11. Ustawa z dnia 6 marca 2018r., Prawo przedsiębiorców, art. 3.

O. Osaulenko,
Doctor of Science in Public Administration, Professor,
Academician of the National Academy of Sciences of Ukraine, Rector;
O. Horobets,
PhD in Economics, Associate Professor, Head of the Department of Statistics,
Information Technologies and Mathematical Methods in Economics;
National Academy of Statistics, Accounting and Audit, Kyiv

INNOVATIVE TECHNOLOGIES IN MILITARY ANALYTICS

Ukraine's technological achievements in the context of a full-scale war have already become known worldwide, in particular in terms of unmanned systems, autonomous navigation, situational awareness platforms, geo-analytics, simulation, demining, damage assessment, etc. A special place is occupied by the implementation of artificial intelligence in improving the warfare strategy. An important aspect in this context is the realization that the armed forces use artificial intelligence not to automate weapons, but to process data and enhance military intelligence, and only in some cases to improve military targeting [1]. At the same time, fully autonomous systems that can operate in unpredictable environments with minimal human intervention have not yet materialized on the battlefield.

Implementation of AI technologies on the battlefield requires the development of a complex process in the learning / training / testing of systems with large amounts of data, in which machine learning algorithms analyze large volumes to inform management decisions with the prospect of identifying patterns and creating models capable of predicting or making decisions. Training sets can be formed from structured and unstructured streaming data, which can be partially or fully transmitted, including from an unmanned aerial system.

At the same time, it is important to understand the complex and multifaceted process of training AI models, which can roughly consist of seven key stages: data collection and preparation, data labeling, algorithm selection, model training, evaluation and testing, optimization and retraining, scaling, and use (Table.).

Table 1

Key stages of AI training using big data: approaches and tools

Stage	Sub-stages	Description	Methods and tools
1. Data collection and preparation	1.1. Identification (or formation) of data sources	Collect structured and unstructured data.	SQL, NoSQL, API, web- scraping, IoT-sensors
	1.2. Data cleaning	Removing noise, filling in missing values, detecting anomalies.	Pandas, OpenRefine, DataWrangler

Продовження таблиці 1

	1.3. Normalization and transformation	Scaling of numerical data, categorization, text and image processing.	StandardScaler, MinMaxScaler, TF-IDF
2. Data marking	2.1 Manual marking	Human factor in object, text, and classification recognition.	Labelbox, Amazon Mechanical Turk
	2.2 Semi-automatic marking	Combination of rules, clustering, and human verification.	Snorkel, Active Learning
	2.3 Automatic marking	Using pre-trained models for recognition and labeling.	Pretrained ML Models (YOLO, BERT)
3. Selecting an algorithm	3.1. Classification	Determining the category of an object (spam/non-spam, object in an image).	Random Forest, SVM, CNN
	3.2. Regression	Predicting numerical values (financial markets, weather).	Лінійна регресія, XGBoost
	3.3. Clustering	Grouping data without labels (market segmentation, anomalies).	K-Means, DBSCAN, PCA
	3.4. Deep learning	Analyze complex structures (images, text, video).	TensorFlow, PyTorch
4.Тренування моделі	4.1.Parameter optimization	Adjusting weights and coefficients by minimizing the error.	Градієнтний спуск, Adam Optimizer
	4.2.Architecture definition	Selecting the depth of the neural network and activation functions.	CNN, RNN, Transformers
	4.3. Computational efficiency	Using GPU, TPU to speed up calculations.	CUDA, Google TPU
5. Assessment and testing	5.1. Division into sets	Training, validation and test sets (70/20/10).	Train-Test Split, K-fold Cross-validation
	5.2. Quality metrics	Measurement of accuracy, sensitivity, F1-measure.	Accuracy, Precision, Recall, AUC-ROC
	5.3. Error analysis	Identification of cases of incorrect predictions.	Confusion Matrix, SHAP Values
6. Optimization and retraining	6.1.Tuning hyperparameters	Selection of optimal model parameters.	Grid Search, Bayesian Optimization
	6.2.Reducing overfitting	Use of regularization, dropout.	L1/L2 Regularization, Dropout
	6.3. Retraining on new data	Updating the model without complete retraining.	Transfer Learning, Online Learning
7. Scaling and use	7.1 Integration into the system	Using the model in the production environment.	Flask, FastAPI, TensorFlow Serving
	7.2 Monitoring and updates	Tracking the quality of the model and updating it periodically.	MLflow, Prometheus, Grafana
	7.3. Ethical aspects and security	Prevention of bias, protection of personal data.	Fairness AI, Differential Privacy

Source: compiled by the authors

Data collection in wartime involves the use of various sources and methods. One of the main sources is the collection of intelligence from many channels, such as satellites, reconnaissance missions, human intelligence, and intercepted communications. These sources provide valuable information about enemy capabilities, intentions, and vulnerabilities. Databases created by the military store a huge amount of data, including historical records, geographic information, and

personal files. These repositories allow for the retrieval and analysis of critical information that can affect military operations. For example, the NSA (National Security Agency, USA), which as of 2013 contained at least 5 zettabytes of data in its data center in Utah. The U.S. Government Communications Headquarters (GCHQ), which is an intelligence and security organization responsible for providing SIGINT and information assurance (IA) signals to the U.K. government and armed forces, can collect up to 10 gigabits of data per second or 21 petabytes per day [2]. At the same time, it is worth noting that most countries, including NATO members, have not been involved in full-scale and high-tech conflicts such as the current war in Ukraine.

Technological advances have completely changed the processes of data collection and analysis for the military. An example in this context is Ukraine's domestic experience and miltech developments, which are ahead of many global analogues or have no alternatives at all.

For example, during the NATO TIDE Sprint 2025 conference in Helsinki, experts praised Ukrainian technologies and declared their readiness to integrate them into the Alliance's systems [3]. Among the main domestic innovations presented by Ukrainian developers to the international community, it is advisable to highlight the following:

DELTA – a digital situational awareness system at the frontline that provides real-time coordination of combat units and management of operations on land and sea.

Avengers – a unique artificial intelligence-based platform that analyzes the world's largest array of data on enemy vehicles, automatically detects targets and increases the accuracy of strikes

UA DRONE ID – a critical protocol for identifying friendly UAVs that prevents erroneous fire and ensures effective integration of drones on the battlefield [4].

As a result, Ukraine has become the first country to test AI solutions in a real war and develop them directly in combat conditions. Thus, alternative sources generate large amounts of data that allow military planners to identify trends, patterns, and anomalies. By analyzing historical data and real-time information (e.g., social media channels, communications intercepts, cartographic changes, etc.), it is possible to develop predictive models to forecast enemy behavior, identify potential threats, and potential outcomes of military operations.

References

1. King, A. (2024). Digital Targeting: Artificial Intelligence, Data, and Military Intelligence. *Journal of Global Security Studies*, Vol. 9, Issue 2. Retrieved from: https://academic.oup.com/jogss/article/9/2/ogae009/7667104

2. Jang, S. (2023).The Role of Data Collection and Big Data in Military War Planning. *CISS AL Big Data.* Retrieved from: https://medium.com/ciss-al-big-data/data-is-constantly-generated-a-collected-in-the-modern-era-by-everything-3738f0d8ac10

3. State Service for Special Communications and Information Protection of Ukraine (2025). The latest technologies and cybersecurity are in the spotlight: experts of the State Special Communications Service of Ukraine took part in the NATO

conference «TIDE Sprint 2025». Retrieved from: https://cip.gov.ua/ua/news/novitni-tekhnologiyi-ta-kiberbezpeka-u-centri-uvagi-fakhivci-derzhspeczv-yazku-vzyali-uchast-u-konferenciyi-nato-tide-sprint-2025]

4. PO "Aerial reconnaissance". Main page Facebook. (2025 Marth,1). Retrieved from: https://www.facebook.com/photo/?fbid=643870088191869&set=pcb.643871131525098&locale=uk_UA]

J. Stasiowska,
Studentka I roku,
studiów II stopnia Ekonomii
Na Wydziale Ekonomii i Finansów;
opiekun merytoryczny:
K. Puchalska,
dr inż.;
Uniwersytecie Rzeszowskim, Polska

CSR W STRATEGIACH FIRM A WYBORY ZAWODOWE STUDENTÓW UNIWERSYTETU RZESZOWSKIEGO

Współczesne przedsiębiorstwa funkcjonują w dynamicznym otoczeniu gospodarczym, w którym zyskuje na znaczeniu nie tylko efektywność finansowa, ale również odpowiedzialność wobec społeczeństwa i środowiska. Koncepcja społecznej odpowiedzialności biznesu (CSR) stanowi integralny element zarządzania w obszarach realnym, finansowym oraz infrastrukturalnym, przyczyniając się do długoterminowego wzrostu wartości przedsiębiorstwa. Coraz więcej firm dostrzega, że angażowanie się w działanie społecznie odpowiedzialne nie tylko wzmacnia ich reputację, ale również pozytywnie wpływa na zatrudnienie i lojalność pracowników, a także wybory konsumencie. Zasadne jest zatem zbadanie czy studenci uczelni wyższych zwracają uwagę w swoich wyborach zawodowych na fakt posiadanej i realizowanej strategii CSR.

Celem badania jest ocena wpływu CSR na preferencje studentów w kontekście wyboru miejsca pracy. Ocena zjawiska wymagała przeprowadzenia badań ankietowych wśród studentów Uniwersytetu Rzeszowskiego. Objęto nimi 410 studentów studiów I i II stopnia. Kwestionariusz został udostępniony w formie internetowej, a gromadzenie odpowiedzi miało miejsce od marca do maja 2024 roku.

CSR w strategiach firm

Społeczna odpowiedzialność biznesu jest szeroko definiowana przez różne organizacje i instytucje. Według Komisji Europejskiej CSR to „odpowiedzialność przedsiębiorstw za ich wpływ na społeczeństwo” [1, s.7]. Definicja ta podkreśla znaczenie dobrowolnych działań podejmowanych przez firmy w celu poprawy