International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 6, December 2025, pp. 5815~5826
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i6.pp5815-5826

Bibliometric analysis to highlight the impacts of digitalization, artificial intelligence, and modern optimization on the human environment during international armed conflicts

Hegazy Rezk[1], Montaser Mahmoud[2]
[1]Department of Electrical Engineering, College of Engineering in Wadi Addawasir, Prince Sattam bin Abdulaziz University, Al-Kharj, Saudi Arabia
[2]Sustainable Energy and Power Systems Research Centre, RISE, University of Sharjah, Sharjah, United Arab Emirates

Article Info

Article history:

Received Sep 1, 2024
Revised Jul 13, 2025
Accepted Sep 14, 2025

Keywords:

Armed conflicts
Artificial intelligence
Bibliometric analysis
Digitalization
International humanitarian law

ABSTRACT

This research is conducted to explore the impacts of digitalization and artificial intelligence (AI) on the human environment during international armed conflicts, aiming to identify trends, challenges, and potential solutions to improve humanitarian aid, decision-making, and conflict resolution strategies. To identify the main research issues about the effects of AI and digitalization on the human environment in conflict situations, this work employs a bibliometric analysis. A bibliometric analysis of the impacts of digitalization and artificial intelligence on the human environment during armed conflicts by examining 544 selected papers from Scopus database has been conducted. Knowledge mapping techniques involving collaboration analysis, co-citation analysis, and keywords co-occurrence analysis methods are adopted in bibliometric analysis. Based on a comprehensive analysis of literature, this work attempts to pinpoint the key areas of interest, knowledge gaps, and new problems in this domain. The findings of this bibliometric analysis contribute to a better understanding of the complex interactions between technology, armed conflicts, and the human environment, with implications for humanitarian action, international law, and conflict resolution efforts. The bibliometric analysis reveals that the United States of America (USA) is by far the leading country in research within this field, with a substantial frequency of 181 documents. It significantly surpasses that of other countries, indicating its dominant position in the research landscape. In sum, the work offers suggestions for further research and policy intervention.

Corresponding Author:

Hegazy Rezk
Department of Electrical Engineering, College of Engineering in Wadi Addawasir, Prince Sattam bin Abdulaziz University
Al Kharj 16278, Saudi Arabia
Email: hr.hussien@psau.edu.sa

1. INTRODUCTION

War is a lethal force, but its repercussions go much beyond the immediate loss of life. Armed conflict not only causes losses on the battlefield but also results in forced migration, refugee movements, the flight of wealth, and the devastation of a society's infrastructure. Social, political, and economic institutions suffer enduring damage. Conflict, particularly civil war, has significant negative implications for development [1]. In addition, military operations discharge hazardous pollutants into the air, causing respiratory issues in both combatants and civilians. Contamination of water sources and elevated public health hazards may result from infrastructure damage, including water treatment facilities and waste management systems [2]. The need for resources such as timber and land can lead to deforestation and land degradation, resulting in ecosystem loss and soil erosion. Disrupting natural carbon sinks and increasing greenhouse gas emissions can exacerbate climate change. Compromised environmental protection and law enforcement measures can also lead to wildlife trafficking [3], [4]. Therefore, it is mandatory to handle these problems during armed conflicts.

The use of digitalization, modern optimization, and artificial intelligence during armed conflict has the potential to enhance military operations significantly. Recent military conflicts between governments and non-state entities have shown the future of warfare [5]. More and more, algorithms are being used to make decisions. These systems use huge amounts of data created by improvements in uncrewed aerial vehicles (UAVs), space, and sensor technologies [6]. This data is then combined in real-time with data from mobile communications, social media, and other "publicly available information." This creates systems where the military is constantly watching. Significantly, this could decrease civilian fatalities and collateral damage, underscoring the humanitarian benefits of these advancements. However, these innovations' legal and ethical effects on civilian populations are currently being assessed.

This progress could potentially lead to shorter wars and a significant reduction in the environmental impact of prolonged combat, fostering a sense of optimism about the future of military operations. However, it is crucial to consider the potential drawbacks. By increasing their dependence on digital technology, military operations may become increasingly susceptible to cyber assaults, data breaches, and disinformation campaigns [7]. These attacks can intensify conflicts and increase the probability of unintended incidents, underscoring the need for caution. Moreover, the production and use of digital equipment contribute to electronic waste, energy consumption, and resource depletion, all of which harm the environment [8]. To prevent armed conflicts involving digitalization, modern optimization, and artificial intelligence from disproportionately impacting the environment, it is crucial to carefully weigh the benefits of these technologies against their potential risks and environmental consequences, guiding our decisions.

Armed forces now have access to better capabilities thanks to digitalization and artificial intelligence (AI) [9], which have changed how wars are fought. These capabilities include cyber warfare tools, autonomous drones, and real-time data analysis. When making strategic decisions, these technologies are more efficient and precise. However, they also bring forth new ethical questions and dangers [10]. There are concerns about the possibility of unintentional injury and a lack of human supervision with autonomous weapons and cyberattacks may interrupt vital services by targeting civilian infrastructure. Therefore, to reduce dangers and safeguard civilians in war zones, legislation and ethical frameworks are necessary to address the complicated and ever-changing role of digitalization and AI in armed conflicts [11], [12].

Recent research reveals an extensive utilization of neural network technology in cyberwar [13], [14]. Some applications include dynamic foreign exchange (FX) conventional market forecasts, intelligent transportation systems (ITS), environmental forecasting and evaluation, irradiance prediction [15] and separating informative tweets from those containing rumors or undetailed useless data. This enhancer is the most effective tool for enhancing capabilities and provides numerous benefits to the military [16]. Human resources, combat and support vehicles, helicopters, state-of-the-art intelligence and communication equipment, artillery, missiles, and infrastructure are just a few examples of the many resources and capabilities that should be considered when making military decisions [17], [18].

AI stand for computer programs that can learn, reason, solve problems, and perceive and interpret language in the same way as humans can [19]. Creating models and algorithms so computers can execute activities typically requiring human intellect is what it is all about. Speech recognition in driverless cars is only one example of the many AI uses [20]. AI is commonly used interchangeably with machine learning or deep learning algorithms [21]. The seven AI patterns include systems driven by goals, systems that can operate independently, conversations that mimic human contact, analytics that can forecast the future, hyper-personalization, and systems that can assist with making decisions [22], as illustrated in Figure 1. Afterward, AI is applied to a particular situation using one or more of these seven patterns [23]. Seven AI patterns include: pattern and anomalies recognition, which identifies patterns in images and speech for example object detection in military surveillance [24]; conversational and human interactions, enabling dialogue between humans and machines including chatbots for military communication [25]; predictive analytics and decisions, which forecasts outcomes based on historical data involving predictive maintenance for military equipment [26]; goal-driven systems, that optimize actions to achieve objectives like autonomous drones [27]; hyperpersonalization, which customizes services based on user behavior such as adversarial networks for personalized soldier training [28]; decision support, AI-assisted decision-making in military operations [29]; and autonomous systems, which allows self-driving military vehicles [30]. These seven AI patterns have recently transformed military operations with their novel capabilities and use for tasks like object identification, decision support, and conversational engagements.

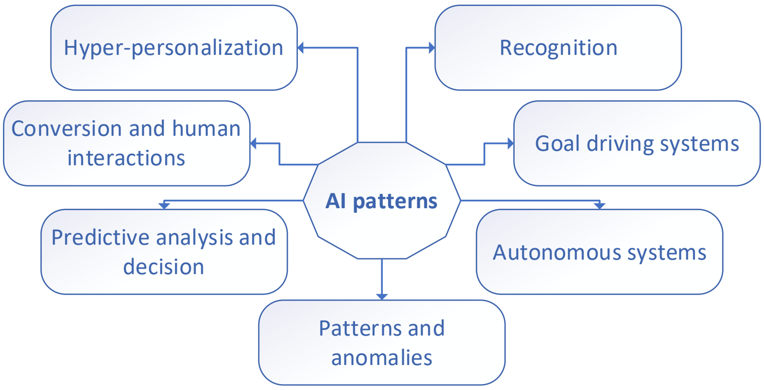


Figure 1. AI main patterns

Intelligent military systems can handle vast amounts of data better than traditional ones [22]. AI's natural calculating and decision-making skills improve combat systems' self-control, self-regulation, and self-actuation. Nearly every military application uses artificial intelligence, and expanding military backing for novel and sophisticated AI technologies will raise demand for AI-driven systems [31]. These applications include autonomous target recognition and tracking, surveillance, cybersecurity, logistics, robotics and drone navigation, and healthcare.

The analysis goals to accomplish a clear understanding of how digitalization and AI affect the human environment during armed conflicts, focusing on their role in decision-making, resource management, and humanitarian response, while recognizing key trends, challenges, and prospects to improve conflict management and resilience. In order to discover the optimal solution to complicated issues in many different fields, including engineering, finance, machine learning, and many more, modern optimization uses sophisticated approaches and tools [32], [33]. Optimization aims to maximize or minimize a function by methodically choosing the ideal input values. The objective is to find the best potential solution while still meeting all the limitations. Contemporary optimization techniques employ mathematical models, computer tools, and complicated algorithms to solve difficult issues instead of more conventional methods [34]. These approaches typically consist of:

a. Metaheuristic optimization algorithms [35], [36]: these optimization algorithms are widely used to resolve complicated optimization issues that deterministic approaches have proven incapable of adequately managing. These algorithms can be classified based on their strategies and working principles as:
   - Population-based vs. single-solution: in each iteration, the algorithms either work on one solution or a population of solutions. Genetic techniques (GA) and particle swarm optimization (PSO) are population-based techniques, whereas simulated annealing (SA) is single-solution-based.
   - Nature-inspired vs. non-nature-inspired: Natural concepts such as Darwinian theory, particle swarms, and ant and bee behavior may inspire metaheuristic algorithms. On the other hand, mathematical or physical strategies like simulated annealing or Tabu search are not nature inspired.
   - Local search vs. Global search: Metaheuristic algorithms may explore the search space globally or refine results locally. Iterative local search methods improve local solutions, such as hill climbing or simulated annealing. Genetic and particle swarm optimization techniques are global search algorithms that explore a larger search area.

b. Convex optimization [37]: convex optimization is a branch of mathematical optimization that concentrates on minimizing convex functions over convex sets. Unique global minima facilitate the efficient and well-structured solution of convex optimization problems. Fundamental algorithms like gradient descent and interior-point methods frequently resolve convex optimization problems. In general, convex optimization is essential for creating scalable and efficient solutions to a diverse array of real-world issues.

c. Stochastic optimization [38], [39]: these optimization techniques randomly choose possible solutions to iteratively explore the solution space. These algorithms try to discover a satisfactory solution in a reasonable time, particularly when the issue is complicated or when there is uncertainty or noise in the system. Stochastic gradient descent (SGD) is one of the most used stochastic optimization algorithms [40]. It calculates the gradient of the loss function for an arbitrarily selected subset of data points or a single data point. This randomness enables it to converge rapidly and circumvent local minima, rendering it appropriate for large datasets. Nevertheless, SGD may necessitate additional computational resources and be susceptible to hyperparameters and randomness.

Modern optimization methods use sophisticated mathematics, vast computer resources, and creative algorithms to solve complicated real-world problems effectively. In many businesses, these strategies simplify procedures, boost efficiency, and foster creativity. The main steps to solve a problem using modern optimization algorithms are illustrated in Figure 2.

The design and development of a future defense force is a complex and challenging issue, where the defense sector has particular challenges that are not found in other application areas [41]. Modern optimization algorithms have been used to address some problems related to the military sector to enhance its performance. For example, they have been used to optimize the design of the UAV [42], to address the complex military fleet mix and upgrade problem [43], cybersecurity enhancement [44], and so many other applications. The analysis goals to explore how modern optimization impacts the human environment during armed conflicts, focusing on their effectiveness in resource allocation, logistics, and decision-making to advance operational efficiency, humanitarian aid delivery, and overall conflict management.

In sum, the research problem can be defined as the lack of a comprehensive understanding of how digitalization and AI impact the human environment during international armed conflicts, which hinders the progress of effective strategies to minimize negative impacts and improve humanitarian efforts. Finally, the significance of the work is understanding how digitalization and AI can alter warfare and how they may harm civilian populations and the environment in conflict zones makes researching the effects of digitalization and AI on the human environment during armed conflicts important. Researchers can discover potential risks and difficulties associated with the employment of these technologies in conflicts. Potential risks and difficulties involve ethical concerns, technological misuse, data privacy issues, and the possibility of exacerbating conflicts. Besides, ways to mitigate their negative effects and improve the protection of civilians and the environment, by looking into and analyzing these impacts. This research has the potential to lessen harm and protect human rights during times of war by assisting in the creation of laws and procedures that support the moral and appropriate application of artificial intelligence and digitalization in combat situations.

The rest of the paper is organized as: Section 2 presents a proposed methodology and gives an explanation about the bibliometric analysis caried out in this paper. Section 3 introduced the results and discussed it including bibliometric overview, Research trends and hotspots and countries contribution and collaboration. The man findings and recommendations are displayed in section 4.

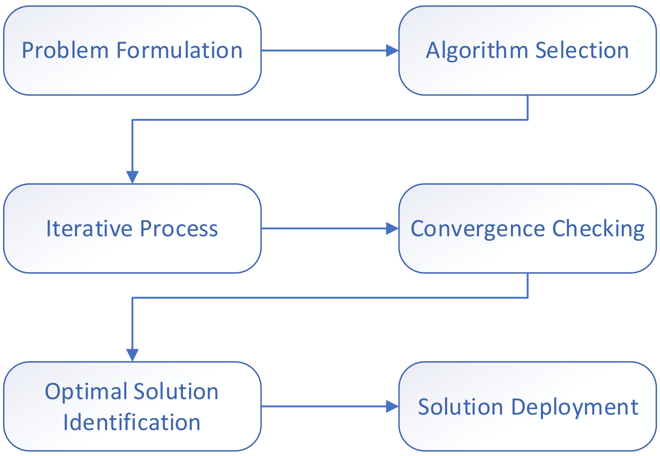


Figure 2. Main steps of a modern optimization procedure

2. METHOD

The bibliometric analysis conducted in this research is divided into two main stages: data collection and data interpretation. Scopus database was chosen due to several reasons, including accessibility, data visualization, ease of export, and wide data availability. The following search query was considered: *(Digitalization OR "Artificial intelligence" OR Cyber) AND ("Armed conflict*" OR "Armed attack*" OR "Armed force*")*. A detailed representation of the methodology followed to conduct the present bibliometric analysis is demonstrated in Figure 3. In this search query, the “*” was mainly used to include the plural of these words, such as armed conflicts, armed attacks, and armed forces. The timespan was kept as default, which resulted in generating results in the duration from 1993 to 2024. Regarding data interpretation, three tools were employed. First, the annual number of publications and related subject areas were directly analyzed utilizing Scopus. The thematic clusters were created using the VOSviewer software, allowing for analyzing the connection between the most occurring keywords. On the other hand, all other results were visualized and analyzed using biblioshiny. Biblioshiny is a web interface for the bibliometrix R package. biblioshiny enables interactive and user-friendly exploration of bibliometric indicators. The data exported from Scopus was directly imported into biblioshiny. Once imported, various metrics could be analyzed by selecting them from the available options in the interface and adjusting the preferences and parameters accordingly. The results include keywords word cloud, keywords frequency over time, countries contribution, annual scientific production of countries, and countries collaboration network.

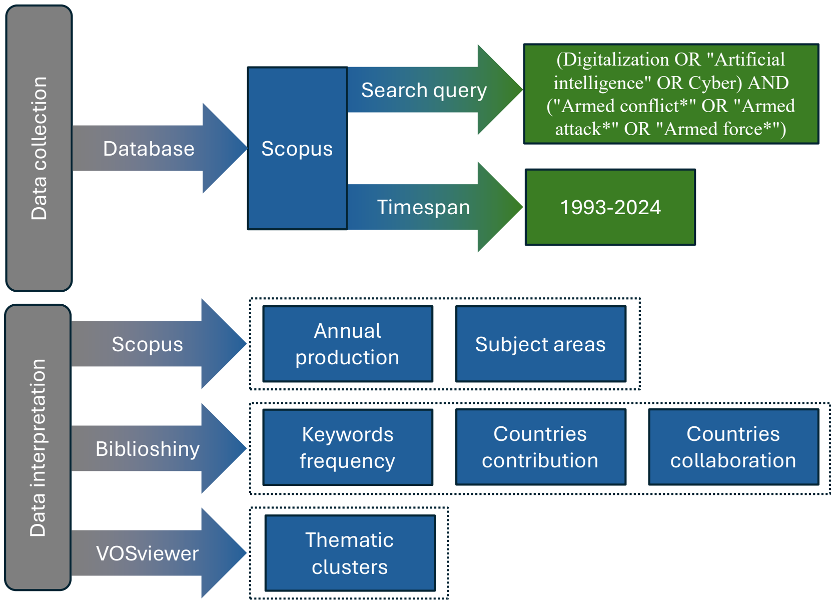


Figure 3. Bibliometric analysis research methodology

3. RESULTS AND DISCUSSION
3.1. Bibliometric overview

The current bibliometric analysis spans from 1993 to 2024, capturing 544 documents with an annual growth rate of 12.73%. Table 1 shows all details related to the main information of the present bibliometric analysis, which was generated through biblioshiny. The documents are diverse, including 208 articles, 171 conference papers, 99 book chapters, and 22 books, suggesting a broad range of dissemination formats. The analysis involves 1018 authors, with 249 contributing to single-authored publications and a low co-authorship rate of 2.09 authors per document. International collaboration accounts for 11.76% of co-authorships, which is also considered a low international collaboration. Additionally, the number of single-authored documents is 298, which accounts for 54.8% of the total number of publications. This tendency toward single-authored publications and limited international collaboration can be attributed to the confidentiality and sensitivity inherent in research related to digitalization, artificial intelligence (AI), and cyber warfare in armed conflicts. The strategic nature of these topics often necessitates restricted sharing of research findings, resulting in more isolated academic efforts.

According to the results generated by Scopus, the most related subject area was Social Sciences, with 289 publications (32%), reflecting a significant focus on the societal, political, and ethical implications of these technologies in conflict scenarios (see Figure 4). Computer Science, with 226 publications (25%), underscores the technical and computational aspects crucial for understanding and developing digital and AI tools in such contexts. The third ranked subject area was Engineering, accounting for 130 publications (14%), which indicates its role in the practical application and development of technologies. There is a gap between the top three ranked areas and the remaining subjects, such that the following subject areas were mathematics, decision sciences, and arts and humanities, accounting for 43 publications (5%), 37 publications (4%), 32 publications (3%), respectively. The "Others" category, comprising 153 publications (17%), includes various sectors such as medicine, business, environmental science, economics, physics, psychology, and materials science.

Table 1. Main information of the bibliometric analysis

Parmeter	Value	Parmeter	Value
Timespan	1993:2024	Article book chapter	1
Sources (journals and books)	336	Article review	1
Documents	544	Book	22
Annual growth rate %	12.73	Book article	1
Document average age	5.68	Book chapter	99
Average citations per doc	6.425	Conference paper	171
Keywords plus (ID)	1946	Conference paper article	1
Author's keywords (DE)	1437	Conference paper book chapter	1
Authors	1018	Conference review	8
Authors of single-authored docs	249	Editorial	2
Single-authored docs	298	Erratum	2
Co-authors per doc	2.09	Letter	1
International co-authorships %	11.76	Note	2
Article	208	Review	24

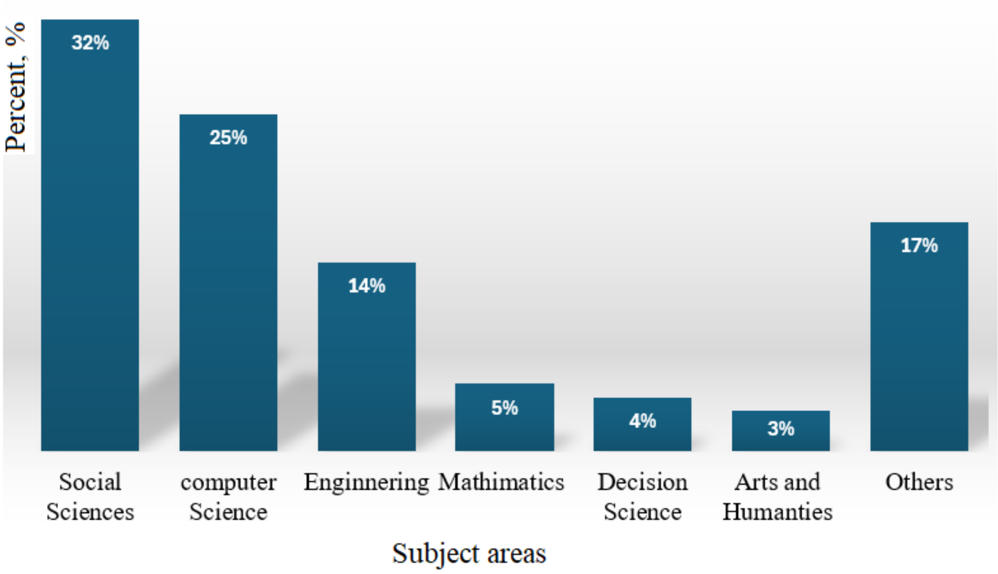


Figure 4. Related subject areas

3.2. Research trends and hotspots

From a modest beginning with sporadic publications in the 1990s and early 2000s, the number of documents began to rise noticeably around 2011. As presented in Figure 5: annual number of publications.5, there are several jumps that were observed, with a particularly sharp growth in 2020, reaching 71 publications. This trend likely reflects the rapid technological advancements and the increasing relevance of digital and AI technologies in security and military contexts. A drop in the number of publications was then observed in 2021 and 2022, which could be attributed to the disruptions caused by the COVID-19 pandemic. After that, the highest peak was achieved in 2023, with 89 publications, resulting from continued research in this field, possibly driven by recent global events or technological breakthroughs. Although the average annual growth rate was not high at 12.73%, there were some years when the growth rate was considerably significant. This is mainly due to the negative growth rate in a few years, such as in 2021. For instance, after 2011, the top three jumps accounted for annual growth rates of 125%, 109%, and 82%, which occurred in 2012, 2020, and 2023, respectively.

The present bibliometric analysis reveals a strong focus on the intersection of AI and cybersecurity with armed conflict and security. "Artificial intelligence" emerges as the most frequent term (see Figure 6), highlighting its significant role in modern conflicts and security studies. This keyword was considerably the highest occurring word, with a frequency of 112. Concurrently, "cyber security" and "network security" are prominent, underscoring the importance of protecting digital infrastructure in conflict scenarios. Additionally, the notable frequencies of "computer crime" and "computers" indicate an awareness of the broader implications of technology in criminal activities and warfare. An illustration of the keywords' occurrence is depicted in Figure 7, showing their frequencies over the investigated timespan.

To further explore the interconnections between the keywords, the thematic clusters were generated using VOSviewer, as shown in Figure 8. The number of occurrences was kept at the default setting, which corresponds to a keyword frequency of 5. This resulted in the creation of thematic clusters comprising a total of 129 words. As can be seen, six clusters were generated: dark blue, light blue, red, green, purple, and yellow. The corresponding top occurring keywords in each of these clusters were artificial intelligence, game theory, armed forces, international humanitarian law, war, and armed conflict, respectively. A huge difference between the number of keywords in each cluster was observed: 39 in the red, 24 in the green, 22 in the dark blue, 17 in the yellow, 17 in the purple, and 10 in the light blue.

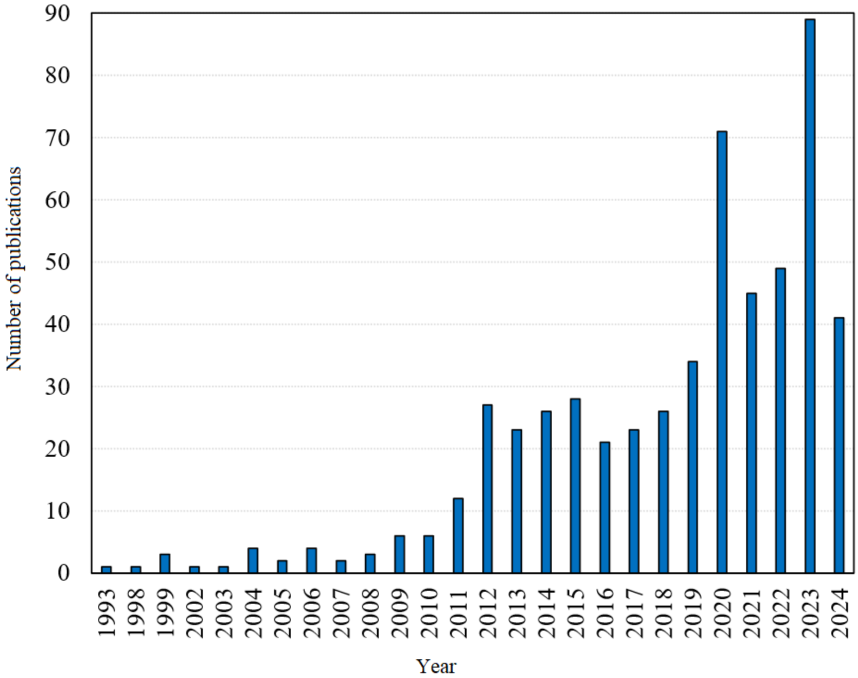


Figure 5. Annual number of publications

Figure 6. Word cloud of most occurring keywords

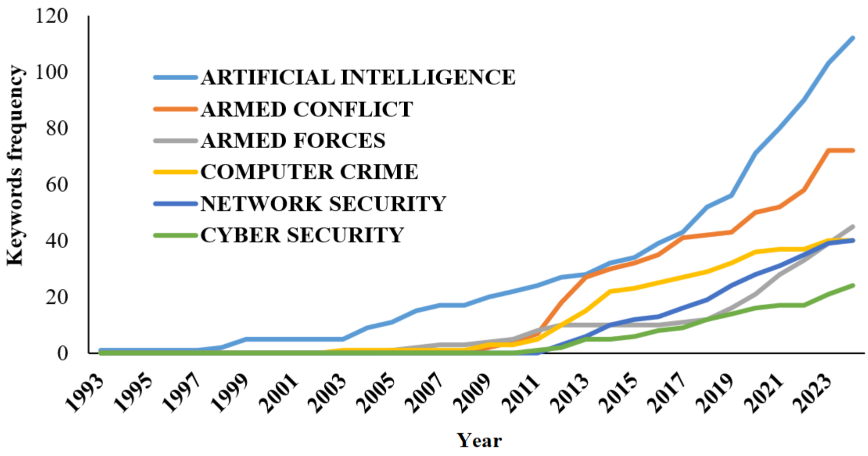


Figure 7. Annual frequency of most occurring keywords

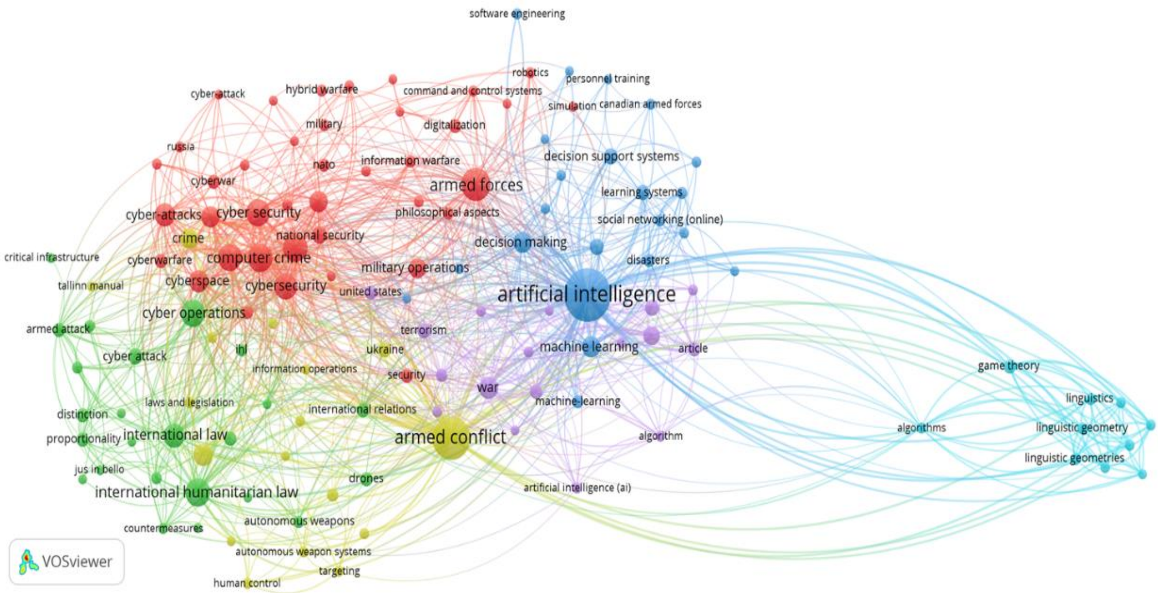


Figure 8. Keywords thematic clusters

3.3. Countries contribution and collaboration

The bibliometric analysis reveals that the USA is by far the leading country in research within this field, with a substantial frequency of 181, as shown in Figure 9. It significantly surpasses that of other countries, indicating its dominant position in the research landscape. The United Kingdom follows with a frequency of 63, and Germany is close behind with 55, but these numbers are notably lower compared to the USA's output. Other countries, including India, Australia, and Canada, have even smaller frequencies, underscoring the USA's preeminence in this area of study. The data clearly illustrates the USA's leading role in advancing research related to the intersection of digitalization, artificial intelligence, cyber warfare, and armed conflict. A detailed presentation of the number of documents published by each of the leading countries in this field is shown in Figure 10.

The scarcity of international collaborations suggests that security and confidentiality concerns are significant factors hindering more extensive international partnerships. Figure 11 underscores the limited scope of international collaboration in this field, which was previously reported as 11.76%. The data reveals that the most significant collaboration is between the USA and the UK, with only 9 publications shared between them. This is followed by a modest 5 documents co-authored by researchers from the USA and Germany. These numbers reflect an extremely low level of international cooperation, highlighting how sensitive research topics in this area may restrict the extent of collaborative efforts.

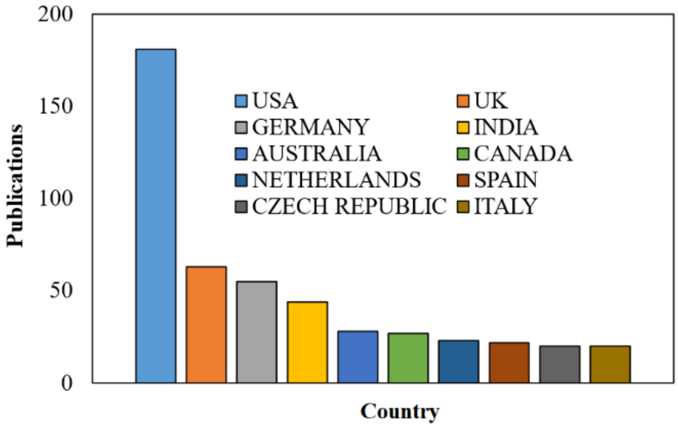


Figure 9. Total number of publications per country

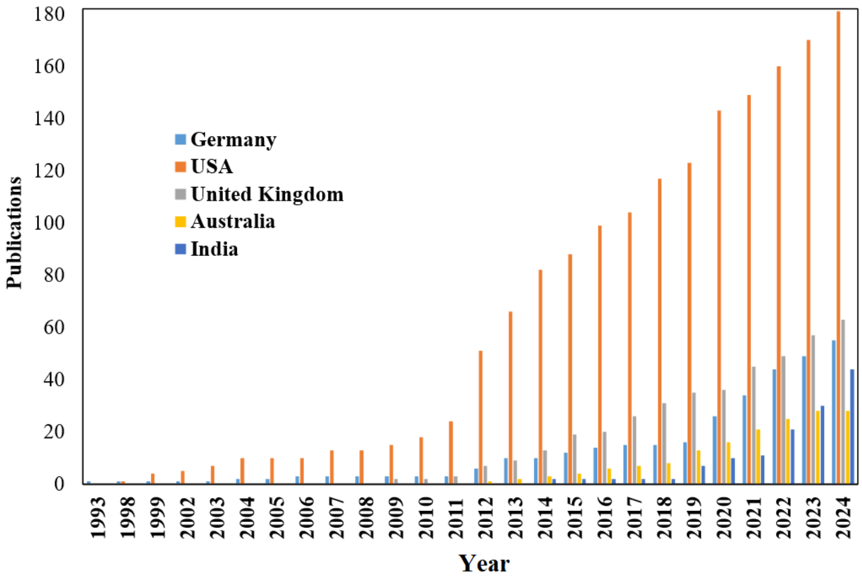


Figure 10. Cumulative number of publications per country over time

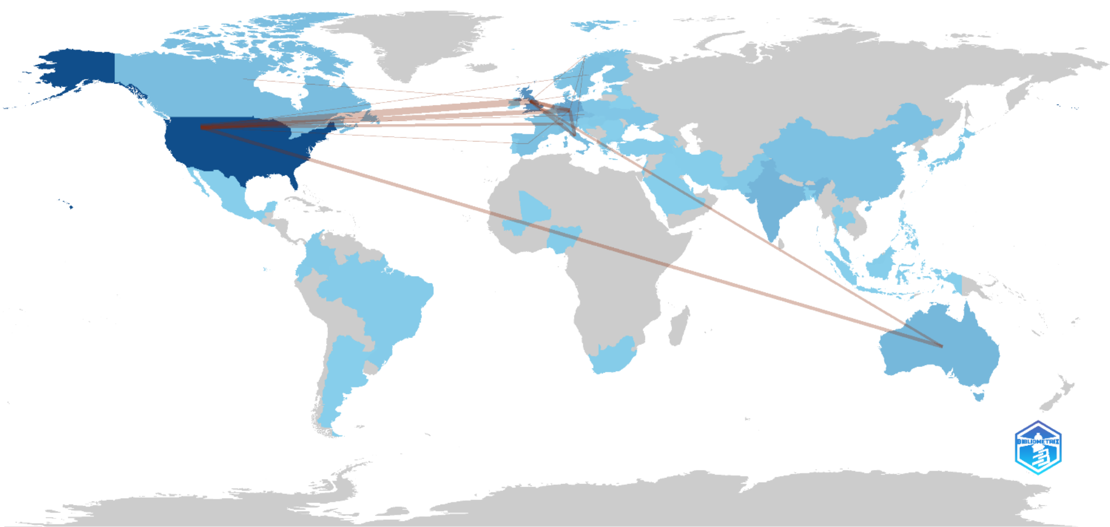


Figure 11. Countries' collaboration network

4. CONCLUSION

Highlighting the impacts of digitalization and artificial intelligence on the human environment during armed conflicts has been presented through a bibliometric analysis. The bibliometric analysis spans from 1993 to 2024, capturing 544 documents with an annual growth rate of 12.73%. The single-authored documents represent around 54.8% of the total number of publications. This tendency toward single-authored publications and limited international collaboration can be attributed to the confidentiality and sensitivity inherent in research related to digitalization, artificial intelligence (AI), and cyber warfare in armed conflicts. The strategic nature of these topics often necessitates restricted sharing of research findings, resulting in more isolated academic efforts. Based on the obtained data by Scopus, the most related subject area was Social Sciences, with 32%, reflecting a significant focus on the societal, political, and ethical implications of these technologies in conflict scenarios. Computer Science, with 25 %, underscores the technical and computational aspects crucial for understanding and developing digital and AI tools in such contexts. Compared with most of the literature reviews in the field, such as those focusing on AI in warfare, digital transformation in crisis response, or cybersecurity in conflict zones, this study provides insights by revealing the distribution structure of literature, the collaboration relationship and the dynamic change of research trends with a transparent, repeatable and objective procedure.

While this study provides valuable insights, it also faces certain limitations. The bibliometric data was sourced solely from the Scopus database, and although it is extensive, it may overlook relevant publications from other indexing platforms. Moreover, the quantitative nature of bibliometric analysis limits deeper exploration of the contextual and qualitative aspects of individual studies. Despite these constraints, the findings reveal a growing research interest in the intersection of digital technologies and conflict, emphasizing the urgent need for ethical frameworks and robust policy development to guide the application of AI in sensitive and high-stakes environments. Further integration of AI technologies in conflict resolution and optimizing digital tools for humanitarian aid during crises can be considered in future research.

ACKNOWLEDGEMENT

The authors extend their appreciation to Prince Sattam bin Abdulaziz University.

FUNDING INFORMATION

The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2024/01/30643).

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Hegazy Rezk	✓	✓			✓			✓	✓	✓				
Montaser Mahmoud	✓	✓	✓	✓	✓		✓		✓	✓	✓			

C : **C**onceptualization	I : **I**nvestigation	Vi : **Vi**sualization
M : **M**ethodology	R : **R**esources	Su : **Su**pervision
So : **So**ftware	D : **D**ata Curation	P : **P**roject administration
Va : **Va**lidation	O : Writing - **O**riginal Draft	Fu : **Fu**nding acquisition
Fo : **Fo**rmal analysis	E : Writing - Review & **E**diting	

REFERENCES

[1] S. Gates, H. Hegre, H. M. Nygård, and H. Strand, "Development consequences of armed conflict," *World Development*, vol. 40, no. 9, pp. 1713–1722, Sep. 2012, doi: 10.1016/j.worlddev.2012.04.031.
[2] S. Garry and F. Checchi, "Erratum to armed conflict and public health: into the 21st century," *Journal of Public Health*, vol. 43, no. 1, pp. e110–e110, Apr. 2021, doi: 10.1093/pubmed/fdaa036.
[3] A. Dienelt, *Armed conflicts and the environment*. Springer, 2022.
[4] N. P. Gleditsch, Nils Petter Gleditsch: Pioneer in the analysis of war and peace, vol. 29. Cham: Springer International Publishing, 2015, doi: 10.1007/978-3-319-03820-9.
[5] H. Lahmann, "The future digital battlefield and challenges for humanitarian protection: a primer," *SSRN Electronic Journal*, 2022, doi: 10.2139/ssrn.4088521.
[6] M. Riahi Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: detection, countermeasure, and future

research directions," *Computers & Security*, vol. 85, pp. 386–401, Aug. 2019, doi: 10.1016/j.cose.2019.05.003.

[7] M. Saaida, "The use of cyber warfare and its impact on international security," *Science for All Publications*, vol. 1, no. 1, pp. 1–5, 2023, doi: 10.5281/zenodo.10841886.

[8] A. Z. Isiksal, "Testing the effect of sustainable energy and military expenses on environmental degradation: evidence from the states with the highest military expenses," *Environmental Science and Pollution Research*, vol. 28, no. 16, pp. 20487–20498, Apr. 2021, doi: 10.1007/s11356-020-11735-7.

[9] A. King, "Digital targeting: artificial intelligence, data, and military intelligence," *Journal of Global Security Studies*, vol. 9, no. 2, Mar. 2024, doi: 10.1093/jogss/ogae009.

[10] R. Fanni and F. Giancotti, "Ethical artificial intelligence in the Italian defence: a case study," *Digital Society*, vol. 2, no. 2, p. 29, Aug. 2023, doi: 10.1007/s44206-023-00056-0.

[11] Z. Stanley-Lockman, "Responsible and Ethical Military AI," *Center for Security and Emerging Technology*, Aug. 2021, doi: 10.51593/20200091.

[12] S. M. Pedron and J. de A. da Cruz, "The future of wars: artificial intelligence (AI) and lethal autonomous weapon systems (LAWS)," *International Journal of Security Studies*, vol. 2, no. 1, pp. 1–28, 2020.

[13] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: literature review and future research directions," *Information Fusion*, vol. 97, p. 101804, Sep. 2023, doi: 10.1016/j.inffus.2023.101804.

[14] I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial intelligence for cybersecurity: a systematic mapping of literature," *IEEE Access*, vol. 8, pp. 146598–146612, 2020, doi: 10.1109/ACCESS.2020.3013145.

[15] B. K. Reddy, N. C. Giri, P. K. Yemula, E. B. Agyekum, and Y. Arya, "Optimal operation of cogeneration power plant integrated with solar photovoltaics using DLS-WMA and ANN," *International Journal of Energy Research*, vol. 2024, no. 1, Jan. 2024, doi: 10.1155/2024/5562804.

[16] C. H. Heller, "Near-term applications of artificial intelligence," *Naval War College Review*, vol. 72, no. 4, pp. 73–100, 2019.

[17] P. Sharma, K. K. Sarma, and N. E. Mastorakis, "Artificial intelligence aided electronic warfare systems- recent trends and evolving applications," *IEEE Access*, vol. 8, pp. 224761–224780, 2020, doi: 10.1109/ACCESS.2020.3044453.

[18] Y. Zhang, Z. Dai, L. Zhang, Z. Wang, L. Chen, and Y. Zhou, "Application of artificial intelligence in military: from projects view," in *2020 6th International Conference on Big Data and Information Analytics (BigDIA)*, IEEE, Dec. 2020, pp. 113–116, doi: 10.1109/BigDIA51454.2020.00026.

[19] S. Das, A. K. Balmiki, and N. C. Giri, "Artificial intelligence enables agile software development life cycle," in *Agile Software Development*, Wiley, 2023, pp. 325–343, doi: 10.1002/9781119896838.ch17.

[20] S. Sachdev, J. Macwan, C. Patel, and N. Doshi, "Voice-controlled autonomous vehicle using IoT," *Procedia Computer Science*, vol. 160, pp. 712–717, 2019, doi: 10.1016/j.procs.2019.11.022.

[21] X. Du-Harpur, F. M. Watt, N. M. Luscombe, and M. D. Lynch, "What is AI? applications of artificial intelligence to dermatology," *British Journal of Dermatology*, vol. 183, no. 3, pp. 423–430, Sep. 2020, doi: 10.1111/bjd.18880.

[22] A. Rashid, A. K. Kausik, A. Al Hassan Sunny, and M. H. Bappy, "Artificial intelligence in the military: an overview of the capabilities, applications, and challenges," *International Journal of Intelligent Systems*, vol. 2023, no. 1, Jan. 2023, doi: 10.1155/2023/8676366.

[23] A. Brisson *et al.*, "Artificial intelligence and personalization opportunities for serious games," *Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment*, vol. 8, no. 5, pp. 51–57, Jun. 2021, doi: 10.1609/aiide.v8i5.12576.

[24] H.-M. Chuang and D.-W. Cheng, "Conversational AI over military scenarios using intent detection and response generation," *Applied Sciences*, vol. 12, no. 5, p. 2494, Feb. 2022, doi: 10.3390/app12052494.

[25] P. Pradhan and A. Satapathy, "Physico-mechanical characterization and thermal property evaluation of polyester composites filled with walnut shell powder," *Polymers and Polymer Composites*, vol. 30, Jan. 2022, doi: 10.1177/09673911221077808.

[26] J. Dalzochio *et al.*, "Predictive maintenance in the military domain: a systematic review of the literature," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–30, Dec. 2023, doi: 10.1145/3586100.

[27] P. Scharre, *Army of none: autonomous weapons and the future of war*. WW Norton & Company, 2018.

[28] K. Qian, C. Liu, B. Yang, and J. Wang, "Hyperpersonalized UAV intelligence based on machine learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, 2021, doi: 10.1109/TITS.2021.3092829.

[29] S. Dai *et al.*, "Recognition of peat depositional environments in coal: a review," *International Journal of Coal Geology*, vol. 219, p. 103383, Feb. 2020, doi: 10.1016/j.coal.2019.103383.

[30] O. Gillath, T. Ai, M. S. Branicky, S. Keshmiri, R. B. Davison, and R. Spaulding, "Attachment and trust in artificial intelligence," *Computers in Human Behavior*, vol. 115, p. 106607, Feb. 2021, doi: 10.1016/j.chb.2020.106607.

[31] M. Taddeo, D. McNeish, A. Blanchard, and E. Edgar, "Ethical principles for artificial intelligence in national defence," *Philosophy & Technology*, vol. 34, no. 4, pp. 1707–1729, Dec. 2021, doi: 10.1007/s13347-021-00482-3.

[32] S. Khan, M. Asjad, and A. Ahmad, "Review of modern optimization techniques," *International Journal of Engineering Research and*, vol. V4, no. 04, Apr. 2015, doi: 10.17577/IJERTV4IS041129.

[33] R. Sureban, V. N. Kulkarni, and V. N. Gaitonde, "Modern optimization techniques for advanced machining processes – a review," *Materials Today: Proceedings*, vol. 18, pp. 3034–3042, 2019, doi: 10.1016/j.matpr.2019.07.175.

[34] K. Lange, E. C. Chi, and H. Zhou, "A brief survey of modern optimization for statisticians," *International Statistical Review*, vol. 82, no. 1, pp. 46–70, Apr. 2014, doi: 10.1111/insr.12022.

[35] X.-S. Yang, "Metaheuristic optimization: algorithm analysis and open problems," in *10th International symposium on experimental algorithms*, 2011, pp. 21–32, doi: 10.1007/978-3-642-20662-7_2.

[36] N. Khanduja and B. Bhushan, "Recent advances and application of metaheuristic algorithms: a survey (2014--2020)," *Metaheuristic and evolutionary computation: algorithms and applications*, pp. 207–228, 2020.

[37] S. Bubeck, "Convex optimization: algorithms and complexity," *Foundations and Trends® in Machine Learning*, vol. 8, no. 3–4, pp. 231–357, 2015, doi: 10.1561/2200000050.

[38] R. Toscano, "Stochastic Optimization Methods," in *Solving Optimization Problems with the Heuristic Kalman Algorithm: New Stochastic Methods*, Springer, 2024, pp. 21–45.

[39] L. A. Hannah, "Stochastic optimization," *International Encyclopedia of the Social \& Behavioral Sciences*, vol. 2, pp. 473–481, 2015.

[40] I. Loshchilov and F. Hutter, "SGDR: stochastic gradient descent with warm restarts," in *ICLR 2017*, 2017.

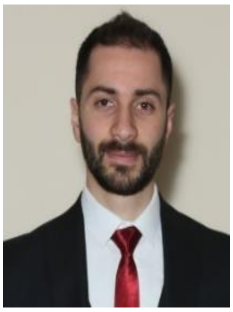
[41] K. R. Harrison *et al.*, "Portfolio optimization for defence applications," *IEEE Access*, vol. 8, pp. 60152–60178, 2020, doi: 10.1109/ACCESS.2020.2983141.

[42] J. Periaux, F. Gonzalez, and D. S. C. Lee, *Evolutionary optimization and game strategies for advanced multi-disciplinary design*, vol. 75. in Intelligent Systems, Control and Automation: Science and Engineering, vol. 75. Dordrecht: Springer Netherlands, 2015, doi: 10.1007/978-94-017-9520-3.

[43] I. M. Ali, H. H. Turan, and S. Elsawah, "A military fleet mix problem for high-valued defense assets: a simulation-based optimization approach," *Expert Systems with Applications*, vol. 213, p. 118964, Mar. 2023, doi: 10.1016/j.eswa.2022.118964.
[44] N. D. Bastian and M. D. Dinmore, "Military and security applications: cybersecurity," in *Encyclopedia of Optimization*, Cham: Springer International Publishing, 2023, pp. 1–10, doi: 10.1007/978-3-030-54621-2_761-1.

BIOGRAPHIES OF AUTHORS

Hegazy Rezk received the B.Eng. and M.Eng. degrees in electrical engineering from Minia University, Egypt, in 2001 and 2006, respectively, and the Ph.D. degree from the Moscow Power Engineering Institute, Moscow. He is currently an associate professor with the department of electrical engineering, collage of engineering in Wadi Addawasir, Prince Sattam bin Abdulaziz University, Saudi Arabia. He has authored more than 200 technical articles. His current research interests include renewable and sustainable energy, energy management, energy efficiency modern optimization algorithms, and modeling based on artificial intelligence. He can be contacted at email: hr.hussien@psau.edu.sa.



Montaser Mahmoud is a post-doctoral researcher at the University of Sharjah (UoS) in the Sustainable Energy and Power Systems Research Centre. He got his PhD in mechanical engineering from City University of London, United Kingdom, in 2022, following a BSc and MSc in mechanical engineering from the Lebanese International University in 2015 and 2017, respectively. His research interests include renewable energy, energy storage systems, energy management, and hybrid energy systems. He can be contacted at email: montaser.mahmoud@sharjah.ac.ae.