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]

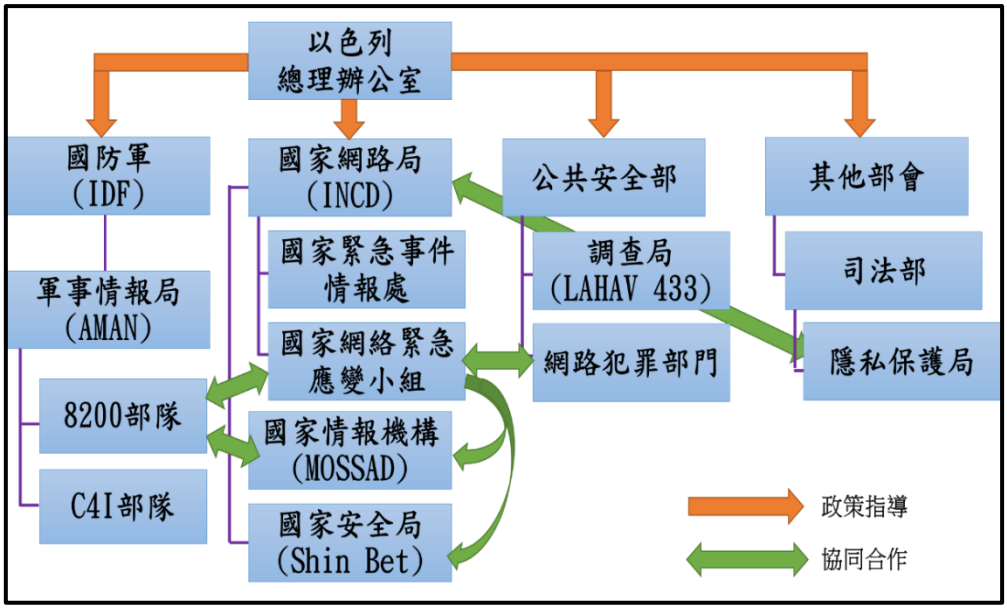
然而，這樣的對內安全作為均集中於總理辦公室掌握，由軍方與情治單位結合民間企業，對包括平民百姓進行網路監控，隨時可能遭濫用於對政敵進行監控。過去曾提出的網路安全法規，並未對此有所改善，反而提議將蒐集到的個資交由網路情報單位處理。2021 年提出的新版網路安全法案，則將個資改為聯繫細節，其餘仍交由總理辦公室權衡後授權監控，事後提請法官授權即可，制衡力道相當薄弱，持續引發公民團體質疑，此法恐將傷害民主治理。[9]

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