

以公開來源情報分析中共軍事活動的 適用性與限制

董慧明

國防大學政治作戰學院中共軍事事務研究所副教授

摘 要

隨著公共領域中的公開來源情資管道愈來愈多，以及數位資訊、網路、大數據技術的普及和迅速發展，國家安全情報工作作法已從傳統的秘密情報手段，向公開來源情報領域擴展。本文聚焦公開來源情資應用和情報處理方式，並以近期攸關臺海安全和中共軍事威脅之 5 則案例，深入探討公開來源情資的適用性和侷限性。透過文獻和實務經驗的綜合研究，可以明確公開來源情報的有效獲取，已成為國家安全工作重點。然而，研究也發現公開來源情資雖能對情報工作者提供目標對象和議題之即時、有利線索，若要更深入地全般掌握動態詳情，仍有其盲點，需要其他情報手段輔助。尤其為求客觀、精準產製情報產品和服務情報用戶，公開來源情報和秘密情報的作業應為互補關係，方能發揮有效預警和趨勢判斷功能，進而及時做好因應和風險管控、危機處理，使國家安全工作更臻周延、完備。

關鍵詞：公開來源情報、秘密情報、國家安全、情報研析、解放軍

The Applicability and Limitations of Using Open Source Intelligence (OSINT) to Analyze the People's Liberation Army's Military Activities

Hui-Ming Tung

Associate Professor, Graduate Institute of China Military Affairs
Studies, Fu Hsing Kang College, National Defense University

Abstract

As the number of Open Source Intelligence (OSINT) channels in the public domain increases, and with the popularity and rapid development of digital information, the internet, and big data technologies, national security intelligence work practices have expanded from traditional secret intelligence methods to the OSINT domain. This paper focuses on the use of OSINT and its processing methods and uses five recent cases related to Taiwan Strait security and PRC military threats as in-depth examples to explore the applicability and limitations of OSINT. Through a comprehensive study of literature and practical experience, the effective acquisition of OSINT has become a key focus of national security intelligence work. However, the research also found that although OSINT can provide timely and advantageous clues to intelligence workers about the target and issues, if a deeper understanding of dynamic details is desired, there are still blind spots that require assistance

from other intelligence methods. To produce and serve intelligence products and services to users objectively and accurately, the operation of OSINT and secret intelligence should be complementary to each other, to effectively perform early warning and trend judgment functions, and then timely respond to and risk control, crisis handling, to make national security work more comprehensive and better.

Keywords: Open Source Intelligence (OSINT), Secret Intelligence, National Security, Intelligence Analysis, People's Liberation Army (PLA)

壹、前言

在國家安全情報領域中，無論是傳統安全或是非傳統安全，秘密情報 (secret intelligence)、公開來源情報 (Open Source Intelligence, OSINT) 向來是研究重點。其中，秘密情報透過隱蔽蒐集和獲取手段，大量運用於政治、外交、軍事等攸關國家重大安全利益方面，因此往往需要透過專業的情報人員訓練、強大的監測、偵察裝備，方能適時取得最具信度、效度之情資 (information) 供作研析、決策之用。從學理方面而論，這種類型的情報主要可區分為人員情報、通信情報、圖像情報、電子情報、訊號情報，¹ 是每個國家最為核心、保密的畛域。

然而，隨著國家安全威脅的性質愈趨複雜、面向愈來愈廣泛，透過公開管道掌握特定議題、情勢的變化，也隨著資訊科技、網路的普及運用而讓情報蒐集的方式趨於多元。以當前備受全球高度關注的臺海安全議題為例，從 1954 年、1958 年、1996 年的三次臺海危機，² 到 2022 年 8 月美國眾議院議長裴洛西 (Nancy Pelosi) 訪臺後，中國人民解放軍（以下簡稱「解放軍」）宣布在臺灣周邊進行「多兵種聯合戰備警巡和實戰化演練」，³ 恰好可

* 本文探討中共軍事活動公開來源情報，所涉資料中的簡體字係考量原始資料之真實性而未做修改，特別予以說明。

¹ Robert M. Clark, *Intelligence Collection* (Washington DC: CQ Press, 2013), p. 13.

² 〈臺灣海峽歷次危機回顧：從一江山島戰役、八二三砲戰到飛彈危機，看美中臺三角關係演繹〉，《BBC 中文》，2020 年 8 月 26 日，〈<https://www.bbc.com/zhongwen/trad/chinese-news-53834569>〉。

³ 〈東部戰區在臺灣周邊海空域組織多軍兵種聯合戰備警巡和實戰化演練〉，《中華人民共和國國防部》，2022 年 8 月 26 日，〈<http://www.>

以充分說明傳統的秘密情報處理、判斷、解決危機的作法，以及加上應用公開來源情報蒐整各方輿情變化的全般過程。不可諱言的是，這四次中共對臺的砲擊、飛彈試射，以及實戰化演訓，同時涵蓋了對當面敵情的秘密蒐集、查證，以及在公開來源管道的過濾可用訊息和政策立場的事實澄清。在虛實交錯的安全環境中，雖有千真萬確的情報，卻也混雜許多各式各樣欠缺參用價值的訊息。基於對這些關係著國家安全情報來源的適用和侷限性思考，成為主要的研究動機。

情報研究領域既深且廣，本文關注公開來源情報，是基於深入探討在形成情報產品、服務情報用戶前，作為敵情分析和國家安全情報工作人員會面對哪些機會和挑戰。如同曾擔任美國海軍陸戰隊情報官的斯蒂爾 (Robert Steele) 在《國家情報和公開來源：從校舍到白宮》(National Intelligence and Open Source: From School House to White House) 一文中所提到：非秘密性的公開訊息約占美國情報來源的 40% 至 95%。⁴ 其中，來自戰地記者、外國媒體、專家、地圖和衛星圖像，對於安全防務部門而言，都是在危機和軍事行動中非常重要的公開訊息來源管道。⁵ 時至今日，公開來源情報的出處已擴及各種明、暗網域之網站、社群媒體和

mod.gov.cn/power/2022-08/26/content_4919478.htm>。

⁴ Robert D. Steele, "National Intelligence and Open Source: from School House to White House," *American Intelligence Journal*, Vol. 14, No. 2 (Spring/Summer, 1993), pp. 29-32.

⁵ Robert D. Steele and Mark M. Lowenthal, "Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations," *Defense Daily Network Special Report*, May 5, 1998, <<https://irp.fas.org/eprint/oss980501.htm>>.

特定功能資料庫。當公開來源情報的價值與日俱增，發揮功用愈來愈大，已和秘密情報形成互補關係，具有重要研究意義和價值。

為了深入探討公開來源情報在國家安全工作中的實際運用情形，本文亦舉出 5 則案例，作為在中共軍事研究領域中，進行敵情研析所遇到的適用和侷限問題例證。透過公開文獻的梳理和實務工作經驗的實證，說明當前我國因應國家安全威脅應該如何認識和應用公開來源情報，進而避免盲點或誤導，提升情報的參用價值和精確性，確保國家安全利益。

貳、公開來源情報的定義和研究發展

在真正成為具有價值的情報前，情資來源的可靠性往往是情報研析人員最審慎重視的項目之一，且只要和情報部門指導要點相符，就算是公開來源情報仍有參用的重要性。因此，明確界定其概念對於國家安全情報工作自有其重要意義。亦即從情報蒐集之初的原始資料，到經過一定程序處理後的情資，再到經過處理確認可做進一步運用的情報，情資在情報處理過程中可謂原料和產品之間的關係。只要情資來源、內容無誤，對於政府部門危安預警、管控安全風險、危機管理皆有不可或缺的作用。

一、概念界定

公開來源情報強調非隱蔽地透過公開途徑蒐集和運用情報目標之公開訊息，是相對於「秘密情報」、「諜報」而言，一門從輿論資訊中蒐集、甄別和獲取資訊，並對其加以分析以得到可行、有價值的情報學問。其中輸入是「訊息」，而輸出卻是「情報」。⁶

⁶ 趙小康，〈公開源情報：在情報學和情報工作中引入 Intelligence 的思考〉，

因此，從公開的意義而論，公開來源情報有別於秘密情報工作中關於情蒐的方法、來源、或是情報運用後有關機密等級的定密、管理做法，在備受重視的趨勢下，亦有愈來愈明確的定義。例如：德國政治學者紹勒 (Florian Schaurer) 和資訊安全專家斯特格爾 (Jan Störger) 認為公開來源情報は為因應政府國家安全需求、面向特定情報用戶，從公開可得、合法獲得、可供大眾使用的訊息來源，經過蒐集、處理、分析、產製之工作循環流程，區分機密等級、傳送的情報。⁷

其次，依據美國「國家情報總監」(Director of National Intelligence)2006年頒布之「情報指令第301號」—《國家公開來源企業》(National Open Source Enterprise)文件，認為公開來源情報是指蒐集、分析和利用公開訊息，及時傳遞至相關情報需求對象、滿足特定情報需求之情報。⁸而2006年財政年度《國防授權法案》第931條(National Defense Authorization Act for Fiscal Year 2006)指出：公開來源情報は針對特定情報需求，由公開可得資料，經過蒐集、利用而進行情報產製，及時分發給適當的用戶。⁹再參考美國陸軍野戰準則FM2-0號《情報》(Army Field Manual FM 2-0: Intelligence)中關於「陸軍情報流程」乙節，也將公開來

《情報理論與實踐》，第32卷第2期（2009年2月），頁23。

⁷ Florian Schaurer and Jan Störger, “The Evolution of Open Source Intelligence (OSINT),” *Intelligencer: Journal of U.S. Intelligence Studies*, Vol. 19, No. 3 (Winter/Spring 2013), pp. 53-56.

⁸ Intelligence Community Directive Number 301, *National Open Source Enterprise*, July 11, 2006, <<https://irp.fas.org/dni/icd/icd-301.pdf>>.

⁹ “National Defense Authorization Act for Fiscal Year 2006,” Sec. 931, <<https://www.govinfo.gov/link/statute/119/3236>>.

源情報界定為將公開可得訊息加以有系統地蒐集、處理、分析，以獲得相關資訊，回應情報需求。¹⁰

再者，北大西洋公約組織 (North Atlantic Treaty Organization, NATO) 曾於 2001 年 11 月出版《公開來源情報手冊》(NATO Open Source Intelligence Handbook)，認為廣泛多元的公開訊息只要經過發現 (Discovery)、鑑別 (Discrimination)、萃取 (Distillation)、發送 (Dissemination) 之謹慎分析過程就能成為有價值的情報，因而視公開來源情報為情報科目之「根基」(Foundation)。¹¹ 另著名智庫「蘭德公司」(RAND Corporation) 於 2018 年 5 月 17 日，公布《為國防事業界定第二代公開來源情報》(Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise) 報告，除了將公開來源情報定義為來自公開訊息，經過蒐集、利用，並且及時傳送給適當的用戶的情報，並且認為網際網路和社群媒體的普及，已讓公開來源情報變得愈來愈冗繁。這份報告將 2005 年作為第二代公開來源情報的起始時間，也讓情報學界更加明確瞭解公開來源情報在資訊化環境下的作用，無論是情資蒐集的技術或是分析的方法，成為重點研究領域。¹²

¹⁰ Headquarters Department of the Army, "Army Field Manual FM 2-0: Intelligence," *FAS Intelligence Resource Program*, March 23, 2010, <<https://irp.fas.org/doddir/army/fm2-0.pdf>>.

¹¹ "NATO OSINT Handbook," *Internet Archive*, November, 2001, <<https://archive.org/details/NATOOSINTHandbookV1.2/mode/2up>>.

¹² Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018), p. 2.

從分析方法、分析手段和分析內容方面而論，公開來源和秘密情報的區分在於對情報來源是否公開的劃定。¹³ 因此，可適度公開的方法、手段和內容也在資訊網路環境愈來愈成熟的今日，應用變得愈來愈廣泛。只要合法地在公開訊息管道獲得可用資料，滿足情報工作需求，有助於將所有發現的訊息整理、分類、鑑定判斷為有用且可操作的情報，便達到公開、可用之前提要件。

二、公開來源情報之研究發展

無論是政治情報、經濟情報、商業情報、技術情報、軍事情報，情報皆有特定的服務對象。在傳統的國家安全情報研究領域中，過去往往有透過秘密途徑、手段獲取的情報才是真正具有價值、作用的偏誤認識。甚至認為公開來源情報可能來自於圖書館、網站資訊、社群媒體的公開訊息，少了神秘性，而被視為無關緊要且毫無用處的刻板印象。然而在實務工作中，情報既然是為特定對象服務，即表示此「對象」主要關注的是某一特定方面，對其有用的訊息。哪怕是在公開、眾人皆知的管道中得到有用的訊息，經過查證、鑑定程序，釐清是否為特定對象所需的某種特定訊息，對於該特定對象而言就是情報。儘管獲取途徑和秘密管道不同，惟公開來源情報能夠發揮的功用實際上並不亞於秘密情報，且情報工作者必須擔負的風險、代價也相對較低，凸顯出投入公開來源情報蒐集和研析在國家安全工作中的價值。

¹³ E. Ben Benavides, *Targeting Tomorrow's Terrorist Today (T4): Through Open Source Intelligence*, February 2009, <http://wikileaks.wikimee.info/gifiles/attach/8/8871_Targeting%20Tomo.pdf>.

情報界普遍認為這種透過公開管道獲取情報的工作方式可溯及 1941 年美國外國廣播新聞處 (Foreign Broadcast Information Service, FBIS) 的成立。¹⁴ 只是這種透過公開管道取得可用訊息的情報工作模式，仍是受到 2001 年美國發生 911 恐怖攻擊事件後，情報機關發現恐怖分子因藏匿於社會人群間不易被發現，呈現出難見、不確定性等特點，因而更加重視公開來源情報的作用。¹⁵ 自此，從公開來源管道獲取情資，成為美國國家安全相關部門不可或缺的情報工作方式。2005 年，美國聯邦政府在「國家情報總監」成立「公開來源中心」(Open Source Center)，¹⁶ 並以此為基礎於 2015 年 10 月更名為「公開來源企業」(Open Source Enterprise)。¹⁷ 該單位以網際網路作為情報主要來源，蒐集美國國內和國際間涵蓋政府部門、經濟、國防、軍事、社會、文化等各方面具有價值的情報內容。當前包括以秘密情報為主的「中央情報局」(Central Intelligence Agency, CIA) 亦成立「分析處」(Directorate of Analysis)，專責蒐集、研析包括新聞報導、社群媒

¹⁴ Department of Defense, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982, <<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/524001r.pdf>>.

¹⁵ Robert D. Steele, "Open Source Intelligence," in Loch K. Johnson, ed., *Handbook of Intelligence Studies* (New York: Routledge, 2007), pp. 147-165.

¹⁶ "Establishment of the DNI Open Source Center Press Release," *Central Intelligence Agency*, November 8, 2005, <<https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr11082005.html>>.

¹⁷ "Open-Source Center (OSC) Becomes Open-Source Enterprise (OSE)," *Federation of American Scientists*, October 28, 2015, <<https://fas.org/blogs/secrecy/2015/10/osc-ose/>>.

體貼文、網站和其他各種公開來源情資。該局針對關鍵的外國事務議題產製之情報研析報告也經常引用或根據公開來源情資，以提供局內其他部門、政府機關，甚至包括總統及其高級顧問等美國官員。¹⁸ 此外，包括國務院的「情報研究局」(Bureau of Intelligence and Research, INR) 主要提供有關外交政策的情報分析、¹⁹ 「國家安全局」(National Security Agency, NSA) 著重訊號情報、網路安全工作，更是極為重視各種公開、網路資訊的蒐集研析。²⁰

除了美國以外，歐洲國家也同樣重視公開來源情報工作發展。例如：「英國廣播公司監測處」(BBC Monitoring) 受到國家內閣辦公室、外交和聯邦事務部等和政府背景相關之政、軍界機構資助，透過在全球廣布的媒體通訊機制，將重要訊息提供英國政府參考。²¹ 此外，隸屬瑞士聯邦國防部之「戰略情報局」(Strategic Intelligence Service)、 「軍事情報局」(Military Intelligence Service) 也都設有公開來源情報工作體系；²² 荷蘭的

¹⁸ “Directorate of Analysis,” *Central Intelligence Agency*, <<https://www.cia.gov/about/organization/>>.

¹⁹ “Bureau of Intelligence and Research,” *U.S. Department of State*, <<https://www.state.gov/bureaus-offices/secretary-of-state/bureau-of-intelligence-and-research/>>.

²⁰ “National Security Agency Mission,” *National Security Agency/Central Security Service*, <<https://www.nsa.gov/>>.

²¹ Laura Johnson, “Translation and Open-Source Intelligence: BBC Monitoring” in Michael Kelly, Hilary Footitt, and Myriam Salama-Carr, eds., *The Palgrave Handbook of Languages and Conflict* (Cham, Switzerland: Palgrave Macmillan, 2019), pp. 251-271.

²² Chris Pallaris, “Open Source Intelligence: A Strategic Enabler of National Security,” *Center for Security Studies (CSS), ETH Zurich*, Vol. 3, No. 32

「情報與安全總局」(General Intelligence and Security Service) 於 2012 年時也曾透過網際網路發現暴力攻擊事件線索，該國《情報與安全服務法》(Intelligence and Security Services Act) 也授權情報與安全總局、「軍事情報和安全局」(Dutch Military Intelligence and Security Service) 監看、攔截網路訊息，讓公開來源情報價值更得以體現。²³ 而「歐洲情報論壇」(The European Open Source Intelligence Forum) 自 2007 年成立以來，亦以促成各專業公開來源情資分析師之間的知識和經驗交換為主要功能。²⁴

再以亞洲地區國家為例，日本外務省於 1984 年 7 月成立國際情報局，透過外交人員、各大商社、公司駐外機構等互通情報，並強化對國際情報蒐集、分析、處理和傳遞能力。尤其是下轄之分析第二課最為重視公開來源情報研究，主要藉由新聞記者、學者以及民間人士的派遣，廣泛蒐集各類情資。²⁵ 而中國大陸的國家安全部、公安部，以及軍方聯合參謀部、政治工作部聯絡局、戰略支援部隊網路空間作戰部隊，甚至是中共中央對外聯絡部、統一戰線工作部等單位除了是為人熟知的情治單位外，參照其 2014 年的《反間諜法》、2015 年的《國家安全法》、《反恐怖

(April, 2008), p. 3.

²³ Flemming E. Haar and Bernardus Haspels, *The Strategic Utility of Small-State Special Operations Forces (SOF) as Information Collectors to Support National Decision-Making* (Monterey, CA: Naval Postgraduate School, 2018), p. 2.

²⁴ Quirine A. M. Eijkman and Daan Weggemans, "Open Source Intelligence and Privacy Dilemmas: Is it Time to Reassess State Accountability?" *Security and Human Rights*, Vol. 23, No. 4 (April, 2013), p. 288.

²⁵ 余賀麟、武文匯，〈論日本走向情報大國之路〉，《情報雜誌》，第 39 卷第 1 期（2020 年 1 月），頁 10-16。

主義法》、2016 年的《網絡安全法》，以及 2017 年的《國家情報法》，亦可發現賦予其所謂「國家情報機構」更大的情蒐和執法權力。²⁶ 至於我國最重要的情報機構「國家安全局」除了在官方網站上設有包括「一週全球重要動態」、「資通安全」、「科技新知」、「特勤工作」、「一般性報告」之公開情報資訊網頁，近年亦成立「情報聯合應變中心」，專責公開情報蒐整有關事項；另參據《國家安全局處務規程》可知該局各部門無論從事國際情報、大陸地區情報、臺灣地區安全情報蒐集，或是執行反情報工作、網域安全情勢、戰略情報研析工作，皆和公開來源情報息息相關。²⁷

參、國家安全工作中的公開來源情報作法

當前各國面臨的國家安全威脅往往是複合且同時涵蓋傳統和非傳統安全領域。國與國之間在競合關係發展進程中，針對特定國家的情蒐重點也已從政治、經濟、軍事等實體層面，延伸至社會網絡。因此，作為國家安全情報領域之重要組成，公開來源情報因強調「公開訊息來源」特點，其發揮的作用愈來愈重要。從過去主要以書報、刊物、廣播和電視新聞、網路媒體作為情資來源，現隨著大數據、數位資訊、網路技術快速蓬勃發展，要從龐大資料的細節中分析出具有重要價值的訊息變得更為容易，且能補足傳統秘密情報手段之不足。例如：美國政府為了運用大數據

²⁶ 翁衍慶，《中共情報組織與間諜活動》（臺北市：秀威資訊，2018），頁 12-19。

²⁷ 〈國家安全局處務規程〉，《全國法規資料庫》，2010 年 4 月 1 日，<<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0020146>>。

的理念和技術提升公開來源資料和國家科技情報的能力，已經提出「大數據研究發展倡議」(Big Data Research and Development Initiative)，²⁸ 可見公開來源已成為不可或缺的重要情蒐途徑。

一、指導和蒐集階段

儘管是在公開訊息環境中作業，惟所獲情資最後要能夠成為有價值的情報，就無法跳脫國家安全情報之指導 (Direction)、蒐集 (Collection)、處理 (Processing)、運用 (Use) 四大步驟程序。²⁹ 基此，針對設定的情報目標，無論是個人、議題、對象，情報指導必須包括完整的範圍、制定情報蒐集計畫、設定優先「情蒐指導要項」，並且提出情報蒐集指導要領。其次在蒐集方面，有別於秘密情報的資料蒐集手段，公開來源更重視的是來自於公共領域開放式資料的源頭、資源。其中，資料源頭來自於訊息的所有者，無論是出自於主動或自願公布相關訊息，或是透過資訊技術獲得所有者不願公開的訊息，只要是公共性質或取自開放式的實體或虛擬空間，且不違反任何版權或隱私法律規範等情況，向公眾合法獲取，皆是情報來源（如表 1 所示）。

²⁸ Gordon Alley-Young, "White House Big Data Initiative," *Encyclopedia of Big Data*, May 12, 2017, pp. 1-5.

²⁹ David Omand, "The Cycle of Intelligence," in Robert Dover, Michael Goodman, and Claudia Hillebrand, eds., *Routledge Companion to Intelligence Studies* (New York: Routledge, 2013), p. 12.

表 1 公開來源情報主要出處

種 類	來 源
公共和開放式資料	政府公布訊息和公共政策報告、公告、預算書表、聯絡資訊、公聽會、專家座談會、法庭證詞、新聞記者會、網站資訊、電視廣播、演講、宣傳資訊。
	免費、開源地理空間圖資，例如：政府部門地理資訊系統。
	社群媒體或是相關媒體的聊天、對話回應內容。
公共和授權使用資料	未出版作品或公報、灰色文獻、技術報告、預印本、專利、工作文件、商業文件。
	專業和學術出版品，例如：期刊、會議、研討會、學術性論文、一般性論文。
	商業和經濟調查資料庫、公私企業、產業分析資料庫、視覺化分析資料庫。
	附帶原始資訊之相片、影像。

資料來源：作者自行彙整

二、研析和處理階段

主要是針對已獲取之公開來源訊息，依據主題、內容或某些原則從事進一步的篩選、分類，進而納入本單位或情報工作團隊、個人之資料庫。雖然這些情資仍多屬於原始的公開來源訊息，未經重整編製，惟其中一些可用之參考資訊，實已具有變為情報之基本條件。也因為在公共領域中，各種有用訊息可謂汗牛充棟，若未經過一套有系統的處理方式，不僅難以發現深層真箇，紛亂繁雜的訊息也會隨時間而被撤除。當大量訊息散落在網際網路各

個角落，而公開來源情報作業，需要有效率地蒐整特定情資。³⁰

（一）設定主題

所有的情報研析工作必須聚焦某個設定的主題，從專業團隊到有個人業餘，從事公開來源情報研究的工作者和體制內情報工作者方法並不相同，惟皆須遵循國家情報和機密保護等法規之作業規範落實執行，避免因相關訊息外洩而危害國家利益或情報工作體系。各類研究主題的設定往往和研究成果為誰所用？能不能用？如何用？密切相關，大致可區分為三種類型：

1、任務型研究主題

針對明確的特定目標對象和情報需求，以契約訂定形式，確定研析內容及時限，對於研究水準的要求較高。

2、需求型研究主題

通常是獨立從事公開來源情報工作單位或人員主要採用的類型。儘管沒有明確的目標對象，但仍會針對某些特定對象的潛在需求去設定研究主題。以現況而論，透過網際網路連上的智庫網站，或是透過經營社群媒體，主動發布特定主題之研究成果，往往就屬於此類。基此，網站或經營者的專業程度，和實際上受到潛在特定對象關注的程度密切相關。

3、興趣型研究主題

主要被本身具備相關專業程度的人員所採用。由於涉及的領域廣泛，惟只要能夠充分發揮個人專業優勢，結合具有潛在或較

³⁰ Clive Best, "Open Source Intelligence," in F. Fogelman-Soulié, ed., *Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security* (Amsterdam: IOS Press, 2008) pp. 331-343.

大影響力的研究主題，便能彰顯研析和處理的專業成果。

（二）基於公開來源情資之處理系統設計

從利用個人電腦處理公開訊息，到設計資料庫，有系統地存儲整理開放性資料，在大數據時代，面對龐大而複雜的訊息來源，更考驗著後續的資料處理能力。一套能夠同時集蒐集、處理、分析、應用功能之情報綜合分析平臺，能夠提供相關決策單位強而有力的技術支援，主要包括情報採編、情報研析、情報服務三大子系統。³¹

1、情報採編系統

是指依據情報採集策略，對公開來源情資進行二次加工，獲取更完整、更有價值、更高層次的情報成果。基此，須對不同訊息來源的資料，進行抽取和結構化等處理。從資訊技術面向而論，這些訊息大都利用網路爬蟲等資料探勘技術抓取社群媒體、資料庫、目標對象之網站介面、原始網頁資料。由於所得檔案格式各不相同，甚至包含許多無效文件，須先處理文件正規化與無效文件篩選。前者是指將不同來原始檔案轉換成相同格式的過程；後者則是刪除文件正規化後的無效文件。進而再針對情報特徵、主題標示實施分類。

2、情報研析系統

是指經過篩選、分類後的情資除了能夠在原始資料庫中對其做索引、查找，更重要的是能夠對於存儲資料進行更深入的分析、統計或是繼續探勘。由於公開來源情報是以數位化形式進行處

³¹ 張恒，〈基於開源情報的情報處理系統模型構建〉，《情報雜誌》，第33卷第3期（2014年3月），頁54-57。

理，透過對系統所採集到的訊息做更深入的資料分析，將更能提供情報工作中更為完整和綜合性的需求支撐。在實務操作中，透過大數據和資料擷取技術，資料庫可以數據、文件兩種形式儲存，並且針對特定目標對象、議題持續進行深度探勘、檢索，以及比較分析，進而為決策提供數據支撐，助於決策評估。

3、情報服務系統

目的在提供各種焦點分析報告、深度專題報告、統計分析報告、研究報告、動態快訊等能夠實現多功能檢索、分類瀏覽功能，提供情報研析人員適當的分析方法和技術，並以簡報、報表、報告等形式產出情報產品，或依服務對象定製的產品需求，提供情報檢索和情報用戶決策支援服務。

表 2 公開來源情報處理系統設計

系統種類	資料來源和作業流程	
情報採編系統	<ul style="list-style-type: none"> ● 智慧情報蒐集子系統 <ul style="list-style-type: none"> ■ 資源主動查找 ■ 網路爬蟲 ■ 內容篩選 ■ 訊息彙整 	<ul style="list-style-type: none"> ● 情報分類處理子系統 <ul style="list-style-type: none"> ■ 資料篩選 ■ 格式化、結構化配置 ■ 語法文字分析 ■ 標示索引、分類
情報研析系統	<ul style="list-style-type: none"> ● 情報資料查找 ● 數據統計 ● 關聯性分析 ● 統計分析 ● 比較分析 	
情報服務系統	<ul style="list-style-type: none"> ● 視覺化分析產品（統計圖、關係圖、報表、時間軸） ● 定期情報發布 ● 特定情報提供 	

資料來源：作者自行整理

三、形成價值情報和運用

公開來源情報處理的最後階段是向情報用戶提供有價值意義的情報報告。惟對於獨立從事公開來源情報工作的單位或個人而言，用戶各層級、體系之的要求標準、側重點並不相同，透過資料存儲和大數據運算能力，甚至再加上人工智慧技術，只要相關技術、技巧運用得當，便能按照情報用戶需求提供成果。公開來源情報已被證明能夠用於特定議題或事件之早期預測，甚至可以用於對已發生之危安事件進行問題本質分析或取證調查，³² 無論是標準要求較高或是目標對象的多元性，公開來源情報的運用已愈來愈廣泛。

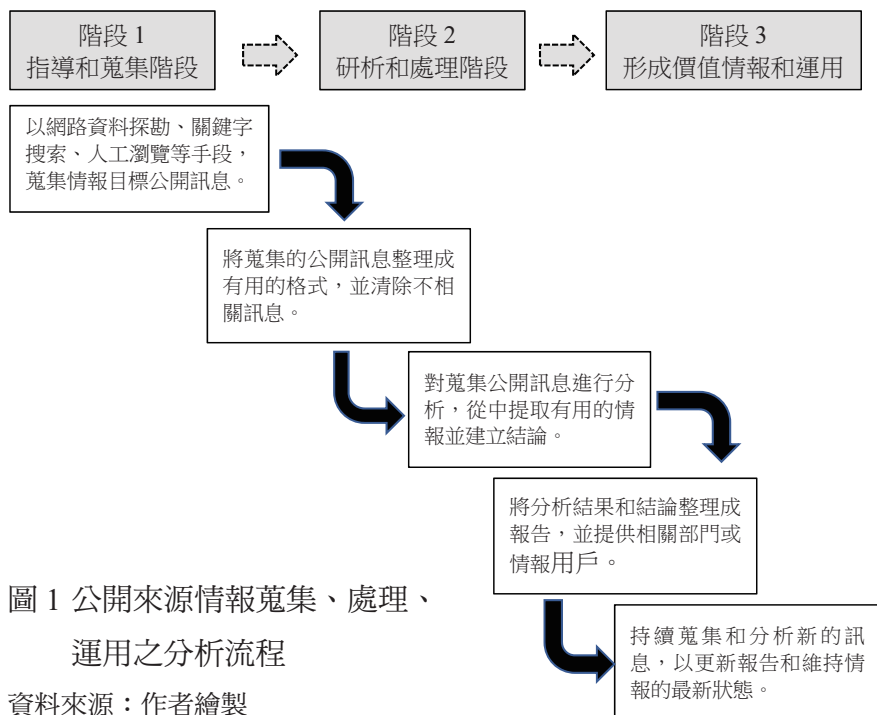
肆、案例探討：中共軍事議題公開來源情報運用之適用和侷限

公開來源情報和其他各種類型的情報手段一樣，皆有各自特定的方法來蒐集資料、研析、處理和製作情報產品，且隨著公共領域中的訊息來源迅速增加，讓這種類型的情蒐方法更具必要性。以臺海安全情勢和中共對臺軍事威脅為例，幾乎已成為國際、國內各種媒體管道的關注熱點。從政府部門官員的發言、專家學者的論點，至各大新聞媒體的報導，再到新媒體、自媒體的評論，各家皆聲稱有獨立的訊息來源，其作出的各種評估、判斷也都互有高見。只是進一步檢視各方見解，仍然虛實交錯，難辨真假。

³² Nihad A. Hassan and Rami Hijazi, *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence* (Berkeley, CA: Apress, 2018), pp. 1-20.

可見除了秘密來源管道具有保密性難以查證外，其他來自公開管道的訊息應有其適用和侷限性可做進一步討論。

本研究提出公開來源情報的蒐集、處理與運用分析流程作為剖析案例的分析工具（如圖 1 所示）。並且假設此一論證分析，能夠解釋公開來源情報在物理、資訊領域中，能夠提供情報工作者針對目標對象和議題之即時、有利線索。惟若要進一步全般掌握內情或對目標對象行為作出精準判斷，也認為需要藉助其他情報手段。基於這個理論性假設，本段即以解放軍「軍用無人機發展」和「實戰化跨區兵力投送演練」兩類案例，說明從中共官方微信公眾號、各大新聞媒體採集的諸多公開訊息，用於評估對臺動武之國家安全情報判斷的適用和侷限性。



一、適用性案例：解放軍無人機軍力發展

解放軍愈來愈注重軍用無人機戰力建設、戰術戰法測試與運用，可從檢索中共官媒、軍媒微信公眾號等公開來源情資中發現端倪，尤以「軍（兵）種部隊訓練」和「國防工業國際武器貿易」為最主要類型。

（一）軍（兵）種部隊訓練

1、空軍智慧無人機競賽

2018年6月，在中國大陸河北省保定市涞水縣「中國電科電子科技園」曾舉辦首屆「無人爭鋒」智慧無人機集群系統挑戰賽。³³ 這項競賽是為了探索未來智慧無人集群作戰概念，由解放軍空軍聯合中國大陸電子科學研究院、清華大學、北京理工大學等單位，按照每項比賽科目，根據比賽成績，除了分別評選出冠軍、亞軍和季軍，授予證書、獎盃等獎勵外，其技術將優先考慮在空軍項目中應用。

從公開來源情資中可見，此次比賽所有參賽無人機區分為固定翼和非固定翼兩組，目的在結合空中作戰背景，設置若干比賽科目，重點考核各參賽隊無人機集群密集編隊、高速精確避障、協同搜索識別與定位、集群協同策略與動態任務規劃、空中精確定位與空中預對接等技術的發展程度。有關比賽場地、科目如表3所示。

³³ 〈6月，空軍將舉辦「無人爭鋒」智慧無人機集群系統挑戰賽〉，《空軍發布》，2018年4月13日，<<https://tinyurl.com/3fetsdfp>>。

表 3 解放軍空軍「無人爭鋒」智慧無人機集群系統挑戰賽

類別	競賽項目
比賽場地	
密集編隊 穿越競速	
編隊協同 偵搜攻擊	
自主回收與 空中受油	

資料來源：解放軍「空軍發布」官方微信公眾號

檢視解放軍空軍微信公眾號公布訊息可知，中共一直有投入無人機至軍事作戰中，為選拔未來空軍的無人機「集群作戰」應用技術做準備。該次由解放軍空軍裝備部主辦、中國電子科學研究院、遠望智庫承辦，以及清華大學、北京理工大學協辦首屆「無人爭鋒」智慧無人機集群系統挑戰賽，設置 3 個比賽項目，軍民均可參與，無不讓人認為中共軍方有意打造無人機兵團。此舉同時也映證了繼 2017 年 6 月，中國電子科技集團公司 (China Electronics Technology Group, CETC) 展示包括 119 架無人機集群技術後，中共再次以舉辦競賽名義培養和提升國內和軍中無人機集群人才與技術，並引發各界對中國大陸無人機集群技術發展現狀之關注。

2、陸軍航空兵有人、無人機協同演練

在當前技術條件下，無人機在戰場上之功能主要用於輔助作戰，以及為主戰力量提供情報支撐和偵察打擊。因此，有人 / 無人機協同將成為空中無人平臺在未來戰場運用的常態。空中有人 / 無人作戰平臺是以有人機為前線指控平臺，按作戰需求適時調整作戰方案，以加強對無人機的指揮控制權，確保作戰任務順利遂行。

以陸軍陸航部隊為例，搜索偵察、火力打擊是其主要職能，以往搜索任務的執行皆須依賴直升機完成。如今，透過無人機加上直升機的組合，成為標準配備的作戰任務執行模式。例如：東部戰區陸軍第 71 集團軍陸航旅在東海海域進行跨晝夜實彈演習期間，利用無人機在數千公尺高空對海上目標進行跟蹤、偵察、識別，並將結果資訊即時傳回指揮中心。再由多架次直 -19 武裝

直升機以超低空掠海快速向目標區域機動，進入射程後，在無人機照射引導下擊中海面標靶。³⁴ 另外像是北部戰區陸軍第 80 集團軍陸航旅的實兵實彈演習，同樣利用無人機抵近敵軍指揮所偵察，並以雷射引導直 -10、直 -19 武裝直升機發射 AKD-10 空對地飛彈摧毀目標。³⁵

再以陸軍集團軍砲兵旅無人機偵察連為例，其偵察車採用 JWP-02 偵察無人機，具備全天候利用光電設備和無線電技術設備進行戰場偵察，以及攜帶大型電子吊艙實施戰區電磁干擾壓制等功能，大幅提高砲兵部隊偵察能力。

檢視這些公開來源情報可發現隨著智慧化、資訊化技術發展，無人機因具有飛行高度高、續航時間長等優勢，在軍事任務方面可應用的用途愈來愈多、作用也變得關鍵重要。當前在陸軍作戰體系中，以無人機引導火力打擊成為實戰化訓練的重點項目。

3、軍用無人機國際武器貿易

受到近年來武裝無人機在國際武器貿易市場的交易日趨熱絡，以及用途愈來愈多元等因素影響，中共亦積極投入軍用無人機的外貿出口。特別是於 2020 年加入聯合國《武器貿易條約》(Arms Trade Treaty) 後，現已成為國際間主要的武裝無人機出口

³⁴ 〈武裝直升機，對海展開全彈種跨晝夜實彈射擊〉，《中國軍網》，2021 年 5 月 25 日，<http://www.81.cn/big5/zq/2021-05/25/content_10039465.htm>。

³⁵ 〈有人無人協同飛行，戰鷹配上「千里眼」〉，《CCTV 軍事頻道》，2021 年 3 月 1 日，<<https://tv.cctv.com/2021/03/01/VIDEMkle1ozmO4aWp3flWckl210301.shtml?spm=C52346.PKs1OTJ9sJ1H.S39569.20>>。

國家。其銷售的對象包括亞洲地區的土庫曼、緬甸、巴基斯坦、沙烏地阿拉伯、阿拉伯聯合大公國、伊拉克、約旦，以及非洲地區的埃及、尼日、阿爾及利亞等國。其中，「翼龍」、「彩虹」系列偵打一體軍用無人機的製造、出口更是受到國際間高度關注。以此檢視 2022 年 8 月中共恣意在臺海周邊劃設禁航區進行軍演，到派出包括「彩虹 -4」、「無偵 -7」、「TB-001」、「KVD-001」、「BZK-005」、「BZK-007」等多型功能無人機逾越海峽中線、侵擾我西南空域等情事來看，解放軍愈來愈注重傳統兵力和融入無人化、智慧化元素的「混合戰」戰術戰法的測試與運用。³⁶ 這些持續加大對臺軍事威脅的強度和力度，破壞臺海和平穩定，意圖片面改變現狀的舉動，其實和「中國航空工業集團」、「中國電子科技集團」等軍工企業、國防工業發展，以及武器對外貿易能力密切相關，進而可明確評估中共積極投入無人機研發，目的除了是為了發揮廉價武器的數量優勢，更要在不引起軍事對抗和軍事衝突升級情況下，保持不對稱作戰優勢之武裝力量選擇。³⁷

檢視上述案例可知，無人機既可有效當作致命武器運用，也可作為非致命武器。以這些案例再持續利用公開來源管道蒐集相關訊息，可發現解放軍空軍至今仍在舉辦相同類型之無人機競賽，而各軍種將軍用無人機納入實戰化軍事訓練中亦已成為常

³⁶ 〈即時軍事動態〉，《中華民國國防部》，2022 年 11 月，<<https://tinyurl.com/3uf6vnrj>>。

³⁷ 胡喆，〈為無人機裝上「智慧大腦」：中國電科發佈智慧無人集群系統多功能處理單元〉，《新華網》，2019 年 10 月 22 日，<http://big5.www.gov.cn/gate/big5/www.gov.cn/xinwen/2019-10/22/content_5443511.htm>。

態，另隨著各種外貿型軍用無人機亮相國際各大航空展、國防展，更可坐實從民間到軍方；從私營企業到國有企業，從中尋覓可造之材和透過軍民融合戰略，刻正積極研製各種功能、類型之無人機，甚至是無人化作戰平臺。可見對相關議題的掌握和對公開來源情資有系統性的持續蒐整，自可看出未來在臺海安全衝突情境中，無人機作戰，或是結合有人機協同作戰，勢必是中共新型作戰力量發展的重點。

二、侷限性案例：解放軍跨區兵力投送和對臺動武能力評估

隨著中共於 2020 年完成軍改，積極的軍事擴張行徑愈來愈明顯，突破太平洋第一島鏈，並將軍事勢力範圍延伸至第二島鏈的意圖更是明確。以解放軍各軍兵種戰訓任務為例，以武力叫陣挑釁的軍事動作不斷增加、升壓，其緊繃的外部安全情勢、明確的目標對象和不甘示弱的軍方態勢，多重因素交織影響已導致解放軍演訓項目的幅度、強度，頻率急遽上升。解放軍正進入軍改後的新軍備、新型戰力適應磨合期，其軍事活動動見觀瞻，其戰力的虛實不僅是各方關注焦點，判斷的依據、指標能否從公開來源情資中得到確切的答案，可從解放軍陸軍兩棲裝甲部隊海上軍演，以及跨區兵力投送演訓案例中得到反思。

（一）解放軍陸軍兩棲裝甲部隊海上軍演

2021 年 7 月 9 日，中國大陸《人民日報》海外網「海客新聞」官方微博以〈央視罕見直播兩棲裝甲部隊海訓 05 式裝甲車搶灘登陸〉為題，報導解放軍東部戰區陸軍第 73 集團軍兩棲重型合

成旅在福建省南部海域進行海上實戰射擊綜合演練。³⁸ 該報導被國內新聞媒體引用，分別以〈央視罕見直播 05 式兩棲甲車海訓，時速 25 公里任踹門奪島先鋒〉、³⁹ 〈備戰登陸臺灣？解放軍秀「踹門奪島」利器〉、⁴⁰ 〈搶灘登島「踹門」利器？大陸自研 05 式兩棲裝甲車演習〉為標題進行轉述報導。⁴¹ 除了兩岸的新聞報導外，事實上當天亦有國內新聞媒體在 YouTube 平臺上配合做即時實況轉播，⁴² 可見這場軍事演訓被用來做為宣傳的意義並不亞於軍事意義。

然而，從公開來源情資的面向再繼續蒐集當天中國大陸中央電視臺的報導可知，各方的報導內容其實南轅北轍，僅能從公開來源情資中得知陸軍第 73 集團軍兩棲部隊的海上軍演訊息屬實，卻無法判斷軍事演訓的真實情況（如圖 2 所示）。

³⁸ 〈央視罕見直播兩棲裝甲部隊海訓 05 式裝甲車搶灘登陸〉，《海客新聞》，2021 年 7 月 9 日，<<https://tinyurl.com/yc28f4w9>>。

³⁹ 魏有德，〈央視罕見直播 05 式兩棲甲車海訓，時速 25 公里任踹門奪島先鋒〉，《ETtoday 新聞雲》，2021 年 7 月 12 日，<<https://www.ettoday.net/news/20210712/2028659.htm>>。

⁴⁰ 陳成良，〈備戰登陸臺灣？解放軍秀「踹門奪島」利器〉，《自由時報》，2021 年 7 月 13 日，<<https://news.ltn.com.tw/news/politics/breakingnews/3602070>>。

⁴¹ 〈搶灘登島「踹門」利器？大陸自研 05 式兩棲裝甲車演習〉，《聯合新聞網》，2021 年 7 月 13 日，<<https://udn.com/news/story/7331/5599418>>。

⁴² 〈大陸 73 軍團兩棲裝甲部隊，海上軍演直擊〉，《中時新聞網》，2021 年 7 月 9 日，<<https://www.youtube.com/watch?v=5uo86lGFmLI>>。



圖 2 中國大陸「海客新聞」微博和中央電視臺報導解放軍陸軍軍演差異比較表

資料來源：

1. 〈央視罕見直播兩棲裝甲部隊海訓 05 式裝甲車搶灘登陸〉，《海客新聞》，2021 年 7 月 9 日，〈<https://tinyurl.com/yc28f4w9>〉。
2. 〈直擊演訓一線，第 73 集團軍閩南某海域複雜環境實彈演練，檢驗兩棲裝甲作戰能力〉，《央視網》，2021 年 7 月 10 日，〈<https://tv.cctv.com/2021/07/10/VIDEtXuDPg5w8LqwBZe1CuQG210710.shtml>〉。

第一，「海客新聞」官方微博報導中出現的是「05 式兩棲步兵戰車」，主要功能是步兵乘載，和中央電視臺報導的「05 式兩棲步兵突擊車」有很大差異。

第二，「05 式兩棲步兵戰車」曾以「海上的帶刀超跑」作為宣傳用辭，⁴³ 而國內媒體所稱的「踹門奪島」利器、先鋒，事實上是指配備 105 公釐口徑膛砲的「05 式兩棲突擊車」，另有關「踹門」之說的報導，回溯公開來源情資，最早其實是見於 2020 年 5 月的解放軍軍事演訓報導。⁴⁴

⁴³ 〈「海上超跑」兩棲步兵戰車助力中國海軍陸戰隊勇奪大賽桂冠〉，《澎湃新聞》，2019 年 8 月 28 日，〈https://www.thepaper.cn/newsDetail_forward_4274863〉。

⁴⁴ 〈兩棲突擊車為何能「啃」「硬骨頭」〉，《央視網》，2020 年 5 月 8 日，

第三，從中央電視臺報導中可以得知，這場演訓主要聚焦戰鬥射擊協同指揮、特情處置等多項實戰課目，參演官兵受訪時則表示演練期間海上風浪太大，影響兩棲登陸車海上航行穩定以及射手瞄準目標。⁴⁵ 可見中央電視臺的報導內容和「海客新聞」官方微博、國內新聞媒體的事實描述極不相同。

從以上案例可以發現，公開來源情報雖然可提供國家安全工作者即時掌握解放軍軍演和動態訊息，惟受限於軍事上的保密性，和政治意義上的宣傳，實際上的演訓詳情並無法從公開來源訊息中如實呈現。必須透過其他的科技情報，甚至是人員情報手段，方能做更明確的雙重確證。

（二）解放軍陸軍跨域兵力投送演訓

2021 年 10 月 14 日，國內媒體同樣轉述中國大陸中央電視臺新聞、中央廣播電視總臺「看臺海」官方微博，以〈兩岸緊張，解放軍臺海一線部隊進行「千人千車千里投送演練」〉為題，報導解放軍陸軍第 81 集團軍在山東半島進行跨域兵力投送演練。⁴⁶ 檢視該報導可知，主要內容轉引自《香港 01》網路傳媒公司報導，其撰文者稱此次兵力投送調用了隸屬渤海輪渡公司「中華復興」輪參與演練，將 96A 主戰坦克裝進船艙，可作為臺海戰事，支援

<<https://tv.cctv.com/2020/05/08/VIDEB9LTUHImlTOGtCGAXA3q200508.shtml>>。

⁴⁵ 〈直擊演訓一線，第 73 集團軍閩南某海域複雜環境實彈演練，檢驗兩棲裝甲作戰能力〉，《央視網》，2021 年 7 月 10 日，<<https://tv.cctv.com/2021/07/10/VIDEtXuDPg5w8LqwBZe1CuQG210710.shtml>>。

⁴⁶ 褚文，〈兩岸緊張，解放軍臺海一線部隊進行「千人千車千里投送演練」〉，《聯合新聞網》，2021 年 10 月 19 日，<<https://udn.com/news/story/7331/5828735>>。

一線作戰部隊的預備力量。⁴⁷

從公開來源情資分析角度而論，該集團軍的跨域兵力投送演練和以「中華復興」輪運輸裝備的作法雖然屬實，惟演練的目的卻和媒體報導內容並不相同。

第一，檢視第 81 集團軍官方微信公眾號「八一軍號」報導可知，演練當天是依據年度軍事訓練計畫，展開整建制遠端戰略投送綜合演練。⁴⁸ 參演部隊是隸屬該集團軍的第 195 重型合成旅（駐地：內蒙古自治區錫林郭勒盟），演練過程採陸運、海運、空運方式進行裝備、人員跨域兵力投送。而該則新聞報導中所指的「千人千車千里投送演練」，事實上是該部隊從駐地啟程後，先利用陸運、空運方式將部隊移動至遼寧省大連市，再從大連港搭乘「中華復興」輪抵達目的地煙臺港。其相關訊息皆可從中共官方微信公眾號、山西新聞網報導中得到確證（如圖 3 所示）。⁴⁹

⁴⁷ 〈兩岸關係緊張，解放軍進行「千人千車千里投送演練」〉，《香港 01》，2021 年 10 月 19 日，<https://www.hk01.com/article/690159?utm_source=01articlecopy&utm_medium=referral>。

⁴⁸ 〈千里機動！百餘輛裝甲是這樣輸送的〉，《八一軍號》，2021 年 10 月 19 日，<<https://tinyurl.com/4zbn2dc4>>。

⁴⁹ 〈軍警攜手，一體聯動，山西省「一站式」服務暖兵心〉，《太原日報》，2021 年 10 月 19 日，<<https://tinyurl.com/ysznpmst>>。

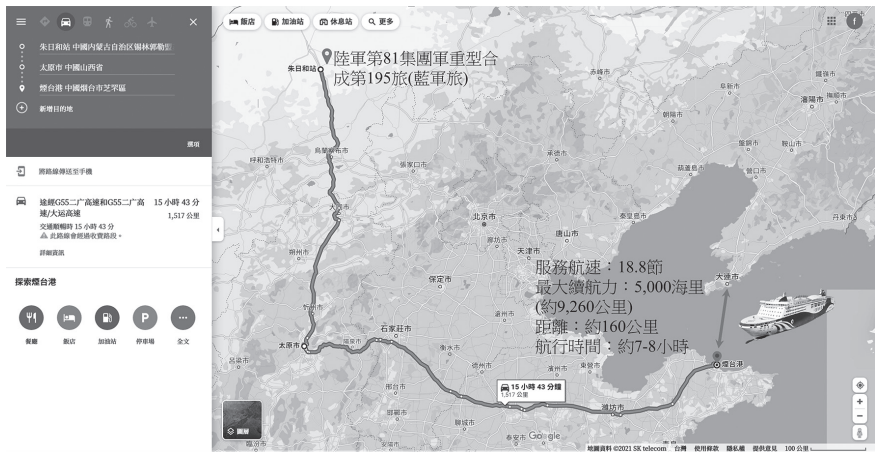


圖 3 解放軍陸軍第 81 集團軍第 195 重型合成旅跨區兵力投送演練示意圖

資料來源：作者利用 Google Map 自行繪製

第二，檢視「中華復興」輪背景資料可知，該輪為 2019 年 11 月 4 日，由黃海造船有限公司為渤海輪渡集團股份有限公司建造的第 12 艘大型豪華客滾船，船長 212 公尺、型寬 28.6 公尺，總噸位 4.5 萬噸。乘客定額為 2,000 人、車道長度 3,070 公尺、3 層車輛艙，裝載車道長 3,000 公尺，可裝載大小車輛 350 餘輛，具備優異的裝載能力。⁵⁰ 該輪至今仍在大連、煙臺兩地航線營運（如圖 4 所示），是山東半島、遼東半島間最便捷航線，海上運輸也較陸地交通大幅縮短路程。從上述公開來源情資，計算該輪的航速、航程，可以推算出從大連開赴中國大陸東部沿岸港口，再轉作為攻臺戰力，航行所需時間至少需要 3 天。可見該部隊的

⁵⁰ 〈郵輪型豪華客滾船「中華復興」輪試航成功〉，《中國新聞網》，2019 年 9 月 27 日，<<https://www.chinanews.com.cn/cj/2019/09-27/8967204.shtml>>。

演訓和媒體揭露的目的，有很大的事實出入。

烟台港10月7日计划航班

航线	发船地点	目的港	运营船舶	开航时间
烟台—大连	烟台港客运站	大连港大连湾客运站	中华复兴	9:00
		大连湾新港客运站	渤海晶珠	11:50
		大连港客运站	棒棰岛	12:20
		大连湾新港客运站	渤海钻珠	14:30
		大连湾新港客运站	渤海翠珠	21:00
		大连湾新港客运站	渤海玛珠	22:30
烟台—大连	同三轮渡码头	大连港大连湾客运站	龙兴岛	9:00
		大连港大连湾客运站	永兴岛	21:00
		大连湾新港客运站	渤海宝珠	23:00
龙口—旅顺	龙口港客运站	大连旅顺新港客运站	渤海翡珠	10:00
		大连旅顺新港客运站	渤海玉珠	21:30
蓬莱—旅顺	蓬莱港客运站	大连旅顺新港客运站	渤海珍珠	22:30

圖 4 「中華復興」輪煙臺、大連往返時刻表

資料來源：〈「中華復興」輪 10 月 7 日首航煙臺至大連航線〉，《膠東在線》，2020 年 10 月 6 日，<<http://www.jiaodong.net/news/system/2020/10/06/014098970.shtml>>。

綜合以上中共軍事領域公開來源情資之運用案例可發現，從指導蒐集到形成、運用有價值的情報，本研究所提出的公開來源情報分析流程能夠解釋從多方公開訊息公布之管道中，獲取包括文字、圖片、影像等關於目標情報議題之可用訊息。經過篩選、分類、比對等處理程序後，進一步得到具有信度、效度之趨勢預測，並能即時對掌握解放軍動態的工作者提供有利線索。公開來源情報在物理、資訊領域可及時提供情報部門做出國家安全情勢評估和告警因應，確有其適用性。

然而本研究也察覺，透過各種訊息管道針對特定議題進行多方查證、深度瞭解雖非難事，惟若要更一步地全般掌握動態詳情，單憑公開來源情報仍有其盲點。此一侷限性必須依賴和秘密情報工作體系的密切協調配合，方能做出更加客觀、精準的情報產製和應用。從公開來源情報的功用而言，主要表現在關於國家安全領域的預警和評估；另對於即時安全情況做出判斷定論，則有賴其他情報工作手段的輔助，才能更加周延、完備。

伍、結論

公開來源情報的管道、數量隨著網際網路環境的普及，以及資訊科技的快速進步，應用層面已愈來愈多元，功用也愈來愈明顯。從國家安全情報機關必須依賴公開來源情報作為工作主要輔助，到解決日常生活中的各種問題，只要能夠掌握訊息來源、具備相關的資訊技能，其執行者也不再僅限於情報工作人員。公開來源情報的精確、可靠、及時更是攸關情報產品的良窳，而包括文字探勘、自然語言處理和機器學習等大數據資料獲得和處理技術更將國家安全情報工作環境拓展至虛擬的網路空間。

本文聚焦於公開來源情報的作法和傳統秘密情報概念做出比較，目的是在凸顯儘管在目前的資訊化環境下，許多情資已呈現出數位化的存儲形式，而為了能夠製作出具有價值性的情報產品，服務情報用戶，公開來源情報同樣必須經過指導、蒐集、處理、運用四大作業程序，搭配情報採編、情報研析、情報服務等系統的建立，才能充分提高數位資源的利用效率，為情報產品提供可靠、可用的素材。

其次，本文也提出了一套分析流程，從中共軍事議題的公開來源情報研究，找出其適用性和侷限性。在列舉的三個適用案例及兩個限制案例中，主要是以關於解放軍武器裝備發展趨勢和部隊演訓類型之公開資料作為論證依據。其中，無論是從各型無人機納入解放軍軍力現代化或國際武器貿易重點項目，或是陸軍部隊在登陸與跨域兵力投送演習中，皆可明確看見軍事發展的重要脈絡，並對其特點作出預示和評估。基此，隨著在公開來源情報領域中揭露的訊息愈多，能夠作為比較、分析的參考基準也就愈客觀，進而能夠提升最終情報產品的品質與價值。然而，從侷限性面向而論，由於國家安全情報往往事涉機敏，尤其是軍事議題，更是保密的重中之重。因此，透過相關案例分析，亦可得知無論是各類軍事活動的實況詳情細節或是內部決策考量因素，實難以完全從公開來源情報中得到確證。因此，增進和傳統秘密情報工作形成更好地協調互補，是克服限制的可行作法。

在目前的國家安全情報工作環境中，對於解放軍等敵情的掌握，已離不開公開資源環境，且只要合理設定關鍵詞，運用合適的檢索系統、網路搜尋引擎，往往就能夠找到對應內容，並再對這些內容進行深入的分析甄別。因此，執行公開來源情報工作，關鍵不外乎語言和相關議題的專業程度。尤其在臺灣處理中共軍事情報工作方面，對同樣熟悉中文的情報蒐集和分析人員而言難度並不高，惟要能夠做出有深度的研析和情報產品，更涉及對中西近代史、中共黨史、解放軍軍史，以及中共黨政軍體制最新變革的掌握和瞭解，缺一不可，否則極易流為獵奇、跟風或是片面解讀。儘管和秘密情報的工作方式有著極大差別，但兩者的相同

點卻都是有賴於長期的投入和保持專注、耐心。

公開來源情報涉及各種領域，惟不外乎「心」、「物」兩大範疇。其中，從適用性而論，對於物理、資訊領域而言，皆可持續深化相關技術的開發而得以不斷進步。然而，從侷限性而論，公開來源情資無法看見目標對象的內心世界和斷定軍事行動最終目的亦為事實。除了對軍事活動的判斷外，檢視中共二十大的黨政軍高層人事變動結果，也可發現在會前各種透過訊息資料的蒐集、比對、分析，最終仍然難抵中共黨國體制之下秘而不宣、非制度化的用人考量。惟這並不表示公開來源情報沒有作用，相反地若能加以重視，持續優化工作環境和提升情資蒐研能量，除了能夠大幅降低情報工作人力、提升工作效率，更能和傳統秘密情報工作相輔相成，形成更完整的國家安全情報防護網。（投稿：2022年11月5日；修訂：2023年1月10日；接受：2023年1月12日）

參考文獻

一、中文部分

(一) 專書

翁衍慶，2018。《中共情報組織與間諜活動》。臺北市：秀威資訊。

(二) 期刊論文

余賀麟、武文匯，2020/1。〈論日本走向情報大國之路〉，《情報雜誌》，第 39 卷第 1 期，頁 10-16。

張恒，2014/3。〈基於開源情報的情報處理系統模型構建〉，《情報雜誌》，第 33 卷第 3 期，頁 54-57。

趙小康，2009/2。〈公開源情報：在情報學和情報工作中引入 Intelligence 的思考〉，《情報理論與實踐》，第 32 卷第 2 期，頁 23-27。

(三) 網際網路

2010/4/1。〈國家安全局處務規程〉，《全國法規資料庫》，
<<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0020146>>。

2018/4/13。〈6 月，空軍將舉辦「無人爭鋒」智慧無人機集群系統挑戰賽〉，《空軍發布》，<<https://tinyurl.com/3fetsdfp>>。

2019/8/28。〈「海上超跑」兩棲步兵戰車助力中國海軍陸戰隊勇奪大賽桂冠〉，《澎湃新聞》，<https://www.thepaper.cn/newsDetail_forward_4274863>。

- 2019/9/27。〈郵輪型豪華客滾船「中華復興」輪試航成功〉，
《中國新聞網》，<<https://www.chinanews.com.cn/cj/2019/09-27/8967204.shtml>>。
- 2020/5/8。〈兩棲突擊車為何能「啃」「硬骨頭」〉，《央視網》，
<<https://tv.cctv.com/2020/05/08/VIDEB9LTUJmITOGtCGAXA3q200508.shtml>>。
- 2020/8/26。〈臺灣海峽歷次危機回顧：從一江山島戰役、八二三
砲戰到飛彈危機，看美中臺三角關係演繹〉，<<https://www.bbc.com/zhongwen/trad/chinese-news-53834569>>。
- 2021/10/19。〈千里機動！百餘輛裝甲是這樣輸送的〉，《八一
軍號》，<<https://tinyurl.com/4zbn2dc4>>。
- 2021/10/19。〈兩岸關係緊張，解放軍進行「千人千車千里投
送演練」〉，《香港 01》，<https://www.hk01.com/article/690159?utm_source=01articlecopy&utm_medium=referral>。
- 2021/10/19。〈軍警攜手，一體聯動，山西省「一站式」服務暖
兵心〉，《太原日報》，<<https://tinyurl.com/ysznpmst>>。
- 2021/3/1。〈有人無人協同飛行，戰鷹配上「千里眼」〉，
《CCTV 軍 事 頻 道》，<<https://tv.cctv.com/2021/03/01/VIDEMkle1ozmO4aWp3flWckl210301.shtml?spm=C52346.PKs1OTJ9sJ1H.S39569.20>>。
- 2021/5/25。〈武裝直升機，對海展開全彈種跨晝夜實彈射
擊〉，《中國軍網》，<http://www.81.cn/big5/zq/2021-05/25/content_10039465.htm>。
- 2021/7/10。〈直擊演訓一線，第 73 集團軍閩南某海域複雜環

- 境實彈演練，檢驗兩棲裝甲作戰能力》，《央視網》，
<<https://tv.cctv.com/2021/07/10/VIDEtXuDPg5w8LqwBZe1CuQG210710.shtml>>。
- 2021/7/13。〈搶灘登島「踹門」利器？大陸自研 05 式兩棲裝甲車演習〉，《聯合新聞網》，<<https://udn.com/news/story/7331/5599418>>。
- 2021/7/9。〈大陸 73 軍團兩棲裝甲部隊，海上軍演直擊〉，《中時新聞網》，<<https://www.youtube.com/watch?v=5uo86lGFmLI>>。
- 2021/7/9。〈央視罕見直播兩棲裝甲部隊海訓 05 式裝甲車搶灘登陸〉，《海客新聞》，<<https://tinyurl.com/yc28f4w9>>。
- 2022/11。〈即時軍事動態〉，《中華民國國防部》，<<https://tinyurl.com/3uf6vnrj>>。
- 2022/8/26。〈東部戰區在臺灣周邊海空域組織多軍兵種聯合戰備警巡和實戰化演練〉，《中華人民共和國國防部》，<http://www.mod.gov.cn/power/2022-08/26/content_4919478.htm>。
- 胡喆，2019/10/22。〈為無人機裝上「智慧大腦」：中國電科發佈智慧無人集群系統多功能處理單元〉，《新華網》，<http://big5.www.gov.cn/gate/big5/www.gov.cn/xinwen/2019-10/22/content_5443511.htm>。
- 陳成良，2021/7/13。〈備戰登陸臺灣？解放軍秀「踹門奪島」利器〉，《自由時報》，<<https://news.ltn.com.tw/news/politics/breakingnews/3602070>>。
- 褚文，2021/10/19。〈兩岸緊張，解放軍臺海一線部隊進行「千

人千車千里投送演練」》，《聯合新聞網》，<<https://udn.com/news/story/7331/5828735>>。

魏有德，2021/7/12。〈央視罕見直播 05 式兩棲甲車海訓，時速 25 公里任踹門奪島先鋒〉，《ETtoday 新聞雲》，<<https://www.ettoday.net/news/20210712/2028659.htm>>。

二、外文部分

(一) 專書

- Best, Clive, 2008. "Open Source Intelligence," in F. Fogelman-Soulié, ed., *Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security*. Amsterdam: IOS Press.
- Clark, Robert M., 2013. *Intelligence Collection*. Washington DC: CQ Press.
- Haar, Flemming E., and Bernardus Haspels, 2018. *The Strategic Utility of Small-State Special Operations Forces (SOF) as Information Collectors to Support National Decision-Making*. Monterey, CA: Naval Postgraduate School.
- Hassan, Nihad A., and Rami Hijazi, 2018. *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence*. Berkeley, CA: Apress.
- Johnson, Laura, 2019. "Translation and Open-Source Intelligence: BBC Monitoring," in Michael Kelly, Hilary Footitt, and Myriam Salama-Carr, eds., *The Palgrave Handbook of Languages and Conflict*. Cham, Switzerland: Palgrave Macmil-

lan, pp. 251-271.

Omand, David, 2013. "The Cycle of Intelligence," in Robert Dover, Michael Goodman, and Claudia Hillebrand, eds., *Routledge Companion to Intelligence Studies*. New York: Routledge, pp. 59-70.

Steele, Robert D., 2007. "Open Source Intelligence," in Loch K. Johnson, ed., *Handbook of Intelligence Studies*. New York: Routledge.

Williams, Heather J., and Ilana Blum, 2018. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. Santa Monica, CA: RAND Corporation.

(二) 期刊論文

Eijkman, Quirine A. M., and Daan Weggemans, 2013/04. "Open Source Intelligence and Privacy Dilemmas: Is It Time to Re-assess State Accountability?" *Security and Human Rights*, Vol. 23, No. 4, pp. 285-296.

Pallaris, Chris, 2008/04. "Open Source Intelligence: A Strategic Enabler of National Security," *Center for Security Studies (CSS), ETH Zurich*, Vol. 3, No. 32, pp. 1-3.

Schaurer, Florian, and Jan Störger, Winter/Spring 2013. "The Evolution of Open Source Intelligence (OSINT)," *Intelligencer: Journal of U.S. Intelligence Studies*, Vol. 19, No. 3, pp. 53-56.

Steele, Robert D., Spring/Summer 1993. "National Intelligence and Open Source: From School House to White House," *American Intelligence Journal*, Vol. 14, No. 2, pp. 29-32.

Young, Gordon Alley, 2017/5/12. “White House Big Data Initiative,” *Encyclopedia of Big Data*, pp. 1-5.

(三) 網際網路

“Bureau of Intelligence and Research,” *U.S. Department of State*, <<https://www.state.gov/bureaus-offices/secretary-of-state/bureau-of-intelligence-and-research/>>.

“Directorate of Analysis,” *Central Intelligence Agency*, <<https://www.cia.gov/about/organization/>>.

“National Security Agency Mission,” *National Security Agency/ Central Security Service*, <<https://www.nsa.gov/>>.

2001/11. “NATO OSINT Handbook,” *Internet Archive*, <<https://archive.org/details/NATOOSINTHandbookV1.2/mode/2up>>.

2006/1/6. “National Defense Authorization Act for Fiscal Year 2006,” Public Law No. 109-163, Sec. 931, <<https://www.govinfo.gov/link/statute/119/3236>>.

2006/7/11. *Intelligence Community Directive Number 301, National Open Source Enterprise*, <<https://irp.fas.org/dni/icd/icd-301.pdf>>.

2015/10/28. “Open-Source Center (OSC) Becomes Open-Source Enterprise (OSE),” *Federation of American Scientists*, <<https://fas.org/blogs/secrecy/2015/10/osc-ose/>>.

2015/11/8. “Establishment of the DNI Open Source Center Press Release,” *Central Intelligence Agency*, <<https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr11082005.html>>.

Benavides, E. Ben, 2009/2. *Targeting Tomorrow's Terrorist Today*

- (T4): *Through Open Source Intelligence*, <http://wikileaks.wikimee.info/gifiles/attach/8/8871_Targeting%20Tomo.pdf>.
- Department of Defense, 1982/12. *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, <<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/524001r.pdf>>.
- Headquarters Department of the Army, 2010/3/23. “Army Field Manual FM 2-0: Intelligence,” *FAS Intelligence Resource Program*, <<https://irp.fas.org/doddir/army/fm2-0.pdf>>.
- Steele, Robert D., and Mark M. Lowenthal, 1998/5/5. “Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations,” *Defense Daily Network Special Report*, <<https://irp.fas.org/eprint/oss980501.htm>>.