International Journal of Law in Changing World

Volume 2 Issue 2 (2023) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v2i2.63

ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY: PERSPECTIVE OF THE GLOBAL SOUTH

Kushal Srivastava
Rashtriya Raksha University, Gujarat, India

Article Information:

Received
July 19, 2023
Approved
July 29, 2023
Accepted
November 27, 2023
Published
December 29, 2023

Keywords:

artificial intelligence,
global south,
internal security,
human rights,
cyber security

ABSTRACT

More than six decades since its inception, Artificial Intelligence (AI) stands at the cusp of a transformative shift. The global perspective on AI has evolved optimistically, as it increasingly permeates every facet of human life. AI is revolutionizing national security strategies and capabilities worldwide, but its impact on the Global South remains a topic of growing significance and concern. Every nation actively seeks to bolster internal security through AI-driven initiatives, including surveillance, cyber security, and autonomous technologies. This review paper delves into AI's role in analyzing vast datasets, uncovering patterns, and identifying security threats and challenges focusing specifically on the Global South. It considers the potential advantages AI offers in enhancing national security capabilities while addressing concerns surrounding its integration. Drawing from existing literature, it presents a comprehensive analysis of AI's prospective future in the cyber and national security domains within these nations. Ultimately, this paper aims to answer whether AI serves as a facilitator in strengthening internal security or poses unforeseen challenges and raises the importance of capacity-building, technology transfer, and international cooperation. It provides valuable insights into the evolving landscape of AI in the context of national security in the Global South.

FOR CITATION:

Srivastava, K. (2023). Artificial Intelligence and National Security: Perspective of the Global South. International Journal of Law in Changing World, 2 (2), 77-87.
DOI: https://doi.org/10.54934/ijlcw.v2i2.63

1. INTRODUCTION

It has been more than sixty years since the concept of Artificial Intelligence ("AI") took its initial form. Since then, there have been several discussions and debates on AI, its future as the focal point, and its potential for a paradigm shift. In an era defined by technological advancement and interconnected global dynamics, the utilization of AI has emerged as a pivotal and transformative force within the realm of national security. The amalgamation of AI's cognitive capabilities and data processing efficiency has ushered in a new era of strategic possibilities, enabling governments and security agencies to elevate their efforts in safeguarding integrity, sovereignty, and peace within the nations. It has the potential and capability to proactively detect threats, and work towards robust cyber resilience, intelligent surveillance, comprehensive data analysis, and informed decision-making. Though the potential of AI in national security is undeniable, it is accompanied by a nuanced landscape of ethical considerations and policy implications [2] [3] [7]. These scenarios advocate for a balanced approach towards imperatives of security and civil liberties, privacy, and human rights. Thus, as we navigate this uncharted territory, the incorporation of AI into national security endeavors compels us to reflect not only on the immense potential it offers but also on the ethical boundaries it prompts us to define.

In addition, such voices intensify when this aspect is evaluated from the perspective of the global south. The contemporary developments within the countries of the global south depict an ongoing challenge that underscores the need for robust governance frameworks and responsible deployment practices. Countries of the global south have been working towards strengthening their internal security and ward off every possible hurdle. The significance of national security in the global south is a multifaceted and profound consideration, deeply rooted in historical legacies, contemporary challenges, and the imperatives of sovereignty, development, and well-being. There are historical contexts that demarcate the vital aspect of sovereignty with such countries. The entire global south is characterized by a diverse range of conflicts, including internal strife, ethnic tensions, regional disputes, and transnational threats. Thus, national security efforts play a pivotal role in mitigating such conflicts, fostering stability, and preventing the escalation of violence that can undermine social progress, economic growth, resource management, and human and economic development [10] [4]. Therefore, addressing national security imperatives in the global south demands collaborative efforts, innovative strategies, and a nuanced understanding of the interconnected nature of global security dynamics [11] [6] [8]. This study attempts to analyze the usage of AI as a tool to safeguard the realm of national security within the jurisdiction of the global south. Moreover, it has been witnessed that the countries falling in the domain of the global

https://doi.org/10.54934/ijlcw.v2i2.63

south often navigates complex geopolitical landscapes that depict the existing geopolitical dynamics. In consideration of these facets, connected countries have initiated technological advancements, digital security, development of robust cybersecurity measures, and working towards enhancing their overall capabilities. The importance of national security in the global south transcends mere military concerns to encompass a holistic and comprehensive approach. Ultimately, a secure Global South contributes to the well-being of its nations and the broader goals of global peace, prosperity, and justice. This study also aims at depicting a descriptive approach towards the perspective of the global south and it analyses the entire situation of AI and its prospective future in the cyber security and national security of the connected nations. The discussion also considered the existence of several concerns about the congruence of AI and national security. Through reviewing various existing literature, it projects a discussion and analyzes different pertinent aspects connected to this domain. Eventually; it attempts to put forward suggestions to the question at hand as to whether AI in national security is a facilitator that can help in strengthening the internal security of nations or whether are we overlooking a hurdle that it may entail and is still a far-sighted dream.

2. LITERATURE REVIEW

The Congressional Research Service (CRS) Report titled "Artificial Intelligence and National Security'" (2020) [9] initiated by acknowledging the escalating aspect of AI in terms of its use of technology and analyses the fact that entities like defense personnel, policymakers, investors of various nature have started being attracted to this very aspect. The military of multiple countries is depicting keen interest in such developments. Countries, like the U.S. and China have already begun integrating their AI systems. This report attempts to explain the trajectory of the entire concept by explaining the definition attached to the term AI. There are debates and discussions in the U.S. Congress regarding the usage and future of military AI. The members of Congress have highlighted the importance of executing a road map in this regard and the need to establish commissions and centers that would work to facilitate the transition in terms of AI-based technologies and strengthen AI-enabled operations and other connected systems. Congress is also in continuous debates about policies and laws to regulate these transactions. The report also highlights the aspects of Intelligence, Surveillance, and Reconnaissance and the importance of analyzing these aspects while considering the evolving domain of connected data and other inputs [9] (p.10). It goes on to explain the usage and volume of AI technologies regarding the logistics scenario, command, control, and information and cyberspace operations of the nation. In addition to depicting the

https://doi.org/10.54934/ijlcw.v2i2.63

need for military AI, this report also emphasizes the existing challenges. The entire process and technology involved, and the cultural transition, are not that easy and flexible.

Moreover, there are many international competitors present and functional in this domain who are indulging and analyzing their mediums and calculations towards the development of AI and its connected elements. Thus, it also accepts the reality of challenges and hurdles that are there in the domain of AI within the national security context. The challenges range from the aspect of autonomy, the race for information superiority, the ambit of predictability, the test of speed and endurance, and the possibilities of instances of exploitation [9] (p.30).

In the paper titled “Artificial Intelligence and Security: Transformation and Consistency” (2022), Aleksei Turobov researches the aspect of dynamics of using AI technology in national security. The paper focuses on vital questions revolving around "who", "what", and “how” regarding the expansion of the security domains and connected issues [12] (p.5). There has indeed been research that depicts the paradigm shift in terms of security and AI technologies and how technology plays an important role in the security sphere. This paper has attempted to analyze the various existing literature on security and technological studies. It also points out the existing lacunae in reporting mechanisms and the lack of available information that talks about the actions of nations towards AI and national security. This paper is an attempt made to analyze the infiltration of AI and its technologies into the domain of national security. The author has tried to execute and test an empirical model to understand and analyze the entire system. It’s also evident that the national security realm has deepened with the escalation of relevant digital technologies. Through evidence, it builds a trajectory and linkage between the aspect of security and the advancement of AI technologies [12].

Moreover, the author of this paper has taken various hypotheses, tested them, and commented on their validity. The premise involves aspects like the evaluation of threat, capabilities of threat response, and dynamics of the use of AI technologies in the security domain during the years 2008-2010 and comparing it with the indicators active in the years 2018-2019. A practical understanding of the entire concept has been demarcated through data interpretations. This research paper also demonstrates that countries lack “alarming", “exaggerated fears”, and leniency on technological changes in national security systems. Connected governments execute their own assessment and implementation mechanism to assess the pros and cons of such aspects. Eventually, through this paper, the author has attempted to measure the changes that society has been witnessing in their execution of security operations as and when technology has gone through a transition [12] (p.9).

https://doi.org/10.54934/ijlcw.v2i2.63

In the paper titled "Artificial Intelligence in War: Human Judgment as an organizational strength and a strategic liability" (2020), the authors Avi Goldfarb and Jon Lindsay try to emphasize the potential of AI in terms of changing the nature of war. AI can act as an enhancer regarding military actions toward data collection, analyzing those data, and making decisions based on such analysis. Paper initiates by emphasizing the change like the prediction that has become more accessible and easier with the help of development in the aspect of machine learning. The authors have divided the entire discussion into four different parts and have debated how added AI technologies have assisted in human decisions and judgments [5] (p. 7). However, a lack of understanding and reasoning of actions within technologies, gives way to the possibility of errors. Thus, it majorly depends on the genuine and sufficient nature of the data that is fed into some particular technologies whose assistance is sought for various endeavors. Then they comment on the war scenario and explain that there has been an information revolution that has boosted the awareness level of war and warfare that are intensively based on data, intelligence, and the entire related ecosystem. However, on the other hand, the economic perspective of military affairs cannot be ignored in its entirety. It also highlights many operational challenges that might creep into the system. There is indeed a difference between the theoretical and practical aspects of a given topic, and the organizational challenges in terms of its usage, analysis, and execution are not an exception. The extent of AI-driven technologies does not only depend on the nature of such technologies but also on the ways, such operational technicalities are used. The organizational, political, and strategic implications have their complexities [5] (p. 7). Ultimately, there is indeed space for human acumen to determine what to consider and what not to consider.

In the special report titled "Artificial Intelligence for Defence and Security" (2022), under the Centre for International Governance Innovation, Daniel Araya comments on the revolutionary nature of the advancements in the field of AI [15]. Contemporary security threats have indeed posed a great challenge to military strategies. It studies the actions and endeavors of several vital countries in terms of AI technologies for their security. Countries' regional and trade ambitions or economic ascendance, and everything, are witnessing a paradigm shift due to the overarching presence of a new element in the game i.e., AI and related technologies. In the current scenario, the strategic arena that a particular nation wants to delve into depends on the application of technologies and their nature. Some strategic giants are working with a motive to transform the entire digital ecosystem. Canada, for instance, has a vital and strong AI talent pool. AI is that prominent subset that includes both the development of machine learning and deep learning [15] (p.8). It also focuses on the importance of coordination among entities. Any automated weapons, some technology-driven strategic operations, complex military networks, or satellite

https://doi.org/10.54934/ijlcw.v2i2.63

applications, every such element needs appropriate coordination for error-free execution and to achieve the desired output. The report also entails a discussion on the importance of cyber security and AI. The data-driven economy has many tedious tasks for any act that revolves around AI and cyber security. When we talk about and debate these two elements, the importance of decentralization in terms of federal data governance is vital. The report also provides recommendations about the transformation of the entire digital infrastructure. Eventually, it projects the importance of collaboration between the industry and the government of the concerned nation for better results. It suggests for countries like Canada that more change is required to enhance military capabilities by tapping the data as per the need and usage. Since this report result from a workshop, it witnessed several vital discussions like the quality assessment of data, the need for military planning, and the execution of an analytical framework [15] (p.8).

In the paper titled "AI and National Security: Major Power Perspectives and Challenges" (2022), Sanur Sharma analyses the postulates of AI and National Security by considering the development of significant economies of the world in this regard. The author, through this paper, has tried to project the fact that AI is more of an enabler of technologies and not a mere technology per se. Private and public sectors have indeed increased their dependency on the domain of AI. Be it-structured flow of data, its appropriate, and cost-effective storage or capable and relevant algorithms are now much more accessible with the help of AI and can challenge human intelligence at different stages. An attempt is made to establish the linkage between the National Security of a country and AI. It also analyses the development with a special focus on the military domain. Another vital part of the paper comments on and analyses the emerging powers of the globe ranging from the USA, China, and India. It analyses the entire trajectory of these three nations regarding their security strategies, and defense plans to keep AI and connected technologies as the focal point. For instance, these countries have been allocating budgets with specific objectives to meet such demands of AI with national security. A country like China has released detailed plans and goals to meet by 2030. Such techniques have AI at their core [13] (p.6). Another facet of the paper acknowledges the regulatory and ethical challenges that are real and evident on the road to meeting such goals. Changing landscape of security and strategy has hidden hurdles that a nation is bound to face while chalking out its course of action. The instances of misuse of such endeavors at the hand of non-state actors cannot be ignored. Ultimately, this paper analyses the threats standing at the door and focuses on the need for countries to keep an eye on such instances [13].

https://doi.org/10.54934/ijlcw.v2i2.63

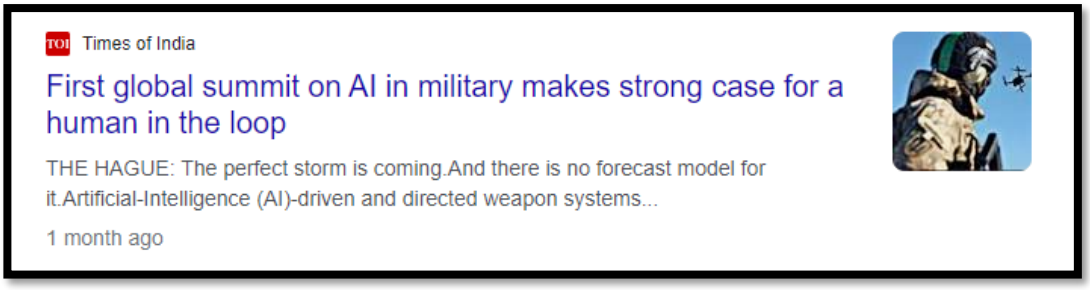
3. DISCUSSION

The interplay of AI and National Security has gained momentum in contemporary times. Several facets are vital to be tabled for discussion and can assist in bringing in a paradigm shift within the ongoing debates both nationally and internationally.

The domain of Military AI

The most significant aspect of AI is to talk about its development regarding the defense of a particular nation. There has been much discussion on the potential that AI holds and its capability to transform the entire defense structure of the country. The military of various countries has opened up and is welcoming AI-based technologies [1]. There is indeed a difference between the theoretical and practical aspects of a given topic, and the organizational challenges in terms of its usage, analysis, and execution are not an exception. The importance of human presence cannot be ignored or replaced. If military AI has to see an escalating trajectory, then such AI-driven technologies cannot depend only on the nature of such technologies but also on the usage of such operational technicalities. In the domain of the military, the organizational, political, and strategic implications have their complexities, and if, AI is to cover the significant aspect, then one has to take note of such complex scenarios. Following is an excerpt from the news that acknowledges that when countries think and debate about military AI, human presence cannot be excluded. This convergence aims to enhance the capabilities and effectiveness of armed forces by leveraging advanced computational techniques and autonomous systems. Military AI encompasses a range of applications, each contributing to the modernization and efficiency of military endeavors. Therefore, AI within the military can bolster and strengthen the domain of cybersecurity, training, simulation, and logistics optimization. The domain of military AI also envisages the facet of ethical considerations, international laws, and accountability for AI-driven actions. Thus, such an element represents the synergy between artificial intelligence and military operations. It drives innovation, efficiency, and effectiveness within the armed forces while necessitating careful deliberation on ethical and legal implications. Responsible integration of Military AI is crucial for maintaining security, stability, and ethical conduct in an evolving technological landscape.

https://doi.org/10.54934/ijlcw.v2i2.63



(Fig. 1.1) (Mund, 2023)

Importance of Collaboration

When we talk about and debate these two vital elements of Military and AI, the importance of decentralization in terms of federal data governance is essential too. It means that there will be hurdles in execution if it goes through checks and balances at different levels. The existing literature gives way to the importance of collaboration between the industries, the government of the concerned nation, and other institutional actors. Such collaborations can only help in achieving the goal that is sought after. If there is consensus and cooperation between entities, it becomes accessible to debate, discussion, research, and talk on solutions towards appropriate governance of AI.

The Perspective of the Global South

Another pertinent element in the discussion of AI and national security is to see the entire trajectory from the perspective of the global south. With the above discussion, it is evident that AI has the potential to transform the military and security landscape of the nations and change the entire nature of the battlefields and thus act as an essential aspect in the domain of national security. In contemporary times, countries of the global south, especially India and China, have emerging countries that are developing and planning security strategies for their citizens. The defense planning and the budget deliberations of recent times are thought upon and executed while keeping AI and connected technologies as the focal point. Countries of the global south are indulging in target-oriented activities and are pretty proactive when it comes to strengthening their internal security, and countries try to ward off hurdles and mitigate them to a great extent in every possible way. In light of the development and increase in the usage of AI, it is worth pondering on the future of AI in the domain of national security from the perspective of the entire domain of the global south. Indeed, every concerned government entity, like the military of such nations, is focusing more on AI-based technologies to enhance their overall capabilities. The significance of national security in the global south is a multifaceted and profound consideration, deeply rooted in historical

https://doi.org/10.54934/ijlcw.v2i2.63

legacies, contemporary challenges, and the imperatives of sovereignty, development, and well-being. The global south is characterized by a diverse range of conflicts, including internal strife, ethnic tensions, and regional disputes. National security efforts play a pivotal role in mitigating such conflicts, fostering stability, and preventing the escalation of violence that can undermine social progress, economic growth, and human development. By addressing the root causes of instability, nations can create an environment conducive to sustainable peace and prosperity. The global south is often disproportionately affected by transnational threats, including terrorism, organized crime, drug trafficking, and human trafficking. Robust national security measures are essential for countering these threats, safeguarding governance structures, and fostering human rights and regional cooperation. The region often navigates complex geopolitical landscapes, marked by shifting alliances, power dynamics, and global interests. Effective national security decisions allow countries to assert strategic influence, negotiate equitable trade agreements, and safeguard regional interests. Furthermore, in an era defined by technological advancements, the global South confronts challenges related to digital security, data privacy, and cyber threats [14]. Ultimately, the importance of national security in the global south transcends mere military concerns to encompass a holistic and comprehensive approach.

Hurdles

Though a lot of discussion has been towards highlighting the potential of AI; however, hurdles in the shape of challenges are the reality. Such, challenges range from the aspect of autonomy, race of information superiority, the ambit of predictability, a test of speed and endurance, and the possibilities of instances of exploitation. In addition to this, there are regulatory and ethical challenges too that are real and evident on the road to meeting such goals. The changing landscape of security and strategy has hidden hurdles that a nation is bound to face while chalking out its course of action. The instances of misuse of such endeavors at the hand of non-state actors cannot be ignored entirely. Moreover, transparency and biases in AI-driven decisions cannot be ignored in their entirety. The probability of vulnerability in terms of privacy issues and cyber-attacks against AI endeavors can have the capability of compromising the national security of a country.

4. CONCLUSION

In contemporary times, we as individuals are witnessing a paradigm shift in the security landscape of the globe, and AI is one major enabler of the same. It will not be wrong to state that if human interpretation meets the appropriate AI interventions, the game can be more reliable and futuristic. One

https://doi.org/10.54934/ijlcw.v2i2.63

needs to accept the fact that today's data is the new oil. There should be well-researched policy documents and regulations in place that would govern the entire transaction happening in this arena. Eventually, the aspect of national security is indeed susceptible to a nation; therefore, nations should analyze the potential of AI towards national security not in haste but in a holistic manner. Nations can create an environment conducive to sustainable peace, prosperity, and unlock their economic potential and uplift their populations through improved living standards and human security. Diplomatic endeavors using AI within the military domain can aim at conflict prevention and resolution and contribute to maintaining stability and global security.

REFERENCES

[1] Agrawal, G, Goldfarb, B. (2020) "How Adversarial Attacks Could Destabilize Military AI Systems," IEEE Spectrum, February 26, 2020. https://spectrum.ieee.org/automaton/artificial-intelligence/embedded-ai/adversarial-attacks-and-ai-systems

[2] Briscoe, E., Fairbanks, J. (2020) "Artificial Scientific Intelligence and its impact on National Security and Foreign Policy," Journal of World Affairs, vol. 64, no. 4, 544-554. https://doi.org/10.1016/j.orbis.2020.08.004

[3] Cyman, D., Gromova, E., Juchnevicius, E. (2021) Regulation of Artificial Intelligence in BRICS and the European Union. BRICS Law Journal, 8(1), 86-115. https://doi.org/10.21684/2412-2343-2021-8-1-86-115

[4] Ferreira, D.B., Giovannini, C., Gromova, E.A, Ferreira, J.B. (2023) Arbitration chambers and technology: witness tampering and perceived effectiveness in videoconferenced dispute resolution proceedings International Journal of Law and Information Technology, Volume 31, Issue 1, 75–90, https://doi.org/10.1093/ijlit/eaad012

[5] Goldfarb, A., Lindsay, J. (2022) "Artificial Intelligence in war: Human judgment as an organizational strength and a strategic liability, 1-12. https://www.brookings.edu/wp-content/uploads/2020/11/fp_20201130_artificial_intelligence_in_war.pdf

[6] Gromova, E.A., Petrenko, S.A. (2023) Quantum Law: The Beginning. Journal of Digital Technologies and Law, 1(1), 62-88. https://doi.org/10.21202/jdtl.2023.3.

[7] Gromova, E., Ferreira, D.B. (2023) Guest Editors' Note on Law and Digital Technologies: The Way Forward. BRICS Law Journal.10 (1), 5-6. https://doi.org/10.21684/2412-2343-2023-10-1-5-6

[8] Gromova, E., Ivanc, T. (2020) Regulatory Sandboxes (Experimental Legal Regimes) for Digital Innovations in BRICS. BRICS Law Journal. 7(2), 10-36. https://doi.org/10.21684/2412-2343-2020-7-2-10-36

[9] Hoadley, D.S., Sayler, K.M. (2020) "Artificial Intelligence and National Security," Congressional Research Service Report, 1-47. https://sgp.fas.org/crs/natsec/R45178.pdf

[10] Johnson, J.S. (2020) "Artificial Intelligence: A Threat to Strategic Stability," Strategic Studies Quarterly, vol. 14, no. 1, 16–39. http://dx.doi.org/10.2307/26891882

[11] Kania, E.B. (2019) "Chinese Military Innovation in the AI Revolution," RUSI Journal 164, no. 5–6, 26–34. https://doi.org/10.1080/03071847.2019.1693803

[12] Turobov, A. (2022) "Artificial Intelligence and Security: Transformation and Consistency," https://wp.hse.ru/data/2022/06/14/1855772364/88PS2022.pdf

[13] Sharma, S. (2022) "AI and National Security: Major Power Perspectives and Challenges", Manohar Parrikar Institute for Defence Studies and Analysis, https://idsa.in/issuebrief/ai-and-national-security-ssharma-120922.

[14] Zhang, Yi, Wu, M., Yijun Tian, G., Zhang, G., Jie L. (2021) "Ethics and privacy of artificial intelligence: Understandings from bibliometrics," Knowledge-Based Systems, Vol. 222, https://doi.org/10.1016/j.knosys.2021.106994

[15] Araya D. (2022) "Artificial Intelligence for Defence and Security, Special Report Centre for International Governance Innovation, 2022. https://www.cigionline.org/static/documents/Araya_AI-for-Defence_SpecialReport_Q4fjNfp.pdf

ABOUT THE AUTHOR

Kushal Srivastava
PhD Scholar and Research Associate (Legal) at Rashtriya Raksha University (An Institution of National Importance), Gujarat, India.
e-mail: kushal.srivastava010@gmail.com
ORCID ID: https://orcid.org/0000-0001-6719-9390
Google Scholar ID:
https://scholar.google.com/citations?hl=en&user=ejpyJsQAAAAJ

ABOUT THIS ARTICLE

Conflict of interests: Author declares no conflicting interests.