Regarding critical development priorities technologies of artificial intelligence in the field of security and defense of Ukraine [unofficial translation]

August 2023

The working group "AI + Security/Defense" of the expert advisory committee on the development of artificial intelligence at the Ministry of Digital Transformation of Ukraine (hereinafter - the Working Group) in accordance with the Concept of the Development of Artificial Intelligence in Ukraine, which was approved by the order of the Cabinet of Ministers of Ukraine dated December 2, 2020 year #1556, taking into account the existing threats to the national security of Ukraine and the development of innovative technologies, the following recommendations were developed regarding the priorities for the development of artificial intelligence technologies in the sphere of security and defense of Ukraine.

The working group conducted an analysis of the practice of developing innovative solutions in the field of security and defense, and concluded **that a critical problem in the field of security and defense is not only hardware, but also software, data collection and exchange, as well as technologies of Artificial Intelligence (hereinafter - AI).**

Today, Ukraine's security and defense challenges are becoming increasingly complex and asymmetric. Classic solutions are not enough to fight such threats as robotic autonomous systems (drones, robots), cyber attacks, terrorism or disinformation campaigns (including using deep fakes). These threats often require complex, integrated, software-based approaches to detect, respond, and neutralize.

Military operations require continuous processing of vast amounts of data, including satellite imagery, sensor data, intelligence reports, and more. Effective collection, analysis and sharing of this data is critical to decision-making and situational awareness. AI plays an important role in processing this data, providing faster and more accurate answers.

AI systems can provide decision makers with real-time information and recommendations based on data analysis from multiple sources. This helps make more informed decisions during military operations.

AI and machine learning provide predictive analytics that are invaluable in the defense sector. These technologies can evaluate large data sets to identify trends, anomalies, and potential threats before they escalate. Predictive models can assist in resource allocation, mission planning, and threat assessment.

Autonomous systems are an extremely important component of the field of security and defense. The development of autonomous military systems, such as drones and unmanned aerial vehicles, requires innovative solutions such as AI to ensure independent autonomous operation, decision-making and adaptation to changing mission conditions.

After the analysis and taking into account our own expertise in the field of AI, the Working Group recommends directing public and private investments to the development of artificial intelligence (AI) technologies, relevant systems and infrastructure in the following directions within 1-3 years in the field of security and defense of Ukraine:

1. AI for unmanned systems (drones, robots) of domestic production:

- autonomous navigation systems (without GPS);
- management systems for the coordinated execution of tasks;

- autonomous task performance systems;
- detection (identification) systems of enemy weapons and equipment;
- data collection and storage systems for the operation of unmanned systems.

2. AI to combat disinformation:

- solutions for dialogues based on generative artificial intelligence;
- tools with deepvoice and deepface technologies for special law enforcement agencies;
- systems for automatic detection of sources of disinformation, bots that are part of coordinated groups involved in foreign influence operations (FIMI);
- automation/standardization of the description of information threats and data exchange;
- marking and detection of hostile generative AI to prevent the spread of disinformation;
- creating datasets and collecting data to create generative AI.

3. AI for logistics systems of national security and defense:

- forecasting the terms of equipment repair based on operating conditions;
- simulation analysis of logistics supply operations;
- systems for forecasting supply and logistics needs and risks;
- control and automation systems of military warehouses;
- systems of autonomous robots for the delivery of military cargo and evacuation of personnel during active military operations.

4. AI for the detection and disposal of mines and ammunition:

- data collection and storage systems from satellites, drones, robots, and other sources (thermal sensors, etc.), and their analysis using AI to detect mine sites;
- identification with the help of AI of places of fighting, their marking for further planning of demining;
- demining work management systems (ground for work in the city, ground for work in the field, underwater);
- demining quality control systems.

5. AI for cyber security, protection of communication, information and technological systems in the defense sphere:

- AI systems for radio intelligence (+ EW extension);
- the latest encryption and data exchange systems;
- use of generative AI (voice) for pen testing (authorization);
- the latest methodologies for protection against social engineering using generative AI (voice, 3D video);
- research (scientific and technical), focused on the development of the necessary innovative cyber security systems to protect critical digital infrastructures using advanced artificial intelligence technologies for automatic analysis and classification of threats.

6. Creation of general conditions for rapid development of AI solutions for security and defense:

- simplification of import and simplification of licensing procedures of components required for training and development of AI-based solutions;

- deregulation, simplification of the procedure for obtaining data from the battlefield for developers of drones, robots and other AI systems;
- simplification of testing processes of innovative products "on the battlefield" by domestic and foreign companies;
- transparency and availability of information for participants in the field of defense tech, availability of public standard conditions for starting cooperation;
- implementation of generally accepted standards of data exchange and accumulation;
- legally and normatively ensure the possibility of data exchange between various market participants and state bodies.

7. General infrastructure and solutions:

- automated battle control systems (Automated / AI assistance);
- solutions for simulating military operations (War games / Military operations research);
- systems of analysis and classification of data from video surveillance cameras;
- systems for collecting and accumulating data from media resources (as part of intelligence data).
- face recognition and identification systems;
- damage assessment systems based on AI and various types of data;
- developed physical data transmission systems (for drones, robots, between different agents);
- AI training datasets and data collection systems available to market participants;
- polygons for testing solutions by domestic and foreign developers;
- data exchange systems between various departments, integration with Government BI systems;
- production of own sensors (stereo cameras, thermal cameras, etc.);

At the same time, we note the following:

- Most of the mentioned projects require highly qualified managers and engineers who have experience working with modern technologies, platforms and AI. The expert committee is ready to provide its expertise on the verification of personnel qualifications;
- The development of the mentioned technologies and systems takes from 6+ months, so the Working Group recommends to start organizing immediately through the provision of specific grants or the creation of appropriate structures for implementation;
- It is also very important that Russia has announced investments in the development of AI of more than one billion US dollars for the next years. Without similar investments and effective project management in this area, it will be very difficult for Ukraine to compete in the field of AI in defense and security in 2-3 years.

Composition of the Working Group:

Tetyana Serhiyivna Avdeeva, Yevhen Mykolayovych Horovy, Oleksandr Romanko, Pavlo Petrovych Pikulin, Serhiy Grigorovich Stirenko, Bulak Anna Oleksandrivna, Oleksiy Petrovych Turuta, Andriy Oleksandrovich Latysh, Volodymyr Grigorovich Begei, Serhiy Kuprienko, Andriy Volodymyrovych Zablovskyi, Maksym Ihorovych Surzhynskyi, Dmytro Oleksyovich Pleshakov , Vitaly Honcharuk, Maksym Korzhenevskyi.

Best regards,

Head of the working group of the EC on the development of the field of artificial intelligence at the Ministry of Digital Transformation of Ukraine

Vitaliy GONCHARUK

e-mail: vitaliy@tiukraine.org