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