Commerce & Management Quarterly, Vol.26, No.2, pp.135~178(2025)

書目共被引與共現網絡中的結構性特徵－以網絡安全研究為案例

STRUCTURAL PROPERTIES ON BIBLIOGRAPHIC CO-CITATION AND OCCURRENCE NETWORK - THE CASE OF FOCUS ON CYBERSECURITY

盧政遠
朝陽科技大學企業管理系台灣產業策略發展博士班
徐毓君*
朝陽科技大學企業管理系台灣產業策略發展博士班
賴奎魁
朝陽科技大學企業管理系特聘教授

Cheng-Yuan Lu
Ph. D. Student, Department of Business Administration, Chaoyang University of Technology
Yu-Jun Hsu
Ph. D. Student, Department of Business Administration, Chaoyang University of Technology
Kuei-Kuei Lai
Distinguished Professor, Department of Business Administration, Chaoyang University of Technology

摘要

本研究旨在探討全球經濟向知識型經濟轉型過程中，技術知識對國家經濟增長和企業競爭力的重要性。隨著科技的快速發展，特別是在資訊技術和數字化領域，科技法律的重要性日益顯現。本研究重點關注網絡安全與科技法律的

*通訊作者，地址：嘉義市大同路102巷10弄8號，電話：0972-217789
E-mail：sir1819@hotmail.com

交互影響，並探討不同行業面臨的網絡威脅及其應對措施。研究方法採用書目計量分析，通過系統檢索 Web of Science 數據庫中的相關文獻，進行引文分析、共被引分析和共現網絡分析，揭示科技法律領域的研究主題結構與關鍵發展趨勢。結果顯示，自 2008 年至 2024 年，科技法律領域的學術研究穩定增長，主要集中在數據保護、網絡犯罪和資訊安全等領域。通過分析，識別出多篇具有高影響力的核心文獻及重要研究者，這些成果對未來的研究和法律制定具有重要指導意義。此外，國際合作在該領域的研究中扮演著重要角色，顯示出全球化的趨勢。研究強調了在應對新技術挑戰時，不斷更新和完善科技法律的重要性，為未來的政策制定提供了實證依據。

關鍵字：科技法律、網路安全、文獻計量分析、共被引網路分析、共現詞網絡分析

ABSTRACT

This study investigates the pivotal role of technological knowledge in fostering national economic growth and strengthening corporate competitiveness amid the global transition towards a knowledge-based economy. With rapid advancements in information technology and digitalization, the relevance of technology law has become increasingly apparent. This research explores the intersection of cybersecurity and technology law, focusing on the network threats facing diverse industries and the strategies implemented to address them. By employing bibliometric analysis, relevant literature was systematically collected from the Web of Science database. Citation analysis, co-citation analysis, and co-occurrence network analysis were conducted to uncover the thematic structure and key developmental trends in the field of technology law.

The results reveal that academic interest in technology law has progressively increased from 2008 to 2024, with predominant themes in data protection, cybercrime, and information security. Through this analysis, several influential publications and prominent researchers were identified, providing valuable insights for guiding future research and legal frameworks. Furthermore, the findings underscore the significance of international collaboration, reflecting a trend toward globalization in the field. This study emphasizes the need for continuous updates to technology law to address the challenges posed by new technological advancements, offering empirical evidence to support future policy-making.

Keywords: Technology Law, Cybersecurity, Bibliometric Analysis, Co-occurrence Network Analysis, Co-citation Network Analysis

壹、緒論

隨著全球經濟從主要依賴勞動力和資本的傳統經濟模式轉變為知識型經濟，科學與技術知識被認為是經濟增長的驅動力，甚至是社會變革的來源。在這種背景下，技術知識的創造和傳播被視為決定一個國家宏觀經濟增長以及公司微觀競爭力的關鍵因素。在整體外部環境中，政策、經濟、科技與社會相互影響。隨著科技的飛速發展，特別是在資訊技術和數字化領域的革新，政策面中的法律體系也面臨來自多方面的新挑戰，科技法律因此成為一個日益重要的研究領域。科技法律涵蓋了智慧財產權、個人資料保護與隱私法、網路安全、電子商務法、人工智能及區塊鏈技術法律等多個方面，這些領域不僅對社會的運行方式產生了深遠影響，也對法律制度提出了新的要求。

網絡攻擊針對主機計算機的信息和服務進行敵對操作，旨在中斷、降低、拒絕或破壞關鍵的信息和服務。網絡安全指的是用來防範此類攻擊的各種防禦機制。而網絡取證則是在攻擊事件後進行數據恢復和追蹤的科學。傳統安全軟件需要大量時間和精力來識別和分類潛在的新威脅，並將這些分類編碼以便未來檢測此類攻擊（Ahmed, Raza, Hussain, Ali, Iqbal, & Wang, 2015）。使用機器學習技術可以使這一耗時的過程更加高效。因此，各種機器學習技術被創建出來以更快速和準確地識別攻擊。網絡安全和取證在所有行業和部門中都是一個嚴重問題，這是由於計算機系統和互聯網能力的普及和快速擴展造成的。高等教育也日益面臨此類威脅。有報導稱，由於網絡攻擊，許多大學發生數據洩露事件。高等教育用戶使用便攜設備，使其高度移動化，這些設備使學生能夠習慣於網絡，允許他們隨時隨地連接到不安全的網絡（Ramim & Levy, 2006）。由於數據和信息的開放性和簡單訪問，網絡安全在高等教育機構中特別難以實施（Kendall, 2022）。不充分的網絡安全使高等教育面臨風險，而各類學術研究數據的存在使得教育機構成為網絡犯罪分子的理想目標（Ulven, 2020）。這意味著高等教育機構，如大學，現在面臨網絡安全威脅（Bondoc & Malawit, 2020）。由於大多數大學採用開放訪問和信息共享文化，它們變得更加容易受到攻擊。這對高等教育來說是一個令人擔憂的狀況，因為黑客行為等網絡威脅可能會中斷學術運營。黑客散布大學的有用信息，並且由於數據已成為商品，他們可以

輕易出售這些知識。大學的在線系統是網絡安全問題的潛在目標，如黑客行為。

在各行各業面臨的網絡威脅方面，金融機構是網絡犯罪分子的主要目標，因為它們處理大量敏感的金融數據。銀行和其他金融服務提供商必須保護客戶的個人信息和財務交易記錄（Makulilo, 2015）。醫療行業：醫療機構處理大量的個人健康信息，這些數據對網絡犯罪分子具有高度吸引力。醫療數據洩露可能對患者隱私造成嚴重影響，並可能導致醫療欺詐（Khan & Hoque, 2016）。零售業：零售企業面臨著支付系統和客戶個人信息的安全威脅。網絡攻擊可能導致支付卡數據洩露，從而影響消費者的信任和企業的聲譽（Wang, D'Cruze, & Wood, 2019）。製造業：製造企業依賴於工業控制系統來管理生產過程。這些系統如果受到攻擊，可能會導致生產中斷和經濟損失（Ani, Daniel, Oladipo, & Adewumi, 2018）。

網絡攻擊對各行各業的正常營運影響大且深遠，是故，各行各業都必須應對網絡攻擊帶來的挑戰。黑客行為可能會中斷業務運營，洩露敏感信息，並導致重大經濟損失。例如，Target 在 2013 年的數據洩露事件導致約 4000 萬張信用卡和借記卡信息被盜，對其聲譽和財務造成嚴重影響。數據安全和取證是數據科學中最重要的方面之一，隨著大大小小的公司獲取大量相關數據，其重要性逐年增加。網絡犯罪分子針對政府、軍隊、國家情報、安全機構、金融機構、公司、企業、醫院、農業等的敏感數據（Grigorovič, 2017）。隨著數據在網絡環境中的重要性日益增加，對網絡治理的理解和實施變得至關重要，並強調了培訓和意識提升在減少網絡安全風險中的作用。這表明了科技法律與網絡治理的重要性，並暗示隨著科技發展，法律制度也需要相應地進行調整（Savaş & Karataş, 2022）。環境變化對科技法律的各個領域帶來了一系列問題和挑戰。這些變化包括技術的迅速發展、社會需求的變化、全球經濟的動盪等。因此，研究人員對科技法律知識流動的關注也在增加，以期制定更有效的法律應對不斷變化的科技環境。以現行科技法律來對應上述的問題，智慧財產權法，涉及專利、版權和商標保護，如《數字千年版權法》（DMCA）。個人資料保護法，如歐盟的《通用數據保護條例》（GDPR）和美國的《加州消費者隱私法》（CCPA）。網絡安全法：如《網絡安全信息共享法》（CISA）和《通用數據保護條例》（GDPR）中的數據安全部分。電子商務法：如《電子簽名法》（ESIGN）和《電子商務指令》（EU e-Commerce Directive）。人工智能及區塊鏈技術法律：涉及智能合約、數字貨幣和自動駕駛汽車的監管，如《人工智能指導方針》和《區塊鏈監管框架》。Savaş and Karataş（2022）提到網絡攻擊對社會運作和法律制度的影響。隨著數據共享和保護的重要性上升，文獻強調了需要持續更新法律以應對技術

變革的挑戰。研究指出，企業需要使用數據來增強決策能力，以適應新技術的快速發展，這也讓數據安全成為核心議題。數據安全和取證是數據科學中最重要的方面之一，隨著大大小小的公司獲取大量相關數據，其重要性逐年增加（Tao et al., 2019）。網絡犯罪分子針對政府、軍隊、國家情報、安全機構、金融機構、公司、企業、醫院、農業等的敏感數據（Grigorovič, 2017）。例如，像微軟和谷歌這樣的知名公司使用數據來為其決策提供洞見，並更好地理解現有技術與下一代技術之間的關係，因此數據也是主要目標。

綜合上述背景所述，近年來學術界對網路攻擊與網路安全投入大量研究，產生了在科學上之學術文件與科技之技術與專利之新穎性新資訊安全知識。這些知識持續地累積並外溢擴散至各行各業，形成網路安全技術領域的演化路徑並揭示了知識流動的模式。為發掘了網路安全研究的新前沿，並預測了未來的趨勢（Sharma, Mittal, Sekhar, Shah, & Renz, 2023）。書目計量分析是採現有的科學演化分析研究之此角度進行；例如引文網絡中的主路徑分析（Main Path Analysis, MPA）被廣泛認為是知識流動和傳播的重要代理。在 Garfield（2004）的歷史學地圖中，新的想法和發現是建立在之前成果之上的理論。通過追蹤引文鏈接的連接性，MPA 方法可以識別知識流動的主要路徑，這種方法廣泛用於檢測科學的演化軌跡。為了深入理解某一領域的動態演化過程，科學研究近年來越來越注重將提取出的主題相互連接，以此作為辨別科學演化狀態的關鍵手段。在過去，研究人員主要依靠專家的知識和經驗來揭示主題之間的演化關係。然而，隨著科學出版物和專利數量的激增，單靠專家知識來分析演化趨勢變得不夠精確，且效率低下，成本高昂（Lu & Liu, 2013）。基於上述之原因，本研究採書目計量分析通過客觀評估研究領域的趨勢和前景來補充傳統文獻評估（Sharma et al., 2023）。這種分析對於突出特定研究領域在若干年或數十年中的演變非常有價值。有多種方法可以用來審查特定主題的科學研究進展。評估性和關聯性回顧是這些方法的主要類別。評估性回顧用於定量研究出版物、作者、組織和國家的絕對研究影響。這種分析包括各種生產力變量，如期刊數量、每年出版物數量、引用次數等（Larivière & Costas, 2016）。

鑒於上述問題陳述（Problem Statement）和文獻探討之綜述中發現的研究缺口（Gap），缺乏時間序列的動態演化，因各創新領域的科學文獻與技術呈現動態增長的趨勢，有必要進行進一步更詳細的研究。因此，我們能夠訂定本研究的主要目標，即在檢全、檢準檢索原則下，使用關鍵詞的檢索方法更有效的識別相關專利文檔，再經書目共被引和共現網絡中等的分析結果，發掘特定領域主題，在計算主題間的相似性與相似矩陣，再結合共被引（Co-citation

Network）和共現網絡（Co-occurrence Network）共同資訊下，以探討技術演化發展的路徑與演化的不同時態之探討（Sharma et al., 2023）。為了有效地研究與完備性揭露相關的文獻與論文文件創新領域，本研究提問先概述一個概觀分析，及一個關鍵研究提問（RQs），並為每個問題提出了具體的解決方法：以下是對每個研究問題（Research Question）的更詳細解釋。

(一) RQ 1：概觀分析

從概觀分析角度來看，對於期刊論文的主題、國家、作者、關鍵詞的熱點和發展趨勢的理解。這種分析可能包括以下幾個方面：技術主題熱點：通過期刊論文利的內容，可以識別出當前和未來的研究熱點。國家分佈趨勢：分析不同國家的合作趨勢。

(二) RQ 2：書目共被引和共現網絡中的結構性特徵

引文分析：由 Garfield, Sher, and Torpie（1964）提出，用於評估科研文獻的影響力和相關性。共現分析：由德里克·德索拉·普萊斯 Price（1965）發展，分析詞彙、等在文獻中的共現關係。

貳、理論背景與文獻探討

一、科技法律的基本概念

科技法律涵蓋了一系列因應科技進步而產生的法律問題和挑戰。智慧財產權（IP）保護創意和創新，包括專利、商標、著作權和商業秘密，鼓勵創新並確保創作者能夠從中獲益（Jensen & Webster, 2014）。數據保護與隱私法如歐盟的《一般資料保護規則》（GDPR），旨在保護個人數據免受濫用（Voigt & Von dem Bussche, 2017）。Hyla（2018）指出，隨著網絡攻擊加劇，外國利用黑客行為獲取經濟利益或表達政治意圖，美國消費者的個人數據和經濟穩定面臨風險。聯邦及州立法者推出的各項網絡安全政策缺乏協調，效果不佳。論文建議應建立一個統一的中央聯邦機構，負責所有網絡安全法規，以制定有效的保護措施來保護敏感數據。而在 Davis（2013）中探討契約法規範個人和企業之間的契約關係，特別是科技領域的軟體授權協議和服務等級協議（SLA），確保服務提供者和消費者之間的權利和義務明確。消費者保護法保障數字產品和服務交易中的消費者權益（Howells, Twigg-Flesner, & Wilhelmsson, 2017）。人工智能（AI）

和機器學習（ML）技術的快速發展帶來算法透明性、AI 偏見、倫理問題和責任界定等法律挑戰（Calo, 2017）。區塊鏈技術和加密貨幣的興起對傳統金融和法律體系提出挑戰，需要新的法律框架來監管初次代幣發行（ICO）和智能合約（De Filippi & Wright, 2018）。反壟斷法與競爭法旨在防止市場壟斷，促進公平競爭（Khan, 2016）。科技的全球化使國際科技法律事務愈發重要，國際法律框架需要適應科技的快速發展，促進國際間的合作與法規統一。這些法律框架共同應對科技進步帶來的挑戰，並隨著科技發展持續演變。

科技的快速發展對社會各個面向都帶來了深遠的影響，法律領域也不例外。隨著 20 世紀後半葉信息科技和生物科技等領域的突破性進展，尤其是網際網路的誕生和普及，科技迅速發展，將人類帶入了資訊時代。資訊的傳播速度和廣度達到了前所未有的程度，同時也縮短了人與人之間的距離。然而，科技的發展在帶來便利的同時，也引發了諸多法律挑戰。正如 Bues and Matthaei（2017）所指出的，法律科技的興起正在改變律師的工作方式，並導致該行業的顛覆性變革。這些挑戰包括網絡犯罪、數據隱私、智慧財產權保護以及人工智慧倫理等。例如，網路空間的開放性和匿名性滋生了網路詐騙、駭客攻擊和網路盜版等犯罪活動；大數據時代的到來使得個人數據的隱私保護成為重要議題；智慧財產權在數位化背景下面臨軟體盜版和網路侵權等新的挑戰；此外，人工智慧的發展也引發了倫理道德方面的擔憂，如人工智慧的責任歸屬和演算法的公平性。科技法律旨在規範與科技相關的各種活動，維護社會秩序，並促進科技的健康發展。

二、資訊安全與法律框架

現代企業對資訊安全管理需求增長，ISO/IEC 17799 和 ISO/IEC 27001 提供了全面框架，強調資訊的機密性、完整性和可用性，並通過認證增強信心。ISO/IEC 27001 採用 PDCA 模型，確保資訊安全管理系統持續改進（Saint-Germain, 2005）。隨著數位化發展，資訊安全成為國家安全戰略的重要部分，各國政策強調技術控制和法律框架的結合（Cavelty, 2007）。攻擊者手法不斷變化，企業在保護資訊資產時面臨挑戰（Lavrov, Zolkin, Aygumov, Chistyakov, & Akhmetov, 2021）。關鍵資訊基礎設施（CII）涵蓋能源、交通等領域，其安全對國家穩定至關重要（Putro & Sensuse, 2021）。現代政策強調多層次保護，包括預防、偵測、應對和恢復（Grobler & Louwrens, 2005）。企業需確保所購買軟體的安全性（Humphreys, 2008）全球資訊安全需國際合作，國際組織如歐洲理事會和國際刑警組織在促進國際標準和協調跨國執法中發揮重要作用（Hong, Chi,

Chao, & Tang, 2003）。

隨著資訊科技的迅速發展，資訊安全已成為個人、企業和國家安全的關鍵要素。為應對這些挑戰，各國建立了相應的法律 3 框架，包括電子簽章法、電腦犯罪法、數據隱私保護法和網路安全法，旨在保障資訊活動的合法性和安全性。例如，Scharnick, Gerber, and Futcher（2016）強調了數據儲存保護對企業的重要性。然而，隨著新技術的出現，如雲計算、大數據和人工智慧，現有法律框架面臨新的挑戰。Omidosu and Ophoff（2016）指出，公眾和企業對資訊安全的意識仍然薄弱，跨境執法困難也使得國際合作顯得尤為重要。現有的法律規範需要不斷更新，以應對日益複雜的網路犯罪和資訊安全威脅。資訊安全法律框架的發展將更加注重數據隱私保護、技術創新和國際合作。隨著數據成為關鍵資源，預計各國將出台更嚴格的隱私保護法律，並加強技術創新以應對新興威脅。Vithanwattana, Karthick, Mapp, George, and Samuels（2022）提到，未來的資訊安全框架需要在理論與實踐中找到平衡，以有效應對新的挑戰。

三、網路安全因應措施

(一) 網路安全的背景與挑戰

隨著科技的快速發展，企業和組織的數字化轉型促使網路安全成為不可忽視的問題。過去的文獻強調了網路攻擊的日益複雜化，如分佈式拒絕服務攻擊（DDoS attacks）、惡意軟體（malware）、網絡釣魚（phishing）等，這些攻擊不僅威脅著組織的數據安全，還會對企業的財務、聲譽和營運造成不可估量的損失（Raimundo & Rosário, 2022）。

(二) 網路安全因應措施的分類與理論框架

過去的文獻針對網路安全因應措施提出了不同的分類，通常可以劃分為技術層面與管理層面的對策。

1. 技術層面的因應措施

技術層面主要涉及到針對網絡威脅的直接技術手段，如防火牆、入侵檢測系統（IDS）、數據加密和身份驗證等。

(1) 防火牆與入侵檢測系統（IDS）：過去的研究中，防火牆被視為網絡安全的第一道防線，過濾進出網絡的流量。與此同時，入侵檢測系統（IDS）通過分析網絡流量來檢測潛在的攻擊（Stallings, 2016）。這些技術工具能夠識別並阻止未經授權的訪問。

(2) 數據加密與身份驗證：數據加密和強化身份驗證（如雙因素身份驗證）被廣泛應用於保護數據的機密性和完整性（Sharma, Tyagi, & Bhardwaj, 2022）。加密技術確保了即使攻擊者進入系統，也無法輕易解密數據。

2. 管理層面的因應措施

管理層面則關注於如何通過政策和培訓來提高組織內部的網路安全意識和操作標準。

(1) 安全政策與規範：文獻指出，制定強有力的安全政策是組織抵禦網絡攻擊的關鍵步驟（Baskerville, 1993）。例如，設置密碼管理策略、數據訪問控制以及員工安全行為規範等。

(2) 員工培訓與安全意識：許多研究強調了員工安全意識的重要性（Sharma et al., 2022）由於員工經常是攻擊的首要目標，通過定期的安全培訓來提高員工的防範意識和識別網絡威脅的能力可以顯著減少攻擊的風險。

(三) 以往文獻對網路安全的因應措施研究

根據以往文獻的做法，研究學者通常通過以下幾種方法來探討網路安全的因應措施。

1. 多層防禦策略（Defense-in-Depth Strategy）

多層防禦策略是一種被廣泛認可的網路安全防護措施，這種策略強調在組織內部實施多重安全措施來抵禦各類威脅。（Pfleeger & Pfleeger, 2012）提出了「防禦深度」模型，這是一種分層防禦策略，將技術和管理措施結合起來，例如結合防火牆、IDS、加密和身份驗證等技術措施，再加上員工培訓和安全政策管理，形成多層次的安全防線。

2. 風險管理框架（Risk Management Framework）

風險管理框架強調識別、評估和優先處理網絡風險，NIST（National Institute of Standards and Technology）的風險管理框架成為許多組織採用的標準（Force,

2017）。這個框架包括風險評估、風險緩解和風險監控三個主要步驟，幫助組織動態應對網絡威脅。

3. 雲端安全與零信任架構（Zero Trust Architecture）

隨著雲計算技術的普及，零信任架構成為近年來受到關注的網絡安全策略之一。根據 Stafford（2020）的零信任模型，組織應該假設內外網絡環境都不可信，並且需要對每一個數據訪問請求進行驗證。這種架構在應對分佈式工作環境和遠程工作中愈加重要。

(四) 文獻對網路安全因應措施效果的評估

過去的研究對不同網路安全措施的效果進行了廣泛的評估：防火牆與入侵檢測系統的效果：Jansen and Grance（2011）表明防火牆和 IDS 能有效阻擋已知的網絡攻擊，但對於新型的攻擊技術（如零日攻擊），這些傳統工具的效果有所限制，這促使研究人員進一步探索行為檢測系統和基於機器學習的網絡防護措施。員工培訓的效果：文獻中，Daengsi, Pornpongtechavanich, and Wuttidittachotti（2022）發現，定期的網絡安全培訓能顯著降低網絡釣魚攻擊的成功率，員工在面對偽裝電郵或不明鏈接時的警覺性大幅提升。

四、書目計量分析與相關研究

書目計量分析透過客觀地評估一個研究領域的趨勢和前景，補充了傳統文獻評估方法（Sharma, Gupta, & Andreu-Perez, 2021；Van Raan, 2005）。這種分析在突顯特定研究領域多年甚至數十年的發展過程中具有重要價值（Zupic & Čater, 2015）。針對某一主題的科學研究進展，書目計量分析提供了多種方法，這些方法主要分為評估性和關聯性兩大類（Borgman & Furner, 2002）。評估性回顧用於定量研究出版物、作者、機構及國家等的絕對研究影響力。該分析包括了各種生產力變數，如期刊數量、每年出版物數量、引用次數等（Majdouline, Baz, & Jebli, 2022）。對於特定領域的研究影響指標，還可以透過專家判斷進行質性評估回顧（Benckendorff, 2009）。另一方面，關聯性回顧技術則集中於上述評估性指標之間的相互關係。合作成果的數量、合作鏈接及相關鏈接強度用於量化和表達這些相互關係。基於引用的關聯、共現和共引分析是其他有用的關聯性指標（Benckendorff & Zehrer, 2013）。共同作者之間的聯繫是不同研究群體間資訊傳遞的關鍵指標（Hu & Racherla, 2008）。理解多產作者及機構之間的研究聯繫需要對引用關聯進行評估（White & McCain, 1998）。跨地域合作／共引的廣度也可由連接強度決定。

本研究整合了評估性和關聯性技術，對網絡安全與網絡取證研究進行了平衡的書目計量分析。書目計量調查（Van Raan, 2005）提供了一個或多個十年間研究領域演變的信息。這些分析通常提供關於個別作者的研究產出及其所屬機構的研究產出、文件、作者、機構與地點之間的合作與引用網絡、熱門主題和關鍵詞（Benckendorff, 2009）、頂級出版期刊、期刊間的關聯等信息。數據可視化工具對於成功展示研究結果並快速得出可操作的結論至關重要。在本研究中，使用了 VoSviewer 進行定量數據分析和網絡安全／取證研究的可視化，這些研究發表於 2011 至 2021 年間的 Web of Science（WoS）。基於合作／引用數據的書目計量分析，VoSviewer 可以創建作者和期刊網絡圖，也可以生成展示研究主題中多個共現詞語之間關係的關鍵詞圖（Van Eck & Waltman, 2010）。最近的網絡安全書目計量研究，例如 Jalali, Razak, Gordon, Perakslis, and Madnick（2019）對醫療領域的網絡安全進行了書目計量分析。該研究考慮了約 472 篇被 Web of Science 和 PubMed 索引的出版物。Rahim（2021）使用書目計量分析了高等教育中的網絡安全研究。Makawana and Jhaveri（2018）應用書目計量法分析了機器學習技術在網絡安全中的影響。Elango, Matilda, and Jeyasankari（2020）使用書目計量分析和關聯搜尋重新定義了網絡安全的關鍵詞。Azambuja and Almeida （2021）分析了工業 4.0 領域的網絡安全出版物。Shukla and Gochhait （2020）發表於 Web of Science 的網絡安全研究進行了簡短的書目計量分析。Nakhodchi and Dehghantanha（2020）應用書目計量工具分析了 Web of Science 上發表的深度學習在網絡安全中的應用研究。這些作者包含了對研究領域、洲、國家、機構、作者、關鍵詞和術語的書目計量分析。

五、共現分析（Co-occurrence network）

共現網絡，有時也稱為語義網絡，是一種用於分析文本的方法，透過圖形化的方式來呈現文本中詞語之間的潛在關係。這些關係可以涉及人、組織、概念、生物（如細菌）或其他在書面材料中出現的實體。隨著符合文本挖掘要求的電子存儲文本的出現，構建和可視化共現網絡的技術變得更加實用和普及（Segev, 2021）。

共現網絡的基本原理是基於特定文本單位內詞語的配對出現來構建的。這些網絡是通過一組標準來定義和連接成對詞語的。例如，如果詞語 A 和詞語 B 在同一篇文章中出現，則它們被視為「共現」。而當另一篇文章中包含詞語 B 和詞語 C 時，則可以將 A 連接到 B，再將 B 連接到 C，從而構建一個由這三個詞語組成的共現網絡。共現的定義標準可以根據具體需求來設置，例如，更嚴格

的標準可能要求一對詞語必須出現在同一句話中（Tavallaee, Bagheri, Lu, & Ghorbani, 2009）。

構建共現網絡的過程包括識別文本中的關鍵詞，計算詞語之間的共現頻率，並分析網絡以發現其中的核心詞語和主題集群。這些網絡可以針對任何給定的詞語列表與任何文本集合進行創建。共現的詞語對通常稱為「鄰居」，它們根據相互之間的聯繫組成「鄰域」。在文本挖掘的背景下，詞語被象徵性地表示為文本字符串。在現實世界中，由詞語識別的實體通常有多個象徵性表示形式，因此將詞語視為由一個主要符號及其同義符號組成是有意義的。如在 COVID-19 大流行期間，學術界對該病毒的研究產出了大量的學術文獻，從數百篇與 COVID-19 相關的學術論文中提取常見的關鍵詞，如：「COVID-19」、「病毒傳播」（Virus Transmission）、「疫苗研發」（Vaccine Development）、「公共衛生」（Public Health）、「臨床試驗」（Clinical Trials）、「社交距離」（Social Distancing），經構建共現矩陣、共現網絡的可視化及分析網絡結構，獲得具體結果：疫苗研發和臨床試驗在文獻中經常共同出現，顯示出這是 COVID-19 研究中的核心主題。公共衛生措施與社交距離在文獻中頻繁共現，表明這些策略是遏制病毒傳播的重要措施。人工智能技術在 COVID-19 研究中逐漸增多，尤其是在分析傳播數據和預測疫情走勢方面。

共現網絡的圖形表示允許直觀地可視化詞語之間的關係，並推斷應用於文本語料庫的詞語字典所代表的領域中的實體關係。有效的可視化通常需要對網絡進行簡化，例如限制每個詞語的鄰居數量，或根據共現的「概率」來設置連接的標準。

此外，共現網絡的底層結構的定量分析也能提供有價值的信息，例如實體之間的整體連接數量、表示子域的實體集群以及同義詞的檢測等。這些信息有助於深入理解文本中的語義結構和主題關聯性。

六、共被引分析網路（Co-Citation Network）

共被引分析（Co-citation Analysis）是一種用來分析和視覺化學術文獻間關聯性的科學技術。它基於這樣一個假設：如果兩個出版物在其他文章的參考文獻中經常被一起引用，那麼這兩個出版物在主題上可能具有相似性（Hjørland, 2013）。這種方法最初是由 Small 和 Marshakova 在 1973 年獨立發展起來的，它已成為文獻計量學中分析知識結構和學科演化的重要工具。在共被引網絡中，當兩個出版物 A 和 B 同時出現在另一個出版物 C 的參考文獻列表中時，它們之間就會建立一個連接。這種連接越頻繁，表示 A 和 B 之間的關聯性越強。共

被引分析主要用於揭示文獻之間的關聯性，並且可以幫助識別一個研究領域的知識結構。具體來說，共被引分析可以幫助識別：核心文獻：那些被頻繁引用的出版物通常在其研究領域中具有重要地位。主題集群：通過分析那些被一起引用的出版物，可以識別出該研究領域的不同主題群體。

經構建共被引矩陣、聚類分析可得幾個主題集群，如隨著數字化轉型的加速，資訊安全（Cybersecurity）成為了保護個人、組織和國家的敏感信息和系統免受網絡攻擊的重要課題。研究人員在該領域發表了大量學術文章，涵蓋了各種主題，如網絡攻擊防護、加密技術、漏洞管理、和隱私保護。共被引分析可以幫助我們揭示資訊安全研究領域的知識結構，識別出最具影響力的文獻和研究趨勢。識別出資訊安全領域中的不同主題集群。例如，經過分析後，我們可能會發現以下幾個主題集群：網絡攻擊防護、加密技術與身份驗證與訪問控制。是故，共被引分析實例展示了如何使用這種方法來揭示學術領域中的知識結構，識別出重要的研究主題和核心文獻，並幫助研究者和企業更好地理解和應對當前和未來的挑戰（Chandola, Banerjee, & Kumar, 2012；Goodfellow et al., 2014；Hochreiter & Schmidhuber, 1997）。

參、研究方法

文獻計量分析是一種使用參考書目分析學術文獻的定量方法，以提供已發表研究的描述、評估和監測（Garfield, 1964；White & McCain, 1998），用於分析該領域的趨勢。方法論的目的是分析出版物、引文和資訊來源。根據 Aria and Cuccurullo（2017）的說法，每種文獻計量方法對於特定的研究問題都是有用的，並且最常見的問題可以使用科學繪圖的文獻計量學來回答。本研究的發展考慮了三個層面的分析：來源、作者和文件，以客觀和可靠的方式進行。首先，研究的重點是識別與每個層級相關的主題的相關性，將相關性理解為最有成效或引用的項目，具體取決於分析單位。其次，使用多種文獻計量技術進行了知識結構。具體來說，概念結構著重於主題和趨勢、具體作品如何影響科學界的知識結構以及顯示作者和國家之間合作的社會結構。

該分析使用 Bibliometrix R-Tool，Aria and Cuccurullo（2017）進行研究，是一個以 R 軟體包為基準並助於使用特定工具進行更完整的文獻計量分析，用於文獻計量和科學計量定量研究。在這方面 R 是最強大、最靈活的統計軟體環

境之一，提供了參與的開源途徑。因此，R 是一套用於資料操作、計算和圖形顯示的整合軟體應用程式（Ligges, 2009）。事實上，在 Bibliometrix 的具體情況下，可以將其與其他相關軟體包整合。為了進行文獻計量分析而製定的步驟是，首先收集數據，然後按層級進行描述性和文獻計量分析。

為了闡明特定技術主題的新穎特徵內容和特徵來源，本計畫提出了一個基於技術特徵相似性的特定技術主題識別模型。該模型特別設計用來處理這些主題內的創新途徑和創新特性。整個過程分為六個步驟：(1)數據收集和創新特性提取；(2)基於創新特性的模型訓練；(3)新穎創新特性的向量化；(4)構建多維創新特性相似性網絡，並使用 k-means 演算法對特性進行聚類；(5)提取聚類特性中的核心關鍵詞和關鍵語義結構；(6)提取主題分析，如圖 1 所示。

一、資料蒐集

(一) Phase 1 資料檢索 Data Search

本研究資料庫取自於Web of Science（WoS）資料庫進行文獻計量分析（Diem & Wolter, 2013；Falagas, Karavasiou, & Bliziotis, 2006）。Web of Science 為世界上最著名的科學引文索引數據庫之一。針對每篇出版物都包含許多詳細信息，包括出版年份、作者、作者地址、標題、摘要、來源期刊、主題類別和參考文獻。本研究利用Web of Science進行針對科技與法律的研究延伸到更廣泛的領域，如網路安全，網際網路法律和研究趨向與未來趨勢等等。第一步在研究中搜索「科技」與「法律」及相關關鍵詞中搜尋出174篇出版物的這些資料並匯出到Excel。而主題分為「出版產量和成長趨勢」、「作者及其合作」、「安全文化期刊出版」、「地理和機構分佈與合作」、「被引用分析」、「引用和同被引用分析」、「主題類別」及「術語」。

(二) Phase 2 資料預處理 Pre-Processing

本研究資料於 2024 年 5 月 7 日從 Web of Science 檢索並利用文獻計量分析進行了搜索及篩選。第二步是根據納入和排除標準對研究進行篩選，將有關於「科技」與「法律」之詞被用作搜尋主題。此主題搜尋意味著術語「科技」與「法律」在出版物的標題、摘要和／或關鍵字中被識別。搜尋詞中已包含引號。這種更嚴格的條件保證了搜尋結果的穩定性（Hao, Chen, Li, & Yan, 2018）。經過反覆核對，對大量文章進行了篩選，並移除部份相關關鍵詞的雜訊，如：AI 管理等。時間跨度設定為 2008 年至 2024 年。所有類型的出版物都包含在搜尋中。而最終篩選結果共獲得 174 篇文獻，並根據研究的相關 174 篇文獻進行

分析。

數據篩選過後，其次吾人使用 Bibliometrix 的功能，以分析和顯示數據與影像。然後使用 Biblimetrix 中的 readfile 和 convert2df 函數。readfile 函數將文字資料載入並轉換為 UTF-8 格式的文字數據，而 convert2df 函數則提取並建立一個資料幀，該資料與 UTF-8 格式的文字資料相對應。建立一個資料幀，該資料與 Bibliometrix 匯出檔案中的分析單元相對應的數據幀。最後，函數 Bibliometric Analysis 從書目資料產生描述性資料。結果可透過 R 語言中的通用函數（plot）繪製。

(三) Phase 3 檢索策略

本研究使用 Biblioshiny 套件將純文字記錄匯入 Bibliometrix R Web 介面。由此獲得的結果將在進一步的章節中進行分析和解釋。進行網路分析後，同時也分析了引用最多的論文，以進行系統性的文獻綜述，如表 1 所示。

二、共現詞網路（Co-occurrence Network）

從共現字網路（Co-occurrence Word Network）得出主題是一種基於文本中詞彙共同出現模式的分析方法。這種方法通過建立詞彙間的共現關係，揭示文本中隱藏的主題或概念。

(一) Phase 1 文字處理與詞彙提取

步驟 1.1：文本清理

1. 去除停用詞：例如，將「的」、「是」、「在」這些對主題無關的詞移除。

2. 去除標點符號：刪除標點符號以便於詞彙的提取和分析。

3. 統一大小寫：將所有文字轉換為小寫，消除因大小寫不同導致的差異。

步驟 1.2：詞彙提取

詞彙提取：從處理過的文本中提取關鍵詞 $w_1, w_2, w_3, \ldots, w_n$，這些詞彙將用於後續的共現分析。

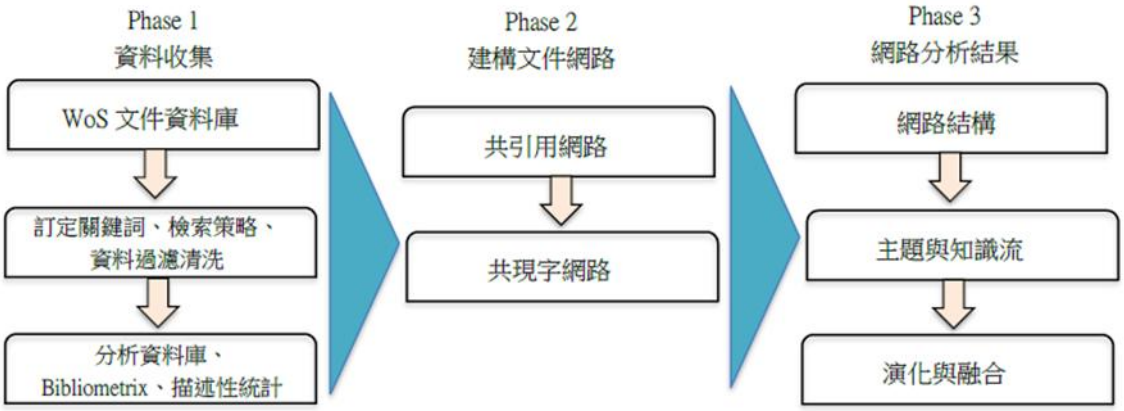

圖 1 研究流程圖

(二) Phase 2 共現矩陣的構建

步驟 2：共現次數

對於每一對詞彙(w_i, w_j)，計算它們在同一文本單位(如段落、句子或文檔) 中共同出現的次數，表示為 M_{ij}。數學公式為：

$$M_{ij} = \sum_{d \in D} f_i(d) \cdot f_j(d) \quad (1)$$

其中，M_{ij} 是詞彙 w_i 和詞彙 w_j 的共現次數。

$f_i(d)$和 $f_j(d)$分別表示詞彙 w_i 和詞彙 w_j 分別表示詞彙 M_{ij} 和詞彙 w_j 在文檔 d 中出現的次數。

(三) Phase 3 共現矩陣的標準化

步驟 3：標準化公式

Jaccard 系數：用於標準化共現矩陣，計算詞彙之間的相似度。

$$S(I,J) = Mij / M_{ii}] + M_{jj} - M_{ij}] \quad (2)$$

表 1　問卷設計內容

搜尋策略	搜尋字串結果
((\"Data Privacy\" OR \"Privacy Breach\" OR \"Privacy Protection\" OR \"Privacy Legislation\" OR \"Privacy Policy\") OR (\"Information Security\" OR \"Data Protection Measures\" OR \"Information Confidentiality\" OR \"Security Vulnerabilities\" OR \"Information Security Management\" OR \"Information Security Audit\")) AND (\"Cybersecurity Law\" OR \"Cybercrime\" OR \"Legal Response to Cyber Attacks\" OR \"Digital Identity Theft\" OR \"Cyber Surveillance Legislation\" OR \"Cyber Law Compliance\")	174

(四) Phase 4 矩陣的稀疏化與降維

步驟 4.1：稀疏化

稀疏化：對於共現頻次較低的詞彙對，將其共現值設置為零，以減少矩陣的維度和計算複雜度。

步驟 4.2：降維

奇異值分解（SVD）：可以使用奇異值分解（Singular Value Decomposition, SVD）技術對矩陣進行降維，保留信息最多的主成分。

$$M=U\Sigma V^T \quad (3)$$

其中，M 是原始矩陣，U 是左奇異向量矩陣，Σ 是奇異值對角矩陣，V^T 是右奇異向量矩陣。

(五) Phase 5 聚類分析與可視化

步驟 5.1：聚類

聚類分析：使用 *K-means* 或層次聚類方法對標準化後的矩陣進行聚類，識別出詞彙之間的主題結構。

步驟 5.2：可視化

網絡圖：將聚類結果和共現矩陣視覺化為網絡圖，節點表示詞彙，邊的粗細表示詞彙之間的共現強度。

(六) Phase 6 結果解釋與應用

步驟 6：結果解釋

主題識別：根據聚類和可視化結果，解釋每個主題群組的含義，並理解詞彙之間的關聯性。

三、共被引網路（Cocitation Network）

(一) Phase 1 文獻數據收集

步驟 1.1：選擇數據源

選擇要分析的文獻數據集，這些數據集可以來自科學數據庫如 Web of Science、Scopus 或 Google Scholar。數據應包含每篇文獻的參考文獻列表。

步驟 1.2：數據預處理

從每篇文獻中提取引用列表，並標記每篇被引文獻（如文獻 A 被文獻 B 引用）。構建包含每篇文獻引用關係的原始數據集。

(二) Phase 2 共被引矩陣的構建

步驟 2：計算共被引次數

共被引次數：對於每一對文獻 i 和 j，計算它們在其他文獻的參考文獻列表中被共同引用的次數。這些次數可以存儲在共被引矩陣 MMM 中。數學公式為：

$$M_{ij} = \sum f_{ik} f_{jk} \quad (4)$$

其中，M_{ij} 是文獻 i 和文獻 j 被共同引用的次數。f_{ik} 和 $f_j k$ 分別表示文獻 i 和文獻 j 是否被文獻 k 引用（是則為 1，否則為 0）。D 是所有文獻的集合。

(三) Phase 3 共被引矩陣的標準化

步驟 3：標準化共被引矩陣

相似性指數：為了消除文獻被引用次數的影響，可以使用相似性指數如 Salton's Cosine Similarity 或 Jaccard 系數來標準化共被引矩陣。這樣可以更準確地衡量文獻之間的共被引關係。

Salton's Cosine Similarity 的公式為：

$$S(_{i,j})= M_{ij} /(M_{ii}\times M_{jj})^{1/2} \quad (5)$$

其中 $S(_{i,j})$是文獻 i 和文獻 j 之間的相似度。

M_{ii} 和 M_{jj} 是文獻 i 和 j 被引用的總次數。

Jaccard 系數的公式為：

$$J(_{i,j})= M_{ij} /(M_{ii}+M_{j}j-M_{ij})^{1/2} \quad (6)$$

這裡，M_{ij} 表示文獻 i 和文獻 j 共同被引用的次數，而 M_{ii} 和 M_{jj} 是它們各自的被引用次數。

(四) Phase 4 網路圖的構建與降維

步驟 4.1：稀疏化

為了簡化分析，可以將共被引次數較低的文獻對（即 M_{ij} 很小的情況）設置為 0，從而得到一個更稀疏的共被引矩陣。

步驟 4.2：降維

可以使用技術如多維尺度分析（MDS）或主成分分析（PCA）對矩陣進行降維，這可以幫助在低維空間中可視化共被引網路。MDS 的數學過程：

$$d_{ij}=(M_{ii}+M_{jj}-2M_{ij})^{1/2} \quad (7)$$

這裡，d_{ij} 是文獻 i 和 j 之間的距離。

(五) Phase 5 聚類分析與主題識別

步驟 5.1：聚類

使用層次聚類或 K-means 聚類方法對文獻進行聚類，這樣可以將文獻劃分為不同的主題群組，反映出文獻之間的主題相似性。

步驟 5.2：主題識別

結合聚類結果和專業領域知識，解釋各個文獻群組所代表的具體主題。

(六) Phase 6 網路可視化與解釋

步驟 6.1：網路圖的生成

將標準化後的共被引矩陣可視化為網路圖，其中節點代表文獻，邊的權重代表共被引次數或相似度。

步驟 6.2：結果解釋

分析網路圖，確定影響力最大的文獻（通常具有最高的連接度），並研究文獻群組之間的關係。

肆、知識結構分析結果

本研究基於文獻計量分析的核心技術，使用 VOSviewer 軟體對從 WoS 下載的文獻進行分析，探討期刊論文的主題、國家、作者、關鍵詞的熱點和發展趨勢（RQ1），以及書目共被引和共現網絡中的結構性特徵與跨組織知識流動（RQ2）。VOSviewer 提供 Full counting 和 Fractional counting 兩種計數方法。Full counting 完全計數每個共現事件，適合強調總體影響力的分析，但可能高估多作者合作中的貢獻。相對而言，Fractional counting 按比例分配權重，更精確反映各參與者在合作中的相對貢獻，特別適合於多重合作情境，避免數據偏差。這種方法在分析書目共被引與共現網絡的結構性特徵時尤為重要，因為它能更準確地提供節點權重，幫助識別真正具有影響力的節點，從而更精確地分析網絡結構。此外，Fractional counting 透過按比例分配貢獻，有助於研究者更準確地掌握跨組織知識流動的全貌。通過這些技術，本研究旨在揭示科技法律領域的研究熱點、地理分佈趨勢及知識流動模式，從而深化對該領域學術和實務應用的理解。

一、描述性統計與概觀分析

本研究首先將資料分析集Ω應用敘述統計分析技術，揭開科技法律發展領域文獻各種表格與圖，這些概觀分析（Overview）資訊除可回應研究提問 1：科技法律發展領域的科學文獻演化趨勢如何，主要研究主題和熱點是什麼？另這些資訊可與各種語意分析網路（Semantic）進行交叉分析，除可回應其它研究提問外，還可進一步揭露進階資訊。如圖 2 與表 2，結果揭示了一些重要的學術

趨勢與合作模式。首先，資料涵蓋的期間從 2008 年到 2024 年，反映了研究的長期發展，並且年均增長率為 9.05%，顯示出該領域的研究活動逐年增長。此外，每篇文件的平均引用次數達到 7.263，表明這些研究具有一定的學術影響力。單一作者的文件比例較低，而每篇文件平均有 3.09 位合著者，顯示出學術合作的重要性，尤其是國際合作的比例達到 28%，進一步強調了跨國界研究合作的普遍性與必要性。這些數據不僅反映了學術研究的活力，還提供了有關研究合作和影響力的重要見解，有助於理解當前學術界的合作趨勢和學術影響。

(一) 科技法律領域的研究動態與趨勢分析之文獻數

在 2008 年至 2015 年間，文章發表數量相對穩定，顯示出對科技法律領域議題的關注，大部分探討以網路犯罪居多。例如：Bossler and Holt（2009）深入探討了網路犯罪的根源及其對受害者的影響，並提出了減少受害風險的策略，因而與網路犯罪密切相關。McGuire and Dowling（2013）提供了對網路犯罪的全面回顧，重點分析了網路犯罪的性質及其影響。這份研究根據學術、行業和政府資料，討論了網路犯罪的類型，包括網路依賴犯罪（如病毒和黑客攻擊）和網路增強犯罪（如網路詐騙和性犯罪）。Li（2015）研究一系列針對網路犯罪的法律行動，探索中國在網路空間的監管模式。為了對互聯網進行控制，中國實施了以刑事化活動、內容過濾和用戶監控為核心的法定法律和行政法規，以維護社區和國家層面的安全與穩定。

在 2016 年至 2022 年這一階段，隨著個人資料保護和網路安全法規的增加，相關文獻數量增多。Kuner（2019）文章分析了數據保護法律在國際合作中的作用，強調跨國界的數據流通需要適當的法律框架來保護個人資料。這在全球化背景下尤為重要，以應對不同國家間的法律差異。Regan（2021）分析了《通用數據保護條例》（GDPR）和加州隱私法的影響，探討隱私立法如何在全球範圍內形成新框架，促進對個人資料的保護。2023 年的發表量出現下降，這可能是由於法律改革或新興技術的影響，雖然具體原因不明，但可以推測學界在該年度的研究焦點有所調整。隨著人工智慧（AI）技術的普及，隱私法規在其發展中扮演著關鍵角色。AI 系統需要處理大量數據，這引發了對個人隱私的擔憂，並可能導致數據濫用。因此，建立適當的隱私法規如 GDPR、CCPA 和 CPRA 變得至關重要，以保護個人資料並平衡 AI 的潛在益處與隱私風險（ElBaih, 2023）。在 ElBaih（2023）探討隱私法規的現狀及其對 AI 發展的影響，強調在 AI 開發過程中納入隱私考量的策略和利益相關者的參與，以促進負責任和倫理的 AI 系統開發，科學年獻的發表篇數如圖 3 與表 3 所示。

圖 2 概觀分析

表 2 概觀分析

Category	Value
Timespan	2008:2024
Sources (Journals, Books, etc.)	125
Documents	175
Annual Growth Rate %	9.05
Document Average Age	4.29
Average citations per doc	7.263
References	7781
Author's Keywords (DE)	630
Authors	513
Authors of single-authored docs	28
Single-authored docs	28
Co-Authors per Doc	3.09
International co-authorships %	28

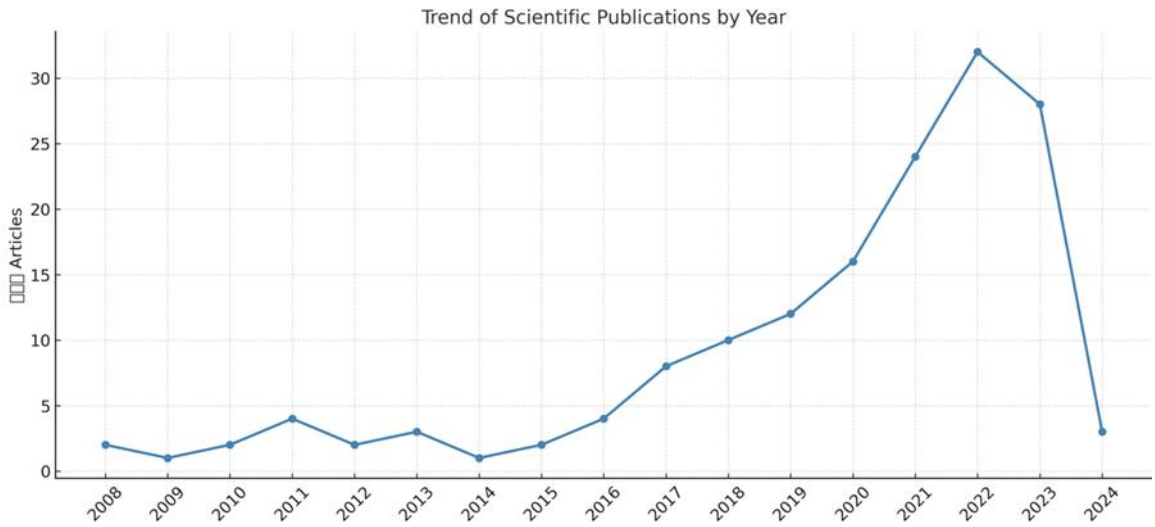

圖 3　科學文獻（年）

表 3　科學文獻數（年度）

Year	Articles
2008	2
2009	1
2010	2
2011	4
2012	2
2013	3
2014	1
2015	4
2016	8
2017	10
2018	12
2019	16
2020	24
2021	32
2022	28
2023	10
2024	3

(二) 國際合作與研究焦點－Three-Field Plot

這張三字段圖（Three-Field Plot）展示了科技法律領域的國際合作與研究焦點，通過連結不同國家（AU_CO）、機構（AU_UN）和關鍵詞（DE），揭示了全球科技法律研究的分佈及其重點。左側欄位顯示了來自美國、英國、印度、以色列等國家的活躍研究者，中間欄位展示了他們所屬的機構，如印度的安米塔維希亞大學（Amrita Vishwa Vidyapeetham）、以色列的特拉維夫大學（Tel Aviv University）和美國的密西根州立大學（Michigan State University）等。右側欄位的關鍵詞如網路犯罪、資訊安全、網路安全等反映了科技法律領域中的主要研究議題，這些主題不僅展示了科技進步對法律的影響，也指出了當前法律研究中的熱點。該圖表顯示出不同地區在網路犯罪和科技法律問題上的關注與研究重點，例如以色列機構在網絡安全和基礎設施保護方面的研究，美國和英國則涵蓋更廣泛的科技法律議題。這張圖不僅強調了科技法律領域國際合作的重要性，還展示了各國研究者如何通過共享知識和資源來應對全球性法律挑戰，提供了對研究趨勢和焦點的全面視角。如圖 4 所示。

二、學術影響力分析

在法律學術研究中，H 指數是一個關鍵指標，用於衡量期刊的學術影響力和權威性。H 指數反映了期刊中的文章被引用的頻率和範圍，因此對於法律學者而言，理解這些數據至關重要。表 4 與圖 5 展示了從「Computer Law & Security Review」到「Algorithms」等多個領域的期刊 H 指數，範圍從 0 到 3。高 H 指數期刊如「Computer Law & Security Review」和「Computers & Security」顯示其在資訊安全和電腦法律領域具有顯著影響力和廣泛認可度。相對而言，中等 H 指數期刊如「IEEE Access」和「Information Security Journal」在其領域內也有相當影響力，但略低於頂尖期刊。低 H 指數期刊如「African Journal of Science Technology Innovation & Development」則可能代表新興或影響力較低的期刊。這些數據對法律學者在選擇發表平台時提供了重要參考，並對學術機構資源分配及法律教育和政策制定者提供了指導。通過選擇高 H 指數期刊發表，學者可以提升其研究的可見度和學術影響力，從而促進其職業發展和學術聲譽的提升。

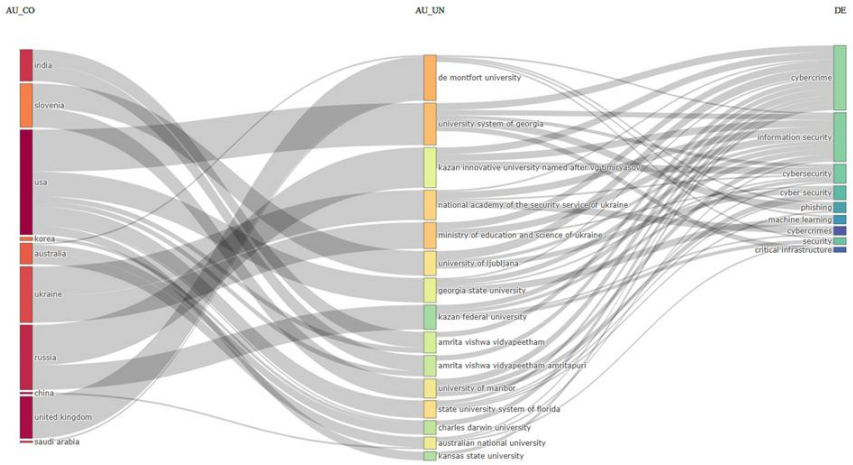

圖 4　三字段圖（國家－機構－關鍵字）

表 4　學術影響力（H 指數）

Element	h_index	g_index	m_index	TC	NP	PY3_start
Computer Law & Security Review	3	5	0.38	6	5	2015
Computers & Security	3	5	0.31	7	5	2017
Computers In Human Behavior	3	5	0.375	6	4	2017
Information And Computer Security	3	5	0.23	9	4	2015
Journal Of Information Security And Applications	3	5	0.24	8	3	2015
Applied Sciences-Basel	2	3	0.25	8	2	2021
Big Data And Cognitive Computing	2	2	0.33	4	3	2021
Cuestiones Politicas	2	2	0.53	14	2	2021
Ieee Access	2	3	0.33	14	2	2021
Information Security Journal	2	2	0.33	7	2	2020
Information Systems Frontiers	2	2	0.18	8	2	2017
International Data Privacy Law	2	2	0.2	6	2	2019
International Journal Of Information Security	2	2	0.25	7	3	2017
Revista Kriminalistiko In Kriminologijo	2	2	0.23	3	2	2019
Security And Privacy	2	2	0.33	4	3	2020
Security Journal	2	2	0.33	3	2	2018
Accounting Organizations And Society	1	1	0.17	4	1	2019
Acm Journal Of Data And Information Quality	1	1	0.14	1	1	2017
African Journal Of Science Technology Innovation & Development	1	1	0.2	2	1	2019
Algorithms	1	1	0.11	1	1	2016
Amazonia Investiga	1	1	0.16	1	1	2017
Asia Pacific Law Review	1	1	0.11	1	1	2016
Australian Journal Of Forensic Sciences	1	1	0.08	1	1	2017
Automatika	1	1	0.075	2	1	2017
Behaviour & Information Technology	1	1	0.115	15	1	2016

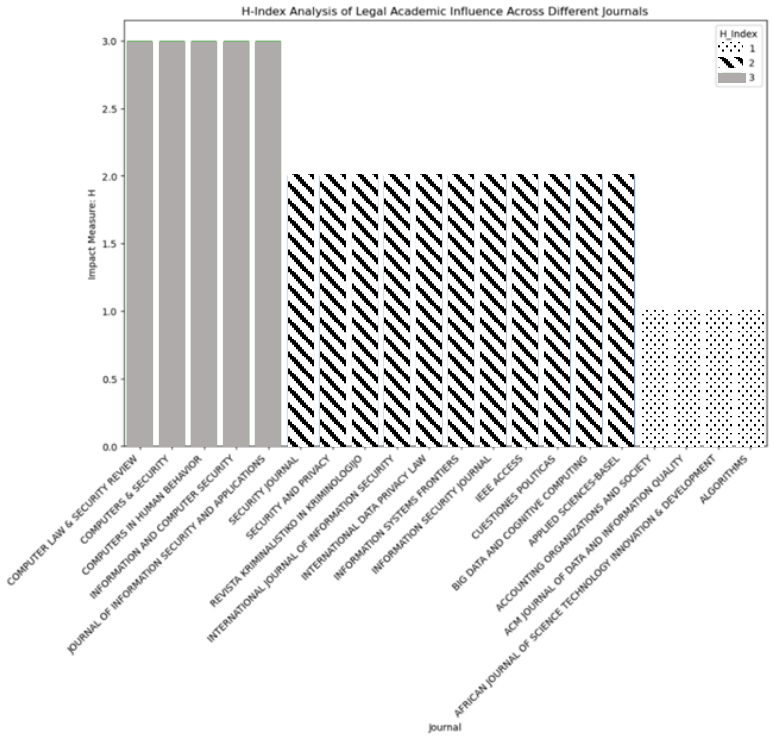

圖 5 學術影響力（H-Index）

三、合作作者網路關係結構－組織（Co-authorship: Organizations）

在分析網絡安全研究出版機構的合作作者關係時，使用分數計數法得到了前 15 個機構的總鏈接強度（TLS）。在這些機構中，Bit4id srl、CEA 和 Ctr Res & Technol Hellas 等機構的 TLS 最高，表現出它們在研究合作中的重要性。每個機構在這些已發表的文獻中都至少被引用了 25 次，但其合作鏈接強度往往小於其總發表數量，這可能表明部分文獻缺少來自其他機構的合作作者。特別值得注意的是，中國機構在該榜單中占據了主導地位，而沙烏地阿拉伯、卡塔爾等地區的機構也名列其中，這表明這些地區在網絡安全研究中扮演了重要角色。這些機構在網絡安全和取證研究中積極合作，為全球該領域的發展作出了重要貢獻。如表 5 與圖 6。

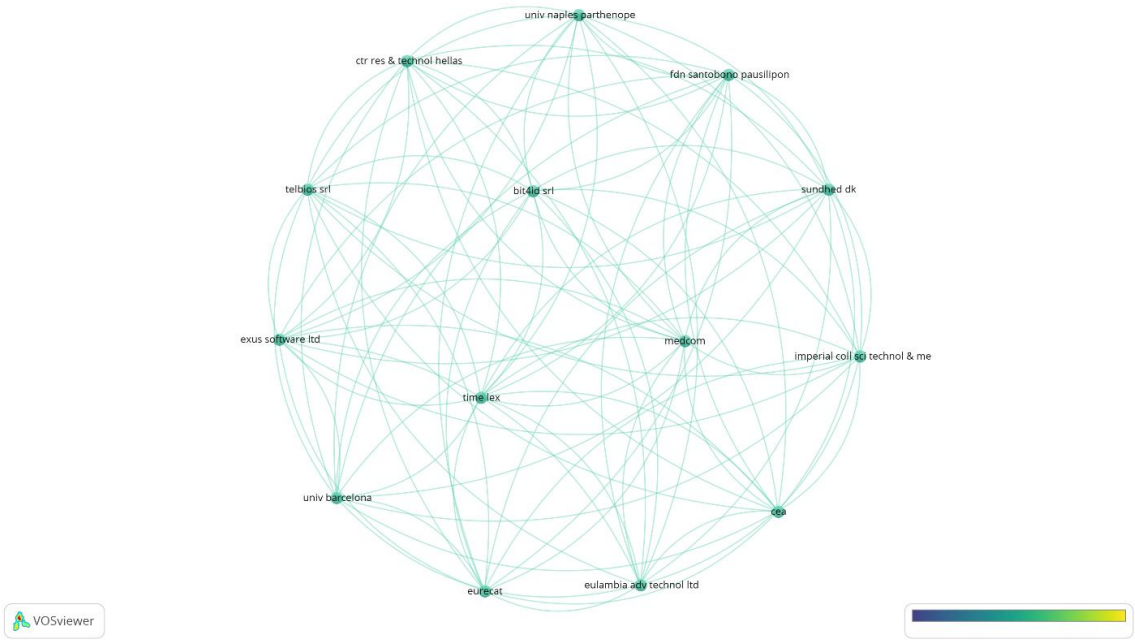

圖 6　合作作者網路關係結構（組織）TLS＞13

表 5　合作作者網路關係結構（組織）TLS＞13

Organization	Documents	Citations	Total Link Strength (TLS)
Bit4id Srl	1	25	13
CEA	1	25	13
Ctr Res & Technol Hellas	1	25	13
Eulambia Adv Technol Ltd	1	25	13
Eurecat	1	25	13
Exus Software Ltd	1	25	13
Fdn Santobono Pausiilpon	1	25	13
Imperial Coll Sci Technol & Med	1	25	13
Medcom	1	25	13
Sundhed Dk	1	25	13
Telbios Srl	1	25	13
Time Lex	1	25	13
Univ Barcelona	1	25	13
Univ Naples Parthenope	1	25	13
King Saud Univ	3	50	10

四、共現字網路結構（關鍵字）

共現字網路結構是一種用來分析文獻中關鍵詞或詞語之間的關聯性的方法。在過去十年間，Web of Science（WoS）上發表的網絡安全和取證領域的文章中，關鍵詞如「網路犯罪」、「資訊安全」和「網路安全」經常一起出現，並且在分析中形成強大的共現網絡。圖中的節點大小代表關鍵詞的出現頻率，而連線則顯示關鍵詞之間的共現關係。較粗的連線表示更強的關聯性，這意味著這些關鍵詞在文獻中經常共同出現。從圖 7 和表 6 中可以看出，「網路犯罪」和「資訊安全」是這個領域中核心的研究主題，它們的高 TLS 值顯示出與其他關鍵詞的緊密聯繫。這些關鍵詞反映了網絡安全領域中的重要研究趨勢和熱點議題。例如，機器學習技術被廣泛應用於網絡安全中，並且與其他相關技術形成了緊密的共現網絡。

五、共被引網路結構－資料來源

根據共被引（Co-citation）分析所生成的資料來源（sources）網絡圖。這類圖表可以幫助識別不同學術文獻來源（如期刊、書籍、會議論文集等）之間的關聯性，並展示它們在研究領域中的相互影響。如表 7 和圖 8 所示，TLS 前五名的期刊依次為 Computers & Security（Comput Secur），以 4570 的 TLS 值領先，這表明它在網絡安全領域中具有核心地位，並且被廣泛引用。Deviant Behavior（Deviant Behav），擁有 2812 的 TLS 值，顯示了其在犯罪學研究中的重要影響力。MIS Quarterly（MIS Quart），以 2811 的 TLS 值位居第三，反映了其在信息系統領域的深遠影響。International Journal of Cyber Criminology（Int J Cyber Criminol），TLS 值為 2413，專注於網絡犯罪的研究，顯示出在該領域的重要性。Computers in Human Behavior（Comput Hum Behav），TLS 值為 2301，聚焦於人類行為與計算機互動，具有廣泛的學術引用。共引分析圖表明，這些期刊之間的引用關係密切，節點的大小與其被引用次數成正比，而節點之間的連線則表示期刊之間的共引用關係。特別是「Comput Secur」，其被引用次數最多，顯示出其在網絡安全領域的關鍵地位。此外，圖中的不同顏色集群代表了不同的研究領域，例如藍色集群可能代表法律和犯罪學相關的期刊，綠色集群則可能集中在信息安全研究。這些集群反映了學術研究中不同領域之間的緊密聯繫，研究者可以通過這些共引用關係，識別出在各自領域中具有核心影響力的期刊，從而更好地理解學術研究的發展趨勢和脈絡。

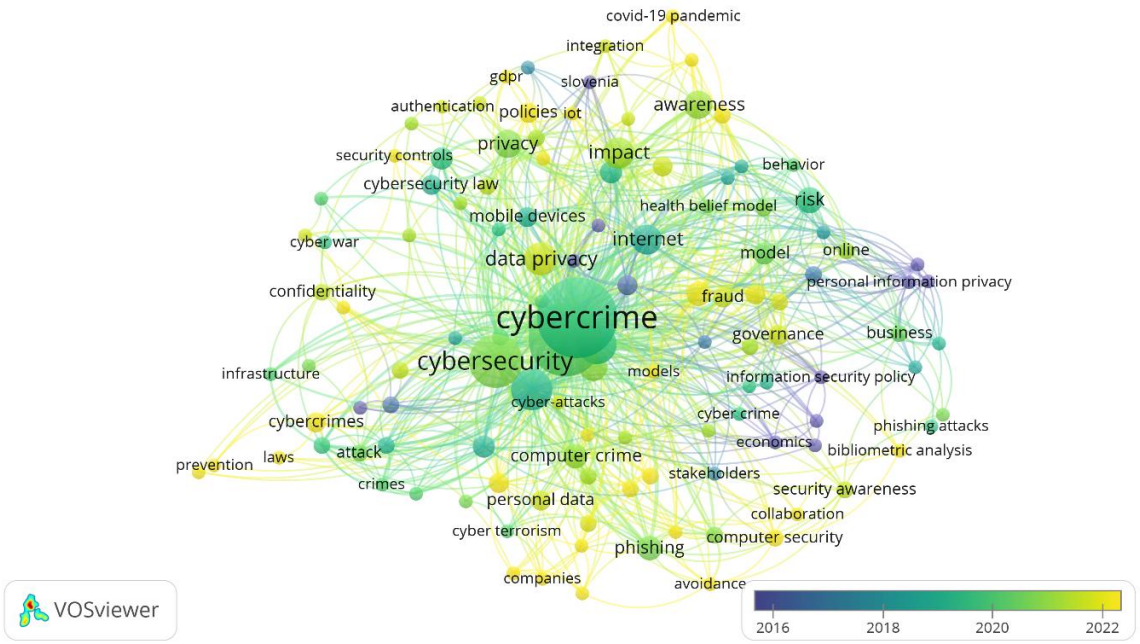

圖 7　共現分析（關鍵字）

表 6　共現字網路結構（關鍵字）TLS：前 15 名

關鍵詞	出現次數（P）	連結數量	總鏈接強度（TLS）
網路犯罪（Cybercrime）	64	67	248
資訊安全（Information Security）	54	62	211
網路安全（Cybersecurity）	29	54	108
安全（Security）	17	45	75
犯罪（Crime）	16	28	83
資料隱私（Data Privacy）	11	32	42
隱私（Privacy）	8	30	35
安全意識（Security Awareness）	7	25	34
駭客攻擊（Cyber Attacks）	7	24	31
網路詐騙（Phishing）	6	22	29
網路罪犯（Cybercrime）	7	23	27
風險（Risk）	7	21	25
網絡基礎設施（Infrastructure）	5	20	24
資訊保護（Information Protection）	5	18	22
電子商務（E-commerce）	5	18	22

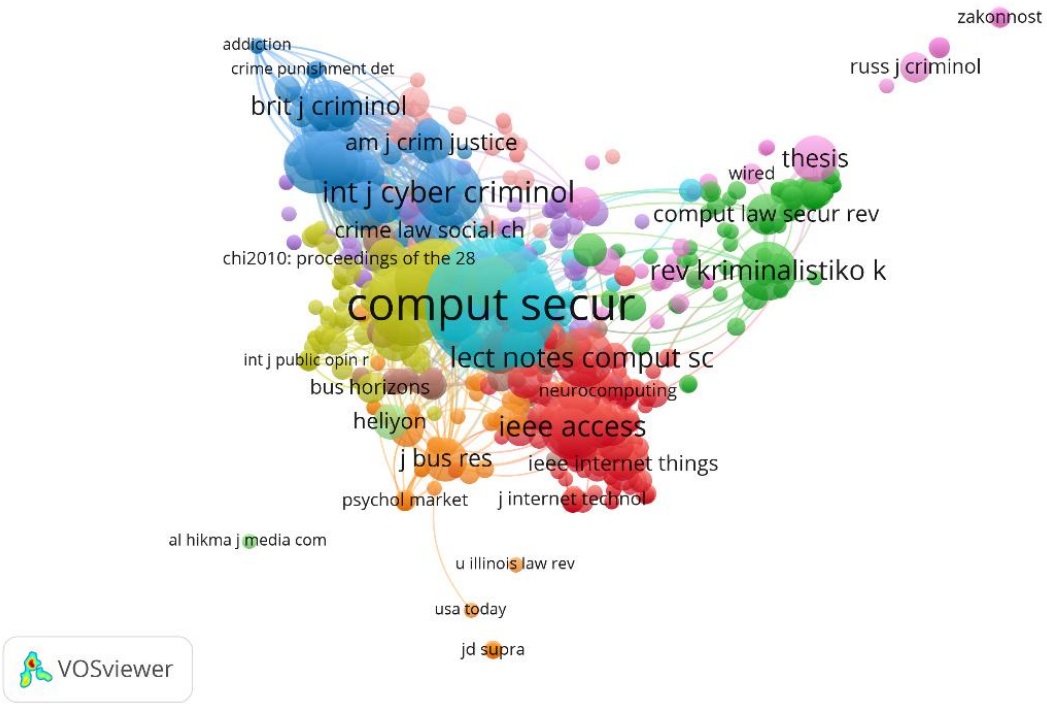

圖 8 共被引網路結構－資料來源（TLS 排名前 15 名）

表 7 共被引網路結構－資料來源（TLS 排名前 15 名）

Source	Citations	Total Link Strength (TLS)
Comput Secur	150	4570
Deviant Behav	34	2812
Mis Quart	60	2811
Int J Cyber Criminol	40	2413
Comput Hum Behav	52	2301
Brit J Criminol	25	1941
Int J Drug Policy	15	1695
Inform Manage-Amster	27	1351
Soc Sci Comput Rev	15	1265
IEEE Access	37	1260
J Res Crime Delin	21	1212
Crime Delinquency	29	1212
Am J Crim Justice	15	1208
Eur J Inform Syst	24	1121
Commun Acm	13	1062

六、討論

本研究通過書目共被引和共現網絡分析，揭示了網絡安全領域內的結構性特徵，並提供了該領域國際合作與研究熱點的全面視角。基於這些發現，我們可以深入討論以下幾個關鍵點，這些點不僅強調了當前研究的價值，也為未來研究的發展方向提供了參考。

首先，研究結果顯示，網絡安全領域的學術發展高度依賴於國際合作和跨學科的聯繫。通過三字段圖的分析，我們發現來自不同國家和地區的研究者在推動該領域的發展中發揮了重要作用，特別是美國、英國和印度等國家的研究者以及他們所屬的研究機構，這些機構在全球學術網絡中占據了核心位置。這種現象表明，網絡安全問題的複雜性和全球性特徵要求國際間的緊密合作，以便更有效地應對各種挑戰。跨國合作不僅促進了知識的流動和共享，也有助於不同法律體系間的相互理解和借鑒，這對於解決全球性網絡安全問題至關重要。

其次，共現網絡分析顯示，「網路犯罪」、「資訊安全」等關鍵詞在文獻中形成了緊密的共現網絡，這表明這些議題在學術界占據了核心地位。這反映出隨著科技的進步，網絡犯罪和資訊安全已成為法律學者和技術專家共同關注的焦點。這些研究熱點的出現也與全球範圍內網絡攻擊和數據洩露事件的頻繁發生密切相關。在這種背景下，學者們不僅需要深入探討網絡安全的技術層面，還需結合法律、政策、社會影響等多維度進行綜合分析，以提出更具操作性和前瞻性的解決方案。

此外，書目共被引分析強調了特定期刊在網絡安全領域內的學術影響力。以《Computers & Security》為例，該期刊在共被引分析中的領先地位顯示了它在推動網絡安全研究中的核心角色。這意味著，研究者在選擇發表平台時，應考慮期刊的 H 指數及其在該領域內的影響力，以提升研究的可見度和影響力。期刊的選擇不僅關係到研究成果的傳播效果，還影響到研究者個人在學術界的聲譽和職業發展。因此，研究者應充分利用這些高影響力期刊所提供的平台，推動其研究成果在更廣泛的學術社群中得到認可。

另一方面，本研究也揭示了全球各地的研究機構在網絡安全領域中的合作情況。儘管一些機構在全球學術網絡中具有較高的總鏈接強度（TLS），如 bit4id srl、cea 和 ctr res & technol hellas，但研究結果顯示，部分文獻仍然缺乏來自其他機構的合作作者。這可能反映了某些機構在推動自主研究方面的優勢，但同時也指出了跨機構合作的潛在不足。特別是來自中國和中東地區的研究機構在全球網絡安全研究中日益顯示出其重要性，這表明這些地區在國際學術舞台上

的地位逐漸提升。然而，為了進一步提升全球影響力，這些機構仍需加強與國際同行的合作，尤其是在共享資源和研究成果方面。

總結來說，本研究揭示了網絡安全領域內的研究動態和結構特徵，強調了國際合作、研究熱點的共現，以及核心期刊的學術影響力。這些討論點為我們理解該領域的發展提供了新的視角，並為未來研究提供了方向。隨著新興技術的不斷出現和網絡安全威脅的增加，研究者應繼續關注這些熱點問題，並通過跨學科和國際合作推動該領域的持續發展。

伍、結論

本研究運用書目共被引分析和共現網絡分析，對網絡安全研究領域的結構性特徵進行了深入探討，並結合國際合作與研究焦點的分析，揭示了該領域在全球範圍內的學術發展趨勢、合作模式、以及主要研究熱點。這一分析不僅確定了網絡安全領域的核心學術資源，還展示了該領域研究的全球性分佈及其跨國合作的情況，提供了對當前研究格局的全面視角。

首先，通過書目共被引分析，我們識別了網絡安全領域內具有重大影響力的期刊和文獻。例如，《Computers & Security》期刊以 4570 的總鏈接強度（TLS）出其在該領域中的核心地位，成為研究者引用最多的來源之一。此結果表明，該期刊在網絡安全研究中具有高度的學術影響力，其所發表的文章對該領域的研究方向和學術討論產生了深遠的影響。同樣，期刊如《Deviant Behavior》和《MIS Quarterly》也顯示出在各自相關領域中的重要性，進一步強調了跨學科研究在網絡安全研究中的價值。

此外，共現網絡分析進一步揭示了網絡安全研究中的主要研究熱點及其相互關聯。分析結果顯示，關鍵詞如「網路犯罪」、「資訊安全」和「網路安全」在文獻中出現頻率高，並形成了緊密的共現網絡，這些關鍵詞代表了網絡安全領域中最受關注的核心議題。例如，機器學習技術被廣泛應用於網絡安全中，與其他技術如數據加密和網絡監控技術形成了強大的共現網絡，顯示出其在實踐中的重要性。這些結果表明，網絡安全領域的研究主題逐漸從傳統的安全防護措施轉向了更複雜的技術應用和政策探討。

在國際合作與研究焦點方面，本研究通過三字段圖（Three-Field Plot）的分析展示了全球科技法律研究的分佈及其研究重點。分析結果顯示，美國、英國和印度等國家的研究者在該領域中活躍，並且這些研究者所屬的機構如印度的安米塔維希亞大學（Amrita Vishwa Vidyapeetham）、以色列的特拉維夫大學（Tel Aviv University）和美國的密西根州立大學（Michigan State University）等，在網絡安全與相關法律問題的研究中發揮了重要作用。特別是這些機構在「網路犯罪」和「資訊安全」等領域的研究活躍度高，並且其研究成果經常被引用，顯示出這些主題在學術界的核心地位。這種國際間的合作不僅推動了全球範圍內的學術交流，也強調了不同國家和地區在應對網絡安全挑戰方面的合作必要性。

進一步的合作作者網路關係結構表明，全球範圍內的研究機構在網絡安全領域中積極合作，共同推動了該領域的發展。研究結果顯示，機構如 Bit4id Srl、CEA 和 Ctr Res & Technol Hellas 在研究合作中具有較高的總鏈接強度（TLS），表現出它們在推動網絡安全研究中的重要性。同時，來自中國、沙烏地阿拉伯和卡塔爾等地區的機構也在該領域中扮演了重要角色，這表明全球性合作在網絡安全研究中的廣泛性和多樣性。

綜合來看，本研究揭示了網絡安全領域的學術研究不僅受到技術發展的驅動，還依賴於國際間的廣泛合作與跨學科的聯繫。書目共被引和共現網絡的結構分析為我們提供了一個全面的框架，幫助理解該領域內的研究趨勢、核心資源以及未來的研究方向。

參考文獻

1. Ahmed, U., Raza, I., Hussain, S. A., Ali, A., Iqbal, M., & Wang, X. (2015). Modelling cyber security for software-defined networks those grow strong when exposed to threats: Analysis and propositions. Journal of Reliable Intelligent Environments, 1, 123-146.

2. Ani, U. D., Daniel, N., Oladipo, F., & Adewumi, S. E. (2018). Securing industrial control system environments: The missing piece. Journal of Cyber Security Technology, 2(3-4), 131-163.

3. Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of Informetrics, 11(4), 959-975.

4. Azambuja, A. J. G. D., & Almeida, V. R. (2021). A bibliometric study of cybersecurity in industry 4.0 publications. Research, Society and Development, 10(3), 4210312937e.

5. Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. ACM Computing Surveys (CSUR), 25(4), 375-414.

6. Benckendorff, P. (2009). Themes and trends in Australian and New Zealand tourism research: A social network analysis of citations in two leading journals (1994-2007). Journal of Hospitality and Tourism Management, 16(1), 1-15.

7. Benckendorff, P., & Zehrer, A. (2013). A network analysis of tourism research. Annals of Tourism Research, 43, 121-149.

8. Bondoc, C. E., & Malawit, T. G. (2020). Cybersecurity for higher education institutions: Adopting regulatory framework. Global Journal of Engineering and Technology Advances, 2(3), 16-21.

9. Borgman, C. L., & Furner, J. (2002). Scholarly communication and bibliometrics. Annual Review of Information Science and Technology, 36(1), 1-53.

10. Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology, 3(1), 400-420.

11. Bues, M. M., & Matthaei, E. (2017). LegalTech on the rise: Technology changes legal work behaviours, but does not replace its profession. In K. Jacob, D. Schindler, & R. Strathausen (Eds.), Liquid Legal: Transforming Legal into a Business Savvy, Information Enabled and Performance Driven Industry, 89-109. Cham: Springer International Publishing.

12. Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. UC Davis Law Review, 51, 399-435.

13. Cavelty, M. D. (2007). Critical information infrastructure: Vulnerabilities, threats and responses. Disarmament Forum, 2007(3), 15-22.

14. Chandola, V., Banerjee, A., & Kumar, V. (2012). Anomaly detection for discrete sequences: A survey. IEEE Transactions on Knowledge and Data Engineering, 24(5), 823-839.

15. Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Education and Information Technologies, 27(4), 1-24.

16. Davis, K. E. (2013). Contracts as technology. New York University Law Review, 88(1), 83-127.

17. De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Cambridge, MA: Harvard University Press.

18. Diem, A., & Wolter, S. C. (2013). The use of bibliometrics to measure research performance in education sciences. Research in Higher Education, 54(1), 86-114.

19. Elango, B., Matilda, S., & Jeyasankari, J. (2020). Redefining Search Terms for Cybersecurity: A Bibliometric Perspective. International Conference on Recent Advances in Computational Techniques (IC-RACT), Mumbai.

20. ElBaih, M. (2023). The Role of Privacy Regulations in AI Development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI). The George Washington University Law School, unpublished paper.

21. Falagas, M. E., Karavasiou, A. I., & Bliziotis, I. A. (2006). A bibliometric analysis of global trends of research productivity in tropical medicine. Acta Tropica, 99(2-3), 155-159.

22. Force, J. T. (2017). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technology (NIST Special Publication 800-37 Revision 2).

23. Garfield, E. (1964). "Science citation index" - A new dimension in indexing: This unique approach underlies versatile bibliographic systems for communicating and evaluating information. Science, 144(3619), 649-654.

24. Garfield, E. (2004). Historiographic mapping of knowledge domains literature. Journal of Information Science, 30(2), 119-145.

25. Garfield, E., Sher, I. H., & Torpie, R. J. (1964). The Use of Citation Data in Writing the History of Science. Philadelphia: Institute for Scientific Information Inc.

26. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Proceedings of the 28th International Conference on Neural Information Processing Systems, 2, 2672-2680.

27. Grigorovič, V. (2017). Cyber Crimes: Analysis of Reasons and Effects for Business Organizations. Mykolas Romeris University, unpublished paper.

28. Grobler, T., & Louwrens, B. (2005). New Information Security Architecture. Paper presented at the Information Security South Africa (ISSA) 2005 Conference, Sandton.

29. Hao, T., Chen, X., Li, G., & Yan, J. (2018). A bibliometric analysis of text mining in medical research. Soft Computing, 22(23), 7875-7892.

30. Hjørland, B. (2013). Facet analysis: The logical approach to knowledge organization. Information Processing & Management, 49(2), 545-557.

31. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780.

32. Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243-248.

33. Howells, G., Twigg-Flesner, C., & Wilhelmsson, T. (2017). Rethinking EU Consumer Law. Abingdon, Routledge: Taylor & Francis.

34. Hu, C., & Racherla, P. (2008). Visual representation of knowledge networks: A social network analysis of hospitality research domain. International Journal of Hospitality Management, 27(2), 302-312.

35. Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information Security Technical Report, 13(4), 247-255.

36. Hyla, E. J. (2018). Corporate cybersecurity: The international threat to private networks and how regulations can mitigate it. Vanderblit Journal Entertainment and Technology Law, 21(1), 309-338.

37. Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: Bibliometric analysis of the literature. Journal of Medical Internet Research, 21(2), e12644.

38. Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. NIST(Special Publication 800-144).

39. Jensen, P. H., & Webster, E. (2014). Patents, transaction costs and academic research project choice. Economic Record, 90(289), 179-196.

40. Kendall, C. L. (2022). The Openness of Higher Education and Implications on Cybersecurity. Utica University, unpublished paper.

41. Khan, L. M. (2016). Amazon's antitrust paradox. Yale lJ, 126(3), 710-805.

42. Khan, S., & Hoque, A. (2016). Digital health data: A comprehensive review of privacy and security risks and some recommendations. Computer Science Journal of Moldova, 24(2), 273-292.

43. Kuner, C. (2019). International organizations and the EU general data protection regulation: Exploring the interaction between EU law and international law. International Organizations Law Review, 16(1), 158-191.

44. Larivière, V., & Costas, R. (2016). How many is too many? On the relationship between research productivity and impact. PloS One, 11(9), e0162709.

45. Lavrov, E. A., Zolkin, A. L., Aygumov, T. G., Chistyakov, M. S., & Akhmetov, I. V. (2021). Analysis of information security issues in corporate computer networks. IOP Conference Series: Materials Science and Engineering, 1047(1), 1-6.

46. Li, X. (2015). Regulation of cyber space: An analysis of Chinese law on cyber crime. International Journal of Cyber Criminology, 9(2), 185-204.

47. Ligges, U. (2009). 'The R book' by Crawley MJ. Statistical Papers, 50(2), 445-446.

48. Lu, L. Y., & Liu, J. S. (2013). An innovative approach to identify the knowledge diffusion path: The case of resource-based theory. Scientometrics, 94(1), 225-246.

49. Majdouline, I., Baz, J. E., & Jebli, F. (2022). Revisiting technological entrepreneurship research: An updated bibliometric analysis of the state of art. Technological Forecasting and Social Change, 179, 121589.

50. Makawana, P. R., & Jhaveri, R. H. (2018). A bibliometric analysis of recent research on machine learning for cyber security. In Y. C. Hu, S. Tiwari, K. K. Mishra, & M. C. Trivedi (Eds.), Intelligent Communication and Computational Technologies: Proceedings of Internet of Things for Technological Development, 213-226. Singapore: Springer International Publishing.

51. Makulilo, A. B. (2015). Privacy in mobile money: Central banks in Africa and their regulatory limits. International Journal of Law and Information Technology, 23(4), 372-391.

52. McGuire, M., & Dowling, S. (2013). Cyber Crime: A Review of the Evidence. Summary of Key Findings and Implications. Home Office (Home Office Research Report No. 75).

53. Nakhodchi, S., & Dehghantanha, A. (2020). A bibliometric analysis on the application of deep learning in cybersecurity. In H. Karimipour, P. Srikantha, H. Farag, & J. Wei-Kocsis (Eds.), Security of Cyber-Physical Systems: Vulnerability and Impact, 203-221. Cham: Springer International Publishing.

54. Omidosu, J., & Ophoff, J. (2016). A Theory-Based Review of Information Security Behavior in the Organization and Home Context. 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), Durban, South Africa: IEEE.

55. Pfleeger, C. P., & Pfleeger, S. L. (2012). Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach. NJ: Prentice Hall.

56. Price, D. J. D. S. (1965). Networks of scientific papers: The pattern of bibliographic references indicates the nature of the scientific research front. Science, 149(3683), 510-515.

57. Putro, P. A. W., & Sensuse, D. I. (2021). Threats, Vulnerabilities and Security Functions in Critical Information Infrastructure. Paper presented at Proceedings of the 2021 8th International Conference on Information Technology, Computer and Electrical Engineering, Semarang.

58. Rahim, N. (2021). Bibliometric analysis of cyber threat and cyber attack literature: Exploring the higher education context. In M. Sarfraz (Eds.), Cybersecurity Threats with New Perspectives, 147-162. London: Intechopen.

59. Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. Applied Sciences, 12(3), 1598.

60. Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. Journal of Cases on Information Technology (JCIT), 8(4), 24-34.

61. Regan, P. M. (2021). Fifty-plus years of information privacy policy-making: The more things change, the more they remain the same. In A. S. Duff (Eds.), Research Handbook on Information Policy, 159-173. Cheltenham, UK: Edward Elgar Publishing.

62. Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. Information Management Journal-Prairie Village, 39(4), 60-62, 64-66.

63. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7-34.

64. Scharnick, N., Gerber, M., & Futcher, L. (2016). Review of Data Storage Protection Approaches for POPI Compliance. 2016 Information Security for South Africa (ISSA), Johannesburg.

65. Segev, E. (2021). Semantic Network Analysis in Social Sciences. UK: Routledge.

66. Sharma, A., Tyagi, A., & Bhardwaj, M. (2022). Analysis of techniques and attacking pattern in cyber security approach: A survey. International Journal of Health Sciences, 6(S2), 13779-13798.

67. Sharma, D., Gupta, P. K., & Andreu-Perez, J. (2021). A review on cyber physical systems and smart computing: Bibliometric analysis. In P. Shah, R. Sekhar, A. J. Kulkarni, & P. Siarry (Eds.), Metaheuristic algorithms in industry 4.0, 1-31. Boca Raton, FL: CRC Press.

68. Sharma, D., Mittal, R., Sekhar, R., Shah, P., & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. Results in Control and Optimization, 10, 100204.

69. Shukla, G., & Gochhait, S. (2020). Cyber security trend analysis using Web of Science: A bibliometric analysis. European Journal of Molecular and Clinical Medicine, 7(6), 2567-2576.

70. Stafford, V. (2020). Zero Trust Architecture. NIST special publication(800-207).

71. Stallings, W. (2016). Network Security Essentials: Applications and Standards. Boston, MA: Pearson.

72. Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. Future Generation Computer Systems, 98, 660-671.

73. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A Detailed Analysis of the KDD CUP 99 Data Set. 2009 IEEE symposium on computational intelligence for security and defense applications, Ottawa.

74. Ulven, J. (2020). High Level Information Security Risk in Higher Education. NTNU, unpublished paper.

75. Van Eck, N., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2), 523-538.

76. Van Raan, A. F. J. (2005). For your citations only? Hot topics in bibliometric analysis. Measurement: Interdisciplinary Research and Perspectives, 3(1), 50-62.

77. Vithanwattana, N., Karthick, G., Mapp, G., George, C., & Samuels, A. (2022). Securing future healthcare environments in a post-COVID-19 world: Moving from frameworks to prototypes. Journal of Reliable Intelligent Environments, 8(3), 299-315.

78. Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer International Publishing.

79. Wang, P., D'Cruze, H., & Wood, D. (2019). Economic costs and impacts of business data breaches. Issues in Information Systems, 20(2), 162-171.

80. White, H. D., & McCain, K. W. (1998). Visualizing a discipline: An author co-citation analysis of information science, 1972-1995. Journal of the American Society for Information Science, 49(4), 327-355.

81. Zupic, I., & Čater, T. (2015). Bibliometric methods in management and organization. Organizational Research Methods, 18(3), 429-472.

113 年 **09** 月 **01** 日收稿

113 年 **10** 月 **01** 日初審

113 年 **10** 月 **20** 日複審

113 年 **10** 月 **25** 日接受

作者介紹

Author's Introduction

姓名	盧政遠
Name	Cheng-Yuan Lu
服務單位	朝陽科技大學企業管理系台灣產業策略發展博士班
Department	Ph. D. Student, Department of Business Administration, Chaoyang University of Technology
聯絡地址	臺中市霧峰區吉峰東路 168 號
Address	No.168, Jifeng East Road, Wufeng District, Taichung City, Taiwan
E-mail	lu.04118@gmail.com
專長	科技管理、創新管理
Specialty	Technology Management, Innovation Management

姓名	徐毓君
Name	Yu-Jun Hsu
服務單位	朝陽科技大學企業管理系台灣產業策略發展博士班
Department	Ph. D. Student, Department of Business Administration, Chaoyang University of Technology
聯絡地址	嘉義市大同路 102 巷 10 弄 8 號
Address	No.8, Alley 10, Lane 102, Datong Road, Chiayi City, Taiwan
E-mail	sir1819@hotmail.com
專長	科技管理、創新管理
Specialty	Technology Management, Innovation Management

姓名	賴奎魁
Name	Kuei-Kuei Lai
服務單位	朝陽科技大學企業管理系特聘教授
Department	Distinguished Professor, Department of Business Administration, Chaoyang University of Technology
聯絡地址	臺中市霧峰區吉峰東路 168 號
Address	No.168, Jifeng East Road, Wufeng District, Taichung City, Taiwan
E-mail	laikk.tw@gmail.com
專長	科技管理、創新管理、專利分析
Specialty	Technology Management, Innovation Management, Patent Analysis