СЕКЦІЯ XII.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

THE ROLE OF BIG DATA IN THE WAR IN UKRAINE AND PUBLIC ADMINISTRATION

Petrov Konstantin
ORCID ID: 0000-0003-1973-711X
Dr. Sc., Professor, Head of Information Control Systems Department
Kharkiv National University of Radio Electronics, Ukraine

Volobuieva Daryna
ORCID ID: 0009-0001-1924-0317
higher education student
Kharkiv National University of Radio Electronics, Ukraine

Kobzev Igor
ORCID ID: 0000-0002-7182-5814
PhD, Associate Professor at the Department of Multimedia Systems and Technologies of the Simon Kuznets
Kharkiv National University of Economics, Ukraine

The ongoing war in Ukraine has highlighted the critical role of Big Data technologies in modern warfare, public administration, and crisis management. In today's digital age, data-driven decision-making has become a vital component in addressing military threats, ensuring effective governance, and coordinating humanitarian efforts. The ability to analyze vast amounts of structured and unstructured data in real-time has allowed Ukraine and its allies to enhance military intelligence, cybersecurity, economic resilience, and public service delivery.

Big Data refers to large and complex datasets that require advanced computational tools for storage, processing, and analysis [1]. With the increasing digitization of warfare and governance, the use of Big Data has expanded beyond traditional business applications to areas such as military strategy, disaster response, and national security.

Since the Russian invasion in 2022, Ukraine has adopted data-driven approaches to strengthen its defense, counter disinformation, and manage

large-scale humanitarian crises. Several governmental and non-governmental organizations have leveraged artificial intelligence (AI), machine learning (ML), cloud computing, and geospatial analytics to process vast amounts of information related to military operations, public services, and economic recovery.

The Russian-Ukrainian conflict has naturally attracted the attention of many researchers and the military to better understand how it affects different sections of society, how information and disinformation are spread, how propaganda affects and how public attitudes are formed in response. Diverse models are applied, and different data sources are examined. For example, the reflection of dynamics of Ukrainian conflict in four different media channels is provided in [2] for visual analysis of the conflict dynamics by means of Big Data.

The concept of "Big Data" is epitomized by three fundamental characteristics: Volume, Velocity, and Variety. The Russia-Ukraine conflict, which began in February 2022, exemplifies these attributes in a striking manner. The war has generated a massive influx of information from a myriad of sources, contributing to an enormous volume of data. This data is not static; it is continually being produced at a rapid pace, demonstrating the "Velocity" aspect. Additionally, the nature of this data is highly diverse, spanning various formats including text, images, videos, and geospatial data, thus embodying the "Variety" component of big data. This convergence of Volume, Velocity, and Variety in the context of the Russia-Ukraine conflict sets the stage for our comprehensive sentiment analysis [3].

In times of war, governments must make rapid, data-driven decisions to ensure national security, economic stability, and efficient resource allocation. Big Data has become a critical tool for public administration in Ukraine, enabling transparency, financial oversight, and crisis management. Below are some of the key areas where Big Data has played a role in governance during the war:

– transparency and Financial Oversight. Governments facing wartime pressures must manage financial resources effectively while maintaining transparency to prevent corruption and misallocation of funds;

– tracking Defense and Humanitarian Aid Spending. The Ukrainian government, along with international organizations, uses data analytics to monitor military and humanitarian expenditures. Platforms like ProZorro, Ukraine's open procurement system, have been instrumental in ensuring accountability in war-related spending. Big Data helps identify suspicious

transactions, detect inefficiencies, and provide real-time reports on financial flows;

– blockchain and Distributed Ledger Technologies. To prevent fraud and ensure transparent financial operations, some aid organizations have started leveraging blockchain technology. For example, the Aid for Ukraine initiative, which collects cryptocurrency donations, utilizes blockchain analytics to track fund distribution and prevent misuse.

Government agencies and financial institutions rely on Big Data to assess the impact of the war on GDP, inflation, and employment. By analyzing financial transactions, supply chain disruptions, and market trends, policymakers can make informed decisions about economic recovery measures.

The war has disrupted global supply chains, affecting Ukraine's exports of grain, steel, and other commodities. Using AI-driven predictive analytics, businesses and government agencies track shipment data, detect bottlenecks in logistics, and forecast potential shortages. Tools like satellite imagery analysis help assess the condition of critical infrastructure such as roads, railways, and ports.

Ukrainian law enforcement agencies use crime-mapping analytics to identify high-risk areas and allocate resources effectively. By analyzing reports from civilians, surveillance camera data, and historical crime patterns, authorities can prevent looting, sabotage, and organized crime activities.

Big Data-powered facial recognition technology has been used to identify Russian soldiers and collaborators. Ukrainian authorities, along with private intelligence firms, have leveraged tools like Clearview AI and FindClone to match social media images with wartime footage, helping to track down war criminals.

Data analytics has also played a role in identifying internal security threats, such as infiltrators or corrupt officials. Advanced AI-driven anomaly detection tools analyze behavioral patterns in government agencies and military units to flag suspicious activities.

The war in Ukraine has demonstrated how Big Data can serve as a powerful tool for military strategy, public administration, cybersecurity, and humanitarian efforts. By leveraging real-time data analytics, Ukrainian forces, government institutions, and international allies have been able to respond more effectively to both military and civilian challenges.

Big Data has played a crucial role in intelligence gathering, strategic planning, and cyber defense. Satellite imagery, social media analysis, and

predictive algorithms have helped Ukraine track enemy movements, counter disinformation campaigns, and enhance national security. In public administration, data-driven governance has improved transparency, optimized economic policies, and ensured efficient allocation of resources. Platforms like Prozorro and Diia have demonstrated how technology can maintain government efficiency even in times of war. In humanitarian efforts, Big Data has facilitated refugee tracking, supply chain optimization, and international aid coordination, ensuring that resources reach those in need more quickly and effectively.

Despite these advancements, several challenges remain, including privacy concerns, cybersecurity threats, infrastructure limitations, and the risk of data manipulation. Addressing these issues will be critical to sustaining the benefits of Big Data in post-war reconstruction.

References:

1. Big Data Defined: Examples and Benefits | Google Cloud. *Google Cloud*. URL: https://cloud.google.com/learn/what-is-big-data
2. J. Mandravickaitė, T. Krilavičius, "Ukrainian Conflict in Media: Two Approaches to Narrative Analysis" URL: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STOMP-IST-178/MP-IST-178-04.pdf
3. K. Kopanov, T. Atanasova. From Open Source Data to Intelligence: Leveraging AI and Big Data for Insights on the Russia-Ukraine Conflict URL: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-205/MP-IST-205-19P.pdf