。首先，需加強本土法律制度建構，明確界定網路攻擊與資安應對的法理基礎。另則須建立具備韌性的數位治理架構，不僅提升防禦能量，更應強化整體社會對資安風險的認知與韌性，加強社會對數位威脅的承受與復原能力及持續性，同時構築邁向兼顧本土需求與國際接軌的資安防禦韌性之國家安全戰略，俾利臺灣於變動不居的網路地緣政治中，確保自身安全與國際法治參與的能動性。

參考文獻

上海合作組織成員國保障國際信息安全政府間合作協定，2009 年 6 月 16 日，https://www.doj.gov.hk/en/external/pdf/lawdoc/127.pdf [Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, June 16, 2009.]

朱玲玲（2019）。從《塔林手冊 2.0 版》看網絡攻擊中國家責任歸因的演繹與發展。當代法學，**2019**（1），70-78。[Zhu, L. L. (2019). Deduction and development of state responsibility attribution in cyber attacks from the perspective of Tallinn manual version 2.0. *Contemporary Law Review*, *2019*(1), 70-78.]

行政院資通安全處（2017）。當前資安情勢分析。行政院，11 月 2 日。https://www.ey.gov.tw/Page/448DE008087A1971/07afd354-6fb9-41dc-9091-929db6d8358a [Department of Cyber Security, Executive Yuan. (2017). *Dangqian zian qingshi fenxi*. Executive Yuan, November 2.]

林昕璇（2023）。淺談網路犯罪、網路戰與網路攻擊之分際線。載於丁綺萍（主編），數位韌性與科技倫理（102-107 頁）。財團法人台灣網路資訊中心。[Lin, H. H. (2023). Qiantan wanglu fanzui, wanglu zhan yu wanglu gongji zhi fenjixian. In Q. P. Ding (Ed.), *Shuwei renxing yu keji lunli* (pp. 102-107). Taiwan Network Information Center.]

孫國祥（2015）。《塔林手冊》的介紹與初步評析。全球政治評論，（51），167-173。[Sun, K. H. (2015). Introduction and assessment of the Tallin manual. *Review of Global Politics*, (51), 167-173.]

黃浩珉（2025）。海底電纜斷裂危機下，台灣維繫「數位生命線」的應變挑戰。報導者，2 月 13 日。https://www.twreporter.org/a/damaged-undersea-cables-raises-alarm-in-taiwan [Huang, H. M. (2025). *Haidi dianlan duanlie weiji xia, Taiwan weixi "shuwei shengming xian" de yingbian tiaozhan*. The Reporter, February 13.]

蘇思云（2025）。海纜安全危機 3 ／專家：海纜如台灣「數位生命線」99% 網路頻寬都靠它。中央社，1 月 10 日。https://www.cna.com.tw/news/aipl/202501100036.aspx [Su, S. Y. (2025). Hailan anquan weiji 3 / Zhuanjia: Hailan ru Taiwan "shuwei shengming xian" 99% wanglu pingkuan dou kao ta. Central News Agency, January 10.]

Broeders, D., De Busser, E., & Pawlak, P. (2020). *Three tales of attribution in cyberspace: Criminal law, international law and policy debates* [Policy brief]. The Hague Program for Cyber Norms. https://www.thehagueprogram.nl/wp-content/uploads/2020/04/Policy-Brief_Three-Tales-of-Attribution_Broeders-De-Busser-Pawlak.pdf

Constitution of the International Telecommunication Union, 1992.

Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 2019 O.J. (L 129) 1.

Couzigou, I. (2018) Securing cyber space: The obligation of States to prevent harmful international cyber operations. *International Review of Law, Computers & Technology*, *32*(1), 37-57. https://doi.org/10.1080/13600869.2018.1417763

Citron, D. K., & Eichensehr, K. E. (2025). Resilience for a digital age. *University of Chicago Legal Forum*, *2024*, 45-74. https://chicagounbound.uchicago.edu/uclf/vol2024/iss1/2

Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. (2021). *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (Report No. A/76/135). United Nations. https://undocs.org/A/76/135

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (Report No. A/70/174). United Nations. https://undocs.org/A/70/174

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, *100*(4), 817-885.

Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, *7*(1), tyab009. https://doi.org/10.1093/cybsec/tyab009

Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, Article 105521. https://doi.org/10.1016/j.clsr.2020.105521

Lin, H. S. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law & Policy*,

4(1), 63-86.

Luzzatto, C. A. (2022). Regulating cyber warfare through the United Nations. *The Cyber Defense Review*, *7*(4), 261-270.

Sander, B. (2019). The sound of silence: International law and the governance of peacetime cyber operations. In T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, & G. Visky (Eds.), *2019 11th International Conference on Cyber Conflict: Silent battle* (pp. 361-382). NATO CCD COE Publications.

Schmitt, M. N. (2015). In defense of due diligence in cyberspace. *Yale Law Journal Forum*, *125*, 68-81.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, *4*(1), 1-37. https://doi.org/10.1515/jms-2016-0184

Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1911, 1963 (Arb. Trib. 1941).

United Nations Convention on the Law of the Sea, 1994.