CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 1, Mei 2024,, hlm. 50-55

Analisis Bibliometrika: 4 Dekade Penelitian *Cyber Weapon* dalam Peperangan Modern

Dedy Hariyadi

Universitas Jenderal Achmad Yani Yogyakarta
Email: dedy@unjaya.ac.id

Abstrak

Dibalik serangan siber terdapat metode baru dalam peperangan modern, yaitu pemanfaatan *cyber weapon*. Artikel ini menggunakan analisis bibliometrika untuk memetakan tren dan kesenjangan dalam studi tentang *cyber warfare*, dengan data yang diambil dari sistem indeks Scopus. Dokumen yang digunakan adalah daftar indeks artikel dari Scopus sebanyak 565 artikel. Hasil analisis menunjukkan peningkatan signifikan dalam publikasi terkait *cyber weapon* sejak tahun 2018, Amerika Serikat sebagai negara kontributor terbesar yang diikuti oleh negara-negara lain seperti India, Britania Raya, Cina, dan Korea Selatan. Selain itu, penelitian ini mengidentifikasi tiga kluster utama: ancaman siber terhadap infrastruktur kritis, strategi pertahanan siber, dan peran spionase dalam serangan siber. Artikel ini juga menyoroti pentingnya pemetaan penelitian untuk mengembangkan strategi mitigasi yang lebih efektif terhadap ancaman *cyber weapon* dan meningkatkan kesadaran global tentang perang siber. Penelitian lebih lanjut diperlukan untuk mengeksplorasi peran kecerdasan buatan dalam taktik *cyber weapon* yang terus berkembang, serta untuk memahami dampak sosial dan ekonomi dari serangan siber.

Kata kunci: *cyber warfare*, *cyber weapon*, analisis bibliometrika, serangan siber, pertahanan siber

4 Decades of Cyber Weapon Research in Modern Warfare: A Bibliometrics Analysis

Abstract

Behind cyber attacks is a new method in modern warfare, namely the utilization of cyber weapons. This article uses bibliometric analysis to map trends and gaps in the study of cyber warfare, with data taken from the Scopus index system. The document used is the index list of 565 articles from Scopus. The results of the analysis showed a significant increase in cyber weapon-related publications since 2018, with the United States as the main contributor, followed by countries such as India, the United Kingdom, China, and South Korea. Additionally, the research identified three main clusters: cyber threats to critical infrastructure, cyber defense strategies, and the role of espionage in cyber attacks. The article also highlights the importance of research mapping to develop more effective mitigation strategies against cyber weapon threats and raise global awareness of cyber warfare. Further research is needed to explore the role of artificial intelligence in evolving cyber weapon tactics, as well as to understand the social and economic impacts of cyber attacks.

Keywords*: cyber warfare, cyber weapon, bibliometrics analysis, cyber attack, cyber defense*

1. PENDAHULUAN

Peperangan modern telah mengalami pergeseran signifikan dengan memadukan perang tradisional dan perang siber. *Cyber weapon* telah menjadi elemen krusial dalam konflik kontemporer. Serangan siber semakin efektif sebagai sarana pertempuran modern dan kemungkinan akan menjadi dimensi paling penting dalam konflik bersenjata di masa depan (Piątkowski, 2017). Doktrin militer kini menampilkan *cyber weapon* tidak hanya sebagai alat untuk mempersiapkan medan perang secara strategis, tetapi juga sebagai komponen penting dalam taktik pertempuran (Jaffe, 2023).

Beberapa contoh serangan siber yang signifikan terhadap negara demokrasi modern, seperti Estonia pada 2007, Amerika Serikat pada 2012, dan Ukraina selama konflik 2013-2015, bahwa *cyber warfare* telah menjadi integral dalam peperangan bagi aktor negara dan non-negara (Boyte, 2019). Namun, penggunaan *cyber weapon* juga menimbulkan paradoks teknologi dibalik perkembangannya, yaitu menimbulkan potensi ancaman, etika, hukum, dan operasional (Bardin, 2025).

Meskipun *cyber weapon* telah menjadi bagian integral dari peperangan modern, masih terdapat kesenjangan dalam penelitian dan pemahaman tentang topik ini. Tidak ada definisi universal tunggal tentang *cyber warfare*. Walaupun dikategorikan sebagai peperangan modern dengan teknologi yang memanfaatkan dan mendukung operasi siber (Daultrey, 2017). Selain itu, masih ada

kebutuhan untuk merevisi definisi konflik bersenjata dalam hukum internasional untuk secara memadai mengatasi tantangan yang timbul dari aktivitas siber yang berkembang. Kesadaran dan kesiapan menghadapi tantangan dan ancaman *cyber warfare* juga masih kurang di beberapa negara, seperti yang ditunjukkan dalam studi kasus Lebanon (J. Hejase, 2015).

Undang-undang Nomor 2023 Tahun 2019 tentang pengelolaan sumber daya nasional untuk pertahanan negara bahwa ancaman terbagi menjadi 3, yaitu ancaman militer, ancaman nonmiliter, dan ancaman hibrida. Ancaman yang dimaksud dapat berwujud dalam bentuk serangan siber (Presiden Republik Indonesia, 2019). Oleh karena itu, diperlukan pemetaan penelitian lebih lanjut untuk mengembangkan strategi komprehensif dalam menghadapi ancaman *cyber weapon* dan meningkatkan kesadaran global tentang perang siber. Metode yang digunakan dalam artikel dalam pemetaan menggunakan analisis bibliometrika.

2. METODOLOGI

2.1. Analisis Bibliometrika

Analisis bibliometrika merupakan metode kuantitatif yang digunakan untuk menganalisis dan mengevaluasi literatur ilmiah berdasarkan data bibliografi seperti jumlah publikasi, sitasi, kolaborasi penulis, dan kata kunci (Nurul Syahida Abu Bakar et al., 2024). Metode ini membantu peneliti memahami tren penelitian, mengidentifikasi karya-karya berpengaruh, dan memetakan struktur intelektual suatu bidang keilmuan (Dissanayake, Popescu and Iddagoda, 2023). Analisis bibliometrika juga dapat digunakan untuk mengeksplorasi pola publikasi, jaringan kolaborasi, dan tema-tema penelitian yang sedang berkembang (Ramadhani, Hariyadi and Nastiti, 2022).

Salah satu manfaat utama analisis bibliometrika adalah kemampuannya untuk mengidentifikasi kesenjangan penelitian (research gaps) dan arah penelitian potensial di masa depan (Abdullah et al., 2023). Dengan menganalisis tren publikasi, sitasi, dan kata kunci, peneliti dapat menemukan area yang belum banyak dieksplorasi atau membutuhkan penelitian lebih lanjut (Eri Mardiani et al., 2023). Hal ini membantu peneliti menghindari duplikasi upaya dan memastikan penggunaan sumber daya yang efektif dalam penelitian (Thomas and Gupta, 2022).

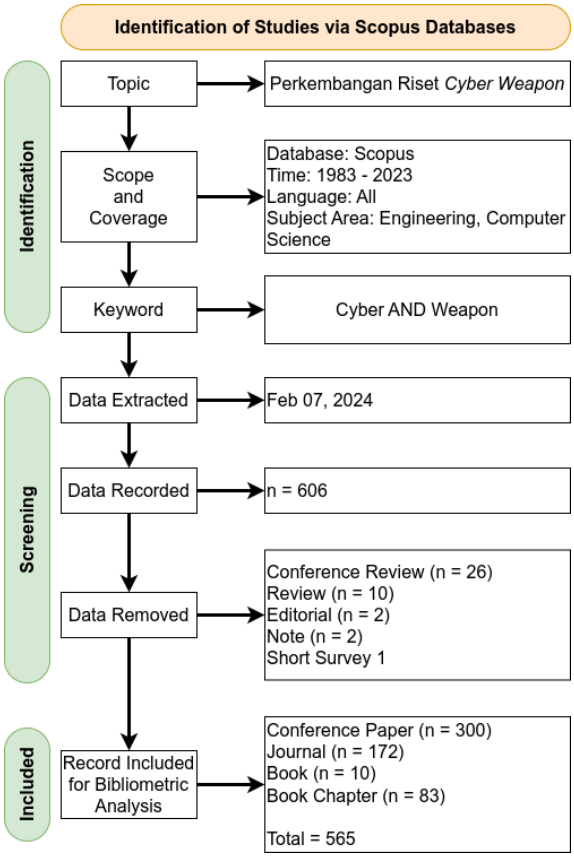
2.2. Sumber Data

Sistem indeks penelitian Scopus memiliki basis data penelitian dan pencatatan sitasi yang besar dengan pencarian yang paling komprehensif. Maka pada artikel ini sumber data yang digunakan adalah sistem indeks Scopus (Wijaya, Setiawan and Shapiai, 2023). Untuk mengetahui lanskap ilmiah dan informasi relevan menggunakan tahapan yang mengadopsi diagram alur PRISMA (Haddaway et al., 2022).

Gambar 1 merupakan strategi dalam pengumpulan data dengan mengadopsi diagram alur PRISMA yang terdiri dari 3 tahapan, *identification*, *screening*, dan *included*. Berdasarkan sistem Indeks Scopus dengan pencarian berdasarkan kata kunci cyber AND weapon terdapat artikel yang terpublikasi dari tahun 1983 - 2024. Maka pada artikel ini rentang waktu pengumpulan data dari tahun 1983 - 2023 dengan ruang lingkup pada bidang *Computer Science* dan *Engineering*. Pembatasan rentang waktu untuk menghindari penambahan data pada rentang waktu berjalan pada tahun tahun 2024.

Artikel yang ditemukan dalam tahapan sebelumnya sebanyak 606 artikel. Tahapan selanjutnya, yaitu *screening* beberapa kategori artikel yang tidak disertakan dalam pengumpulan data. Adapun artikel yang tidak disertakan diantaranya, *Conference Review* sebanyak 26 artikel, *Review* sebanyak 10 artikel, *Editorial* sebanyak 2 artikel, *Note* sebanyak 2 artikel, dan *Short Survey* sebanyak 1 artikel.

Total artikel yang terkumpul sebanyak 565 artikel yang terbagi dalam beberapa kategori. Kategori *Conference Paper* sebanyak 200 artikel, *Journal* sebanyak 172 artikel, *Book* sebanyak 10 buku, dan *Book Chapter* sebanyak 83 artikel.



Gambar 1. Tahapan Pengumpulan Data yang Mengadopsi PRISMA

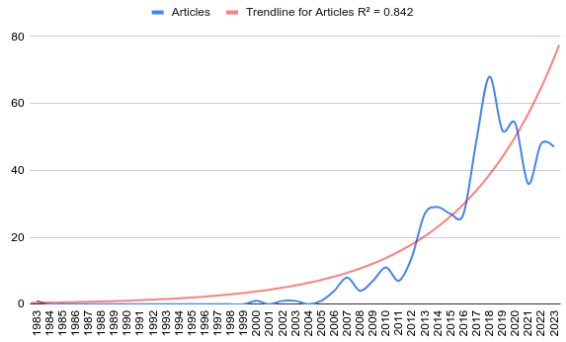
3. HASIL DAN PEMBAHASAN

3.1. Tren Publikasi

Kehadiran internet pada awalnya untuk mendukung sektor militer (Ruttan, 2006). Bertepatan dengan dipublikasikan internet ke publik pemanfaatan teknologi informasi, Laboratorium Penelitian Material di Australia melakukan penelitian tentang material persenjataan dengan memanfaatkan bahasa pemrograman Fortran pada tahun 1983 (Northeast, 1983).

Tren penelitian tentang *cyber weapon* diawali dengan publikasi yang dilakukan oleh Defense *Technical Information Center* Australia pada tahun 1983. Dalam rentang 1983 - 1999 tidak ada publikasi dari penelitian atau implementasi *cyber weapon*. Artikel tahun 2000 muncul menyampaikan potensi pemanfaatan teknologi canggih terutama *cyber weapon* yang digunakan pelaku tindak kejahatan untuk melumpuhkan infrastruktur kritis dan menimbulkan kekacauan (Bunker, 2000).

Penelitian mulai menunjukan peningkatan sangat tajam pada tahun 2018 dengan spektrum yang lebih luas. Artikel tentang cyber weapon yang diterbitkan mencapai 68 artikel, seperti yang ditunjukan pada Gambar 2. Adapun tema penelitian tahun 2018 mencakup perkembangan dan dampak *cyber weapon*, pertahanan dan keamanan siber, strategi analisis potensi ancaman siber, keamanan dan privasi data, etika dan hukum internasional, rekayasa sosial, dan konektivitas antar teknologi.



Gambar 2. Tren Penelitian Per Tahun

3.2. Analisis Negara Kontributor

Amerika Serikat adalah negara yang paling banyak memiliki keterkaitan antar negara dengan 161 dokumen. Selain mendominasi pada jumlah keterkaitan dokumen antar negara, Amerika Serikat juga memiliki sitasi dan *total link strength tertinggi*.

Berdasarkan Tabel 1 negara asia yang masuk dalam 10 besar negara dengan publikasi terbanyak tentang cyber weapon adalah India, Cina, dan Korea Selatan. Negara yang paling dekat dengan Indonesia juga memiliki keminatan tentang *cyber weapon*, yaitu Malaysia dan Australia.

Walaupun Malaysia tidak masuk dalam 10 besar negara yang mempublikasikan tentang *cyber weapon* tetapi melakukan penelitian bersama dengan lembaga di Amerika Serikat atau negara lain. Adapun tema yang disampaikan dalam penelitian tersebut adalah tentang potensi *cyber weapo*n yang memanfaatkan berita bohong dan *cyber bullying* (Rezayi et al., 2018).

Pada tahun sebelumnya, Malaysia juga menyikapi meningkatnya potensi serangan siber dengan melakukan penelitian tentang penyebaran *malware*. Tujuan dari penelitian tersebut melakukan identifikasi dan mendeteksi aktivitas *malware* pada ruang siber. Dengan diketahui pola serangan diharapan dapat diimplementasi pada sistem peringatan dini terhadap potensi serangan siber (Yusof et al., 2016).

Tabel 1. 10 Besar Negara Kontributor

Negara	Dokumen	Sitasi	Total Link Strength
Amerika Serikat	161	1191	20
India	52	436	8
Britania Raya	48	440	10
Cina	23	329	6
Korea Selatan	23	98	2
Australia	17	749	6
Itali	16	247	6
Jerman	13	28	2
Belanda	11	67	5
Estonia	11	95	3

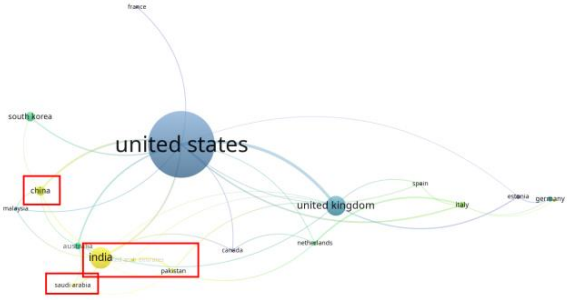
3.3. Pemetaan Negara Kontributor

Keterkaitan dokumen antar negara tentang *cyber weapon* dipetakan dalam sebuah jejaring keterkaitan yang ditunjukan pada T dengan 3 kluster. Masing-masing kluster memiliki kedekatan dalam melakukan penelitian cyber weapon.

Tabel 2. Kluster Negara Penelitian

Kluster	Negara
Biru	Amerika Serikat, Korea Selatan, Malaysia, Cina, Perancis
Hijau	Britania Raya, Swiss, Spanyol, Itali, Jerman, Estonia
Merah	India, Canada, Australia, Belanda, pakistan, Saudi Arabia, UEA

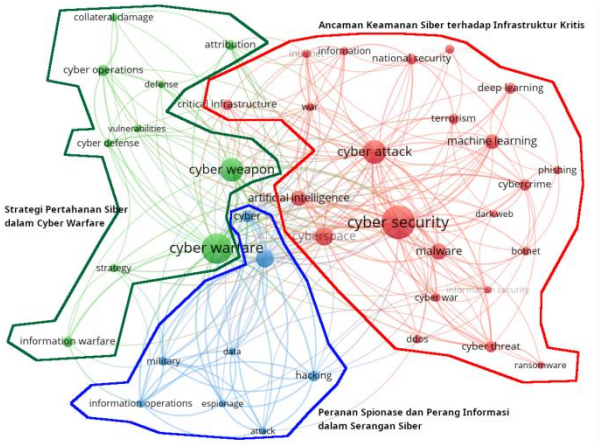
Berdasarkan keterkaitan dokumen antar dokumen melalui visualisasi *overlay* dapat dikategorikan negara yang produktif berdasarkan periode tahun. Warna kuning menunjukan periode terbaru dari negara yang produktif. Gambar 3 menunjukan beberapa negara yang produkti dalam era 2020-an diantaranya, Cina, India, Arab Saudi, UEA, dan Pakistan.



Gambar 3. Negara Kontributor Penelitan *Cyber Weapon*

3.4. Pemetaan *Co-occurance of Keywords*

Analisis *co-occurrence of keywords* merupakan metode yang digunakan untuk mengidentifikasi hubungan dan pola antara kata kunci dalam suatu korpus literatur. Metode ini menggunakan kata kunci sebagai *node* dan kemunculan bersama kata kunci sebagai tautan antar *node* (*vertex*) yang membentuk jejaringan keterkaitan. Analisis ini dapat mengungkapkan struktur pengetahuan, tren penelitian, dan sinergi antar topik dalam suatu bidang (Ozek et al., 2023). Pada artikel ini menggunakan perangkat lunak VOSviewer untuk melakukan analisis *co-occurrence of keywords*i dan memvisualisasikan hasilnya dalam bentuk peta pengetahuan (Du et al., 2024).



Gambar 4. Peta Jejaring Kluster Penelitian

Melalui VOSviewer menghasilkan analisis *co-occurrence of keywords* dalam bentuk visualisasi seperti pada Gambar 4. Berdasarkan analisis tersebut terdapat 3 kluster riset dengan topik ancaman keamanan siber terhadap infrastruktur kritis (kluster merah), strategi pertahanan siber dalam cyber warfare (kluster hijau), dan peranan spionase dan perang informasi dalam serangan siber (kluster biru). Masing-masing kluster yang terbentuk disebabkan oleh kemunculan kata kunci dan keterkaitannya. Tabel 3 menunjukan kemunculan kata kunci pada masing-masing kluster.

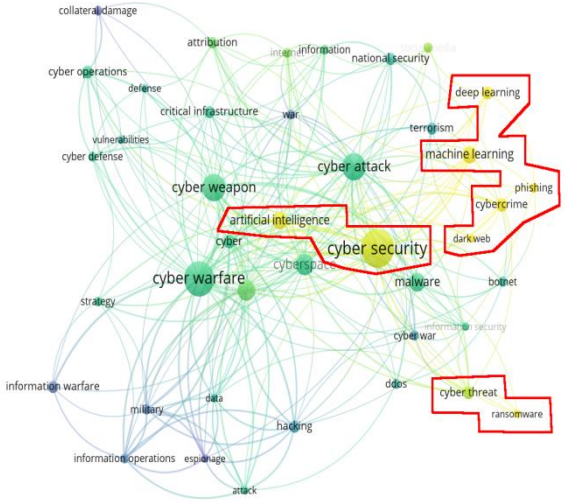
Tabel 3. Kluster Topik Berdasarkan Kata Kunci

Kluster	Kata Kunci
Merah	artificial intelligence, botnet, critical infrastructure, cyber attack, cyber security, cyber threat, cyber war, cybercrime, cyberspace, dark web, ddos, deep learning, information, information security, internet, machine learning, malware, national security, phishing, ransomware, social media, terrorism, dan war
Hijau	attribution, collateral damage, cyber defense, cyber operations, cyber warfare, cyber weapon, defense, information warfare, strategy, dan vulnerabilities
Biru	attack, cyber, data, espionage, hacking, information operations, military, dan security

3.5. Penelitian Lanjutan Cyber Weapon

VOSviewer memiliki fitur untuk memberikan wawasan kemunculan kata kunci dan keterkaitan berdasarkan tren dari masa ke masa, yaitu visualisasi *overlay*. Visualisasi overlay dari VOSviewer masih berkaitan dengan analisis *co-occurrence of keywords* yang dapat menunjukan potensi penelitan yang akan datang. Selain itu peneliti melalui fitur ini dapat memahami evolusi tema penelitian dan tren yang muncul sehingga mempermudah membuat prediksi penelitian yang akan datang (Suryantoro, Udin and Qamari, 2023).

Gambar 4 memvisualisasikan kemunculan kata kunci dan keterkaitan berdasarkan fitur visualisasi *overlay* dari VOSviewer. Terlihat bahwa kata kunci yang dapat digunakan untuk penelitian yang akan datang tentang *cyber weapon* diantaranya: d*eep learning*, *machine learning*, *phishing*, *cyber crime*, *darkweb*, *artificial intelligence*, *cyber security*, *cyber threat*, dan *ransomware*. Artinya di masa yang akan datang *cyber weapon* akan mengalami evolusi baik taktik, teknik, dan prosedur sehingga diperlukan pendekatan dalam penanganan serangan siber yang berbasis *cyber weapon* menggunakan algoritma kecerdasan artificial.



Tabel 4. Visualisasi *Overlay* Penelitian

4. KESIMPULAN DAN SARAN

Peperangan modern yang menggabungkan elemen tradisional dan siber, dengan penekanan pada penggunaan *cyber weapon* sebagai komponen penting dalam konflik saat ini. Melalui analisis bibliometrika, artikel ini memetakan tren dan kesenjangan dalam studi tentang *cyber warfare*, menunjukkan peningkatan signifikan dalam publikasi terkait sejak tahun 2018. Amerika Serikat muncul sebagai kontributor utama dalam penelitian ini, diikuti oleh negara-negara seperti India, Britania Raya, Cina, dan Korea Selatan. Penelitian ini mengidentifikasi tiga kluster utama: ancaman siber

terhadap infrastruktur kritis, strategi pertahanan siber, dan peran spionase dalam serangan siber. Temuan ini menunjukkan bahwa ancaman terhadap infrastruktur kritis menjadi perhatian utama dalam konteks keamanan nasional. Selain itu, strategi pertahanan siber yang efektif perlu dikembangkan untuk menghadapi ancaman yang terus berkembang. Artikel ini juga menyoroti pentingnya pemetaan penelitian untuk meningkatkan kesadaran global tentang perang siber. Dengan meningkatnya ketergantungan pada teknologi, peran kecerdasan buatan dalam taktik senjata siber menjadi semakin relevan.

Penelitian lebih lanjut diperlukan untuk mengeksplorasi strategi mitigasi yang lebih baik dan dampak dari *cyber weapon* terhadap keamanan global. Artikel ini memberikan wawasan penting tentang dinamika baru dalam peperangan modern dan perlunya perhatian lebih terhadap ancaman siber. Selain itu, penting untuk melakukan studi komparatif antara berbagai negara dalam hal kebijakan dan strategi pertahanan siber untuk memahami praktik terbaik. Penelitian tentang dampak sosial dan ekonomi dari serangan siber juga perlu dilakukan untuk memberikan gambaran yang lebih komprehensif tentang risiko yang dihadapi. Terakhir, meningkatkan kesadaran global tentang perang siber dan implikasinya terhadap keamanan nasional harus menjadi fokus utama dalam penelitian mendatang.

DAFTAR PUSTAKA

Abdullah, K.H., Roslan, M.F., Ishak, N.S., Ilias, M. and Dani, R., 2023. Unearthing Hidden Research Opportunities Through Bibliometric Analysis: A Review. Asian Journal of Research in Education and Social Sciences, 5(1), pp.251–262.

Bardin, J.S., 2025. Cyber Warfare. In: Computer and Information Security Handbook. [online] Elsevier. pp.1345–1380. https://doi.org/10.1016/B978-0-443-13223-0.00087-4.

Boyte, K.J., 2019. The Evolution of Cyber Warfare in Information Operations Targeting Estonia, the U.S., and Ukraine. [chapter] https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-8304-2.ch007. https://doi.org/10.4018/978-1-5225-8304-2.ch007.

Bunker, R.J., 2000. Weapons of mass disruption and terrorism. Terrorism and Political Violence, 12(1), pp.37–46. https://doi.org/10.1080/09546550008427548.

Daultrey, S., 2017. Cyber Warfare: A Primer. SSRN Electronic Journal. [online] https://doi.org/10.2139/ssrn.3803732.

Dissanayake, H., Popescu, C. and Iddagoda, A., 2023. A Bibliometric Analysis of Financial Technology: Unveiling the Research Landscape. FinTech, 2(3), pp.527–542. https://doi.org/10.3390/fintech2030030.

Du, Q., Zhao, R., Wan, Q., Li, S., Li, H., Wang, D., Ho, C.W., Dai, Z., Chen, Y. and Shan, D., 2024. Protocol for conducting bibliometric analysis in biomedicine and related research using CiteSpace and VOSviewer software. STAR Protocols, 5(3), p.103269. https://doi.org/10.1016/j.xpro.2024.103269.

Eri Mardiani, Waqiah, Saununu, S.J. and Zani, B.N., 2023. Analyzing the Global Visibility and Influence of Social Enterprise Research: A Bibliometric Review of Citation, International Collaboration, and Cross-Cultural Perspectives. West Science Interdisciplinary Studies, 1(08), pp.576–586. https://doi.org/10.58812/wsis.v1i08.182.

Haddaway, N.R., Page, M.J., Pritchard, C.C. and McGuinness, L.A., 2022. PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. Campbell Systematic Reviews, 18(2), p.e1230. https://doi.org/10.1002/cl2.1230.

J. Hejase, H., 2015. Cyber Warfare Awareness in Lebanon: Exploratory Research. International Journal of Cyber-Security and Digital Forensics, 4(4), pp.482–497. https://doi.org/10.17781/P001892.

Jaffe, J., 2023. Cyber Weapons and the Fifth Domain: Implications of Cyber Conflict on International Relations. In: F. Mazzi, ed. The 2022 Yearbook of the Digital Governance Research Group, Digital Ethics Lab Yearbook. [online] Cham: Springer Nature Switzerland. pp.51–56. https://doi.org/10.1007/978-3-031-28678-0_5.

Northeast, E., 1983. USERSIN - An Interactive User-Interface for FORTRAN SIN. [online] Defense Technical Information Center. Available at: <https://books.google.co.id/books?id=ftTwnAEACAAJ>.

Nurul Syahida Abu Bakar, Wan Fairos Wan Yaacob, Yap Bee Wah, Wan Marhaini Wan Omar, and Utriweni Mukhaiyar, 2024. Visualising Current Research Trends in Class Imbalance using Clustering Approach: A Bibliometrics Analysis. Journal of Advanced Research in Applied Sciences and Engineering Technology, 38(2), pp.95–111. https://doi.org/10.37934/araset.38.2.95111.

Ozek, B., Lu, Z., Pouromran, F., Radhakrishnan, S. and Kamarthi, S., 2023. Analysis of pain research literature through keyword Co-

occurrence networks. PLOS Digital Health, 2(9), p.e0000331. https://doi.org/10.1371/journal.pdig.0000331.

Piątkowski, M., 2017. The Definition of the Armed Conflict in the Conditions of Cyber Warfare. Polish Political Science Yearbook, 1(46), pp.271–280. https://doi.org/10.15804/ppsy2017117.

Presiden Republik Indonesia, 2019. Undang-Undang Republik Indonesia Nomor 23 Tahun 2019 Tentang Pengelolaan Sumber Daya Nasional Untuk Pertahanan Negara.

Ramadhani, E., Hariyadi, D. and Nastiti, F.E., 2022. A Bibliometrics Analysis of Digital Forensics Research in Indonesia Based on Scopus Index: 2012-2021. In: 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA). IEEE. pp.1–6. https://doi.org/10.1109/ICITDA55840.2022.9971449.

Rezayi, S., Balakrishnan, V., Arabnia, S. and Arabnia, H.R., 2018. Fake News and Cyberbullying in the Modern Era. In: 2018 International Conference on Computational Science and Computational Intelligence (CSCI). [online] 2018 International Conference on Computational Science and Computational Intelligence (CSCI). Las Vegas, NV, USA: IEEE. pp.7–12. https://doi.org/10.1109/CSCI46756.2018.00010.

Ruttan, V.W., 2006. Inventing the Internet. In: Is War Necessary for Economic Growth?, 1st ed. [online] Oxford University PressNew York. pp.115–129. https://doi.org/10.1093/0195188047.003.0006.

Suryantoro, E., Udin, U. and Qamari, I.N., 2023. A bibliometric analysis using VOSviewer: Leadership in infection prevention and control. Multidisciplinary Science Journal, 5(2), p.2023022. https://doi.org/10.31893/multiscience.2023022.

Thomas, A. and Gupta, V., 2022. Tacit knowledge in organizations: bibliometrics and a framework-based systematic review of antecedents, outcomes, theories, methods and future directions. Journal of Knowledge Management, 26(4), pp.1014–1041. https://doi.org/10.1108/JKM-01-2021-0026.

Wijaya, A., Setiawan, N.A. and Shapiai, M.I., 2023. Mapping Research Themes and Future Directions in Learning Style Detection Research: A Bibliometric and Content Analysis. Electronic Journal of e-Learning, 21(4), pp.274–285. https://doi.org/10.34190/ejel.21.4.3097.

Yusof, R., Mas'ud, M.Z., Selamat, S.R., Abdollah, M.F., Sahib, S. and Dollah, F.M., 2016. Formulating Generalize Malware Attack Pattern Using Features Selection. 11(5).