《安全與情報研究》第七卷第二期　　中華民國 113 年 7 月
Security and Intelligence Studies, Vol. 7, No. 2　　July 2024

暗網資訊蒐集分析之運用與挑戰

賴義鵬

中央警察大學資訊管理學系助理教授

摘 要

隨著網路技術的快速發展，網路上的情報資訊變得日益豐富多元，各國也開始重視對網路公開情報的蒐集工作。網際網路中明網、深網和暗網等不同層面的區別變得更加明顯。本文探討了在暗網中如何主動進行資訊爬取的議題，然而由於暗網中存在許多重複內容的網站，可能是為了反情報目的而設立的，因此在進行資訊蒐集時必須特別注意身份的隱匿性。此外，本文介紹了資訊查證分析的 3 個參考面向，以確保所獲取的資訊的準確性和可信度。由於暗網的匿名性，它也成為吹哨者或內部不滿人士向外界提供資訊的管道。因此，建立被動網站或張貼論壇貼文，進行被動式的接觸，也成為一個重要的資訊蒐集途徑。在暗網的資訊蒐集過程中，結合被動和主動的方法十分重要，同時亦須使用技術工具來保護個人隱私和資訊安全。透過這些方法，可以有效地進行暗網的資訊蒐集，獲取有價值的情報，並確保個人和組織的安全。最後，本文提供了資訊蒐集流程，以幫助讀者更好地理解在暗網中進行資訊蒐集的過程和方法。這些方法和技巧將有助於提升資訊蒐集的效率和準確性，同時保護個人和組織的資訊安全。

關鍵字：資訊網路、情資蒐尋、個資洩漏、暗網

The Utilization and Challenges of Dark Web Information Collection and Analysis

Yeu-Pong Lai

Assistant Professor, Department of Information Management,
Central Police University

Abstract

As network technologies have rapidly developed, the information available on the internet has become increasingly rich and diverse, prompting nations to pay more attention to the collection of open-source intelligence (OSINT) from the internet. The distinctions between the clear web, deep web, and dark web on the internet have become more pronounced. This article discusses the issue of proactively crawling data on the dark web. However, due to the presence of many websites with duplicate content on the dark web, which may have been set up for counterintelligence purposes, it is crucial to pay special attention to the anonymity of one's identity when collecting data. Furthermore, the article introduces three reference aspects for data verification and analysis to ensure the accuracy and reliability of the acquired information. The anonymity of the dark web also makes it a channel for whistleblowers or disgruntled insiders to provide information to the outside world. Therefore, establishing passive websites or posting on forums to engage in passive contact has also become an important intelligence collection method. In the process of collecting intelligence on the

dark web, combining passive and active methods is crucial, while also using technical tools to protect personal privacy and information security. Through these methods, it is possible to effectively collect intelligence on the dark web, obtain valuable information, and ensure the safety of individuals and organizations. Finally, the article provides a data collection process to help readers understand the process and methods of collecting intelligence on the dark web. These methods and techniques will help improve the efficiency and accuracy of intelligence collection while protecting the information security of individuals and organizations.

Keywords: Information Network, Intelligence Search, Personal Information Leakage, Dark Web

壹、前言

資訊發展促進了網路技術的進步，使得網路速度更快、傳輸頻寬更大、資訊內容更多元，也促進了社群資訊交流的蓬勃發展，使得人們可以透過社群媒體與來自世界各地的人們分享資訊和意見。所以對於資訊蒐集的管道與方法也更加多元，除了傳統的書籍、雜誌、報紙等紙本資訊，亦可透過網路、社群媒體、手機 APP 等多種管道蒐集資訊，而一般網站，為吸引使用者連接與增加曝光度，無不以令人熟悉好記憶的網域名稱來命名，希望用搜尋引擎即可搜尋得到，並希望能提高自己網站在蒐尋結果的排名；有些網站內容則限制成員才可以取得，因而需要使用帳號密碼授權與登入，來進行資訊的交流，交流內容無法輕易公示與大眾，這些網路名為深網；然而也有一些網站，需要特殊的瀏覽器、特殊授權或是特殊設置才能訪問的網路，稱之為暗網，其上的資訊是隱蔽的，一般人很難找到，因為其隱蔽性，暗網也成為犯罪者習慣使用的非法物品交易管道或是情資交換的平臺，這是因為暗網非常複雜且不斷變化，網站域名時常更換變動與關閉，所以需要專門的知識和技能才能有效的蒐集情資。

針對明網可以藉由網路平臺或是通訊軟體來進行蒐集，對於情資蒐集有需求的公司，多會設計網路爬蟲程式，對特定網路的平臺或是公開的網路社群進行資訊蒐集，此外也可採人工的方式，由搜尋引擎網站來進行大範圍議題式的情蒐，如 google 搜尋引擎的搜尋方式可以使用「關鍵字 + 空格 +site:ptt.cc」來搜尋特定網站，在此例中為對 ptt.cc 網站進行關鍵字搜尋；使用「inurl: 關鍵字」來搜尋與關鍵字相關網頁連結；使用「intext: 關

鍵字」來搜尋與關鍵字有相關的網頁內容；使用「關鍵字 + 空格 +filetype: 檔案類型」來搜尋搜尋與關鍵字相關特定類型檔案。

然而，近年來因為個人資料保護議題的重視，以及歐盟要求與之進行貿易或提供服務的商業公司與網路平臺，必須遵循其所訂定的《一般資料保護規則》(General Data Protection Regulation, GDPR)，因此許多網站限制僅可由已登入會員來進行資訊的閱讀與查找，以及許多社群團體設定為不公開閱覽，即搜尋引擎或是爬蟲程式無法逕行取得內容，這類的網路屬深網，所以進行情資蒐尋僅能藉由內部吹哨者；或是創建該平臺帳號、申請加入此封閉社團或是以打入方式進行目標會員接觸請求邀請加入；加入社團後蒐集相關情資，進行內部拉攏的拉出方式，針對社團中帳號名稱進行其他網路平臺帳號搜尋，如採用使用者名稱搜尋線上網站 https://namechk.com/ 等，來多方面了解社團帳號使用者；再探究活動與犯罪情資進行提前預警；針對社團中的資訊進行資料備份與保存；對於保存的資訊進行人別確認與涉案追查，以型繪現實環境中該活動的真實性與關聯性。

深網中有更進一步以特殊瀏覽器與通訊協定來進行社群資訊分享或是物品販售的暗網，因為網站主機與連線的使用者主機皆在隱匿的安全網路中，所以無法確認主機實際位址，對於人員身分的掌握十分困難，也導致無法進行前述的查證，不過對於打入相關環境與社團來蒐集情資，仍為情資蒐集工作中值得發展的一環。

基於國家安全與情報目的手段或針對犯罪的犯罪偵查手段，皆須受法律所規範，有一定的授權範圍與核准程序，如《通訊保

障監察法》第 10 條「依第 7 條規定執行通訊監察所得資料，僅作為國家安全預警情報之用。但發現有第 5 條所定情事者，應將所得資料移送司法警察機關、司法機關或軍事審判機關依法處理」；《國家情報工作法》第 6 條「情報工作之執行，應兼顧國家安全及人民權益之保障，並以適當之方法為之，不得逾越所欲達成目的之必要限度」，第 7 條「情報機關應就足以影響國家安全或利益之下列資訊進行蒐集、研析、處理及運用」。可見國家安全與犯罪偵查皆是為了發現真實，針對人所做的行為進行資訊的蒐集，因此本文以犯罪偵查所需取得情資為軸心來進行分析討論。

隨著科技的進步，資訊蒐集的管道日漸多元，有些使用者資訊與業務資訊遭大型資訊公司暗地進行記錄，而被做為其他應用，如大型語言模型訓練，因這些資訊已被轉化至模型架構參數中，可能藉由適當的大型語言應用操作來取得相關的訊息，這些都是情資可能的來源管道，但是最重要的還是要進行情資價值與正確性評估，下一節將就情報蒐集分類、公開情報蒐集等方向進行討論，再針對學者所提出可對暗網身分進行查證的文獻進行介紹，第參節則就情蒐方法進行討論，先討論暗網中網站的分布與內容等概況，再說明暗網中各式情資蒐尋的管道，然後以主動與被動方式來進行情蒐。

在主動情蒐方面，本文將提供 Linux 系統指令，說明如何操作；至於被動情蒐方式，則可採建立網站或於論壇發言，本文並以美國中央情報局 (CIA) 建立網站，等候暗網使用者與其聯繫或於暗網招募員工，做為案例說明。此外，本文也強調情蒐時須以技術工具保護個人隱私和資訊安全，以保護個人和組織的安

全，因為暗網中也可能成為反情蒐的管道。根據帕斯德·加林多亞 (Pastor-Galindoa) 等人於 2024 年 1 月的研究報告顯示，他們在 93 天內，用自動化系統識別了 80,049 個洋蔥網站服務，並描述了其中 90% 的特徵，發現內容多為重複，只有 6.1% 的網站是獨立提供資訊，亦即許多網站可能為假網站，或是被利用來進行反情蒐的網站，[1] 所以在暗網中進行特定議題的情蒐時，需要注意保護資訊安全，以免成為對方反情蒐或反情報的對象。

貳、文獻探討

一、情報蒐集的途徑與分類

情報的蒐集為一古老的議題，而隨著國家組織架構、蒐集目標、科技進步、情資儲存方式等面向的變遷而有改變。英國國防部對於情報領域 (Intelligence Discipline) 分類如後：(1) 聲學情報 (Acoustic Intelligence, ACINT)、(2) 地理空間情報 (Geospatial Intelligence, GEOINT)、(3) 影像情報 (Imagery Intelligence, IMINT)、(4) 人員情報 (Human Intelligence, HUMINT)、(5) 測量與特徵情報 (Measurement and Signature Intelligence, MASINT)、(6) 公開來源情報 (Open Source Intelligence, OSINT)、(7) 訊號情報 (Signals Intelligence, SIGINT)、(8) 材料和人員利用 (Materiel and Personnel Exploitation, MPE)。[2]

---

[1] Javier Pastor-Galindoa, Hông-Ân Sandlin, Félix Gómez Mármola, Gérôme Bovetb, and Gregorio Martínez Péreza, "A Big Data Architecture for Early Identification and Categorization of Dark Web Sites," *Future Generation Computer Systems*, Vol. 157, No. 2 (2024), pp. 67-81.

[2] United Kingdom Ministry of Defense, *Joint Doctrine Publication 2-00:*

「聲學情報」(ACINT) 是從聲學現象的蒐集和處理中獲得的情報，如潛艇、傳感器、和船隻所蒐集的海底情報；「地理空間情報」(GEOINT) 是從影像和地理空間資訊分析獲得空間和時間的情報，通常輔以額外的情報來源進行補充；「影像情報」(IMINT) 是指源自於地面、海上、空中、或太空的傳感器所獲取的影像，可以勘校其他情報或是做為定位的情報；「人員情報」(HUMINT) 是指來自人的情報，是由個人提供之資訊或是經由互動與監視所蒐集得到的情報；「測量與特徵情報」(MASINT) 是指來自於傳感器的數據分析，可用於識別任何來源、發射器、或發送者的情報；「公開來源情報」(OSINT) 是指來自公開可用資訊的情報，目前如媒體監測、學術團體、和民間行業都可能提供有價值的情報；「訊號情報」(SIGINT) 是指接收非指定接收者的電子通訊以及電磁傳輸訊號，包括攔截雷達發射訊號與電子識別訊號；「材料和人員利用」(MPE) 是指系統性蒐集拘留個人或是回收材料所取得的情報，包含了鑑識、醫療、金融、化學、武器、和技術等面向。

若是將前述的分類方式應用在情報操作的人員辨認與事實細節的拼湊上，可概略轉化為：(1) 公開來源情資 OSINT 包含網路巡邏與情蒐、應用社群網站帳號與內容、論壇網站帳號與內容、通訊軟體帳號與內容等；(2) 人員情資 HUMINT 項目包含調查筆錄、報案筆錄、檢舉證人筆錄、第三人提供等；(3) 訊號資訊情資 SIGINT 包含線上監聽、通信紀錄、手機聊天內容、網站連線紀

Understanding and Intelligence Support to Joint Operations (JDP 2-00), August 2011, pp. 2-11~2-14.

錄等；(4) 地理空間資訊情報 GEOINT 包含監視器影像、高速公路 ETC 記錄、基地臺紀錄等；(5) 測量與特徵資訊情資 MASINT 包含現場生物跡證、槍彈鑑識、數位鑑識等。

二、公開情報蒐集

英國國防部所述的情報蒐集目標主要是為了軍事目的，我國許多的靜態情資業已由警政單位與其他機關進行網路交換方式來取得，並儲存於相關的資料庫系統之中，如國民身分證資料、入出境資料、車籍資料、刑事案件資料、同囚會客資料等，所以犯罪偵查人員與犯罪預防單位，要進行犯罪偵查或是治安狀況情資分析，尤要對「公開來源情報」進行資訊蒐集，才能掌握動態的資訊態勢，以充分利用資源以整合資訊來強化與理解所得資訊，但也因為網際網路與資訊技術的發展，大量資訊可以由網路取得，可用資訊（正確資訊）和錯誤資訊（假訊息）持續增加，早期蒐情者與分析者是分開的角色，但是現在最好的蒐情者不是一個間諜，也不是一顆衛星，而是一個受過專業訓練的分析師，[3] 需要分析師來整理與判斷。

1993 年英國肯特 (Kent) 警察局推行肯特警政模式 (Kent Policing Model)，此模式除了強調針對罪犯所做的核心調查，並更有策略性的運用線民，將情資納入決策，為情報導向警政 (Intelligence-Led Policing) 的開端，[4] 情報導向警政採用最新技術

[3] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (New York: Cambridge University Press, 2003), p. 10.

[4] Bureau of Justice Assistance (BJA), *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice, 2005/09), p. 9. <https://www.ojp.gov/pdffiles1/

來蒐集和分析數據，使警方取得有價值的情報。這些情報資訊可用於部署警務人員和有限的資源，以便在最需要警力的社區進行高效、有效的執法。同時，情報導向警政也與社區成員及其他執法機構建立合作關係，蒐集有關犯罪活動的觀察和情報，所以情報的蒐集、分析與運用，及與其他執法機構的情報分派與分享，成為情報導向警政中重要的一環。傳統常見的情報蒐集方式有：實體監視（親自監視或由調閱監視影像）、電子監視（定位追蹤或竊聽）、線民、臥底人員、報紙報導與網路來源、歷史記錄（例如戶役政、刑案資料、車籍資料、契約、財產稅記錄等）。[5]

1996 年美國「亞斯平－布朗委員會」(Aspin-Brown Commission) 調查報告要求情報部門善用公開資訊，[6] 但明網與深網中的公開資訊十分龐雜，明網中的資訊，司法警察可以經由資料的調閱，取得登記、交易、使用紀錄、登入紀錄等歷史資訊，來進行犯罪偵查及資訊蒐集，再佐以身分查證、通訊紀錄、金流流向、前案紀錄、人際網路、行跡作息等面向的資訊進行分析，其後持續深入與調閱資料以求發現事實。犯罪可概分為有被害人的犯罪與無被害人的犯罪，例如財產犯罪、暴力犯罪、侵犯隱私犯罪、欺凌犯罪等是屬於有被害人的犯罪，而毒品犯罪、賭博犯罪、金融犯罪、環境犯罪、國家安全犯罪、選舉犯罪等屬無被害人的犯罪。在案件偵查的過程中，有被害人的犯罪，可自被害人所提供的犯罪者

bja/210681.pdf>.

5 Ibid., p. 6.

6 Morten Hansen, “Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community,” *Intelligence and National Security*, Vol. 29, No. 1 (2014), p. 64.

接觸面向為始，如人流、金流與資訊流等進行資料的蒐集與查證，再加上偵查人員的分析與推測進行下一階段的查訪與資訊蒐集；對於無被害人的犯罪，須由偵查人員進行相關的情資蒐集，擴大情資來源的管道，並經過持續的過濾與篩選，逐步查證，以及依之前的來源與事件，研判目前取得的情資可信度。

三、暗網公開情報蒐集流程

有關在暗網中進行情報蒐集的方法，旺楚克 (Tashi Wangchuk) 與拉托德 (Digvijaysinh Rathod) 提出了一個暗網調查框架，可在暗網蒐集資訊以獲取公開來源情報 (OSINT)，[7] 他們以 Dark2Clear 工具抓取暗網網站隱藏的服務 URL，進行暗網用戶電子郵件地址以及其他可疑電子郵件位址的蒐集，並將蒐集的電子郵件與公開來源情報比對，以進一步辨識及追查使用者身分（流程如圖 1）。

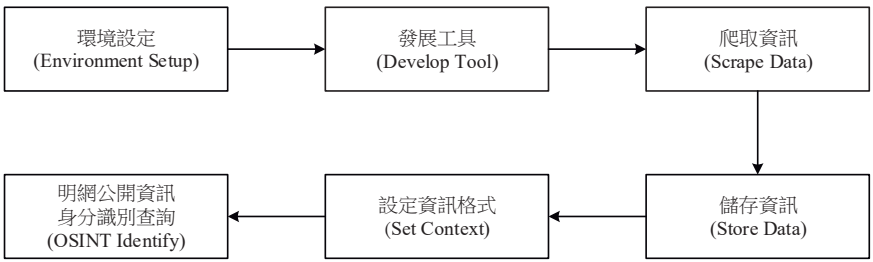


圖 1：Tashi Wangchuk 等人的暗網使用者身分識別流程

資料來源：Tashi Wangchuk and Digvijaysinh Rathod, "Opensource Intelligence and Dark Web User De-Anonymisation," *International Journal of Electronic Security and Digital Forensics*, Vol. 15, No. 2 (2023), p. 149.

[7] Tashi Wangchuk and Digvijaysinh Rathod, "Opensource Intelligence and Dark Web User De-Anonymisation," *International Journal of Electronic Security and Digital Forensics*, Vol. 15, No. 2 (2023), pp. 143-157.

德瓦拉詹 (Sasirekha Devarajan) 等人則是設計程式來系統性的蒐集和清理暗網頁，來研究專門銷售非法和有害產品的暗網市場，爬蟲模組透過洋蔥路由 (Tor) 網路，蒐集有關產品、賣家和價格的關鍵資訊，資料清理模組清理和組織爬蟲程式的數據保持其完整性並將其轉換為可處理的格式，資料探勘模組使用聚類、分類和關聯規則資料探勘等技術從處理的資訊中提取知識來識別與了解趨勢（如圖 2 所示）。[8]

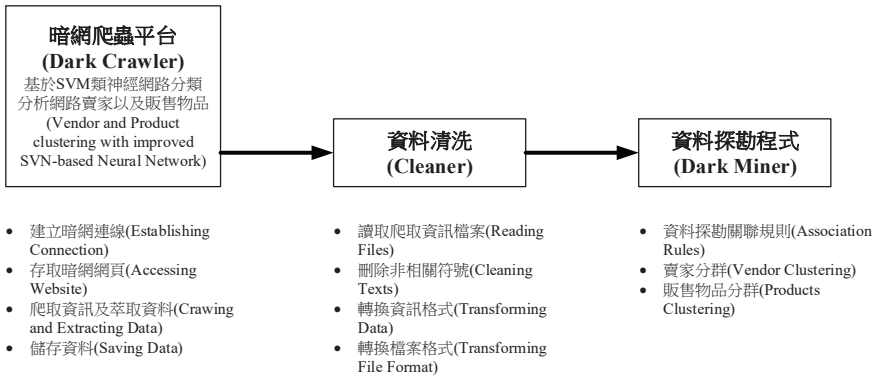


圖 2：Sasirekha Devarajan 等人的暗網爬蟲分析流程

資料來源：Sasirekha Devarajan, et al., “Enhancing Dark Web Classification: A Dynamic Crawler and Robust Classification Framework,” *International Journal of Intelligent Systems and Applications in Engineering,* Vol. 12, No. 6S (2024), p. 4.

亞達夫 (Ashok Yadav) 等人也提到如何以電子郵件輔以公開情資來進行身分調查（如圖 3 所示）。以電子郵件來查找搜尋引

[8] Sasirekha Devarajan, Pakutharivu Panneerselvam, Aditya Mudigonda, and Perichetla Kandaswamy Hemalatha, “Enhancing Dark Web Classification: A Dynamic Crawler and Robust Classification Framework,” *International Journal of Intelligent Systems and Applications in Engineering*, Vol. 12 No. 6S (2024), pp. 1-9.

擎、外泄資訊、及電子郵件查詢工具等，查詢是否得知該電子郵件的使用人；另外也可以電子郵件名稱來查詢社群網路是否相似的帳號名稱；以及針對郵件表頭來查詢組織單位網域名稱，或是電子郵件正文檢查內容的語言、簽名和附件等等；圖中 Received-SPF 欄位包括寄件者的 IP 位址以及主機名稱，此外也有些參數，例如 pass，表示郵件來源有效、soft-fail 表示可能來源為虛假的、neutral 代表來源有效性但很難判斷為確定或未知。至於亞達夫等人文中提到使用調查查詢的工具則包括：Email dossier、Email hippo、Hunter、Email Checker、Email Validator、scamdex、ipTRACKERonline 等。[9]

金敏傑 (Minjae Kim) 等人則是以加密貨幣金流與暗網中留言的評論來進行比較，來進行人別地確認。首先，他們透過對人工所蒐集的暗網交易數據進行深入分析，例如文中有採用 2020 年 5 月 7 日至 2020 年 9 月 14 日期間所發生的 40,415,437 筆交易進行實驗，發現包含比特幣價格和物品交付的交易資訊，確定了與所揭露的資訊相關的比特幣地址，將使用人所使用的各錢包與交易相關幣流整理特徵，而提出一個比特幣多層啟發式演算法。根據他們的實驗結果顯示，大約 31.68% 的暗網市場評論資料數據與真實的比特幣交易相符，並且發現 122 個與絲綢之路相關的隱藏加密或幣錢包集群，判斷的假陰性率 (false negative) 高達 91.7%。[10]

---

[9] Ashok Yadav, Atul Kumar, and Vrijendra Singh, "Open-Source Intelligence: A Comprehensive Review of the Current State, Applications and Future Perspectives in Cyber Security," *Artificial Intelligence Review*, Vol. 56 (2023), pp. 1-32.

[10] Minjae Kim, Jinhee Lee, Hyunsoo Kwon, and Junbeom Hur, "Get off of

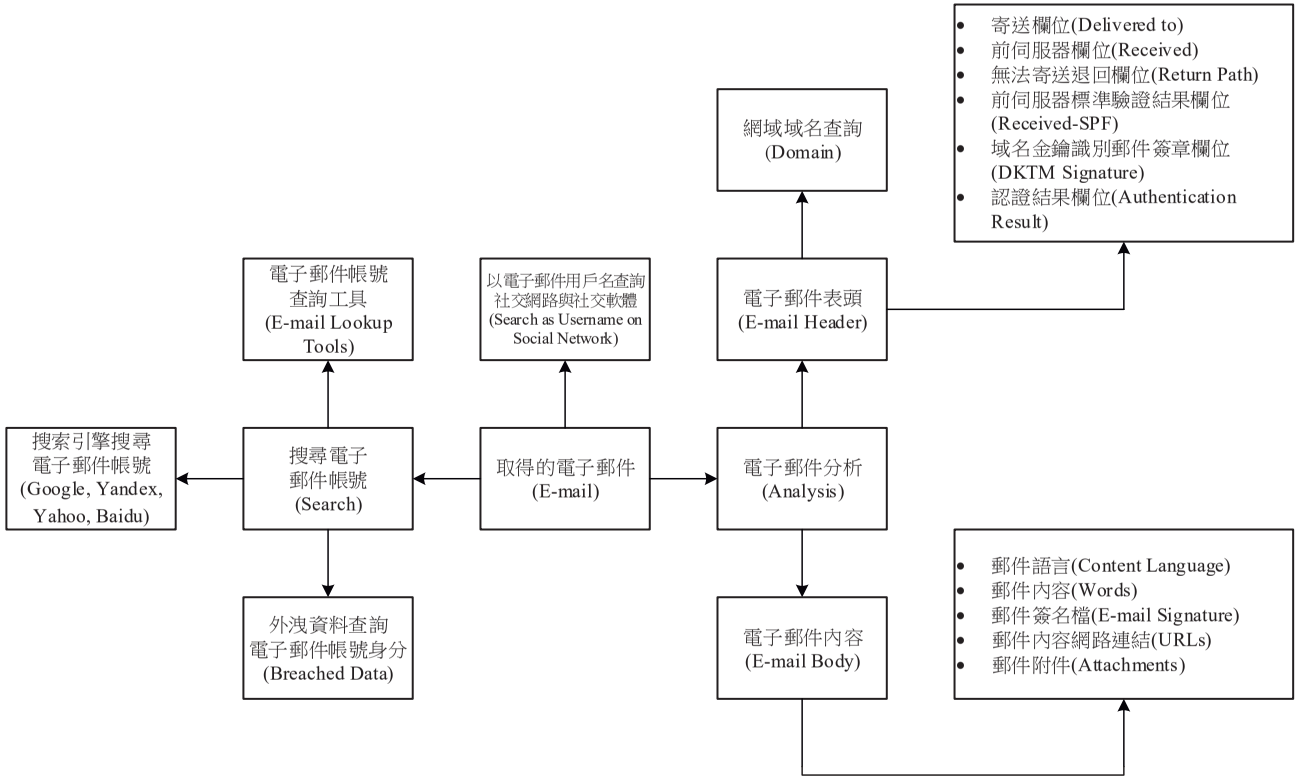


圖 3：Ashok Yadav 等人所提 E-mail 調查攻擊介面

資料來源：Ashok Yadav, Atul Kumar, and Vrijendra Singh, “Open-Source Intelligence: A Comprehensive Review of the Current State, Applications and Future Perspectives in Cyber Security,” *Artificial Intelligence Review*, Vol. 56 (2023), p. 17.

參、暗網情報蒐集

本文所探討之暗網情報蒐集方法，是針對在暗網中可能影響國家安全或利益的資訊，進行蒐集、或分析資訊來源管道與可能的提供者；至於真實性與其他已知徵候或其他管道取得情資的交互應證等研析，須由其他單位與人員執行，因此，無涉後續情報處理和運用，以及應用保防、偵防和安全管制措施反制外國或敵對勢力等問題，換言之，本文所分析之情蒐方法與蒐集策略，僅限於暗網資訊蒐集層級。

一、情蒐範圍與挑戰

在知名防毒軟體廠商卡巴斯基 (Kaspersky)[11] 與艾維斯特 (Avast)[12] 的官方網頁中，有提及深網 (deep web) 與暗網 (dark web) 的介紹，與這 2 家公司在暗網上資訊安全實務深入研究分析的報告。從其報告得知，在網際網路上，這些公共空間 (public spaces) 被稱為表面網路 (surface web)，是網頁、網頁應用程式以及搜尋機器人（或稱為網路爬蟲 web crawler）可以索引，且在明網可以保存文件、媒體文件等資料，任何人都可以使用搜尋引擎找到並查看，無需付費、註冊或安裝特殊軟體。然而，網路也有許多谷歌 (Google)、必應 (Bing) 和其他搜尋引擎無法搜尋到的角落，這

Chain: Unveiling Dark Web Using Multilayer Bitcoin Address Clustering," *IEEE Access*, Vol. 10 (2022), pp. 70078-70091.

[11] Leonid Grustniy, "Darknet, Dark Web, Deep Web, and Surface Web - What's the Difference?," *Kaspersky Daily*, <https://www.kaspersky.com/blog/deep-web-dark-web-darknet-surface-web-difference/38623/>.

[12] Ivan Belcic and Brittany Nelson, "What Is the Dark Web and How to Access It?," *Avast Academy*, <https://www.avast.com/c-dark-web>.

些範圍稱為深層網路 (deep web)。

深網主要由無法透過正常方式搜尋和開啟的所有網路頁面所組成，因為搜尋機器人 (web crawler) 無法對它們建立索引，例如某些網站需要登入帳號密碼與輸入人機驗證 (CAPTCHA) 來避免機器人自動登入進行內容掃描。在深層網路中多數的網站是對使用者是無害而且有用的，而暗網 (dark web) 主要是用於可疑活動 (questionable activities)，使用非標準的通訊協定 (protocols) 來傳送資料，因此多數的瀏覽器無法瀏覽其內容，暗網上可能有毒販、軍火商、敲詐勒索者、與數位資料賣家等在使用，另外也有些持異議政見者、主張言論自由人士、吹哨者 (whistleblowers)、以及更多人使用暗網，逃避迫害者也會在暗網網路上匿名交流。

帕特爾 (Hrishitva Patel) 認為「暗網」是一個術語，允許使用者保持匿名、秘密開展業務以及存取無法透過傳統方式獲取資訊的網路。[13] 因為暗網使他們能夠隱藏自己的搜尋行為，無論這些行為是否涉及非法活動。由其所蒐集的資訊來判斷，無法確切知道暗網中網站的數量，估計約在 10,000 到 100,000 個活動網站，提供匿名販售槍枝、毒品、外洩的個人資訊、甚至人口販運資訊。因為匿名性，讓使用者得以在不受審查的環境中自由、公開地討論想法，所以情報單位可以運用機會存取各種來源的數據，如國家安全威脅的情資、策劃恐怖攻擊的情資、洗錢和其他非法活動的資訊，由於暗網能保護資訊提供者及消息來源的安全，如果情報單位善用暗網，將可取獲具有價值的情資。

[13] Hrishitva Patel, "Comparison of Data Fluctuations that Lead to Cyber Security Attacks: A Difference between Surface, Deep and Dark Net," *Asian Journal of Research in Computer Science*, Vol. 16, Issue 4 (2023), pp. 297-308.

帕斯德·加林多亞 (Pastor-Galindoa) 等人曾經使用 Kubernetes 容器管理軟體來建立虛擬主機處理叢集，其上部署 Kafka 軟體來進行資訊的訂閱與蒐集，並以 MinIO 物件來進行非結構化資料的儲存，再用 Kubeflow 模型開發平臺來進行訓練建模與分析的工作，所建立的系統不斷的自不同來源（threat intelligence 威脅情報、code repositories 程式碼儲存庫、web-Tor gateways 明暗網閘道和 Tor repositories 儲存庫），以洋蔥路由 (Tor) 網路下載 HTML 並使用 MinHash 與 LSH 文本相似計算來對內容進行重複資料刪除，以及使用 BERTopic 主題建模技術來建模。在 93 天內，系統識別了 80,049 個洋蔥網站服務，並描述了其中 90% 的特徵，發現內容多為重複，只有 6.1% 的網站是獨立提供資訊，自暗網的 HTML 文件中，發現 5 個最受歡迎的內容包括性和暴力內容、資料庫、搜尋引擎、carding 梳理、加密貨幣和市場。在其實驗中，發現了 14 個網站有 13,946 個複製網站，這些網站每天的鏡像率非常相似，這表示暗網中可能有許多網路釣魚的假網站。[14]

二、暗網網路情蒐搜尋引擎

明網中有各大搜尋引擎軟體爬取網路上網站的內容提供使用者查詢，而這些明網中的搜尋引擎無法取得暗網中的資訊。因此暗網中使用異於明網的搜尋引擎，常見的有 Ahmia、Haystak、Torch、DuckDuckGo、Not Evil、DarkSearch 等，使用這搜尋引擎可以更好地隱藏用戶的 IP 位址和位置資訊，來提高匿名性；也

[14] Javier Pastor-Galindoa, Hông-Ân Sandlin, Félix Gómez Mármola, Gérôme Bovetb, and Gregorio Martínez Péreza, "A Big Data Architecture for Early Identification and Categorization of Dark Web Sites," *Future Generation Computer Systems*, Vol. 157, No. 5 (2024), pp. 67-81.

能夠索引到明網搜尋引擎無法抓取的隱藏網頁和暗網網站，搜尋範圍更廣。暗網搜尋引擎通常不會記錄用戶的搜尋歷史和個人資訊，可以提供更好的隱私保護；此外，因為 IP 位址的匿名與變動，查詢到的資料不限於某些網路審查和封鎖，或僅提供該地區性的資料，因此搜尋者可以獲取更多資訊，也包括各種非法資訊，如毒品、武器交易等資訊。

有些暗網網站僅羅列在暗網中存在的時間長短排序，如 The Hidden Wiki 網站、Tor Links 網站等，蒐集者也可以由這樣的列表來進行目標網站網址的蒐集，或是由新聞網站或是論壇來取得資訊，如 ProPublica 網站、DeepDotWeb 網站、Dread forum 網站。

三、主動方式蒐集資訊

針對暗網中資訊的蒐集方式，可以設計爬蟲程式進行網站資料複製蒐集，或以加入論壇透過貼文與回應的方式。在此先使用 torsocks 程式來進行 shell 包裝，進入洋蔥路由 (Tor) 網路，在這樣的 shell 下執行命令並隱藏 IP 位址，或是將 proxychains 設定為連接洋蔥路由 (Tor) 網路，再由 proxychains 來 disb 網站，可以使用的指令如下：

```
$sudo apt install tor torsocks
$sudo systemctl start tor
$torsocks -p 9050 dirb https://target.onion
或是
$sudo apt install tor torsocks proxychains
$sudo systemctl start tor
$socks5 127.0.0.1 9050
$proxychains disb https://target.onion
```

進行這些操作時，需注意是否有發生前節所述，下載的網站內容是否為偽造的網站，以免被反滲透，或是取得假資訊。故需再就網站進行檢測，例如以 nikto 檢驗（指令如下：$torsocks -p 9050 nikto -host https://target.onion），以免該網站為蜜罐 (Honeypot) 或是遭植入 clickjacking 的程式碼，若網站遭植入 clickjacking 程式碼，則連接該網站上的 hyper-link 會被重導連接到其他網站。

蜜罐是模擬成有價值的目標系統或資源，以吸引攻擊者進行攻擊，從而蒐集攻擊者的行為和工具，如果設計的爬蟲程式連接入蜜罐，取得的資訊可能是為防範資料洩漏而製造的假資料，且可能被反向植入惡意程式而遭追蹤。前述的 clickjacking 是一種隱藏惡意程式碼的攻擊手段，通常將惡意內容隱藏在看似無害的元素（如鏈結或是按鈕圖示）下，誘騙使用者點擊，如利用 iframe 將目標網頁嵌入惡意網頁中，當爬蟲程式搜尋觸發點擊時，實際上是在點擊被隱藏的目標網頁上的元素，從而導致重定向到其他網站。

四、被動方式蒐集資訊

由於暗網的匿名性，可取得內部吹哨者或是對組織不滿人員所提供的資訊，或是使我方的潛伏人員，以安全的方式秘密遞送資訊。美國中央情報局 (CIA) 也在暗網中架設網站進行人員的招募。CIA 的暗網網址為 : ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion，其網頁如圖 4 與圖 5，15 可供人員

[15] 參見 CIA 的暗網網站網址 <http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion>.

在線上進行資料填報申請，馬庫奇 (Ben Makuch) 在 2019 的報導指出，美國的情報機關已經開始利用暗網，例如，CIA 在一份新聞稿中宣布推出自己的洋蔥網站，CIA 公共事務主任布拉梅爾 (Brittany Bramell) 也指出：「我們的全球使命要求個人可以從任何地方安全地造訪、接觸我們，創建洋蔥網站只是我們走向人們所在之處的眾多方式之一」。[16] 由新聞稿中可以看出，CIA 運用暗網主要是為了諜報活動：招募和情報蒐集。CIA 在暗網招募人員的做法引起了一些爭議，有人認為，這會破壞暗網的匿名性，並可能導致暗網被用於政府監控。然而，CIA 表示，他們在暗網招募人員的做法是安全和合法的，並符合美國的國家利益。

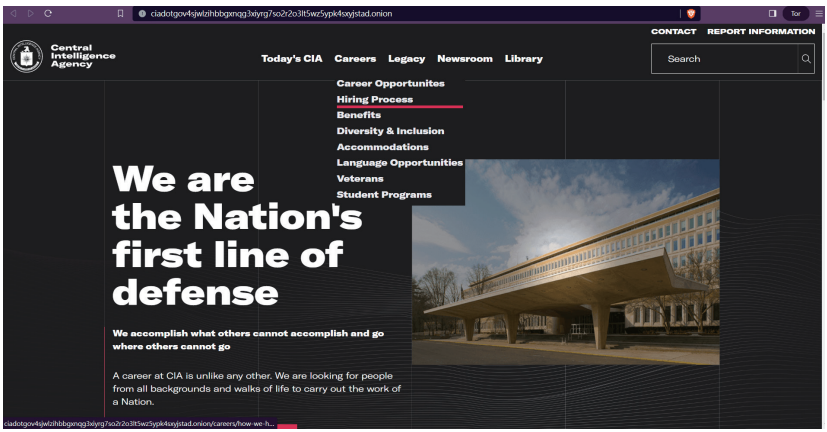
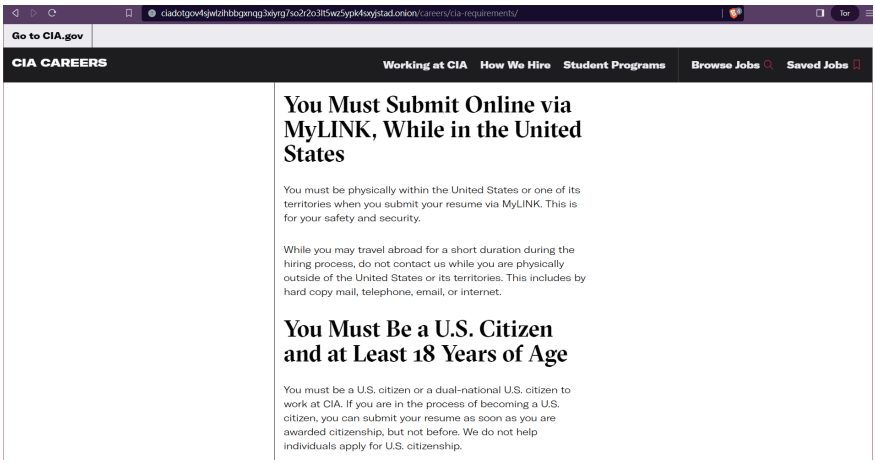


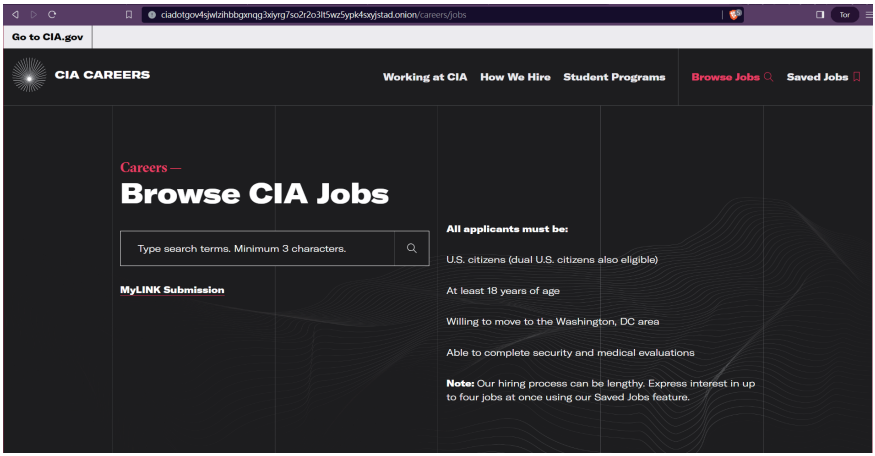
圖 4：美國中央情報局 (CIA) 暗網首頁

資料來源：
<http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion>

[16] Ben Makuch, “The CIA Will Use its New Dark Web Site to Collect Anonymous Tips,” *Vice Media*, May 8, 2019, <https://www.vice.com/en/article/xwnyew/the-cia-will-use-its-new-dark-web-site-to-collect-anonymous-tips>, 存取日期：2023 年 10 月 9 日。



(a)



(b)

圖 5：美國中央情報局 (CIA) 運用暗網進行人員招募

資料來源：<http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion>

CIA 在暗網招募人員的優點包括：可擴大招募範圍、提高安全性、降低成本等，因為暗網是一個相對封閉的網路，不受政府監管，可以接觸到更多傳統管道難以接觸到的潛在人員。例如，在暗網中，CIA 可以接觸到對政府不滿、希望向西方提供情報的外國人；而暗網的匿名性也可以幫助 CIA 保護潛在人員的安全。在傳統管道中，潛伏人員或情報提供人員在與 CIA 探員聯繫時，可能會面臨被政府監控或報復的風險，但是在暗網中，潛伏人員或情報提供人員可以透過加密工具和匿名通信手段與 CIA 探員聯繫，以降低被發現的風險。

此外，在暗網中招募人員或是取得情報可以降低 CIA 的招募成本與相應的風險。在傳統管道中，CIA 需要投入大量人力和物力來招募人員，進行人別確認與價值評估，是以人為本，而暗網招募可能轉變為以資訊為本，雖然除已特定知道真實身分的潛伏人員或情報提供人員外，其他匿名資訊提供者，可能因為暗網的匿名性，無法與之連絡，而有失聯的狀況，不過也因為有匿名提供者，使得情資取得的管道可以擴展。為此，CIA 在暗網中建立了官方網站，提供招募資訊和聯繫方式，並在暗網論壇和聊天室發文，以主動接觸聊特定天室中成員，擴大接觸範圍招募人員，另外也在暗網中留下明網社交媒體帳號，如 Instagram 帳號：@cia，讓暗網用戶可以直接以其他管道接觸進行招募。

綜上所述，本文整理了暗網情蒐的方法，並以圖 6 顯示。首先，依據情蒐指導要項於 Tor Shell 下進行加密通道資訊存取，並以暗網搜尋引擎進行網站搜尋與社群留言，後將情蒐目標網站內容進行爬取，與分析蒐集所取得的錢包地址、內容、與電子郵件，

另創建或克隆相似網站，來進行被動式資訊蒐集，前述資訊分析與識別之結果存入資料庫進行後續分發運用，另再就蒐集所獲資訊，進行下一輪深化或特化資訊的蒐集，以此循環。

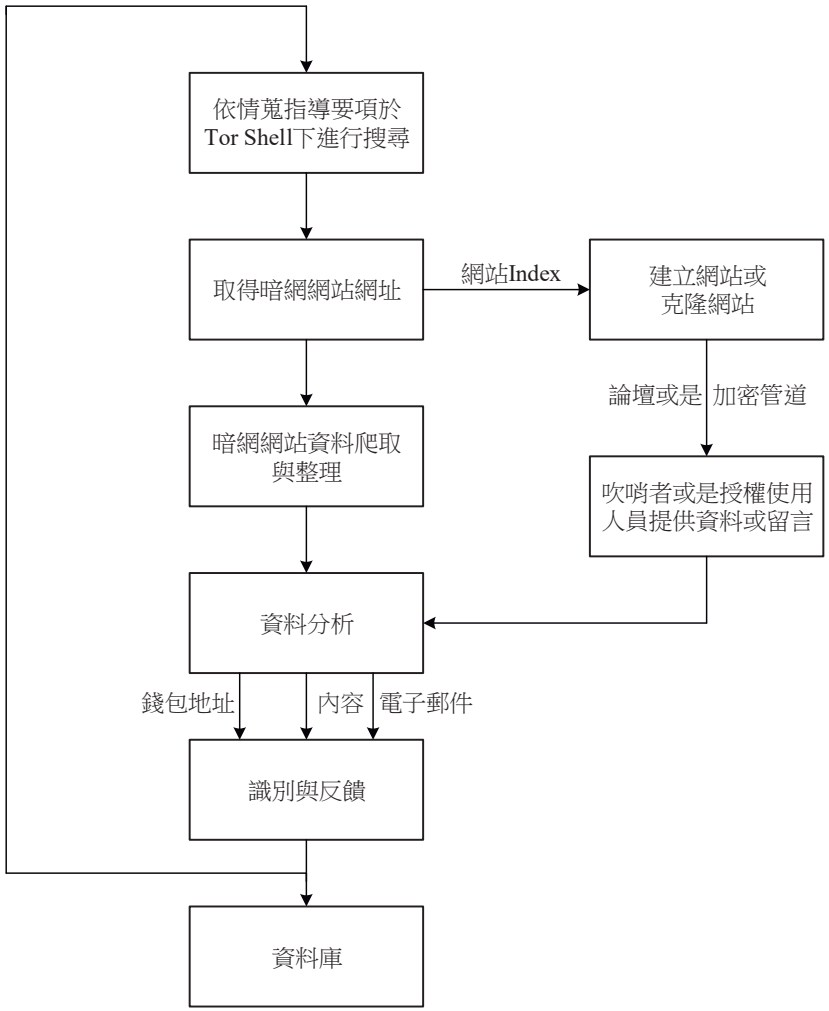


圖 6：暗網資訊蒐集流程

資料來源：作者自行繪製

肆、暗網資訊蒐集的限制與實際案例

一、暗網資訊蒐集的動機與限制

暗網使用者的動機可能包括：(1) 國家利益，例如駭客可能是受國家指使，為了國家利益進行網路攻擊，取得資訊並公布於暗網，由於難以查證來源，他們可以不暴露身分，同時造成公布機敏資料的傷害，也因為這樣的目的，不會留下聯繫的電子郵件與付款資訊。(2) 個人利益：有些使用者為了個人利益，會在暗網上販賣被盜取的個人資料，他們可以通過電子郵件聯繫和加密貨幣付款等方式進行交易，同時隱藏自己的身分。(3) 勒索與威脅：一些使用者會在暗網上勒索他人，並公開部分資訊來威脅恐嚇被勒索者，此時有可能留下（或不留下）相關電子郵件或加密貨幣錢包資訊，端視勒索者的習慣。(4) 情報蒐集：一些國家會利用暗網進行蒐集情報，或是進行反情報活動，以增加資訊的來源與管道，擴大不同群體的接觸方式。(5) 其他非法活動：暗網還可能被用於恐怖組織進行人員招募與募款、販毒、洗錢、雇傭殺手等非法活動，使用者利用暗網的匿名性來逃避法律制裁與執法者的追蹤。

不過，暗網也有連線處理速度之問題，因為暗網是加密通訊的緣故，會有無法連線與反應較慢的狀況，對於取證和聯絡都有一定的困難度。此外，暗網網站也可能因為使用者數量減少而關閉，因其不像明網有廣告或是推播的方式來吸引使用者，所以消失速度很快。使用暗網做為情資蒐集管道時，所得資訊需要用其他資訊進行驗證，因為若是資訊提供者斷絕聯繫，幾乎無法取得

後續資訊，也無法建立穩固與信任的關係，因此需要以其他方式取得的資訊進行後核實驗證，並由這些傳統情資資訊管道進行情資的穩固發展。

表 1：暗網與明網的特性對照表

特性	暗網	明網
網址域名	使用混亂的命名結構創建，往往難以記住	向特定的網域管理機構申請註冊，有特定域名結構與組織定義
訪問方式	需要特殊的瀏覽器、特殊授權或特殊設置	可以使用一般的瀏覽器和搜索引擎
搜尋引擎	不可被公開搜尋	可被公開搜尋
通訊協定	使用特殊的通訊協定，以加密、代理、匿名方式傳輸	標準的 TCP/IP 通訊協定
內容類型	經常包含非法交易、違法活動等	主要包含合法的資訊和服務
使用者	使用者身份和活動痕跡難以被追蹤	使用者身份和活動痕跡可以被追蹤
聯絡方式	使用 PGP 加密來保護通訊內容	通常不會使用加密技術來保護通訊內容
網站存續時間	存續時間通常較短，防執法單位追查致曝光率低，使用者通常需加入特定加密通訊群組以通知網址變更	存續時間長，希望能有高的曝光率與使用者再訪率

資料來源：作者自行整理

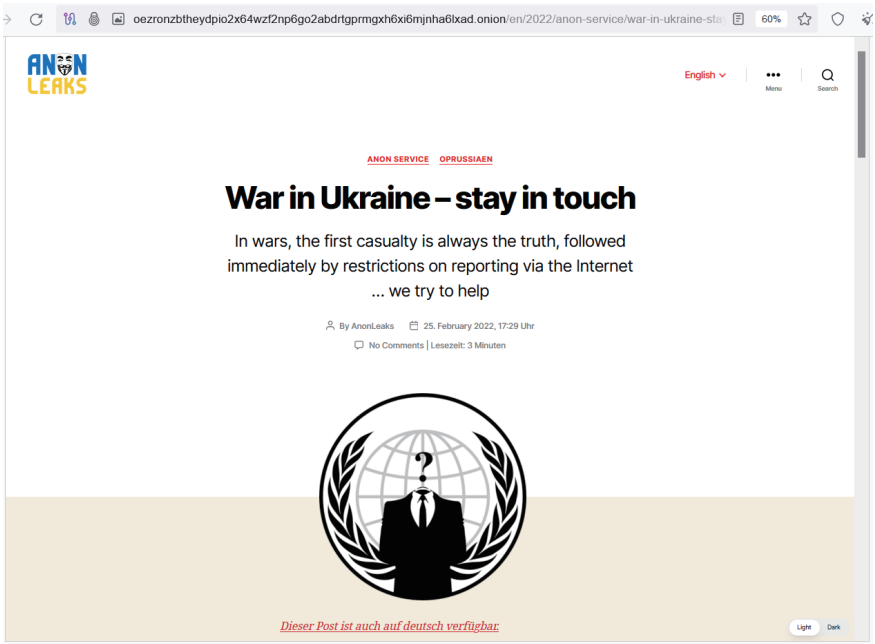
二、實際案例介紹

（一）戰爭情報與恐怖主義運作情報的蒐集

2022 年 2 月 24 日，俄羅斯總統普丁 (Vladimir Putin) 在向俄羅斯全國講話中宣布展開「特別軍事行動」(special military operation)，對烏克蘭發動全面入侵，這是第二次世界大戰以來歐洲最大規模的戰爭之一。然而，俄羅斯在戰爭開始前即已進行網路攻擊。根據報導，俄國利用分散式阻斷服務攻擊 (DDoS) 讓烏克蘭政府相關網站暫時無法使用，特別是在烏克蘭東部盧甘斯克 (Lugansk) 和頓涅茨克 (Donetsk) 的網際網路基地臺服務嚴重中斷。烏克蘭各地也出現零星的網路中斷，美國和歐盟將攻擊歸咎於俄羅斯的軍事情報局 (GRU)。當攻擊開始後，烏克蘭首都基輔 (Kyiv) 與第二大城市哈爾科夫 (Kharkov) 也出現了網路中斷的情況，網路大約只剩下四分之三，但衛星網路受到較嚴重的影響，只剩下 25% 的通訊效能。[17] 同年 2 月 26 日，由於瓦西里基夫 (Vasylkiv) 和基輔兩地出現激烈戰鬥，使得網際網路的骨幹網路供應商 GigaTrans 出現重大斷訊，一度造成網路僅剩兩成的狀況。然而這些斷訊情況並非持續性的。整體而言，網路在 2 月 26 日到 3 月 10 日間大約維持在 8 成到 6 成之間的可用性 (availability)，有時候部分地區的可用性甚至跌到 5 成以下。這些數據顯示，儘管遭受俄羅斯的網路攻擊，烏克蘭的網路基礎設施仍能維持相當程度的運作，但戰爭對網路的影響不可忽視。

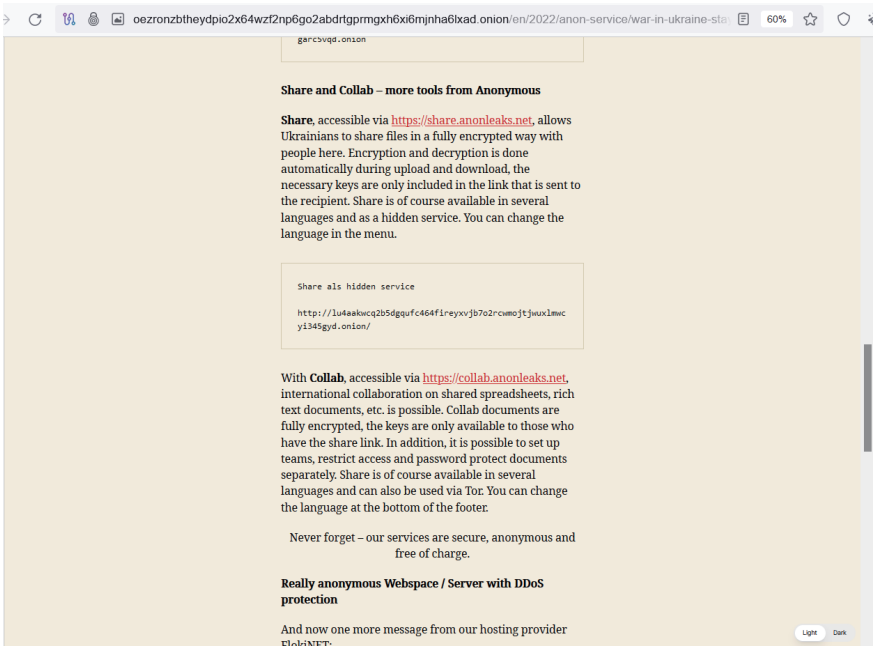
[17] Communications Security Establishment, Government of Canada, 2022. *Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine.*

由於戰爭期間網路仍得以運作，使得烏克蘭民眾紛紛上傳戰爭相關資訊，成為抵禦俄羅斯資訊戰的重要力量。[18] 戰爭爆發後，烏克蘭民眾自發蒐集俄軍動態，上傳給軍方情報單位；民眾共同記錄俄軍在烏的破壞行為，如對民宅、民生設施、油管的攻擊、對校園的轟炸等，在暗網中也有相關的網站供民眾上傳資料。



(a)

[18] 劉致昕、陳映妤，〈來自俄烏資訊戰前線的警告：反制假訊息，別讓絕望吞噬事實和光明〉，《報導者 THE REPORTER》，2022/3/3，<https://www.twreporter.org/a/russia-ukraine-war-2022-information-warfare>。



(b)

圖 7：暗網網站，供民眾上傳戰爭情資

資料來源：
<http://oezronzbtheydpio2x64wzf2np6go2abdrtgprmgxh6xi6mjnha6lxad.onion>

俄羅斯入侵烏克蘭戰爭第 7 天時，俄國攻勢更加猛烈，除了連續轟炸烏克蘭城市，也大軍逐步包圍首都基輔。由於俄方加大資訊戰的攻擊力道，在暗網中出現針對烏克蘭社交工程攻擊資訊的駭客組織，以及鼓吹一般民眾加入攻擊烏克蘭的網站（圖 8）。

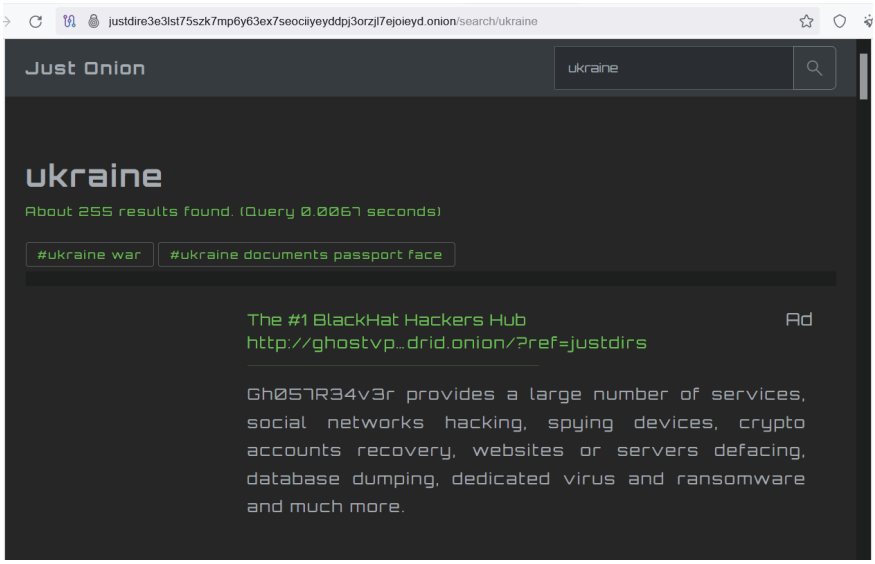
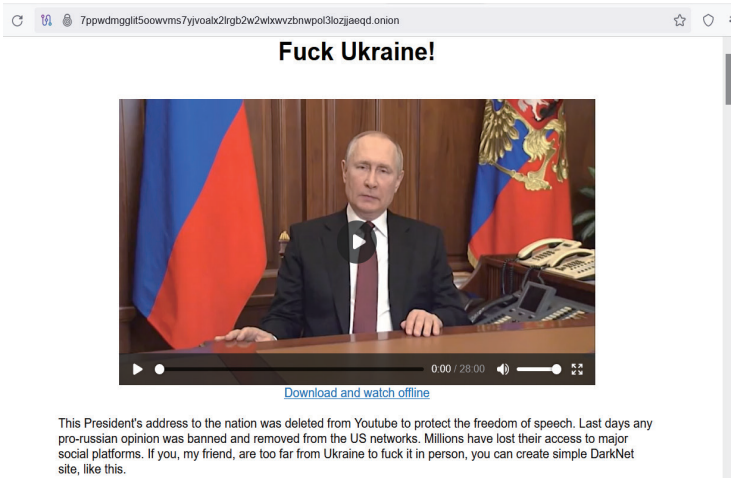


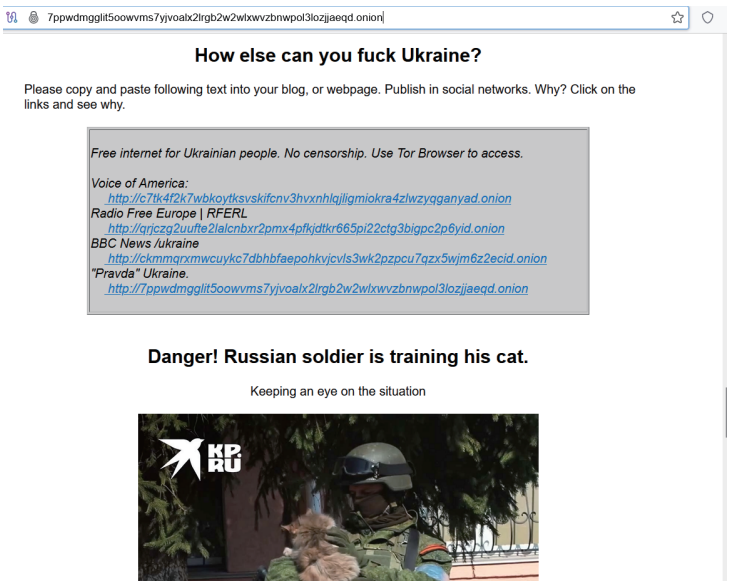
圖 8：提供針對烏克蘭進行社交工程攻擊資訊的駭客組織 Gh057R34v3r

資料來源：<http://justdire3e3lst75szk7mp6y63ex7seociiyeyddpj3orzjl7ejoieyd.onion>

此外，暗網中也出現以普丁肖像作為號召的網站，並提供其他特定暗網網站之網址（圖 9），目的在傳播關於戰爭、暴力等非法和極端的內容，對使用者造成負面影響，例如激化對抗情緒等，甚至影響接觸者參加招募活動、加入傭兵或志願軍，所以無法設立在明網之中。而此暗網網站提供的網址可能透過瀏覽的方式，遭植入遠端操控程式，成了參與非法活動的主機，例如成為發送假訊息的跳板主機，或是成為 DDoS 網路攻擊的殭屍電腦。



(a)



(b)

圖 9：招募民眾點擊親俄頻道的暗網網站

資料來源：<http://7ppwdmgglit5oowvms7yjvoalx2lrgb2w2wlxwvzbnwpol3lozjjaeqd.onion/>

此外，暗網除了能成為戰爭情報蒐集與欺敵訊息傳播的管道，也可能被恐怖組織用作募款與發展的平臺，所以值得情報機關對暗網進行恐怖組織發展的情蒐，例如伊斯蘭國 (IS) 曾使用暗網進行思想傳播、募款、人員招募，由於暗網屬地下化隱匿的網站，有利於接觸不方便曝光的恐怖分子，這些恐怖分子可以藉由暗網平臺獲取協調一致的攻擊時間或組織運作訊息，因為在暗網使用 Tor 匿名瀏覽器，透過多層加密路由來隱藏用戶的 IP 地址和地理位置，恐怖分子可利用 Tor 訪問暗網上的秘密網站和論壇，以規劃和協調他們的行動且不會被追蹤，而聯繫的電子郵件則可用加密的方式傳送，如使用 ProtonMail 和 Tutanota 等網站式的端到端加密電子郵件服務。ProtonMail 甚至可以設定電子郵件自毀的功能，用於在非 ProtonMail 用戶電子郵箱中自動刪除信件，Tutanota 則嚴格要求傳輸認證，與非 Tutanota 用戶通信時需交換密碼，這些都提高了偵測與分析恐怖分子聯絡狀況的難度。此外，恐怖分子也可利用暗網論壇和聊天室匿名交流，分享策略、情報和計劃，甚至招募新成員。圖 10 展示了一個暗網中傳播伊斯蘭國思想的頻道與接受捐款的網站。

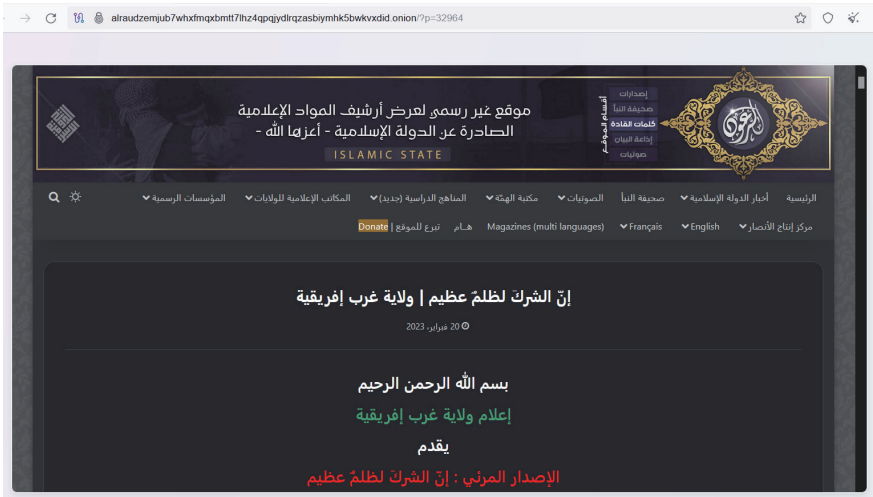


圖 10：伊斯蘭國交流與捐款的暗網網站

資料來源：<http://alraudzemjub7whxfmqxbmtt7lhz4qpqjydlrqzasbiymhk5bwkvxdid.onion/?p=32964>

（二）公務機密資料的外洩與販賣

2024 年 4 月媒體揭露，有人在暗網兜售我國外交部的機密資料，賣家標榜是第一手資料，且過去未曾流出，內含的公文時間橫跨 2022 至 2024 年，最近一份資料為 2024 年 3 月，檔案總共有 4 GB，皆為 PDF 檔案，資料包含 7 份公文，其中 2 份是「我與邦交國雙邊關係燈號評估簡表」，另有 2 份是駐美代表處電報、2 份為駐美國代表處經濟組的公文，最後一份為是來自財團法人國際合作發展基金會（國合會）的公文。[19] 另外，2024 年 4 月我邦交國帛琉遭駭客攻擊，該國總統點名是中國政府所為，共有

[19] 周峻佑，〈外交部傳出機密外洩，邦交國關係評估表遭暗網兜售〉，《IThome》，2024/04/19，<https://www.ithome.com.tw/news/162409>。

2 萬份政府文件遭駭客攻擊取得並公布在暗網，被竊文件包含美國在帛琉軍事設施的資料、臺灣與帛琉關係的細節、日本海上自衛隊船艦人員名單等。宣稱攻擊此次事件為其所為的駭客組織為「龍之力」(DragonForce)，並聲稱其動機純粹是為了謀取經濟利益，並揚言將再度打擊帛琉。但是帛琉財政部資安官員安遜 (Jay Anson) 告訴紐約時報，北京利用勒索軟體組織犯案，可降低與華府之間的外交摩擦風險。安遜也認為，「龍之力」已從他處獲取報酬，「這次行動是關於政治，與支付贖金無關」。這起網路攻擊肯定具有政治動機，因為「龍之力」並未積極洽談贖金。[20] 外交機密文件外洩，不僅會暴露各國的外交策略和軍事部署，也可能導致外交關係的緊張，甚至引發軍事衝突的風險。

而標定發動攻擊駭客組織身分的方法，通常是以使用工具與流程來進行分析，英國安全軟體和硬體公司 Sophos 分析報告指出中國國家支持針對東南亞國家使用網路間諜活動，Sophos 研究人員哈拉米洛 (Paul Jaramillo) 等人在《駭客新聞》(The Hacker News) 分享的一份報告中表示：「駭客活動背後的總體目標是保持對目標網路的訪問，進行網路間諜活動，以支持中國國家利益。包括連線訪問關鍵資訊網路系統、對特定用戶進行偵察、蒐集敏感的軍事和技術訊息以及部署各種惡意軟體植入程式以進行命令和控制 (C2) 通信。中國國家支持代號為「猩紅宮」(Crimson Palace) 的駭客，一直進行「複雜、長期」網路間諜活動，「猩紅宮」由 3 個團體組成，彼此具有相同的策略，證據顯示最早

[20] 陳成良、楊堯茹，〈遭駭客攻擊，帛琉總統：中國做的〉，《自由時報》，2024/06/04，<https://news.ltn.com.tw/news/politics/paper/1649536>。

的活動可以追溯到 2022 年 3 月。這 3 個團體為「阿爾法集團」(Cluster Alpha)、「布拉爾集團」(Cluster Bravo)、與「查理集團」(Cluster Charlie)。阿爾法集團（2023 年 3 月－ 2023 年 8 月），與被追蹤為駭客組織 BackdoorDiplomacy、REF5961、Worok 和 TA428 的參與者表現出一定程度的相似性；布拉爾集團（2023 年 3 月）則與駭客組織 Unfading Sea Haze 有共同點；至於查理集團（2023 年 3 月－ 2024 年 4 月）則與 APT41 內的一個子群「地球龍」(Group Earth Longzhi) 有重疊。[21]

BackdoorDiplomacy 是一個中國 APT 集團，[22] 自 2010 年起活躍，主要攻擊外交機構、通訊公司和政府機構，其目的是進行間諜活動和情報蒐集，BackdoorDiplomacy 的攻擊方法包括：(1) Supply chain attacks：攻擊供應鏈中的小公司，以便進入目標的系統。(2)Living-off-the-land：使用現有的系統資源和工具，避免引起注意。(3)Custom malware：使用自行開發的惡意軟體。(4) Advanced reconnaissance：使用進階的間諜技術，蒐集目標系統的資訊。[23]

BackdoorDiplomacy 的目標包括：(1) 外交機構、(2) 通訊公司、(3) 政府機構。依萊斯安全團隊 (Elastic's security team) 於 2023 年 10 月發布了一份關於網路間諜組織 REF5961 的報告，這是他們

[21] "Chinese State-Backed Cyber Espionage Targets Southeast Asian Government," *The Hacker News*, June 5, 2024, <https://thehackernews.com/2024/06/chinese-state-backed-cyber-espionage.html>.

[22] APT 是 Advanced Persistent Threat 的縮寫，指「進階持續性滲透攻擊」。

[23] Niels G., "BackdoorDiplomacy: A Detailed Analysis of a Chinese APT Group," *Linkedin*, Jan 25, 2023, <https://www.linkedin.com/pulse/backdoordiplomacy-detailed-analysis-chinese-apt-group-groeneveld>

在東南亞國家協會 (ASEAN) 成員國外交部網路上發現的網路間諜組織。依萊斯安全團隊表示，它發現該組織的工具與它追蹤的另一個網路間諜組織 REF2924 的惡意軟體相鄰。REF5961 的武器庫包括 EAGERBEE、RUDEBIRD 和 DOWNTOWN 等惡意軟體。TA428 製作了特殊的魚叉式網路釣魚誘餌電子郵件，其中包含與目標實體相關的數據，甚至表明他們致力於破壞組織，從先前針對目標或其員工的攻擊以及與選定受害者密切合作的受感染公司蒐集數據，進行網路釣魚電子郵件攻擊，以附件方式將可以利用 CVE-2017-11882 漏洞來執行任意程式碼的 Microsoft Word 檔案夾帶進入目標對象電腦進行攻擊。這些組織因為工具與程序手法及攻擊標的等特徵，英國安全軟體和硬體公司 Sophos 將之歸類並命名為「阿爾法集團」。[24]

經過英國安全軟體和硬體公司 Sophos 評估認為，這些重疊的活動集群團體很可能是在單一組織的指導下精心策劃的協調活動的一部分。該攻擊因使用未曾發現的惡意軟體、已知惡意軟體 EAGERBEE 系列的更新版本、已知惡意軟體 NUPAKAGE、已知惡意軟體 PowHeartBeat、已知惡意軟體 RUDEBIRD、已知惡意軟體 DOWNTOWN (PhantomNet) 和已知惡意軟體 EtherealGh0st (aka CCoreDoor) 等。但是集團的目標與方式有分工，「阿爾法集團」專注於映射伺服器子網路、列舉管理員帳戶以及對目錄伺服

[24] Paul Jaramillo, Morgan Demboski, Mark Parsons, and Sean Gallagher, "Operation Crimson Palace: Sophos threat hunting unveils multiple clusters of Chinese state-sponsored activity targeting Southeast Asian government," *Sophos News*, June 5, 2024, <https://news.sophos.com/en-us/2024/06/05/operation-crimson-palace-sophos-threat-hunting-unveils-multiple-clusters-of-chinese-state-sponsored-activity-targeting-southeast-asia/>.

器 (Active Directory) 基礎設施進行偵察，專注於停用防毒保護、提升權限和進行偵察；「布拉爾集團」優先使用有效帳戶進行橫向移動；「查理集團」的活動持續時間最長，專注於間諜活動和資料外洩，部署 PocoProxy 程式在受感染的系統上建立持久性的指揮和控制通訊，著重於外洩大量敏感資料，包括軍事和政治文件。[25]

根據帛琉官員說明駭客組織的目的分析，以及攻擊手法與暴露的工具，雖帛琉官員無提供文獻說明「龍之力」與「查理集團」的「地球龍」是否有關，然其確信此次文件洩漏於暗網的攻擊與中國有關。故對於暗網中洩漏資訊者的身分，須由多方已知的訊息進行研判分析。

伍、結論

網路來源的公開情資搜尋來源包括媒體、網路社群、觀察報告、專業及學術活動、與深網或暗網等，本文具焦在暗網資訊蒐集，而暗網中的網站卻有許多重複的克隆網站，這些網站也許是各式不同組織所建立的釣魚網站或是蜜罐 (Honeypot) 來反向進行情蒐。故於暗網中以爬蟲程式主動蒐集目標網站或是論壇資訊，需要注意保護個人隱私和資訊安全。使用技術工具如洋蔥路由 (Tor)、torsocks 和 proxychains，可以有效地進行暗網的情資蒐集，保護個人隱私並確保資訊安全，透過這些工具隱藏真實 IP 地址，避免被追蹤和監控。所取得資訊或是所接觸對象亦須進行查證，但是暗網主要特性為匿名性，僅可由資訊內容、資訊提供者電子

[25] Ibid.

郵件、與加密貨幣金流等 3 個方向來進行分析研判。在前節的暗網公布帛琉文件的案例中，是由資訊內容與目的來分析，方式是以已知的駭客攻擊團體手法、目的以及工具來歸類，再由歸類所得的組織業經確信為何國或單位所主使，來猜測可能的資訊洩漏攻擊者。

除前主動方式進行資訊爬取與資訊蒐集，本文也介紹美國 CIA 架設官方網頁進行人才招募與情資蒐集，因暗網中不乏持異議政見者、言論自由主張者、或是吹哨者等活動。這些人在暗網中散佈資訊可以避免追蹤以致身分曝光，也可以免除媒體糾纏、糾紛澄清、與政治壓力、甚至遭受迫害等問題，所以暗網中的使用成員十分多元，內容林林總總，包括論壇發言、資訊提供、物品販賣等。總之，在暗網的情資蒐集中，需要結合被動和主動的方法，並且使用技術工具保護個人隱私和資訊安全。透過這些方法，可以有效地進行暗網的情資蒐集，獲取有價值的情報，同時保障個人和組織的安全。（投稿：2024 年 4 月 16 日；修訂：2024 年 5 月 27 日；接受：2024 年 5 月 31 日）

參考文獻

一、專書

Treverton, Gregory F., 2003. *Reshaping National Intelligence for an Age of Information.* New York: Cambridge University Press.

二、期刊論文

Devarajan, Sasirekha, Pakutharivu Panneerselvam, Aditya Mudigonda, and Perichetla Kandaswamy Hemalatha, 2024. "Enhancing Dark Web Classification: A Dynamic Crawler and Robust Classification Framework," *International Journal of Intelligent Systems and Applications in Engineering,* Vol. 12, No. 6S, pp. 1-9.

Hansen, Morten, 2014. "Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community," *Intelligence and National Security,* Vol. 29, No. 1, pp. 58-81.

Kim, Minjae, Jinhee Lee, Hyunsoo Kwon, and Junbeom Hur, 2022. "Get off of Chain: Unveiling Dark Web Using Multilayer Bitcoin Address Clustering," *IEEE Access,* Vol. 10, pp. 70078-70091.

Pastor-Galindoa, Javier, Hông-Ân Sandlin, Félix Gómez Mármola, Gérôme Bovetb, and Gregorio Martínez Péreza, 2024. "A Big Data Architecture for Early Identification and Categorization of Dark Web Sites," *Future Generation Computer Systems,* Vol. 157, No. 5, pp. 67-81.

Patel, Hrishitva, 2023. "Comparison of Data Fluctuations that Lead to Cyber Security Attacks: A Difference between Surface, Deep and Dark Net," *Asian Journal of Research in Computer Science,* Vol. 16, Issue 4, pp. 297-308.

Wangchuk, Tashi, and Digvijaysinh Rathod, 2023. "Opensource Intelligence and Dark Web User De-Anonymisation," *International Journal of Electronic Security and Digital Forensics,* Vol. 15, No. 2, pp. 143-157.

Yadav, Ashok, Atul Kumar, and Vrijendra Singh, 2023. "Open-Source Intelligence: A Comprehensive Review of the Current State, Applications and Future Perspectives in Cyber Security," *Artificial Intelligence Review,* Vol. 56, pp. 1-32.

三、官方文件

Bureau of Justice Assistance (BJA), 2005/09. *Intelligence-Led Policing: The New Intelligence Architecture.* Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice. <https://www.ojp.gov/pdffiles1/bja/210681.pdf>.

Communications Security Establishment, Government of Canada, 2022. *Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine.*

U.S. Government Publishing Office, 1996/03/01. *Preparing for the 21th Century: An Appraisal of U.S. Intelligence.* <https://www.govinfo.gov/app/details/GPO-INTELLIGENCE/context>.

United Kingdom Ministry of Defense, 2011/08. *Joint Doctrine Publication 2-00 Understanding and Intelligence Support to Joint Operations (JDP 2-00).*

四、網際網路

2024/06/05. “Chinese State-Backed Cyber Espionage Targets Southeast Asian Government,” *The Hacker News,* <https://thehackernews.com/2024/06/chinese-state-backed-cyber-espionage.html>.

Belcic, Ivan, and Brittany Nelson, 2021/11/30. “What Is the Dark Web and How to Access It?,” *Avast Academy,* <https://www.avast.com/c-dark-web>.

Grustniy, Leonid, 2021/02/01. “Darknet, Dark Web, Deep Web, and Surface Web - What’s the Difference?,” *Kaspersky Daily,* <https://www.kaspersky.com/blog/deep-web-dark-web-darknet-surface-web-difference /38623/>.

Jaramillo, Paul, Morgan Demboski, Mark Parsons, and Sean Gallagher, 2024/06/05. “Operation Crimson Palace: Sophos threat hunting unveils multiple clusters of Chinese state-sponsored activity targeting Southeast Asian government,” *SOPHOS NEWS,* <https://news.sophos.com/en-us/2024/06/05/operation-crimson-palace-sophos-threat-hunting-unveils-multiple-clusters-of-chinese-state-sponsored-activity-targeting-southeast-asia/>.

Makuch, Ben, 2019/05/08. “The CIA Will Use its New Dark Web Site to Collect Anonymous Tips,” *Vice Media*, <https://www.vice.com/en/article/xwnyew/the-cia-will-use-its-new-dark-web-site-to-collect-anonymous-tips>.

Niels, G., 2023/01/25. “BackdoorDiplomacy: A Detailed Analysis of a Chinese APT Group,” *Linkedin,* <https://www.linke-

din.com/pulse/backdoordiplomacy-detailed-analysis-chinese-apt-group-groeneveld>.

Peterson, Marilyn B., 2022. "Intelligence Basics Revisited," *Academia,* <https://www.academia.edu/38121702/Intelligence_Basics_Revisited>.

周峻佑，2024/04/19。〈外交部傳出機密外洩，邦交國關係評估表遭暗網兜售〉，《IThome》，<https://www.ithome.com.tw/news/162409>。

美國中央情報局的暗網網站，<ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion>.

陳成良、楊堯茹，2024/06/04。〈遭駭客攻擊，帛琉總統：中國做的〉，《自由時報》，<https://news.ltn.com.tw/news/politics/paper/1649536>。

劉致昕、陳映妤，2022/3/3。〈來自俄烏資訊戰前線的警告：反制假訊息，別讓絕望吞噬事實和光明〉，《報導者 THE REPORTER》，<https://www.twreporter.org/a/russia-ukraine-war-2022-information-warfare>。