Methodological Concepts of Appling AI into Military and Economic Capabilities Data Analysis

Vadym PAKHOLCHUK[1], Kira HORIACHEVA[1*]

[1] Military Institute of Taras Shevchenko National University of Kyiv, Yulii Zdanovskoi St., 81,03189, Kyiv, Ukraine

*Correspondence: *horyachevakira@gmail.com*

Abstract

This paper explores the strategic application of Artificial Intelligence (AI) in enhancing military and economic capabilities. Utilizing a systematic and comparative methodology, this study assesses the potential and challenges of AI technologies, including Large Language Models (LLMs) and their impact on defense and economic sectors. Data from authoritative sources like the United Nations and various strategic studies institutes underpin a comprehensive analysis. Key findings demonstrate that AI significantly advances military efficiency and economic forecasting, akin to its transformative potential observed in digital marketing and cyber defense. The study underscores the necessity for ethical guidelines and robust validation to mitigate AI's inherent biases and misuse. This research not only reaffirms AI's pivotal role in modern strategic contexts but also emphasizes the need for continuous innovation and ethical oversight in its deployment.

KEY WORDS: *military capabilities; economic capabilities; artificial intelligence (AI); large language models (LLM); defence.*

Citation: Pakholchuk, V., Horiacheva, K. (2024). Methodological Concepts of Appling AI into Military and Economic Capabilities Data Analysis. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.25

2. Introduction

A range of studies have explored the use of AI in defense, intelligence, and economic data analysis. According to Atif (2021) AI has potential benefits in military applications, HRMS, decision making, disaster prevention and response, GIS, service personalization, interoperability, extensive data analysis, anomaly and pattern recognition, intrusion detection, and new solution discovery using the highly configurable system and real-time simulation. For example, there is a significant potential for improvement in the effectiveness of special forces and amphibious units through the use of artificial intelligence. The role of artificial intelligence in conventional weapons as a factor in strategic deterrence and nuclear weapons, accelerating the innovation race. As a result, the strategic importance of artificial intelligence as a project of the future, with a comparison to the nuclear race of the mid-twentieth century. However, it is noted that only certain tasks have been solved on data analysis and pattern recognition, text translation. The pivotal role of the AI in in military strength evaluation and national security was emphasized by Utsav (2023).

Truong (2020) conduct a survey of the applications of AI for cybersecurity, discussion on potential security threats from adversarial uses of AI technologies, and the identification of potential research challenges and open research directions of AI in cybersecurity. Leenen (2021) emphasizes the potential of AI and big data analytics in cyber defense, particularly in detecting patterns and correlations in security event data. Big data analytics and artificial intelligence have the potential to enhance cyber defense. Current automated systems based on syntactic rules may not be sophisticated enough to handle the complexity in the cyber defense domain.

Damaševičius (2023) provides a comprehensive overview of AI's impact on various fields, including economics, finance, and innovation. This is further supported by Ruiz-Real (2020), who identifies AI's role in business and economics, particularly in digital marketing and decision making. These studies collectively highlight the transformative potential of AI in these domains, from enhancing forecasting techniques to improving cybersecurity and business operations. Taylor (2019) found that AI-enabled systems enhance defense capabilities, the challenges in acquiring such systems for governmental

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

defense, and the need to recognize the misalignment of AI procurement with established procurement elements. According to Ramirez (2020) artificial intelligence methods used to predict economic indicators are artificial neural networks, adaptive systems of diffuse neuro inference, genetic programming, support vector regression, machines extreme learning and other machine learning techniques. One of the most promising AI technologies is LLMs. Despite the fact that it is very difficult to monitor developing new models and architectures, the vast majority of the principles remain the same.

2. Investigation Results

To determine the potential consequences of the use of AI for military and economic capabilities assessment we used a systematic approach. Its components were used as a methodological basis, which made it possible to present a holistic vision of the system architecture of capabilities analysis.

The comparative method allowed authors to compare the potential of different instruments and models that were developed in the area of LLM, and to assess the possible consequences of using them. The basis of the work was the data from different sources: the United Nations (UNROCA), Stochholm International Institute of Peace Research (SIPRI), International Institute of Strategic Studies and Statista. By integrating these approaches and data sources, the study not only underscored the transformative potential of AI in enhancing strategic capabilities but also highlighted the critical need for careful and contextual application of these technologies to avoid unintended consequences.

During the development of necessary architecture, we started from interviewing practioners in defense industry to create the list of requirements for our project. It was necessary to construct a system that could work completely on offline network or locally on only one machine. This could give us a possibility to work with sensitive information. The other consideration was about incorporation of users' metadata to restrict their access according to the privilege level. In our case we tested only local models on CPU/GPU which could be loaded into RAM. The increasing complexity of military operations necessitates robust and secure data management systems. In the modern strategic context, the application of AI into the assessment of military and economic capabilities presents both transformative potential and complex challenges.

Our experimental setup involved interviewing practitioners in the defense industry to tailor AI systems to actual operational needs. This was crucial to ensure that our architecture could operate robustly in sensitive environments, disconnected from any network, hence safeguarding against cyber threats. These findings resonate with Truong et al. (2020) who discuss the dual-edged nature of AI in cybersecurity, stressing both its potential in fortifying cyber defenses and its vulnerabilities to adversarial attacks. To address this, we have developed an architecture designed specifically for data exchange within the defense industry, capable of operating entirely offline at the local level.

This architecture encompasses several critical components, each interlinked to ensure secure, efficient, and rapid data processing and retrieval. The resulting schema is presented in Fig. 1.

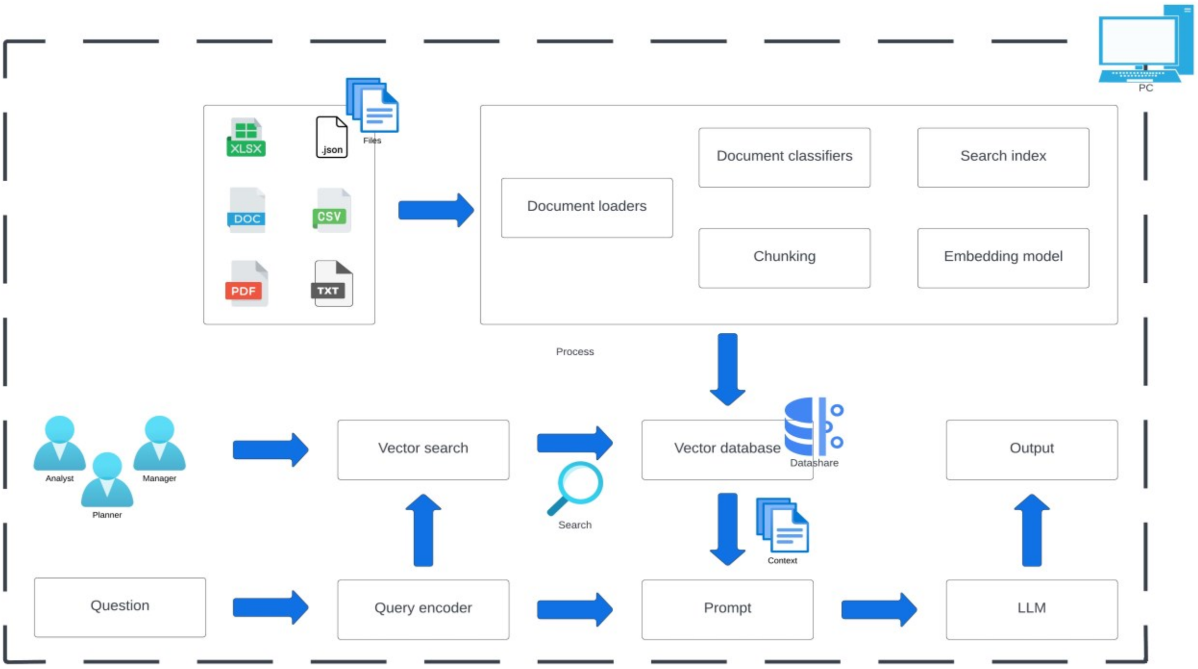

Fig. 1 The architecture of data exchange in defense industry based on offline network at the local level

Fig. 1 illustrates the architecture of data exchange in the defense industry, designed to operate within an offline network at a local level. The diagram shows a multi-layered network structure, emphasizing robust security protocols and isolated data handling mechanisms to ensure secure data flow without external connectivity. This architecture supports localized decision-making and maintains high data integrity and security, crucial for sensitive military environments.

The system is designed to cater to three primary user roles: Analysts, Managers, and Planners. Each role has tailored access to the system, ensuring that users can efficiently perform their specific operational tasks. Analysts are primarily engaged with data analysis, Managers oversee operational integrity, and Planners use the data for strategic decision-making.

Data enters the system through Files, which consist of various documents and data feeds. These are first processed by Document Loaders, which upload and store data within the system. Subsequently, Document Classifiers categorize the uploaded data into relevant groups for easier accessibility. The Chunking process then breaks down large files into smaller segments, enhancing the manageability of data. This processed data is indexed by the Search Index for quick retrieval and further encoded into vectors by the Embedding Model, which facilitates advanced data retrieval techniques based on semantic content.

The core of the system's interactivity with users is the Query process. Users input Questions, which are transformed by the Query Encoder into vector forms. These vectors are used to conduct searches within the Vector Database, which stores all encoded data. The Vector Search mechanism identifies and retrieves the vectors most relevant to the query, ensuring that users receive the most pertinent information.

LLMs are trained on large volumes of text, typically billions of words, that are simulated or taken from public or private data collections. This enables them to interpret textual inputs and generate human-like textual outputs. LLMs already help search engines understand a question and formulate an answer. Breakthroughs in the LLM field have the potential to drastically change the way organizations conduct military and economic capabilities, including enabling the automation of tasks previously done by humans, from generating code to answering questions. A key feature of this architecture is the integration of LLM. The LLM processes Prompts, which are refined queries formulated based on user Questions and the results of the Vector Search. It synthesizes information from the Vector Database to generate Outputs that are contextually relevant and insightful.

The final Output from the LLM is presented back to the users, providing them with actionable insights and answers to their queries. This Output can influence subsequent user interactions with the system, as users refine their questions based on the received information, creating a dynamic and iterative process of inquiry and analysis.

Further, our analysis identified the necessity for AI systems to incorporate user metadata effectively to adjust access based on privilege levels—a critical factor in maintaining data integrity and operational security. This aspect of data management and classification draws parallels with Leenen and Meyer (2021) who advocate for the integration of big data analytics and AI to detect patterns and correlations in security event data, significantly boosting cyber defense mechanisms.

This detailed breakdown provides a comprehensive understanding of how each component functions within the network and their interdependencies. The deployment of such an architecture allows for the safe handling and processing of sensitive information, mitigating the risks of cyber threats and data breaches. By integrating advanced AI capabilities at the local level, this system enhances real-time analytical processing and decision-making. The figure clearly demonstrates a strategic approach to integrating technology with operational needs, providing a scalable solution that can be adapted for various military applications. The ability to operate independently of a central network reduces latency and increases response efficiency, crucial for operations in remote or sensitive environments.

An important advancement in our study was the application of AI in offline settings, utilizing local models that ensure sensitive data remains within the confines of the intended operational environment. This approach aligns with Taylor (2019) who discusses the challenges governmental bodies face in procuring sophisticated AI systems that comply with established standards yet are agile enough to meet contemporary defense needs.

Our research also highlighted the potential of AI to transform economic analysis, as discussed by Ramirez (2020) who explores various AI methodologies like neural networks and support vector regression in predicting economic indicators. These techniques enable a more nuanced understanding of economic trends, which can be pivotal in strategic planning and resource allocation.

The deployment of the AI-driven architecture we developed signifies a methodological innovation in the use of AI for military and economic capabilities data analysis. It not only enhances real-time analytical processing and decision-making but also ensures the safe handling of sensitive information. This dual capability is crucial in a strategic context where both speed and security are paramount.

The synthesis of AI with traditional data analysis methodologies, as explored in our architecture, offers a comprehensive approach to understanding and leveraging AI's capabilities in military and economic contexts. By integrating cutting-edge technology with rigorous validation processes, we can better anticipate and mitigate the risks associated with AI applications, ensuring they contribute positively to national and economic security.

Overall, the deployment of this AI-enhanced architecture signifies a strategic approach to integrating technology with operational needs, providing a scalable and secure solution adaptable to various military applications. It exemplifies a methodological innovation in the use of AI for military and economic capabilities data analysis, ensuring the safe handling of sensitive information while mitigating the risks associated with cyber threats and data breaches.

The security risks associated with AI technology are profound, especially when applied to strategic military and economic domains. Numerous studies have highlighted a variety of security concerns surrounding AI, encompassing ethical issues, technical vulnerabilities, and data integrity. Given these concerns, it is imperative for government bodies to bolster their support through increased financial investment and the establishment of robust policies. Such measures are vital to foster a conducive environment for the sustainable growth of the AI industry within national security frameworks.

At a technical level, our research emphasizes the necessity of developing AI systems that are not only advanced but also secure from potential cyber threats, a challenge that requires significant investment and innovation. On the matter of data and ethical security, the sensitive nature of the data involved—especially in military applications—demands stringent protection measures. This involves crafting laws that safeguard personal and organizational data privacy without stifling AI innovation.

Our approach advocates for AI systems that respect humanistic values and adhere to ethical guidelines, ensuring that AI operations within the defense sector are conducted responsibly. Efforts must be concentrated on discovering and implementing best practices that enhance the ethical decision-making capabilities of AI systems, thus ensuring that these technologies act in ways that are beneficial to society and aligned with broader strategic objectives.

3. Conclusions

This research demonstrated the potential for AI and advanced computational techniques to transform the analysis of military and economic capabilities. Extending these approaches to broader sectors could accelerate discovery and technology development. The data-driven analysis enabled by large language models points towards new possibilities for recognizing patterns and generating insights from vast troves of unstructured data related to economic and military factors. By training LLMs on domain-specific corpora of reports, research, and policy documents, they can surface non-intuitive relationships from across disciplines. Reinforcement learning further allows optimizing complex decisions and strategies through iterative modeling.

Together, the integration of knowledge-driven AI with rigorous statistical analysis and validation provides a methodology for military and economic analysis superior to either humans or AI alone. This study demonstrated the value of mixing computational and experimental methods in a hybrid intelligence approach. Applied thoughtfully, AI can enhance foresight and quantitative modeling to better inform capability planning and policy.

However, care must be taken to validate AI systems to prevent biases and misuse. Ongoing research should ensure transparency and ethics around military and economic AI applications. Overall, this emerging field promises to transform data-driven anticipation of threats and opportunities in a complex world, if deployed responsibly. For the practitioner sphere, this work provides theoretical basis and guidance to those currently employed in the field, enabling them to quickly seize the unlimited potential of AI in military and economic development. Nonetheless, for researchers working in this field, we outline the profile of each topic area and the research gaps, which will have an important enlightening force and stimulating effect on future research in this field.

References

1. **Ali D.A.** Artificial intelligence potential trends in military. Foundation University Journal of Engineering and Applied Sciences. 2021; 2(1): 20–30.
2. **Gaire U.S.** Application of artificial intelligence in the military: An overview. Unity Journal. 2023; 4(01): 161–174.
3. **Truong T.C., Diep Q.B., Zelinka I.** Artificial intelligence in the cyber domain: Offense and defense. Symmetry. 2020; 12(3), 410.
4. **Leenen L., Meyer T.** Artificial intelligence and big data analytics in support of cyber defense. In Developments in information security and cybernetic wars. IGI Global. 2019; 42–63.
5. **Damasevicius R.** Artificial intelligence techniques in economic analysis. Economic Analysis Letters. 2023; 2(2): 52–59.
6. **Leenen L, Meyer T.** Artificial intelligence and big data analytics in support of cyber defense. In Research anthology on artificial intelligence applications in security. IGI Global. 2021; 1738–1753.
7. **Taylor T.** Artificial intelligence in defence. The RUSI Journal. 2019; 164(5-6): 72–81.
8. **Ramirez K.M., Hormaza J.M., Soto S.V.** Artificial intelligence and its impact on the prediction of economic indicators. In ICEMIS'20: The 6th international conference on engineering & MIS 2020. ACM, 2020.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of CNDCGS 2024 and/or the editor(s). CNDCGS 2024 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.