Jurnal Peperangan Asimetris
Volume 11, Nomor 2, 2025 E-ISSN 2830-0475

Cyber Warfare in the Perspective of Modern Air Defense Strategy: Bibliometric Mapping and Global Research Directions

Perang Siber dalam Perspektif Strategi Pertahanan Udara Modern: Pemetaan Bibliometrik dan Arah Riset Globa

Argantara Heli Kurniyanto[1], Asep Adang Supriyadi[2], Rudi Sutanto[3]
Defense Strategy Program, Universitas Pertahanan, Indonesia
heli.arga@gmail.com

Abstrak. Cyber warfare has become a critical domain in modern air defense strategies, surpassing traditional kinetic capabilities to include resilience against advanced digital threats. This study conducted a comprehensive bibliometric analysis using Bibliometrix R and VOSviewer to map the global research landscape on cyber warfare from 2005 to 2025. A dataset consisting of 333 publications indexed in Scopus was systematically selected through the PRISMA framework, enabling the identification of publication trends, leading authors, collaboration networks, and thematic clusters. Findings show significant growth in literature after the Stuxnet incident (2010), with research evolving from normative debates on national security toward technical issues such as malware detection, network resilience, and artificial intelligence (AI)-driven defense systems. Keyword co-occurrence and overlay analysis revealed a new focus on IoT, cyber operations, and decision-making processes, highlighting the convergence between technological innovation and strategic policy. Additionally, international law and humanitarian considerations emerged as essential complementary dimensions. The study emphasizes that cyber warfare is inherently multidisciplinary, requiring the integration of technical, strategic, legal, and ethical perspectives. The findings provide valuable insights for policymakers, military strategists, and the academic community, offering a roadmap for strengthening cyber resilience in air defense systems and promoting international cooperation.

Kata Kunci: cyber warfare, modern air defense, bibliometric analysis, VOSviewer, military strategy, military digital literacy

Abstrak. Perang siber telah menjadi domain kritis dalam strategi pertahanan udara modern, melampaui kemampuan kinetik tradisional dengan memasukkan ketahanan terhadap ancaman digital tingkat lanjut. Studi ini melakukan analisis bibliometrik komprehensif menggunakan Bibliometrix R dan VOSviewer untuk memetakan lanskap penelitian global mengenai perang siber pada periode 2005 hingga 2025. Sebanyak 333 publikasi terindeks Scopus dipilih secara sistematis melalui kerangka kerja PRISMA, sehingga memungkinkan identifikasi tren publikasi, penulis terkemuka, jaringan kolaborasi, dan klaster tematik. Temuan menunjukkan pertumbuhan signifikan literatur setelah insiden Stuxnet (2010), dengan evolusi riset dari perdebatan normatif terkait keamanan nasional menuju isu teknis seperti deteksi malware, ketahanan jaringan, dan sistem pertahanan berbasis kecerdasan buatan (AI). Analisis ko-occurence kata kunci dan overlay mengungkap fokus baru pada IoT, operasi siber, dan proses pengambilan keputusan, yang menyoroti konvergensi antara inovasi teknologi dan kebijakan strategis. Selain itu, hukum internasional dan pertimbangan kemanusiaan muncul sebagai dimensi pelengkap yang penting. Studi ini menegaskan bahwa perang siber bersifat multidisipliner, membutuhkan integrasi perspektif teknis, strategis, hukum, dan etika. Temuan ini memberikan wawasan berharga bagi pembuat kebijakan, perencana strategi militer, dan komunitas akademik, menawarkan peta jalan untuk memperkuat ketahanan siber dalam sistem pertahanan udara serta mendorong kerja sama internasional.

Kata Kunci: perang siber, pertahanan udara modern, analisis bibliometrik, VOSviewer, strategi militer, literasi digital militer

1. INTRODUCTION

Transformation of warfare in the 21st century has seen a fundamental shift from conventional conflict to more complex multidomain warfare. Conflicts no longer take place only on land, sea, and air, but have also expanded into cyberspace, outer space, and the information domain (Robinson et al., 2015). One of the most prominent aspects of this shift is the expansion of cyber warfare, which targets not only civilian infrastructure but also military defense systems (Robinson et al., 201 Sharma, 2010). Attacks on radar, command and control (C2), and air defens communication networks have shown that air superiority is now determined not only by kinetic force, but also by the ability to protect digital systems (Sepúlveda

Estay et al., 2020).

Cyber warfare has evolved into a strategic domain in modern defense architecture. Major countries such as the United States, Russia, and China are integrating artificial intelligence (AI), the Internet of Military Things (IoMT), and advanced encryption technologies to strengthen their national air defense systems (Nicholson et al., 2012; Rid, 2012). However, this digitalization creates a paradox: on the one hand, it increases operational effectiveness, but on the other hand, it opens up new vulnerabilities to sophisticated cyber attacks. Advanced persistent threat (APT) attacks targeting automated radar systems or satellite communications have proven that cyber warfare is no longer a complement, but a primary domain in national defense strategy (Jr, 2011; Young et al., 2007).

Cases of cyber penetration of air defense systems have even occurred in countries with high digital capabilities. Incidents of disruption to military communication networks in Russia and intrusion into US air sensor systems reinforce the fact that no country is completely safe from cyber attacks. This vulnerability creates a military-digital paradox: the successful development of air defense technology often creates new vulnerabilities that can be exploited by opponents. Therefore, the concept of cyber resilience is very important in the context of modern defense (Sepúlveda Estay et al., 2020).

Although studies on cyber warfare continue to evolve, most research is still fragmentary. Many studies focus on specific technical aspects such as AI algorithms for radar, military communications encryption, or missile defense systems, without linking them strategically to modern air warfare (Bistron & Piotrowski, 2021). This creates a knowledge gap regarding the direct link between air defense strategy and cybersecurity. The lack of systematic review also hinders the consolidation of knowledge needed for evidence-based policy formulation at the national and international levels.

In the context of defense strategy development, mapping the global research

landscape is crucial. Bibliometric methods offer a way to explore knowledge networks, identify scientific collaborations, and trace thematic dynamics in the field of cyber warfare. Using tools such as Bibliometrix R and VOSviewer, this study was able to reveal publication trends, dominant keywords, citation patterns, and international collaboration clusters (C. Chen, 2017; van Eck & Waltman, 2010). Bibliometric analysis also allows for the identification of knowledge gaps that can be used as a basis for developing new research roadmaps and defense strategies.

This study has three main contributions. First, it conceptually affirms that air defense strategies cannot be separated from digital security governance. Second, methodologically, it presents the integration of Bibliometrix R and VOSviewer to map scientific clusters and main citation paths in cyber warfare research. Third, it strategically provides policy directions for strengthening military digital literacy, integrating air defense with national cyber security, and opportunities for international collaboration (Gartzke & Lindsay, 2015; Stoddart, 2016).

The implications of this research are not only limited to the national context but also contribute to the international discourse on multidomain security. The results of bibliometric mapping can be utilized by organizations such as NATO, the ASEAN Defense Ministers' Meeting (ADMM), and the United Nations Institute for Disarmament Research (UNIDIR) to develop standards, norms, and adaptive defense diplomacy strategies. In the context of ASEAN, Indonesia has a strategic opportunity to become a pioneer in integrating air-cyber defense strategies through regional cooperation based on scientific research (Azad et al., 2023; Konigsburg, 2022).

Thus, this research not only serves as an academic product, but also as a strategic instrument for formulating evidence-based defense policies. The resulting global research cluster map is expected to strengthen national resilience while expanding Indonesia's contribution at the international level.

2. METHOD

2.1. Bibliometric Analysis

Bibliometric analysis is a quantitative method used to evaluate the development of a field of research through scientific publications. This technique allows researchers to map trends, identify the most influential authors, and reveal collaboration networks between countries and institutions. Various studies have emphasized that bibliometric analysis can provide a comprehensive picture of scientific dynamics while identifying research gaps (X. Chen & Zhang, 2023).

In this study, two main analysis tools were used, namely Bibliometrix R (biblioshiny) and VOSviewer. These two tools complement each other: Bibliometrix R excels in descriptive analysis, while VOSviewer has more interactive network visualization capabilities (Mittal et al., 2025). A number of previous studies have also shown that the integration of the two is effective in examining citation characteristics, author productivity, and keyword mapping (Kara et al., 2025; Mittal et al., 2025).

Bibliometrix R, which is operated through the biblioshiny interface, makes it easy to perform publication analysis without the need to write complex programming code. This application is used to: (1) extract metadata from the Scopus and Web of Science databases, (2) calculate annual publication trends, (3) analyze the distribution of journals, countries, and institutions, and (4) identify dominant keywords that describe the focus of the research (X. Chen & Zhang, 2023; Lim et al., 2024).

In addition, Biblioshiny enables the creation of thematic maps that show the relationships between topics. For example, research in the field of dentistry can show the relationship between in vivo/in vitro study designs and high citations (X. Chen & Zhang, 2023). The use of bibliometrics has also been widely adopted to assess journal performance, measure citation impact, and analyze cross-country scientific collaboration (Olufunke & Okuoyo, 2023; Shayegan & Mohammad, 2021).

VOSviewer was developed to visualize bibliometric data in the form of networks. In this study, VOSviewer was used for: (1) co-citation analysis, to identify literature that is often cited together, (2) co-authorship analysis, to see collaboration between authors and institutions, (3) co-occurrence analysis, which displays a map of the relationship between keywords in publications.

This approach has been widely applied, for example in studies on cyber security (O. S. Albahri & A. H. AlAmoodi, 2023; Peng et al., 2025; Radebe & Njenga, 2025), cyber resilience (Annarelli et al., 2020; Sepúlveda Estay et al., 2020), and artificial intelligence technology (O. S. Albahri & A. H. AlAmoodi, 2023). Cluster-based visualization from VOSviewer facilitates the interpretation of global collaboration patterns and the mapping of major research themes (van Eck & Waltman, 2010).

The strength of this methodology lies in the integration of the two. Bibliometrix R provides in-depth descriptive statistical analysis, while VOSviewer provides intuitive visual representations. This integration allows researchers to not only identify the most influential authors or the most cited journals, but also how the relationships between these entities are formed. Previous studies have confirmed that this combination of methods is effective for revealing the structure and dynamics of research in various fields (Kara et al., 2025; Lim et al., 2024).

2.2.Data Sources

The Scopus database was chosen as the primary source because it has extensive publication coverage, high indexing quality, and provides comprehensive citation information for scientific analysis (M. C. Chen et al., 2023). By utilizing data from Scopus, this study attempts to map the current publication landscape using a selection process that follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow as suggested in previous studies (Kumari & Tiwari, 2025; Olufunke & Okuoyo, 2023).

The data collection strategy is visualized through the PRISMA diagram (Figure 1), which consists of three main stages: identification, screening, and inclusion. The

initial search was conducted using the keywords cyber AND warfare, which produced indexed articles from 2005 to 2025.

The initial search found 2,085 articles. In the screening stage, the keywords were refined from cyber AND warfare to "cyber warfare". This change aimed to improve the relevance of the search results, as the use of Boolean operators produced broad but unfocused articles, while searching with the exact phrase "cyber warfare" ensured that only publications that actually discussed the topic of cyber warfare were captured (Gholampour & Kostova, 2025; Olufunke & Okuoyo, 2023).

After keyword-based filtering, several categories of documents that did not meet the research criteria were also excluded, including 193 book chapters, 85 books, 39 reviews, 410 conference papers, 53 conference reviews, 7 editorials, 4 short surveys, 4 notes, and 2 erratum documents. This selection process resulted in 351 articles that met the criteria.

Next, an eligibility test was conducted by removing non-English articles, which included 7 Russian, 4 Portuguese, 2 Spanish, 1 Slovenian, 1 Persian, 1 Norwegian, 1 French, 1 Mandarin, and 1 Arabic publications. After the entire selection process was completed, the number of articles eligible for analysis in this study was 333 publications.

With these systematic steps, a credible and representative dataset was obtained, enabling the bibliometric analysis results to comprehensively describe the development of research related to cyber warfare.

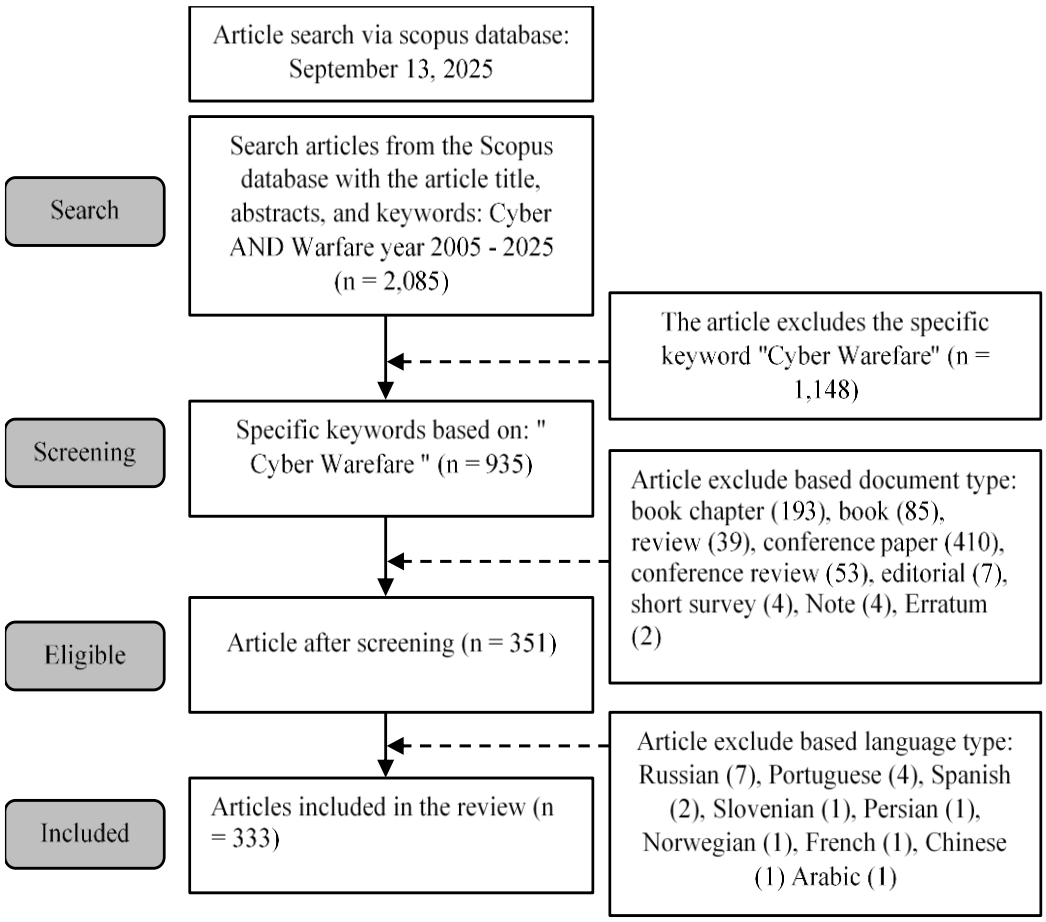

Figure 1. Information Flow using PRISMA

3. RESULT AND DISCUSSION

3.1.Publication Trends

The development of literature on cyberwarfare over the past two decades (2005–2025) shows a consistent growth pattern in line with the increasing intensity and complexity of global cyber threats. Publications on cyber warfare show fluctuating dynamics but tend to increase significantly. In the early period (2005–2009), the number of articles was still limited, ranging from 3 to 7 publications per year. This reflects that during this period, academic discourse was still focused on the basic concepts of network security and critical infrastructure vulnerabilities.

The year 2010 was an important turning point. The number of publications increased sharply from 7 articles (2009) to 19 articles (2010). This surge coincided with the revelation of the Stuxnet attack, which was the first cyber attack proven to cause physical damage to Iran's nuclear infrastructure. This case triggered a wave of academic research on cyber warfare as a new geopolitical instrument (Lindsay, 2013a).

In the 2010–2019 period, publication trends tended to fluctuate, but remained at a higher level than in the previous period. Research topics during this period were dominated by case studies of real attacks such as Stuxnet, Duqu, GhostNet, and Operation Aurora, as well as studies on the security of Supervisory Control and Data Acquisition (SCADA) systems, which are increasingly connected to corporate networks (Stoddart, 2016).

Entering the 2020–2025 period, the number of publications again experienced a significant increase. The focus of research shifted towards issues of system resilience, software protection, and the role of global regulation and governance. Articles discussing innovative technical approaches, such as software watermarking (Iwendi, Jalil, Javed, Thippa Reddy, et al., 2020), as well as normative discourse on artificial intelligence governance (Roberts et al., 2021), increasingly dominated the literature. Overall, the graph shows a peak in academic production in recent years, reflecting the urgency of the topic of cyber warfare in the contemporary cybersecurity landscape.

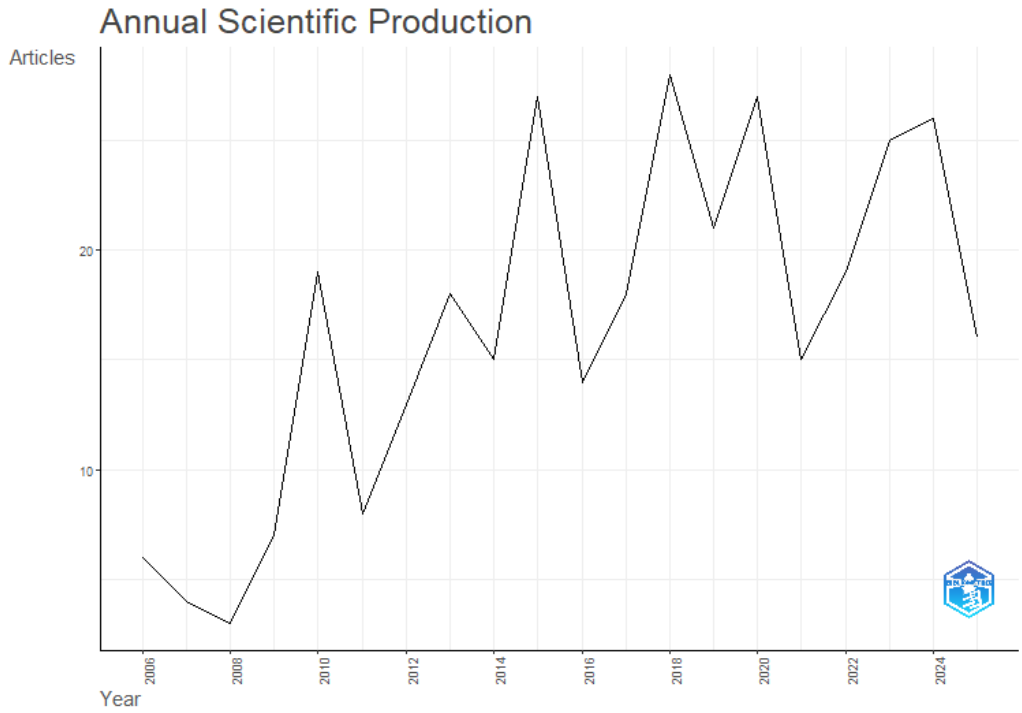

Figure 2. Annual research trend

3.2.Top Ten Author Analysis

In this rapidly evolving digital age, understanding the dynamics of cyber warfare is becoming increasingly important, especially when cyber threats impact not only information technology systems, but also geopolitical stability and global security (Brady, 2019; Krelina, 2021). An important aspect of bibliometrics is the identification of the most relevant authors, which can provide deep insights into how the discourse on cyber warfare has developed through the contributions of academics and practitioners from various disciplines (Linnenluecke et al., 2020).

Shin is listed as the author with the most publications. His research focuses on the security of cyber-physical systems and the design of technical frameworks for attack mitigation (Shin et al., 2018b, 2018a). His works are widely referenced in the development of cybersecurity methodologies integrated with critical infrastructure.

Fulghum ranks next with a concentration on defense policy and national strategy. He outlines (K. Kim et al., 2022) how cyber warfare has changed the geopolitical paradigm and demands the adaptation of modern military doctrine (Fulghum, 2010).

This perspective makes Fulghum an important reference in contemporary international relations analysis.

Janicke contributes through his studies on industrial system vulnerabilities and digital forensics. His research emphasizes intrusion detection and cyber situational awareness, particularly in the context of manufacturing systems and critical infrastructure (Robinson et al., 2019). This contribution is important because it integrates technical and operational aspects within the framework of industrial security.

Goel examines the relationship between risk management and organizational resilience to cyber threats. By emphasizing organizational resilience, it is relevant to the development of network security policies at the corporate and government agency levels (Goel & Hong, 2015).

Harrington reviews international legal aspects of cyber warfare, particularly regarding state responsibility and rules of engagement. He asserts that the absence of global consensus remains an obstacle to efforts to establish an international cyber legal order (Harrington, 2008).

Jang discusses more technical aspects through zero-trust system design and hardware and software security verification. His work in Electronics (Switzerland) demonstrates the importance of applying the zero-trust paradigm in facing increasingly complex modern threats (Jang et al., 2023).

Jones highlights ethical and public policy issues related to cyber conflict. He raises moral debates about the impact of cyber attacks on civilians and the ethical dilemmas in the use of digital technology for military purposes (Robinson et al., 2018).

Khalil examines the role of cyber operations in modern armed conflicts. He asserts that cyber attacks are now an integral part of national defense strategies, requiring updates to international legal and military doctrines (Khalil et al., 2024).

Lee focuses on the integration of artificial intelligence in cybersecurity. His research on privacy protection in the AI transformation environment highlights the

importance of developing adaptive security systems to deal with algorithm-based threats (Lee et al., 2025).

Lindsay contributes to the strategic aspect by reviewing the Stuxnet case as a milestone in cyber warfare. He emphasizes how the attack changed the dynamics of global security while opening a debate about the boundaries between open warfare and covert operations in the digital realm (Lindsay, 2025).

Thus, these ten authors demonstrate a diversity of perspectives: from technical and strategic to legal and ethical. This diversity confirms that the study of cyber warfare is a multidisciplinary field that requires a collaborative, cross-disciplinary approach.

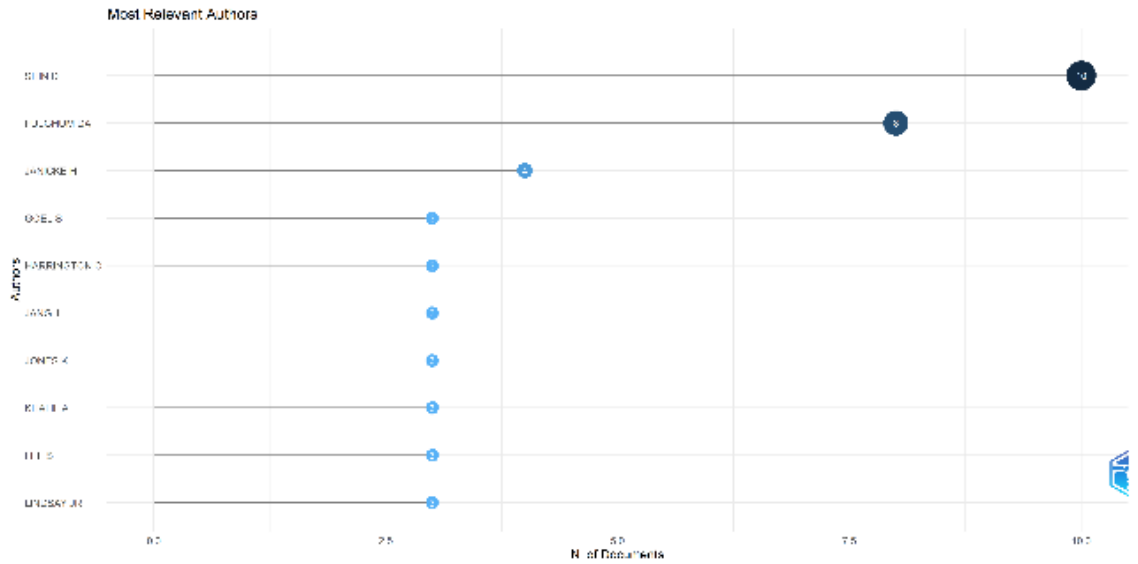

Figure 3. Top Ten Author

3.3.Author Mapping

Mapping author collaborations using VOSviewer provides a comprehensive overview of the network of cooperation between researchers in the field of cyber warfare. The visualization shows several major clusters that have formed, representing co-authorship relationships and the direction of research collaboration. Scientific collaboration analysis often serves as a catalyst in the development of

theories, methodologies, and practical applications in the field of cyber security (Costa et al., 2023).

Table 1. Author Contribution Cluster

Cluster	Author
Green	Shin D, Shin G, Yooun H
Red	Jang J, Kim K, Yoon S, Lee S, Ahn M
Blue	Oh H, Kim S

The mapping shows that Shin D. occupies a central position in the network with extensive connections to various other authors, such as Jang, Kim, Oh, and Yoon. Shin's dominant position confirms his role as a hub author who is not only productive but also plays an important role in bridging the exchange of ideas between research clusters. Shin's research focuses on cyber-physical systems security frameworks that support the strengthening of digital infrastructure resilience (Shin et al., 2018a, 2018b).

Jang and Kim form a close collaboration node, particularly in technical research related to security system design and zero-trust model testing (Jang et al., 2023; S. Kim et al., 2022). This network shows a research development direction that integrates AI-based technology with adaptive security systems, which is also reinforced by Lee et al.'s (2025) research on artificial intelligence-based privacy protection. This interconnection reflects a modern research trend that prioritizes resilient systems in the face of increasingly complex cyber threats.

In addition, another cluster led by Yoon and Ahn shows a concentration on regional-scale research, with close connections between authors (Yoon & Yun, 2020; Jisoo et al., 2024). Cross-institutional collaboration often forms a solid research

ecosystem, especially on multidisciplinary issues such as cyber law, public policy, and industrial security (Robinson et al., 2019; Khalil & Anandha, 2024).

Harrington and Lindsay's positions are not strongly reflected in this technical network, but their contributions in the dimensions of international law and geopolitical strategy confirm that cyber warfare is not only based on technical aspects, but also includes global legal and policy implications (Harrington, 2007; Lindsay, 2013b). Thus, the integration between technical and non-technical clusters is key to developing a more holistic framework for understanding cyber warfare.

Overall, the author's mapping through VOSviewer shows that cyber warfare research has a strong pattern of collaboration among technical researchers, with Shin D. as the main connector. However, multidisciplinary research is still needed so that technical studies can be aligned with legal, ethical, and defense strategy issues. This mapping provides insight that the future of cyber warfare research depends on increasingly close and complementary cross-disciplinary collaboration.

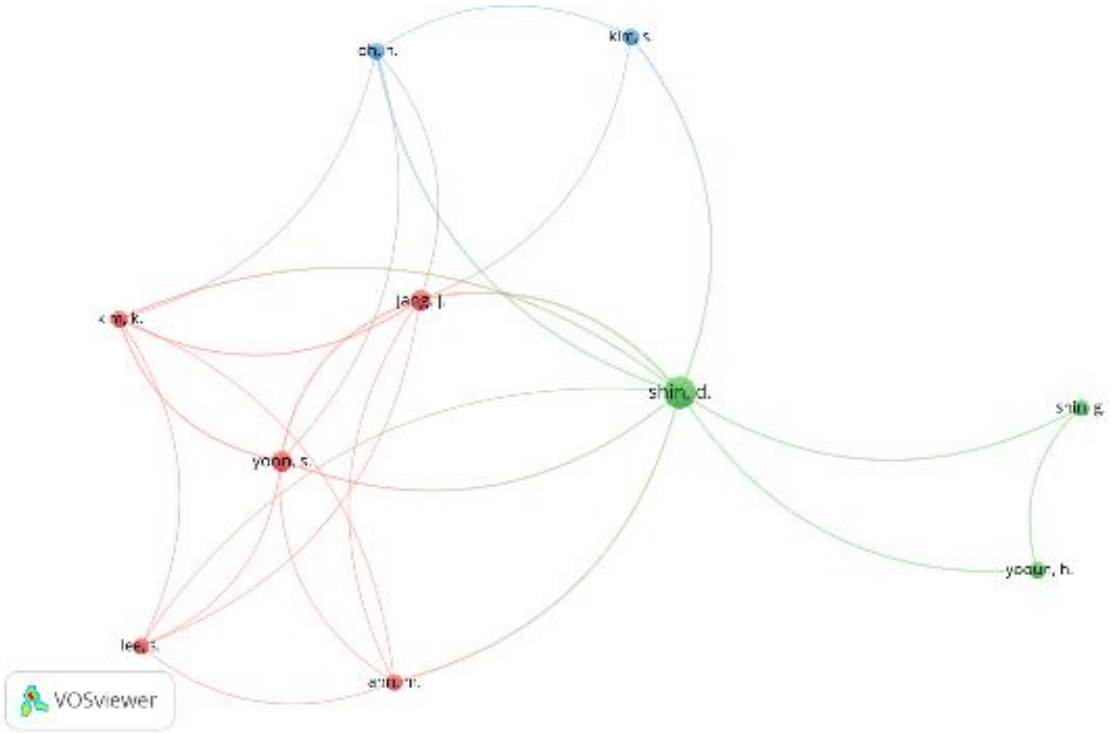

Figure 4. Cyber Warfare Research Author Contributor

3.4.Co-occurance of Keywords Analysis

The co-occurrence of keywords approach is used to examine the relationship between keywords in literature, where each keyword is positioned as a node, while the connection between keywords is represented by connecting lines (links). In this way, a conceptual network can be constructed to reveal the existing knowledge structure, research trend dynamics, and thematic relationships between mutually supportive topics (X. Chen & Zhang, 2023).

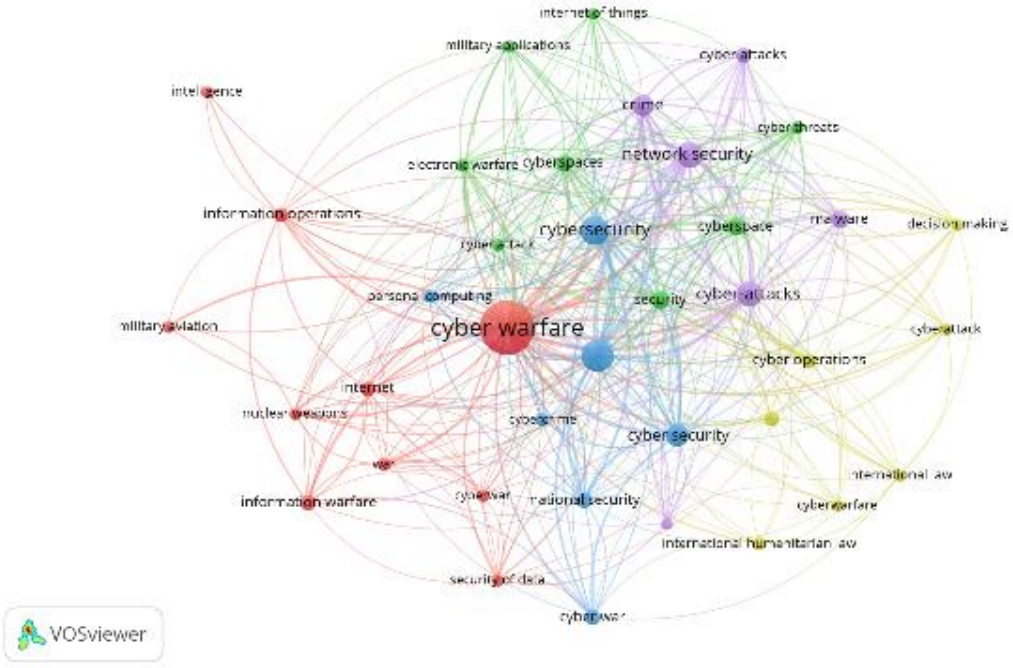

Figure 5. Research Cluster Network Map

The mapping results show five clusters with different colors, each indicating a research focus in the field of cyber warfare.

The red cluster emphasizes strategic issues related to cyber warfare, such as information operations, information warfare, intelligence, and nuclear weapons. This connection confirms that cyber warfare is often positioned alongside conventional and nuclear military instruments and is part of modern defense strategies (Shin et al.,

2018b, 2018a). Furthermore, this discourse shows that cyber warfare is seen as a geopolitical instrument with implications for global stability (Roberts et al., 2021).

The blue cluster focuses on the dimensions of cyber security related to national security, data security, and cybercrime. This theme reflects the integration of cyber security in the protection of critical national infrastructure and public policy governance. Research in this cluster emphasizes the importance of digital risk mitigation as part of the national security agenda (Nicholson et al., 2012; Lindsay, 2013a).

The green cluster highlights aspects of technology and its applications, particularly those related to the internet of things (IoT), electronic warfare, and military applications. This issue shows how technological developments are expanding the scope of cyber warfare, particularly in the context of the use of digital systems in the military domain (Xu et al., 2012; Iwendi, Jalil, Javed, Gadekallu, et al., 2020).

The purple cluster focuses on technical vulnerabilities, such as network security, malware, cyber threats, and crime. This theme reflects the technical dimensions of cyber warfare related to detection, prevention, and response to cyber attacks. Research in this cluster strengthens the understanding of digital threats and network protection mechanisms (Sood & Enbody, 2013; Akhtar & Feng, 2022).

The yellow cluster describes normative issues related to international law, international humanitarian law, and decision making in the context of cyber operations. This focus emphasizes the importance of international legal governance to regulate conflicts in cyberspace and provide a framework of legitimacy for the use of digital instruments for military purposes (Robinson et al., 2015; Sharma, 2010).

3.5.Future Research on Cyber Warfare

The results of overlay visualization with VOSviewer show the temporal dynamics in research on cyber warfare. The colors on the map indicate the development of

research focus from year to year, where dark blue represents the early period (around 2016–2017), while green to yellow marks more recent research (2019–2022).

In the early phase, research centered on fundamental concepts such as information warfare, national security, and intelligence. These topics emphasized the equivalence of cyber warfare with traditional military instruments and its role in national defense strategy (Lindsay, 2013a; Roberts et al., 2021). Research at this stage tended to be normative and conceptual, focusing on security frameworks and geopolitical threats.

As digital technology developed, research shifted towards more specific technical issues, such as network security, malware, and cybercrime. This period was marked by efforts to strengthen network defenses through the development of attack detection and mitigation methods (Sood & Enbody, 2013; Nicholson et al., 2012). This study contributes to a deeper understanding of the technical aspects of cyber attacks and the protective measures that can be implemented.

Current research trends (marked in green-yellow) show the emergence of new themes, particularly related to the internet of things (IoT), cyber operations, and decision making. These topics indicate that future cyber warfare research will increasingly focus on the integration of smart technologies, cyber operations automation, and decision making based on big data and artificial intelligence (Iwendi, Jalil, Javed, Gadekallu, et al., 2020; Xu et al., 2012). This development marks a shift from merely technical security issues to the use of adaptive systems capable of predicting and responding to threats in real time.

In addition, international law and humanitarian law aspects have also shown an increase in recent research, along with the increasing urgency of global regulations to anticipate the escalation of digital conflicts (Robinson et al., 2015; Sharma, 2010). This indicates that future research will not only focus on technical dimensions, but also on the development of international legal and policy frameworks that can serve as a basis for legitimizing actions in the cyber realm.

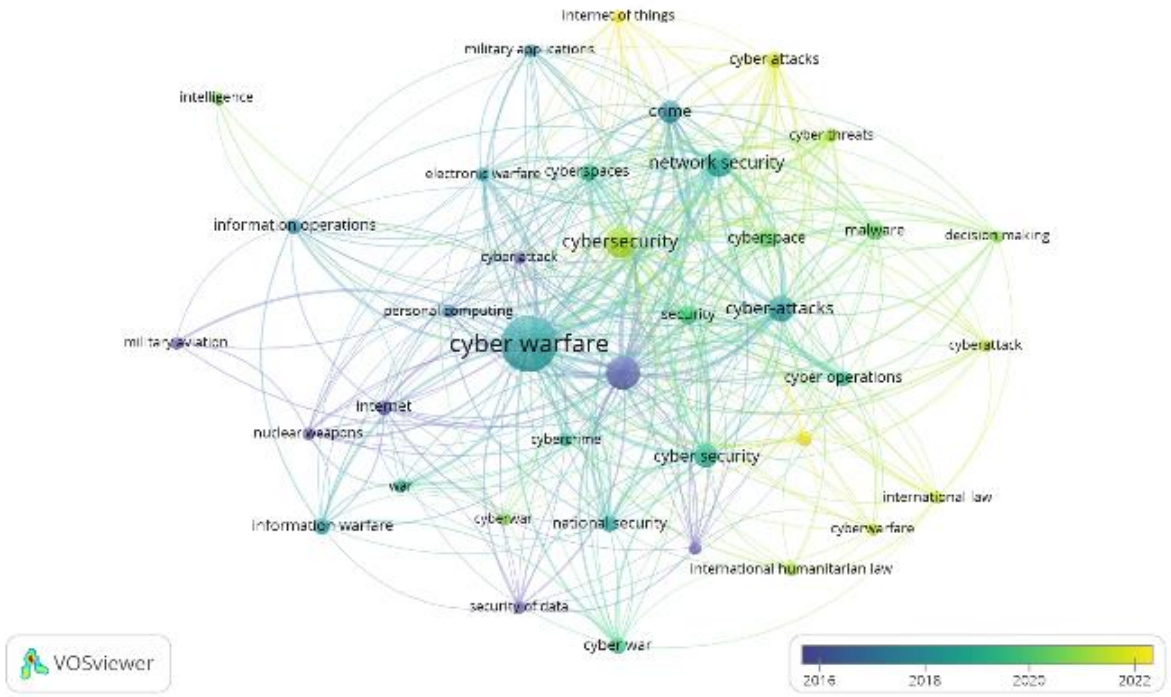

Figure 6. Research Overlay Visualization

4. CONCLUSION

Based on the results of bibliometric analysis of 333 publications related to cyber warfare from 2005 to 2025, it can be concluded that:

1. Research growth has shown a significant upward trend since 2010, triggered by the Stuxnet incident, which opened up a new paradigm of cyber warfare as a geopolitical and military instrument.
2. Mapping of authors and collaborations reveals the dominance of technical researchers such as Shin and Jang, who focus on cyber-physical systems and zero-trust security, as well as strategic researchers such as Lindsay and Harrington, who examine legal and geopolitical aspects.
3. Keyword analysis reveals five main clusters: (a) defense strategy and information operations, (b) national security and cybercrime, (c) military technology such as IoT and electronic warfare, (d) technical issues such as malware and network

security, and (e) aspects of international law and humanitarian law.

4. Future research directions are moving towards issues of smart technology integration, cyber operations automation, and global governance that emphasizes international legal legitimacy.

Thus, this study confirms that cyber warfare is a multidisciplinary domain that requires synergy between technological innovation, air defense strategies, legal governance, and military digital literacy. The results of this mapping can be used as a basis for developing evidence-based defense policies, while strengthening Indonesia's contribution to the multidomain security discourse at the international level.

REFERENCE

Akhtar, M. S., & Feng, T. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. Symmetry, 14(11). https://doi.org/10.3390/sym14112304

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. Computers and Industrial Engineering, 149(January), 106829. https://doi.org/10.1016/j.cie.2020.106829

Azad, T. M., Haider, M. W., & Sadiq, M. (2023). Understanding Gray Zone Warfare From Multiple Perspectives. World Affairs, 186(1), 81–104. https://doi.org/10.1177/00438200221141101

Bistron, M., & Piotrowski, Z. (2021). Artificial intelligence applications in military systems and their influence on sense of security of citizens. Electronics (Switzerland), 10(7). https://doi.org/10.3390/electronics10070871

Brady, H. E. (2019). The challenge of big data and data science. Annual Review of Political Science, 22, 297–323. https://doi.org/10.1146/annurev-polisci-090216-023229

Chen, C. (2017). Science Mapping: A Systematic Review of the Literature. Journal of Data and Information Science, 2(2), 1–40. https://doi.org/10.1515/jdis-2017-0006

Chen, M. C., Chen, S. H., Cheng, C. D., Chung, C. H., Mau, L. P., Sung, C. E., Weng, P. W., Cathy Tsai, Y. W., Shieh, Y. S., Huang, R. Y., & Cheng, W. C. (2023). Mapping out the bibliometric characteristics of classic articles published in a Taiwanese academic journal in dentistry: A scopus-based analysis. Journal of Dental Sciences, 18(4), 1493–1509. https://doi.org/10.1016/j.jds.2023.03.015

Chen, X., & Zhang, G. (2023). Mapping the Research on University-Industry Collaborative Innovation of Individuals: A Scientometric Analysis. IEEE Access, 11(August), 86318–86334. https://doi.org/10.1109/ACCESS.2023.3304902

Costa, A. P., Moresi, E. D., Pinho, I., & Halaweh, M. (2023). Integrating Bibliometrics and Qualitative Content Analysis for Conducting a Literature Review. 2023 24th International Arab Conference on Information Technology, ACIT 2023. https://doi.org/10.1109/ACIT58888.2023.10453680

Fulghum, D. A. (2010). U.S. completes cyber-attack and defense framework. Aviation Week and Space Technology, 172(19). https://www.scopus.com/inward/record.uri?eid=2-s2.0-77952939357&partnerID=40&md5=285627321bded27ea046a5409e08d187

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies, 24(2), 316–348. https://doi.org/10.1080/09636412.2015.1038188

Gholampour, S., & Kostova, I. (2025). Citation begets citation : overview of highly cited papers of pathological biomineralization with emphasis on research trends , main actors , reasons. https://doi.org/10.1108/GKMC-08-2024-0518

Goel, S., & Hong, Y. (2015). Cyberwar games: Strategic jostling among traditional adversaries. Advances in Information Security, 56, 1–13. https://doi.org/10.1007/978-3-319-14039-1_1

Harrington, C. (2007). USAF explores development of cyberspace warfare doctrine. Jane's Defence Weekly, DEC. https://www.scopus.com/inward/record.uri?eid=2-s2.0-38149002097&partnerID=40&md5=8b8eb8358b3bea690acb3d421dcd25a6

Harrington, C. (2008). USAF doctrine pushes cyber warfare as kinetic alternative. Jane's Defence Weekly, APR. https://www.scopus.com/inward/record.uri?eid=2-s2.0-43449096917&partnerID=40&md5=0446e074d27a26a5c9ae166eb3fa0adf

Iwendi, C., Jalil, Z., Javed, A. R., Gadekallu, G., Kaluri, R., Srivastava, G., & Jo, O. (2020). KeySplitWatermark: Zero Watermarking Algorithm for Software Protection against Cyber-Attacks. IEEE Access, 8, 72650–72660. https://doi.org/10.1109/ACCESS.2020.2988160

Iwendi, C., Jalil, Z., Javed, A. R., Thippa Reddy, G., Kaluri, R., Srivastava, G., & Jo, O. (2020). KeySplitWatermark: Zero Watermarking Algorithm for Software Protection against Cyber-Attacks. IEEE Access, 8, 72650–72660. https://doi.org/10.1109/ACCESS.2020.2988160

Jang, J., Kim, K., Yoon, S., Lee, S., Ahn, M., & Shin, D. (2023). Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated With Cyber Asset Damage. IEEE Access, 11, 45113–45128. https://doi.org/10.1109/ACCESS.2023.3273612

Jisoo, J., Jung, S., Ahn, M., Kim, D., Youn, J., & Shin, D. (2024). Research on Quantitative Prioritization Techniques for Selecting Optimal Security Measures. IEEE Access, 12, 103848–103859. https://doi.org/10.1109/ACCESS.2024.3433404

Jr, J. S. N. (2011). Nuclear Lessons for Cyber Security ? Strategic Studies Quarterly, 5(4), 18–38.

Kara, B. C., Şahin, A., & Dirsehan, T. (2025). BibexPy: Harmonizing the bibliometric symphony of Scopus and Web of Science. SoftwareX, 30(December 2024). https://doi.org/10.1016/j.softx.2025.102098

Khalil, A., & Anandha Krishna Raj, S. (2024). Challenges to the Principle of Distinction…in Cyber Warfare: Navigating International Humanitarian Law Compliance. Prawo i Wiez, 49(2), 109–131. https://doi.org/10.36128/PRIW.VI49.769

Khalil, A., Bitar, M., & Anandha Krishna Raj, S. (2024). A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War. TalTech Journal of European Studies, 14(2), 49–72. https://doi.org/10.2478/bjes-2024-0016

Kim, K., Yoon, S., Lee, D., Jang, J., Oh, H., & Shin, D. (2022). Study on Prioritization of Actions by Classifying and Quantifying Cyber Operational Elements Using 5W1H Method. IEEE Access, 10, 74765–74778. https://doi.org/10.1109/ACCESS.2022.3190530

Kim, S., Jang, J., Kwon, O.-J., Kim, J.-Y., & Shin, D. (2022). Study on Cyber Attack Damage Assessment Framework. IEEE Access, 10, 59270–59276. https://doi.org/10.1109/ACCESS.2022.3179977

Konigsburg, J. A. (2022). Modern Warfare, Spiritual Health, and the Role of Artificial Intelligence.

Krelina, M. (2021). Quantum technology for military applications. EPJ Quantum Technology, 8(1). https://doi.org/10.1140/epjqt/s40507-021-00113-y

Kumari, A., & Tiwari, M. (2025). Evolution of research on resource dependency theory: a bibliometric exploration of its correlation with the firm's performance. Kybernetes, September. https://doi.org/10.1108/K-12-2024-3239

Lee, S., Huh, J.-H., & Woo, H. (2025). Security System Design and Verification for Zero Trust Architecture. Electronics (Switzerland), 14(4). https://doi.org/10.3390/electronics14040643

Lim, W. M., Kumar, S., & Donthu, N. (2024). How to combine and clean bibliometric data and use bibliometric tools synergistically: Guidelines using metaverse research. Journal of Business Research, 182(May), 114760. https://doi.org/10.1016/j.jbusres.2024.114760

Lindsay, J. R. (2013a). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lindsay, J. R. (2013b). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lindsay, J. R. (2025). Stuxnet revisited: From cyber warfare to secret statecraft. Journal of Strategic Studies. https://doi.org/10.1080/01402390.2025.2481447

Linnenluecke, M. K., Marrone, M., & Singh, A. K. (2020). Conducting systematic literature reviews and bibliometric analyses. Australian Journal of Management, 45(2), 175–194. https://doi.org/10.1177/0312896219877678

Mittal, P., Yadav, S., Dadhich, A., Kalra, S., & Ajmera, P. (2025). Academic performance and sleep: a visualization and mapping of research trends. Health Education, September, 1–15. https://doi.org/10.1108/he-02-2025-0023

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. Computers and Security, 31(4), 418–436. https://doi.org/10.1016/j.cose.2012.02.009

O. S. Albahri, & A. H. AlAmoodi. (2023). Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. Mesopotamian Journal of CyberSecurity, 2023, 158–169. https://doi.org/10.58496/mjcsc/2023/018

Olufunke, O., & Okuoyo, O. (2023). A Bibliometric Analysis and Science Mapping of Recommendation Systems Research from 1987 to 2022. 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals, SEB-SDG 2023, 1, 1–11. https://doi.org/10.1109/SEB-SDG57117.2023.10124525

Peng, P., Xie, X., Claramunt, C., Lu, F., Gong, F., & Yan, R. (2025). Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. Transportation Research Part E: Logistics and Transportation Review, 195(December 2024), 1–22. https://doi.org/10.1016/j.tre.2025.103971

Radebe, F. M., & Njenga, K. (2025). Bibliometric Mapping of Scientific Production and Conceptual Structure of Cyber Sextortion in Cybersecurity. Social Sciences, 14(1). https://doi.org/10.3390/socsci14010012

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. AI and Society, 36(1), 59–77. https://doi.org/10.1007/s00146-020-00992-2

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers and Security, 49(November 2017), 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An introduction to cyber peacekeeping. Journal of Network and Computer Applications, 114, 70–87. https://doi.org/10.1016/j.jnca.2018.04.010

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2019). Developing cyber peacekeeping: Observation, monitoring and reporting. Government Information Quarterly, 36(2), 276–293. https://doi.org/10.1016/j.giq.2018.12.001

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. Computers and Security, 97. https://doi.org/10.1016/j.cose.2020.101996

Sharma, A. (2010). Cyber Wars: A Paradigm Shift from Means to Ends. Strategic Analysis, 34(1), 62–73. https://doi.org/10.1080/09700160903354450

Shayegan, M. J., & Mohammad, M. M. (2021). Bibliometric of Semantic Enrichment. 2021 7th International Conference on Web Research, ICWR 2021, 202–205. https://doi.org/10.1109/ICWR51868.2021.9443147

Shin, G., Yooun, H., Shin, D., & Shin, D. (2018a). Hybrid feature selection method based on a naïve bayes algorithm that enhances the learning speed while

maintaining a similar error rate in cyber ISR. KSII Transactions on Internet and Information Systems, 12(12), 5685–5700. https://doi.org/10.3837/tiis.2018.12.005

Shin, G., Yooun, H., Shin, D., & Shin, D. K. (2018b). Incremental learning method for cyber intelligence, surveillance, and reconnaissance in closed military network using converged IT techniques. Soft Computing, 22(20), 6835–6844. https://doi.org/10.1007/s00500-018-3433-1

Sood, A. K., & Enbody, R. J. (2013). Targeted cyberattacks: A superset of advanced persistent threats. IEEE Security and Privacy, 11(1), 54–61. https://doi.org/10.1109/MSP.2012.90

Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. International Affairs, 92(5), 1079–1105. https://doi.org/10.1111/1468-2346.12706

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Xu, S., Lu, W., & Zhan, Z. (2012). A stochastic model of multivirus dynamics. IEEE Transactions on Dependable and Secure Computing, 9(1), 30–45. https://doi.org/10.1109/TDSC.2011.33

Yoon, S., & Yun, J. (2020). From confrontation to conflict between China and Taiwan: Major challenges for Taiwan's counter strategy. Korean Journal of Defense Analysis, 32(3), 351–370. https://doi.org/10.22831/kjda.2020.32.3.002

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. Information Systems Management, 24(4), 281–287. https://doi.org/10.1080/10580530701585823