Bibliometric Analysis of Cyber Warfare Research in Africa: Landscape and Trends

Jabu Mtsweni[1,2] and Mphahlela Thaba[1]
[1]Council for Scientific and Industrial Research, Pretoria, South Africa
[2]Stellenbosch University, Security Institute for Governance and Leadership in Africa, Faculty of Military Science, Saldanha, South Africa

mtswenij@gmail.com
jthaba@csir.co.za

Abstract: As the digital landscape continues to evolve, cyber warfare has emerged as a prominent domain of warfare, with superpower nations actively demonstrating their capabilities in the cyberspace. This study posits that African countries exhibit a relative lag in research and development of cyber warfare capabilities, as evidenced by the absence of African nations in the National Cyber Power Index released by the Belfer Centre for Science and International Affairs in 2022. To address this knowledge gap, this paper presents a comprehensive bibliometric analysis of cyber warfare research and development within the African continent. The analysis aims to illuminate research productivity, performance, science mapping, and key contributors at both national and institutional levels. It seeks to uncover thematic trends, pinpoint key research areas, and identify research connections within the African context. This research evaluates the African continent's research participation and development in the cyber and/or information warfare domain over the past 23 years. The analysis encompasses scholarly articles and conference proceedings published between 2000 and 2023, utilizing Scopus as the primary data source. Preliminary findings suggest that cyber warfare research in Africa is concentrated in a limited number of countries, with South Africa emerging as the leading contributor. A comparative analysis further reveals that developed countries generally outpace African nations in cyber warfare research and development, corroborating the rankings presented in the National Cyber Power Index (NCPI) and Global Cybersecurity Index (GCI).

Keywords: Cyber security, Cyber warfare, Cyber operations, Cyber defence, Cyber attacks, Information warfare

1. Introduction

African nations face significant challenges in establishing and operationalizing cyber warfare capabilities (Thaba & Mtsweni, 2023). The Global Cybersecurity Index (GCI), a benchmark assessment of countries' cybersecurity commitments conducted by the International Telecommunications Union (ITU), highlights the relative underdevelopment of cybersecurity in many African countries (ITU, 2021). This underdevelopment manifests in several areas, including: (1) inadequate legal frameworks to support cybersecurity efforts; (2) insufficient technical measures to safeguard against cyberattacks and threats; (3) underdeveloped organizational structures for managing cyber risks and responding to incidents; (4) limited capacity building initiatives to cultivate a skilled cybersecurity workforce; and (5) weak international cooperation mechanisms for sharing cyber threat intelligence and conducting joint cybersecurity exercises.

In contrast, the National Cyber Power Index (NCPI), which focuses on the offensive aspects of cybersecurity and includes at least 30 countries, features only one African country (i.e., Egypt) (Voo, et al., 2022). This disparity reflects the dearth of research and development in cyber warfare capabilities within Africa, compared to countries like the United States, China, and Russia where cyber warfare capabilities are advanced and operationalized.

This research employs a bibliometric analysis technique to advance the comprehension of cyber warfare research in Africa, offering a valuable resource for scholars and policymakers alike. Through a comprehensive assessment of research productivity, performance, and regional dynamics, this study lays the groundwork for fostering collaboration, innovation, and knowledge dissemination within Africa's evolving cyber warfare landscape.

The rest of this paper is structured as follows: Section 2 provides context and overview on the definitions of terms used in this paper as well as the literature review. In Section 3, the research methodology adopted is presented with the bibliometrics analysis process explained, including data collection profiles. Section 4 presents the results of the bibliometric analysis using VOSviewer and Bibliometrix tool. In Section 5, a high-level comparative analysis is presented to put the bibliometric analysis of African countries on cyber warfare research

in perspective. Section 6, discusses the research results, limitations, and implications. The paper is concluded with a summary and future research recommendations in Section 7.

2. Cyber Warfare: Literature Review

As explained by Thaba and Mtsweni (2023), the cybersecurity domain is quite broad and encompasses various interpretations and definitions depending on the context. Therefore, providing a clear definition and context for cyber warfare is crucial.

2.1 Definitions and Context

In this paper, we define *cyber warfare* as the defensive and offensive capabilities of a nation-state to influence, protect, manipulate, or exploit cyberspace for strategic national objectives. Moreover, the terminologies used in cyber warfare research vary across studies (Lukin, 2019; Colarik, 2017). For instance, cyber warfare is sometimes spelled as cyberwar (one word), which can impact bibliometric analysis. Additionally, in some countries, the term "cyber defense" is written with a hyphen ("cyber-defense"), while in others, it is written without a hyphen ("cyber defense"), and in other cases with the UK spelling (“cyber defence”). These variations are quite common in the cybersecurity terminologies. In this research, we attempted to consider these different variations in our data collection. Nevertheless, we accept that it will remain challenging to catch-all the different variations within the search queries.

2.2 Cyber Warfare Research in the 21st Century

The development of cyber warfare capabilities by nation states is evident even though African nations seem to be lagging. The modern conflicts observed in Europe, Asia, Africa, and other continents are showing that kinetic warfighting is increasingly supported by cyber operations at different levels. The Russia-Ukraine war is a typical example where different cyber dimensions have been demonstrated (Willet, 2023). The conflict between Israel and Palestine has seen cyber-attacks escalate between nations, including a shutdown of Iran’s gas stations by the Israeli hacker group (The Times of Israel, 2023). In Europe, the North Atlantic Treaty Organization (NATO) agreed in 2016 to recognize cyber warfare as an operational domain (Binnendijk, et al., 2019), and this is a clear demonstration that cyber warfare will continue to play a role in modern-conflicts and African countries should not be found wanting.

It is also evident that some countries, through foreign nation-state actors are already using cyber-weapons as means to entrench their economic influence and/or governments’ manipulation in Africa. Several incidents have been observed in Mozambique (Thaba & Mtsweni, 2023), Kenya (Fielder, 2021), Nigeria, Ethiopia, South Africa, Sudan, and Ghana in the recent past (Amoah, 2019; Mtsweni & Thaba, 2021).

Over and above the common cyber defence capabilities, developed nations have been building offensive capabilities (Voo, et al., 2022) arranged through national structures such as Cyber Command. These capabilities include: (1) Cyber surveillance and monitoring, (2) Cyber foreign intelligence gathering, (3) Information control and manipulation, (4) systems destruction and hacking, and (5) cyber competence development, amongst others.

2.3 Related Work

Bibliometric analysis (Donthu, et al., 2021) studies have been exponentially increasing across all research disciplines since 2019, with close to 50,000 research results on Google Scholar between 2019-2023 (4 years), compared to approximately 41,100 between 2010-2018 (8 years). This suggests that bibliometric analysis studies have taken off because of their nature of providing insights and trends. Google trends between 201-2023 also confirms this exponential growth (see Figure 1).

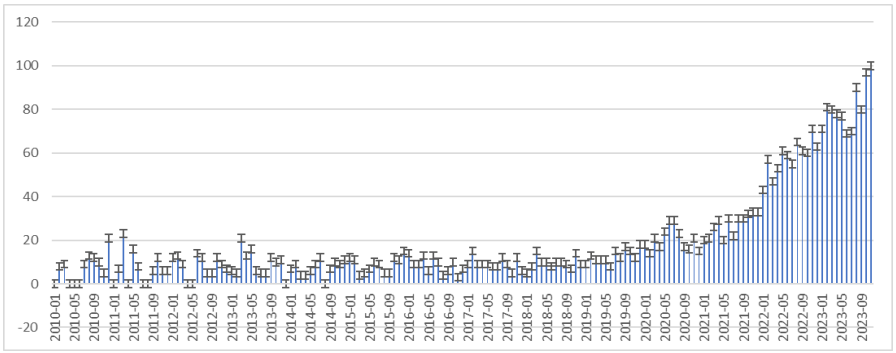

Figure 1: Google Trends on bibliometric analysis (2010-2023) (x: interest in % and y-years)

In the realm of cybersecurity, there is a growing trend in employing bibliometric analysis in research studies. Rahim (2021) utilized this technique to investigate the trends in literature regarding cyber threats and cyber-attacks within the Higher Education context from 2004 to 2019 on a global scale. The study encompassed a comprehensive analysis of scientific performance in this domain, revealing that South Africa ranked at #14, while other African nations, such as Nigeria and Morocco, find themselves towards the bottom of the top 100 in relation to cyber threats and attacks research publications.

Nobanee, et al., (2023) conducted a bibliometric analysis on literature related to cybercrime and cybersecurity risks, evaluating global research developments. This comprehensive study analysed 749 articles spanning from 1999 to 2021, utilizing the Scopus database and VOSviewer platform. The findings of the study showed a growing trend on cybersecurity risks even though some research gaps still exist in the field.

Kyrdoda, et al., (2023) delved into cybersecurity technology research from 2011 to 2021 using bibliometric analysis, discovering a notable surge in interest with over 1,100 papers published in the past decade. Interestingly, the analysis demonstrated the absence of African authors in the top contributors to cybersecurity research, with no African country ranking in the top 15 publications, each boasting a citation count of over 42 per document. The United States and China emerged as leaders in cyber technology research during the specified timeframe.

Tse, et al., (2015) employed the bibliometric analysis technique to explore trends and patterns in privacy and ethics within the IEEE Security and Privacy journal, focusing on the period from 2003 to 2014. While shedding light on certain aspects of cyber warfare, the study did not unveil any insights related to the African continent.

Through the literature review, it is apparent that no bibliometric analysis has been conducted on cyber warfare research specifically in Africa, nor on general cybersecurity trends. Thus, the current research study is deemed relevant and timely, aiming to fill this gap by providing valuable insights into the research and development trends within African countries.

3. Research Methodology

In this paper, we employed a bibliometric analysis technique to study cyber warfare research, developments, and capabilities in Africa spanning the past 23 years (2000-2023). The choice of bibliometric analysis as the research methodology stems from its widespread use in business, academia, and various domains to understand trends over time.

Bibliometric analysis is defined as a quantitative method for gauging the research impact and productivity of scholars and institutions (Donthu, et al., 2021). It entails analysing citations in scholarly publications to establish connections to other works or researchers and is widely applied in fields such as library and information science and research evaluation (van Eck & Waltman, 2010; Aria & Cuccurullo, 2017).

The benefits of bibliometric analysis are manifold. Its quantitative nature allows for objective measurements, and its transparency, utilizing publicly available data, facilitates easy replication of results within the same domain and period. Furthermore, its scalability enables the analysis of numerous publications over an extended period (Donthu, et al., 2021).

However, it is crucial to note the limitations of bibliometric analysis, particularly in cases where research data or information about a topic is not published in scientific publications or publications are not indexed by databases

such as Scopus or Web of Science. Consequently, this study was restricted to the research and development of published cyber warfare research data indexed by Scopus.

To complement the bibliometric analysis, we enhanced the research findings through a comparative analysis (Blair-Walcott, 2023) against the top five cyber power countries based on NCPI for research validation.

3.1 Stages of Bibliometric Analysis

In conducting the bibliometric analysis, a standard process was followed as depicted in Figure 1 below. This process was adapted from (Donthu, et al., 2021).

Figure 2: Bibliometric Analysis Stages (source: authors)

- Conducting a bibliometric analysis involves a systematic process of searching, analyzing, and interpreting data to identify trends, patterns, and insights in scholarly literature. The following are the steps followed.
- **Step 1: Define research question and objectives for bibliometric analysis:** for the research study, we defined the research question as "***what are the trends in research on cyber warfare in Africa over the past 23 years?***". The objective for this research was to identify and understand the cyber warfare research capability development trends and landscape in Africa in the context of globalization and digital transformation.
- **Step 2: Choose techniques and databases for bibliometric analysis:** we chose performance analysis, science mapping, and network analysis techniques as appropriate for this research study. In performance analysis, our focus was on publication, citation, and collaboration analyses. In science mapping, we focused on authors' relationships, topics, and thematic analyses. We also opted for network analysis by conducting clustering and visualization on the collected data as demonstrated in Section 4. We opted to using Scopus for data collection. This was because at the time of this research, it was able to support an export of a large-data set (up to 20,000 records at a time) compared to Web of Science. It is also one of the most trusted sources of research data and impact analysis.
- **Step 3: Formulate search query and collect the bibliometric data**: the keywords defined for the search query were: *"Cyber War*" OR "Cyber Defen*" OR "Cyber Offen*" OR " Cyber Oper*" OR "Cyberwar*" OR "Infowar*" OR "Information War*" OR "Cyber-war*" OR "Cyber-Defen*" OR "Cyber-Offen*".* There are still several challenges in the cyber domain in terms of agreed-upon taxonomy, terminologies, and definitions and for our search query, we attempted to be as inclusive as practical on the different variations in the cyber warfare domain. We used Boolean operator "OR" in Scopus to combine keywords and phrases closely related to the research topic. Data collection focused on final and in the press publications in conference papers, research articles, book chapters, editorials, letters, and surveys.
- **Step 4: Collect and refine the bibliometric results**: we collected the data and reviewed the search results. We then refined the data through the identification of relevant publications, countries, and affiliations for further analysis. We finally extracted the sampled data through a comma-separated values (CSV) file.
- **Step 5: Analyze, interpret, and visualize the bibliometric analysis**: the extracted CSV data file was imported into the VOSviewer platform (van Eck & Waltman, 2010) for visual analysis, Bibliometric tool (Aria & Cuccurullo, 2017) for other analysis not found in VOSviewer. Excel Data Analysis (Microsoft, 2021) was also employed in cases where we noticed duplicates and for cleaning and merging of data with same names that had different variations.

3.2 Bibliometric Analysis Tools

Biometric analysis is a complex process since it involves several technical steps and large datasets. Over the years, researchers have, as a result, developed open-source tools that simplifies and support the analysis process. In this study, we benchmarked a series of tools for this purpose as summarized below.

- **VOSviewer** (van Eck & Waltman, 2010) is a free software platform for constructing and visualizing bibliometric networks. It can be used to create maps of co-authorship, co-citation, and co-occurrence networks. VOSviewer is particularly well-suited for analysing large datasets, and it can produce high-quality visualizations that are easy to interpret.
- **CiteSpace** (Chen, 2014) is a free Java-supported tool for visualizing and analysing trends and patterns in scientific literature. It is primarily used for Web of Science data, but it can also import data from other sources such as arXiv and PubMed. CiteSpace is particularly useful for identifying emerging trends and hotspots in research.
- **Bibliometrix** (Aria & Cuccurullo, 2017) is a versatile R-tool package for performing comprehensive science mapping analysis of scientific literature suitable for handling large datasets. It provides a wide range of command-line and web-based tools for data import, cleaning, and analysis, as well as for creating visualizations.
- **Science of Science (Sci2)** (Lewis & Alpi, 2017) is a modular and open-source toolset specifically designed for the study of science. It includes a wide range of tools for data collection, analysis, and visualization. Sci2 is particularly well-suited for analysing large-scale scientific datasets.

For this study, we opted for the VOSviewer platform and Bibliometrix R-tool because these tools were free to use, easy to access and setup, demonstrated wide usage in literature, and provided for different visualizations.

4. Bibliometrics Analysis Results

As of 26 November 2023, an initial total of 33,420 research documents were retrieved using the Scopus database search engine as per the defined search keywords. The date range used was between 2000-2023. The search scope was within “all the fields” as defined by Scopus. When the search scope was limited to “article title, abstract, and keywords” only 6,091 documents were found, globally. A total of 4,727 documents were found based on the search query on the “abstracts” of the research publication. Limiting the search results to only the relevant keywords found in the research articles, a total of 2,774 documents were extracted from different research institutions across the globe. When we limited the search query to the relevant “article title”, 1,878 articles were found.

Employing different layers of filtering on search queries is crucial for an objective understanding of cyber warfare research trends in Africa, preventing overstating or understating the search results. Thoroughness is also essential to avoid misinterpreting the results due to the limitations of keyword searches. Using only one type of search query can lead to duplicated or irrelevant results. For example, searching within “all fields" in Scopus articles may yield results where the defined keywords appear in sections unrelated to cyber warfare. Conversely, using the "article title" search may exclude relevant publications if they do not include the keywords in the title.

For purposes of the analysis, we opted to use bibliometric data for Africa retrieved within a combination of “Article title, Abstract, and Keywords” search query. This, we believe may provide a general overview and insights of the cyber warfare research trends in Africa over the past 23 years.

We subsequently excluded retracted publications, raw data papers, and erratum publications from the analysis. The data was restricted English-written publications; however, this language limitation was not considered for the comparative analysis. Furthermore, we filtered the results by focusing on the identifiable African countries.

A total of 154 documents were discovered using this limited search query purely focusing on cyber warfare related research in Africa. From the analysis, it appears that the first indexed publication on Scopus on cyber warfare for Africa is from 2005 as the data returned contained years 2005-2023. This means our analysis covered 18 years instead of the 23 years as per the research objectives.

4.1 Publication Analysis

Focusing on the African content, only 154 publications written by over 254 co-authors were found on Scopus focusing on the subject matter. An estimated 68% of the research in cyber warfare originates from South Africa and the rest from other African countries.

Most publications on cyber warfare research in Africa are published in conference proceedings (61.7%), Book Chapters (16.9%), and Journal Articles (18.8%). Over 40% of the publications discovered are in Computer Science, with 25% in Engineering. As per Table 1, the most common source for cyber warfare research publications by African authors is the European Conference on Information Warfare and Security and International Conference on Information Warfare and Security. Since the names of sources change every year, especially on conference proceedings, some of the data in the Table 1 below may not be complete.

Table 1: Most relevant sources of cyber warfare research in Africa

Sources	Articles
EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY	23
INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY	22
LECTURE NOTES IN NETWORKS AND SYSTEMS	5
INFORMATION SECURITY FOR SOUTH AFRICA	3
EUROPEAN CONFERENCE ON INFORMATION MANAGEMENT AND EVALUATION	3
ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES	3
COMPUTER AND INFORMATION SECURITY HANDBOOK	3
LECTURE NOTES IN COMPUTER SCIENCE	3

Figure 3 below shows that since 2005, the African continent has been slowly increasing research on cyber warfare, starting from below 5 articles per year in 2005 to 15 articles (on average) in 2023. The growth rate of publications on cyber warfare in Africa is estimated at 17.7% over the past 18 years.

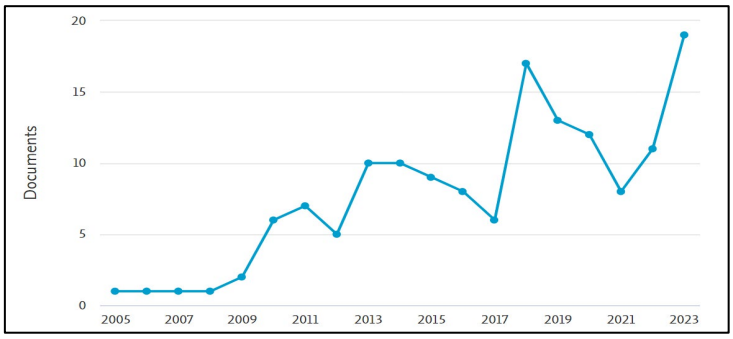

Figure 3: Cyber warfare research publication trends since 2005

4.2 Keywords, Trends, and Thematic Analysis

Relevant keywords provided by authors of the papers and occurred for more than 5 times in the Scopus core database were considered in the final analysis. Based on the 154 documents, 77 items met the threshold and a total of 8 clusters were generated with a total link strength of 404 based on the analysis done on VOSviewer. As may be noted in Figure 4 below, cyber warfare was a dominant cluster and links to a series of topics including cyber-crime, cyber defence, information operations, cyber terrorism, cyber counter-intelligence, cyber-attack, and others.

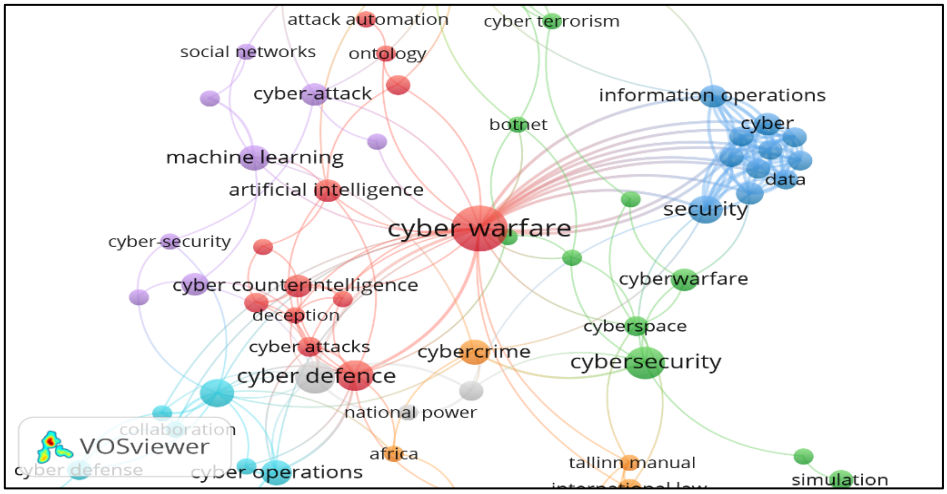

Figure 4: Keyword analysis on cyber warfare research in Africa

4.3 Authors, Collaboration, and Publication Impact Analysis

Figure 5 below shows the top ten authors in cyber warfare research in Africa over the past 18 years. Author "van Niekerk, B" has published, according to the data collected and filtering, 18 articles, followed by "Leenen L" with 14 articles. Both these authors have been productive in the cyber warfare domain since 2010.

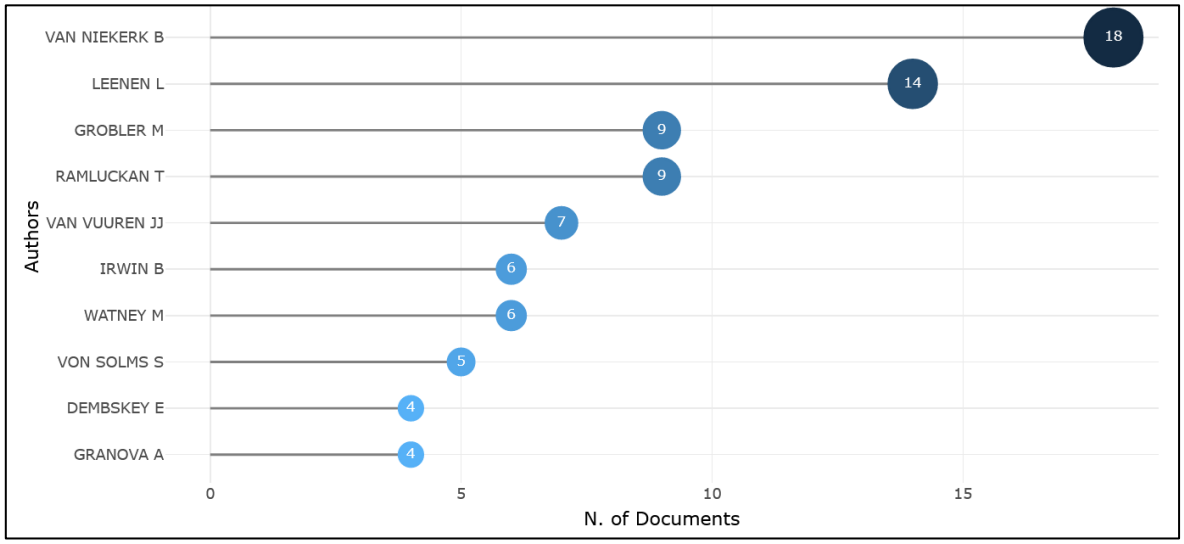

Figure 5: Author's productivity on cyber warfare research over time

In terms of collaboration networks amongst authors in Africa, the networks are quite diverse, albeit not strong. Author "Leenen, L" had a diverse collaboration network with different cohorts of researchers including those in the military environment.

The impact of cyber warfare research in Africa as depicted in Figure 6 and was at an average citation of 3.27 per document by end of year 2022. The top author had the highest h-index of five on cyber warfare research. These results are supported by the research published by Kyrdoda, et al., (2023) where African countries do not appear in the list of top countries with high-impact cybersecurity research.

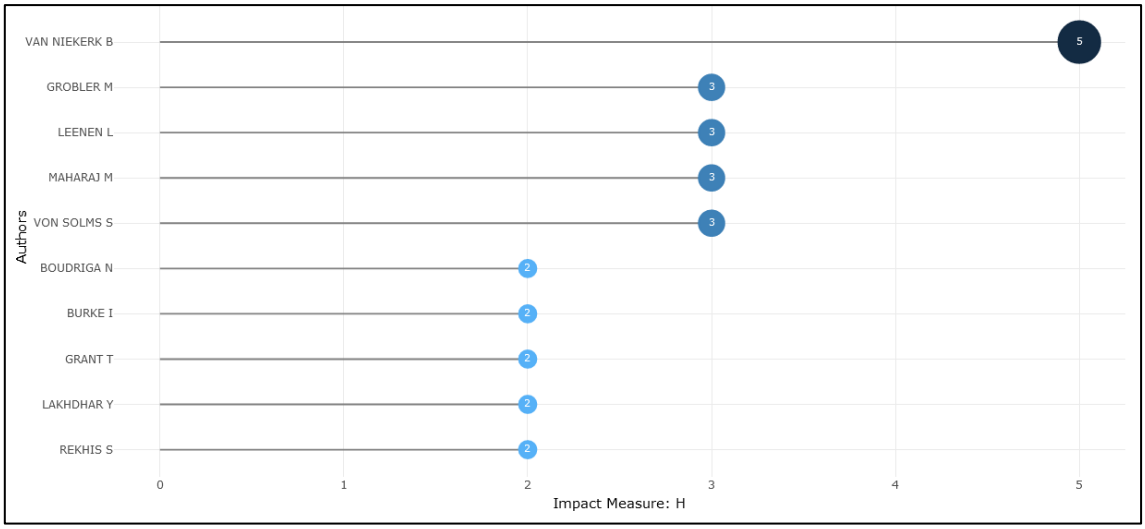

Figure 6: Publication impact factor analysis on cyber warfare research

Figure 7 shows the research collaborations through co-authorships between African countries.

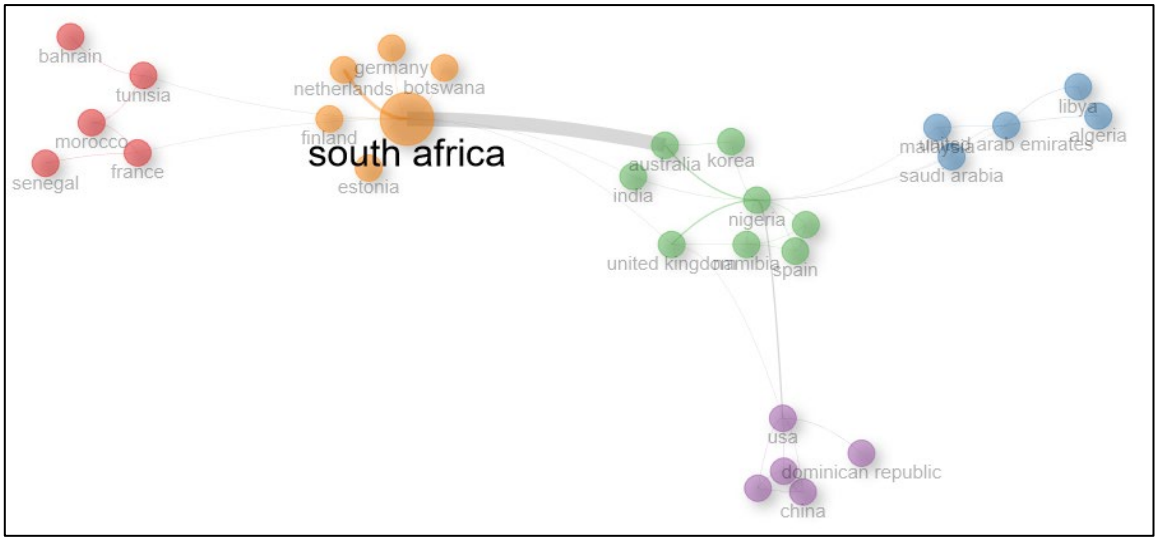

Figure 7: Research collaborations on cyber warfare research in Africa

The active countries (>5 articles) on cyber warfare research in Africa that were found in the collected data are: (1) South Africa, (2) Nigeria, (3) Morocco, (4) Tunisia, and (5) Algeria. The bibliometric analysis revealed that research collaborations within the cyber warfare domain in Africa tends to be with countries outside the region. And that there are limited collaborations between African authors on this subject matter as demonstrated in Figure 7.

4.4 Research Organisations and Funding Analysis

The organisations that are involved in the publications of cyber warfare research in Africa are mostly based in South Africa (see Figure 8) with the University of Carthage in Tunis and Covenant University in Nigeria, and Abdelmalek Essaadi University in Morrocco being the only institutions outside South Africa featuring in the top 10.

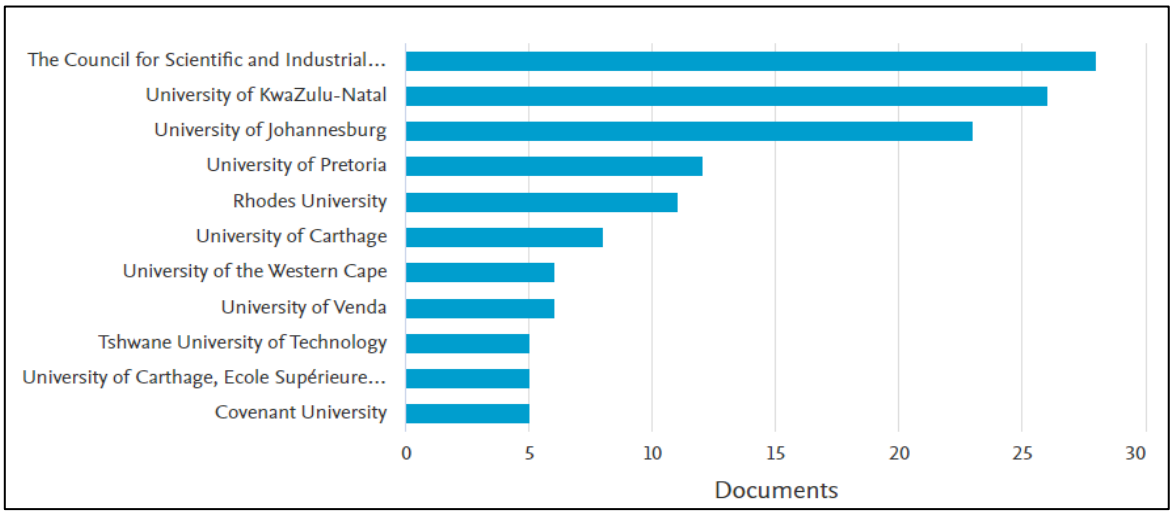

Figure 8: Research affiliations on cyber warfare in Africa

The organisations that are involved in the publications of cyber warfare research in Africa are mostly based in South Africa (see Figure 8) with the University of Carthage in Tunis and Covenant University in Nigeria, and Abdelmalek Essaadi University in Morrocco being the only institutions outside South Africa featuring in the top 10.

The analysis indicated that cyber warfare research funding in Africa is limited, and was generally supported by the National Research Foundation, South African Department of Defence, Armscor Ledger Program, Security and Software Engineering Research Centre and in some instances by overseas sponsors such as Hague Centre for Strategic Studies between 2005-2023.

5. Comparative Analysis

To contextualize the cyber warfare research trends and landscape in Africa, a comparative analysis was also conducted. This was done by choosing the top five countries in the National Cyber Power Index (NCPI) (Voo, et al., 2022) and use the same keywords to extract high-level publication data based on "article titles, abstract, and keywords" and other indicators as presented in Table 2. In Africa, South Africa* was used for comparison purposes because it had close to 70% of the publications in cyber warfare research over the past 18 years as of November 2023.

Based on the comparative analysis, the US is dominating across all publication indicators. The cyber warfare research in the US, China and UK is driven by a diverse set of research, private, and public institutions, including the military. The research in this domain tends to be funded by different funding sources or agencies, mostly local funding agencies in the United States and China. In South Africa, it emerged from the analysis that all cyber warfare research is driven by research and academic institutions. Funding sources of cyber warfare research in Africa is also limited to few funding agencies.

In addition, developed countries tend to succeed in collaborating with other research authors across the globe. Thus, the USA has a large group of research affiliations involved in cyber warfare research due to local and international collaborations. This, in our view, ultimately translates to a higher research impact.

Table 2: Comparative analysis of countries in cyber warfare research

Country	Search results within all fields	Search results in abstracts	Search Results in keywords	Search Results in article title	Search Results in Article title, abstract, and keywords*
United States of America	9,966	1,691	1,012	741	2,192
Republic of China	3,483	416	233	73	463
Federation of Russia	811	155	104	36	206
United Kingdom	3,352	353	198	187	489
Australia	1,695	157	86	55	191
South Africa*	697	87	71	42	105

6. Discussion, Implications, and Limitations

The bibliometric analysis study has yielded valuable insights into the landscape of cyber warfare research and development in Africa. Upon examining the sample of documents retrieved through the Scopus search query, it becomes evident that research activity in this domain is relatively limited. Only a total of 154 documents were sampled from African countries collectively, in contrast to 2,192+ documents for the United States over an 18-year period. This translates to approximately 9 research publications per year for Africa, compared to 122 articles from the United States and 27 articles from the UK per year.

Consolidated efforts are recommended between research affiliations and authors to elevate the rate of cyber warfare research. This could be achieved by establishing African publication forums and conferences specifically focusing on cyber warfare. According to the analysis, most of the African cyber warfare research is published in overseas-based research platforms.

Furthermore, the comparison reveals that cyber warfare research in Africa constitutes only 7% of the entire body of research in the United States and approximately 75% of the research output in the Russian Federation (refer to Table 2: "article title, abstract, and keyword" column for details). This significant discrepancy underscores the need for increased attention and investment in cyber warfare research and development within the African context.

The analysis also suggests that only two authors in the entire African continent have been consistently publishing in cyber warfare research over the past 18 years using the sampled data from Scopus, and both researchers are based in South Africa. This also translates to the limited publication impact of cyber warfare research in Africa,

with only 2.1 citations per published document, while in countries such as the USA, this can even reach 40+ citations per cyber warfare research publication.

An observation from the research findings is that African countries do not adequately collaborate or co-author research work in this domain. This limitation hinders the growth of cyber warfare research in Africa as well as its associated impact. It is recommended that African researchers need to break down barriers and intentionally collaborate on cyber warfare research with the public and private entities, ultimately assisting state entities in establishing and operationalizing cyber warfare capabilities.

Research findings indicate that countries that are highly productive in cyber warfare research are supported by a large cohort of active research affiliates, engage in multi-disciplinary collaborations, work with national security and defence agencies, and receive national research sponsorship. Therefore, it is recommended that for African states to grow their cyber warfare research activities, investments need to be made by both the public and private sectors.

On a positive note, the primary topics of research on cyber warfare in Africa are comparable to those in developed nations, suggesting that African nations are conducting relevant research in the third domain, albeit in a limited scope.

Limitations identified in this research study include the fact that Scopus indexing does not cover the entire research universe, potentially understating the African perspective. Keyword searches also have limitations that may impact the extent of research on cyber warfare in Africa. Furthermore, the results may be negatively affected by diverse naming conventions in article titles, authors' affiliations, publication platforms, and other factors. The bibliometric analytical tools are also not yet mature enough to automatically eliminate not so obvious duplicates due to varying naming conventions, requiring manual intervention, which may introduce errors and bias in the analysis.

7. Conclusion and Future Research

The research and development of cyber warfare capabilities in Africa are currently limited. However, South Africa stands out as a leader in this field, actively contributing to the global community and ranking twelfth in the number of cyber warfare research publications, with the USA leading all countries. This research highlights the potential of bibliometric analysis in revealing trends and patterns within a selected research domain. The findings emphasize that bibliometric data is rich and can offer valuable insights for defining research directions and supporting policy formulations. Nevertheless, it is essential to acknowledge the challenges associated with retrieving data for research from databases like Scopus. To address some of these limitations, a comparative analysis was employed. It is important to note that these limitations are not exclusive to research in Africa but are widespread. Therefore, this research contributes not only to the cyber warfare research landscape in Africa, but also to the broader global context. In future research, it may be worthwhile to focus on studies indexed Web of Science and Scopus to understand the trends broadly. It may also be useful to consider using Google Scholar for a bibliometric analysis as it tends to index majority of publications. Lastly, studying the mandates and profiles of research affiliations involved in cyber warfare research could be helpful for African countries to improve cyber warfare research.

Acknowledgement and Declaration

This work received support from the Council for Scientific and Industrial Research in South Africa. Generative AI in Google Bard and ChatGPT were utilized on limited basis for language editing, sentence construction in certain sections of this document. All sources employed for this research are duly cited below.

References

Amoah, M., 2019. Sleight is right: Cyber control as a new battleground for African elections. *African Affairs,* 119(474), pp. 68-89.

Aria, M. & Cuccurullo, C., 2017. bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of informetrics,* 11(4), pp. 959-975.

Binnendijk, A. L. et al., 2019. *Operationalizing cyberspace as a military domain.* 2019 ed. Santa Monica: Rand Corporation.

Blair-Walcott, K., 2023. Comparative Analysis. In: J. M. Okoko, S. Tunison & K. D. Walker, eds. *Varieties of Qualitative Research Methods.* s.l.:Springer, Cham, pp. 79-84.

Chen, C., 2014. *The citespace manual,* Drexel: College of Computing and Informatcs.

Colarik, H. D., 2017. The Hierarchy of Cyber War Definitions. In: G. Waag, M. Chau & H. Chen, eds. *Intelligence and Security Informatics.* s.l.:Springer, Cham.

Donthu, N. et al., 2021. How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research,* 133(2021), pp. 285-296.

Fielder, J. D., 2021. Cyber security in Kenya: Balancing economic security and internet freedom. In: *Routledge Companion to Global Cyber-Security Strategy.* s.l.:Routledge, pp. 543-552.

ITU, 2021. *Global Cybersecurity Index 2020.* [Online] Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf [Accessed 24 November 2023].

Kyrdoda, Y., Marzi, G., Dabić, M. & Daim, T. U., 2023. Cybersecurity Technology: An Analysis of the Topic from 2011 to 2021. In: *Cybersecurity. Applied Innovation and Technology Management..* s.l.:Springer, Cham.

Lewis, D. M. & Alpi, K. M., 2017. Bibliometric Network Analysis and Visualization for Serials Librarians: An Introduction to Sci2. *Serials Review,* pp. 239-245.

Lukin, K., 2019. Russian Cyberwarfare Taxonomy and Cybersecurity Contradictions Between Russia and EU: An Analysis of Management, Strategies, Standards, and Legal Aspects. In: *National Security: Breakthroughs in Research and Practice.* s.l.:IGI Global.

Microsoft, 2021. *Use the Analysis ToolPak to perform complex data analysis.* [Online] Available at: https://support.microsoft.com/en-us/office/use-the-analysis-toolpak-to-perform-complex-data-analysis-6c67ccf0-f4a9-487c-8dec-bdb5a2cefab6 [Accessed 25 November 2023].

Mtsweni, J. & Thaba, M., 2021. Building an Integrated Cyber Defence Capability for African Missions. *Journal of Information Warfare,* 21(1), pp. 17-34.

Nobanee, H. et al., 2023. Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime.*

Rahim, N., 2021. Bibliometric Analysis of Cyber Threat and Cyber Attack Literature:Exploring the Higher Education Context. In: M. Sarfraz, ed. *Cybersecurity Threats with New Perspectives.* Kuwait: IntechOpen.

Thaba, M. & Mtsweni, J., 2023. *Developing Robust Cyber Warfare Capabilities for the African Battlespace.* Athens, Greece, European Conference on Cyber Warfare and Security.

The Times of Israel, 2023. *Israel-linked group claims cyberattack that shut down 70% of Iran's gas stations.* [Online] Available at: https://www.timesofisrael.com/israel-linked-group-claims-cyberattack-that-shuts-down-70-of-irans-gas-stations/ [Accessed 21 December 2023].

Tse, J. et al., 2015. A bibliometric analysis of privacy and ethics in IEEE Security and Privacy. *Ethics and Information Technology,* 17(2015), pp. 153-163.

van Eck, N. J. & Waltman, L., 2010. Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics,* 538(84), p. 523.

Voo, J., Hemani, I. & Cassidy, D., 2022. *National Cyber Power Index 2022,* Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Willet, M., 2023. The Cyber Dimension of the Russia–Ukraine War. *Survival: October-November 2022,* Issue Apr 2023, pp. 7-26.