財團法人國防安全研究院
Institute for National Defense and Security Research

中華民國 110 年 11 月 9 日　　第 13 期

國防情勢特刊

網路作戰

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	1
軍文交織的美國網路防護體系	杜貞儀	13
英國的協作式網路戰力建構	吳宗翰	24
平戰結合的以色列網路作戰部隊	曾怡碩、洪嘉齡	34

⊙ NOVEMBER 9, 2021 ⊙

Defense Situation Special Edition Vol 13

Cyberwarfare

The Legality of Cyber Operation: An Analysis of the Concept of Sovereignty in the Cyber Context under International Law	*Alice Chang-Jung Yang*	1
The interwoven US civil-military cyber protection system	*Chen-Yi Tu*	13
Building UK's Cyber Defense Capabilities Using A Collaborative Network Framework	*Tsung-Han Wu*	24
Meeting Peacetime and Wartime Demands: Israeli Cyber Operations Units	*Yi-Suo Tzeng* *Chia-Ling Hung*	34

⊙ NOVEMBER 9, 2021 ⊙

編輯報告

曾怡碩

網路安全與決策推演研究所

網際網路的建立與營運，一開始是完全基於信任原則，當初並未預料會有今日萬事萬物聯網的榮景，也沒有設想網路會因為受個人、企業與政府機關的倚重，而衍生網路攻擊、竊密與資料外洩等資安議題，更未預見時今轉而奉行的零信任政策。當資料的產生、傳輸與儲存都倚賴網路，網路空間自然成為窺伺、竊取與竄改、破壞資料的場域。駭客個人或團體、企業的商業間諜與政府的情報作為，加上層出不窮的駭侵攻擊事例，交織構成國家安全的機會與挑戰，各國政府因而成立專責網路安全單位予以應處。

軍隊與情報機構將網路空間視為新型態作戰場域，紛紛建立規模不等的網路作戰部隊，遂行網路攻擊與防禦。然而，這樣看似再自然也不過的作戰攻防，在遭遇網路空間特性之際，卻衍生出新型態安全威脅的因應難題。

灰色地帶衝突本質

首先，網路攻擊即使造成全球規模的衝擊，仍屬未達戰爭門檻的灰色地帶衝突層級。軍方力求清晰的接戰程序與交戰規則，在網路作戰領域，遭遇到需處理模糊空間的嚴厲挑戰，多會訴諸有相當詮釋尺度的國際法。國際法領域專家學者對於網路作戰原屬陌生，但經過多年努力，以及有北約組織第一版《塔林手冊》的問世，作為討論修正基礎後，第二版《塔林手冊》對於網路作戰的規範逐漸具體成形。本期特刊國際法篇章勾勒這個曲折蜿蜒的過程，也呈現箇中待解難題。

網戰特質影響部隊任務特性

其次，除了平時與戰時難以界定，由於網路空間難以劃界築籬，網路作戰也難以嚴格區分前線與後方，加上網路攻擊往往難以經溯源

即據以確切歸責攻擊源頭，當境內關鍵基礎設施遭受網路攻擊，究竟是由負責抵禦外來威脅的軍方網戰部隊出面，還是交由國內情治部門的網路作戰單位處理，成為民主治理國家安全的新興課題。

針對這個課題，本期特刊藉由美國、英國、以色列網路作戰部隊的任務與運作上的實例研究，發現這些國家不論是軍方或情治部門的網路作戰單位，都被賦予針對境內關鍵基礎設施遭受網路攻擊之應處任務，其中美國有明確授權，協作部分也嘗試制定規則與運作調整。

另一個研究發現則是網路作戰部隊多採境內外前進部署／主動防禦的攻勢作為。這樣的傾向，可歸因於網戰本身從一開始就與情報作戰密不可分。美國的網路作戰司令部與國家安全局過去是一套人馬、兩塊招牌；英國網路作戰部隊與 MI6 有深厚淵源；而以色列 90%的情資來自其 8200 網戰部隊。

網路作戰兼具情報作戰的本質，雖然仍有民主監督情報作業機制的爭議，但至少讓網路作戰部隊具備可在境內從事主動防禦部署的空間與彈性。對此，本期特刊英國篇章敘明近期單獨成立網路作戰部隊的來龍去脈，而美國篇章則引介美國網路作戰司令部與國土安全部對於網路防禦協作的探試，值得後續觀察。

平戰結合有利部隊人力運用

最後，各國網路作戰部隊都面臨人員的選訓與留用的難題。以色列鼓勵網路作戰後備役人員，投入資安新創並形成產業生態體系，該作法已成為全球津津樂道之標竿。本期特刊以色列篇章，則著重於其網路作戰人力養成過程，發現以色列是以「全政府模式」，循前進部署方式，自高中階段開始培養挑選網路作戰人才，而後備體系建立產業人才回部隊制度，更有助於交流新知與召募業界新血。這樣的職涯良性循環，成為以色列年輕學子積極爭取加入網路作戰部隊的誘因，或可提供我國相關部門作為後續制度變革參考。

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

軍文交織的美國網路防護體系

杜貞儀

網路安全與決策推演研究所

壹、前言

美國網路戰略目標，在於透過改變攻擊者行為、阻絕利益、強加成本建立重層網路嚇阻（Layered Cyber Deterrence），降低重大網路攻擊事件的頻率與嚴重程度，以及對美國國家力量及影響力的傷害。[1]作為少數具備攻勢能力的國家，以往對於美國網路戰略落實的關注，多半在於網路司令部（USCYBERCOM）的形成、整合及形成戰力，如何從前身——戰略司令部（USSTRATCOM）所屬的全球網路作戰聯合特遣部隊（Joint Task Force- Global Network Operation, JTF-GNO）及網戰聯合職能編組指揮部（Joint Functional Component Command- Network Warfare, JFCC-NW）合併，並進一步升格為獨立的單一司令部，較少著墨其軍文交織的面向。雖然美軍已將網路空間作戰（cyberspace operation）明確定義為攻勢網路作戰（Offensive Cyber Operation, OCO）、守勢網路作戰（Defensive Cyber Operation, DCO）以及國防部資訊網路維運（Department of Defense information network（DODIN）Operation）三部分。[2]但屬守勢作為的網路防護，過去較不受外界關注。

然而，隨著網路威脅樣態變化，網路司令部起初以因應伊斯蘭國恐怖攻擊的任務目標與內容，也需逐漸調整、轉向，以對未來的大國競爭做好準備。當美國情報體系指控俄羅斯在 2016 年美國選舉期間進行一系列的干預，試圖影響選舉結果時，美網路司令部在積極防護作

[1] Cyberspace Solarium Commission, “Cyberspace Solarium Report,” March 2020, https://www.solarium.gov/report.

[2] 網路空間任務定義出自“Joint Publication 3-12: Cyberspace Operation,” Joint Chief of Staff, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf。關於 JTF-GNO 於反恐任務的角色，請另參杜貞儀〈美國網路任務部隊目標標定與效益評估〉,《國防情勢月刊》第 152 期。

為的任務與角色，才逐漸為人所知。2018 年底美國土安全部下新設之網路與基礎設施安全局（Cyber and Infrastructure Security Agency, CISA）成立，整體網路防護體系勢必進行跨部會的整合。

尤其 2020 年底一系列的網路安全事件，更加凸顯跨部會以及公私協力的重要性。包括 SolarWinds 這樣極具針對性、本質上為接近國家層級間諜行為的供應鏈攻擊，以及微軟 Windows Exchange 遭駭事件中，國家行為者的輕率攻擊行徑，與作為關鍵基礎設施的「殖民管道」（Colonial Pipeline）公司遭勒索軟體攻擊，一系列事件的影響層面極廣，現有之美國政府網路防護體系顯得窮於應付。由網路司令部為主體、代表美國國防部及軍方在網路空間執行任務，以及負責境內安全的國土安全部及其網路與基礎設施安全局間，其各自在美國網路防護體系的角色與任務範圍是否須重新檢視，還有哪些可能的改善方向，也是後續檢討的重點。

本文將由美國網路安全體系的防護層面進行探討，並以其軍文交織的特色進行介紹，從中呈現軍方在境內網路防護任務能夠扮演的角色，以做為我國國家網路安全政策方向參考。

貳、美國網路安全體系建構

一、美國網路安全體系建構及網路司令部編制

美國政府的網路安全體系，起初由情報及執法機關組成，包括法務部所屬的聯邦調查局，以及國家安全局（National Security Agency, NSA）。依照 2006 年美《網路作戰之國家軍事戰略》（*National Military Strategy for Cyberspace Operations*）的定義，美軍在網路空間作戰的主要角色有三，分別是：保衛國家、國家級事件應變以及關鍵基礎設施防護。[3]而在網路司令部 2018 年升格為獨立的單一司令部時，與主掌訊

[3] "National Military Strategy for Cyberspace Operations (U)," Joint Chiefs of Staff, December 2006, https://www.hsdl.org/?%20abstract&did=35693. (Unclassified version with redacted)

號情報的國家安全局共享空間、人力與資源，形成「身兼雙職」（dual-hat）的架構，以此加速網路司令部發展，也展現出網路安全與情報密切相關的本質。

網路任務部隊（Cyber Mission Force, CMF）是網路司令部的直屬戰力，依 2012 年經參謀長聯席會議核可的編制，共有 133 支部隊，約 6200 名人員。各部隊依照其職掌與任務，共分為：網路防護隊（Cyber Protection Team）：負責國防部資訊網路（DODIN）防護並在遭到入侵時進行反應；國家任務隊（National Mission Team）負責偵測敵方網路活動、阻止攻擊並反擊；戰鬥任務隊 （Combat Mission Team）則是進行戰鬥網攻行動，以支援網路司令部及各作戰指揮部（Combatant Command）的優先任務；最後則是為國家及戰鬥任務隊提供任務分析與計畫支援的網路支援隊（Cyber Support Team）。[4]

目前網路司令部編制的 133 支網路任務部隊，分別編入直屬網路司令部的國防部資訊網路（Joint Force Headquarters- DOD Information Networks）聯合部隊指揮部、網路聯合部隊指揮部（Joint Force Headquarters- Cyber）、網路國家任務部隊指揮部（Cyber National Mission Force Headquarters）、與各軍種的網路指揮部及各區域作戰指揮部（見圖 1）。[5]其中陸軍常備役共有 41 支網路任務部隊，加上屬預備役之陸軍國民兵的 11 支網路防衛隊，以及陸軍後備役的另外 10 支網路防衛隊，使來自陸軍的網路任務部隊，成為美國網路戰力的最主要構成

[4] 關於美國網路司令部網路任務部隊如何藉由演訓驗證、形成戰力，請參考杜貞儀，〈美國網路任務部隊與訓練環境發展〉，《國防情勢月刊》第 146 期。

[5] "DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Forces," U.S. Government Accountability Office, March 6, 2019, https://www.gao.gov/assets/700/697268.pdf.

單位。[6]

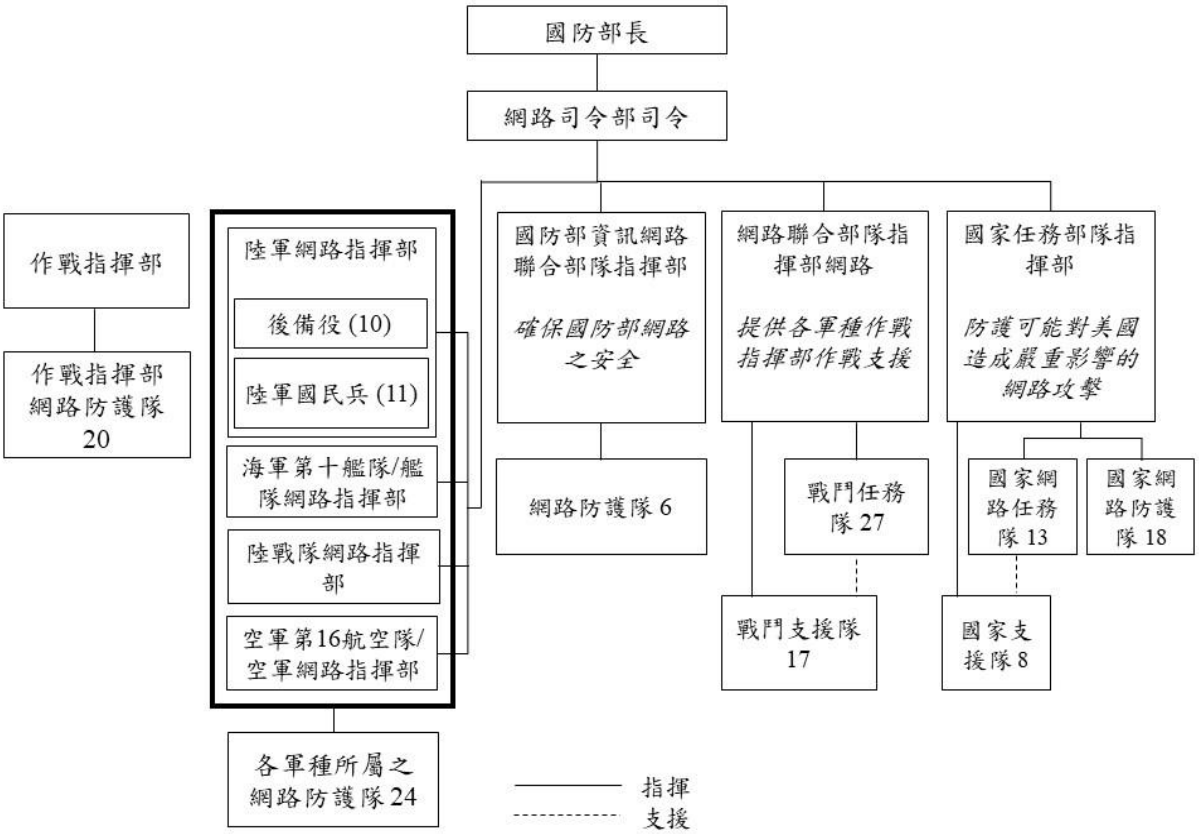


圖 1、美國網路司令部編制及網路任務部隊配屬

資料說明：單位/役別後數字表示所屬網路任務部隊數目，預備部隊之陸軍後備役、國民兵以括弧表示。

資料來源：作者翻譯自美課責審計署報告（見註 5），並參考 2019 年美國空軍第 16 航空隊（Sixteenth Air Force）復編之相關新聞更新單位名稱，見 “Sixteenth Air Force (Air Forces Cyber): Legacy 2021,” June 2021, https://www.16af.af.mil/Portals/80/16%20AF%20Legacy%202021%20(V20210607).pdf?ver=5v8vlCX5WM3PjV_4Pdsr3Q%3d%3d 。

二、國土防衛架構下的網路防護

雖然網路空間沒有明顯疆域，但為了明確定義網路作戰的範圍，美國防部在《聯戰準則 3-12：網路空間作戰》（*Joint Publication 3-12: Cyberspace Operation*）中，仍將網路空間劃分為藍、紅、灰三個部

[6] “DOD Fact Sheet: Cyber Mission Force,” U.S. Army Cyber Command, February 2020, https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/.

分。其中藍色代表美國、其任務夥伴或其他美國防部受命防護的區域。雖然美國防部的現行命令僅防護美國防部網路，但網路部隊亦須為接獲請求時，防護其他美國政府單位、或美國與盟國的關鍵基礎設施進行準備。紅色則是敵方所控制的網路空間，其餘不符合紅或藍兩者定義的區域，則列為「灰色」網路空間。[7]

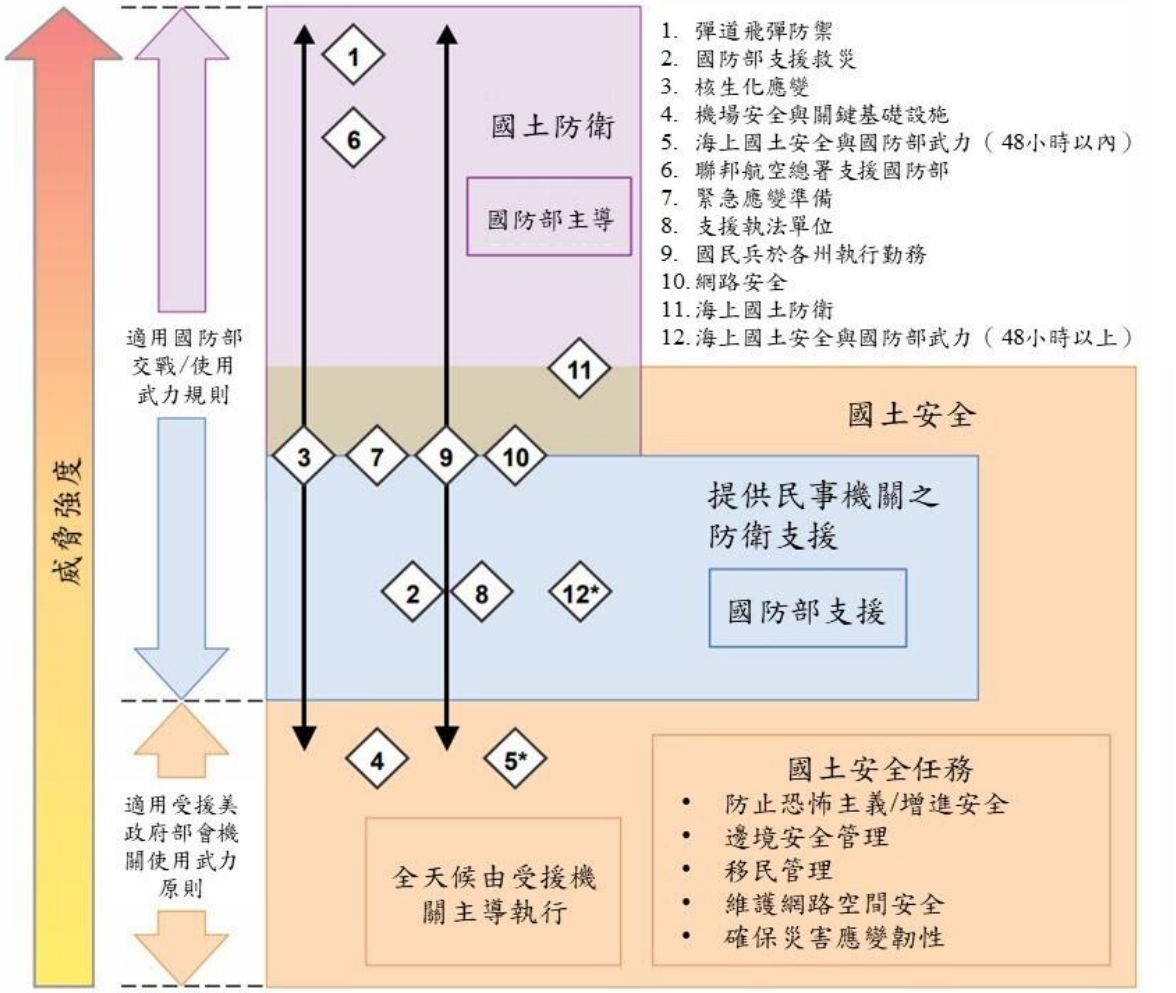


圖 2、美國土防衛、國土安全、提供民事機關之防衛支援間關聯圖

資料說明：網路安全為項目 10，威脅強度略同於緊急應變準備，並適用美國防部交戰/使用武力規則。

資料來源：翻譯自《聯戰準則 3-28：提供民事機關之防衛支援》(*Joint Publication 3-28: Defense Support to Civil Authorities*)

美國既有的國土防衛架構是基於核生化防護、彈道飛彈防禦及反恐等需求而建立的（圖 2），在此架構下，潛在威脅警示、干擾並且擊

[7] "Joint Publication 3-12: Cyberspace Operation," Joint Chief of Staff, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

退威脅以及保障任務完成（mission assurance）三個部分由國防部主導，而在提供民事機關之防衛支援（Defense Support to Civil Authorities, DSCA）中，國防部另外亦須就救災、執法、緊急應變準備等任務支援其他政府單位。[8] 就如美軍對由執法單位主導的緝毒行動（Counter Narcotics Operation）提供支援，美軍支援國內的網路防護工作，亦同樣以 DSCA 的架構為基礎。[9]

關鍵基礎設施安全則由美國土安全部統籌，並依照關鍵基礎設施特性進一步分為 16 類，各由不同的機關主管與協調。美國防部在關鍵基礎設施安全防護上，具有雙重角色，不僅是聯邦政府的一員，也是國防工業（Defense Industrial Base）關鍵基礎設施的協調機關（Sector-Specific Agencies, SSA）。作為聯邦政府的一員，美國防部在部會層級必須對國防關鍵基礎設施進行威脅辨識、排序、評估、復原及防護的工作，並與其他政府部會機關合作，保護所有關鍵基礎設施及資源。作為國防工業關鍵基礎設施的協調機關，除與公部門合作外，也需要與私部門進行協調。

參、挑戰與未來展望

一、網路防護跨部會合作的實例與挑戰

在網路司令部成立後，就關鍵基礎設施網路防護相關作為，對內分享事件應變情報，對外則持續接戰（Persistent Engagement），以對駭客團體強加攻擊成本的方式，嚇阻進一步攻勢，目前已有兩項公開實例。首先是針對 2020 年美國選舉，有 2016 年俄羅斯干預的前例在先，網路司令部與國家安全局共同成立選舉安全組（Election Security Group），並與聯邦調查局、CISA 進行交換情報。與國民兵的合作，則

[8] "Joint Publication 3-27: Homeland Defense," Joint Chief of Staff, April 18, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf.

[9] "Joint Publication 3-28: Defense Support to Civil Authorities," Joint Chief of Staff, October 29, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf.

設有仿照醫療後送資料的「資安 9 項」（Cyber 9-line），以結構化的方式擬定狀況回報格式，加速情報分享，讓各州國民兵部隊能夠取得網路司令部的情報並加以運用（圖 3），並在美國大選多州同時舉辦總統候選人初選的「超級星期二」（Super Tuesday）等關鍵時刻提供支援。

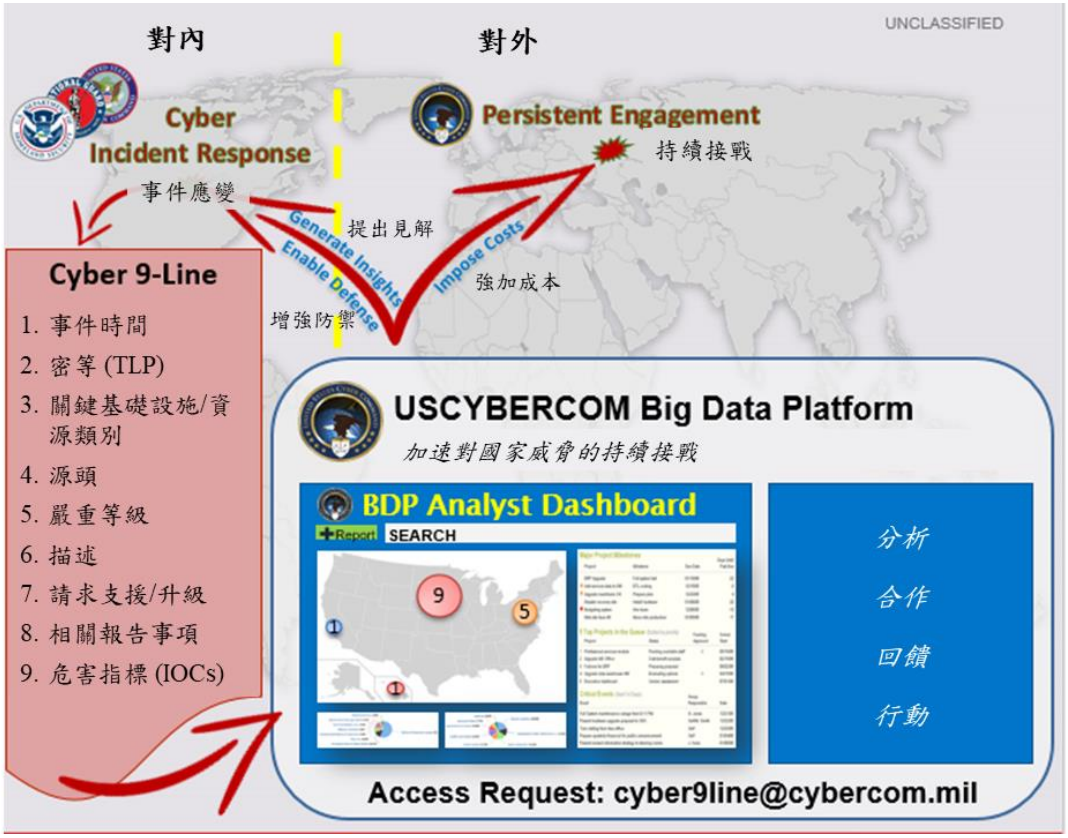


圖 3、「資安 9 項」與網路防護的內外分工

資料來源：美國網路司令部

在 2020 年的新冠肺炎疫情下，這樣的協作機制亦在網路防護上扮演極為重要的角色。由於預期駭客將試圖取得新冠肺炎疫苗開發資料，為支援美政府加速疫苗開發生產的「曲速行動」（Operation Warp Speed），美國土安全部的 CISA 藉由前節敘述之 DSCA 機制，請國民兵及陸軍後備役網路部隊提供醫藥產業之網路安全支援。這也顯示美軍在境內網路安全防護的角色，並不僅限於各級政府機關，在必要時，

協調機關亦能依照既有機制向美國防部提出申請，支援屬於私部門的關鍵基礎設施提供者。[10]

不過，美國防部與國土安全部在網路防護的合作關係，其實仍面臨挑戰。美國防部總督察長曾就十年來雙方合作的概況進行調查，發現美國防部與國土安全部雖然就網路安全合作簽有備忘錄，但並無依照備忘錄制定實施計畫。從幾項實例來看，既有機制似乎能夠運作，不過由於缺乏明確定義雙方角色、責任、里程碑以及完成日期的實施計畫，就保護國家關鍵基礎設施而言，雙方仍可能基於認知差異而影響整體合作。即便 2020 年影響許多聯邦政府部門以及私部門單位 2020 年的 SolarWinds 事件，與明文規定的合作實施計畫無關，本次事件也已彰顯國防部與國土安全部合作因應所有網路威脅時的重要性。若有更具體之規範作法，將能夠幫助雙方達成其維護網路安全的共同目標。[11]

二、建立聯合網路防禦協作機制並提供所需資源因應威脅

基於過往的合作經驗，CISA 依據《2021 財政年度國防授權法》（*National Defense Authorization Act of 2021*, NDAA）所賦予的權限，於 2021 年 8 月宣布成立聯合網路防禦協作機制（Joint Cyber Defense Collaborative, JCDC），以此匯集公私部門協力合作，以共同抵禦關鍵基礎設施的網路威脅，從而引領國家網路防禦計畫的制定。從公開資料中揭示 JCDC 的主要目的，在於藉由這項新的合作機制，協調跨聯邦部門、各州地方政府、民間或組織等合作夥伴，來識別、防禦、檢測和應對涉及國家利益或關鍵基礎設施的惡意網路攻擊，尤其是勒索軟

[10] Paul M. Nakasone, "Posture Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the 117th Congress Senate Armed Services Committee," United States Senate Committee On Armed Services, March 25, 2021, https://www.armed-services.senate.gov/download/nakasone_03-25-21.

[11] "Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations (DODIG-2021-100)," Department of Defense Office of Inspector General, July 12, 2021, https://www.dodig.mil/reports.html/Article/2691902/audit-of-the-department-of-defenses-implementation-of-the-memorandums-between-t/.

體，同時建立事件應變框架，進而提升國家整體資安防護和應變能力。

JCDC 辦公室將由美國土安全部、司法部、網路司令部、國家安全局、聯邦調查局及國家情報總監辦公室（Office of the Director of National Intelligence, ODNI）組成。另外，JCDC 將與自願參與的夥伴合作、協商，包括州、地方、部落和地區政府、資訊共享與分析組織和中心（ISAOs/ISACs），以及關鍵資訊系統的擁有者和營運商，以及其他如微軟、亞馬遜、谷歌等私部門之服務提供商。甫成立之 JCDC，是否能夠自過往合作經驗中學習，釐清各方認知差異、角色、以及責任，將會是後續觀察的重點。

然而，美國土安全部需請求國防部支援，可能也反映文職單位缺乏足夠資源因應威脅的普遍問題。以往大型災害緊急應變，美聯邦政府基於《斯塔福德災害救援和緊急援助法》（*Stafford Disaster Relief and Emergency Assistance Act*）有系統地對州和地方政府提供災難應變的援助，包括動用聯邦基金。需求單位亦可經由 DSCA 機制向國防部提出支援請求，國防部則依法向需求單位報支開銷。[12]此《斯塔福德法》是否適用於網路攻擊所造成的災害，或另設網路安全事件應變與復原基金支應，有待進一步釐清。[13]但基於此法精神，美國防部提供原先任務以外的額外支援，均屬於有償服務（on reimbursable basis）。

最後，網路安全的核心在於人才，美國軍方有其固定培育體系，但文職人員則無，因而由人工智慧國家安全委員會（National Security Commission of Artificial Intelligence, NSCAI）提出設立聯邦數位學院

[12] 如新冠肺炎疫情宣布緊急狀態後的相關支援經費報銷概況，美國防部總督察長辦公室已有初步審計報告公開，詳見 Department of Defense Office of Inspector General, "Audit of the Reimbursement for Department of Defense Mission Assignments for Coronavirus Disease–2019 Pandemic Response in the U.S. Northern Command Area of Responsibility (DODIG-2021-091)," June 11, 2021, https://www.dodig.mil/reports.html/Article/2654551/audit-of-the-reimbursement-for-department-of-defense-mission-assignments-for-co/。

[13] Matt Lyttle & Yvonne Manzo, "When Cyber-Attacks Lead to Disaster, Does Stafford Act Apply?" Infosecurity Magazine, September 3, 2021, https://www.infosecurity-magazine.com/opinions/cyber-attacks-disasters-stafford/.

（Federal Digital Service Academy） 的倡議，並得到國際國防通信電子協會（AFCEA International）的支持，希望能夠藉由設立專注於網路安全與人工智慧的文官學院，來培育聯邦政府的數位、網路相關文職人才。[14]不過，拜登政府目前的網路安全政策規劃中，尚未提及人才培育部分，此可能因疫情與其他更急迫之議題，而未有機會進一步討論，但此仍將會是對於解決人力短缺的選項之一。

肆、結語

從美國網路防護體系的發展以及實際案例，可看出建構如民事機關之防衛支援（Defense Support to Civil Authorities, DSCA）的具體機制，是軍方參與關鍵基礎設施網路安全防護的基礎條件，並明確界定主導者、參與角色以及分工。確立情報分享機制，則能更有效的促進橫向聯繫以及情報運用。然而即使美網路司令部，其主要任務仍是對外持續接戰，尤其威脅情報有價，進行資訊分享與交換並提供實質支援，均有其成本，只有互利互惠的機制才能持續運作。對於與日俱增的網路安全威脅，無論災害緊急應變《斯塔福德法》未來是否涵蓋網路攻擊所造成的災害，或另設基金支應，美國拜登政府於建立聯合網路防禦協作機制、提供各級政府應變資源依據並強化政府相關人才培育的動向，仍值得持續觀察。

本文作者杜貞儀為國立臺灣大學海洋所理學博士，現為財團法人國防安全研究院網路安全與決策推演研究所助理研究員。

[14] AFCEA International, “Establishing a Federal Digital Service Academy,” *SIGNAL Magazine*, April 2021, https://www.afcea.org/signal/resources/linkreq.cfm?id=349.

The interwoven US civil-military cyber protection system

Chen-Yi Tu

Assistant Research Fellow

Abstract

The objectives of US cyber strategy is to establish Layered Cyber Deterrence through shaping behavior, denying benefits and imposing costs to reduce the frequency of severe cyber attacks and their damages to US national power and influence. Previous study on the implementation of US cyber strategy usually focused on the formation, integration, and achieving operational capabilities of the United States Cyber Command. The defensive cyber operation, however, receives relatively less attention. Civil-military interweaving is one of the major characteristics of the US cyber defense. Within the current homeland defense framework, the US Department of Defense supports other government units for disaster response, law enforcement and other missions through mechanism of Defense Support to Civil Authorities (DSCA). The US military also supports domestic cyber defense with the same mechanism. Some existing examples of such supports are election security and COVID-19 vaccine development, both span across the public and private sectors. Therefore, building a mechanism such as the DSCA is fundamental for military participation in the cyber defense of critical infrastructure. Moreover, establishing an intelligence sharing mechanism can further enhance the lateral communication and effective use of intelligence.

Keywords: cyber defense, homeland defense, critical infrastructure, whole-of-government approach

英國的協作式網路戰力建構

吳宗翰

網路安全與決策推演研究所

壹、前言

國家與非國家行為者透過網路途徑從事攻擊行為（cyber attack），已經構成國家安全課題的重大挑戰。面對網攻手法不斷推陳出新且日益複雜化，各國政府建構網路防禦力量時，可參考他國經驗協助自身從事相關變革。

本文專篇介紹英國網路戰力概況。在這裡，網路戰力被視為是一國政府應對網路攻擊的總體反應能力。[1]它包含該國的網路空間戰略觀、處置挑戰的原則、資源配置方式以及單位之間的互動機制關係等。首先指出，英國的問題意識與改革動力至少來自兩個脈絡，一者源自與盟邦美國長期互動得到的啟發；一者來自脫歐（Brexit）以降英國反思自身在全球位置所做的戰略性調整作為。這兩種脈絡共同促成目前的協作式（collaborative）框架。

本文結構安排如下。首先陳述英國的網路防禦戰略概念，指出其並不止於被動回應，反之，主動出擊亦構成其反制潛在敵人的立論。接著介紹隸屬於國家通訊情報總局（Government Communications Headquarters, GCHQ）的國家網路安全中心（National Cyber Security Centre, NCSC）以及主要由情報部門、國防部門合作成立的國家網路部隊（National Cyber Force, NCF）。二者各自側重守勢與攻勢兩種立足點，亦可視為處理對內部挑戰與對外部挑戰之分。本文最後於小結處

[1] 網路戰力的概念可取自網路能力（cyber capabilities/cyber power），後者目前尚無一統一的標準。筆者參考國際戰略研究所（International Institute for Strategic Studies, IISS）以及哈佛大學甘迺迪學院貝爾弗科學與國際事務研究中心（Belfer Center for Science and International Affairs, Harvard Kennedy School）的相關指標，英國在其研究中全球排名分別列屬於第二等級（與中俄以色列等同級）或第三強（位居美、中之後）。見 Cyber Capabilities and National Power: A Net Assessment, IISS, June 28, 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power; Julia Voo et al., National Cyber Power Index 2020, Belfer Center for Science and International Affairs (Cambridge: Harvard Kennedy School, 2020)。

試論英國發展經驗對台灣的可能啟發。

貳、英國網路防禦戰略觀：主動防禦

英國在網路戰略的論述與能力建構受到盟邦美國極大的影響而有諸多相通之處。雙方在大方向上均採取「主動防禦」（active defense）的概念，甚至刻意強調自身所擁有的「進攻」（offensive）能力。這顯示出，英國網路防禦的重點並非僅著重在被動式的防護攻擊，同時還要能採取措施主動（proactive）阻斷潛在敵手的進犯，先發制人式（pre-emptive）地保護英國網路空間。基於此，透過各類型的建設完善自身在網路空間的韌性更是重要關鍵。[2]此外，由於潛在敵手造成的威脅可能會隨時間推移而有變化，因而在不同階段，反制措施也會有所差異。

不過，相較於美國，英國政府在其整體網路戰略中國家的角色更為吃重，是採取全政府/國家（whole-of-government/whole-of-nation）途徑。2009 年英國政府在其《英國的網路安全戰略》（*Cyber Security Strategy of the United Kingdom*）中即揭示了它將採取中心化的途徑規劃相關能力發展，並整合公、私部門，使其能一體化應對網路威脅。在之後的2011年以及2016年個別發布的《網路安全戰略》（*Cyber Security Strategy*）、《國家網路安全戰略》（*National Cyber Security Strategy 2016-2021*）中，這個思維始終維持一貫，並獲得進一步發展。總體言之，英國力圖在「防衛敵人的攻擊」、「遏制敵人將英國視為目標」，以及「不斷創新與發展技術以領先對手」領域各有進展。這幾個核心目標雖看似有別，實際上相輔相成。[3]

---

[2] Alessandro Marrone and Ester Sabatino, "Cyber Defense in NATO Countries: Comparing Models," Istituto Affari Internazionali, 2021.

[3] UK Office of Cyber Security and UK Cyber Security Operations Centre, Cyber Security Strategy of the United Kingdom (London: Cabinet Office, June 2009)；Cyber Security Strategy, GOV.UK. November 25, 2011, https://www.gov.uk/government/publications/cyber-security-strategy; National Cyber Security Strategy 2016 to 2021, GOV.UK, November 1, 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

為持續達到這些目標，英國投入可觀的資源從事研發、整合、創新，運用靈活政策逐步建構英國的網路戰力，包括設立相關網路計畫、網路中心甚至成立新部隊等；另一方面，為了追求能持續維持相對的優勢，英國也著重與盟邦共享情報，並透過與盟邦合作，而共同在國際場域發揮影響力，以維護其共同國家利益。

脫歐以來，英國亟欲擺脫長年的「歐洲的英國」框架，因而提出「全球的英國」（Global Britain）路線。2021 年 3 月底英國提出《競爭時代下的全球英國：安全、國防，發展與外交政策總評估》（*Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*）。該文件除了盤點未來可能面臨之國安挑戰外，在網路領域亦指出，基於國安需求，發展進攻網路能力勢在必行。同時間，由英國下議院發布的《2021 整合檢討：崛起的國防科技》（*Integrated Review 2021: Emerging Defence Technologies*）中，英國也聲稱要做一「負責任的民主網路強國，並能夠過網路空間保障英國的利益」，矢言持續在各方面競爭條件下領先對手。[4]這些文件共同顯示主動防禦必未隨脫歐而有所更迭，在脫歐後，仍是英國之網路防禦戰略觀與發展重心。

參、國家網路安全中心：防衛關鍵基礎設施

國家網路安全中心為英國國家通訊情報總局下轄之單位。它設立於 2016 年 10 月，是英國《國家網路安全戰略 2016-2021》計畫中的重點項目之一。中心前身包括國家通訊情報總局的資訊安全小組、網路評估中心（Centre for Cyber Assessment, CCA）、電腦網路危機處理中心（Computer Emergency Response Team, CERT-UK）、國家基礎設施保護中心（Centre for the Protection of National Infrastructure, CPNI）的網路部

[4] "The Integrated Review 2021," GOV.UK, March 16, 2021, https://reurl.cc/L7mqqx; Danny Steed, The UK's Integrated Review and the future of cyber, clcano, July 1, 2021, https://reurl.cc/jg1oo2; Claire Mills, *Integrated Review 2021: Emerging Defence Technologies* (London: House of Commons, March 25, 2021).

門等單位整併而來，編制雇員至 2021 年預計約有 950 人。[5]

儘管實際上國家網路安全中心同時具備攻、守能力，[6]防守性的（defensive）防禦才是該中心的核心要務。中心主要負責監控政府與民間部門的網際網路與通訊系統安全，特別是「關鍵基礎設施」（critical infrastructure）部分，這點對於英國正在進行中的智慧城市建構尤為重要。[7]中心並負責協調「跨政府部門」與「政府—民間」的網路安全工作，這其中包括提供應對網路安全事件的措施指南。

從範圍看來，國家網路安全中心幾乎主責全英國境內，連結產業、政府、學術、法律施行者、軍事部門以及整體社會，主旨在「幫助英國成為最安全的安居樂業之處」（Helping to make the UK the safest place to live and do business online）。

國家網路中心還設有「網路安全資訊分享平台」（Cyber Security Information Sharing Partnership, CiSP）提供平台使用者分享網路安全情資。[8]所謂的網路安全事件，包括社交工程（social engineering）、釣魚攻擊（phishing）、進階持續性威脅（advanced persistent threat, APT）、勒索病毒攻擊（ransomware attack）等。國家網路中心也會不定期發布相關報告，揭露資安事件（可能）攻擊來源、攻擊手法等訊息。來自國家級（state-sponsored）的網路攻擊與駭客的行動，特別是來自中、俄的行動，更是受其嚴密監視。[9]

此外，國家網路中心也會參與其他國內外單位聯防，交換並提供重要情報。這些單位包括國防部、北約組織（NATO）以及五眼聯盟

[5] "About the NCSC," National Cyber Security Centre, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do; National Audit Office, Progress of the 2016–2021 National Cyber Security Programme (London: National Audit Office, 2019), p. 39.

[6] Reuters Staff, "Britain's GCHQ to wage cyber war on anti-vaccine propaganda - The Times," *Reuters*, November 9, 2020. https://www.reuters.com/article/uk-britain-security-gchq-cyber-idUKKBN27O0XP.

[7] Umberto Bacchi, "Watch out for hackers, Britain's spy agency tells smart cities," *Reuters*, May 7, 2021, https://www.reuters.com/article/us-britain-tech-city-idUSKBN2CO1E3.

[8] CiSP, National Cyber Security Centre, https://www.ncsc.gov.uk/section/keep-up-to-date/cisp.

[9] Reuters Staff, "Watch out for Russia and China, UK's cyber security boss says," *Reuters*, March 26, 2021, https://www.reuters.com/article/us-britain-security-cyber-idUSKBN2BI24L.

（Five Eyes，FVEY）等。

肆、國家網路部隊：「軍事與情報」的整合

在 2020 年 11 月 19 日，英國國防部、國家網路中心與情報部門軍情 6 處（MI6）共同成立國家網路部隊，派令後者從事網路行動。國家網路部隊的職責在於支援英國在外交、經濟、政治與軍事方面的行動，也包括打擊與防範對兒童的犯罪等。與網路中心以防禦為中心的立場不同，英國國家網路部隊實際上針對的主要對象有三，即所謂敵對勢力、恐怖組織團體、駭客與高度組織化的網路犯罪等涉有國安威脅疑慮者，並主要採取攻擊姿態，高調宣示其「駭侵能力」（offensive hacking capabilities）。而其中設定的假想敵對團體與國家，不諱言就是伊斯蘭國與中、俄。[10]

從人員組成來看，國家網路部隊的組成甚為複雜。除了最初的設立組織國防部、國家網路中心與情報部門軍情 6 處外，國防科學技術實驗室（Defence Science and Technology Laboratory, Dstl）亦有參與。事實上，英國政府正是希望透過其人員組成來源如此多元的方式，促進單位之間的互動，獲得刺激並能將成果回饋給各單位。這些不同機構的人員，預期為國家網路部隊分別帶來不同優勢。譬如國防部能提供軍事作戰知識、國家通訊情報總局能提供其單位的全球情報能力、軍情處能提供特工人員與相關技術、國防科學技術實驗室則能貢獻其研發等。這種納多重單位於一體的做法，與中國戰略支援部隊看似有可比擬之處；但實際上英國的整合幅度更大，已經跳脫單一部門下次級單位間的橫向聯繫。

國家網路部隊的成立對英國而言，不啻是一個里程碑，其意涵顯

[10] National Cyber Force transforms country's cyber capabilities to protect the UK, GCHQ, November 19, 2020, https://www.gchq.gov.uk/news/national-cyber-force; Dan Sabbagh, "UK unveils National Cyber Force of hackers to target foes digitally," *The Guardian*, November 19, 2020, https://www.theguardian.com/technology/2020/nov/19/uk-unveils-national-cyber-force-of-hackers-to-target-foes-digitally; Matt Burgess, "The UK created a secretive, elite hacking force. Here's what it does," WIRED, November 28, 2020, https://www.wired.co.uk/article/national-cyber-force-uk-defence-gchq.

示其終於設計出一個「軍事—情報夥伴關係」的包容性框架，而得以將長期各自分散發展的網路安全專業人員整合起來。可以想見，其與現存的各類網路安全單位，特別是國家網路安全中心，預期將存在高度協力的合作關係；與政府涉及通訊（communications）的部分也都有一定程度的聯繫。此外，政府對於國家網路部隊的定位也會動態性的影響這些合作關係。

從時程言，國家網路部隊的成立，意味著英國意識到過去的機制已不足以應付數位資訊時代下網攻構成的巨大安全挑戰，而須更全面性地整合資源因應。近年來，英國國內面臨遽增的網路犯罪，以及伊斯蘭國、極端主義的興起，歐盟之間的脫歐議題，乃至「全球的英國」路線的實踐，國際之間大國競爭，加之 2019 年底以降爆發的全球新冠肺炎（COVID-19）疫情，在在迫使唐寧街不得不進行更深刻的改革。與此同時，長年的經濟停滯不前，也使得政府在這個過程中，僅能選擇性的投入相對多的資源。在多方面評估後，網路能力顯然是一重要且涵蓋多領域的項目，是以英國政府由此著手。

綜合相關研究，國家網路部隊脫胎自 2014 年創立的「國家進攻網路計畫」（national offensive cyber programme, NOCP）；當時，由於 2018 年爆發俄國以神經毒劑襲擊前俄國特工的「索爾茲柏里事件」（Salisbury Incident），英國政府意識到敵對潛在敵意國家造成的威脅，而擴大計畫，將當時成員編制由 500 名提升至 2,000 名。2020 年 11 月 19 日，當英國首相強生（Boris Johnson）對外宣布將大幅提高英國的國防預算與成立國家網路部隊時，他表示目標人數預計再於 2030 年調高至 3,000 員。[11]

[11] "UK has mounted covert attacks against Russian leadership, says ex-mandarin," *The Guardian*, October 24, 2020, https://www.theguardian.com/technology/2020/oct/24/uk-has-mounted-covert-attacks-against-russian-leadership-says-ex-mandarin; Helen Warrell, "National Cyber Force will target UK adversaries online," *Financial Times*, November 20, 2020, https://www.ft.com/content/a41b34e7-a8fc-4bce-92e4-508cd1c83ba9.

如前述提到，國家網路部隊主要擔任進攻型角色。不過，這並不意味部隊可以恣意發動攻勢，反之，它的行為仍然服膺於國際法與國際規範；換言之，其行動「須合法、符合國際規範且合乎比例的」（legal, ethical and proportionate）。此外，部隊對外行動也會與英國政府同美國、五眼聯盟、北約的合作關係一致，除例常性的情報與人員交流外，必要時預料也將參與共同行動。

由於成立至今不久，加之高度服膺仍在發展中的「全球的英國」路線，有關英國國家網路部隊的資訊仍然十分有限，該部隊從組織到任務也可能充滿變動性。惟從一個大架構而言，可以區分出它與國家網路中心的差異在於外、內之別，前者更偏向具有軍事打擊色彩，而後者則比較類似處理網路事件的警察。當然這只是一種粗略的類比，並不完全能做角色職責上的精細對照。

儘管如此，2021 年 4 月英國智庫單位亨利・傑克遜協會（Henry Jackson Society）研究員撰文指出，英國國家網路部隊在法律、職權、戰略等面向存在不少疑問，這些有賴後續解決。同月，一份由英國倫敦大學國王學院出版的報告也表達了類似看法。報告指出，政府需要盡快釐清國家網路部隊的定位，從角色與職責訂立相關優先順序，以免失去組織焦點。該報告也指出，即便政府所謂的 2030 目標達成，使部隊人數達 3,000 人，但比起許多網路軍事大國，其規模並沒有過人之處；例如，比起美國網路指揮部的編制，2030 的目標僅有前者的一半。報告同時提供建議，有關國家網路部隊的總體戰略發展應放置在英國打造結合常備役、後備役與民間力量一體的「全軍」（Whole Force）構想脈絡中。[12]

[12] Danny Steed, The National Cyber Force: directions and implications for the UK, REALINSTITUTOELCANO, April 18, 2021, http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/cybersecurity/ari18-2021-steed-the-national-cyber-force-directions-and-implications-for-the-uk; Joe Devanny, Andrew Dwyer, Amy Ertan, and Tim Stevens, *The National Cyber Force that Britain Needs?* (London: King's College London, April 2021).

伍、小結

本文透過對相關報告與部隊組織單位的爬梳，勾勒出英國網路戰力的基本樣貌。粗略而言，英國的情報部門—國家通訊情報總局下轄的國家網路安全中心，以及由情報與國防單位綜合而成的國家網路部隊，共同構成英國網路戰力的砥柱。儘管看似在組織與功能有所重疊，但其實這些單位有其各自核心執掌與側重要點，例如國家網路中心專注關鍵基礎設施與資安事件防護；國家網路部隊應付敵國、恐怖主義、組織犯罪等。在不同層面，這些單位可跨單位支援協助。總體言之，這種以政府為中心，而又富極具彈性、看似分散而又彼此聯繫的協作式網絡（network），正是英國網戰單位的特色。

本文認為，英國數量適中而質精的網路戰力，相當適切當前台灣發展目標。英國建構網路戰力的經驗可提供台灣借鑑。從人數編制而言，英國國家網路部隊的 3,000 員編制，尚少於我國資通電軍的 7,000 員，然而其組成的多元性與複雜性更勝後者。英國如何在戰略層面上，打造全國家一體的網路防禦能力，並具體落實到跨情報、軍隊部門的合作，以及進一步達到公、私部門的協力整合，值得相關單位研議參考效法。

近來，網路安全人才的養成教育與後備引發關注，英國在相關事務作為亦可借鑑。例如，其在國防科學院下設有「網路安全學校」（Defense Cyber School），提供國防部官兵以及其他政府單位公務員，從實務到中高階理論的多樣化課程，並肩負提供國防部上校級人員相關進修學程，[13]顯現出主事者已將網路視為高階幹部的必備技能。另外，為因應崛起的網路戰事威脅，英國政府另也在戰略司令部（Strategic Command）下，成立聯合網路後備部隊（Joint Cyber Reserve Force），由來自陸、海、空軍中的現役與後備軍人，以及沒有軍事經驗

[13] About the Defence Cyber School, Defence Academy of the United Kingdom, https://www.da.mod.uk/colleges-and-schools/technology-school/defence-cyber-school/.

的平民所組成。透過每年固定召集並訓練這群具備資通訊技術的專家，政府也可在必要時動員補充戰力。[14]這些經驗對於我國，應有一定啟示作用。

本文作者吳宗翰為英國倫敦大學國王學院博士，現為財團法人國防安全研究院網路安全與決策推演所助理研究員。

[14] "Working for UKStratCom," GOV.UK, https://www.gov.uk/government/organisations/strategic-command/about/recruitment；有關網路後備部隊的討論可參考杜貞儀，〈網路後備部隊的可能性與限制〉，《國防情勢特刊》，第 5 期（2020 年 9 月），頁 27-35。

Building UK's Cyber Defense Capabilities Using A Collaborative Network Framework

Tsung Han Wu

Assistant Research Fellow

Abstract

Cyberwarfare launched by state and non-state actors is a severe national security challenge for governments in the world today. To deal with cyber attacks in which tools evolve rapid and yet complicated, governments make various efforts on national and international levels for cyber defense. Learning from others to improve self-performance is also necessary.

This short essay analyzes the cyber defense capabilities of the UK. The author first introduces the cyber defense strategic concept that the UK holds, suggesting that it does not take a passive posture, rather, it has a proactive and preemptive stance. The author then describes the cyber defense units and forces following the aspects of intelligence, military and those that combine both. To be specific, the UK National Cyber Security Centre, as well as the National Cyber Force, are individually examined. Together, they form a web-like defensive framework. The author summarizes the UK models and experiences and then offers clues as recommendations for those interested in considering appropriate ways of improvement in the Taiwan context.

Keywords: UK Cyber Defense Capabilities, UK Cyber Strategy, UK National Cyber Security Centre, UK National Cyber Force

平戰結合的以色列網路作戰部隊

曾怡碩、洪嘉齡

網路安全與決策推演研究所

壹、前言

以色列在網路作戰上的戰力頗負盛名，也自豪宣示列入全球前五強；歷史上第一例實際運用的網路武器 Stuxnet 蠕蟲，就是由以色列與美國國安局共同研發運用。[1]在敵意環伺的威脅處境下，人口僅9百餘萬的以色列，可以運用網路作戰形成不對稱作戰利器。然而，數位資訊時代資訊安全威脅高漲的情勢，資安產業需才孔急的壓力，網路作戰單位難以進用及留用網戰人才，儼然已形成窒礙。對此，以色列的作法往往成為效法的範例。究竟以色列在網路作戰部隊任務、組成，有何特質，以及其人員選用、訓練、流動，如何結合資安產業發展，以下將接續分析，並提出可供我國借鏡之處。

貳、以色列網路安全戰略特質

一、網路安全戰略

以色列的安全戰略，深受其建國第一任總理本古里安（Ben-Gurion）影響，強調靈活應變之彈性，通常不太對外公開其國家安全戰略或軍事準則。循此，2017 年由國家網路局（INCD）公布的《國家網路安全戰略》，倡議採取威懾和反擊手段阻絕網路威脅，並精進網路防禦韌性，但對於施行細則，則迄今未對外公開。整體而言，以色列國家網路戰略有三層次，不同程度地體現了本古里安所強調之嚇阻、決定性勝利、早期預警、國際結盟原則——加強網

[1] Elena Chachko, "Persistent Aggrandizement? Israel's Cyber Defense Architecture," *Hoover Institution Aegis Series Paper* (No. 2002), August 26, 2020, pp. 7-8, https://www.hoover.org/research/persistent-aggrandizement-israels-cyber-defense-architecture. Also see Sean Cordey, "The Israeli Unit 8200 – An OSINT-based study Trend Analysis," *ETH Zürich CSS Report*, December 31, 2019, p. 10, https://doi.org/10.3929/ethz-b-000389135.

路防禦日常威脅的強度、透過國際合作培養系統性網路韌性、增強民間全國性網路防禦以減緩嚴重網路威脅的傷害。在網路防禦組織層級上，確定國家網路局（Israel National Cyber Directorate, INCD）於平時總責督導角色，並負責與軍情部門之協調。軍方（Israeli Defense Forces, IDF）則於緊急事件時整合攻勢與守勢作為。此外，政府透過教育與產業發展，增進網路安全防禦能力。[2]

二、對外主動防禦

現今美軍網路部隊所遵奉的前進部署（defending forward），其實早為以色列網路作戰單位奉為圭臬，只是名義轉為網路主動防禦（active defense），[3]在強鄰環伺之下，積極進行情報蒐集研判與敵後破壞。[4]網路作戰可遂行滲透竊聽與癱瘓攻擊，因此不僅情報單位如莫薩德（Mossad）、辛貝特（Shin Bet）都建置網戰單位，90%的情資及情報活動更是透過軍方的8200網戰部隊（Unit 8200）取得。[5]在情報早期預警功能之外，透過網路滲透部署以色列自身研發的網路病毒，更是以色列網路作戰藉境外先制攻擊，進而達到威懾嚇阻效果的重要手段。[6]

三、對內持久交戰

以色列雖為民主多元國家，面對境內巴勒斯坦族裔、阿拉伯移工以及哈瑪斯等組織的可能威脅，對於國內安全採持久交戰（persistent engagement）原則，[7]持續監控對境內高價值目標之網路威脅。尤其對於網路攻擊關鍵基礎設施，更是絲毫不能鬆懈，國家

[2] Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture," *ETH Zürich Cyberdefense Report*, September 2020, p. 5, https://css.ethz.ch/en/services/digital-library/publications/publication.html/e7ad9067-e6f9-422d-a633-5665b9327ba3.
[3] Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture," *ibid.*, p. 16.
[4] Sean Cordey, "The Israeli Unit 8200 – An OSINT-based study Trend Analysis," *ibid.*, p. 9, p. 13.
[5] Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture," *ibid.*, p. 16.
[6] Sean Cordey, "The Israeli Unit 8200 – An OSINT-based study Trend Analysis," *ibid.*, p. 9, p. 13.
[7] Elena Chachko, "Persistent Aggrandizement? Israel's Cyber Defense Architecture," *ibid.*, p. 1.

網路局透過民營業者威脅情資分享，情報組織辛貝特則透過通訊設施對於可疑分子的跟監，而軍方電腦勤務局的 C4I 部隊負責國內關鍵基礎設施防護，也會協同辛貝特，對國內進行監控。[8]

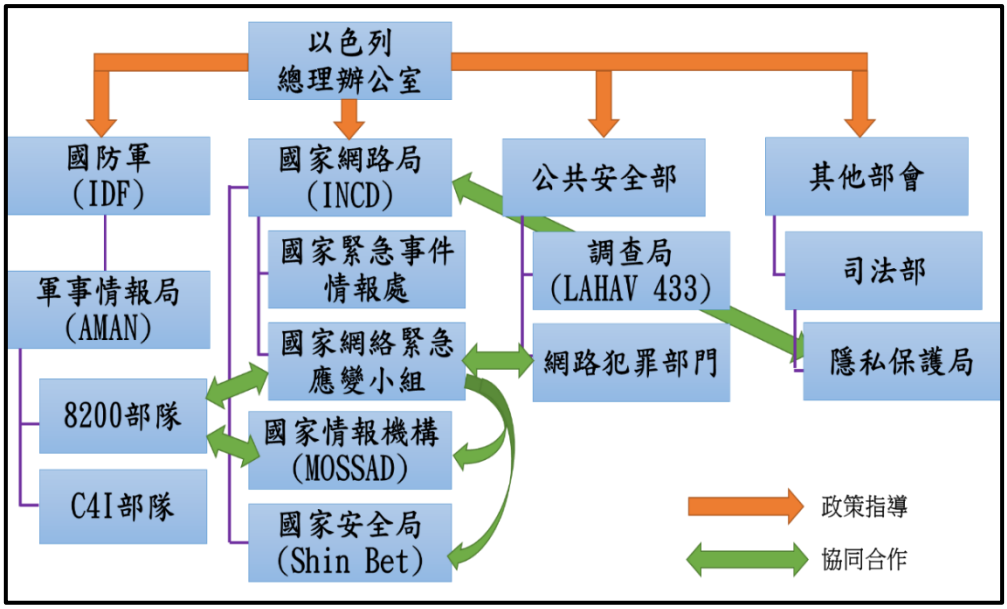
然而，這樣的對內安全作為均集中於總理辦公室掌握，由軍方與情治單位結合民間企業，對包括平民百姓進行網路監控，隨時可能遭濫用於對政敵進行監控。過去曾提出的網路安全法規，並未對此有所改善，反而提議將蒐集到的個資交由網路情報單位處理。2021 年提出的新版網路安全法案，則將個資改為聯繫細節，其餘仍交由總理辦公室權衡後授權監控，事後提請法官授權即可，制衡力道相當薄弱，持續引發公民團體質疑，此法恐將傷害民主治理。[9]

參、以色列網戰部隊組成、選訓與戰力運用

一、組成

以色列在網路作戰層面形成了以總理辦公室為主的結構，國家網路局與莫薩德、辛貝特同樣直屬總理辦公室(如下圖)。國家網路局負責國家網路空間保衛，建立和推進國家網路能量創新發展，下設資訊安全局（INCB）和網路管理局（NCSA）兩大核心機構。資訊安全局（INCB）負責制定國家網路法規、推進國際合作，同時保障國內關鍵基礎設施和產業的網路安全；網路管理局（NCSA）負責民事領域網路防禦事宜，設有國家網路緊急應變小組（CERT-IL）負責國家網路安全事件管理、情報共享等，是以色列民間部門負責資訊安全和網路事務的主要單位。[10]

[8] Jasper Frei, “Israel’s National Cybersecurity and Cyberdefense Posture,” *ibid.*, pp. 15-16.
[9] Elena Chachko, “Persistent Aggrandizement? Israel’s Cyber Defense Architecture,” *ibid.*, pp. 5-7.
[10] Jasper Frei, “Israel’s National Cybersecurity and Cyberdefense Posture,” *ibid.*, pp. 14-15.



圖、以色列網路組織架構

資料來源：Jasper Frei, Israel's National Cybersecurity and Cyberdefense Posture, *ETH Zürich Cyberdefense Report*, September 2020, p. 14.

情報單位中，國家安全局（ISA），又名辛貝特，負責保護政府網路系統、國家基礎設施訊息系統及金融資料等。下設國家情報安全局（NISA），負責管理國家互聯網基礎設施，制定網路安全目標、實施計劃等。辛貝特過去統管國家基礎設施，與國家網路局一番周旋之後，讓出大部分國家基礎設施保護職責，但仍保有關鍵資通訊基礎設施保護的功能，據此具備國內網路監控的情報能量。[11]

以色列國防軍持續推動網路作戰能量發展，2017 年，以色列國防軍（IDF）整合軍事情報局中的 8200 部隊和 C4I 部隊等機構。連同其他網路部隊，詳見下表。

[11] Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture," *ibid.*, p.15.

表、以色列網路戰部隊

部隊名稱	任務與職掌
8200 部隊[12]	以色列國防軍的信號情報蒐集單位，主責網路攻擊任務。
C4I 部隊[13]	負責以色列國防軍內部的網絡安全，以及為軍方開發資通訊基礎設施、軟體和密碼基礎。
指管通訊部隊	負責以色列國防軍內部 C4ISR 傳輸及防護等工作。 Mamram[14]：負責開發支持所有軍隊運作的 IT 基礎設施，發展適合各種武器需求的應用技術，並為軍隊提供網路防護服務。 Hoshen[15]：負責管理國防軍的通信指管系統。 Matzov[16]：為以色列加密及網路安全技術最高權威單位，提供政府網路攻防情資及網路安全技術服務。

資料來源：作者整理自公開資料，詳見註解 12-16。

二、選測、訓練與運用

（一）提前選測

以 8200 部隊為例，該部隊現役人數據稱達 5,000 員，退役人數列為機密。現役服役年數比一般以色列國防軍多達 1 至 4 年，意謂每年約 25%為選用之新血。網路作戰部隊有計畫性針對高中進行選測召募，學生進行篩選之後，再進行舉薦。經過推舉的 17 歲男女，要先通過第一階段的心理測試、體檢與學歷審核，之後進行第二階

[12] "Repression Diplomacy:The Israeli Cyber Industry," *Who Profits*, June 2021, p. 2, https://whoprofits.org/wp-content/uploads/2021/06/Repression-Diplomacy.-The-Israeli-Cyber-Industry.-June-2021.pdf.

[13] "Repression Diplomacy:The Israeli Cyber Industry," *ibid.*, p.2.

[14] Alon Braun,"The Secret Unit Behind Israel's Startup Nation Success," *Entrepreneur*, November 24, 2021, https://www.entrepreneur.com/article/359047.

[15] "Battleground of the Future: Inside the Unit that Connects the IDF," Israel IDF, May 19, 2014, https://www.idf.il/en/minisites/technology-and-innovation/battleground-of-the-future-inside-the-unit-that-connects-the-idf/.

[16] James A. Lewis and Katrina Timlin,"Cybersecurity and Cyberwarfare," The United Nations Institute for Disarmament Research, 2011, p. 14, https://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

段長達半天的面試，並特地由 8200 部隊年輕成員進行面試，由於這些年輕成員具有高度動機主動找到合宜接替人員，故咸信此舉將有利於挑選出高素質新血。最後一輪測試，目的在於衡量包括數學、加密、語言等知識及好奇心、決心、分析思考、領導技巧、團隊合作、迅速適應力、跳出思考窠臼、快速學習力等特質。[17]

（二）部隊訓練

一旦通過選測而成為 8200 部隊新血，就要在 Glilot Junction 軍事基地經歷至少 6 個月、每天長達 12 至 18 小時，從清晨到深夜的網路作戰技術性訓練，研習電子工程、加解密、通訊以及阿拉伯語、情報分析、信號情報、資料挖礦，再加上高壓訓練模擬。負責訓練的教導員為年長幾歲的年輕成員，視情況調整教學方式，教導未來工作上所需之專業品質與技巧。教導員擷取結業所要求的競爭力及責任，結合技術與情報問題，讓新血發揮創意——例如建構軟體將敵方加密訊息予以破解，並於研析訊息內容後，提出可行行動方案。結訓之後，新血分發至 8200 部隊裡的不同單位，職責雖不盡同，但各自任務本質維持不變。[18]

（三）戰力運用

無論是 8200 部隊、C4I 部隊，還是莫薩德、辛貝特等情報組織的網路作戰單位，其網路作戰的主要目的，就是在協助以色列軍方的實體空間作戰。[19]2007 年以色列網戰部隊以網路攻擊配合電戰部隊，癱瘓敘利亞俄製對空雷達，有效支援以色列戰機空襲敘利亞核設施，即為知名代表作。[20]以色列國防安全所強調的彈性以及威懾，也充分體現在以色列軍方結合實體與網路虛擬空間的作戰環境。

---

[17] Sean Cordey, “The Israeli Unit 8200 – An OSINT-based study Trend Analysis,” *ibid.*, p. 12.
[18] Sean Cordey, “The Israeli Unit 8200 – An OSINT-based study Trend Analysis,” *ibid.*, pp. 12-13.
[19] Sean Cordey, “The Israeli Unit 8200 – An OSINT-based study Trend Analysis,” *ibid.*, p. 8.
[20] Sean Cordey, “The Israeli Unit 8200 – An OSINT-based study Trend Analysis,” *ibid.*, p. 9.

2019 年以色列軍方在辛貝特協助下，直接空襲炸毀哈瑪斯網戰組織藏身之大樓，樹立虛擬與實體空間整合作戰的成功案例。[21]

以色列網路作戰主要運用自力發展的網路武器，例如自行研發出高斯（Gauss）、迷你火焰（miniFlame）、杜庫 2（Duqu2）等網路間諜工具包，專門用來竊取系統訊息和敏感資料。[22]此外，在網路防護技術發展方面，以色列不僅建立網路防禦系統，還建置軍用智慧手機加密網路；2014 年建立的「數位鐵穹」計劃（Digital Iron Dome）保護關鍵資訊基礎設施及國防體系，並提供網路攻擊的準確來源俾利反制。[23]接著還陸續發展高堡（High Castle）、水晶球（Crystal Ball）、櫥窗（Showcase）和控制論+（Cybernet+）等項目。此外，以色列也曾與美國合作研發網路武器，諸如 8200 部隊與美國國家安全局（NSA）合作開發了震網（Stuxnet）、杜庫（Duqu）、火焰（Flame）等惡意軟體，可針對網路及工控系統實施攻擊。[24]

肆、結論與建議

以色列新任總理 Naftali Bennett 在 2021 年 7 月 14 日演講指出，網路攻擊不僅是以色列國安最大的敵人，也是全世界共同面臨最嚴峻的威脅。值得注意的是，Bennett 總理本身曾任以色列資安公司執行長。[25]根據《IT 人》報導，《以色列國土報》曾釋出過一份統計：「近 40%的以色列高科技創新企業家曾服役於以軍科技部門；

---

[21] 黃彥鈞，〈武力反擊網路攻擊！以色列直接空襲摧毀哈瑪斯網軍基地〉，《科技新報》， 2019 年 5 月 7 日，https://technews.tw/2019/05/07/israel-air-strike-to-ḥamas-cyberattack/。

[22] Sean Cordey, “The Israeli Unit 8200 – An OSINT-based study Trend Analysis,” *ibid.*, p. 9.

[23] 鍾張涵，〈以色列成為全球第二大資安強國　關鍵竟是這支神祕部隊〉，《天下雜誌》， 2019 年 2 月 14 日， https://www.cw.com.tw/article/5093988?template=transformers。

[24] Sean Cordey, “The Israeli Unit 8200 – An OSINT-based study Trend Analysis,” *ibid.*, p. 9；黃梅茹，〈【台灣要如何戰勝中國網軍】以色列每天被網路攻擊都沒事，就靠這支「8200 部隊」〉，《公民報橘》， 2019 年 3 月 4 日，https://buzzorange.com/citiorange/2019/03/04/how-does-israel-cyber-8200-security-works/。

[25] 科技部駐以色列代表處科技組，〈以色列總理呼籲成立「全球網路盾（Global Cybernet Shield）」〉，科技部網頁， 2021 年 8 月 5 日，https://www.most.gov.tw/israel/ch/detail/341fee19-e131-4ddb-be2a-185ac9c463ce。

其中有 10%在情報單位 8200 部隊服役過。包括 Argus、Cato Networks、CGS Tower Networks、Comilion 等在內的幾十家以色列網路安全公司，產品或服務範圍幾乎涵蓋了網路安全與資訊系統的各項領域。這些公司不歸國防軍領導，但他們的創始人以及骨幹都曾在 8200 部隊服役。」[26]

鑒於以色列後備役年齡至 50 出頭，逐年積累形成龐大綿密的網路後備戰士體制，在資安產業建立優越的資安生態系，與以色列網路作戰部隊人力流動無縫接軌，更讓以色列網路作戰部隊在每年召募近千員新血時，能夠以良好職涯出路提供入伍的強大誘因。[27]此外，8200 部隊退伍後備役人員須每年回部隊服役的規定，既有助於網路作戰部隊自外界汲取最新知識能量，俾利精進教育訓練；另一方面也有助於後備役之業界人士了解軍中後輩能耐與屆退最新動態，俾利轉介錄用新血成為產業生力軍，形成雙贏局面。[28]以色列結合新員選用、後備訓練、產業發展的人才流動生態系統，值得我國效法應用於新兵召募、軍事訓練役、國軍志願役、後備教召以及資安產業發展。

本文作者曾怡碩為美國喬治華盛頓大學政治學博士，現為國防安全研究院網路安全與決策推演所所長，研究領域為軍隊與網路安全、中國資訊作戰、中國數位監控；洪嘉齡為退役海軍中校，具資通訊系統規劃及資訊安全專長，曾於參謀本部通資次長室資通安全處以及國安會資安辦任職，現為國防安全研究院網路安全與決策推演所助理研究員。

[26]零日情報局，〈解構全球網軍之以色列網路作戰部隊〉，《IT 人》， 2020 年 3 月 31 日，https://iter01.com/460968.html.

[27] Sean Cordey, “The Israeli Unit 8200 – An OSINT-based study Trend Analysis,” p. 14，鍾張涵，〈以色列成為全球第二大資安強國　關鍵竟是這支神祕部隊〉，《天下雜誌》， 2019 年 2 月 14 日，https://www.cw.com.tw/article/5093988?template=transformers。

[28] Sean Cordey, “The Israeli Unit 8200 – An OSINT-based study Trend Analysis,”pp. 14-15；吳書緯，〈專家：仿以色列 建資安產業生態循環圈〉，《自由時報》， 2021 年 8 月 9 日，https://news.ltn.com.tw/news/politics/paper/1465718。

Meeting Peacetime and Wartime Demands: Israeli Cyber Operations Units

Yi-Suo Tzeng、Chia-Ling Hung

Assistant Research Fellow、Assistant Research Fellow

Abstract

The cyber security industry has urgent demand for talent, making recruitment and retention of cyber operations talent difficult for cyber operations units. Israel's approach has become a model for many. This article describes the missions of the cyber operations forces of Israel's military and intelligence branches and reveals its combination of national security community and private sector for carrying out proactive cyber defense. From advance selection and testing of talent, special training in their military unit to the practical experience accumulated in their military unit, cyber operations service personnel become a new force in the cyber security industry after being decommissioned. On the other hand, Israel has used a rigorous reserve system to gradually build up a huge and dense cyber reserve warrior network. The building of an outstanding cyber security ecosystem by the cyber security industry and its seamless joining with the manpower flow of Israel's cyber operations forces allows its cyber operations forces to use good career opportunities after military service as an incentive when recruiting new blood every year.

Also, after decommissioning from cyber operations forces, reservists are required to return to serve each year, which helps cyber operations forces absorb new external knowledge and facilitates refinement of education and training. It also allows reservists who are themselves working in the cyber security industry to return to the military and see the

ability of their juniors and the latest decommissioning situation, allowing new blood to be directly recruited to the cyber security industry, creating a win-win situation. Israel's talent flow ecosystem combining new recruit selection, reserve training and industry development is worthy of emulation and application by Taiwan in recruitment, conscript military training, voluntary military service reserve educational mobilization and development of the cyber security industry.

Keywords: Israel 8200 Unit, cyber defense, cybersecurity start-up, cybersecurity ecosystem

出版說明

「財團法人國防安全研究院」設立宗旨為增進國防安全研究與分析，提供專業政策資訊與諮詢，拓展國防事務交流與合作，促進國際戰略溝通與對話。

現設有 4 個研究所，本院研究範圍涵蓋：國家安全與決策、國防戰略與政策、中共政軍、非傳統安全與軍事任務、網路作戰與資訊安全、先進科技與作戰概念、國防資源與產業、量化分析與決策推演等領域。

本刊各篇文章由本院研究人員、以及外部學者、專家撰擬，以 5,000 字以內為度，稿件均經審稿程序，其著作權為本刊所有，未經同意，請勿轉載。

※本特刊內容及建議屬作者意見，不代表財團法人國防安全研究院之立場。

發行人：霍守業 ｜ 總編輯：林成蔚 ｜ 副總編輯：嚴振國
編輯主任：蘇紫雲 ｜ 專題主編：曾怡碩 ｜ 執行主編：洪瑞閔
責任校對、助理編輯：陳亮智、林彥宏、江炘杓、劉姝廷、陳力綺
出版者：財團法人國防安全研究院
院址：10048 臺北市中正區博愛路 172 號
電話：（02）2331-2360　傳真：（02）2331-2361
Institute for National Defense and Security Research
No.172, Bo-Ai Road, Chongcheng Dist., Taipei City, Taiwan（R.O.C.）
Tel:886-2-2331-2360　Fax:886-2-2331-2361

財團法人國防安全研究院

Institute for National Defense and Security Research