# 網路作戰之合法性：
# 網路情境下國際法主權概念之分析

楊長蓉

國防戰略與資源研究所

## 壹、前言

「網路作戰」（Cyber Operations）或「網路空間作戰」（Cyberspace Operations）為近年越來越常見的新作戰型態，儼然成為國際衝突的主要戰場之一。網路之虛擬特性所造成的影響，多為干擾性或財產損失，與傳統作戰之物理上損害與傷亡常有不同，不一定能用傳統方式予以法律上的評價，故目前就網路作戰之合法性有諸多討論，包括網路空間作為新興領域（domain），應如何針對網路空間建立新秩序，以及在新規則與秩序建立之前，網路空間是否為法律真空狀態等議題。

國際上目前普遍觀點是現有國際法可以適用到網路作戰。[1]然而「如何」適用國際法，則仍有待共識形成。原因除了網路空間是新興領域之外，尚取決於各國自身利益以及如何因應敵意網路作戰方式。網路作戰之合法性主要涉及之國際法原則與國家義務有三：「尊重主權」（respect for sovereignty）、「不干預原則」（principle of non-intervention）以及「禁止武力使用」（the prohibition of the use of force），存有不少模糊空間與爭議地帶。

由於目前大多數網路作戰皆未達國際法上「武力使用」或是「武裝衝突」（armed conflict）等適用標準，故本文主要就可能「侵害國家主權」（violation of sovereignty）之網路作戰進行討論與分析。限於篇

[1] United Nations, “Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” UN Doc. A/68/98, June 24, 2013, para. 19 (‘UN GGE 2013 Report’); see also “Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” UN Doc. A/70/174, July 22, 2015, paras. 24-5 (‘UN GGE 2015 Report’).

幅，本文不討論歸因（attribution）的問題，[2]所提之型態皆假設為國家支持（state-sponsored）為前提的網路作戰。

## 貳、西方觀點之網路作戰：國際法與塔林手冊

國際法上關於構成「武力使用」標準通常涉及一定程度物理上之損害，但網路作戰所造成之損害與效果有別於傳統作戰，例如以電腦病毒癱瘓他國政府電腦是否構成「戰爭行為」（act of war）？如果病毒僅是暫時癱瘓或使電腦運轉降速，評價是否相同？哪些才是合於國際法的網路作戰？若某國的網路作戰所造成的影響在「規模與效果」（scale and effects）上與實體作戰類似，就有可能構成「戰爭行為」而適用國際法，包括《聯合國憲章》「禁止武力使用」相關規定以及日內瓦公約（Geneva Conventions）等，應無疑義。但實際上要「如何」適用，卻有許多爭議與不明之處。

《塔林手冊》（Tallinn Manual）即是在這種背景下產生，2013 年第一版《塔林手冊：適用於網路戰的國際法》（Tallinn Manual on the Law of Cyber Warfare）檢驗國際法如何適用與管理「網路戰」（cyber warfare），主要包括「訴諸戰爭權」（*jus ad bellum*）與「交戰中的法」（*jus in bello*，或稱武裝衝突法、國際人道法）。《塔林手冊》為國際上第一步全面、系統性探討與解釋網路戰可能的法律問題，出版後即引起廣泛的討論與批評，惟批評塔林手冊者，多是出於其適用與範圍上之誤解與誤用，而並非針對《塔林手冊》內容本身。故在 2017 年第二版 《塔林手冊 2.0 適用於網路作戰的國際法》（Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations）中，擴大了其涵蓋範圍，並更嚴謹檢視「網路作戰」相關國際法，並在序言中再次強調該手冊「本身」並非國際法，不具有任何官方性質，亦不代表北約組織

[2] 歸因主要涉及是技術發展與證據面向問題，並不影響「某行為是否違反國際法」的判斷，且國際法上亦未就歸因之證據標準（standard of proof）定義，故不影響本文之討論。

或任何單獨國家的意見。《塔林手冊》主要的意義是反映現有（至少西方觀點）、客觀上的「實然法」（*lex lata*），但不代表法律發展方向，內容中亦避免使用「應然法」（*lex ferenda*）的主張。

## 參、國際法對網路作戰之規範：「尊重主權」？

「網路作戰」依據《塔林手冊》的定義，為「在網路空間或通過網路空間，為實現目標而對網路能力的使用。」這定義與美國國防部所發佈的文件中之定義相似。[3]美國國防部透過定義「網路空間」來看網路作戰，其由在網路空間或透過網路空間之國防部軍事、情報以及一般日常作戰所組成。[4]需注意的是，「網路作戰」亦不同於「資訊作戰」或「資訊戰」。[5]《塔林手冊 2.0》標題改用「作戰」（operation）而不使用「戰爭」（warfare）一詞，一方面彰顯手冊內容不僅適用於狹義的「戰爭」，另一方面亦避免與修辭性的戰爭概念混淆，特別是在非國際法領域討論，時常將「網路戰（爭）」的概念與「網路犯罪」（cyber crimes，應適用內國刑法）或「網路攻擊」（cyberattacks）[6]等網路行為混合討論，而不利於辨別。

至於網路作戰是否有違反國際法，涉及國家對國際法的理解，特別是主權概念在網路空間的適用，這部分意見相當分歧。另外，在判斷網路作戰之合法性，仍須視該事件本質而定，無論是所謂的「攻擊型」（offensive）或「防禦型」（defensive），又或是所謂的「主動防禦」（active defense）網路作戰，其是否合於國際法以及是否產生國家

[3] U.S. Joint Chiefs of Staff, "*Joint Publication* 3-12: *Cyberspace Operations,*" *June 8, 2018*, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[4] "*Defense Primer*: Cyberspace Operations," *Congressional Research Service*, December 15, 2020, https://crsreports.congress.gov/product/pdf/IF/IF10537/7.

[5] 至少在西方觀點，網路作戰有別於「資訊戰」不同，見前註 4. 惟並非所有國家有此分別，對網路空間的概念也不一定相同。例如俄羅斯在公開與政策文件並不使用「網路作戰」，亦不使用 'Cybersecurity' 而是 'information security'，但這又與西方所認知的 infosec 不同。參考 The Ministry of Foreign Affairs of Russia, "Doctrine of Information Security of the Russian Federation", December 5, 2016, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163。

[6] 「網路攻擊」不一定是指涉國際法上武力行為，與聯合國憲章第 51 條之「武裝攻擊」（armed attack）並不相同，可能只是指涉某種網路行為（cyber measures）或網路事件（cyber incidents），是否構成武力使用或武裝攻擊仍需視個案狀況是否符合相關要件而定。

責任（state responsibility），仍須依個別情境做個案判斷，並不能依字面上做認定或判別。以下先就國際法之主權概念做一說明。

## 一、國家主權之意涵

主權，對國家而言是根本性的存在，也是國際法的核心原則。依據 1928 年《帕爾馬斯島仲裁案》（Island of Palmas Arbitral Award）對主權的定義，主權是「在與他國的關係之中，主權突顯出獨立；獨立是指在不受其他國家影響下，行使國家功能的權利」。[7]主權主要有三個核心權利，領土主權（territorial sovereignty）、國家權力獨立性（independence of state powers）以及各國主權平等（equality of states），又稱外部主權，這些權利彼此之間互相關聯，且為國家主張他國違反其主權之基礎。

《塔林手冊》將主權分為內部主權以及外部主權來做說明。領土主權屬於主權對內面向，包括領土的完整性，係指國家在其領域範圍內擁有最高的法律權威，以及國家權力之獨立性，或是一國政治獨立權（political independence），[8]國家有自由選擇其政治、經濟及文化制度之權利。[9]此概念亦反映在《聯合國憲章》第 2 條 7 款不干涉他國內政原則，惟國家的行為仍受限於國際法的規範，例如國際人權法。[10]此外，國家對於在其領域內的人或事物擁有完整與排他的權威，也就是國家在其領域內可行使排他性管轄權。原則上，領土主權之對內與對外面向皆適用於網路空間。

---

[7] "Island of Palmas (Netherlands v USA)," *Permanent Court of Arbitration*, April 4, 1928, 2 RIAA 829, 838.

[8] Ibid.

[9] "Case Concerning the Military and Paramilitary activities in and against Nicaragua (Nicaragua v U.S.A.)," *International Court of Justice*, June 27, 1986, para. 205. (hereinafter 'Nicaragua case')

[10] "Resolution on the Promotion and Protection and Enjoyment of Human Rights on the Internet," UN Doc A/HRC/20/L.13; UN GGE 2015 Report, para. 13(e), "States should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the internet […]."

## 二、網路空間與侵害主權

依據《塔林手冊》，國家不能進行侵害他國主權之網路作戰（Rule 4）。侵害國家主權，通常指發生在一國在未獲得另一國之同意（consent）的情況下，在該國行使專屬於該國之主權行為。[11]也就是說，若有侵害受害國領土完整性，或是有干預、影響受害國之固有政府功能的行為，即為侵害他國主權。

侵害主權之作為通常涉及物理性入侵一國領域，像是侵入領土、領空，或執行警察權（例如未經地主國允許在該國逮捕嫌犯）等，但網路空間之虛擬特性，其領域範圍與疆界並非如此明確，且網路行為不一定對領域有直接物理上或是有形影響，故對於「何為網路空間之合法行為」仍有爭議。不過，即使行為人未在他國領土內，其境外行為也有可能侵害他國主權，物理上之損害也不一定是必要條件，國際環境法目前亦有不少這樣的案例，例如某國之污染行為影響了鄰國之環境，也會構成主權侵害。[12]網路作戰亦有類似的特性，雖多為遠端操作，且難以確認行為人，但不應影響侵害主權事實之認定。就證據與技術層面，境外的行為或許較難以證明，但在法理上侵害他國主權的行為，似乎不因行為人在境內或境外之作為而異。

## 三、「主權原則論」與「主權規則論」

惟在網路空間情境（cyber context）下，違反國家主權是否即構成違反國際法？這議題因涉及新興領域與個別國家之網路能力，成為近幾年西方國家爭論之處。差別在於，即使不涉及武力使用，若一國之行為有違反國際法，受害國在合乎條件下可以採取「反措施」（countermeasures）回應，[13]故如何認定主權範圍，可能造成國家間對

[11] "Corfu Channel Case (U.K. v Albania)," *International Court of Justice*, April 9, 1949, para. 69-70; Nicaragua case, para.213.

[12] "Trail Smelter Arbitration (*United States v. Canada*)," *Arbitral Tribuna*l, March 11, 1941.

[13] Article 49 of the International Law Commission's Draft Articles on State Responsibility. 聯合國官方文件中文版譯為「反措施」，惟國內有翻譯為「相對措施」或「反制措施」者。

立甚至升高衝突，也可能讓對主權採取廣義概念的國家（例如中國、俄羅斯），更常援引違反主權，作為對抗他國之國際行為。[14]這涉及到國家對於禁止「侵害主權」究竟只是一個原則，即「主權原則論」（sovereignty-as-principle）；或是本身即為國際法的主要規則（primary rule），亦即「主權規則論」（sovereignty-as-rule）的認定。

《塔林手冊》一致的立場是「主權規則論」，即禁止侵害（他國）主權本身係國際法的主要規則；意即，若有國家侵害另一國之主權，會構成國際不當行為（internationally wrongful act），而產生國家責任（state responsibility）。不少國家亦採取此立場，包括奧地利、德國、法國、荷蘭、伊朗等。至於採取「主權原則論」者，目前僅有英國。[15]英國認為，至少在網路情境下，主權原則只是國家互動的指引，但違反尊重主權原則本身並不等於違反國際法，除非同時涉及違反不干預原則或禁止武力使用等，方有法律後果。

「主權規則論」認為，網路作戰若對受害國造成了影響，或是影響該國固有政府功能，等於是在他國領土行使專屬警察權，因此侵害了受害國的領土主權——法國即是採取此立場。法國主張，任何針對法國網路設施（digital systems）、或是對法國境內造成影響的網路攻擊，即為違反法國的主權，而可能產生國家責任。[16]然而，若採取英國的「主權原則論」，除非另有符合「強制」（coercion）要件，構成違反「不干預原則」，始有國家責任。這可能是因為英國為具有強大網路能

[14] Harriet Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention," *Chatham house*, December 2019, p.20.

[15] U.K. Attorney General's Office, "Cyber and International Law in the 21st Century," May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. 美國國防部亦曾發表類似意見， U.S. Department of Defense, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," March 2, 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/，但這與其他美國官方聲明並不完全一致。

[16] French Ministry of the Armies, "*International Law Applicable to Operations* in Cyberspace" September 2019, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

力之國家，故即使明知此立場會遭受不少抨擊，[17]英國仍然選擇公開表態，主要是出於戰略考量，意圖保有合法網路作戰之彈性與空間。

即使採取「主權規則論」，仍然有不少爭議尚待解決，特別是對於侵害他國主權是否應有基本門檻之限制，或是一定要造成某種「效果」（effects）才算數？若不設限，可能會導致「侵害主權」認定過廣，任何未授權的網路入侵行為，皆會構成違反一國主權。[18]例如，德國雖也採取「主權規則論」之立場，但見解較法國保守，認為即使是關鍵基礎設施（critical infrastructure）受到網路攻擊影響，也只是國家主權受到侵害的指標之一，攻擊關鍵基礎設施「本身」並不直接等於違反國家主權，仍需有一定物理上之損害與影響，才會違反領土主權。[19]

就目前國家實踐而言，並非所有未經他國同意之網路行為皆構成主權侵害，例如多數國家皆有情資蒐集的網路諜報活動（cyber espionage），即使被侵入國知情，也不一定對入侵國做出違反主權的指控。[20]《塔林手冊》亦認為網路諜報本身並非違反國際法的行為，應視其手段與所造成的影響而定（Rule 32）。

## 四、判斷標準：「規模與影響」

究竟何時網路作戰會構成侵害他國主權？亦即，侵害他國主權的要件為何？目前國際上對此並無定論，對主權的範圍也有不同見解，是應採取量化標準，例如受害國之損害規模、受影響的人數？或是，

---

[17] Michael Schmitt, "Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention," *International Law Studies* Vol. 96 (2020), pp. 549-576.

[18] 認為即使未造成何損害也會違反他國主權。E.g. Russell Buchan, *Cyber Espionage and International Law*, (Hart Publishing, 2018), pp. 51 ff。

[19] German Federal Government, "On the Application of International Law in Cyberspace,", March 2021, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf.

[20] 例如，俄羅斯在 2016 年駭入美國民主黨全國代表大會（Democratic National Convention）信箱，進而影響總統選舉的行為，並不構成戰爭行為，而屬於一種政治間諜（political espionage）。時任歐巴馬（Barack Obama）政府並未就是否「違反國際法」發表意見，而是採取其他手段處理，包括經濟制裁俄羅斯間諜與官員，驅逐俄羅斯情報人員等。

應採質化標準，例如攻擊的本質？目前不少國家使用不同程度損害影響（harmful effects）作為判斷標準，類似於「禁止武力使用」情境下之網路攻擊的認定，要件主要包括嚴重性（severity）、對社會影響的規模（the scale of the effects on society），惟各國所採取之要件仍有所不同。原則上，若網路作戰所造成之規模與影響可與非網路情境相比擬，基本上會構成侵害主權。

這些判斷標準各國有不同見解，國家採取「主權規則論」或「主權原則論」亦會影響網路作戰合法性的認定。《塔林手冊》依據不同損害程度試圖提供判斷標準：

1. 物理上之損害或傷害：例如 2010 年的「震網」（Stuxnet）即是極少數有構成物理上損害之網路攻擊。
2. 網路設施失去功能性：例如入侵電腦並散播病毒造成電腦無法使用，例如 2012 年全球最大石油公司 Saudi Aramco 遭到 Shamoon 病毒攻擊。
3. 干擾性，但不至於完全失去功能：使電腦速度變慢、操作不同、竄改或刪除資料等。

## 肆、非西方觀點：「網路主權」概念

《塔林手冊》強調，國家對於網路空間本身（*per se*）並不能主張主權（Rule 1）。然而，目前中國、俄羅斯與部份集權國家，將國家領土主權以及領域概念延伸至網路空間，也就是主張國家可以對網路本身主張主權，這是出於前述主權之對內面向，國家對境內的網路基礎設施以及相關活動可行使獨立與排他性的主權，如此則與非網路情境無異。

中、俄等國即是依此提出「網路主權」（cyber sovereignty）的概念。網路主權是中國自行定義、欲控制其境內網路使用之權利所發展的概念，主要用於其定義下的網路治理。在網路主權概念之下，國家

對於網路以及個人資料之傳輸與流通，可採取更嚴格的管控。中國主張，國家當然有控制本國網路空間之權，國家可依自己認為適合的方式治理互聯網（internet），而不受他國政府干涉；亦即，在其領土的網路空間內相關的內容、資訊以及服務等，有排他性管轄權。俄羅斯亦提出類似的「數位主權」（digital sovereignty）概念，並在 2019 年 10 月通過《網路主權法》（Sovereign Internet Law），進一步管制網路自由。[21]

然而，此概念與西方所主張的「網路空間自由使用」有所衝突，美國與多數民主國家反對此一概念，認為互聯網應是全球性與開放的，國家對於流通過其境內的網路交通，僅應行使最低限度的控制。[22]西方所謂的「資訊安全」（information security）是理解為保護資訊與系統，並非控制使用者。[23]不過在近年，「網路主權」的概念似乎影響部分西方國家對網路的管制，由此可見中、俄論述之影響性。[24]

中國、俄羅斯等國雖未對國際法在網路空間之合法性發表官方立場文件，亦主張應對網路空間建立一套新規範，[25]卻也承認國際法在網路空間的適用。[26]但其對主權概念之一貫立場採取廣義概念，可能更常會針對他國網路活動援引侵害主權。[27]此外，網路主權概念雖然原則上符合國際法，但中、俄對於國際法的理解與適用，與西方標準不同，隨著中國網路能力與政治實力崛起，若其掌握網路空間的話語權

[21] "Russia just brought in a law to try to disconnect its internet from the rest of the world", *CNBC*, November 1, 2019, https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html.

[22] NATO Strategic Communications Centre of Excellence, "Russia's Strategy in Cyberspace," June 2021, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf.

[23] Ibid.

[24] 例如英國似乎部分接受網路主權的概念而對網路有進一步管制，但原則上還是主張自由開放的網路。Justin Sherman, "How to Regulate the Internet Without Becoming a Dictator," *Foreign Policy*, February 18, 2019, https://foreignpolicy.com/2019/02/18/how-to-regulate-the-internet-without-becoming-a-dictator-uk-britain-cybersecurity-china-russia-data-content-filtering/.

[25] Annex to "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, International Code of Conduct for Information Security," UN Doc. A/69/723.

[26] See 2013 UN GGE Report, para. 19.

[27] 見前註 14, p. 20.

（discourse），對國際法的發展可能有不利的方向。[28]

## 伍、結論

網路作戰之合法性無法一概而論，除了須視具體狀況，國家對於國際法上主權概念的理解，亦影響合法性之判斷。近年越來越多國家發表關於網路空間適用國際法的官方立場文件，可以看出至少大方向是一致的，即在規模與影響上符合一定程度，仍可能因侵害他國主權而違反國際法。不過，國家如何回應他國之網路作戰，乃是政治性決定，並取決於各國之網路能力。國家亦有可能出於戰略考量而以非法律方式處理，或未對其合法性表態。部份集權國家出現的網路主權論述，雖也符合國際法原則，但可能藉此限制網路之自由與開放，值得密切關注。

本文作者楊長蓉為英國布魯內爾大學法學博士，現為財團法人國防安全研究院國防戰略與資源研究所助理研究員，研究領域為國際法、國際刑事法、國防政策與產業。

[28] Julian Ku, "How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare," *Hoover Institution*, August 17, 2017, https://www.hoover.org/research/how-chinas-views-law-jus-ad-bellum-will-shape-its-legal-approach-cyberwarfare.

# The Legality of Cyber Operation: An Analysis of the Concept of Sovereignty in the Cyber Context under International Law

*Alice Chang-Jung Yang*

*Assistant Research Fellow*

**Abstract**

'Cyber operations', according to the Tallin Manual, is 'the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyber space.' The effects caused by the 'virtual' characteristic of cyber space which are mainly interferences or property losses, are quite different to the physical effects of traditional warfare, such as death and injury, and thus it might be improper to evaluate cyber operations via traditional means. At present, the legality of state-sponsored cyber operations is still under discussion.

The general view of the international community is that international law can be applied to cyber operations. The question, however, is *how* to apply international law, which not only have States' self-interests played a significant role, but also depending on the cyber capabilities of States in responding to hostile cyber operations. Consequently, there is still substantial room for debate and certain issues in this area are left with ambiguity. Even for cyber operations which are below the threshold of the use of force, a violation of international law could occur due to infringements of a state's sovereignty, and thus entitling the victim State to respond with lawful countermeasures. Therefore, the concept and scope of sovereignty is fundamental to the determination of the legality of cyber operations. The different perceptions of sovereignty between States might cause irritations and

will likely further fuel ongoing conflicts. Authoritarian states, such as China and Russia, which have adopted a wide concept of sovereignty, are more likely to invoke the duties of other states to respect their sovereignty when acting against other States' cyber operations. These authoritarian states also attempt to use the concept of 'cyber sovereignty' to exert further controls in cyber space. As to within the Western States, there is some disagreement as to whether 'respect for sovereignty' is a principle under international law, that is, 'sovereignty-as-principle' or whether it is a 'primary rule' *per se*, that is, 'sovereignty-as-rule'. This article discusses and analyzes the concept of sovereignty from the perspective of international law, in order to determine the legality of state-sponsored cyber operations.

**Keywords:** Cyber Operations, Sovereignty, Tallinn Manual