網路後備部隊的可能性與限制

杜貞儀

網路作戰與資訊安全研究所

壹、前言

隨著近年網際網路擴張並深入社會、經濟各層面，各國為維護網路空間安全，成立專門部隊因應已成趨勢。然而，公私部門對相關人才需求孔急，各國專門部隊在多方競爭下，也多半面臨程度不等之招募困境，故有「網路後備部隊」（cyber reserve）的構想，希望能以此解決缺乏常備兵力的問題。不過，正如網路專門部隊仍處於發展階段，網路後備部隊此一通稱，實際上涵蓋徵兵制之義務役後備部隊、募兵制之志願役後備部隊、由民間志願者組成的準軍事組織（paramilitary institution）等不同類型，故比較其異同，對於了解其優劣以截長補短，實有必要。

本篇將簡介網路後備部隊概念、特性與發展脈絡，並以較具代表性之英美兩國及愛沙尼亞為例，比較募兵之志願後備部隊及準軍事組織兩種網路後備部隊類型的異同，並分析其限制與挑戰，再簡介近期對於不同模式成效的檢討與改進提案，以作為借鏡與參考。

貳、網路後備部隊概念與發展

所謂的「網路後備部隊」，一般指以後備兵力於網路領域（cyber domain）執行軍事任務。[1]就目前各國網路作戰之專門軍事部隊演進觀察，其編制多半是由既有之各軍種資通電單位，或是由負責訊號情報（signal intelligence, SIGNIT）之單位所衍生、擴編而來，而後備部隊亦將相關專長納入，組成類似編制單位，擔任任務支援的角

[1] 此定義參考 Marie Baezner, “Study on the use of reserve forces in military cybersecurity: A comparative study of selected countries,” CSS Cyber Defense, April 2020.

色，依需求透過定期教育召集進行訓練，此類無論組成為義務役或志願役，均可視為狹義之網路後備部隊。

然而，依照後備部隊的一般定義，為維護國家安全之軍事力量，協助常備部隊執行任務，且部隊成員並非以執行軍事任務維生，故廣義之網路後備部隊亦涵蓋由志願者組成之準軍事組織，不僅有明確編制，平時即納入軍事指揮管制體系，同樣應視為後備兵力之一環。[2]

做為新興作戰領域，網路空間建構於實體層（physical layer）之上，其基本架構最早雖源於美國軍方之研究計畫，但目前實體設施在絕大部分均為民間所有，且影響範圍遍及各項關鍵基礎設施，深入日常生活之所有層面。網路空間之軍、民不易明確區分，兩者合作亦是維護整體網路安全是不可或缺之一環。如此之任務特性，似乎相當適合介於常備部隊成員與一般民眾之間的後備部隊參與。在市場競爭激烈的今日，訓練耗時長的專業資安人才，通常不易於軍中留用，網路後備部隊也逐漸被視為一項可兼顧其職涯發展的方案，藉此吸引專業人才加入。[3]

此外，由於資通訊產業發展一日千里，使軍民科技發展與應用產生落差，透過在民間資通訊相關產業任職的網路後備部隊成員，於志願性軍事任務中應用其民間工作之技能與經驗，將有機會藉交流縮短兩者差距，並促進公私協力，以及公民社會與軍隊間相互認識與了解，也是支持成立網路後備部隊的一項主要論點。不過，雖然網路後備部隊具有數項優勢，但各國相關部隊於近五年來的發展，是否真能達成其成立時設定之目標，仍有待觀察，以下將透過實際案例進行探討。

---

[2] 民防概念應用於網路空間，較完整之探討可另參 Greg Austin, “Civil Defence Gaps Under Cyber Blitzkrieg,” International Conference “Research and Education for the Cyber Storm,” January 18, 2019, https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/Cyber%20blitzkrieg%207%20Feb%202019%20CONF%20VERSION.pdf。

[3] Lomsky-Feder, E. , Gazit, N., Ben-Ari, E., 2008. Reserve Soldier as Transmigrants, Moving between the Civilian and Military Worlds. Armed Forces Soc. 34, 593-614. http://doi.org/10.1177/0095327X707312090.

參、網路後備部隊案例探討

一、英國、美國之志願役後備部隊

英國與美國採行募兵制，常備與後備部隊均由志願役構成，包含陸海空三軍。後備部隊之招募對象及管道，兩國均與常備部隊大致相同，並且有常後備互轉（transitioning）之機制。為因應網路所帶來之挑戰，兩國均以成立單一聯合作戰指揮機構，不過，兩國網路後備部隊之任務、訓練方式與實際編制則仍有差異。

英國於 2013 年於戰略司令部（Strategic Command）所屬之國防情報局（Defense Intelligence）設立聯合網路群（Joint Forces Cyber Group, JFCyG），下有聯合網路部隊（Joint Cyber Unit, JCU），及其後備部隊（Joint Cyber Reserve Force, CRF）。聯合網路後備部隊成員，來自即將退役的現役軍人、後備軍人以及未有服役經驗的一般人，以具備相關專長為優先考量，所有成員均需通過安全查核，且依照加入之軍種有每年最低工作天數。聯合網路部隊又如大多數之英國軍方單位，各個單位均位於特定駐地，後備部隊成員每年還需參與至少 19 至 27 天之訓練，包括週末之共同任務、以及週間可遠距完成之工作項目，若有需要也可能透過動員在長時間執行任務。[4]

美國 2009 年成立網路司令部（CYBERCOM），下設有其直屬戰力之網路任務部隊（Cyber Mission Teams），又可進一步區分為網路防衛隊（Cyber Protection Team），負責國防部訊息網路（DOD Information Network, 即美軍軍網）防護，並在遭到入侵時進行反應；國家任務隊（National Mission Team）負責偵測網敵活動、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，以支援各作戰司令部的優先任務；最後則是為國家及戰鬥任務隊提供任務分析與

[4] "Working for JFC," *Gov.uk*, https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment （Access date: September 1, 2020）.

計畫支援的網路支援隊（Cyber Support Team）。[5] 在現有 133 支網路任務部隊中，後備單位（包括陸軍、空軍之後備及國民兵）僅參與網路防衛隊。[6] 但後備單位之人員專長（見表 1）、訓練內容與標準，和常備部隊大致相同，加入後備需至少服役八年，並參與每月一次的週末訓練及為期兩週之年度訓練。以國民兵而言，此年度訓練即以網路防護為主的「網路盾牌」（Cyber Shield）演訓，其內容因應網路威脅與時俱進，今年也將包含假訊息在內的資訊作戰（information operation）防護納入演練範圍。[7]

表 1、美國陸軍網路相關之軍事專長（Military Occupation Specialty）代碼一覽

網路 Cyber	通信 Signal Corps	情報 Military Intelligence	資訊網路工程 Information Network Engineering Functional Areas
***17A: 網戰官（Cyber warfare officer）**	***25A: 通信官（Signal officer）**	35A: 情報官（Military intelligence officer）	26A: 網路系統工程官（Network systems engineer）
17B: 網路電磁活動官（Cyber electromagenetic activity Officer -EW）	255A: 通訊服務准尉（Information services technician）	352N: 訊號情報分析准尉（Signal intelligence analysis technician）	26B: 資訊系統工程官（Information systems engineer）
170A: 網戰准尉（Cyber operations technician）	255N: 網路管理准尉（Network management technician）	***35N: 訊號情報士（Signal intelligence analyst）**	26Z: 資深資訊網路工程官（Senior information network engineer)

[5] 詳見杜貞儀，〈美國網路任務部隊與訓練環境發展〉，《國防情勢月報》，第 146 期。

[6] "Department of Defense Cyber Approach: Use of the National Guard and Reserve in the Cyber Mission Force," *Office of the Secretary of Defense Reserve Force Policy Board*, August 18, 2014.

[7] Mark Pomerleau, "National Guard cyber exercise increase focus on information operations," *C4ISRNET*, September 2, 2020, https://www.c4isrnet.com/cyber/2020/09/02/national-guard-cyber-exercise-to-increase-focus-on-information-operations/.

		***35P: 密碼語言士（Cryptologic linguist）**
170B: 網路電磁活動准尉（Cyber electromagenetic activity technician - EW）	255S: 資訊保護准尉（Information protection technician）	35Z: 訊號情報（電戰）士官長（Signals Intelligence (Electronic Warfare) / Senior Sergeant/ Chief）
***17C: 網戰士（Cyber operations specialist）**	255Z: 資深網路運營准尉（Senior network operations technician）	
***17E: 電戰士（Electronic warfare specialist）**	***25B: 資訊科技士（Information technology specialist）**	
	***25D: 網路防護士（Cyber network defender）**	

說明：星號表陸軍後備目前招募專長，粗體則為陸軍國民兵。准尉（warrant officer）為美軍介於軍士官間的職銜，擔任技術專家、教練與顧問。

資料來源：U.S. Army, https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories.html; Issac R. Porche III, et al., "Cyber Power Potential of the Army's Reserve Compone-nt," RAND, 2017, https://www.rand.org/pubs/research_reports/RR1490.html.

為加強部隊與產學連結，美國陸軍後備部隊 2015 年設立網路公私協力計畫（Cyber Private Public Partnership），與 6 所大學及 12 家公司合作，包括微軟、Verizon 及 T-Mobile 等資通訊公司，提供現役軍人轉為後備時的持續進修與就業管道。[8]

二、愛沙尼亞防衛聯盟之網路防衛隊

愛沙尼亞（Estonia）之網路防衛隊（Cyber Defense Unit）是最

[8] U.S. Army Reserve, "Army Reserve Launches Partnership to Create Pathway for Cyber Warriors," January 20, 2020, https://www.usar.army.mil/Featured/Private-Public-Partnership/Cyber-P3/.

為著名的網路後備部隊案例，但以後備部隊編制而言，愛沙尼亞實際上應屬特例。自 1991 年恢復徵兵制後，愛沙尼亞目前除志願役之國防軍（Estonian Defence Forces, Eesti Kaitsevägi）外，同時有義務役構成之後備部隊，及志願者構成之準軍事組織「防衛聯盟」（Estonia Defence League, Eesti Kaiseliit）。「防衛聯盟」平時即直接受國防部管轄，支援平時與戰時軍民單位任務。[9]

愛沙尼亞國防軍下設有網路指揮部，構成網路部隊主力，而 2007 年俄羅斯對愛沙尼亞網路攻擊，不僅使北大西洋公約組織（NATO）

於愛沙尼亞首都塔林設立網路安全卓越中心（Cooperative Cyber Defence Centre of Excellence, CCDCOE），也促使「防衛聯盟」於 2009 年成立網路防衛隊，並於 2011 年正式經政府核定。網路防衛隊屬志願性質，開放所有愛沙尼亞公民參加，不需具備軍旅經驗。而在招募需求中，強調欲申請者需忠於國家、通過背景調查，並有網路安全相關經驗或對此議題感興趣。「防衛聯盟」授予網路防衛隊成員高度自主性，提供基本網路安全訓練課程，但不強制所有成員參加，而專門領域訓練仍由個人自主安排。

由於網路防衛隊是志願參加，故無設置役期，參與任務既不支薪、也無任何法律上之強制力，完全仰賴成員之個人道德責任。但愛沙尼亞企業對於網路防衛隊有相當高的評價，對員工參與採較為開放的態度。[10]而在國際交流部分，除參與北約相關演練（如網路防護演練「鎖盾」Locked Shield）外，由於「防衛聯盟」與美國馬里蘭州國民兵有正式合作關係，也會與其網路部隊進行共同演練與交流。

肆、網路後備部隊之限制與挑戰

從英國、美國及愛沙尼亞之案例，可看出網路後備部隊雖然可能

[9] "Estonian Defence League," *Eesti.ee*, December 19, 2019, https://www.eesti.ee/en/security-and-defense/voluntary-participation-in-national-defence/estonian-defence-league/.
[10] 同註 1。

勝任各種角色，但採行與常備役相近之要求，且訓練地點位置與期間是否支薪，在招募上仍可能成為一大挑戰，降低其申請意願。對此，美國以可機動部署之訓練架構，讓後備部隊成員能在自家附近參與訓練。但即使解決招募問題，以美國現行後備部隊管理為例，亦有過於強調先滿足達成全作戰能力（full operating capability, FOC）所需之認證，而忽視建立戰備狀態之缺失，不易維持部隊戰力，此於 2019 年 3 月已遭課責審計署（Government Accountability Office, GAO）提出報告檢討。[11] 這表示，即便擁有龐大之網路後備兵力，缺乏管理與追蹤，也可能無法完全發揮其應有之功能。

目前網路後備部隊主要仍是參與防護與支援任務為主，但網路防護必須長時間投入，全日 24 小時監控可能之威脅，透過維持專注、警覺並積極協調應變，才能對可能發生的威脅超前防護。因此負責監控之資訊安全防護營運中心（Security Operation Center, SOC），一般由正職人員擔任，具共同工作經驗與默契，透過建立工作流程，確保工作延續性，盡量將漏失潛在威脅之風險降至最低。後備部隊參與網路防護，因無法全時投入、配合此緊湊的工作流程，其成效也曾受質疑。[12]

最後，網路後備部隊較少進行攻擊任務，亦反應各國雖使網路後備部隊參與維護網路安全，但在安全風險管控仍有限制與挑戰。執行任務時，網路後備部隊無可避免將接觸機敏資料，因此既有之安全查核制度徹底落實就更顯重要。由於後備部隊並非全職參與軍事任務，通常不會賦予和常備部隊相同之安全層級，也限制其能從事的任務範圍。本篇探討之英國、美國、愛沙尼亞案例，均明確表示加入後備部隊需通過安全查核，公開資料尚無法得知是否因單位任務性質而有差

[11] 見註 5。

[12] Jamie Collier, “Cyber Reserves Are Not A Silver Bullet,” *War on the Rocks*, May 22, 2020, https://warontherocks.com/2020/05/cyber-reserves-are-not-a-silver-bullet/.

異，不過為避免機密洩漏，除必備的安全查核制度外，甚至可考慮採取提升作業安全（operation security）的作法，如進一步限制資料攜行範圍等。

伍、結論

由本篇探討之案例可知，以後備兵力做為各國之網路後備部隊，確實為可行之方向，具體模式仍處於發展試行階段，尚未有一套適合各國情境的通用作法。雖然從與產學合作提案、或民間企業對員工參與後備部隊的態度觀察，藉由網路後備部隊促進軍方與公民社會相互了解，似已有相當成效，不過，就目前各國案例而言，藉由招募現成專業人力，是否確實能降低訓練成本或達成補實缺員的目標，可能還需要進一步研究證實。而後備部隊管理、參與任務性質與安全風險，是網路後備部隊最主要的挑戰，也因各國之政治、軍事、社會狀況不同而有差異，在參考各國作法並採用時，仍需留意。

本文作者杜貞儀為國立臺灣大學海洋所博士，現為財團法人國防安全研究院網路作戰與資訊安全研究所博士後研究。

Cyber Reserve Force: Possibilities and Limitations

Chen-Yi Tu

Postdoctoral Fellow

Abstract

Generally speaking, cyber reserve force refers to a reserve force that carries out military missions in the cyber domain to solve the problem of insufficient standing force stemming from the difficulty of recruitment for specialized forces due to competition for talent between the public and private sectors and using public-private cooperation to carry out exchange between the military and the people. Due to the fact that the specialized force is still in the development stage, the composition of the cyber reserve force has a different form.

This paper discusses the two examples of the voluntary reserve of the UK and US recruitment system and the paramilitary organization of Estonia. It will show that a cyber reserve force is feasible and is highly effective in terms of promoting exchange between the military and people.

However, further implementation still faces limitations such as difficulty of recruitment, the conflict of the part-time nature of the reserve and the requirement for a large amount of time to be spent on monitoring the Internet, and the need for security approval because of the likelihood of coming into contact with sensitive information when carrying out a mission.

This shows the significant challenges faced in terms of reserve force management, nature of mission participated in and security risk. When referring to and adopting the approaches of other countries, attention still has to be paid to political, military and social differences to formulate a plan that matches our national situation.