10.6326/NDJ.202209_37(3).0002

以色列8200網路間諜部隊對我國省思

Reflections the R.O.C. from IDF 8200 Cyber Spy Unit

張哲鐘 (Che-Chung Chang)
陸軍砲兵第四三指揮部中校後勤科長

彭群堂 (Chun-Tang Peng)
國防大學戰爭學院上校戰略教官

摘　　要

以色列國防軍的國防預算是全中東地區僅次於沙烏地阿拉伯，身爲世界上最有作戰經驗的武裝部隊，以色列在網路方面可與世界大國並駕齊驅，而8200部隊在世界上爲各國的情報專家公認最令人畏懼的網路間諜部隊，其任務等同於英國通信總部，或者是美國國家安全局，其電子作戰及監控能力，足以擾亂敵對國家的政、經、軍、心，其從事蒐集情報和破譯密碼，利用信號情報、視覺情報、人員情報及地理空間情報等方式蒐集數據，然而，我國在面臨中共嚴峻軍事威脅之下，及早獲得當面戰略及戰術情資是刻不容緩，其關係到我國各級戰略的因應作爲，究竟以色列的網路作戰部隊其任務、特質、組成、運用、訓練及如何結合民間產業發展，可供借鏡參考，爲我國未來發展高科技結合情報蒐集目標，以確保國家的安全與發展。

關鍵詞：以色列8200部隊、資電網路攻擊、不對稱作戰

Abstract

The Israel Defense Forces (IDF) have the second highest defense budgets in the Middle East (which is only less than Saudi Arabia). As one of the world's most experienced armed forces, the IDF is as capable as any other world's major powers in cyberspace. Intelligence experts worldwide consider Unit 8200 as one of the most formidable cyber espionage forces and have missions similar to the British Government Communications Headquarters (GCHQ) and the U.S. National Security Agency (NSA). IDF's electronic warfare and surveillance capabilities could disrupt a rival country's political, economic, military, and psychological aspects. This force is also responsible for intelligence collection and breaking/deciphering enemy codes, as well as collecting all sorts of signals intelligence, imagery intelligence, human intelligence, and geospatial intelligence. Like Israel, the Republic of China (ROC) is under severe military threats from the People's Republic of China (PRC). It is critical for our military to acquire real-time strategic and tactical intelligence for rapid responses at all levels. As a result, the ROC could benefit from understanding the missions, characteristics, organization, employment, training, and private industry cooperation strategies of Unit 8200, to develop advanced technology based on intelligence requirements and to ensure our national security and future development.

Keywords: IDF Unit 8200, Information/Computer/Cyber Attacks, Asymmetric Warfare

壹、前　　言

自1948年立國至今，以色列雖然是小國，但其國防預算是全中東地區僅次於沙烏地阿拉伯的國家，其綜合國力卻可撼動中東地區，甚至全世界，除有完善的動員制度外，其中有一段無形的戰力：就是8200部隊（希伯來語：8200 הדיחי, Unit 8200）為以色列不對稱戰略非常重要的部分；8200部隊的任務，長期以來是負責破解翻譯來自於世界各國的政府、國際機構、跨國公司、政治團體及個人電話錄音、電子郵件，範圍涵蓋歐洲、亞洲、非洲與中東等地區，充分運用網路作戰形成不對稱作戰手段。[1]

目前我國在面臨中共嚴峻軍事威脅之下，不對稱戰略的戰略及戰術的作為是我建軍備戰刻不容緩議題，這關係到我國各級戰略的因應作為，究竟以色列的網路作戰部隊其任務、特質、組成、運用、訓練及如何結合民間產業發展，可供為我借鏡參考，本研究以「以色列8200部隊」作為主體，首先從其歷經的戰役來看資訊及網路戰的起源概念開始，其次針對該部隊發展背景與經過，最後探討隊我國軍防衛作戰提出發展策略與建議，以對我國未來建軍備戰之參考。

貳、以色列國防架構組成與8200部隊源起

一、國防軍組織架構

以色列國防軍（Israel Defense Forces，後簡稱IDF）是由陸、海、空軍所組成，並有其他的準軍事部門共同負責不同層面的國家安全，自建軍以來，以色列國防軍的目標是保衛國家的存在和獨立，每個士兵都有義務戰鬥，並按照國防軍的價值觀和命令行事，同時維護國家法律和人民的尊嚴，尊重作為民主國家的價值觀，其主要憑藉著人員訓練精良與完善的制度，而不是取決於兵力的數量，成為世界上作戰經驗豐富的部隊之一。其總參謀部下轄規劃局、情報局、作戰處、深度總部、人力局、軍法院、電腦處、技術和後勤處與北方司令部、中央司令部、南方司令部、本土前線司令部等4個地方司令部，而著名的以色列8200部隊即是情報局下轄所屬單位。（如圖1）

二、網路作戰組成

以色列網路作戰是以總理辦公室為主要組織架構，下轄國家網路局、以色列情報特務局（莫薩德）與國安局（辛貝特），國家網路局主要負責國家網路規劃、推動、發展與安全，並分別設有網路管理局和資訊安全局兩個核心機構。[2] 網路管理局負責網路管理安全事件與情報共享，而資訊安全局負責制定國家網路法規、推動國際間合作，並維護國內基礎關鍵設施與產業網路安全。[3] 情報特務局（莫薩德）是以色列的情報組織，負責在國外收集情報任務、秘密外交和特攻破壞敵方民用和軍事目標。國家安全局（辛貝特）任務負責保護國家網路系統、關鍵基礎設施資訊系統、金融資料等，下轄國家安全情報局負責國家網路基礎設施，訂定網路安全目標與實施計畫，具備國內網路情報監控

1 Tel Aviv, "Israel builds up its cyberwar corps," *UPI*, NOV. 2, 2012, <https://www.upi.com/Defense-News/2012/11/02/Israel-builds-up-its-cyberwar-corps/52421351881449/>（檢索日期：2021年12月18日）

2 Lior Tabansky, "Israel Defense Forces and National Cyber Defense," *Connections*, Vol. 19, No. 1, Winter 2020, p. 49.

3 Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture," September, 2020, pp. 14-15.

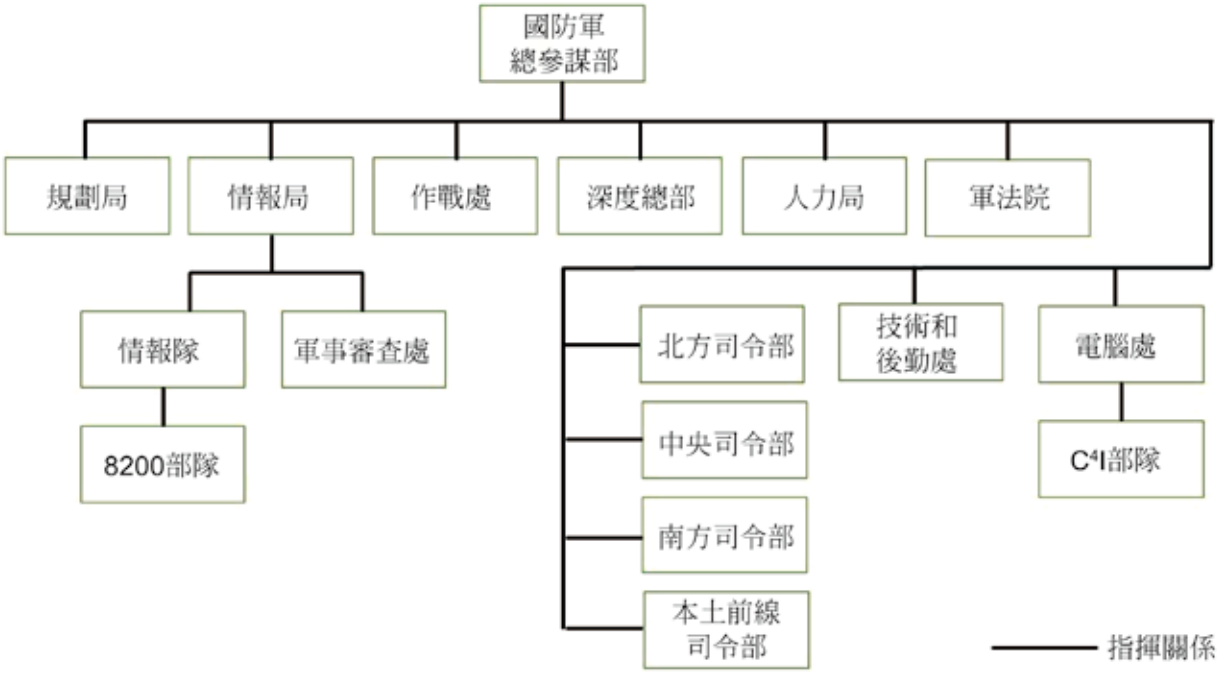

圖1　以色列國防軍組織架構

資料來源：參考以色列國防網站，https://www.idf.il/（檢索日期：2022年4月1日）及筆者綜繪

功能。[4]

以色列國防軍持續發展網路作戰方面能量，於2017年整合軍事情報局的8200部隊、C^{4}I部隊等機構與其他指管通訊部隊，（組織圖，如圖2）其任務執掌分述如下：

(一)8200部隊：以色列國防軍的信號情報蒐集單位，主責網路攻擊任務。

(二)C^{4}I部隊：負責以色列國防軍內部的網路安全，以及為軍方開發通訊基礎設施、軟體和密碼基礎。

(三)其他指管通訊部隊：負責以色列國防軍內部C^{4}ISR傳輸及防護等工作。

三、8200部隊源起

以色列國防軍前身是英國管治時期猶太人的準軍事組織—哈加拿，也是最早猶太領土上的常駐武裝部隊，最初巴勒斯坦猶太地區的情報是依賴於人員的情報來源，以及猶太人和阿拉伯人之間的密切關係；在任務期間，開始對全國電話交換機中流動的資訊進行監測，在獨立戰爭中，阿拉伯軍隊於無線電系統運營商面前，製造了新的對抗以控制權力。從1920年開始，以色列情報人員在巴勒斯坦地區開始了情報蒐集活動，在1938年之後便獲得了進一步的發展，由莫迪凱珊瑚(Mordechai Coral)領導的SJ組織負責，其中包括偵聽和破譯密碼在內的活動；在獨立戰爭開始時，該單位的組織成員被解散，但他們在無政府資助的情況下，以「S.M. 2」組織名稱繼續存在，當時該單位繼續由莫迪凱珊瑚負責，且被定義為：「通過收聽廣播，獲取有關每個校園內敵人的資訊」，其中較大的成就便是破譯獨立戰爭中埃及軍隊的密

4 Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture," p. 15.

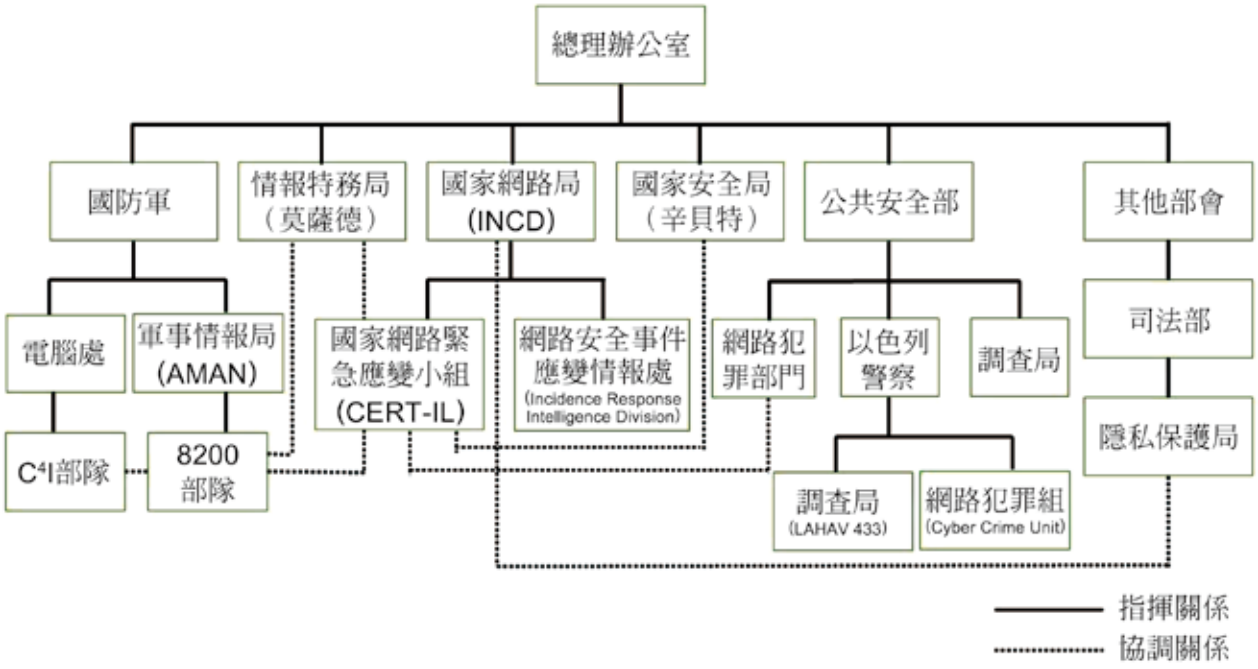

圖2　以色列網路指揮架構

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

碼，並監聽埃及在獨立戰爭結束時討論停火協議時的對話；與此同時被圍困的耶路撒冷有一個名為沙凡(Shafan)的秘密解碼組織，其成員包括魯文・布魯姆（1961～1966年515部隊指揮官）、語言學家雅科夫・波洛茨基、耶霍舒亞・布勞、什洛莫・莫拉格和伊斯蘭學者大衛・茲維・貝內特，這些單位於1948年底始合併，即是信號情報蒐集的開始，1956年5月該單位改名為「515部隊」，就是現在稱為8200部隊前身。[5]

參、8200部隊各時期戰史與運用概述

以色列8200部隊在世界上是被各國的情報專家，公認最令人畏懼的網路間諜部隊，其任務等同於英國通信總部，或者是美國國家安全局，其電子作戰及監控能力，足以擾亂敵對國家的政、經、軍、心，該部隊的使命是「拯救生命、防止恐怖與其他攻擊」，雖然這支部隊在任務上的本質是防禦，但這並不與使用先發制人的手段攻擊目標相衝突，其從事蒐集情報和破譯密碼，利用信號情報、視覺情報、人員情報及地理空間情報等方式蒐集數據，使以色列國防軍擁有龐大的原始數據，其情報佔有量超過了情報總量的90%以上；[6] 8200部隊獲得到原始訊息後，經過整理後成為有用的情報資料庫，使用大數據分析找到共通性，以提供分析人員以

5 Aviezer Yaari, Amikam Shapira, "וניעידומה תשרומל זכרמהמ וחטיבו וניעידום וניזגמ :הונ מלמ," No. 30, 2002, p. 6.

6 夏洛山，〈以國神祕部隊曝光　AI首次介入戰爭〉，《大紀元網》，2021年6月5日，<https://www.epochtimes.com/b5/21/6/5/n13001442.htm>（檢索日期：2021年10月15日）

多角度、多途徑解讀所獲得的訊息，透過這些基礎訊息去判斷訊息間相互關聯性，進而執行軍事行動、無人機暗殺或逮捕行動，所以有一部分的工作是在處理歐洲、中東、非洲、巴勒斯坦領土等境外活動。綜上可知，其將網路攻擊與防禦行動相結合起來，當然其中也涵蓋各類型通信、翻譯、譯密與分析等特殊信號情報，在各時期發展如下：

一、六日戰爭(Six-Day War)

1967年6月6日，也就是六日戰爭的第二天，以色列截獲來自埃及與約旦的元首通聯電話，在談話中，埃及總統賈邁勒．阿卜杜勒．納賽爾(Gamal Abdel Nasser)誤導約旦國王侯賽因．伊本．塔拉勒(Hussein Ibn Talal)，謊稱埃及空軍從當日早上開始就在以色列機場遭到襲擊。事實上埃及空軍在前一天大部分戰機都被以色列摧毀了，而埃及這樣做是為了讓最初不願意積極參戰約旦，願意投入這場戰爭中；而埃及提供的虛假消息讓約旦考量其利益而開始動心，進而讓約旦宣布參與對以色列用兵並協助埃及作戰。另外納賽爾總統建議兩國在早上同時宣布（包含美國和英國飛機從地中海東部的航空母艦起飛）向埃及和約旦機場的飛機實施襲擊。[7]

此時，由於以色列國防部長摩西．達揚(Moshe Dayan)伺機製造一場戰場迷霧，讓全世界包括以色列居民在內，都不知道以色列在陸上和空中整體戰勝的程度。依摩西．達揚的決定，錄製了截聽埃及與約旦的對話並在IDF頻道上播放，儘管以色利武裝部隊負責人阿哈龍．亞里夫(Aharon Yariv)少將表示反對，其理由為擔心對話本文和錄音公布的結果，其情資蒐集來源和方法將可能被披露；這是以色列首次公開被其截獲的對話，之所以決定公布這消息，是因為擔心埃及正在以同樣手段試圖將蘇聯捲入戰爭，正如國防協議中所承諾的那樣，以防美國對以色列進行干預。在六日戰爭之後到蘇聯介入期間，該單位協助GSS定位從西奈半島到埃及情報部門的廣播特工活動，[8] 到了1968年8月，該部隊更名為「848部隊」。

二、贖罪日戰爭(Yom Kippur War)

1973年10月5日，即戰爭開始前一天的情報研究文件評估指出：「埃及計畫重新發動敵對行動的可能性很低」，這份報告足以讓以色列面對阿拉伯聯軍喪失先制作戰契機，[9] 而大部分失敗歸因於研究部和軍事情報局局長伊萊．澤拉少將的資訊研判。848部隊的「特別措施」是以色列國防軍面對埃及的「信號情報蒐集」手段，這支部隊提供埃及打算開戰的可靠資訊，在贖罪日戰爭爆發前，848部隊指揮官約爾．本—波拉特(Yoel Ben Porat)上校和情報部門負責人梅納赫姆．迪格利(Menachem Digli)上校向武裝部隊負責人伊萊．澤拉少將要求採「特別措施」，以查明埃及軍隊正在為戰爭做準備，或者這只是一場遭拒絕的演習，最終阿里耶．沙列夫(Aryeh Shalev)准將批准了這項「特別措施」；直到戰爭爆發前幾個小時，國防部長摩西．達揚瞭解「特別措施」調查結果，但卻

7 Avner Cohen, "The 1967 Six-Day War," Wilson Center, June 5, 2017, <https://www.wilsoncenter.org/publication/the-1967-six-day-war>（檢索日期：2021年11月20日）

8 Rafi Kitron, "יניס רוזאב כ"בשה ירגוב לש ירבדמה רודב הנד היגלטסונה," Malam View, Vol. 65, February, 2013, pp. 6-10.

9 Robert McNamara, "The Yom Kippur War of 1973," ThoughtCo, February 21, 2020, <https://www.thoughtco.com/yom-kippur-war-4783593>（檢索日期：2021年10月20日）

認同澤拉少將的評估不會發生戰爭。

另外，在10月5日（戰爭爆發前21小時）截獲破譯出伊拉克駐莫斯科大使向巴格達外交部發出的電報，內容稱蘇聯公民從敘利亞和埃及撤離，是因為敘利亞和埃及意圖進行發動戰爭，其中毫無疑問地表明戰爭即將爆發。但以色列情報部門的警告沒有即時送達參謀長大衛．埃拉扎爾(David Elazar)處，也沒有得到適當的分析，所以並沒有改變對參謀長及其周圍幕僚的評估；儘管戰場和情報有許多跡象顯示戰爭即將開始，而該部隊的指揮官約爾．本一波拉特(Yoel Ben Porat)上校竭盡全力說服他們戰爭迫在眉睫，但最後始終沒有成功被認同；而後在贖罪日戰爭期間，在作戰全程適時幫助提供情資給第36師，使其攻擊前往戈蘭高地增援敘利亞的伊拉克部隊，以及幫助第162師摧毀位於西奈半島小苦湖地區的埃及第25裝甲旅，[10] 致使以色列國防軍在為期18天的戰爭中得到最終的勝利，但這場勝利對以色列付出了人力與經濟的雙重損失(死亡2,800人及受傷9,000多人)，經濟損失估計高達70億美元。戰後該部隊更名為現名「8200部隊」。

三、電腦病毒攻擊

2004年3月，伊拉克戰爭後情報系統調查委員會發表了一份報告，其中提議除其他事項外，將該單位從情報司中移除，並將其轉變為國家情報管理的情報機構，美國和英國的情況類似。在2009年與美國國安局共同研發運用Stuxnet電腦病毒，[11] Stuxnet是一種惡意的軟體，也是一組非常「乾淨」，沒有多餘程式碼，難以追蹤的病毒，比一般病毒大20倍，裡面塞了4組具完整攻擊能力的「零日」模組，並且完全針對工業設施攻擊。[12] 該病毒是與破壞基礎設施有關的電腦病毒家族中較著名的一種。旨在執行破壞性操作，或在電腦用戶在瀏覽網頁時使用這種病毒竊取部分用戶數據，或給用戶帶來損害，這種病毒具有快速的鋪展性，並且由於其強大的著色、複製和逃避能力而難以擺脫。[13] 而攻擊者使用Stuxnet利用多個「零日攻擊」(Zero-Day Attack)[14] Windows軟體系統漏洞，並且搜索受到病毒感染的電腦，查找控制機電設備軟體的連接，並發送損壞裝備的指

10 Ephraim Lapid, "לילגב סולשה תמחלמב יברק ויעידוע לע," Malam View, Vol. 64, October, 2012, p. 38.

11 James Andrew Lewis, "Iran and Cyber Power," CSIS, June 25, 2019, <https://www.csis.org/analysis/iran-and-cyber-power>（檢索日期：2021年11月20日）

12〈零日網路戰：史上最惡病毒「Stuxnet」的真相，竟是場殘酷的新型態戰爭〉，《INSIDE硬塞的網路趨勢觀察》，2016年8月16日，<https://www.inside.com.tw/article/6984-zero-days〉（檢索日期：2022年7月21日）

13 拉伊德．阿尤布，〈伊朗納坦茲最新核反應堆針對敏感設施電子戰中使用的技術和方法〉，《半島網》，2021年4月13日，<https://chinese.aljazeera.net/opinions/journalist-column/2021/4/13/%E4%BC%8A%E6%9C%97%E7%BA%B3%E5%9D%A6%E5%85%B9%E6%9C%80%E6%96%B0%E6%A0%B8%E5%8F%8D%E5%BA%94%E5%A0%86%E9%92%88%E5%AF%B9%E6%95%8F%E6%84%9F%E8%AE%BE%E6%96%BD%E7%94%B5%E5%AD%90%E6%88%98%E4%B8%AD%E4%BD%BF>（檢索日期：2022年7月21日）

14 即是在「漏洞發現」到「修補漏洞」中間會有一段空窗期，因為發現漏洞時，軟體公司會需要一段時間來製作修補程式，但是通常「發現」這個漏洞的人就是駭客，所以修補程式發布時，攻擊程式可能也會同時出現，所以電腦因此被攻陷。

令，透過縝密計畫感染核電廠電腦，致使伊朗納坦茲核設施的濃縮鈾離心機，近9,000臺中，有1,000臺運轉失靈而被成功癱瘓，據調查此次事件為美國與以色列於2006年起展開的秘密行動，這種病毒具有癱瘓國家基礎設施，程式碼多達1萬5千多行，並已植入伊朗多年，且擴散到十幾個國家，[15] 而在2014年該國出口的網路安全產品，更是超越軍事硬體設施。2015年12月23日，在烏克蘭電廠內控制系統電腦屏幕上的光標開始自動移動，當他們試圖控制光標移動時，發現自己已經被踢出電腦系統之外，一名駭客正在遙遠的地方控制著他的電腦；該次網路攻擊影響10萬餘人的日常生活，且時間長達6個小時，這種類型的網路攻擊可能是由高度專業化的敵人完成。[16]

四、果園行動(Operation Orchard)

以色列於2004年底前即認為北韓暗中協助敘利亞發展核子武器，並於2007年9月6日時，派遣不具有匿蹤能力的F-15第三代戰機，裝備有雷射導引炸彈，在預警機、電戰機與地面特種部隊相互配合之下，突破敘利亞先進「道爾」防空飛彈系統(Tor Missile System)，轟炸摧毀隱藏在沙漠深處的核工廠，並於任務後安全返航，而成功的關鍵就是網路部隊。先行透過網路攻擊手段，使用「舒特」機載網路攻擊系統，[17] 這個系統是利用網路病毒侵入敵人電腦、通信系統與雷達站，而無須摧毀便能滲透目標網路，全面接管敘利亞防空雷達網，使戰機直抵敘利亞腹地如入無人之境。

五、全面披露行動(Operation Full Disclosure)

2014年3月5日，以色列國防軍突擊隊在紅海攔截並扣押伊朗的商船Klos C（巴拿馬註冊），在船上發現遠端導彈並被懷疑運往加薩地帶，藏在裝滿標有波特蘭水泥的伊朗袋子的貨櫃中，最後聯合國專家小組得出結論，這些武器來自伊朗，並將被送往蘇丹，[18] 指責伊朗違反了武器禁運，並於聯合國安理會第1929號決議授權各國扣押伊朗禁止出口的物品，這次行動是該部隊透過先進的通信與網路能力，進而獲得最終的情報。

六、奧杰羅事件

2017年5月，黎巴嫩政府指控以色列對該國的奧杰羅電信公司(Ogero Telecom)，進行複雜的網路攻擊，透過語音訊息，傳達給了一萬多名黎巴嫩人民假消息，指責真主黨領袖就是該國最高軍事指揮官死亡的幕後黑手。[19]

七、防範恐怖攻擊

2018年2月21日，以色列宣布8200部隊獲得了有關ISIS即將在澳大利亞實施的重大

15 愛伊米，〈以色列網路武器的興起〉，《德若資訊網》，2021年2月27日，<https://iemiu.com/zh-tw/history/36282.html〉（檢索日期：2021年11月20日）

16 Christian Borys，〈對抗網絡戰的網絡安全實驗室〉，《BBC英倫網》，2018年1月16日，<https://www.bbc.com/ukchina/simp/vert-fut-42705462>（檢索日期：2022年7月21日）

17 Eric Sof, "Operation Orchard: Bombing of the Syrian Nuclear Reactor," Spec Ops Magazine, March 31, 2022, <https://special-ops.org/operation-orchard-bombing-syrian-nuclear-reactor/#google_vignette>（檢索日期：2022年4月2日）

18 Sean Cordey, "The Israeli Unit 8200 An OSINT-based study," Center for Security Studies, December 2019, p. 9.

19 Sean Cordey, "The Israeli Unit 8200 An OSINT-based study," Center for Security Studies, p. 9.

襲擊的重要訊息，[20] 並將情資交給澳大利亞情報部門，阻止該組織對一架從澳大利亞飛往阿拉伯聯合酋長國的潛在恐怖攻擊，並在實施恐怖襲擊之前逮捕了恐怖分子。

除此之外，2020年11月2日伊朗核科學家穆赫辛・法克里扎德(Mohsen Fakhrizadeh)遇刺案中，伊朗官方經過調查認為，即是以色列運用衛星遙控武器，結合人臉識別與AI人工智慧完成暗殺任務；2022年5月22日時，伊朗伊斯蘭革命衛隊高級軍官哈桑・賽亞德・霍代伊(Hassan Sayad Khodai)在其住所附近遭槍擊身亡，也是自2020年伊朗核物理學家法赫里扎德遇害以後，遭暗殺的伊色列最高級別人員。

綜上所述，以色列8200部隊可以超越地面作戰的限制，採取非傳統手段運用資訊、網路系統，遠距離對敵國的關鍵基礎設施破壞及散播假訊息，造成國家運作延宕與社會民心動盪，並且癱瘓雷達站與電子作戰能力，侵入軍方網路系統，執行網路作戰及攔截監聽各種情資，另外還可以執行海外暗殺行動，並且提供國內與海外的國安單位，以有效打擊預防國際恐怖活動發生。

肆、以色列8200部隊手段探討

鑑於以色列8200部隊其任務、組織、編裝仍屬重要機密，在官方公布數據資料與文獻查詢方面不易獲得及辯證，雖然無法有直接證據指出為該部隊所為，但可由六日戰爭、贖罪日戰爭、網路病毒攻擊、果園行動、全面披露行動、奧杰羅事件、暗殺行動、防範恐怖攻擊等任務中，均有其運作的脈絡可循，綜合上述戰史及官方資料，可歸納出以色列8200部隊具有以下特徵：

一、網路空間開創不對稱作戰：係指軍力弱者對上強者的戰爭中，如何取勝或達成戰鬥目標的作戰思維。雙方都可能在各種能力（力量、時間、空間、武器技術、手段及戰術戰法等等）上有其優劣，有時扮演強者，有時扮演弱者，運用以小博大方式獲取勝利。「網路戰」具備「不對稱作戰」之中，「攻擊敵人之關鍵節點、破壞其作戰節奏、癱瘓其作戰能力」的優勢，又可稱為「無國界」或「無煙硝」的戰爭，其戰場在無所不在的網路空間(Cyberspace)。

二、電信監控、破譯功能：運用電信監控和資訊等技術，追蹤或破解敵可能行動，取得敵企圖與行動。

三、網路病毒癱瘓攻擊：個人、組織、部隊或國家遭受到惡意軟體、病毒、網路釣魚、DDoS和其他各種類型的網路攻擊，導致生命、資源、時間等損失或作戰失敗。

四、偽訊息散播：偽訊息是資訊戰當中「認知作戰」的一環，若每天從通訊軟體接收大量偽訊息，將會影響地區、全國甚至世界的觀點；如近期的俄烏戰爭所釋放出的偽資訊（合成偽戰況）。

五、情報整合運用：運用監控和資訊技術，掌握敵情報資訊和其他威脅，統籌分析網路攻擊相關情報，通過AI及大數據等方式共用分析結果，對網路攻擊迅速做出反應及反制。

以色列8200部隊在「不對稱作戰」概念下，以新型戰爭模式的「混合戰」為手段，

20 Sean Cordey, "The Israeli Unit 8200 An OSINT-based study," Center for Security Studies, p. 9.

綜合運用其中的資訊戰、網路戰、認知空間作戰等眾多手段，相互配合達成作戰任務，故本次針對上述的不對稱作戰概念，以及該部隊所使用的混合戰手段做歸納探討，以概略恢復其具體輪廓：

一、8200部隊支援國防軍達成不對稱作戰癱瘓敵作戰能力

1990年代之後，全世界隨著資訊的便利、科技的進步與全球化影響之下，各國家都接受到一定程度的衝擊，而世界各國的安全也面臨到更多方面的挑戰，所以「不對稱安全威脅」(Asymmetrical Security Threat)是在這個背景下產生。[21]「不對稱作戰」最早源自於美國後冷戰時期的作戰思維，這個思維主要是擺脫過去正規及高科技作戰，而要將非正規的威脅納入未來可能改變戰局模式；所謂不對稱作戰會與對稱作戰的性質、目的、類型的作戰運用不相同，主要是發揮自己的優點，打擊敵人弱點，以達到軍事或政治目的，[22] 戰爭中弱方有時採用非常規作戰手段來彌補軍事力量在質量和數量上的不足，其前提是強方不願付出沉重的形象代價，如果決定採取類似方式，將受到國際壓力。[23] 由於不對稱作戰會因為國情及環境不同，所產生的解釋及意義也不完全相同，也有部分學者認為僅是一種對作戰方式的陳述，且過去的戰爭均有運用。[24]

德國著名學者克勞斯．彼得．薩爾巴赫(K.SAALBACH)在其《Cyber War Methods and Practice》一書的「網路戰」將網路戰區分為三種型態。第一種型態，舉凡對電腦、資訊、網路及電腦所依存的系統實施攻擊，即稱為「網路攻擊」(Cyber Attack)；第二種型態，係以上攻擊行動具有恐怖主義背景，以達成恐怖主義目的，稱為「網路恐怖主義」(Cyber Terrorism)；第三種型態，若攻擊行動目標係非法獲得某些資訊，則稱為「網路間諜」(Cyber Espionage)，就如同以色列8200部隊。[25]

瞭解戰爭或作戰的不對稱性表現型式，始能針對這些不對稱性的要素加以運用、調整、組合、轉化，並形成優勢，進而戰勝敵人。[26] 近年來隨著科技發展，使得武器效能大幅提升，但科技所帶來的優勢並無法應付所有戰爭，加上戰爭型態已變為多元化及全方位，逐漸脫離傳統戰爭思維模式，進而產生所謂程度不同的不對稱作戰思維。[27] 故靈活運用科技、網路及資訊能力，使不對稱

21 張祥山，〈非傳統不對稱安全威脅初探〉，《展望與探索》，第4卷，第4期，民95年4月，頁35。

22 李晧、張瑞麟，〈「不對稱作戰」之發展探討〉,《海軍學術雙月刊》，第46卷，第3期，2012年3月，頁35。

23 Anthony H. Cordesman, "The Arab-Israeli Military Balance in 2010," CSIS, June 29, 2010, <https://www.csis.org/analysis/arab-israeli-military-balance-2010>（檢索日期：2021年12月2日）

24 蔡昌言、李大中，〈不對稱戰爭相關理論及其應用於中國對臺戰略之研析〉，《遠景基金會季刊》，第8卷第3期，2007年7月，頁1-35。

25 K. SAALBACH, "Cyber war method and practice" V.3.0, Nov. 2011, p. 3-5.

26 謝游麟，〈孫子「不對稱」思想對國軍軍事戰略之啟示〉，《國防雜誌》，第24卷第5期，2009年9月，頁83。

27 Steven Metz，謝凱蒂、楊紫函、蔣永方譯，《21的武裝衝突：資訊革命與後現代戰爭》(Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare)（臺北：國防部史政編譯局，1990），頁48-49。

作戰之戰力倍增，是弱國反制強國主要手段，也是戰力優勢者，可運用高科技武器，在未接觸對方情況下，對其弱點予以致命打擊；[28] 另戰力劣勢者，亦可針對高科技武器的弱點實施攻擊，使其優勢戰力無法發揮，兩者均可減少傷亡及達成作戰目標；正如以色列國防軍於中東地區所面臨的威脅，8200部隊充分發揮其優勢，支援以色列國防軍遂行不對稱作戰，方能確保其國家安全。

二、資訊作戰

目前全世界軍事發展較先進的國家武器裝備，不論是主戰或支援裝備都朝向資訊化發展，作戰平臺具有資訊獲得及處理能力；攻擊武器隨著時代進步，逐漸達到智慧化，發射後主動追蹤與目標精準打擊，而作戰指揮透過C^4ISR實現自動化，[29] 並且發展成網路戰、電子戰等武器裝備及技術手段。[30] 第一次以阿戰爭之後，515部隊（8200部隊前身）情報工作主要區分2個部分，分別是攔截敵人資訊與負責破解密碼、參數蒐集，而破解密碼、參數蒐集的能力主要是早期以色列工程師開發，其中也有一些是蘇聯移民過來的，但規模比現在小許多，經費預算也相當有限；1967年六日戰爭期間，已經能夠攔截與破譯埃及和敘利亞空軍通信，這也使得規模較小的以色列空軍可以確實掌握空域，並能在短暫的戰役中擊敗埃及、敘利亞與約旦軍隊，大幅擴大以色列的領土；到了現代8200部隊的監聽與攔截各種訊號及情報技術已相當成熟，每天都要監聽周邊國家的動靜，其中也包含巴勒斯坦控約旦河西岸與西南方加薩走廊等爭議地區，並且提早偵破恐怖活動，協助安全部隊將其危安份子逮捕。

資訊戰這個名詞是在波灣戰爭後才開始有的軍事作戰研討，就我國對「資訊戰」定義而言，廣義來說，是運用各種手段影響敵方並防護我方決策程序與資訊系統之行動，以創造資訊優勢；但在狹義方面，是運用資訊科技影響敵方並防護我方指管程序與資訊系統之行動，以獲取戰場資訊優勢；[31] 故資訊作戰貫穿作戰全程，且為聯合作戰的重心，並遍布於戰爭中各個領域，戰爭焦點成為爭取資訊優勢，為爭奪制海、制空權及其他空間控制權關鍵，亦是成為主導聯合作戰的行動，在未來戰爭中的資訊領域將越來越激烈，資訊戰會與制海、制空權融合為一體，且自始自終將圍繞著保持資訊權做激烈抗爭；另外關注的是美軍不僅提出戰役、戰鬥層級的資訊作戰，更提出了戰略層級的資訊作戰，未來戰爭關鍵將取決於資訊戰的成

28 黃惟喬，〈不對稱作戰對現代戰爭的影響〉，《國防大學軍事學部論文集》，桃園：國防大學，2004年，頁46-47。

29 Roksana Gabidullina, "The Future of U.S.-Russian Arms Control: Principles of Engagement and New Approaches," CSIS, March 12, 2021, <https://www.csis.org/analysis/future-us-russian-arms-control-principles-engagement-and-new-approaches>（檢索日期：2021年11月20日）

30 曹潤生，《冷戰後中共資訊戰之發展》（臺北：國際事務與戰略研究所碩士在職專班／碩士論文，2006年1月），頁18。

31 Mike Dahm, "The Reality of War Should Define Information Warfare," U.S. Naval Institute, March 2021, <https://www. usni.org/magazines/proceedings/2021/march/reality-war-should-define-information-warfare>（檢索日期：2021年12月25日）

敗。

三、網路作戰

以色列於2009年以一種「軍用級」的Stuxnet網路病毒，成功破壞納坦茲的核離心機，使其近9,000臺之中有1,000臺運轉失靈而成功癱瘓；在2007年果園行動中成功掌握並以木馬程式駭入敘利亞政府官員電腦，發現電腦硬碟有核工廠相關資料與數百張照片，照片清楚顯示核工廠在不同時期的建設證據，攻擊當日以電戰機實施網路系統攻擊，入侵敘利亞雷達防空系統，接管並限縮敵方察覺以色列軍機進入領空，使其完成投彈任務又安全返回以色列基地；[32] 2014年全球披露行動中，8200部隊運用先進的網路與通信能力，讓以色列突擊隊在紅海成功攔截伊朗運往蘇丹的軍用武器和裝備，讓世界各國感覺以色列的國防軍和情報部門有一種不可戰勝的態勢。

現行網路已經遍布全球，不僅改變了人類生活，也將產生變化肆應未來戰場，並且演化出另一種作戰型式，以下就特點分述如下：

(一)可於任何時間、地點及方式進行網路攻擊。

(二)攻擊的目標較廣闊，範圍不僅侷限於軍事設施。

(三)受到網路攻擊時，對於攻擊者較不易判斷。

(四)對於攻擊效程無法精確掌握，並對下次攻擊無法做有效偵測與防護。

(五)可於短時間內藉由小攻擊，癱瘓對方重要設施。

網路作戰是近幾十年來於軍事領域中的新興課題，而且各國在相互競爭中，掀起一場創世紀的革命，其重要性就等同於核武器的出現，[33] 而未來大規模傳統戰爭將不復見，取而代之的是朝向較高技術、小規模、低衝突型式的未來戰爭。鑑於全球正蔓延發展網路作戰，且網路發展已經超出國家地域的限制，等同政治、經濟、軍事活動的重要性，故網路作戰係運用網路對他國進行經濟、政治、科技、文化、軍事等作戰行為；另外也可以在俄烏戰爭中發現到，隨著地緣政治緊張局勢升級，也增加了關鍵基礎設施的網絡攻擊強度；電腦網路安全公司Trellix Threat Labs首席科學家兼首席工程師Christiaan Beek曾表示：「我們正處於網路安全的關鍵時刻，並且在不斷擴大的攻擊面中觀察到越來越多的敵對行為」。對俄烏戰爭Trellix Threat Labs也一直在觀察與調查針對烏克蘭的惡意程式和其他網路威脅，通過破壞對設備運行方式，使目標喪失功能。Trellix對俄軍入侵烏克蘭前期過程中，所使用的Whispergate和HermeticWiper等惡意程式，運用病毒破壞該國內部通信，以降低系統的穩定性。[34] 而TeamT5也於2021年7月研究發現兩個攻擊南韓的惡意程式樣本，與後門程式MemzipRAT有高度關聯性，同樣均

32 Lior Tabansky, "Israel Defense Forces and National Cyber Defense," Connections, Vol. 19, No. 1, p. 55.

33 John B. Alexander著，楊連仲譯，〈使用非致命性武器的未來戰爭〉（臺北：國防部史編局，2001年4月），頁169。

34 Sarah Erman, "Trellix Finds Escalation of Cyberattacks Targeting Critical Infrastructure as Geopolitical Tensions Rise," Trellix, April 27, 2022, <https://www.trellix.com/en-us/about/newsroom/news/news-detail.html?news_id=2019cc26-3450-4b0d-b238-82d49348dcb7>（檢索日期：2022年7月28日）

為安裝程式。這一波攻擊主要是針對南韓某航太產業公司，該受駭客入侵公司當時為南韓前十大企業之一，業務範圍涵蓋航太、化學、金融、IT服務等。駭客利用尚未揭露的VPN伺服器漏洞，駭入目標環境並部署惡意程式。就此推測駭客仍可能利用VPN系統漏洞，發動更大型、損害更嚴重的攻擊，未來也不排除轉變為供應鏈攻擊的可能。[35]

然而「網路戰」定義係指敵對雙方陣營針對戰爭行為利用資訊與網路環境，遂行爭奪制資訊權，利用電腦網路系統確認網路及資訊系統安全，並且有計畫破壞敵對方的網路及資訊系統。[36] 在實質定義方面，網路戰屬資訊戰另一種演化方式，是在有系統的規劃下進行一連串的破壞行動，與傳統戰爭相互比較，可以明顯發現其具有隱匿性、猝然性、代價性及不對稱性及參與性的特性，[37] 這是一個網路攻擊的領域，由於其全球影響力，可能類似於核戰爭。[38] 例如近年來以色列和沙烏地阿拉伯密切往來與接觸，間接提高了伊朗的網路能力，而使伊朗能夠將概念化網路攻擊融入更大的軍事行動。伊朗使用的工具通常來自修改過的網路惡意程式，不具更先進的網路武器的破壞性影響。[39]

四、認知空間作戰

以色列8200部隊在2017年奧杰羅事件中，掌握到網路、語音訊息攻擊的成本低，且不受到距離限制及傳播速度快，所產生影響層面廣的特性，發布偽訊息干擾黎巴嫩政府運作，迫使該國政府耗費相當人、物力去調查、澄清，對黎國的國內社會影響很大。而認知作戰通常都是針對某個特定事件，進行複合式具體作為飽和攻擊，其後續發展與企圖都具有潛在威脅，徹底嚴重影響國家安全，然而伴隨著網路與通訊媒體發達，訊息的產製及傳播速度都非常快，且在該國政府難以查證下，對於要如何避免到升級成區域衝突，將面臨著有一定的困難度，因此認知空間作戰的對象鎖定是「人」，透過心理作戰層面的社會群體間隙與矛盾，加以擴大與激化對立，即是該項作戰成功的關鍵條件。

認知空間主要是指人的意志、信仰、價值觀及情感等無形空間，存在於每個人的主觀意識中，也是認知活動所影響到的範圍與領域，並且由無數的個體認知空間累積成國家認知空間，[40] 而孫子兵法所云：不戰而

35 TeamT5 Media Center, "Another CloudDragon attack abusing VPN zero-day vulnerability to target South Korean entities," TeamT5, July 1, 2021, <https://teamt5.org/en/posts/another-clouddragon-attack-abusing-vpn-zero-day-vulnerability-to-target-south-korean-entities/>（檢索日期：2022年7月28日）

36 Todd Harrison, "Battle Networks and the Future Force," CSIS, August 5, 2021, <https://www.csis.org/analysis/battle-networks-and-future-force>（檢索日期：2021年11月20日）

37 李承禹，〈中共網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用〉，《復興崗學報》，第90期，2007年12月，頁252。

38 James Andrew Lewis, "Cyber Attacks, Real or Imagined, and Cyber War," CSIS, July 11, 2011, <https://www.csis.org/analysis/cyber-attacks-real-or-imagined-and-cyber-war>（檢索日期：2022年4月11日）

39 James Andrew Lewis, "Iran and Cyber Power," CSIS, June 25, 2019, <https://www.csis.org/analysis/iran-and-cyber-power>（檢索日期：2022年5月20日）

40 朱雪玲、曾華鋒，〈制腦作戰：未來戰爭競爭新模式〉，《解放軍報》，2017年10月17日，<http://www.81.cn/jfjbmap/content/2017-10/17/node_12.htm>（檢索日期：2022年7月4日）

屈人之兵，善之善者也，即是最高作戰指導原則，雖然傳統的戰爭仍然是在物理空間中進行，但隨著時代的演進與科技的進步，戰爭的本質已經昇華為心理及精神層面，儼然成為新型態作戰空間重心，而空間範圍也會隨著生活圈持續擴大，憑藉語言、文字、社群網路、書報雜誌、語音訊息等宣傳為攻擊武器，透過各種不同面向滲透、破壞，將偽訊息傳播到國內任何地方，最終影響到國家整體意識型態及其價值觀，造成國家社會內部動盪不安、自亂陣腳、驚慌失措、通貨膨脹、經濟蕭條，使人民喪失對國家的信任，最終實現以戰逼降、不戰而屈人之兵之作戰理念。

五、軍、民合作人才培育

以色列8200部隊現役人數保持約在5,000員，已經退伍的人數一直被該國列為機密，而在人員選拔困難度，僅次於空軍飛行員，同時在過程中也較為神秘，這個部門尤其在網路領域與其他情報單位人才競爭相當激烈；而8200部隊遴選新兵早在高中時期就開始，馬格希米姆(Magshimim)是網路教育中心的旗艦專案，旨在透過為國內青年創造機會來推動社會變革，讓他們在網路技術領域脫穎而出，會透過學校推薦資優學生進行篩選，並派專員前往至各學校觀察考核，並透過學校課程融入程式編輯或每週兩次3小時課程，每週完成10小時網路作業及每年參加2次研討會培訓，[41] 而在兩輪的選拔過程中，區分數學、解釋、閱讀理解、分析思維和領導能力快速學習能力、快速適應、身體狀況與心理評估等。[42]

經過選拔錄取人員就不再接受傳統軍事訓練，而是參加電腦課程的專業軍事訓練，在培訓的過程中是相當保密的，每天約12至18小時訓練，訓練範圍從電腦工程、程式編碼到阿拉伯語文訓練，還會訓練情報蒐集、分析等，並且定期舉辦模擬高壓訓練，培訓結束後這些人會被分發到8200部隊的子單位服務，可能會被賦予不同工作，但大致還是會與原本受訓專長性質的工作相同，基本上在這個單位平均服役年限為4年（可自願延長役期），年度約以25%的比例遞補，而這些成員在退役之後，會成為預備役回到社會從事各行各業或者繼續就讀大學，[43] 並且每年要回到部隊實施3週的進修培訓，直到年滿40歲為止；除此之外，8200部隊退伍軍人會創立協會，來協助學校的畢業生與退伍軍人就業服務，為各公司來招聘人才投入各種產業。

伍、對我防衛作戰省思

中共領導人習近平主席自2012年執政以來，以復興民族主義為出發點，提出「中國夢」核心主義，企圖終結百年國恥，確立「強軍夢」的國家重要戰略，而臺灣自1895年清末甲午戰爭馬關條約割讓日本後，直至1949年國民政府輾轉到臺灣，對於中共而言，臺灣期間均未回歸大陸版圖，所以視為終結百年國恥的最終密碼，假使臺灣一日不

41 John Reed, "Unit 8200: Israel's cyber spy agency," *Financial Times*, July 10 2015, <https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c>（檢索日期：2022年3月20日）

42 財團法人國防安全研究院，〈網路作戰〉，《國防情勢特刊》，第13期，2021年11月9日，頁38。

43 Sean Cordey, "The Israeli Unit 8200 An OSINT-based study," Center for Security Studies, p. 14.

回歸大陸，就代表著將持續百年國恥，這也就是中共不惜一切代價堅持兩岸統一的最主要原因，並且在中共十九大報告中清楚表示「兩個一百年」的目標，「十四五規劃」與「2035年遠景目標綱要」提出2027年「建軍百年」願景；[44] 維持兩岸之間的和平穩定已經是國際共識，世界各國對於臺海安全均維持高度關注，我國位於「島嶼戰略」第一島鏈重要位置，積極防範極權主義入侵及擴張的前線，國軍以提升自我防衛能力與建構安全屏障為目標，期能堅實國防戰力，確保臺灣周邊海、空域交通線暢通。[45]

2022年2月，當俄羅斯於烏克蘭邊境集結軍隊時，就可以預判俄國將以大規模、破壞性的網路攻擊，之後隨著2月24日俄烏戰爭爆發，俄羅斯對烏克蘭關鍵部門進行持續的攻擊，但大多數都被證明是無效的，而烏國的指揮和能力基本上也沒有因此而中斷，是因為該國有志願網路戰士軍隊協助防禦和進攻，他們已證明是烏克蘭全面防禦的關鍵要素，所以政府功能僅發生了輕微的影響；網路作戰需要時間來發展，必須制定強有力的計畫並明智地選擇目標，對銀行、電網和通信基礎設施的攻擊具有破壞性，但不是決定作戰勝利的關鍵因素，[46] 我們可以清楚瞭解在俄烏戰爭模式下，中共仍會積極運用其國力，擴大地緣政治影響力，以混合戰、聯合封鎖作戰、聯合火力作戰及全面作戰等方式，達到解放臺灣之目的，但所使用的手段不會脫離不對稱作戰概念、資訊作戰、網路作戰、認知空間作戰等運用方式，若我國不持續強化建軍整備、國防自主而讓中共取的全方面優勢，或內部出現權力真空混亂時，則為求轉移大陸人民注意力，進而激發民族主義情緒，以武力訴求解決兩岸問題的可能性就大增。就當前兩岸情勢，共軍對臺不對稱作戰即以首戰就是決戰方式展開，兩岸一旦開啟戰爭，共軍會以戰略、戰役、戰術等行動相互緊密配合，運用特種空降突襲作戰及先期滲透的情報人員，對我國的作戰重心指揮系統進行高強度密集點穴作戰，癱瘓並干擾電子、交通、通信、監偵、防禦體系，在外國勢力尚未介入的狀況下，令我政、經、軍、心防禦體系瓦解，並且在短時間內無法平衡恢復，使首戰迅速發展成決戰，以減低作戰發展的不確定因素。以下就我國當前處境提出建議。

一、發展AI不對稱作戰

面對戰爭型態的改變，可以按照裝備種類區分冷兵器、熱兵器、機械化、訊息化等四種戰爭時代，而當戰場上廣泛運用AI技術時，可以推動智能化戰爭加速進入一種新戰爭型態，這個時候智能化的指揮、作戰方式、裝備、維修等作戰方式，將超越兵力、火力、資訊力與機動力成為主要趨勢，並且是決定作戰成敗的關鍵力量，[47] 從以色列8200部隊可以清楚瞭解處理大量的情報資料中，軟體運用是扮演相當重要的一環，透

44 中華民國110年國防報告書編纂委員會，《中華民國110年國防報告書》，2021年10月，頁26。

45 中華民國110年國防報告書編纂委員會，《中華民國110年國防報告書》，頁32。

46 Emily Harding, "The Hidden War in Ukraine," *CSIS*, June 15, 2022, <https://www.csis.org/analysis/hidden-war-ukraine>（檢索日期：2022年7月7日）

47 蕭介雲，〈智慧國防靠AI中科院啟動十年大計〉，《新新聞網》，2019年9月19日，<https://www.new7.com.tw/NewsView.aspx?t=03&i=TXT20190912103315WIS>（檢索日期：2021年12月20日）

過不同的AI可以快速串連情報資料與決策分析；將AI運用在最近幾年國人最關心的共機（艦）常態化繞臺威脅上，當偵測到敵方動態時，透過整合情資就能立即分析其目的、隸屬單位、威脅範圍、過去訓練狀況等重要參數資料，做為威脅預判與戰場管理的參考，另外建立國防雲端系統將各聯合作戰與行政管理系統分層管制鏈結起來，透過各大數據分析、研判，可有效降低共同協調與作業時間，以面對未來快速的戰爭節奏。[48]

以運用AI結合情監偵系統為例，即便是無人載具也是需要地面人員導控，根據回傳的雷達、影像、聲紋資料做人工處理，耗時冗長不符作戰效益，未來國防部可結合國內科技產業共同研究，研發可以朝向從偵查到攻擊的過程中，透過AI經由自我學習過濾有意義的訊息，可以大幅減少武器系統反應時間，[49] 以色列鐵穹防空系統就是最好的範例，有效減低百姓傷亡與財產損失，因此人力不再是戰爭勝負的關鍵；另外臺灣以及外離島地區海岸線較長，在人力不足的情況下容易產生危安盲區，雖然政府計畫以光電監視系統補足，但還須倚靠傳統人力判斷，未來如可結合AI系統判讀影像資料，可大幅減少人工情資判讀時間，更進一步取代傳統光電監視器；最後就是發展無人機的「滯空攻擊彈藥(Loitering Munition System)」，這類系統會依造預先設定的程式在目標區上空巡弋，一旦發現目標就會依照指令追蹤監視、即時影像回傳與攻擊目標。[50]

然而遏制敵人發動戰爭的行為其實也是一種「嚇阻」的方式，我國雖然缺乏大國的科技實力，因此只有往其他「不對稱」手段來反制，尤其是資訊科技的不對稱所導致的威脅，已經成為今日「不對稱作戰」重要的一環，因此我國只要在各方面展現出強大實力，讓敵人可以清楚知道輕易挑起戰爭，自己本身將可能受到極大的報復與損害，以符合我國對於「不對稱作戰」的概念，進而達到「不戰而屈人之兵」的最高境界。

二、資訊安全轉型主動源頭打擊

英國於2010年10月發表的國防戰略與安全評估(The Strategic Defence and Security Review, SDSR)中，「國際恐怖行動」、「國際軍事危機」、「網路攻擊」及「大型天然災害」等4項為最具影響國家安全，其中網路攻擊僅次於恐怖攻擊行動，由此可知網路資訊安全防護不可輕忽，通常一般人認為資訊網路安全範疇即是防止外來駭客滲透侵入，但這個觀點並不完全可以涵蓋全部，[51] 就整體資安管理系統而言，防護大致可以區分管理層面及技術層面兩個部分，在管理層面主要以建立防火牆、設置防毒軟體與偵測入侵硬體等，而在技術層面部分，舉凡下載修補

48 Lindsey R. Sheppard, "Fly-Fight-AI: Air Force Releases New AI Strategy," *CSIS*, September 13, 2019, <https://www.csis.org/analysis/fly-fight-ai-air-force-releases-new-ai-strategy>（檢索日期：2021年11月20日）

49 紀永添，〈紀永添專欄：臺灣如何建構未來的不對稱戰力〉，《上報網》，2018年4月2日，<https://www.upmedia.mg/news_info.php?SerialNo=37799&Type=2>（檢索日期：2021年12月23日）

50 王臻明，〈先發射再瞄準：改變傳統戰術的繞行式械彈系統〉，《鳴人堂網》，2021年5月4日，<https://opinion.udn.com/opinion/story/120873/5291844>（檢索日期：2021年12月23日）

51 James Andrew Lewis, "Dismissing Cyber Catastrophe," *CSIS*, August 17, 2020, <https://www.csis.org/analysis/dismissing-cyber-catastrophe>（檢索日期：2021年11月20日）

漏洞程式、瀏覽安全網頁、不要開啟來路不明網路郵件、定期更新密碼、防毒軟體等，而網路資訊安全的目的是要有機密性、可用性與完整性，面對現代化訊網路作戰，上述主要防護方式雖然可以大幅降低外來攻擊，但對於整體而言仍有待加強，[52] 主要原因是防護方式大多屬「被動式」，缺乏網路攻擊的「主動防護」要素，而以色列在網路防禦方面，它在本質上更具有「攻擊性」，著重於特定的攻擊者與攻擊手段。[53]

以俄烏戰爭為例，不只在軍事行動中產生人員傷亡與經濟損失，俄羅斯陸續的網路攻擊更是接連不斷，相關的政府部門、關鍵基礎設施、軍事單位、電視臺、學術機構，都是網路攻擊的目標。[54] 烏克蘭國家特殊通信和信息保護局報告稱，在3月23日至29日期間，其關鍵基礎設施發生了65次網路攻擊，美國微軟公司也證實從戰爭開始到4月8日，俄羅斯支持的駭客組織對烏國發起了200多次網路攻擊，其中37次具有破壞性，且永久破壞了數十個組織的數百個系統中的文件。甚至有駭客竄改烏克蘭網站，宣布該國已經投降的假訊息影響民心，很明顯看得出來俄羅斯的目標似乎很簡單，就是要破壞人民對烏克蘭政府的信心；[55] 而烏克蘭在2月26日也在網路徵求具網路資訊專長人員，企圖針對俄羅斯關鍵基礎機構及軍事目標予以還擊報復。[56]

所謂「知彼知己，百戰不殆」，建立網路資訊戰能力，首先要知道敵方運作方式與網路駭客的心理與行為。因此我國可以藉由臺灣的資訊電子產業優勢，結合國內民間企業能量發展，藉與國內產官學研業者與專家定期研討分析與未來發展趨勢，[57] 發展以資訊網路戰為主的不對稱作戰能力，透過戰略支援部隊與民間網軍、駭客，持續對敵執行政經網戰、民間基礎設施擾亂戰，尋找程式漏洞及潛伏病毒，伺機癱瘓整體運作，直接打擊癱瘓對敵網路攻擊源頭，轉化防禦成為主動，不但可以對我國基礎關鍵設施先制防護，更可以提升整體防護作戰能力。

臺灣具有高科技資訊人才，技術及網路防護實務經驗豐富，應整合公私部門與法治運作，建立商用衛星、數位化通訊、公共網路平臺，並結合友盟增進資安科技交流及情資分享；另整合中華電信及民營通資系統，納入國軍備援體系，並常態化實施跨部會網路攻防實戰演練，強化整體資通戰力與應變能力。

三、強化資通電軍網路作戰特質

52 簡華慶，〈網路資訊戰所扮演角色及因應策略之研究〉，《國防雜誌》，第27卷，第1期，2012年，頁131。

53 Dmitry (Dima) Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy," *The Washington Quarterly*, Vol. 40, No. 2, Summer 2017, p. 118.

54 Seth G. Jones, "Russia's Losing Hand in Ukraine," *CSIS*, February 18, 2022, <https://www.csis.org/analysis/russias-losing-hand-ukraine>（檢索日期：2022年3月10日）

55 Emily Harding, "The Hidden War in Ukraine," *CSIS*, June 15, 2022, <https://www.csis.org/analysis/hidden-war-ukraine>（檢索日期：2022年7月7日）

56 周峻佑，〈資安週報：2022年3月1日至4日〉，《iThome網》，2022年3月5日，<https://www.ithome.com.tw/news/149711>（檢索日期：2022年3月28日）

57 簡華慶，〈網路資訊戰所扮演角色及因應策略之研究〉，頁136。

以色列—美國網路安全公司Check Point於5月18日發布的一份有關俄烏戰爭的報告，內容表示俄羅斯許多郵件是由中共支持的駭客發出的，目的是誘使目標人員下載並打開含有惡意程式的文件。這行動通常只有國家支持的情報機構才會使用的能力；使用的方法和代碼類似於以前與中共有關的駭客組織所使用的攻擊。[58] 該報告更凸顯，中共網路間諜的大規模資訊收集策略愈發精細，其目標範圍不斷擴大。另也發現中共的攻擊似乎專注於收集資訊和知識產權，而不是製造混亂或破壞，顯示中共積極從俄烏戰爭吸取經驗，為未來戰爭預作研究與準備。為提升國軍資訊作戰能力，我國資通電軍指揮部於2017年6月29日正式成軍，其任務平時統合國軍網路、電子及資通平臺等三大領域，執行網路空間安全維護、電磁頻譜偵蒐及指管系統建立與維運，以支援國軍資通安全緊急應變，確保各項指管系統暢通，戰時除依令執行國軍資通安全防護任務外，並協防國家關鍵資訊基礎設施，以確保國家安全，此將超越傳統的空中、海域及地面的防衛概念，成為重層嚇阻戰略下的第一層嚇阻兵力；以色列國防軍將網路安全視為軍事戰略的一部分，並建立其網路指揮的組織與專業性，[59] 鑑於網路空間難以界定平時及戰時，而網路作戰也不容易區分前線及後方，再加上網路攻擊因駭客間諜均以偽冒手段，利用程式去建立假IP數據封包，讓看起來像組織網路內合法的有效位址，以利修改、改變路由或刪除資料，背後身分虛實真假不易溯源，當國內關鍵基礎設施受到網路攻擊時，可以仿效以色列8200部隊負責抵禦外來軍事及非軍事網路威脅任務，充分結合民間資源能量，與國內防毒軟體公司及具專長人員技術合作，針對國內重要基礎設施及重要軍事設施，透過各種模擬連續網路病毒攻擊、癱瘓，找出系統漏洞與潛藏病毒予以修正，藉以提升資訊網路防護強度；另網路作戰通常具備情報的本質，經研究發現網路作戰大多是採用境外前進部署或主動防禦作為，主要是因為網路作戰與情報本來就是無法切割，以美國為例，國家安全局與網路作戰司令部即是同一組人馬，而地處中東地區的以色列有90%情報均來自8200網路部隊，[60] 使各級指揮官可以獲得更多戰場資訊，並對敵人的位置與以色列國防軍在戰場部隊，產生共同全方面的詳細評估，[61] 除了具有早期情報預警的功能外，更是可以透過境外網路先制攻擊達到威嚇效果，在我國雖然有民主監督情報機制爭議，但至少要可以具備在境內從事主動防禦的空間與彈性。[62]

四、發展認知空間作戰

認知空間作戰的目的就是要結合心理戰、輿論戰，再加上透過網路媒體的宣傳戰及訊息戰等綜合操控模式，形塑對我有利

58 Ronen Bergman, Kate Conger，〈報告稱中國駭客試圖竊取俄羅斯國防數據〉，《紐約時報中文網》，2022年5月20日，<https://cn.nytimes.com/china/20220520/china-hackers-russia/>（檢索日期：2022年5月23日）

59 Deborah Housen-Couriel, "National Cyber Security Organisation: Israel," *NATO CCD COE*, March 2017, p. 14.

60 Jasper Frei, "Israel's National Cybersecurity and Cyberdefense Posture," September, 2020, p. 16.

61 Gadi Eizenkot, "Cyberspace and the Israel Defense Forces," *Cyber, Intelligence, and Security*, Vol. 2, No. 3, December, 2018, p. 103.

62 財團法人國防安全研究院，〈網路作戰〉，《國防情勢特刊》，第13期，2021年11月9日，頁35。

的條件，改變敵人的認知，進而達到改變行為，當前的戰爭型態發展快速，難以區分平、戰時均可發起攻擊，不受作戰平臺限制。所以為避免武力衝突，近幾年世界各國已將戰場已經逐漸轉移到社群網路，舉凡YouTube、TikToK頻道或FaceBook、Twitter網路社群論壇，都已經開始瀰漫著戰火的煙硝，意圖奪取民眾對事件的認知及詮釋的話語權，所以我們可以瞭解到認知空間作戰的攻擊大都是來自境外或敵對國外勢力，且行動是有組織並經過有效的協調，最後其背後都會有特定的目的或動機；過去相互擁核國家將力求避免直接軍事對抗，而導致相互報復性毀滅，故更能確認發展認知空間作戰是首選戰場；[63] 另外烏克蘭總統澤倫斯基(Volodymyr Zelenskyy)運用資訊作戰向各國國會發表演說，適時發布俄烏戰爭中，烏國人民遭受到屠殺等即時戰況，以認知作戰手段向世界增取到國際奧援。

因此我們也可以清楚知道認知空間作戰，並不是僅可以單獨依靠國防力量獨力完成，而是要提升到國家整體力量，統合國內各部會以發揮所長，並透過製造並散播虛假且有爭議性訊息，讓敵人對過去的認知產生懷疑，進而擴大其內部的分化與對立，消耗敵對國家的國力，達到不戰而屈人之兵目的；然要達到此作戰目的，通常可以透過傳統媒體與網路這兩種方式，來操控敵對國家的國內輿論，前者可以拉攏國際間具權威的新聞媒體，闡述我國是歷史的正統與自由民主是普世價值，並且透過後者網路散播政府的貪腐、人權遭剝奪打壓、國家對於天災沒有因應措施、國內人民對政策反感等訊息，都可以有效地消耗對方的正常運作。當然，所使用的訊息可能是正確的，但更多的是真假各半，亦或者是完全抹黑的虛假內容，進而造成敵對國家內部局勢動盪搖擺、人民意見分歧。

五、培育人力平戰結合

世界各國的專業化網路作戰部隊對於人力的選用較不易，隨著網路威脅態樣變化，也需要逐漸調整與轉向，以面對未來敵人做好準備，然而著重在網路人才培養是主要關鍵，並且人員退伍後要如何結合民間產業持續發展國防產業，戰時納入後備動員能量充實戰力。未來我國可以學習色列的提前部署方式，自高中、大學開始資助培訓相關專長人才，畢業後加入資通電軍部隊，經過長時間、高強度的密集訓練，研習網路攻擊、網路防護、電子工程、通信、加解密、訊號情報、情報分析等高壓訓練，完訓後就自己本身的專長運用在網路作戰方面，退伍後在保密安全無虞的情況下，可以輔導他們選擇加入高科技相關職場公司，繼續深造其網路專長。透過能量潛藏於民間，透過與民間協調夥伴關係，共同識別、抵禦、檢測、應對攸關國家安全與基礎設施等的網路駭客惡意攻擊，進而提高國家資訊安全防護及緊急應變能力；亦可循後備體系使人才軍文交織歷練，藉不同的職務重新檢視任務範圍是否還有改善的方向，以提升組織工作效能，戰時動員選充返回原部隊補充戰力，如此更有助於軍方與民間的技術交流，這樣完善的職涯規劃更能吸引優秀青年積極加入資通電軍部

63 James Andrew Lewis, "Cognitive Effect and State Conflict in Cyberspace," *CSIS*, September 26, 2018, <https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace>（檢索日期：2022年7月4日）

隊。[64]

陸、結　　語

從2022年俄烏戰爭初期發現，雖然烏克蘭軍力遠不如俄羅斯，但卻已經徹底改變將俄國速戰速決作戰計畫，改變為持久作戰的城鎮戰方式，其中運用無人機執行通訊、偵察等任務，靈活不對稱作戰，隨著網路科技的快速進步，電腦與網路的使用日漸普遍，而網路戰成為世界各先進國家關注焦點，甚至被認定為未來戰爭主流的第五戰場。網路安全的重要性主要有三項：第一，在現實環境中，存在具敵意蓄意傷害、竊取的反社會行為者，第二，逐漸依賴數位科技完成生活中的社會職能，第三，無論如何精心設計數位科技系統，都還是有不可避免的弱點，[65]然而現今資訊網路作戰型態已經沒有平時及戰時區分，更沒有空間與時間的限制，只要駭客透過網路攻擊，輕則竊取個資、財務，重則國家機密資料外洩、指揮體系癱瘓。[66]因此發展以資訊網路戰為主的不對稱作戰能力，轉化防禦成為主動，直接打擊癱瘓對敵網路攻擊源頭更可以提升整體防護作戰能力。

現代戰爭中的決勝關鍵即是結合戰術戰法的網路作戰，網路作戰主要在戰力整合，但是近年來中共透過網路、電子、平面及廣播媒體引起國內民眾畏戰心理，而仍持續研究資訊網路作戰的理論、戰術、戰法及戰具，並藉由各種演訓進行驗證，對於我國新成立的資通電軍指揮部，無論在建軍規劃、聯合作戰定位、戰備任務、教育訓練與其他軍種協調等，都還要相互磨合及驗證，面對未來的新型戰爭型態及各種作戰空間環境，不僅是要國軍做好準備，而是全體國民都要做好準備，以堅定愛國抗敵意志，除了參酌以色列實戰成功經驗外，要從延攬優秀的網路人才，並整合產、官、學、研等能量，才可以憑藉資安防護網，確保關鍵基礎設施與軍事安全。

（收件：111年5月23日，接受：111年7月28日）

64 財團法人國防安全研究院，〈網路作戰〉，《國防情勢特刊》，第13期，頁39。

65 曾于蓁，〈網路安全對國家安全之重要性：以臺灣的網路安全為例〉，《發展與前瞻學報》，第30期，2020年12月，頁8。

66 吳嘉龍，〈網路科技發展與資訊安全管理研究探討〉，《危機管理學刊》，第10卷，第2期，2013年9月，頁84。

參考文獻

中文部分

專書譯著

John B. Alexander著，楊連仲譯，2001/4。《使用非致命性武器的未來戰爭》。臺北：國防部史編局。

Steven Metz著，謝凱蒂、楊紫函、蔣永方譯，1990。《21的武裝衝突：資訊革命與後現代戰爭》(Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare)。臺北：國防部史政編譯局。

期刊論文

李晧、張瑞麟，2012/3。〈「不對稱作戰」之發展探討〉，《海軍學術雙月刊》，第46卷，第3期，頁35。

李承禹，2007/12。〈中共網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用〉，《復興崗學報》，第90期，頁252。

吳嘉龍，2013/9。〈網路科技發展與資訊安全管理研究探討〉，《危機管理學刊》，第10卷，第2期，頁84。

張祥山，2006/4。〈非傳統不對稱安全威脅初探〉，《展望與探索》，第4卷，第4期，頁35。

曾于蓁，2020/12。〈網路安全對國家安全之重要性：以臺灣的網路安全為例〉，《發展與前瞻學報》，第30期，頁8。

黃惟喬，2004。〈不對稱作戰對現代戰爭的影響〉，《國防大學軍事學部論文集》，桃園：國防大學，頁46-47。

蔡昌言、李大中，2007/7。〈不對稱戰爭相關理論及其應用於中國對鼎戰略之研析〉，《遠景基金會季刊》，第8卷，第3期，頁1-35。

謝游麟，2009/9。〈孫子「不對稱」思想對國軍軍事戰略之啟示〉，《國防雜誌》第24 卷，第5期，頁8。

簡華慶，2012/1。〈網路資訊戰所扮演角色及因應策略之研究〉，《國防雜誌》，第27卷，第1期，頁131。

學位論文

曹潤生，2006/1。《冷戰後中共資訊戰之發展》。臺北：淡江大學國際事務與戰略研究所碩士在職專班。

官方文件

中華民國110年國防報告書編纂委員會，2021/10。《中華民國110年國防報告書》，頁26-32。

財團法人國防安全研究院，2021/11/9。〈網路作戰〉，《國防情勢特刊》，第13期，頁35-39。

網際網路

王臻明，2021/5/4。〈先發射再瞄準：改變傳統戰術的繞行式械彈系統〉，《鳴人堂網》，<https://opinion.udn.com/opinion/story/120873/5291844>。

朱雪玲、曾華鋒，2017/10/17。〈制腦作戰：未來戰爭競爭新模式〉，《解放軍報》，<http://www.81.cn/jfjbmap/content/2017-10/17/node_12.htm>。

周峻佑，2022/3/5。〈資安週報：2022年3月1日至4日〉，《iThome網》，<https://www.ithome.com.tw/news/149711>。

紀永添，2018/4/2。〈紀永添專欄：臺灣如何建構未來的不對稱戰力〉，《上報網》，<https://www.upmedia.mg/news_info.php?SerialNo=37799&Type=2>。

夏洛山，2021/6/5。〈以國神祕部隊曝光AI首次介入戰爭〉，《大紀元網》，<https://www.epochtimes.com/b5/21/6/5/n13001442.htm>。

愛伊米，2021/2/27。〈以色列網路武器的興起〉，《德若資訊網》，<https://iemiu.com/zh-tw/history/36282.html>。

蕭介雲，2019/09/19。〈智慧國防靠AI中科院啟動十年大計〉，《新新聞網》，<https://www.new7.com.tw/NewsView.aspx?t=03&i=TXT20190912103315WIS>。

外文部分

期刊論文

Aviezer; Shapira, Amikam, 2002. "וזגמ :חוּנ מלמ וזיעידומ וחטיבו וזיעידומה תשרומל זכרמהמ ז," Yaari, No. 30, p. 6.

Adamsky, Dmitry (Dima), Summer 2017. "The Israeli Odyssey toward its National Cyber Security Strategy," *The Washington Quarterly*, Vol. 40, No. 2, p. 118.

Couriel, DeborahHousen-, 2017/3. "National Cyber Security Organisation: Israel," *NATO CCD COE*, p. 14.

Cordey, Sean, 2019/12. "The Israeli Unit 8200 An OSINT-based study," *Center for Security Studies*, pp. 9-14.

Eizenkot, Gadi, 2018/12. "Cyberspace and the Israel Defense Forces," *Cyber, Intelligence, and Security*, Vol. 2,. No. 3, p. 103.

Frei, Jasper, 2020/9. "Israel's National Cybersecurity and Cyberdefense Posture," p. 16.

Frei, Jasper, 2020/9. "Israel's National Cybersecurity and Cyberdefense Posture," pp. 14-15.

K. SAALBACH, 2011/11. "Cyber war method and practice" V.3.0, p. 3-5.

Kitron, Rafi, 2013/2. "ירבדמה רודב הנד היגלטסונה יניס רוזאב כ"בשה ירגוב לש," *Malam View*, Vol. 65, pp. 6-10.

Lapid, Ephraim, 2012/10. "תמחלמב יברק וזיעידומ לע לילגב סולשה," *Malam View*, Vol. 64, p. 38.

Tabansky, Lior, Winter 2020. "Israel Defense Forces and National Cyber Defense," *Connections*, Vol. 19, No. 1, pp. 49-55.

網際網路

Aviv, Tel, 2012/11/2. "Israel builds up its cyberwar corps," UPI, <https://www.upi.com/Defense-News/2012/11/02/Israel-builds-up-its-cyberwar-corps/52421351881449/>.

Cohen, Avner, 2017/6/5. "The 1967 Six-Day War," *Wilson Center*, <https://www.wilsoncenter.org/publication/the-1967-six-day-war>.

Cordesman, Anthony H., 2010/6/29. "The Arab-Israeli Military Balance in 2010," *CSIS*, <https://www.csis.org/analysis/arab-israeli-military-balance-2010>.

Dahm, Mike, 2021/3. "The Reality of War Should Define Information Warfare," *U.S. Naval Institute*, <https://www.usni.org/magazines/

proceedings/2021/march/reality-war-should-define-information-warfare>.

Erman, Sarah, 2022/4/27. "Trellix Finds Escalation of Cyberattacks Targeting Critical Infrastructure as Geopolitical Tensions Rise," *Trellix*, <https://www.trellix.com/en-us/about/newsroom/news/news-detail.html?news_id=2019cc26-3450-4b0d-b238-82d49348dcb7>.

Gabidullina, Roksana, 2021/3/12. "The Future of U.S.-Russian Arms Control: Principles of Engagement and New Approaches," *CSIS*, <https://www.csis.org/analysis/future-us-russian-arms-control-principles-engagement-and-new-approaches>.

Harrison, Todd, 2021/8/5. "Battle Networks and the Future Force," *CSIS*, <https://www.csis.org/analysis/battle-networks-and-future-force>.

Harding, Emily, 2022/6/15. "The Hidden War in Ukraine," *CSIS*, <https://www.csis.org/analysis/hidden-war-ukraine>.

Jones, Seth G., 2022/2/18. "Russia's Losing Hand in Ukraine," *CSIS*, <https://www.csis.org/analysis/russias-losing-hand-ukraine>.

Lewis, James Andrew, 2019/6/25. "Iran and Cyber Power," *CSIS*, <https://www.csis.org/analysis/iran-and-cyber-power>.

Lewis, James Andrew, 2020/8/17. "Dismissing Cyber Catastrophe," *CSIS*, <https://www.csis.org/analysis/dismissing-cyber-catastrophe>.

Lewis, James Andrew, 2011/7/11. "Cyber Attacks, Real or Imagined, and Cyber War," *CSIS*, <https://www.csis.org/analysis/cyber-attacks-real-or-imagined-and-cyber-war>.

Lewis, James Andrew, 2018/9/26. "Cognitive Effect and State Conflict in Cyberspace," *CSIS*, <https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace>.

McNamara, Robert, 2020/2/21. "The Yom Kippur War of 1973," *ThoughtCo*, <https://www.thoughtco.com/yom-kippur-war-4783593>.

Reed, John, 2015/7/10. "Unit 8200: Israel's cyber spy agency," *Financial Times*, <https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c>.

Sof, Eric, 2022/3/31. "Operation Orchard: Bombing of the Syrian Nuclear Reactor," *Spec Ops Magazine*, <https://special-ops.org/operation-orchard-bombing-syrian-nuclear-reactor/#google_vignette>.

Sheppard, Lindsey R., 2019/9/13. "Fly-Fight-AI: Air Force Releases New AI Strategy," *CSIS*, <https://www.csis.org/analysis/fly-fight-ai-air-force-releases-new-ai-strategy>.

TeamT5 Media Center, 2021/7/1. "Another CloudDragon attack abusing VPN zero-day vulnerability to target South Korean entities," *TeamT5*, <https://teamt5.org/en/posts/another-clouddragon-attack-abusing-vpn-zero-day-vulnerability-to-target-south-korean-entities/>.