The Central Research Institute
of the Armed Forces of Ukraine

Military Science

JOURNAL

Vol. 2 No. 1

ISSN (print): 2786-9318
ISSN (online): 2786-9326

themilitaryscience.com

The Central Research Institute
of the Armed Forces of Ukraine

Military Science
JOURNAL

Vol. 2 No. 1

ISSN (print): 2786-9318
ISSN (online): 2786-9326

themilitaryscience.com

УДК 355/359:623.09/98 (08)
DOI: 10.62524/msj.2024.2.1
ISSN (print): 2786-9318
ISSN (online): 2786-9326

Засновник: Центральний науково-дослідний інститут Збройних Сил України

Журнал засновано науковою радою Центрального науково-дослідного інституту Збройних Сил України, протокол № 12 від 13.12.2023 року (ідентифікатор медіа – R30-02019 Національна рада України з питань телебачення та радіомовлення, рішення № 1327, протокол № 26 від 09.11.2023 р).
Видається з грудня 2023 року, чотири рази на рік.

Метою журналу є висвітлення результатів наукових пошуків дослідників з актуальних військово-теоретичних, військово-спеціальних питань та безпеки держави.

Науковий профіль видання:
073 – Менеджмент;
122 – Комп’ютерні науки;
125 – Кібербезпека та захист інформації;
253 – Військове управління (за видами збройних сил);
254 – Забезпечення військ (сил);
255 – Озброєння та військова техніка;
256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Рекомендовано до друку науковою радою ЦНДІ ЗС України
(протокол № 3 від 03.04.2024 року)

РЕДАКЦІЙНА КОЛЕГІЯ

Голова редколегії: Семененко О. д-р військ. наук, проф.
Заступник голови редколегії: Дейнега О. д-р військ. наук, проф.

Члени редколегії:

Абрамова М.	канд. екон. наук, ст. наук. співроб.	Кірсанов С.	д-р техн. наук, ст. наук. співроб.
Богданович В.	Заслужений діяч науки і техніки України, д-р техн. наук, проф.	Коваль В.	канд. військ. наук, ст. наук. співроб.
		Лисенко О.	Заслужений діяч науки і техніки України, д-р техн. наук, проф.
Білейшіс М.	PhD, Prof. Dr. (Литовська Республіка)	Марко І.	Заслужений економіст України, д-р екон. наук, проф.
Волобуєв А.	д-р техн. наук, ст. наук. співроб.		
Годзь С.	д-р військ. наук, ст. дослід.	Машкін О.	д-р техн. наук, ст. наук. співроб.
Грищук Р.	Заслужений діяч науки і техніки України, д-р техн. наук, проф.	Мірненко В.	Заслужений працівник освіти України, д-р техн. наук, проф.
Гусак Ю.	д-р військ. наук, проф.	Павловський О.	д-р військ. наук, проф.
Дєнєжкін М.	д-р військ. наук, проф.	Потетюєва М.	д-р екон. наук, доц.
Дудзевічюте Г.	PhD, Assoc. Prof. Dr. (Литовська Республіка)	Потьомкін М.	д-р техн. наук, проф.
		Соломицький О.	д-р військ. наук, ст. наук. співроб.
Закусило П.	д-р військ. наук, проф.	Ткач І.	Заслужений економіст України, д-р екон. наук, проф.
Залужний В.	доктор філософії		
Керіган-Киру Д.	BA, PhD (Республіка Ірландія)	Ткач М.	д-р екон. наук, проф.
		Хомчак Р.	д-р військ. наук, ст. дослідник.

Відповідальний редактор: Васянович М., канд. військ. наук, ст. дослід.
Технічний редактор: Шнукало А.

Адреса редакції:	**Телефон:**	**E-mail:**	**Інформаційний сайт:**
проспект Повітряних Сил, 28Б 03049, Київ, Україна	+38 (044) 520-19-44	crsi@post.mil.gov.ua	themilitaryscience.com

Журнал індексується агентствами: Crossref, Google Scholar, OUCI, Scilit, OCLC.

Редакція може не поділяти точку зору авторів.
Відповідальність за зміст поданих матеріалів несуть автори.

© ЦНДІ ЗС України, 2024

Contents

Zaluzhnyi V., Hryshchuk R., Solomytskyi O., Hrachov I.
The Armed Forces of Ukraine unmanned systems future development 5

Semenenko O., Koval V., Vodchyts O., Dobrovolskyi Y.
A multi-domain operation - a modern view at the forms and methods of military operations adapting to the environment of challenges and threats transformation 17

Chepkov I., Dovhopoly A., Biloborodov O., Panteleiev S.
Technologies of information and psychological influence on people in modern wars 35

Nordlöf J., Bengtsson K.
On the importance of continuous development in the military domain 53

Ledwidge F.
Realising Ukraine's military potential in the Space Domain 60

Peredrii O., Snitsarenko P., Sarychev Y., Zubkov V.
A conceptual approach to improving the information support of the prospective Armed Forces of Ukraine 70

Raymond M.-P., Fournier E.
An access to innovation program to enhance the technological capabilities of the armed forces 83

Sliusarenko M., Baranov S., Voytsehovskiy R.
The impact of the russian-ukrainian war on economic processes in russia: analysis and forecasting 89

Tymchuk V., Trysnyuk V.
The systematic review of variety of military, weapon, combat and warfare system-of-systems wuth their new classification and ontology depiction for further concept and design development for the Armed Forces of Ukraine 102

Furmanov K., Hutchenko O., Hutchenko K.
Methodological approach to determining the nomenclature of mobile assets for acomplishment the tasks of nuclear threat detection and assessment 117

Godz S., Taran O.
Methodological aspects of justifying the specialists training duration of the armed forces branches of a formation (unit) 128

Mashkin O., Maslenko S.
Complex modeling of complicated processes: analytical model parameters adaptation in solving qualimetric problems 144

Semenenko O., Abramova M., Yarmolchik M.
The sufficiency of the State's economic capabilities to ensure the necessary level of defense needs forecasting improving method ……..153

Kholokh O.
Methodological principles of forming the "image of the enemy" in the minds of ukrainian servicemen during the russian-ukrainian war ……... 166

Kulahin K., Nos I., Solonets O., Kvitkin K.
Implementation of the emerging and disruptive technologies as the key to technological superiority in modern warfare …… 177

Pantiushenko R., Chaika Y.
Artificial intelligence in the sphere of cybersecurity: innovations, challenges, and development prospects…….. 200

Сушак М., Братусь Ю., Васянович М.
Вирішення задачі забезпечення справності парку авіаційної техніки Збройних Сил України в умовах особливого періоду …… 207

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.01

The Armed Forces of Ukraine unmanned systems future development

Valery Zaluzhnyi
Philosophy Doctor
Commander-in-Chief of the Armed Forces of Ukraine
General Staff of the Armed Forces of Ukraine
03168, Air Force of Ukraine Avenue, 6, Kyiv, Ukraine
e-mail: uzvk_mou@post.mil.gov.ua
ORCID : 0000-0002-1947-501X

Ruslan Hryshchuk
Honored Statesman of Science and Technology of Ukraine, Doctor of Technical Sciences,
Professor, Head of the Central Research Institute of the Armed Forces of Ukraine
Central Research Institute of the Armed Forces of Ukraine
03049, Air Force of Ukraine Avenue, 28 B, Kyiv, Ukraine
e-mail: Dr.Hry@i.ua
ORCID : 0000-0001-9985-8477

Oleksiy Solomytskyi
Doctor of Military Sciences, Senior Researcher
Head of Department
Central Research Institute of the Armed Forces of Ukraine
03049, Air Force of Ukraine Avenue, 28 B, Kyiv, Ukraine
e-mail: solosa1@gmail.com
ORCID: 0000-0001-8061-8895

Ihor Hrachov
Head of Department
Captured and Advanced Weapons and Military Equipment Research Center
General Staff of the Armed Forces of Ukraine
03168, Air Force of Ukraine Avenue, 6, Kyiv, Ukraine
e-mail: ig43194@gmail.com
ORCID: 0009-0003-9108-7059

Abstract. The relevance of the article is due to the Armed Forces of Ukraine unmanned systems development normative forecasting need in order to achieve a superiority over the enemy. One of the futures` main provisions of the Armed Forces of Ukraine unmanned systems development has been outlined. Futures have been developed by using a modified method of "branches" as a component of foresight (scenario forecasting). Elements of SWOT analysis and the cognitive-dynamic method of forecasting were also applied in the part regarding normative forecasting. The future of the Armed Forces of Ukraine unmanned systems development is presented as the desired version of the development of these systems in the future, using cause-and-effect logic. Within its framework, the main trends in the development of unmanned systems in the leading countries of the World were considered. The list and content of the main stages of development of futures according to the modified method of "branches" are presented. The forecasting horizon is defined. The author's view on the ecosystem of unmanned systems that has apeared in Ukraine is offered. The results of the analysis of the stakeholders of the considered ecosystem are presented with the distribution of their

influence and interest according to the Mendelov and Johnson matrices. Based on the analysis of external and internal factors that will influence the development of unmanned systems, as well as the future operating environment, the key results that must be achieved to realize the main development goal and the main ways (actions, influences) to achieve them are determined. The key results cover two main areas - as organizational and technological and as combat also. In addition, the priority directions for the unmanned systems of the Armed Forces of Ukraine development by components, levels, types and technical aspects have been determined. The proposed futures may be used both as for more detailed regulatory forecasting of the unmanned systems development, for example, when developing of a corresponding foresight, as during the program documents (strategies, concepts, etc.) development or priorities of the State's military and technical policy determination.

Keywords: unmanned systems, forecasting, futures, foresight.

Introduction

Unmanned systems (USs) have been gradually developing for several decades, but recently, as a result of technological breakthroughs, this process has become explosive. USs have rapidly broken the realities of combat activities, their role on the battlefield has significantly increased, they have occupied their niche and are rapidly expanding it, becoming indispensable during the performance of a number of missions, multiplying the capabilities of some elements of conventional forces and means and nullifying the advantages of others.

The rapid USs development has attracted a lot of attention to forecasting the prospects of their development. Quite a lot of analytical (Volkogon V., 2019; Kuprinenko O., 2021; Shugurov O., 2007), scientific and prognostic (Zaluzhnyi V., 2023; Semenenko O., 2023; Pathak M., 2017) and of a program nature (Kohn E., 2020; Heiming G., 2021; Chawla S., 2015) publications have appeared on this issue.

Ukraine currently occupies a leading position in the USs application, the tactics for their use development, and the main directions of their development for the near future formation. It is necessary to maintain and consolidate the position of the leader in this field, acquiring opportunities for the development and scaling of the USs production, that will allow to achieve an asymmetric advantage over the enemy.

Many countries of the World are making a lot of efforts to develop USs, based on their views on warfare, needs and capabilities. Ukraine, being in a state of war, is currently at the forefront of the USs development process, given the possibility of testing them under combat conditions. It should be noted that each country chooses its own vector of security development, taking into account the realities of the military and political situation, the range of threats and the views of the military and political leadership on the development of the national armed forces. The results of the priority directions analysis of the views on the USs development in the leading countries of the world are shown in the table. 1.

However, the USs development is somewhat chaotic, without a unified plan. Therefore, it is necessary to determine the main trends, it is necessary to develop them specifically in accordance with the needs of the Armed Forces of Ukraine (AF of Ukraine).

That is why the development of scenarios for the Armed Forces of Ukraine USs development is an urgent task.

Methodological Framework

The basis of the USs development proposed futures (forecast) of the is based on the modified method of "branches" as an element of the methodology of scenario forecasting (foresight) (Rhydderch, 2009). At the same time, by futures we mean the desired version of the development of the USs of the AF of Ukraine in the future, developed using cause-and-effect logic (Zgurovsky Z., 2021).

Table 1. The main directions of the USs development in the leading countries of the World

Country	Directions of development	A promising goal
USA	Use of artificial intelligence, autonomous systems and smart sensors in robotic agents. The development of systems that can function in interaction with human beings, increasing the speed of decision-making and providing advantages in the military operations conductment.	Increasing the ability of troops to adapt to a changing combat environment and ensure a technological advantage over potential adversaries.
United Kingdom	Development and implementation of autonomous systems to support combat operations. Developing systems with artificial intelligence and machine learning to increase the efficiency and security of its own military forces.	Ensuring the level of readiness and combat capabilities, the ability to adapt to complex modern threats and dynamic combat conditions.
France	Development of the USs to provide support for combat operations and logistics on the ground. The development of robotics to increase the efficiency of combat maneuvers and optimize supplies.	Improving the capability for the operational mobility and providing support in changing combat environments.
Germany	The development of the USs, that are focused on medical, intelligence and logistical directions. The emphasis is also placed on issues related to the ethics and safety of using USs systems application in the military operations.	Ensuring the health and safety of servicemen, expanding the capabilities of conducting intelligence and supporting logistical processes on the battlefield.
Turkey	Development of various types of USs, including combat robots, intelligence systems and logistics systems, etc. Attention is focused on the creation and implementation of advanced technologies.	Increasing the combat capabilities of military forces, providing additional support for military operations and reducing risks for military personnel.

Results and Discussions

The development of futures based on the "branches" method (Rhydderch, 2009) involves the following stages (Fig. 1).

1. Tasks forecasting definition and time horizon.
2. Identification of stakeholders (drivers), trends and key factors and events that influence the development process.
3. Determination of key (required) results to focus on.
4. Determination of factors or actions that must be implemented to achieve the desired results.

In accordance with the proposed procedure, the future development of the USs of the Armed Forces of Ukraine has been developed.

1st stage. The main goal of the military purposes USs development is to increase the combat effectiveness of their use and combat capability of the Armed Forces of Ukraine with the provision of technological superiority. At the same time, attention should be focused on saving people's lives and military resources (ammunition, weapons and military equipment, etc.).

This goal should be achieved in the next year and a half, that determines the futures horizon.

When having achieved this goal, we will have the opportunity to:

effectively solve the complex missions of a wide range under the conditions of confrontation with an enemy that has a numerical advantage;

preserve the life and health of military personnel;

to fetter the enemy's initiative, limit his operational capabilities;

to contribute to the innovative development of the national defense-industrial complex (DIC);

expand military-technological partnership with other countries.

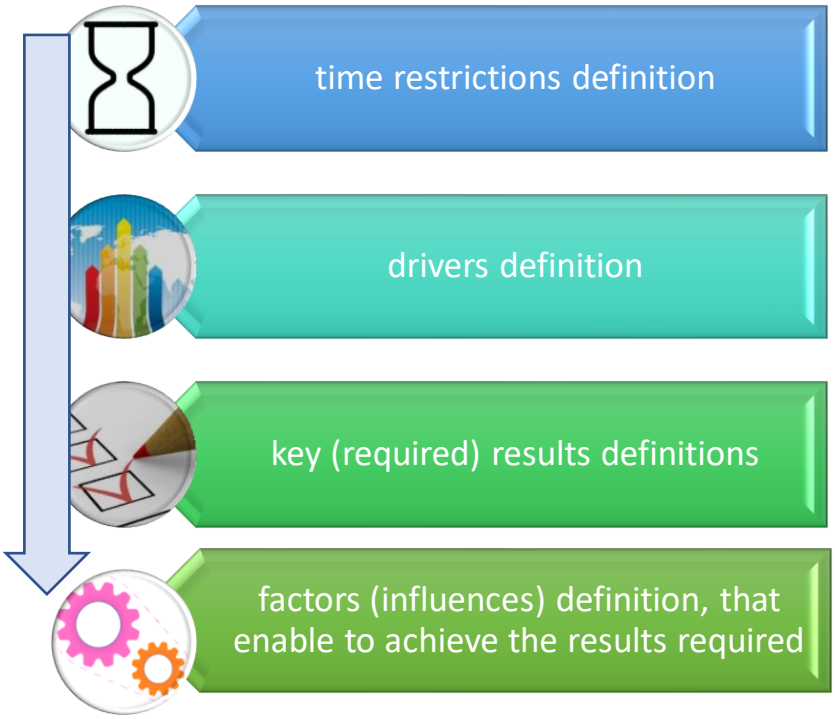


Figure 1. The main stages of futures developing

2nd stage. In Ukraine, the USs ecosystem (Fig. 2) origin, as built on the principles of synergy and self-organization, is a closely interconnected set of unmanned vehicles of various purposes, organizations and structures, that engaged in their development, production, procurement, supply and operation, control subsystems, logistics and personnel training, which ensure the development and application of USs as intended, and also determines the legal, economic, organizational and other conditions of these processes.

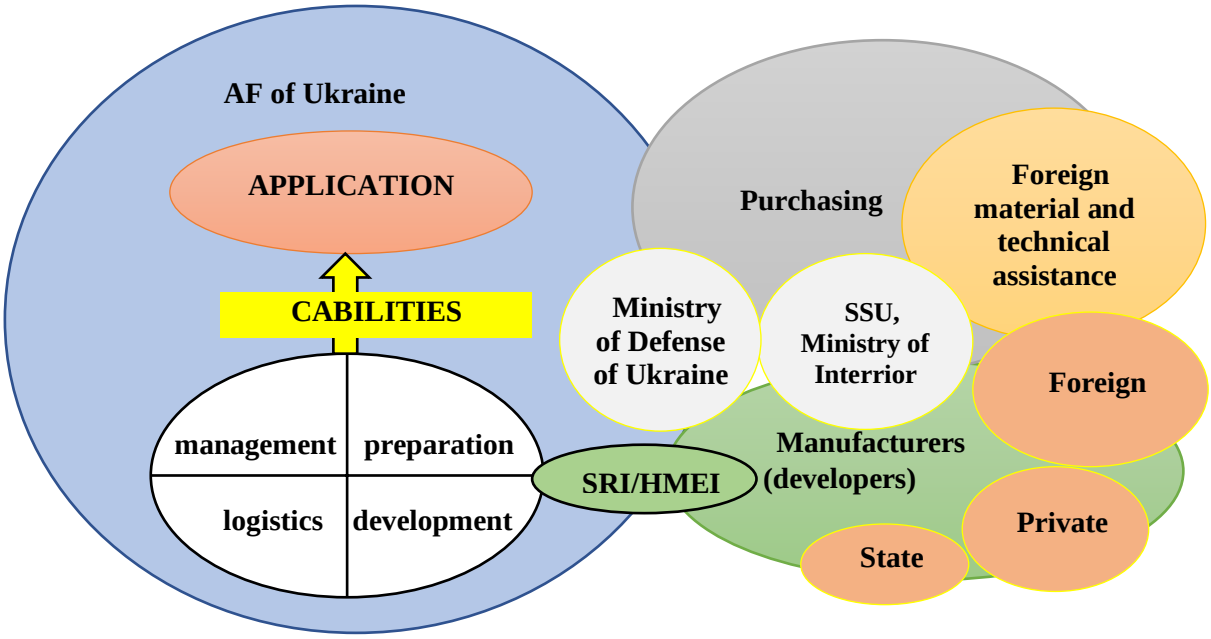


Figure 2. The ecosystem of unmanned systems

The overall goal of the ecosystem participants is to create an environment and ensure conditions for the effective development and application of USs, implementation of innovative breakthroughs and maintaining a technological advantage over the enemy.

According to the ecosystem participant's analysis results, the stakeholders were divided according to the "influence – interest" criterion (Fig. 3), that will allow a more rational distribution of efforts during the organization of the USs development. The distribution of their interest and influence in the development processes of USs is shown in fig. 4 by the Johnson matrix. It should be noted that the degree of influence and interest is indicated in a relative form, while the leaders occupy approximately the same positions.

The nearest future USs development will be influenced by a combination of external and internal factors, that are presented in the table. 2.



Figure 3. Mendelian matrix "influence – interest"

Thus, the development of security will take place in the conditions of an unstable external environment, which will be characterized by multi-vectored and asymmetric threats, the instability and ineffectiveness of international security organizations, the preservation of confrontation with the russian federation (even in the "frozen" phase), the rapid development of technologies, in particular artificial intelligence, and their uncontrolled distribution.

When determining the prospects for the development of USs, it is necessary to take into account that this process will be complicated due to limited funding, insufficient development of the production base, dependence on foreign technologies and components, as well as conflicts of interests.

At the same time, it is necessary to ensure the harmonious development of the USs ecosystem: increasing the share of ground-based and maritime USs and at the same time expanding the

possibilities of their application.

The operational environment in the part related to USs will be characterized by the following factors:

USs on the battlefield became its integral component, besides, they turned out to be a fairly universal tool – relatively inexpensive, one that does not require complex technological processes, easy to use (manage) and capable of performing a wide range of missions;

USs change the nature and course of war, forcing to review the role and place of other combat systems on the battlefield and the tactics of their use;

USs have a shortened life cycle (due to the rapid development of technologies), which determines the dynamism and continuity of further changes in the future;

advanced technologies (USs swarms, artificial intelligence, innovative materials, etc.) will even more radically change the nature of warfare.

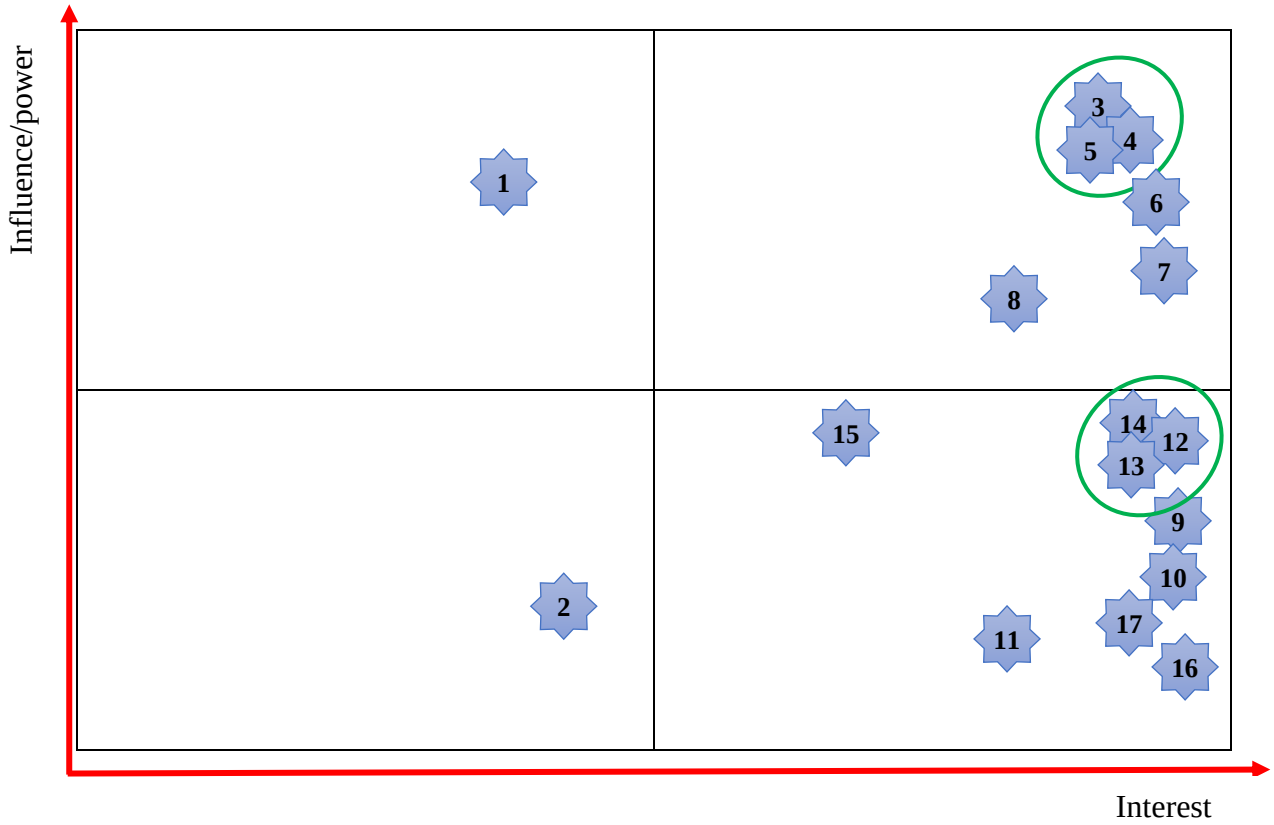


Figure 4. Johnson's matrix "influence - interest"
(stakeholders are numbered according to Fig. 3)

***3rd stage*.** Further implementation of USs will increase the efficiency and accuracy of operations, reduce risks to servicemen, and expand the capabilities of the Armed Forces of Ukraine. For the successful development of the Armed Forces of Ukraine USs, attention should be paid to the development of appropriate strategies, financing of scientific research and development of the defense industry. Multifaceted cooperation with foreign partners is also important.

In order to ensure the sustainable development of USs, it is necessary to create prerequisites for the formation of a self-sufficient, sustainable and high-tech ecosystem of USs in the AF of Ukraine, which will become a provider of relevant capabilities for our armed forces.

This will make it possible to provide the AF of Ukraine with the latest unmanned weapons and highly qualified personnel, and, as a result, to form an asymmetric strategic advantage over the

enemy, which dominates in terms of numbers, resources and industrial base.

Table 2. The main external and internal factors that will affect the development of unmanned systems in the short term

External factors (military and political environment)	Internal factors
The military and political situation in the World and around Ukraine in the next few years will remain tense and unstable and will be characterized by global rivalry between the democratic and authoritarian worlds.	The drone industry in Ukraine remains fragmented and unsystematic.
	Production and technological capacities are insufficient and cannot meet the needs of the Armed Forces of Ukraine.
Ukraine will continue to be on the edge of the conflict between the two worlds, and russia will remain a strategic threat to its statehood.	The financial provision of the needs of the Armed Forces of Ukraine in USs remains at a relatively high, but insufficient level, and the structure of funding sources and expenditures do not contribute to the harmonious development of the industry.
The West (Partners) will continue to support Ukraine, but the level of support may vary depending on the domestic political situation in the Partner States and the presence of other sources of tension in the World.	The combat component is presented fragmentarily, mostly by the tactical link of unmanned aerial systems.
Ukraine will have access to technologies, markets and global production capacities, but this will be dependent on lots of factors.	The existing system of staffing and training of USs crews does not allow to fully realize the potential of unmanned capabilities.

The realization of the goal of the development of USs involves the achievement of the following key results:

1. Moderation mechanisms of the USs ecosystem have been formed, which will allow directing the development of the industry in the interests of meeting the needs of the AF of Ukraine.
2. An effective combat component of the USs has been formed, which will make it possible to gain an asymmetric advantage on the battlefield.

4th stage. To achieve the first key result, it is necessary to:

1. Create effective communication mechanisms between manufacturers of unmanned systems, The Ministry of Defense of Ukraine (MoD of Ukraine), the AF of Ukraine and other interested institutions. For this purpose, it is necessary:

to improve the regulatory framework for regulation of production, certification, licensing, procurement, operation and granting of rights regarding the possibility of using USs;

create a proactive system of interaction between the customer (the Ministry of Defense of Ukraine) and developers (manufacturers) for the prompt provision/receipt of requirements for safety and security, introduce coordination councils, online platforms (portals), technology parks (techno-hubs), etc.;

to introduce the practice of organizing conferences (round tables, etc.) with the participation of customers and developers (manufacturers) on the creation and production of USs;

implement a system of scientific support (feedback) during the development (production) of USs.

2.To implement stimulating mechanisms of Research & Development (R&D) (competitions, tenders) for the creation of USs in priority areas, increasing the scientific and technological potential of the sector and creating the latest breakthrough technologies. For this, it is necessary to initiate at the state level issues regarding the stimulation of R&D, in particular regarding:

deduction of investments in R&D from the tax base of companies, preferential tax rates and "tax holidays", accelerated depreciation of fixed assets;

simplification and acceleration of the processes of development of requirements, technical

tasks, tests, certification and acceptance into service (revision and development of DSTU (State Standards of Ukraine);

creation of a grant (incentive) system for the implementation of priorities and requirements for samples, as well as stimulation of developers (manufacturers) during the execution of an order for the creation of USs;

implementation of transparent tenders in areas of development of USs;

expansion of the codification system in relation to USs of military purpose.

3. To develop effective mechanisms of system integration of technological solutions of various manufacturers (technological system integrator of the national level in the field of unmanned systems). Ways to achieve this task are:

implementation of world quality standards and certification during the development of technical tasks and acceptance into service, organization of cooperation between domestic developers and manufacturers of BPS within the state, as well as with foreign developers and manufacturers;

creation of a single coordination center for the system integration of technological solutions of various manufacturers;

introduction of an effective system of centralized management of access to modern safety and security technologies; implementation of an adaptive contracting system (in order to quickly make changes to technological solutions);

creation of patent boxes, mechanisms for protecting intellectual property and payment of royalties, etc.

4. Implement mechanisms for rapid scaling of serial production of unmanned systems. To introduce these mechanisms, it is necessary:

to provide priority financing for the development and production of USs as one of the main and promising areas of development of the defense industry of Ukraine;

to search for and use new ways and areas of realizing the potential of enterprises in the changing conditions of the external environment within the framework of the chosen mission, giving priority to the evolutionary type of innovative policy and offensive strategy;

implement innovations in the technical re-equipment of industry enterprises based on new digital technologies and industrial robotics technologies;

to contribute to the creation of conditions for the organization of production of components for USs, reduction of dependence on foreign suppliers and organization of USs production on the basis of the most successful solutions.

5. To improve the mechanisms of organizing the procurement of unmanned systems. For this you need:

carry out further development of the electronic procurement system taking into account EU requirements and standards, best international practice;

to expand international cooperation in the field of public procurement;

take systematic measures to reduce corruption risks and increase the level of transparency and control over the actions of customers and the responsibility of officials, as well as strengthen internal control;

implement mechanisms for ensuring the fulfillment of obligations;

initiate at the state level the creation of credit lines for developers and manufacturers;

to ensure the simplification of the contracting procedure in the Ministry of Defense and the Armed Forces of Ukraine, as well as the procedures for collecting documents and admitting to the operation of USs.

To achieve the second key result, it is necessary to:

1. To ensure the creation (improvement/expansion) of the USs management vertical in the areas of generation (development, preparation, provision) and application management. For this purpose,

you need:

to improve the USs management system (select a separate vertical);

to implement modern processes and procedures of planning and application of USs with further integration of USs military management bodies into a single combat information space, to ensure the effective operation of which to create an automated control system (ACS) of USs based on the principles of interoperability with existing (prospective) ACS troops and information systems;

during the work of the military management bodies, implement modern decision-making procedures and planning the use of USs at the operational and strategic levels;

to create a system of logistical support for the USs of the AF of Ukraine.

2. Create mechanisms for effective selection, recruitment and training of personnel. For this:

implement effective mechanisms for the selection and recruitment of professionally trained personnel with the professional, psychological, and moral and business qualities necessary for the management of USs;

to implement a single standardized multi-level (from tactical to strategic level) system of training of USs specialists, taking into account the specifics of the missions to be performed, to integrate into the system of personnel training of the AF of Ukraine the system of training in non-state (volunteer, private and foreign) schools thanks to the synchronization of training programs, as well as to carry out special training of specialists for the logistics support units to acquire knowledge and skills of technical maintenance and repair of USs;

to improve the management system and career management of USs specialists.

3. To increase the system of collection, study and implementation of experience in the application of USs. Ways of implementation are:

inclusion in the existing system of summarizing the experience of the issue of the application of USs;

using the experience gained during the improvement of the existing and creating perspective organizational structures of the tactical, operational and strategic level, which are responsible for the use of USs, taking into account the adoption of new models of USs;

taking into account the experience gained during the development of guidance documents on the combat use of USs;

improvement of the mechanism of dissemination of experience (examples) of USs application and its introduction into the USs specialist training system.

4. To increase the capabilities of the operational and strategic link of the air component of the USs, as well as the ground and sea components. The development of the capabilities (carriers of capabilities) of the USs shall be carried out in order of priority:

causing damage;

support (demining, demining, etc.);

reconnaissance (increasing awareness in the environment);

command and control (creation of USs networks for various purposes);

movement, maneuvering, logistics.

At the same time, the main efforts must be concentrated in the following areas (Table 3).

High autonomy, modularity, the ability to connect to a network and exchange data, the implementation of combined control and navigation systems (satellite/inertial/terrain), and the development of optical homing systems should be considered the main principles during the development of USs.

One of the main technical aspects during the development of USs is the implementation of elements of artificial intelligence in control systems, which will allow automatic recognition of objects (targets), capture, tracking and guidance of USs, automated data exchange between system elements.

This will significantly increase the efficiency of the application of USs, as well as make it

possible to reduce the burden on operators and the requirements for their competence. In the future, the process of using, for example, an attack UAV should look like this (Fig. 5).

In addition, during the development of a new generation of security systems, it is necessary to implement dual-purpose technologies, for example, LIDAR (Light Identification, Detection and Ranging) – a technology for obtaining and processing information about distant objectives using active optical systems to detect even disguised targets; non-lethal laser weapons (LWS/NL) for blinding guidance and personnel, etc.

Table 3. Prospective development directions of the Armed Forces of Ukraine unmanned systems

Component	Level	Type	Technical aspects
AIR	strategic	percussion (kamikaze); intelligence	development of unmanned aerial vehicles (UAVs) capable of ensuring the missions at the operational-tactical (operational, strategic) level (increased range and power, capable of operating in large groups with high autonomy, interconnection and different functional purposes (UAV groups - reconnaissance/strike/EW etc)); development of means capable of independently receiving external targeting from other UAVs, detecting, identifying, homing and hitting targets with minimal operator intervention (only at the stage of attack confirmation); creation of "swarms of drones", when one operator is able to control several UAVs simultaneously.
	operative	impact (reusable, kamikaze, FPV); intelligence	
	tactical	impact (reusable, kamikaze, FPV); intelligence	
GROUND	tactical	minesweeping (mining and demining); strike; intelligence; logistic (security)	Development: demining/demining robots; impact robots (machine gun, missile, anti-tank, artillery, mortar, anti-aircraft defense, kamikaze (self-propelled mines)) with a high degree of autonomy (see aviation); reconnaissance robots (network of remote sensors - optical, acoustic, seismic, etc.); portable (portable) robots of various purposes (impact, reconnaissance); auxiliary robots (for evacuating the wounded, transporting goods, transporting ammunition, CEW, etc.)
SEA	operative	strike (reusable, kamikaze); mine barriers	Development: surface/semi-submerged and underwater (shock and reconnaissance); surface/semi-submerged and underwater carriers of missile (anti-ship) torpedo and mine weapons (mine barriers).

Conclusion

Thus, the proposed futures reveal such a version of the future that will allow in a relatively short time to ensure the development of USs in the most important directions for the AF of Ukraine, taking into account existing trends, the capabilities of the state and partners, and is the most acceptable, from the point of view of the authors. At the same time, the trends for Ukraine were determined taking into account the experience of the other countries, but depending on the needs of our State.

During the development of the futures, the sequence of implementation of certain measures aimed at the development of USs was not established, given the need to implement them in a very short time, the aggression of the russian federation, the difficult economic situation and the limited technological capabilities of Ukraine.

It should be noted that the analysis of stakeholders indicates a relatively low degree of involvement of scientific research institutions (SRIs) of the Armed Forces of Ukraine in the development of USs. In order to provide effective scientific support for the processes of development, adoption and operation of the latest anti-aircraft defense systems, it is necessary to increase the role

and weight of theSRIs.

The directions of further research may be the development of a foresight for the development of the Armed Forces of Ukraine USs and program documents regarding the development of the USs (strategies, concepts, doctrines, etc.).

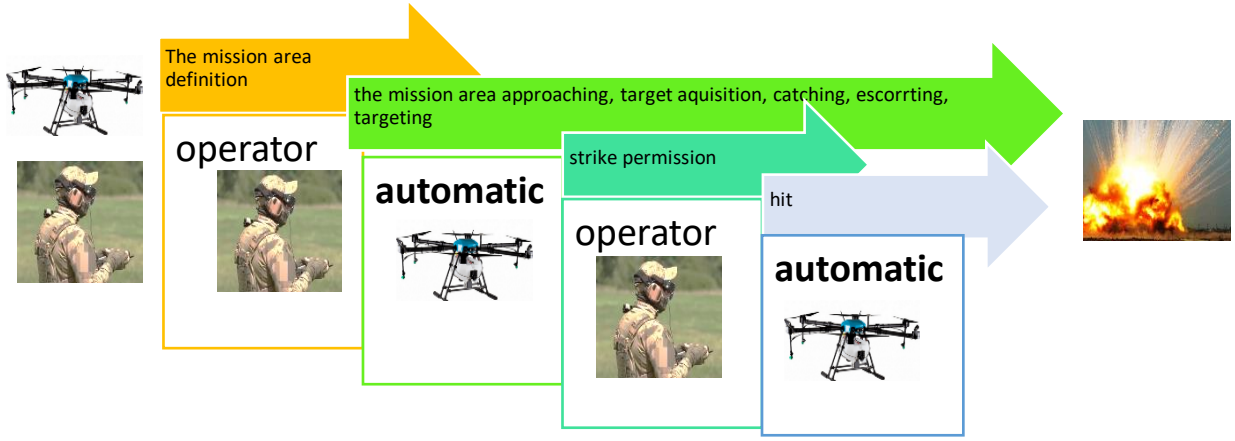


Figure 5. A promising procedure for the high degree of autonomy attack UAV application

Recommendations

The materials of the article my be used as an integral part of the foresight of the development of the unmanned systems of the Armed Forces of Ukraine, as well as during the formation and implementation of the military and military-technical policy of Ukraine. The article may be useful to specialists of information and analytical services, scientists and analysts that are involved in the development of the forecasts, development and justification of State decisions regarding the development of the USs domain.

References

1. "Eyes of the Army" US Army Roadmap for Unmanned Aircraft Systems 2010–2035. (2009). US Army UAS Center of Excellence: Fort Rucker, Alabama.
2. Albus, J., Cross R., & Duffy, J. (2018). Robotics and Autonomous Systems for Military Applications. *Journal of Defense Management*.
3. Bajart, A., & Förstner, W. (2021). *Robotics in Defense and Public Safety*. Springer.
4. British Army Approach to Robotics and Autonomous Systems. (2021). United Kingdom.
5. Carpin, S., Lewis, M., Liu, M., & Wang, M. (2018). *Field and Service Robotics*: Results of the 11th International Conference. Springer.
6. Chawla, S., Sreeram, A. N., & Pai, R. U. (2015). Application of Unmanned Aerial Vehicles in Modern Warfare. *International Journal of Computer Science and Mobile Computing*.
7. Croft, H. (2021). *Smarter Customer: The British Army & the Tech Revolution*. https://www.defenceiq.com/army-land-forces/editorials/smarter-customer-thebritisharmy the-tech-revolution/
8. Defense Advanced Research Projects Agency (DARPA) publications. https://www.darpa.mil/
9. Developing Future Capabilities: Robotics and Autonomous Systems. (2023). STC.
10. Kohn, E. (2020). *Concept for robotic and autonomous systems*. Australian Defense Force.
11. Heiming, G., & Geiger, W. (2021). *UGV Probot in der Felderprobung der Bundeswehr*. https://soldat-undtechnik.de/2021/10/mobilitaet/28943/ugvprobot in der felderprobung der bundeswehr/
12. Pathak, M., Bhandari, V. & Kumar, R. (2017). Autonomous Systems in Defense Environments:

Challenges and Opportunities. *International Journal of Advanced Research in Computer Science and Software Engineering*.
13. Rhydderch, A. (2009). *Scenario Planning*. Foresight Horizon Scanning Centre. https://gisf.ngo/wp-content/uploads/2020/02/0350-Rhyddarch-2009-Foresight-Horizon-Scanning-CentreScenario-Planning.pdf
14. Siciliano, B., & Khatib, O. (2016). *Springer Handbook of Robotics*, 2nd Edition. Springer.
15. Singh, AK, Verma, R., & Kumar, S. (2016). Applications of Robotics in Defense. *International Journal of Computer Science and Information Technologies*.
16. Singh, P., Khanna, A., & Bhatia, R. (2017). Unmanned Ground Vehicles for Military Applications. *Defense Science Journal*.
17. Strode, T., Beckworth, J. (2015). *Manned Unmanned Teaming (Ground) (MUM-T (G)) in Network Integration Evaluation (NIE)* 16.1, Maneuver Battle Lab.
18. The US Army Operating Concept – Win a Complex World 2020–2040. (2020). *TRADOC Pamphlet 525-3-1*. 2014.
19. The US Army Robotic and Autonomous Systems Strategy. (2021).
20. Tucker, P. (2021). US Army to Stage Largest Robot Tank Experiment Ever. https://www.defenseone.com/technology/2021/10/us-army-stage-largest-robottank-experimentever/186110/
21. US Army Capabilities Integration Centers System Threat Assessment Report (STAR) for Soldier as a System (SaaS) for 2022. (2022). US Department of the Army.https://apps.dtic.mil/sti/citations/AD1059546
22. Volkogon, V. V., Rul, O. M. & Volosyanko, M. M. (2019). Development and Application of Robotic Systems in the Armed Forces of Ukraine. *Military Technical Collection*.
23. Automated robotic weapons systems: a new challenge to the military security of Ukraine. (2017). https://niss.gov.ua/sites/default/files/2017-02/Ozhevan-86924.pdf
24. Blinkov, Yu. Prospects for the development of unmanned aviation in leading NATO countries. https://mil.in.ua/
25. Zaluzhnyi, V. F., Shaptala, S. O., & Koval, V. V. (2023). *Principles of development of robotic systems in the Armed Forces of Ukraine* (Ed. Semenenko, O. M.). Central Research Institute of the Armed Forces of Ukraine.
26. Zgurovsky Z. (Ed.) (2021). *Foresight of the development of the defense-industrial complex of Ukraine in the time horizon of 2021–2030*. KPI named after Igor Sikorskyi, "Polytechnic" Publishing House.
27. Kuprinenko, O. M. (2021). *Problems of creating ground robotic complexes for the needs of the Armed Forces of Ukraine*. https://doi.org/1034169/2414-0651.2021.4(32)
28. Semenenko, O., Baranov, S., Akinina, T., Dobrovolsky, Yu., Yarmolchyk, M. & Musienko, V. (2023). Conceptual views on the development and application of robotic complexes in the Armed Forces of Ukraine (concept, tasks, classification, management system, application tasks, prospects). *Social Development and Security*, No. 13 (3), P. 24–42. https://doi.org/10.33445/sds.2023.13.3.2
29. Solomytskyi, O. I. (2020). *Development of the theory and practice of forecasting the military and political situation* [Diss. dr. troops Sciences, Central Research Institute of the Armed Forces of Ukraine].
30. Shershakov, O., Shemaev, V., Begma, V. & Sklyar, N. (2020). *Regarding the development of the production of unmanned robotic systems based on public-private partnerships: an analytical note*. Institute of Strategic Studies.
31. Shugurov, O. S. (2007). Development of military ground robotic systems in the context of new concepts of management: perspectives of Ukraine. *Strategic priorities*. No. 4 (5). P. 198–205.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.02

A multi-domain operation – a modern view at the forms and methods of military operations adapting to the environment of challenges and threats transformation

Oleh Semenenko
doctor of military sciences, professor
Deputy Head of the Central Research Institute
of the Armed Forces of Ukraine for scientific work
03049, 28B Povitroflotskyi prospect, Kyiv, Ukraine
ORCID: 0000-0001-6477-3414

Volodymyr Koval
candidate of military sciences, senior researcher,
Deputy Chief of the General Staff of the Armed Forces of Ukraine,
03168, 6 Povitroflotskyi Prospect, Kyiv, Ukraine
ORCID: 0000-0002-6209-6779

Oleksandr Vodchyts
candidate of technical sciences, docent
Head of the department
Department of military training National Aviation University
Kyiv, Ukraine
ORCID: 0000-0002-3294-7632

Yuzef Dobrovolskyi
candidate of technical sciences, associate professor, senior researcher
Deputy Head of the Department of Academic Affairs
Department of military training National Aviation University
Kyiv, Ukraine
ORCID: 0000-0002-1077-1402

Abstract. Relevance of the article is due to the fact that Ukraine is currently faced with an operational response to hybrid threats from russia problem of, that include not only military aspects, but cyber security, information warfare, disinformation, non-military measures and other non-traditional methods of warfare also. One of the modern approaches to adopt the forms and methods of Defense Forces (Armed Forces) of Ukraine application of the to the conditions of the development of crisis situations of a military nature the transition to planning and conducting multi-domain operations, i.e. the simultaneous combination of actions in several spaces (domains) at once may be considered. The use of multi-domain operations technology is considered one of the ways to counter the enemy's hybrid threats effectively today. Therefore, the main goal of the article is to reveal the theoretical and practical essence of planning and conducting multi-domain operations, as well as the peculiarities of their organization and implementation. The main methods of research are methods of analysis and synthesis, deduction and induction. The main results of the article are what is defined in it: key features of a multi-domain space military operations conducting; basic aspects of planning and carrying out multi-domain operations; main measures for the preparation and implementation of

multi-domain operations; modern features of the transformation and prospects for adapting the forms and methods of military operations conducting by the Armed Forces of Ukraine in the multi-domain space. The materials of the article can be useful to the leaders of the Armed Forces of Ukraine at the operational and strategic levels, as well as to scientists and researchers in the barnches of research on issues related to the Armed Forces of Ukraine use and ensuring the military (national) security of the State.

Keywords: military operations, domain, use of armed forces, armed conflict, multi-domain operation, multi-domain space, armed aggression, hybrid war, national security, forms and methods of conducting military operations, russian-Ukrainian war, State Defense Forces.

"Technology is the only weapon that can win modern warfare" – Eric Schmidt

Introduction

The research and publications on the topic of the Defense Forces (DF) of Ukraine application forms and methods adaptation to modern challenges and threats of a global nature analysis is a key stage in the development of strategies and tactics in the field of national security. The topic of adaptation of the Ukraine's DF forms and methods of application of to modern challenges and threats became especially relevant during the active phase of the russian-Ukrainian war, that began since February 24, 2023. The Armed Forces (AF) and other components of the DF of Ukraine were forced to look for ways to adapt to new realities and improve strategies for responding modern challenges and threats (Donald M. Snider, & Lewis Sorley, 2016), (Matthew Kroenig, 2018), (Pylypenko, O., & Bazar, O., 2015), (Sun Tzu, approximately V century BC), (Carl von Clausewit., 1832), (Shust, V., & Pavelko, A., 2018), (lesson Shenanigans – Kenyan Hybrid Warfare), (Election Shenanigans – Kenyan Hybrid Warfare), (Menacing Malware Shows the Dangers of Industrial System Sabotage), (Gorbulin, V., 2017), (Daniel T. Lasica, 2009). During this period, there was a need for an operational response to hybrid threats from russia, covering not only military aspects, but also cyber security, information warfare, disinformation, non-military measures and other non-traditional methods of warfare.

The experience of the ongoing war in Ukraine and in the Middle East (the Arab-Israeli war) analysis results show that current research on the adaptation of the forms and methods of DF applying to conduct of modern warfare subject should be clearly focused on the main aspects, namely: evaluation of effectiveness the use of troops (forces) taking into account modern aspects of the use of innovative technologies; ensuring cyber security; improvements in military doctrine and strategic planning; the development of international cooperation in confronting the aggressor country to ensure stability and security not only in the region, but also in the context of a global scale.

Today, it becomes clear that one of the key areas of research is the optimization of strategies for adaptation of the DF to hybrid threats, which combine military, informational, cybernetic, non-traditional (non-standard) and non-military aspects. It is also important to study the possibilities of introducing innovations in military technologies and tactics of military operations, taking into account modern requirements and the realities of the geopolitical situation. The further development of research is aimed at improving strategies for military training and education, as well as developing effective mechanisms for interaction with other components of national security and other countries, unions, blocs to ensure their own security.

The results of such studies analysis will contribute to optimizing the use of resources and increasing the efficiency of the defense system development under the conditions of modern geostrategic challenges.

Materials and Methods

The forms and methods of the DF of Ukraine application to the modern, transformed environment of challenges and threats (the environment of conducting military operations) ways of adapting study will allow to reveal the main patterns and trends of the further development of the defense sphere of Ukraine, to develop strategies for adapting and improving the Armed Forces to the changing conditions of the situation, and will also contribute increasing the effectiveness of national security in crisis situations (Donald M. Snider, & Lewis Sorley, 2016), (Matthew Kroenig, 2018), (Pylypenko, O., & Bazar, O., 2015), (Sun Tzu, approximately V century BC), (Carl von Clausewitz,1832), (Shust, V., & Pavelko, A., 2018), (lesson Shenanigans – Kenyan Hybrid Warfare), (Election Shenanigans – Kenyan Hybrid Warfare), (Menacing Malware Shows the Dangers of Industrial System Sabotage), (Gorbulin, V., 2017), (Daniel T. Lasica, 2009), (John, R., & Davis, Jr., 2013), (Horbach, V., 2017), (Semenenko, O., Vodchyts, O., Tolok, P., Mytchenko, S., Hetman, A., & Tarasov, O., 2023), (Portnov, A., 2017), (Abroskin, I., 2022), (New technologies: changing the nature of irregular warfare, 2020), (Sungurovskyi, M., & Gavrilyuk, O., 2019), (Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O., 2022), (Semenenko, O., Voronchenko, I., Moskalenko, I., Abramova, M., & Kharitonov, K., 2021). As a result of the analysis, it became clear that this topic is of great importance for the development of military strategy, tactics, organization and structure of the Armed Forces (Defense Forces), the definition of national security strategies, and also helps to determine the key aspects of the study, namely:

historical examples and cases of adaptation of military strategies and tactics to crisis situations study. For example, analysis of military strategies changes in during World Wars, Cold War conflicts, etc.;

the study of how the development of new technologies affects the capabilities and methods of the military force use, which may involve analyzing the impact of drones, cyber weapons and other innovations on military activities;

the study of how geopolitical changes in the world affect the strategy and tactics of military operations. Adaptation may be necessary due to the changes in enemy forces and means, areas of influence and other factors;

the influence of the social context on the development of military strategies analysis. For example, how society reacts to armed conflicts and how this affects decision-making by the military leadership;

the impact on the adaptation capabilities of the armed forces (defense forces) of the economic restrictions study. Financial restrictions may affect the development of new weapons systems and military equipment, as well as technologies;

the impact of international relations and diplomacy on military strategies and adaptation possibilities, etc study.

the forms and methods of DF of Ukraine application to the transformed environment of challenges and threats adaptation requires a comprehensive approach and careful analysis.

Results

One of the modern approaches to the Ukraine's DF forms and methods application adaptation to the conditions of the development of crisis situations of a military nature of can be considered the transition to multi-domain operations (MDO), that is, a simultaneous combination of actions in several spaces (domains) at once. The use of multi-domain operations is a way to counter hybrid threats from the enemy.

The multi-domain operation is a modern view at the forms and methods of conducting military operations transformation, focused on complex tasks solving in a changing geopolitical environment.

This approach takes into account the importance of integration and synergy in-between different areas of military activity, as well as other important factors. The main aspects of this modern approach include (Election Shenanigans – Kenyan Hybrid Warfare), Menacing Malware Shows the Dangers of Industrial System Sabotage), (Gorbulin, V., 2017), (Daniel T. Lasica, 2009), (John, R., & Davis, Jr., 2013), (Horbach, V., 2017), (Semenenko, O., Vodchyts, O., Tolok, P., Mytchenko, S., Hetman, A., & Tarasov, O., 2023), (Portnov, A., 2017), (Abroskin, I., 2022), (New technologies: changing the nature of irregular warfare, 2020), (Sungurovskyi, M., & Gavrilyuk, O., 2019), (Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O., 2022), (Semenenko, O., Voronchenko, I., Moskalenko, I., Abramova, M., & Kharitonov, K., 2021):

integration of domains. MDO considers the role of land, sea, air, cyberspace and space as interdependent components, where actions in one domain can affect others and vice versa. Integration of these domains allows creating more effective and flexible strategies;

use of technology. MDO actively implements advanced technologies, such as artificial intelligence, cyber defense, autonomous systems and others, to increase the accuracy, efficiency and speed of conducting operations;

flexibility and adaptability. Modern threats and conflict scenarios can change dramatically, and the MDO makes it possible to adapt more quickly and flexibly to new conditions, providing an effective response to various challenges;

synergy with other areas. Outside of military activities, the MDO can interact with economic, political and other aspects, contributing to the creation of an overall strategy to achieve national and international goals;

information management and reporting. MDO requires a high level of information management to make informed strategic decisions and ensure effective control over operations.

In general, MDO is a modern approach to warfare aimed at optimizing the use of resources, increasing efficiency and reducing risks in a high-tech warfare environment.

A multi-domain operation is a military strategy that involves the integration of actions and resources in various military and civilian spheres (domains) to achieve a comprehensive strategic effect. Domains can include land, sea, air, space, information and electromagnetic spaces (Fig. 1).

Main multidomain spaces:

Land. Territorial operations on the land surface, including on land and the coast;

Sea. Operations in maritime space, as well as on the surface and under water;

Air. Military activities in the air space and in the atmosphere;

Space. Use of space resources, in particular satellites, to provide communication, intelligence and navigation;

Information and Cyberspace. Use of information technologies and networks for obtaining, processing and transmitting information.

Modern multi-domain operations are defined by a high degree of integration and cooperation

between the armed forces and other components of society. Information power and cyberspace have gained great importance, because conflicts can unfold not only in physical, but also in virtual space.

The main activities for the preparation and implementation of the multi-domain operations include:

integration and coordination by ensuring effective interaction between forces and assets in all domains;

information dominance, that is ensured by the use of information superiority, including cyberspace, for control and manipulation;

technological advantage, that is provided by the use of the advanced technologies in the fields of intelligence, communication, automation and weapons;

conducting regular training and simulations to increase the level of training and try different scenarios;

creation of the flexible command and control structures for quick response to changes in the combat environment, etc.

Multi-domain operations are becoming an increasingly important aspect of strategic planning as modern military operations are increasingly complex and integrated (Shust, V., & Pavelko, A., 2018), (Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O., 2022). Modern features of conducting military operations in the multi-domain space are determined by the wide use of various technologies and strategies covering several different domains. The table 1 shows several key features of conducting military operations in a multi-domain space with their characteristics.

The transformation of the forms of the military operations conducting in the land domain contains numerous aspects that reflect new requirements, technological and strategic changes in the modern military sphere.

The new technologies and strategies development occurs in the context of changes in the nature of threats, the geopolitical environment, and sociocultural factors.

The application of the latest technologies, such as unmanned systems, artificial intelligence, cyber weapons and smart military systems is one of the key aspects of the transformation. These technologies make it possible to increase the accuracy and efficiency of operations, as well as reduce risks for military personnel. Strategic changes consist in rethinking of the military doctrine and tactical approaches to ground operations. Increasing emphasis on hybrid warfare, cyber security, and responding to new forms of threats such as terrorism and non-standard combat scenarios are becoming important parts of the strategic rethink. In particular, it becomes important to integrate various types of troops and means of warfare to create more flexible and comprehensive strategies. Particular attention is paid to the development of mobility, communication system and information power to ensure a quick and coordinated response to modern threats. In general, the transformation of warfare on land reflects the need to innovate and adapt to changes occurring in the modern military environment to ensure national security and global stability.

The transformation of warfare in the airspace is taking place in the context of various technological and strategic changes that define new requirements and capabilities for the Air Force. In connection with the emergence of advanced technologies and the evolution of strategies, the Air Force is rethinking its role, moving from traditional conflicts to modern forms of military operations. Technological changes involve the development of new types of aircraft, the use and development of unmanned (robotic) systems, and the introduction of artificial intelligence in air operations. These technologies contribute to increasing the accuracy, maneuverability and intelligence of the Air Force.



Figure 1. Modern features of the Armed Forces of Ukraine transformation and prospects for adapting the forms and methods of military operations of conducting in the multi-domain space

The presented military operations in a multi-domain space conducting features are determined by rapid technological development and the need to adapt to modern challenges in the global military environment.

Table 1. The multi-domain space military operations conducting key features

No	Features	Characteristic	Importance for the transformation of military operations
1	Integration and interaction	Ensuring effective interaction and integration of various types of forces, i.e. land, sea, air, space and information space.	Synergy of actions in all domains, which allows more effective use of various military and civilian resources.
2	Digital warfare and cyberspace	Conducting conflicts in cyberspace and using digital technologies to wage a war.	Attacks on information systems, cyberespionage, influence on communication networks are becoming an integral part of military operations.
3	Mass use of drones	Large-scale use of unmanned systems for reconnaissance, attacks and various missions in all domains.	Increasing efficiency, reducing risks to life, but also new challenges arise, such as the danger of drone attacks.
4	Hybrid war	The use of various methods, including military, informational, economic and political, to achieve strategic goals.	Applying a combination of traditional and non-traditional methods to obtain benefits.
5	Hypersonic means and anti-weapon countermeasures	Hypersonic means and systems development to counter hypersonic strikes.	Increasing the speed and complexity of weapons, as well as developing means of countering these attacks.
6	Satellite systems and space domains	Use of space systems for reconnaissance, navigation, communications and warfare.	Ensuring geostationary superiority and responding to challenges in the field of anti-satellite countermeasures.
7	Hybrid management and artificial intelligence	Use of artificial intelligence systems for decision-making and automation of combat processes.	Increased responsiveness and adaptability, but with associated ethical and security challenges.

The main aspects of the transformation of the forms and methods of conducting military operations are given in the table 2 and in the fig. 1.

Table 2. The forms and methods of the military operations conducting transformation main aspects

No	Key features of military operations conducting	Characteristic	Importance for the transformation of military operations
		Domain "Land"	
1	Integration of technologies	Use of modern technologies to increase the accuracy and efficiency of operations on land, such as artificial intelligence, cyber defense, precision weapons.	Improving intelligence capabilities, ensuring accurate and efficient operations.
2	Mobility and expeditionary operations	Mobile military formations development and application and rapid response to changes in the environment concepts.	The ability to move forces and assets quickly to adapt to new threats and challenges.
3	Comprehensive intelligence and surveillance	Use of intelligence from various sources, including drones, satellite systems, intelligence groups.	Providing full-fledged information accounting of the situation for effective decision-making.
4	Hybrid warfare on land	Application of various methods, including informational, economic, cyber and military, to achieve strategic goals.	A new level of complexity in military conflicts that requires flexibility and adaptation.
5	Tube (rocket) artillery and missile systems	Improvement and mass use of artillery and missile systems for accurate hitting of targets on land.	Increasing the range and accuracy of hitting targets.

Table 2 (countinuation). The forms and methods of the military operations conducting transformation main aspects

6	Inventory management and logistics	Application of the latest technologies for efficient management of stocks, supply and logistics.	Increasing the speed and efficiency of moving military formations and material resources.
7	Hybrid threats and countermeasures	Measures to protect against hybrid threats such as terrorism and hybrid attacks.	Increasing the ability to cope with new forms of hostile activity.
8	Training and learning	Application of modern methods of training and simulations to prepare the military for operations on land.	Ensuring a high level of readiness and adaptability of forces.
Domain "Air"			
1	Unmanned aviation and drones	Wide use of unmanned aerial vehicles (UAVs) for reconnaissance, strike and logistics tasks.	Increasing reconnaissance capabilities, reducing risk for pilots, new challenges in the field of cyber defense.
2	Hypersonic aircraft	The use and development of aircraft capable of traveling at the speeds, that are highly exceeding the speed of sound.	Increased speed and unparalleled ability to react quickly.
3	Integration and network operations	Air Force interactions with other domains and the use of network technologies to provide coordination and information sharing.	Improved operational efficiency through improved communication and data sharing.
4	Electronic warfare and cyber defense	The use of electronic warfare for intelligence and support missions, as well as enhancing the cyber defense of the air systems.	Providing protection against electronic attacks and ensuring the integrity of systems.
5	Vertical take-off and landing vehicles and helicopters	Increasing the use of vertical take-off and landing (VTOL) to improve mobility and operational efficiency.	Ability to operate in conditions where access to conventional airfields is limited or impossible.
6	Aircraft capable of autonomous flight	The development of aircraft capable of autonomous flight and performing tasks without the direct control of the pilot.	Improving the effectiveness and capabilities of missions through autonomy.
7	Lots of data and analytics	Using large amounts of data and analytics for decision-making and intelligence at various stages of tasks.	Improving the ability to analyze and use intelligence information.
8	Global presence	Increasing the ability to have a global presence and respond quickly to threats anywhere in the world.	Ensuring rapid response to conflict escalation and security threats.
9	Development of hypersonic technology	Use of hypersonic technologies to create and improve means of conducting military operations in airspace.	Increasing the speed and efficiency of operations.
Domain "Sea"			
1	International security and protection of sea routes	Ensuring the security of sea routes and control over territorial waters to protect against threats and hostile influence.	Preservation of maritime freedom and economic interests.
2	Expeditionary operations and power projection	The ability to project military power over long distances to solve strategic tasks quickly and effectively.	Flexibility and ability to respond to different threats in different parts of the world.
3	Multidomain integration	Interaction with air, land and space for synergy and ensuring integrated operations.	Improving coordination and effectiveness between different domains of warfare.
4	Anti-submarine warfare	Development of means and strategies for detecting and countering underwater objects.	Ensuring the safety of the maritime space and avoiding underwater threats.
5	Means of countering the aerial threats	Development and application of means of combating air attacks for the protection of ships and other objects.	Ensuring security against air threats and increasing defense capabilities.

Table 2 (countinuation). The forms and methods of the military operations conducting transformation main aspects

6	Naval Blitzkrieg and Hybrid Warfare at Sea	Use of hybrid warfare strategies in the maritime environment, including asymmetric and non-standard threats.	Adapting to a variety of threats and conducting operations in a complex environment.
7	Environmental awareness and infrastructure	The ability to conduct military operations, taking into account the impact on the environment and existing infrastructure.	Ensuring sustainable use of maritime space and taking into account environmental aspects of military operations.
8	Global presence and capacity to deliver humanitarian aid	Ensuring the possibility of providing humanitarian aid and the ability to respond to natural disasters quickly.	Use of naval forces to support global humanitarian tasks.
9	Ensuring full security of maritime logistics infrastructure	Measures to protect naval bases, ports and logistics infrastructure from possible threats.	Ensuring long-term operational capability through secure provisioning and support.
Domain "Cyberspace"			
1	Cyber protection and cyber security	Development of measures to protect critical infrastructures and information systems from cyberattacks.	Ensuring stability and security in the information space.
2	Cyber military operations and cyber attacks	Carrying out operations in cyberspace with the aim of causing damage, gathering information or hindering the work of the adversary.	The use of cyber means as a component of military conflict.
3	Information warfare and influence	The use of information means to manipulate public opinion, influence decision-making, and create an image of the enemy.	Directed influence on the information field to achieve military and political goals.
4	Artificial intelligence in cyberspace	Using artificial intelligence to identify and analyze threats, automate cyber defense and implement cyberattacks.	Improving the speed and accuracy of response to cyber threats.
5	Cyber military forces and cyber command	Creation and development of specialized military units for conducting operations in cyberspace.	Ensuring expert qualification and ability to conduct cyber military operations.
6	Cyber special operations and cyber intelligence	The use of cyber means for conducting intelligence, gathering information and implementing special operations in cyberspace.	Carrying out actions in cyberspace for the purpose of obtaining intelligence information and ensuring security.
7	Cyber hybrid threats	The combination of cyberattacks with other types of threats such as information, hybrid warfare and cyber terrorism.	Complication of warfare and increase in the number of potential threat options.
8	International cyber coordination and regulations	Development of international standards, provisions and treaties for cyber military relations regulation.	Ensuring stability and control in cyberspace.
	Training and training of cyber defense forces	Development of training and training programs to ensure high qualification of cyber specialists.	Training the military to operate effectively in cyberspace and respond to cyber threats.
Domain "Space"			
1	Space intelligence and response	Application of satellite systems for reconnaissance, navigation and ensuring the accuracy of military operations.	Ensuring high-quality intelligence and prompt response to changes in the situation.
2	Space communication and signal communications	Use of space systems to ensure continuous and secure communications between military units.	Ensuring effective communication and coordination over long distances.
3	Space defense and anti-satellite means	Development of systems and technologies for protection against attacks on space assets and anti-satellite means.	The normal functioning of space vehicles guaranteeing and protection against enemy interference.

Table 2 (end). The forms and methods of the military operations conducting transformation main aspects

4	Space Armed Forces	The development and use of military systems located in outer space for the implementation of various tasks.	Ensuring military superiority and the ability to conduct operations at various levels.
5	Cooperation in outer space	Development of international cooperation and standards for the use of outer space for peaceful and military purposes.	Reducing the possibilities of conflicts in outer space and joint implementation of projects.
6	Space intercontinental strike means	The use of space means to deliver strikes (carrying out strikes?) over long distances between continents.	Ability to influence strategically and conduct global operations.
7	Space electronic warfare	The use of electronic means of influence in outer space for reconnaissance and enemy interference tasks.	Ensuring the effectiveness of electronic warfare and control over the electromagnetic space.
8	Exploration and navigation in outer space	Use of satellite systems for reconnaissance and navigation to support operations in other domains.	Ensuring the accuracy and reliability of information for conducting military operations.
9	Space ecological consciousness	Consideration of outer space from the point of view of preserving its sustainable functioning and maintaining environmental cleanliness.	Reducing the impact of military operations on the space environment.

Strategic changes reflect a rethinking of the tasks and functions of the Air Force in modern military conflict. There is an increasing emphasis on integration with other types of forces, including cyber and space forces. The strategies also involve adapting to hybrid threats such as cyberattacks and unmanned aerial vehicles. Flexibility, mobility and the ability to adapt to the changing conditions of the theater of operations are key requirements for the Air Force. The development of communications and information technology systems is also important to ensure effective coordination and communication during hostilities. All this indicates the need for a constant innovative approach and a modern definition of the role of air forces in military strategies, in particular, to ensure safety and efficiency in modern combat conditions.

The transformation of the forms of conducting military operations in the "Sea" domain contains a number of key aspects that reflect modern trends, technological development and strategic changes in the maritime military environment. The transformation of the conduct of military operations in the maritime space takes place in the context of changes in geostrategic conditions, technological innovations and the needs of the modern security environment. One of the key aspects of the transformation is the development of new technologies in the field of naval warfare. The use of unmanned vessels, nuclear and hybrid energy systems, effective means of intelligence and communication makes it possible to conduct operations more accurately and provides an advantage in the maritime space. It is important to adapt strategies to changes in geostrategic conditions. Growing competition for resources, the development of the Arctic as a new arena for geostrategic interests, as well as the impact of climate change on sea lanes require new strategies for conducting maritime operations. The conditions of the modern security environment also reflect the need to ensure maritime security, combat transnational threats such as piracy and terrorism, and the ability to effectively interact with other types of military and civilian structures. In general, the transformation in naval warfare is defined by the need to adapt to new challenges and opportunities arising in a changing global context and the development of innovative strategies and technologies to ensure maritime security and the effective conduct of operations in this important domain.

The transformation of warfare in the Cyberspace domain is taking place in connection with the rapid development of technologies and changes in the nature of military threats. The transformation of conducting military operations in cyberspace is determined by rapid technological development and the emergence of new challenges in this area. Adaptability and innovation are becoming key

factors for effective operations in this space. In today's world, cyberspace has become an important field for conducting military operations, as digital technologies have penetrated all spheres of life. Advances in artificial intelligence, cyberattacks, and other aspects of cybersecurity are creating new opportunities for warfare while simultaneously endangering national and international security. Changes in the nature of threats in cyberspace require constant improvement of strategies and technical solutions. In particular, the ability of countries and military organizations to adapt their approaches to new technologies and skills of cyber military threats is important. Cyber security innovation, cyber threat studies, and training of military personnel are becoming critical components to ensure successful operations in this critical space. Given these transformations, it is important to maintain international cooperation and develop cybersecurity standards to create a united line of defense against cyber threats and ensure stability and security in this important military domain.

The transformation of the military operations in the "Space" domain conducting forms is taking place in the context of the rapid development of space technologies and strategic changes in the geostrategic environment. This process involves not only technical aspects, but also the formation of new strategies and tactics aimed at ensuring national security in outer space. With the advent of new technologies such as satellites, space weapons and space intelligence systems, the role of space in the military has become extremely important. Countries are actively working to develop and improve means of space warfare to ensure strategic superiority and control in outer space. At the same time, changes in the geostrategic environment require the adaptation of strategies for warfare in outer space. The growing competition between countries for resources and influence in space makes it urgent to develop and implement effective strategies aimed at preserving national security in this new military domain. In this context, there is a need for international cooperation and the development of international standards for the regulation of space warfare in order to prevent conflicts and ensure stability in space. National and international policy efforts should be directed toward creating balanced and sustainable strategies for warfare in outer space to preserve peace and stability at the planetary level. The transformation of the military operations conduct in outer space is determined by the struggle for control and use of this domain resources, as well as the resolution of issues of international cooperation and environmental sustainability.

The russian-Ukrainian war has showed that the transformation of modern forms and methods of conducting military operations is currently place actively taking as a result of the influence of both the hybridization factor and the technological factor of military confrontation. The main types of operations that characterize the conduct of military operations in the russian-Ukrainian war include point and mass drone strikes, mass and combined unmanned operations, as well as, in order to counter drones, anti-drone operations, etc.

Spot and mass drone strikes have become an important component of modern warfare strategies.

Spot drone strikes are strikes aimed at specific objects or targets in a limited area. Point strikes try to minimize collateral damage and are aimed at specific, often strategically important, objects. Point-of-care drone strikes require precise targeting, high accuracy of strikes, the ability of artificial intelligence to recognize and select targets, and coordination with other systems.

Mass drone strikes are strikes where many drones launch synchronized attacks on large areas or groups of targets. The purpose of such strikes is to maximize the impact and coverage of the territory. Massive drone strikes require a large number of drones, synchronization of attacks, effective communication and control of a group of drones. Algorithms for the distribution of targets are used for optimal coverage of the territory.

The main measures for the preparation and execution of drone strikes include:

intelligence and recognition. It is necessary to have reliable intelligence to accurately identify targets;

technical training. Provide drones with high accuracy, high speed and the ability to evade anti-

aircraft weapons;

communication and management. Provide a reliable control and communication system between drones and operators;

protection against countermeasures. Countermeasures implementation (antiviruses, electromagnetic protection systems, etc.).

It is important to note that the use of drones in military operations should be in accordance with international legislation and rules, and ethical and humanitarian issues may arise in this connection.

A mass drone operation is the coordinated activity of a large number of unmanned aerial vehicles (drones) with the aim of influencing a defined area or objects, often using a significant number of drones to simultaneously attack or perform different tasks.

Massive unmanned operations are a modern approach to conducting operations that can provide great flexibility and efficiency in various situations. Consideration of ethical, legal and security issues is an important aspect when designing and implementing such operations.

A combined unmanned operation is a type of military strategy that uses a combination of different types of unmanned vehicles and their interaction to achieve complex strategic goals. This strategy involves the use of a variety of drones with different functions and capabilities in a single, coordinated operation. Combined Unmanned Operations use different types of drones to maximize efficiency and a wide range of capabilities in different scenarios. Effective planning, technology integration and security are key components of successful implementation of such operations.

An anti-drone operation is a military or civilian activity aimed at detecting, identifying, interacting or neutralizing unmanned aerial vehicles (drones) that may pose a threat to security, privacy or violate laws and regulations. An anti-drone operation requires a comprehensive approach to identify and neutralize potential threats that may arise from the use of drones.

The main characteristics and measures for carrying out the above types of modern operations in various domains are presented in the table. 3.

In today's combat environment, warfare is increasingly dependent on the use of unmanned aerial vehicle, including targeted and massed drone strikes, massed and combined unmanned operations, and counter-drone operations (anti-drone operations).

Multi-domain operations involve interaction and coordination between different domains or areas of activity, such as information security, network communications, data processing, cloud computing, and others. Here are some of the main modern technologies used in a multi-domain operations system:

artificial intelligence (AI): AI is used to automate the decision-making processes, analyze large volumes of data, make predictions, and more. In multi-domain operations, AI can be applied to automate threat response, anomaly detection, and improve overall operational efficiency;

Blockchain: Blockchain technology provides a decentralized and reliable data storage system that can be useful for data security and identity verification in multi-domain operations;

cyber security: cyber security technologies such as network firewalls, intrusion detection systems (IDS), access management systems (AMS), data encryption and many others are used to protect multi-domain operations from cyberattacks;

cloud computing: cloud services provide the ability to store and process data in different domains through virtual computing resources, which facilitates data exchange and collaboration between different domains;

Internet of Things (IoT): IoT devices enable the collection and exchange of data between various objects and systems. In multi-domain operations, they can be used to collect data from different domains and provide their analysis and management;

process automation: the use of various automation tools, such as robots with artificial intelligence (Robotic Process Automation, RPA) or automated control systems, makes it possible to optimize processes in multi-domain operations and reduce the level of errors;

data analytics: Data analysis technologies such as machine learning, natural language processing (NLP) and others help extract valuable insights from large volumes of data collected from different domains to support decision-making in multi-domain operations.

Table 3. Combined and massive unmanned operations and anti-drone operations conducting main characteristics and measures

Characteristic	Content of the main activities
Massive unmanned operation	
Massiveness	Number of drones: Mass drone operations involve a significant number of drones that can be used for a wide range of tasks.
Various functions	Attacks: Depending on the operator's needs, drones can perform air or ground attacks. Intelligence and Reconnaissance Tasks: Drones can be used for intelligence gathering and data transmission.
Coordination and communication	Control systems: There is a need for reliable and secure control systems to effectively coordinate the actions of a large number of drones. Communication networks: creation of reliable communication networks for transmitting commands and receiving information in real time.
Automation and artificial intelligence	Autonomy: Some mass operations may involve autonomous drones that independently perform tasks based on programming and analysis of the surrounding environment. Artificial Intelligence: Using artificial intelligence algorithms to identify and analyze targets and optimize decisions in real time.
Security and challenges	Defense against interference: development of means of protection against electromagnetic interference and other threats to unmanned systems. Information security: protection against hacker attacks and ensuring the confidentiality and integrity of data.
Application in various fields	Military use: Mass drone operations are widely used by the military to carry out attacks, reconnaissance and other tasks. Civilian use: applications in civilian areas such as natural disaster intelligence, agricultural sector, etc.
Combined unmanned operation	
Various drones	Tactical aircraft: drones designed for close-range attacks and reconnaissance. Strategic Drones: Drones capable of long-range operations and large-scale missions. Reconnaissance drones: designed for information gathering and reconnaissance without interfering in the combat space.
Integration and coordination	Joint communications: ensuring effective information exchange between different types of drones and command centers. Control systems: development of a single control system to coordinate the entire network of unmanned aerial vehicles.
Automation and artificial intelligence	Autonomy Systems: Using Autonomy Technologies to Make Independent Decisions by Drones in Real Time. Artificial intelligence: implementation of artificial intelligence algorithms for analysis and interpretation of received data and automation of decision-making processes.
Distribution of tasks	Drone Specialization: Using drones with various specialized capabilities to effectively perform specific tasks. Interaction between classes: ensuring the interaction and synchronization of the operation of different classes of drones.
Adaptability and flexibility	Responsiveness: the ability of a drone network to adapt to changes in the combat environment and shift focus to the most important tasks. Backup Mechanisms: Implementation of security measures and backup mechanisms to avoid losses in case of loss of individual drones.

Table 3 (end). Combined and massive unmanned operations and anti-drone operations conducting main characteristics and measures

Safety and ethics	Cyber threat protection: ensuring network security and protection against cyberattacks. Ethical aspects: consideration of ethical principles in the use of unmanned systems in military operations.
Anti-drone operation	
Detection and recognition	Using radars, thermal imaging sensors, optical cameras and detection systems to recognize drones in the air. Consideration of various characteristics of drones, including size, speed, shape and other parameters.
Identification and classification	Using identification systems that can identify the type and model of drones. Application of databases for classification of drones and recognition of their manufacturers.
Interaction and interception	Using crash signals to disrupt drone operation and loss of control. Use of interception systems, such as radio frequency or other methods of jamming the drone's signal.
Physical intervention	Using means of physical interference to destroy or operate drones, such as using lasers or other energy systems.
Protection against cyber threats	Preventing the possibility of hacking and taking control of drones. Protection against attacks on infrastructure and management systems.
Intelligence and counterintelligence	Carrying out constant monitoring of the airspace to identify potential threats. Use of drones or other means to detect and recognize drones.
Use of technical means	Installation of anti-drone systems such as radars, signal jammers and interceptors. Application of technical means for detection and blocking of unmanned aerial vehicles.
Staff training and education	Training of personnel for effective interaction and response to various scenarios of anti-drone operations. Use of simulators and training grounds for training.
Legislative measures	Establishing rules and restrictions on the use of drones in certain areas or at a certain distance from objects that need protection.
Coordination with airports and air traffic control	Cooperation with airports and air services to control drones to identify and eliminate potential threats.
Ensuring security	Installation of defense systems against cyberattacks and provision of appropriate security measures for anti-drone systems.

These technologies can be used separately or in combination to create integrated management systems and optimize multi-domain operations.

The study of modern technologies in the system of multi-domain operations is of great importance during a conflict such as the russian-Ukrainian war for several reasons:

ensuring security and defense capability: thanks to the use of advanced technologies in the multi-domain operations system, countries have the opportunity to ensure more effective control over their territorial interests and reduce the risks of military threats;

cyber security and information warfare: Cyber security and information warfare are given a lot of attention in modern conflicts. Thanks to the research of the latest technologies, countries protect their information resources and infrastructure from cyberattacks, as well as carrying out their own operations in this area;

efficient use of resources: It is possible to optimize the use of resources that may be limited during a conflict thanks to the development and implementation of modern management technologies;

international cooperation: the modern technologies in the system of multi-domain operations study may contribute to cooperation between countries working together to solve modern security challenges;

moral and ethical aspect: the use of advanced technologies also requires discussion of moral and ethical issues that may arise as a result of their implementation, in particular, in the field of automation and robotization of military operations.

Therefore, the modern technologies in the system of multi-domain operations study during the ongoing russian-Ukrainian war is critically important for ensuring national security, effective use of resources, and successful conduct of military operations.

Discussions

The main prospects for the forms and methods of military operations conducting transformation in the modern combat environment include:

deep, dynamic development of technologies: the prospects include the continuous development of technologies in the field of unmanned aviation, the improvement of artificial intelligence systems and the increase of the autonomy of drones;

integration with other technologies: interaction of unmanned systems with cybernetic and other modern technologies to create highly effective and complex military strategies;

ethical and legal aspects: the production and use of drones requires attention to ethical and legal issues, particularly those related to privacy, security and liability.

In general, the introduction of unmanned technologies opens up new opportunities for conducting military operations, providing a more effective and safer strategy compared to traditional methods. At the same time, new challenges arise related to protection against anti-drone threats, regulation of use and development of ethical standards in the military sphere.

Conclusion

The research and implementation of modern technologies in the system of multi-domain operations are of great strategic importance in the context of the ongoing russian-Ukrainian war. The security challenges, including cyber threats, hybrid attacks, and information warfare, that are given today's, the effective use of advanced technologies is becoming a key aspect for ensuring national security and defense capability.

The research in this field helps countries strengthen their defense capabilities, improve the protection of critical infrastructure, respond effectively to threats, and ensure the safety of their citizens. In addition, it promotes international cooperation and exchange of experience between countries to counter modern security challenges.

The investment in the research of modern technologies in the system of multi-domain operations, in general, is a critically important element of the strategy of ensuring national security and successful conduct of military operations under the conditions of the modern geopolitical environment.

Recommendations

Multi-domain operations, that cover different types of warfare and use a variety of military and non-military means, are becoming an important part of a strategic planning in today's combat environment.

We offer the basic recommendations for the prospects for the development of such operations formation, taking into account the experience of the russian-Ukrainian war and the Israeli war against Hamas in 2023.

1) Integration of various types of troops. Development and improvement of communication and communication systems between the components of the armed forces, including land, air, sea and

space components, which will contribute to more effective coordination and joint work between various branches of military activity.

2) Information warfare and cybernetic aspects. The growing role of cyber operations and information warfare in multi-domain conflicts. Establishing cyber measures to affect enemy communications systems, electronic systems and infrastructure.

3) Use of unmanned technologies. Intensive development and use of unmanned aerial vehicles in all areas of military activity, including reconnaissance, strikes, transportation and medical assistance. Effective use of drones can provide an advantage in combat operations.

4) Synergy with special operations forces. The importance of the special forces that can perform a variety of tasks in different areas of the combat zone. The operational mobility and flexibility of such forces make them a key component of multi-domain operations.

5) The technologies of hybrid warfare and modern conflicts application. Consideration of hybrid threats, that include not only military, but also political, economic and other aspects. Adapting strategies to the specifics of hybrid warfare and using conflict experience to build more complex strategies.

6) Development of innovations in technologies and weapons. Application of advanced technologies such as artificial intelligence, pattern recognition and cyber-physical systems. Improvements in weapons and equipment to ensure accuracy, maneuverability and reliability in a multi-domain conflict.

7) Taking into account the geopolitical aspect and international cooperation. Development of strategies that take into account geopolitical realities and the possibility of international cooperation in multi-domain operations. Joining the efforts of different countries can become a key element for ensuring stability and countering threats.

8) Development of humanitarian aspects. Consideration of humanitarian aspects in planning and conducting operations. Balanced strategies that take into account the needs of local populations can contribute to saving lives and restoring stability after conflict ends.

9) Application of the non-military methods of confrontation. Development and implementation of the non-military methods of confrontation, such as diplomacy, economic pressure and other non-aggressive strategies to achieve the goal without escalating the conflict.

10) Active use of asymmetric warfare technologies. Taking into account the possibilities of asymmetric threats and warfare techniques. Optimizing strategies for fighting small but technologically advanced opponents.

11) Ensuring cyber security. The growing focus on cyber security in multi-domain operations, given the possibility of cyberattacks on critical military and civilian infrastructure.

12) Emphasis on training and preparation. Development of education and training programs for military and civilian personnel aimed at understanding and effective use of various means and methods in multi-domain operations.

Considering these aspects, multi-domain operations become necessary for effective warfare in today's world, especially during conflicts where a variety of technologies are used and flexible and adaptive strategies are defined. The abovementioned main aspects of multi-domain operations take into account the dynamics of the modern combat environment and develop in accordance with modern challenges and trends in the military sphere. Multi-domain operations require the integration of various means and strategies to achieve a comprehensive and effective response to modern threats.

Acknowledgments

The authors declare that they have no competing interests in the subject of the article.

References

1. Donald M. Snider, & Lewis Sorley (2016). *Understanding War: An Annotated*

Bibliography. Washington, DC. Strategic Studies Institute, US Army War College. P. 157.
2. Matthew Kroenig (2018). *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters*. Oxford. Oxford University Press. P. 312.
3. Pylypenko, O., & Bazar, O. (2015). *Military art of Ukraine: history and modernity*. Kyiv. Criticism. C. 256.
4. Sun Tzu. *The Art of War*. (approximately V century BC). Ancient China.
5. Carl von Clausewitz. (1832). *On War*. Berlin. Dümmlers.
6. Shust, V., & Pavelko, A. (2018). *Military strategy: theory and practice*. Kyiv. NUOU. P. 320.
7. lesson Shenanigans – Kenyan Hybrid Warfare (Book). ASIN B08DMZJ893.
8. Election Shenanigans – Kenyan Hybrid Warfare (Book). ASIN B08DGP72MH.
9. Menacing Malware Shows the Dangers of Industrial System Sabotage.
10. Gorbulin, V. (2017). What kind of Phoenix will be born from the ashes of the global hybrid war? 3d of November. *Mirror of the week*.
11. Daniel T. Lasica. (2009). Strategic Implications of Hybrid War: A Theory of Victory. *School of Advanced Military Studies*.
12. John, R., & Davis, Jr. Defeating Future Hybrid Threats. (2013). *Military Review*, September-October 267. 7. Armed Forces Journal: Hybrid vs. compound war (eng.) (1.10.2009). http://armedforcesjournal.com/hybrid-vscompound-war/
13. Horbach, V. (2017). *Military strategy of Ukraine*. Kyiv. NUDU. P. 256.
14. Semenenko, O., Vodchyts, O., Tolok, P., Mytchenko, S., Hetman, A., & Tarasov, O. (2023). The main theoretical and practical aspects of conducting proxy wars and hybrid wars in the modern global geopolitical and security environment: history, theory, practice, forms and methods, experience for Ukraine. *Social development and security*, No. 13 (3), pp. 1–23. https://doi.org/10.33445/sds.2023.13.3.1
15. Portnov, A. (2017). *Ukrainian wars: from the collapse of the Soviet Union to modern conflicts*. Kyiv. KM-Buks. P. 312.
16. Abroskin, I. (2022). *Hybrid warfare: threats and responses*. Kyiv. Yakabu Publishing. 305 p.
17. New technologies: changing the nature of irregular warfare. (2020). Modern Diplomacy. https://moderndiplomacy.eu/2020/05/11/emerging-technologies-changing-nature-of-irregular-warfare.
18. Sungurovskyi, M., & Gavrilyuk, O. (2019). *Military reform in Ukraine: strategic challenges and solutions*. Kyiv. Institute of National Security Problems named after I. Yavornytskyi. P. 160.
19. Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O. (2022). Russia's military expenditures analysis and their structure in the period 2010-2022 (some aspects of the influence and consequences of the russian-Ukrainian war for Ukraine). *Social development and security*, No. 12 (5), pp. 116–129. https://doi.org/10.33445/sds.2022.12.5.11.
20. Semenenko, O., Voronchenko, I., Moskalenko, I., Abramova, M., & Kharitonov, K. (2021). A methodological approach to assessing the ability of the national economy to ensure a sufficient level of defense capability. *Social Development and Security*, 11(5), 133–145. https://doi.org/10.33445/sds.2021.11.5.13
21. Solomytskyi, A., Semenenko, O., Onofriychuk, P., Slyusarenko, M., Baranov, S., & Mitchenko, S. (2022). Forecasting the risk of armed conflict based on the analysis of military costs. *Social Development and Security*, 12 (1), 164–

174.https://doi.org/10.33445/sds.2022.12.1.15

22. Semenenko, O., Deinega, O., Voronchenko, I., Borysyuk, S., Mytchenko, S., & Taran, O. (2021). To the question of the transformation of the forms and methods of military operations in the conditions of hybrid wars. *Social Development and Security*, 11 (2), 256–271.https://doi.org/10.33445/sds.2021.11.2.22
23. Wojtowicz, T., & Król, D. (2019). Multi-domain battle. The new doctrine of the Armed Forces of the United States. *Zeszyty naukove akademii sztuki wojennej*. Vol. 112, No. 3. P. 64–78.
24. Semenenko, O., Taran, O., Mytchenko, S., & Butenko, R. (2022). Recommendations on the forms and methods of use of the Defense Forces of Ukraine adapting to the conditions of conducting military operations, taking into account the influence of the hybridization factor. *Collection of sciences. pr. CSRI of the Armed Forces of Ukraine*, 2 (101), 16–31.

The Central Research institute
of the Armed Forces of Ukraine
Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.03

Technologies of information and psychological influence on people in modern wars

Ihor Chepkov
Doctor of Technical Sciences, Professor
Head of the Central Research Institute of Armament
and Military Equipment of the Armed Forces of Ukraine
The Central Research Institute of Armament and Military Equipment
of the Armed Forces of Ukraine
03049, Povitroflotskyi prospect, 28 B, Kyiv, Ukraine
ORCID: 0000-0002-4294-4152

Anatoly Dovhopoly
Doctor of Technical Sciences, Professor
Principal researcher of the Central Research Institute of Armament
and Military Equipment of the Armed Forces of Ukraine
The Central Research Institute of Armament and Military Equipment
of the Armed Forces of Ukraine
03049, Povitroflotskyi prospect, 28 B, Kyiv, Ukraine
ORCID: 0000-0001-9227-9771

Oleh Biloborodov
Doctor of Technical Sciences, Senior researcher
Head of Scientific Research Subdirectorate of the Central Research Institute of Armament and
Military Equipment of the Armed Forces of Ukraine
the Central Research Institute of Armament and Military Equipment
of the Armed Forces of Ukraine
03049, Povitroflotskyi prospect, 28 B, Kyiv, Ukraine
e-mail: 22bredly@gmail.com
ORCID: 0000-0003-3166-2659

Serhii Panteleiev
Researcher of the Central Research Institute of Armament and Military Equipment of the Armed
Forces of Ukraine
the Central Research Institute of Armament and Military Equipment of the Armed Forces of
Ukraine
03049, Povitroflotskyi prospect, 28 B, Kyiv, Ukraine
ORCID: 0009-0004-2895-388X

Abstract. The article analyzes trends in the development of methods and means of information-psychological warfare in the world and in Russia. The types, principles of operation and features of the use of information and psychological weapons, as well as the technical means and technologies on which they rely, are considered. Information is provided on existing models of information-psychological weapons and examples of their use by different countries. The possibility of Russia using information and psychological weapons against the defense forces and citizens of Ukraine is considered as a real threat to the national security of the state. The risks of transformation of the consciousness and subconscious of the population under the influence of information and

psychological weapons are analyzed. The mechanisms of influence of television and the Internet on human consciousness are indicated, as well as the principles of their use by the enemy during psychological operations against Ukraine. The need for Ukraine to take preventive measures to protect military personnel and citizens of Ukraine from the effects of information and psychological weapons is pointed out.

Keywords: information and psychological warfare, information and psychological weapons, psychophysical influence, psychological operation, psychometrics, Big Data, psychoprobing, neurolinguistic programming, artificial intelligence, conscious warfare, laser weapons, acoustic weapons.

Introduction

In modern wars, the role of non-lethal types of weapons based on technologies of psychophysical influence on a person, the so-called information and psychological weapons (IPWep), is increasing. Such technologies can be implemented in various ways, including through the use of mass media and social networks, electromagnetic radiation of various types (laser, light, radio frequency) and mechanical (acoustic) waves.

It should be understood that identifying cases of the enemy's use of informational and psychological weapons and taking appropriate countermeasures requires special equipment, appropriate software (in particular, using AI) and trained specialists. At the same time, artificial intelligence (AI) technologies can be used both for the formation and for the purpose of detecting the psychophysical impact on a person.

IPsS has an informational and psychological impact both on an individual person and on large groups of people, or on the vast majority of the population of the affected country (victim country). The main means of influence are mass media (printed materials, television, radio, Internet, social networks) (Makarenko, 2017), (Anisimovych-Shevchuk, 2022), (Kopan,2016), (Vorobyova, 2010), (Volkogonov, 1983), (Smirnov, 2013).

A state that conducts information and psychological warfare (IPW) forms its policy of influence on information and information resources. This policy is aimed at the population and armed forces of the victim country, its own population, as well as at the public consciousness of the international community.

Psychophysical influence is one of the important tools of IPWep. Technical means and technologies that can be used for psychophysical influence include (Makarenko, 2017):

- generators of electromagnetic radiation;
- infrasound and ultrasound generators;
- laser and light emitters;
- computer technologies for the use of large databases (Big Data), AI, virtual reality.

Psychophysical weapons include means of transmission:

- subconscious acoustic information;
- subconscious visual information;
- subconscious combined information.

Subliminal combined information is transmitted through technical means and methods:

- visual and acoustic information;
- neurolinguistic programming;
- training effects on groups of people.

The use of informational and psychological weapons and their countermeasures require knowledge of the methods and mechanisms of their action. Therefore, the task of analyzing and summarizing the methods and mechanisms of action of these types of weapons is urgent.

The purpose of the work: analysis of the state and trends in the development of methods and

means of information and psychological warfare in the world and Russia using:

- information and psychological weapons;
- computer technology as a weapon;
- psychophysical weapons;
- methods of using AI for informational, psychological and psychophysical influence.

Methodological Framework

1. Information and psychological warfare.

Informational and psychological warfare is understood as intentions, efforts, planned psychological operations, applied with the help of methods of propaganda, disinformation, manipulation to a certain audience in order to influence its consciousness, will, emotions, motives, objective judgments (Makarenko, 2017), (Kopan,2016), (Vorobyova, 2010).

The main goals of IPW are usually (Smirnov, 2013), (Pocheptsov, 2002), (Mukhametov, 2010):

- ensuring decision-making and encouraging the authorities of the victim country to take actions that would satisfy the needs of the aggressor country;
- undermining the legitimacy of the political power and international authority of the victim country;
- destabilization of the situation in the victim country, provoking political protests, social conflicts, undermining the moral and psychological state of the population of the victim country;
- undermining the defense capability of the victim country and the combat capability of its armed forces;
- supporting the actions of internal forces aimed at destroying or harming one's state, including by corrupting the authorities and political elite;
- replacement of the socio-cultural identity of the entire population or its part in the victim country, change of national values and foundations of state formation.

As shown in works (Zorina, 2016), (Karyakin, 2014), (Yudin, 2021), (Biloborodov, 2022), the main forms of IPW are:

- psychological operations against the top leadership, population and troops of the victim country;
- public diplomacy, which is the main means of implementing the so-called "soft power" and consists of foreign policy information, scientific and educational exchanges, programs in the field of culture and other forms of humanitarian cooperation;
- foreign policy propaganda aimed at the dissemination of views, ideas and theories for the formation of citizens of the worldview set by the leadership of the aggressor country, concepts that reflect the interests of the subject of propaganda - the aggressor country and stimulate appropriate practical actions;
- special secret psychological operations that stimulate political and social destabilization in the victim country.

Psychological operations. Psychological operations against the top leadership of the state, the population, and the armed forces are based on destabilization technologies and methods of destroying legitimate power (Akhmadullin, 2007). These technologies are used by mass media (mass media), which in one way or another depend on the enemy. Such mass media turn into information and psychological weapons and carry out the enemy's orders, manipulate people's consciousness, deliberately fabricate messages that distort real social reality (Aronson, 2003).

The basis of political destabilization is the simultaneous actions of the centers of generation of appropriate content for all types of mass media with Internet resources located outside the state, the so-called "fifth column" and corrupt high-ranking officials. As a rule, this content is directed to the audience using all the listed technologies of information warfare.

The IPW scheme is quite simple and consists of the following:

- development of predetermined content;
- organization of content delivery channels;
- engaging the audience of viewers, listeners and readers.

TV. Television, which combines video and audio channels of information perception, has an extremely powerful effect on human consciousness. When watching television, people perceive events as happening before their eyes, as if they were witnessing the events, which gives them credibility. The term "zombie fighter" describes it very accurately. People under the influence of television often behave like zombies, obediently carrying out the programs laid down by the authors of hostile propaganda.

In order to present the materials programmed by the aggressor country, programs are created that are understandable in terms of content and do not require intellectual tension, while at the same time stirring emotions. The predominance of emotions over the mind is a feature of the standard behavior of an unconscious person who is not familiar with the psychotechnologies of influencing the human mind.

In media manipulation, the content customer uses factors (Aronson, 2003):

- short memory of a person;
- there is no objectivity for people if they are personally involved in a conflict that threatens their interests and values;
- in order to understand a phenomenon, a person needs to have the name of this phenomenon, and the name in a hidden form explains and programs the reaction to it. Through words and concepts, a picture of the world is created, and with media manipulation, this picture is deliberately distorted.

To ensure media manipulation, the main methods of information dissemination are fragmentation and immediacy. Fragmentation (shredding, localization) is the dominant method of information dissemination. Immediacy (reporting directly from the scene of events) is currently one of the main principles of journalism. A false sense of urgency leads to the loss of the ability to distinguish information according to the degree of importance. The mental process of sorting, which under normal conditions contributes to the understanding of information, is not able, in conditions of time shortage, to perform this function. Concentration of attention on the events taking place at the moment destroys the necessary connection with the past, prevents the full picture of the event from being understood.

That is why one of the tasks of the state media policy should be a qualified analysis of the content of television content and the adoption of appropriate response measures.

Internet. The Internet is a relatively new tool of social engineering, which radically changes the cognitive balance of a modern person. You can instantly find the information you need on the Internet, despite the fact that the average citizen usually does not think about whether this information is true. Content generators on the Internet use the traditional trust of a person in the printed word, even if this word is not in a book, but on a computer screen.

According to the conclusions of the Global Digital report, in 2023, 5.16 billion people were Internet users. This means that 64.4% of the world's population has access to the Internet (Global Digital, 2023).

Despite the fact that there are system centers of content generation on the Internet, users of the Internet and social networks believe that the content is created by ordinary users like them, therefore they trust this content and are not inclined to check the authenticity of news and facts given on the networks.

In Ukraine, according to a USAID-Internews study, 92% of Ukrainians cannot distinguish fakes from the truth (Omelianenko, 2020). The lack of critical thinking and the availability of so much information makes people vulnerable to the imposition of views and values by other people and states.

In order to preserve the conscious attitude of the citizens of Ukraine to the content on the Internet and the formation of a statesman's position in them, it is necessary to strengthen the

information policy in Ukraine and take measures to protect its citizens from hostile narratives.

Computer technology as an informational and psychological weapon. Psychometrics and Big Data. Psychometrics, or psychometrics (from the Greek psyche - soul and metron - measure), is the field of knowledge of the theory and practice of measuring phenomena in the field of psychology. This is an applied branch of psychology, which is aimed at the development of measurement procedures (tests, questionnaires, questionnaires, projective methods). This is a branch of science about such properties of psychological tests as the type of measurement scales, reliability, validity, discriminability, internal consistency, etc.

The purpose of psychometric measurement is to establish the individual psychological differences of an individual by comparing his indicators with the indicators of other people. This makes it possible to explain the behavior and predict the development of the individual (Glushko, 1994).

Before the cybernetization of society, in world practice, the results of psychometric research conducted by means of questionnaires were used to determine the psychological properties of a person. After the research, a psychometric portrait (profile) of a person was compiled, based on which a person's behavior in extreme conditions, in a team, career growth, etc. was predicted.

Of course, understanding how a person will react to certain stimuli provides a rich set of tools for manipulating a person.

The development of the Internet, computer databases and social networks gave access to information about a person without his consent.

The paradox of the situation is that the author of modern approaches to psychometrics and Big Data is a person (Michal Kosinski), who warned many times about the huge risks of uncontrolled use of psychometric technologies for processing large sets of data about people (Kosinski, 2015). In some ways, this story is reminiscent of the creators of the hydrogen bomb, who created the most powerful weapon to destroy humanity, and then began to advocate for its ban.

American scientist, Stanford University professor Michal Kosinski, a Pole by origin, one of the world's leading scientists in the field of psychometrics and Big Data, proved back in 2012 that the analysis of 68 likes on Facebook is sufficient with a probability of 95 percent to determine skin color. with a probability of 88 percent - homosexuality, with a probability of 85 percent - for which party a person will vote in the elections. Belonging to a certain religion, parental divorce, addiction to alcohol or drugs were also taken into account. Kozinsky claimed that after analyzing 150 likes, he will know a person better than his parents (The Insider, 2016).

Using the methods of M. Kozinsky, the consulting company Cambridge Analytica has developed a model that allows you to assess the personality of every adult US citizen according to certain parameters, as well as to influence their behavior.

The Cambridge Analytics company in D. Trump's previous election campaign divided the country's population into 32 personality types. Personal messages were prepared for each type of personality, based on the analysis of specialists (Kosinski, 2015), (The Insider, 2016), this technology played one of the decisive roles in the voting results. Similar approaches were used when voting for the exit of Great Britain from the European Union (Brexit) and in the election campaign of the President of France (The Insider, 2016), (Madanapalle, 2017), (Grassegger, 2017).

Based on the use of similar technologies in the Russian Federation, the Social Data Hub company was established in 2014, which offers its solutions to advertising agencies, analysts, banks, marketing specialists in social networks, politicians and other consumers. Another company of the same founder, Fubutech, "helps officials look for dissidents, cooperates with large corporations" (Pisarev, 2017).

Neurolinguistic programming. The KGB of the USSR, and today the special services and the military of the Russian Federation, together with scientists and political technologists, developed and are developing methods of changing people's behavior by forming their given programs. One of the

most effective methods is neuro-linguistic programming (NLP). NLP is an influence on people's thoughts at the conscious and subconscious levels, aimed at changing behavior by forming predetermined behavioral programs in a "disguised" verbal and linguistic form, including hypnosis techniques and technical means of information influence (Mikhailov, 2002), (Makarenkov, 2019).

Psychotechnologies of psychoprobing (psychodiagnosis), psychocorrection and NLP are a fundamentally new direction in science, which allows non-pharmacological diagnosis and correction of a person's psychophysiological state by accessing semantic memory (subconscious).

Conscientious war. The development of methods of influencing human consciousness and social consciousness led to the formation of even more sophisticated theories and technologies of IPW, which are the basis of the so-called "conscientious war".

According to the publication (Zadorozhny, 2021), "conscientious war is a war on the destruction of consciousness. At the heart of such destruction lies the destruction of a person's ability to freely identify who a person wants to become and within the limits of which cultural and historical tradition."

Since 2015, Ukrainian scientists and political scientists in their publications (Yudin, 2021), (Biloborodov, 2022), (Kolodiy, 2015), (Vashchenko, 2020), (Mulyava, 2021), (Shumka, 2022), (Ostapenko, 2022) predicted the destructive consequences of Russian-oriented mass media in the information space of Ukraine. It was these mass media that waged a war aimed at the destruction of consciousness.

Therefore, for a long time, the world and the citizens of Ukraine were forced to impose the "Russian peace" and the Russian Orthodox Church, which, as evidenced by criminal cases against its hierarchs in Ukraine, often acted as agents of an enemy country.

Consciousness war, in contrast to overt military actions, is not aimed at capturing foreign territories, but is aimed at capturing the consciousness of people who live in these territories.

The experience of Russia's aggression against Ukraine proved that a war of conscience can be used before the start of open aggression, both with the aim of making another country an obedient puppet of the aggressor country, and to shake the mood of the population of the victim country, aimed at destabilizing society and forming a "fifth column ".

Thus, media manipulation technologies on television, influence on people's behavior through social networks, use of a person's psychological profile as a result of psychoanalysis and Big Data information to control human behavior - all these are manifestations of informational and psychological weapons.

2. The use of Russian AI in information and psychological warfare.

AI is increasingly being used in the information and psychological warfare waged by Russia.

As stated in (Oracle, 2023), "AI is the ability of artificial intelligent systems to perform creative functions that were traditionally considered the prerogative of man, the development of science and technology for the creation of intelligent machines, especially intelligent computer systems."

The use of AI in PSV is based on the ability of the system during self-learning to create programs for solving PSV tasks (Google, 2024). Generative AI (Google, 2024), (Infobae, 2022), (Malevskaya, 2023) is crucial for content creation, which in the process of learning and processing information creates new content, both textual, audio and visual.

Generative AI can talk, write software codes, create images from scratch, describe videos, and create personalized content, chatbots, virtual assistants, and more. Generative AI is primarily a type of machine learning model, it does not have emotions and does not think independently, but it is able to find patterns effectively.

It is precisely these capabilities of AI that are used by the Russian side to conduct ISv against Ukraine. Russian propagandists use AI to create a large number of fakes, manipulations and pseudo-television stories purporting to be from Ukrainian TV channels and other mass media on YouTube, FB and distributed in other social networks. The main tasks of these stories are to manipulate public

opinion, spread misinformation, sow panic and despair among the citizens of Ukraine. At the same time, AI is used by propagandists of the Russian Federation to distort the domestic and foreign policy of Ukraine among the population of partner countries, for example (Infobae, 2022), (Malevskaya, 2023).

A dangerous factor for the national security of Ukraine is the dissemination of hostile information by the domestic mass media, which often cannot distinguish that this is content specially created by the enemy, succumb to emotions, and sometimes representatives of the "fifth column" in the mass media do it deliberately at the behest of their masters from Russia.

The enemy's use of AI simultaneously with the intensification of hostilities, bombings and shelling of the territory of Ukraine and the IPSO aims to achieve psychological destabilization of society and the Defense Forces of Ukraine.

It should be noted that Ukrainian specialists are already introducing AI into the system of combating Russian propaganda (Pylypov, 2023).

3. Psychophysical influence.

Radio frequency weapons of thermal action. Weapons based on electromagnetic radiation (EMF) of the radio frequency range of thermal action are based on the effect of human absorption of EMF energy, as a result of which body tissues are heated, the higher the field intensity and the longer the exposure time.

Excess heat is removed to a certain limit by increasing the load on the thermoregulation mechanism. However, starting from the value of the radiation intensity I = 10 mW/cm^2, which is called the thermal threshold, the body cannot cope with heat removal, and the body temperature rises.

The leaders in the field of development and use of thermal microwave weapons are, of course, the USA. The first sample of such a weapon was produced in 2005 with the purpose of dispersing crowds. The principle of its action consists in irradiating people with 3 mm waves. Rays with a wavelength of 3 mm penetrate the human body by only 0.3-0.4 mm, while water and blood molecules boil almost instantly at this depth in the subcutaneous layer. A person feels unbearable pain. The surface of the skin heats up to 40-50°C, which exceeds the human pain threshold. In this state, a person tries to leave the radiation zone. The official tactical and technical characteristics are closed, but in the literature (Military informant, 2010), (Bin.ua, 2012) it is believed that an antenna with a diameter of up to 2 meters is used as a emitter. The wavelength is 3 mm, the range is 1000 meters.

The installation called ADS was developed by the American company Raytheon in 2007. It has a radiation wavelength of 3 mm, a range of 500-1000 meters (Military informant, 2010), (Bin.ua, 2012).

These installations were used in Iraq and Afghanistan. It is planned to be used both in land and sea operations of the US Armed Forces, and in police operations (Bin.ua, 2012), (Cairns, 2010).

In the People's Republic of China, a WB-1 microwave installation with a radiation wavelength of about 8 mm has been developed (Computerra, 2014).

For decades, publications of the Russian Federation covered the theoretical foundations of the creation of microwave installations and the medical consequences of the influence of microwaves on the human body. The paper (Military informant, 2015) provides information on the creation of a high-power microwave weapon for countering high-precision weapons and UAVs at long distances (tens of kilometers). Such weapons can be used on the battlefield against the personnel of the defense forces of Ukraine.

Radio frequency weapons of information action. As mentioned above, a power flux density of 10 mW/cm^2 is considered the limit of thermal impact on a person. All other powers of microwave influence are attributed to non-temperature (informational) influence and are associated with the occurrence of ionic currents and electric potentials in cell molecules, changes in the permeability of cell membranes and corresponding processes.

The non-thermal (informational) electromagnetic influence on biological objects consists in the

excitation of oscillations of the body's components at the level of cells, subcells, neurons, DNA, and others. These excitations of the components of the body at their own frequencies, or close to them, affect the state of the body as a whole. By choosing the frequency of irradiation or the frequency of modulation of irradiation, it is possible to influence the physical state, the state of consciousness and subconsciousness of a person (Khabarova, 2000), (Uzdensky, 1999), (Devyatov, 1991), (Khabarova, 2002), (Gryzlova, 2004), (Kravkov, 2006), (Kolesov, 2000), (Nikulin, 2002), (Sidorenko, 2009).

Excitation of the organism at low-level EMF is due to the fact that any living organism is a complex oscillatory system of self-consistent modes. When such a system is affected by an external disturbance with a frequency that coincides with the resonant system or is close to it, an organism's reaction occurs, either therapeutic (for example, microwave resonance therapy), or destabilizing the work of individual subsystems of the organism or the organism as a whole. In other words, the body and its subsystems down to the subcellular level can be excited at resonant frequencies.

In addition, the body is a non-linear self-oscillating system, so periodic external disturbances lead to periodic changes in some parameters. With appropriate ratios of parameters and frequency of external disturbances, the system can enter parametric resonance.

Further studies (Khabarova, 2000), (Uzdensky, 1999), (Devyatov, 1991), (Khabarova, 2002), (Gryzlova, 2004), (Kravkov, 2006), (Kolesov, 2000), (Nikulin, 2002), (Sidorenko, 2009) established that, firstly, the human nervous system, especially the higher nervous activity sensitive to the electromagnetic field, and, secondly, that EMF has a so-called informative effect when affecting a person at intensities below the threshold value of the thermal effect. The degree and nature of the impact of EMF on the human body depends on:

- radiation intensity;
- frequency of oscillations;
- surface area of the irradiated body;
- individual characteristics of the body;
- irradiation mode (continuous or intermittent);
- duration of exposure;
- the combined action of other factors.

Thus, by selecting the necessary frequency range and density of the EMF flow, it is possible to influence individual organs and the general condition of a person.

EMFs in the centimeter and decimeter range artificially create auditory hallucinations (Hmong, 2003), (Corera, 2021). The technology for creating auditory hallucinations is based on the fact that radio frequencies generate sounds in absorbing materials in a pulse mode of sufficient peak power. The phenomenon of auditory response depends on the energy per pulse, and not on the average density of the EMF flow.

Based on the publications (Membrana, 2008), (Hambling, 2008), (Borger, 2021), a model based on the influence of low-intensity radio frequency radiation MEDUSA has already been created in the USA. Microwaves generate sound of any intensity in a person's head.

The work (Borger, 2021) provides information about the repeated use of radio frequency radiation weapons by the former USSR against US citizens. Based on the testimony of the victims, the effect of this weapon coincides with the effect of the MEDUSA installation. The authors assume that such a weapon, in addition to the Russian Federation, may be in service in the People's Republic of China.

Based on the lack of appropriate war ethics on the part of the Russian Federation, it is possible to predict the use of radio frequency weapons by the enemy on the battlefield.

Acoustic weapon. Summarizing the materials of publications (Kirsanov, 2014), (Belous, 2009), (Gakaev, 2015), (kara881, 2018), (Smirnov, 1990) on the creation of acoustic weapons shows that the influence of high-power acoustic radiation can lead to the loss of the human body’s performance, and on the other hand, sub-noise acoustic signals create the possibility of managing the

psychophysical state of a person.

The effect of acoustic radiation of different levels on a person is determined as follows (Gakaev, 2015):

- up to 50 dB usually does not cause a harmful effect on a person;
- 50-60 dB can cause a psychological effect, manifested in deterioration of mental activity, weakening of attention, speed of reactions, difficulty in working with masses of information;
- 60-90 dB, the pulse accelerates, blood pressure rises, vessels narrow, which worsens the blood supply to organs and systems;
- above 90 dB, significant functional disturbances occur: hearing sensitivity decreases, the activity of the stomach and intestines deteriorates, a feeling of nausea, headache, tinnitus appears;
- at a noise level of 120 dB and above, a mechanical effect is exerted on the organ of hearing, which manifests itself in the disruption of connections between individual parts of the inner ear, a possible rupture of the eardrum. Such high noise levels affect not only the hearing organs, but also the whole body. Sound waves, penetrating through the skin, cause mechanical vibrations of body tissues, as a result of which nerve cells are destroyed, small blood vessels rupture, etc. The indicated pathological changes of the ischemic or hemorrhagic type can lead to epileptiform attacks on the part of the nervous system, to ulcerative defects in the digestive system, to myocardial infarction in the heart, and to acute circulatory disorders in the myocardium, brain, pancreas, and other organs.

High and ultrasonic frequencies (from 5 to 30 kHz) can cause overheating of internal organs up to deadly high temperatures, tissue burns and dehydration.

Resonance phenomena of the influence of acoustic vibrations on a person. Man, as a complex biological system, has its own frequencies of oscillations of biological subsystems. Resonance effects can be achieved at low sound levels, but when the vibration frequencies coincide with the excitation frequencies. When the natural frequencies of the internal organs and the acoustic impact coincide, vibration occurs in the corresponding organs, which is accompanied by painful sensations. At the same time, infrasound can "shift" the tuning frequencies of internal organs (Studfile, 2008).

Thus, acoustic waves cause a wide range of reactions of the human body. The severity of the consequences increases with increasing sound pressure. Some researchers point to the spectral dependence and resonant nature of the body's reaction to acoustic influence.

The main elements of acoustic weapons are a generator and a sound converter. The most common are piezoelectric and magnetostrictive transducers.

The United States achieved the greatest success in creating acoustic weapons. The LRAD (Long Range Acoustic Device) series, developed by American Technology Corporation using the technology of piezoelectric acoustic emitters, became the most famous. According to known data, the frequency range is 0.72-6.6 kHz (according to other data, it is 2.1-3.1 kHz). The main sound energy of the LRAD samples is focused in a sector of about 30°. The effective range of use of these means is 50-300 m (Slavaland, 2013), (Rambler, 2002).

Another well-known model series is the HS (HiperStrike) and MA of the Ultra Electronics Corporation (USA) using the technology of electrodynamic generation of acoustic waves. Open sources note a wide frequency range of samples (0.375-18 kHz for HS-24, 0.21-10 kHz for HS-60) and high directional properties of samples (the main sound energy of HS samples is focused in a sector of about 10-25°), and samples of the MA series were developed for circular action (360°).

Another example of an acoustic weapon is the MAHD-R (MOOG Acoustic Hailing Device) model from MOOG (USA). According to known data, the frequency range is 0.02-20 kHz. The main sound energy of the specified sample is focused in a sector of about 30°. The sound pressure at a distance of 1 m is 151 dB. It is interesting that this sample is the only one that is positioned on the market as an acoustic weapon.

LIPE (Laser-Induced Plasma Effect, developed by the U.S. Department of Defense's Joint Non-Lethal Weapons Program) was developed in the United States in order to increase the selectivity of

the action and the reliability of operation. The principle of operation of the specified sample of acoustic weapons consists in the formation of a plasma cell in the area of the target location with the help of a laser and its subsequent rapid heating and formation of an explosive acoustic wave with a power of 130-140 dB (Dsnews, 2020).

Loudspeaker devices in service with the Russian Federation can be considered examples of acoustic weapons: sound broadcasting stations ZS-82, ZS-88 (nominal frequency range 0.3-3.5 kHz, sound pressure about 100 dB), ZS-96.03.

The Russian Federation is also conducting research on the use of acoustic antenna arrays. This technology is used in acoustic emitters AI-40, AI-91. They work in the frequency range of 2-5 kHz, the main sound energy of AI samples is focused in a sector of about 7-15°.

Although the purpose of powerful acoustic devices is officially presented as a means of transmitting sound data (commands, alerts) over long distances, the experience of use clearly indicates their purpose to influence the psychophysiological state of a person. Examples of this are the use of acoustic weapons during anti-terrorist and anti-piracy operations on the coast of Somalia, during police operations (Pittsburgh, Ferguson, USA), Georgia, Israel, Afghanistan, Iraq (Slavaland, 2013), (Rambler, 2002), (Dsnews, 2020), (Offshore-energy, 2019), (Russon, 2012), (Popkov, 2021), (Lederman, 2008).

Attention should be paid to the factors that can bring non-lethal weapons into the category of lethal, since a number of samples of acoustic weapons have a lower limit of the frequency range of about 100 Hz, and acoustic vibrations with a frequency of 100 Hz have a destructive effect on the human body (Kirsanov, 2014).

An important uncertain influence is the modulation of acoustic oscillations, in which the fundamental (carrier) frequency is safe, but the coincidence of the modulation of the carrier frequency with human resonant frequencies can turn a non-lethal weapon into a lethal one.

Based on the level of open scientific research and available samples of acoustic weapons, there is a possibility of its use by the aggressor against servicemen and citizens of Ukraine.

Laser non-lethal weapon. Laser non-lethal weapons can be used to blind military personnel and to psychologically affect them.

The effect of blinding laser radiation on enemy servicemen is achieved by the fact that a directed red or green laser beam causes temporary blindness and a psychological effect. Military personnel lose combat capability and the ability to coordinate actions. This can especially affect the work of snipers and military personnel who observe through optical devices (Topwar, 2015). At a specific power of laser irradiation of human eyes of 1 mW/cm2, temporary blinding of a person is achieved. The International Electrotechnical Commission established that the specific radiation power of lasers should be no more than 2,5 mW/cm^2. Such power of radiation does not cause irreversible consequences for human vision (Doswald-Beck, 1996).

In the former USSR, experimental blinding complexes "Sangvin" and "Stiletto" were developed. In the Ministry of Internal Affairs of Russia, blinding weapons, for example, the Potok complex (Apocalypse, 2021), have been adopted.

Pulsating light. Pulsating light that hits the retina is perceived by humans as continuous light (Jyngli, 2022), (Gmleds, 2011), but the human brain registers these pulsations. The work of the human brain is disturbed at a pulsation coefficient of 5-8 % and frequencies of 100 Hz. Pulsations of 20 % and 100 % cause the same negative effect on the work of the central nervous system (CNS), and to a greater extent on the neural elements of the cerebral cortex and the photoreceptor elements of the retina.

Developments of LED devices are known, in which a large number of colored LEDs that emit low-frequency pulses of light are installed. These pulses of light affect most people, causing nausea, dizziness and spatial disorientation. The greatest impact on the human psyche is pulsed radiation of the red spectrum with a frequency of 15 Hz, at a very low intensity (almost invisible light) with a

steep leading edge of the pulses. With such radiation, people experience epilepsy, a feeling of malaise, nausea, dizziness, and loss of consciousness during rapid movements (Zaur, 2019).

In addition, a prototype stroboscopic weapon has been developed based on a green laser that emits strobes of radiation. This weapon does not allow effective shooting, causes loss of balance and orientation in space, and in some cases is accompanied by a feeling of nausea (Yuferev, 2014).

The stroboscopic system "Owls" was created in the Russian Federation. This stroboscope is designed to suppress the visual-optical and optical-electronic channels of observation and aiming of small arms at night and in the twilight. This system causes spots of light at a distance of 2 km in front of the eyes, and in 45 % of cases dizziness, nausea and disorientation. The radiation of the "Owl" in the visible and part of the infrared spectrum with high-frequency brightness modulation effectively suppresses night vision devices, infrared laser rangefinders, ATGM guidance systems at a distance of up to 5 km. In the USA, a similar system is called the "Protective Light Channel" (Wikipedia, 2012).

Psychophysical weapons based on subliminal acoustic information are means of psychophysical weapons intended for covert violent action on the subconscious mind of a person or group of people. Psychophysical means are based on the principle of suggestion (suggestion), which consists in influencing an individual or a group of people and is perceived at the subconscious level. People have a desire to obey and change their behavior under the influence of an outsider, while the person is sure that this is his choice or initiative.

The Russian scientist, academician I. V. Smirnov (Smirnov, 1994/1), (Smirnov, 1994/2), (Smirnov, 1994/3), (Smirnov, 1990), (Smirnov, 2013).

These methods are based on psychoprobing and psychocorrection of a person under the influence of sound. Psychoprobing is an assessment of a person's personality, which is based on the method of encoding language, preserving its semantic content. Thanks to psychoprobing, they get relevant answers to the questions asked. In addition, a psychological portrait (profile) of a person is created. A person unconsciously answers the questions. Psychoprobing is the most accurate tool for researching a person's mental activity. Psychocorrection is the correction of a person's internal picture of the world, the initiation of a person's state and behavior adequate to the given program. Psychocorrection is carried out with the help of stories developed based on the results of psychodiagnostics specifically for each person. The psychotechnology of correction is based on neurolinguistics – programming with the help of specially prepared language and acoustic structures (suggestive stories), so these technologies have the names "psycholinguistics" and "psychosemantics". A specially developed plot programs a person, but the person does not suspect it. The plot is conveyed to a person when listening to audio recordings. She listens to the recording, but only hears music or acoustic noise.

Psychophysical influence based on subconscious visual information. Unlike audio suggestion, subconscious visual information is instantly perceived by a person. This influence on the human psyche is more profound and long-lasting, since visual systems affect not only the intellect, but also the emotional and sensory basis of a person.

Today, methods of presenting information frame by frame are intensively developed. Each frame contains only a part of the suggestive image, which is not enough for its conscious perception. With the successive presentation of such frames, on a subconscious level, the parts of the figurative suggestion are combined into a single image. This approach is close to NLP methods and is used, including, in computer viruses.

One of the effective methods of influencing the human psyche is color, which can cause both positive and negative emotions. A specially organized effect of color dynamics can be an effective way of modifying a person's consciousness, behavior and physical state.

The effect of psychological influence is significantly enhanced with the combined use of audio and visual influences.

Conclusions

Based on the results of the analysis of the current state and trends in the development of methods and means of informational and psychological warfare in the world and in Russia, it can be concluded that today a powerful scientific and technological basis for conducting such wars has been created, and an increase in the scale of the aggressor's use of informational and psychological weapons can significantly increase the risks for of national security of Ukraine.

Some developments are already being used by Russia against Ukraine, and in the near future it is possible to expect the aggressor to use the entire arsenal of technical means available to him and conduct organizational measures aimed at escalating information and psychological warfare.

First of all, it concerns the use of:

1. Psychotechnologies of psychoprobing, psychocorrection, and neurolinguistic programming for the purpose of non-medicinal correction of the psychophysiological state of Ukrainian citizens by accessing and influencing semantic memory (subconscious). The use of media manipulation technologies with the use of television, the Internet, Big Data and social networks for this purpose creates the prerequisites for increasing the vulnerability of the population of Ukraine to hostile influences and increasing the risks of transforming people's consciousness and the formation of favors with parameters set in advance by the enemy.

2. Artificial intelligence in information and psychological warfare. Its use can greatly increase the effectiveness of these wars. Generative intelligence is capable of creating personalized content, which leads to the appearance in the information space of a large number of pseudo-television stories and various fakes, the task of which is to manipulate public opinion, disinformation, sow panic and despair among the citizens of Ukraine, and distort the domestic and foreign policy of Ukraine.

3. Psychophysical effects of weapons, namely:

- radio frequency weapons of thermal action based on electromagnetic radiation, which causes unbearable pain on the surface of the skin of military personnel, as a result of which he is forced to leave the radiation zone;

- a radio-frequency weapon of information action, which affects individual organs and the general condition of a person and can cause auditory hallucinations by selecting the frequency range and density of the electromagnetic flow;

- acoustic weapons, based on the fact that acoustic waves cause a wide range of reactions in the human body (acceleration of the pulse, increase in blood pressure, headache, nausea, etc.). The degree of severity of the consequences of its use depends on the sound pressure and spectral characteristics of the sound;

- laser weapons for blinding military personnel and psychological pressure on them on the battlefield;

- weapons based on pulsating light, which can cause epilepsy, a feeling of malaise, nausea, dizziness, and with rapid movements, loss of consciousness, depending on the radiation parameters.

The specified circumstances require awareness of the necessary protective measures and the development of appropriate technologies and means of countermeasures against informational and psychological weapons.

References

1. I beat pirates with a hose and a sonic cannon." https://www.offshore-energy.biz/httpwww-worldmaritimenews-comarticleshipping8135i-beat-pirates-with-a-hose-and-sonic-cannon/.
2. Active Denial System mikrovolnovaya sistema. (2010). Active Denial System microwave system. Military informant. 18.05.2010. https://military-informant.com/army/acdesy-sp-1270449268.html.
3. Aditya Madanapalle. (2017). Big data and psychographic profiling helped Donald Trump win the US presidential election. 31.01.2017. https://www.firstpost.com/tech/news-analysis/big-

data-and-psychographic-profiling-helped-donald-trump-win-the-us-presidential-election-3696847.html.
4. Akusticheskoye oruzhiye: kak ono «strelyayet». Acoustic weapons: how they "shoot." URL: https://news.rambler.ru/other/37732548-akusticheskoe-oruzhie-kak-ono-strelyaet/.
5. Amerikanskiye voyennyye pokazali «luchevuyu pushku» v deystvii, ispytav yeye na lyudyakh. (2012). The US military showed a "ray gun" in action, testing it on people. Bin.ua/12.03.2012. https://bin.ua/news/foreign/world/127547-amerikanskie-voennye-pokazali-luchevuyu-pushku-v.html.
6. Anisimovych-Shevchuk, O. V. Suchasni informatsiyno-psykholohichni vplyvy v systemi mizhnarodnykh vidnosyn u konteksti rosiys′ko-ukrayins′koyi viyny 2014–2022 rokiv. (2022). *Modern informational and psychological influences in the system of international relations in the context of the Russian-Ukrainian war of 2014–2022*. https://www.academia.edu/105430665.
7. Kolodiy, A. Boykot rosiys′koho kino. (2015). *Boycott of Russian cinema*. 02.01.2015. Facebook. https://www.facebook.com/norukino/?locale=ru_RU.
8. Apokalipsis viki/oruzhiye/ênergeticheskoye oruzhiye/lazer. Apocalypse wiki/weapons/energy weapons/laser. https://apocalypse.fandom.com/ru/wiki/.
9. Aronson, E., Pratkanis, E. Epokha propagandy: Mekhanizmy ubezhdeniya, povsednevnoye ispol'zovaniye i zloupotrebleniye. (2003*). The Age of Propaganda: Mechanisms of Persuasion, Everyday Use and Abuse*. St. Petersburg: prime. – EUROSIGN. 384 p.
10. Biloborodov, O. O., Dovgopolyy, A. S. (2019). Tekhnolohiyi informatsiyno-psykholohichnykh viyn ta informatsiyno-psykholohichna zbroya. Technologies of informational and psychological warfare and informational and psychological weapons. *Armament and military equipment*. Kyiv: TsNDI OVT of the Armed Forces of Ukraine. No. 4 (24). https://doi.org/1034169/2414-0651. 2022. 4 (24). P. 93-99.
11. Chto takoye II? Uznayte ob iskusstvennom intellekte. What is AI? Learn about artificial intelligence. Oracle Cloud Free Tier. https://www.oracle.com/cis/artificial-intelligence/what-is-ai/.
12. Chto takoye svetodiodnyy stroboskop? V chem vred? What is an LED strobe? What's the harm? https://ru.gmleds.com/info/what-is-led-strobe-what-s-the-harm-64344099.html.
13. V Kitaye poyavilos' mikrovolnovoye oruzhiye. (2014). Microwave weapons appeared in China. *Computerra*. Institute of Evolutionary Economics. 21.12.2014. https://iee.org.ua/ru/prog_info/30325/.
14. Dan Cairns. US army heat ray gun in Afghanistan. (2010). *BBC News*. 07/15/2010. https://www.bbc.com/news/newsbeat-10646540.
15. Hambling, D. Microwave ray gun controls crowds with noise. (2008). *NewScientist*. 3 July. https://www-newscientist-com.translate.goog/article/dn14250-microwave-ray-gun-controls-crowds-with-noise.
16. Deepfakes, trafik dannykh i drony: iskusstvennyy intellekt v voyne mezhdu Rossiyey i Ukrainoy. (2022). Deepfakes, data traffic and drones: artificial intelligence in the war between Russia and Ukraine. https://www.infobae.com/ru/2022/03/22/deepfakes-data-traffic-and-drones-artificial-intelligence-in-the-war-between-russia-and-ukraine/.
17. Devyatov, N. D., Golant, M. B., Betsky, O. V. (1991). Millimetrovyye volny i ikh rol' v protsessakh zhiznedeyatel'nosti. *Millimeter waves and their role in life processes*. *Radio and communications*. Moskow.
18. Filin (stantsiya vizual'no-opticheskikh pomekh). Owl (visual-optical jamming station). https://ru.wikipedia.org/wiki/филин.
19. Gakaev, D. A. Vliyaniye shuma i infrazvukov na organizm cheloveka. (2015). The influence of noise and infrasounds on the human body Text: immediate. *Young scientist*. No. 15 (95).

P. 261-264. https://moluch.ru/archive/95/21473/.
20. Glushko, A. N. Osnovy psikhometrii. (1994). *Basics of psychometrics*. Moscow: GVMU RF Ministry of Defense. 100 p.
21. Corera, G. «Gavanskiy sindrom». Vinovaty li mikrovolny v zagadochnoy bolezni diplomatov SSHA po vsemu miru. (2021). "Havana Syndrome" Are microwaves to blame for the mysterious illness of US diplomats around the world? *BBC.News* 11.09.2021. https://www.bbc.com/russian/features-58505621.
22. Gryzlova, O. Yu., Subbotina, T. N., Yashin A. A. (2004). Biorezonansnyy effekt v vozdeystvii nizkointensivnogo krayne vysokochastotnogo na reproduktivnuyu funktsiyu myshey. Bioresonance effect in the influence of low-intensity, extremely high-frequency on the reproductive function of mice. *Electrodynamics and technology of microwave, EHF and optical frequencies*. T.12. No. 1-2. P. 94-98.
23. Grassegger, H. & Krogerus, M. The Data That Turned the World Upside Down. (2017). *How Cambridge Analytica used your Facebook data to help the Donald Trump campaign in the 2016 election*. 28.01.2017. https://www.vice.com/en/article/ mg9vvn/how-our-likes-helped-trump-win.
24. Holovni vysnovky zvitu Global Digital 2023. (2023). Key findings of the Global Digital 2023 report. https://www.linkedin.com/pulse/main-conclusions-of-the-report-global-digital-2023-75min-club.
25. Ideal'noye oruzhiye: zvukovaya volna nizkoy chastoty. (2018). Ideal weapon: low frequency sound wave. Live journal/08/21/2018. https://kara881.livejournal.com/50817.html?
26. Pylypov, I. SHI proty propahandy: yak startap Mantis Analytics boret′sya z rosiys′koyu dezinformatsiyeyu. (2023). AI vs. Propaganda: How Startup Mantis Analytics Fights Russian Disinformation *Economic truth.* 11/15/2023. https://www.epravda.com.ua/publications/ 2023/11/15/706604/.
27. Julian Borger. Microwave weapons that could cause Havana Syndrome exist, experts say. (2021). *The guardian*. 2 Jun 2021. https://www.theguardian.com/science/2021/jun/ 02/microwave-weapons-havana-syndrome-experts.
28. Karyakin, V. V. Strategii nepryamykh deystviy, «myagkoy sily» i tekhnologii «upravlyayemogo khaosa» kak instrumenty pereformatirovaniya politicheskikh prostranstv. (2014). Strategies of indirect actions, “soft power” and technologies of “controlled chaos” as tools for reformatting political spaces. *Information Wars*. No. 3(31). pp. 29-38.
29. Khabarova, O. V. Bioeffektivnyye chastoty i ikh svyaz' s sobstvennymi chastotami zhivykh organizmov. (2002). Bioeffective frequencies and their connection with the natural frequencies of living organisms. *Biomedical technologies and radio electronics*. No. 5. P. 56-66.
30. Khabarova, O. V. Rezonansnyye effekty v zhivykh organizmakh. (2000). *Resonance effects in living organisms.* Preprint IZMIRAN, No. 4 (1132). Moscow. March.
31. Kolesov, S. N. Dissertatsiya na soiskaniye uchenoy stepeni doktora meditsinskikh nauk. «Razd. 3.2. Otsenka glubiny proniknoveniya SVCH-izlucheniya na modelyakh razlichnykh tkaney». Dissertation for the degree of Doctor of Medical Sciences. "Sec. 3.2. Estimation of the penetration depth of microwave radiation on models of various tissues.” https://www.rest.ru/rus/literature/dissertation/kolesov_dis_cd.html.
32. Kopan, O. V., Melnyk, V. I., Informatsiyno-psykholohichna viyna yak zasib manipulyuvannya lyuds′koyu svidomistyu. (2016). *Informatsiya i pravo*. Information and psychological warfare as a means of manipulating human consciousness. *Information and law*. 2(17/2016). pp. 92-98. https://ippi.org.ua/kopan-ov-melnik-vi-informatsiino-psikhologichna-viina-yak-zasib-manipulyuvannya-lyudskoyu-svidomisty.
33. Kravkov, A. V. Effekt neteplovogo (informatsionnogo) vozdeystviya elektromagnitnogo izlucheniya krayne vysokoy chastoty na biologicheskiye ob"yekty i cheloveka. (2006). *The*

effect of non-thermal (information) influence of extremely high frequency electromagnetic radiation on biological objects and humans. Short review. Kyiv. https://www.calameo.com/books/001038164cea38791e8b1.

34. Lederman, J. US to press concerns over incidents in meeting with Cubans. https://apnews.com/article/69f57822ed364056bef2b02808701b8f.
35. Doswald-Beck, L. Novyy protokol ob osleplyayushchem lazernom oruzhii. (1996). New protocol on blinding laser weapons. *International Journal of the Red Cross*. May. https://international-review.icrc.org/ru/articles/new-protocol-blinding-laser-weapons.
36. Makarenkov, E. V., Durneva, M. A. Analiz tekhnologiy neyrolingvisticheskogo programmirovaniya, kak instrumenta politicheskogo protivoborstva. (2019). Analysis of neurolinguistic programming technologies as a tool of political confrontation. *Bulletin of Chelyabinsk State University*. No. 12 (434). Philosophical sciences. No 54. pp. 89-94. DOI:IO.2444/1994-2796-2019-11212.
37. Maria Malevskaya. Feyki, manipulyatsii i drugiye produkty IPSO: kak rossiyskaya propaganda ispol'zuyet iskusstvennyy intellekt protiv ukraintsev. (2023). Fakes, manipulations and other IPSO products: how Russian propaganda uses artificial intelligence against Ukrainians. Vikna-News/ 12/01/2023. https://vikna.tv/ru/dlia-tebe/vijna-v-ukrayini/kak-rossijskaya-propaganda-ispolzuet-ii-i-fejki-protiv-ukrainczev/.
38. Maryna Ostapenko. Konstsiyental′na viyna yak element hibrydnoyi viyny. (2022). Conscientious warfare as an element of hybrid warfare. *Scientific journal of the National Pedagogical University named after M. P. Drahomanov*. Vol. 22, No 32. https://sj.udu.edu.ua/index.php/pnspd/article/view/1285.
39. MEMBRANA: Oruzhiye-meduza sozdayet trubnyy glas v golove. (2008). The jellyfish weapon creates a trumpet sound in the head /07/22/2008. https://www.membrana.ru/paticle/12809/.
40. Michal Kosinski, Ph.D. – Publications. URL: https://neurotree.org/neurotree/publications.php?pid=128111.
41. Mikhailov, B. V., Serdyuk, A. I., Fedoseev, V. A. Psikhoterapiya v obshchesomaticheskoy meditsine. Klinicheskoye rukovodstvo. (2002). Psychotherapy in general somatic medicine. Clinical manual. Under the general direction. ed. B. V. Mikhailova. Kharkov: Prapor. 128 p.
42. Mukhametov, R. S. Rol' publichnoy diplomatii v formirovanii mezhdunarodnogo imidzha Rossii. (2010). Sovremennaya Rossiya i mir: al'ternativy razvitiya (Rossiya i Zapadnaya Yevropa, vliyaniye obrazov stran na dvustoronniye otnosheniya). The role of public diplomacy in the formation of the international image of Russia. *Modern Russia and the world: development alternatives (Russia and Western Europe, the influence of country images on bilateral relations)*: materials of the international scientific and practical conference. Barnaul: Publishing house Alt. Univ. pp. 111-116.
43. Vashchenko, N. M. Teoretychnyy vymir doslidzhennya ponyattya «konstsiyental′na viyna» v umovakh hibrydnoyi ahresiyi Rosiyi proty Ukrayiny. (2020). The theoretical dimension of the study of the concept of "conscientious war" in the context of Russia's hybrid aggression against Ukraine. *Educational and Scientific Institute of Journalism*. 31.03.2020. http://journ.univ.kiev.ua/nauka1/archives/2068.
44. Nikulin, R. N. Fizicheskiye mekhanizmy vozdeystviya SVCH – izlucheniya nizkoy intensivnosti na biologicheskiye ob"yekty. Physical mechanisms of the impact of low-intensity microwave radiation on biological objects. https://www.dissercat.com/content/fizicheskie-mekhanizmy-vozdeistviya-svch-izlucheniya-nizkoi-intensivnosti-na-biologicheskie.
45. Generativnom iskusstvennom intellekte. About generative artificial intelligence. https://support.google.com/websearch/answer/13954172?hl=ru.
46. Yudin, O., Matviychuk-Yudina, O., Suprun, O. Informational psychological warfare and social

engineering technologies. (2021). *ResearchGate*. July 2021. DOI:10.18372/2310-5461.50.15684. https://www.researchgate.net/publication/362766470_informacijno-psihologicna_vijna_ta_ tehnologii_socialnogo_ inziniringu.

47. Oruzhiye pod zapretom. Chast' 7. Osleplyayushcheye lazernoye oruzhiye. Weapons are prohibited. Part 7. Blinding laser weapons. *Military review*. http://topwar.ru/65859-oruzhie-pod-zapretom-chast-7-osleplyayuschee-oruzhie.html.
48. Pisarev, A. SocialDataHub: Kak eks-reklamshchik sdelal biznes na Big Data i prodayet uslugi byvshim kollegam (i chinovnikam). (2017*). How an ex-advertiser made a business on Big Data and sells services to former colleagues (and officials)*. 02/10/2017. http://incrussia.ru/fly/ socialdatahub-kak-eks-reklamshchik-sdelal-biznes-na-big-data-i-prodaet-uslugi-byvshim-kollegam-i-chi.
49. Pocheptsov, G. G. Psikhologicheskiye voyny. (2002). *Psychological warfare*. Moscow: Refl-book; TO.; Wakler. 528 p.
50. Psikhotronnoye oruzhiye. Zvukovoye oruzhiye. (2013). Psychotronic weapons. Sonic weapon. 06/11/2013. https://slavaland.ru/part/content/content.php?content.324.4#. WoP0jOlf0uV.
51. Popkov, R. Zvukovaya pushka dlya razgona demonstratsiy v Rossii. Chto takoye «neletal'naya akusticheskaya sistema». A sound cannon to disperse demonstrations in Russia. What is a “non-lethal acoustic system”. https://cripo.com.ua/likbez/?p=211769/.
52. Russon, M.-A., Brown, M. Shooting: *What is the LRAD Sound Cannon Being Used on Ferguson Protesters?* https://www.ibtimes.co.uk/michael-brown-shooting-what-lrad-sound-cannon-being-used-ferguson-protesters-1461260.
53. Makarenko, S. I. Informatsionnoye protivoborstvo i radioelektronnaya bor'ba v setetsentricheskikh voynakh nachala XXI veka. (2017). *Information warfare and electronic warfare in network-centric wars of the early 21st century. Monograph*. St. Petersburg: Science-intensive technologies. 546 p.
54. Shumka, A. V. Rosiys′ka ahresiya v Ukrayini 2022 roku yak konstsiyental′na viyna. (2022). Russian aggression in Ukraine in 2022 as a war of conscience. PolUkr (*Polish-Ukrainian portal*) /20.12.2022. https://www.polukr.net/uk/blog/2022/12/rosijska-agresija-v-ukraini-jak-konceptualna-vijna/.
55. Sidorenko, V. M. Mekhanizm vozdeystviya slabogo elektromagnitnogo izlucheniya na cheloveka. (2009). The mechanism of the effect of weak electromagnetic radiation on humans. *News of the Southern Federal University*. No. 10. Technical sciences. Taganrog.
56. Smirnov, A. A. Informatsionno-psikhologicheskaya voyna. (2013). Information and psychological warfare. *Free Thought*. No. 6 (1642). pp. 81-96.
57. Smirnov, I. V., Beznosyuk, E. V. Komp'yuternyye psikhotekhnologii semanticheskogo analiza bessoznatel'nogo. (1994). Computer psychotechnologies for semantic analysis of the unconscious. *Russian Psychoanalytic Bulletin*. No. 3.
58. Smirnov, I. V., Beznosyuk, E. V. Psikhokorrektsiya, psikhoprofilaktika, psikhoterapiya. (1990). Psychocorrection, psychoprophylaxis, psychotherapy. *Medical psychology and psychohygiene*, p. 53.
59. Smirnov, I. V., Beznosyuk, E. V. Komp'yuternyy psikhoanaliz i psikhoterapiya. (1994). Computer psychoanalysis and psychotherapy. *Medical assistance*. Moscow: Medicine. No. 4.
60. Smirnov, I. V., Beznosyuk, E. V. Metody neosoznavayemoy psikhoterapii, psikhokorektsii i psikhosemanticheskogo analiza s subsensornym vvedeniyem informatsii. (1994). Methods of unconscious psychotherapy, psychocorrection and psychosemantic analysis with subsensory introduction of information. *Psychotherapist of Russia*. Moscow: Medicine. No. 3.
61. Sobstvennyye kolebaniya razlichnykh organov cheloveka. Natural vibrations of various human organs. https://studfile.net/preview/5165070/page:14/.
62. Stroboskop kak oruzhiye. Strobe as a weapon. https://jyngli.by/a45778-stroboskop-kak-

oruzhie.html.
63. SVCH slukhovoy effekt. Microwave auditory effect. https://hmong.ru/wiki/Microwave_ auditory_ effect.
64. The Insider. Rassledovaniye Das Magazin: Kak Big Data i para uchenykh obespechili pobedu Trampu i Brexit. (2016). Das Magazin investigation: How Big Data and a couple of scientists ensured victory for Trump and Brexit. 07.12.2016. https://hvylya.net/uk/analytics/
65. 114056-kak-big-data-i-para-uchenyih-obespechili-pobedu-trampu-i-brexit.
66. Tretiakov, O. V., Zacarny, V. V., Bezsonny, V. L. *Ohorona praci*. URL: https://pidru4niki.com/18060203/bzhd/shum_yogo_vidi.
67. Uboynyy zvuk: kakoye ono, samoye "gumannoye" oruzhiye v mire? Killer sound: what is it, the most “humane” weapon in the world? https://www.dsnews.ua/world/uboynyy-zvuk-kakoe-ono-samoe-humannoe-oruzhie-v-mire--31072015090800.
68. Uzdensky, A. B. Realizatsiya v kletkakh rezonansnykh mekhanizmov biologicheskogo deystviya sverkhnizkochastotnykh magnitnykh poley. (1999). Implementation of resonant mechanisms of the biological action of ultra-low-frequency magnetic fields in cells. Proceedings of the 2nd international conference “*Electromagnetic fields and human health*” September 20-24. Moscow. From 43.
69. V Rossii sozdana «SVCH-pushka» dlya vyvoda iz stroya bespilotnikov i vysokotochnogo oruzhiya. (2015). Russia has created a “microwave gun” to disable drones and precision weapons. Military informant/06/15/2015. URL: https://military-informant.com/army/v-rossii-sozdana-svch-pushka-dlya-vyvoda-iz-stroya-bespilotnikov-i-vysokotochnogo-oruzhiya.html.
70. Belous, V. Oruzhiye XXI veka. (2009). Weapons of the XXI century. *International life*. No. 1. P. 104-129.
71. Mulyava, V., Grigoriev, V. Protydiya konstsiyental′nym vplyvam rosiys′koyi propahandy na osobovyy sklad Zbroynykh Syl ta naselennya Ukrayiny. (2021). Counteraction to the conscious influence of Russian propaganda on the personnel of the Armed Forces and the population of Ukraine. Bulletin of the National Defense University of Ukraine named after Ivan Chernyakhovsky. 07.05.2021. http://visnyk.nuou.org.ua/article/view/229903.
72. Kirsanov, V. V., Grigorieva, I. G. Vozdeystviye akusticheskikh kolebaniy (slyshimogo shuma, infrazvuka, ul'trozvuka) na okruzhayushchuyu prirodnuyu sredu. The impact of acoustic vibrations (audible noise, infrasound, ultrasound) on the natural environment. https://www.vozdeystvie-akusticheskih-kolebaniy-slyshimogo-shuma-infrazvuka-ultrozvuka-na-okruzhayuschuyu-prirodnuyu-sredu.pdf.
73. Victoria Omelianenko. Internet yak mozhlyvist′ i zahroza dlya ditey: yak znayty balans. (2020). The Internet as an opportunity and a threat for children: how to find a balance. *Ukrainian Pravda*. https://life.pravda.com.ua/columns/2020/11/24/243138/.
74. Vladimir Akhmadullin. Psikhologicheskiye operatsii – moshchnoye oruzhiye sovremennykh voyn. (2007). Psychological operations are a powerful weapon in modern warfare. 14.12.2007. *Independent Military Review*. https://psyfactor.org/lib/psywar43.htm.
75. Volkogonov, D. A. Psikhologicheskaya voyna: Podryvnyye deystviya imperializma v oblasti obshchestvennogo soznaniya. (1983). Psychological warfare: Subversive actions of imperialism in the field of social consciousness. Moscow: Military Publishing House. 288 p.
76. Vorobyova, I. V. Informatsiyno-psykholohichna zbroya yak samostiynyy zasib vedennya informatsiyno-psykholohichnoyi viyny. (2010). Informational and psychological weapons as an independent means of conducting informational and psychological warfare. *Armament systems and military equipment*. No 1. pp. 141-144. http://nbuv.gov.ua/UJRN/soivt_2010_1_ 32.
77. Yuferev, S. Osleplyayushchiy lazer okazalsya effektivneye predupreditel'nogo ognya. (2014). A blinding laser turned out to be more effective than warning fire. Military Review /

09/11/2014. https://topwar.ru/57978-osleplyayuschiy-lazer-okazalsya-effektivnee-predupreditelnogo-ognya.html.

78. Zadorozhny, G. V. Konstsiyental′na viyna – providna forma heoekonomichnoho pidkorennya svidomosti yak novoho predmetu pratsi v umovakh neoliberal′noyi hlobalizatsiyi. (2021). Consciousness war is the leading form of geo-economic subjugation of consciousness as a new subject of labor in the conditions of neoliberal globalization. *Bulletin of Economic Science of Ukraine*, No. 1 (40). P. 199-206.
79. Zaur, Sabina. Stroboskopicheskoye oruzhiye – ot Arkhimeda do russkogo «Filina». (2019). Stroboscopic weapons - from Archimedes to the Russian "Filin". Axar.az/13.02.2019. https://ru.axar.az/news/politika/349271.html.
80. Zorina, E. G. Tekhnologii podryva legitimnosti gosudarstvennoy vlasti, ispol'zuyemyye v internet-prostranstve. (2016). Technologies for undermining the legitimacy of state power, used in the Internet space. *Information Wars*. No 1(37). pp. 78-80.
81. Igor Smirnov. Psikhotronnoye oruzhiye, psikhozondirovaniye. (2013). Psychotronic weapons, psychoprobing - REN-TV report / 08/17/2013. https://imperiya.by/show/psychoprobing.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.04

On the importance of continuous development in the military domain

Jonas Nordlöf
Licentiate of Engineering
Head of Department, Communications Electronic Warfare Systems
The Swedish Defence Research Agency
SE-164 90 Stockholm, Sweden
e-mail: jonas.nordlof@foi.se

Kristofer Bengtsson
Master of Political Science
Head of Department, Electronic Warfare Assessment
The Swedish Defence Research Agency
SE-164 90 Stockholm, Sweden
e-mail: kristofer.bengtsson@foi.se

Abstract. A significant percentage of modern products and systems purchased from the defense industry are difficult for the buyer to adapt or develop for new needs after lessons learned on the battlefield. This results in the procured systems having unnecessarily short lifespans. This paper contains a literature survey of the implementation and adaptation of military systems, combined with the authors' own observations from real cases of procurement in the military domain. Furthermore, this paper presents concepts for continuous development in the military domain, addressing several of the issues observed with modern systems. The term "continuous development" is here defined as the continuous modification, improvement and enhancement of military equipment or a military technical system over the course of its life cycle. The paper outlines how compatibility, flexibility and interoperability relate to unmanned aerial vehicles, counter unmanned aerial systems operations and electronic warfare operations, their role in continuous development and why these concepts are important on the modern battlefield. We contend that the ability to modify equipment increases adaptability, and therefore survivability, in conflict scenarios where new threats continuously appear. The paper concludes with recommendations of practical value for the defense industry on how equipment can be adapted to facilitate continuous development.

Keywords: continuous development, electronic warfare, EW, procurement, interface accessibility.

Introduction

As demonstrated during the Russian full-scale invasion of Ukraine it is hard to overrate the importance of versatile and potent military materiel as well as the flexibility in accepting and making use of said materiel. Many lessons can be drawn from this war, not only from a strictly military point of view but also from an industrial and government perspective with regard to how military materiel is produced and used. *Compatibility*, *flexibility*, and *interoperability* are key factors emphasized in this regard. Ukraine has received foreign military materiel and has, after a short training period, been able to put the materiel into good use on the battlefield. The creativity and innovativeness of Ukraine's use and integration of these systems (Jones et al, 2023) has at times even surprised the donating nations. This is indeed not only worthy of admiration but also clearly worthy of studies in the years to come: how did Ukraine achieve this effective implementation and what lessons can be drawn from it?

The authors suggest that one valuable lesson is the importance of continuous development in the military domain. The term "continuous development" is defined in this paper as the continuous *modification, improvement* and *enhancement* of military equipment or a military technical system over its life cycle.

Blakcori et al. (2024) note that procuring commercial unmanned aerial vehicles (UAVs) is often beneficial in the long-term provided that these systems employ open-architecture and modular systems, which are highly suitable for continuous development. For instance, the Ukraine-made Wild Hornet unmanned aerial system (UAS) can be customized to operate at different signal frequencies making it harder to jam by Russian electronic warfare (EW) systems (Roslin, 2023).

Experience from Ukraine also shows that almost all autonomous systems become obsolete over a six-week cycle due to enemy EW-tactics (Kaushal et al., 2023). Such systems then need to be modified or replaced. However, slow procurement processes can delay the acquisition for an extended period of time, well above the required six-week cycle, making these reacquisitions inadmissible at times. For such cases, development and modifications of available systems is the only viable option. For instance, procurement of counter UAS (C-UAS) systems by NATO and individual allies has been hindered for up to two years between the definition of requirements and contract execution (Borsari and Davis, 2023). Thus, the ability to conduct continuous development with military equipment and systems at hand is important because

(1) the systems will be adaptable to new threats and strategies,
(2) it enables the integration of lessons-learned from the front lines,
(3) it ensures that the equipment is relevant for a longer period of time, and
(4) it ensures soldiers' trust in their equipment, with regard to the before mentioned factors, thus increasing morale and overall combat efficiency.

As noted by Kaushal et al (2023), less focus should be put on designing a perfect system and more on continually adapting the software, frequencies and other aspects to keep ahead of the adversary.

Methodological Framework

This paper presents results and conclusions based on a literature survey of the implementation and adaptation of military systems, combined with the authors' observations and experiences from real cases of procurement in the military domain. The focus is specifically to investigate and evaluate the concept of continuous development for military applications with the purpose of identifying possible benefits and challenges.

Results

Military systems can be procured in several different ways. In recent years, there has been a transition from having a large set of technical specifications to instead defining a set of operational goals, or abilities, which need to be fulfilled. For the purpose of this paper, the authors suggest that procurements can be generalized into the following three broad categories:

- Category I: Buying off-the-shelf with limited ability to make changes in the equipment
- Category II: Buying off-the-shelf with access to modification capabilities
- Category III: Designing to specification

In order to integrate enhanced abilities in Category I equipment, it is often necessary to make new procurements. This can be acceptable for equipment with low cost and low survivability on the battlefield. However, this is seldom acceptable for other types of equipment, such as more advanced vehicles, *e.g.*, fighter jets, larger naval vessels or main battle tanks, due to the acquisition cost and logistical and infrastructural factors following in the wake of such enterprises.

There are several examples of Category I procurements where the equipment, not seldom highly advanced and therefore expensive, has become ineffective due to new threats. Since the buyers cannot

adapt Category I equipment to address these new threats by themselves, they must rely on the supplier to make the necessary changes. This is somewhat troublesome as specific threats, or other factors, might not necessarily be prioritized by the supplier. This could degrade the user´s trust and reliance in the equipment.

As new procurements are often needed in order to enhance the functionality of the original equipment, Category I procurements are not necessarily the best course of action. Therefore, national in-house development is often considered the only admissible approach in order to ascertain overall combat efficiency. However, this kind of materiel development is expensive and conducted at severe financial risk for the developing organization, especially if the equipment becomes too specialized due to national geographical and/or operational requirements.

Category III procurements have historically been common, especially in Sweden, with systems such as JAS 39 Gripen, CV90, Visby-class corvettes, submarines and the Archer artillery system. However, these tend to be quite complex projects with a high degree of risk for the developing nation and is therefore less prevalent today. Category II procurements therefore seem to be a viable cost-efficient solution. However, this requires that the supplier can provide potential buyers with a complete accessible interface, which enables national adaptations and enhancements for national specific demands and needs as they develop over time.

The authors argue that, to a greater extent, the concepts of Category II need to be integrated into equipment provided by the industry as these are not presently available in most equipment on the market today. This would enable national development of integrity critical systems. Furthermore, by making such equipment available, the suppliers will gain a commercial competitive benefit and the prospect of collaborations between military forces and the producing industry partner is improved.

UAV, C-UAS and EW-operations

This section emphasizes how compatibility, flexibility and interoperability relates to UAVs, C-UAS and EW-operations, their role in continuous development and how these are enabled by Category II equipment.

Compatibility: Experiences from modern military conflicts show that the effectiveness of UAVs depends on their integration into a wider military ecosystem centered on mutually supporting and enabling capabilities, such as EW, cyber, and intelligence gathering (Borsari and Davis, 2023). By providing the modification capabilities in Category II equipment to the user, this integration can be facilitated, through continuous development, even though the overall ecosystem is radically changed.

Flexibility: It has also been shown that, due to anti-radiation loitering munitions (Kasapoglu, 2020), the survivability of electromagnetic-radiating systems on the modern battlefield is low. Thus, reducing the time EW-systems spends emitting signals is crucial for the survivability of the system. Products bought off-the-shelf tend to have very general forms of jamming waveforms, the most common ways of jamming found in these products are barrage jamming. By using information of specific adversarial systems, gathered from different types of intelligence operations, more sophisticated jamming techniques can be utilized. As an example, utilizing knowledge about the 5G communication protocol, a denial-of-service (DoS) attack can be achieved on the 5G-system, which is designed for robustness and reliability (Rinaldi et al., 2021), by only jamming 0.1% of the OFDM subcarrier symbols (Lichtman et al., 2018). Similar results are expected to be obtainable for military systems.

In C-UAS and EW operations, classified information gathered through intelligence operations cannot always be shared with the industry. This often makes Category II procurement the only option, as modifications need to be performed by the military forces themselves in order to keep confidentiality, and as Category I often does not meet current and future needs. Furthermore, with highly flexible systems, approaches to handle new threats can be incorporated into current equipment.

The importance of this is underlined by lessons-learned from Ukraine, where critical systems need updates and modifications on a regular basis to keep ahead of enemy EW-tactics (Kaushal et al., 2023).

Interoperability: Even though new technology and new operations can be found on the modern battlefield, effective data management and interoperability across domains remain critical for the success of any military force (Blakcori et al., 2024). Whether unmanned systems are used to increase the precision of artillery (Kunertova, 2023) or to strike naval vessels (Sadler, 2023), they need to be coordinated with other domains in the battlespace.

In order for the industry to support these key factors in their products, increased focus and effort should be put on, (1) the use of highly compatible standards (compatibility) and (2) the ability for a user nation to modify threat and countermeasure libraries and mission data (flexibility). This technical compatibility enables interoperability (Moon et al, 2008), which in collective defense is of the utmost importance in order to, in turn, enable multilateral multi domain operations (MDO) within the realms of an overarching doctrinal strategy.

Interoperability and technical compatibility in an ever-changing world with ever-increasing geopolitical frictions have a great importance in the conduct of successful military operations. This is especially true in the defense of democratic and humanistic values against opponents with a total disregard for said values and who strive to achieve their agenda by any means necessary. Technological and operational adaptability together with allies is what enables success, this can be achieved in cooperation between government, academia and industry. This cooperation is also what needs to drive military innovation.

Alignment

In a larger perspective, military systems have developed from being hardware-defined, and thereby not easily altered without significant hardware modifications, to being software-defined, where, *e.g.*, the operating frequencies can be changed by a single line of code. This trend of software-defined military systems (Soare et al, 2023) makes the concept of *continuous development* even more appealing, as the modification of software can significantly increase the efficiency of military systems. Previously, the change might have included severe alterations due to the need for exchanging hardware components, which in turn could feed a need for redesigning the whole system to fit the new hardware. Software dependency is not all good, *e.g.*, increased need for experts at lower echelons to properly maintain and service the equipment, but the fact that certain changes to software can enhance a system's capabilities without changing the overall design is definitely one of the real benefits.

Continuous development of a software-based system is not necessarily without challenges between different actors and especially between nations with regard to the EW domain, which often is highly secretive in its nature. Although manageable, the exchange of data and information often needs to be accepted on the highest national decision level. To utilize the benefits of software-defined systems (and to some extent mitigate the challenges set out above), the key factors of compatibility, flexibility and interoperability need to be incorporated in the industrial product development, design and production. This can be achieved by implementing common industry standards.

The modification capabilities needed to enable continuous development range over several functions in a C-UAS or EW-system. In this paper we propose the following list of configuration or modification access needed for different purposes and capabilities:

- threat libraries for classification of emitters
- countermeasure libraries for dispenser systems and ECM waveforms
- modification of signal detection and signal estimation algorithms
- improving localization capabilities of surveillance systems

- sensor fusion and integration with command and control systems
- low-level access to data streams for detailed analysis

There are widely used standards that enable the above capabilities. Software standards such as SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology) (DSTL, 2021) and CESMO (Combined ESM Operations, NATO STANAG 4658) can be used to integrate systems and improve commander situation awareness. Data standards such as SigMF (Signal Metadata Format) (Hilburn et al, 2018) can be used for analysis and artificial intelligence. Data stream standards like the VITA 49 Analog RF-Digital Interface (Cooklev et al, 2012) are widely used for real-time signal processing and can be used to extend detection and other capabilities. Hardware standards like SOSA (Sensor Open Systems Architecture) enable modularity in hardware and extensive changes over the lifetime of a system (Collier et al, 2016).

Discussion

This paper is foremost aimed at addressing matters regarding procurement of military materiel and more specifically, materiel for UAV, C-UAS and EW operations. Interoperability is key and needs to be taken into consideration already at the design phase; will the system be compatible with systems from other, friendly, nations/actors?

Technical compatibility and flexibility not only enables continuous development in collaboration with others, but foremost it enables interoperability, which is deemed as essential for the efficient conduct of military operations in the (near) future (Weissmann and Nilsson, 2023). This, in turn, is driven by the overall worsening geopolitical environment, foremost in terms of the Russian war of aggression against Ukraine but also with regard to more increasing tensions between Western countries and Iran and China (Holmquist and Englund, 2020).

One way to enable continuous development is based on the adherence to standards and that partner countries and industry actors to a greater extent can engage in standardization processes and also agree on common standards. The adherence to common standards together with accessible interfaces would to a large extent enable partners to commit to continuous development. This could also feed the industry with new interesting business portfolios at the same time as the equipment stays relevant for a longer time. The overall combat effectiveness is also enhanced with less time spent training personnel on new, highly specialized equipment.

The immediate gains with using Category II equipment are assessed to provide a positive cost-benefit for governments and major industry partners. It also opens up the possibility for allies and partners to enhance already proven and potent military materiel to a lower cost. Lastly, Category II equipment would allow more experience to be pooled together to make equipment stay relevant in the face of time and emerging threats. This, in addition, is deemed by the authors to be cost reducing, as new materiel does not have to be procured to the same extent.

Conclusion

Given the geopolitical layout, interoperability is of the essence. One way to accomplish this is through technical compatibility. Technical compatibility, in turn, comes as a result of standardization, but can also be achieved through continuous development by partners and allies.

The industry embracing these factors is of the utmost importance. Applying a continuous development approach enables actors to conduct efficient procurement of military equipment that is capable of defeating the enemy today, tomorrow and beyond, without having to reinvest in new system designs.

The benefits for the industry also lies in the fact that if one user of a particular kind of military system has come up with a novel enhancement, this can benefit the original industry partner as well and might open up for new business collaborations.

This paper concludes that utilizing Category II equipment is considered the most beneficial

means of producing and procuring military equipment. This approach has several advantages over Category I and Category III, partly from an economic perspective but also from the perspective of compatibility, flexibility, interoperability and efficient conduct of military operations together with allies and partners.

Recommendations

The authors recommend all industry partners to increase the buyers' access to modification capabilities in military systems, thereby providing means for a continuous development of systems and to achieving a better outcome on the battlefield.

Acknowledgments

The authors would like to acknowledge the technical assistance of Per Brännström, Dr. Leif Festin and Simon Ahlberg.

References

1. Blakcori, N., Stathakis, L. I., Koutsoukos, L. D., Kirilov, L. K. (2024). The Evolving UAS Threat: Lessons from the Russian-Ukrainian War Since 2022 on Future Air Defence Challenges and Requirements. NATO, Integrated Air and Missile Defence Center of Excellence
2. Borsari, F., Davis, G. B. (2023). An Urgent Matter of Drones, CEPA. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/,Accessed March 10, 2024.
3. Collier, C. P., Lipkin, I., Davidson, S. A., Dirner, J. (2016). Sensor Open System Architecture (SOSA). In Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation. SPIE.
4. Cooklev, T., Normoyle, R., Clendenen, D. (2012). The VITA 49 analog RF-digital interface. IEEE Circuits and Systems Magazine, 12(4), 21-32.
5. Defence Science and Technology Laboratory, DSTL (2021). SAPIENT autonomous sensor system, https://www.gov.uk/guidance/sapient-autonomous-sensor-system,GOV.UK, Accessed March 10, 2024.
6. Hilburn, B., West, N., O'Shea, T., Roy, T. (2018). Sigmf: the signal metadata format. In Proceedings of the GNU Radio Conference (Vol. 3, No. 1).
7. Holmquist, E., Englund, J. (2020). China and Iran - an unequal friendship. The Swedish Defence Research Agency (FOI).
8. Jones, S., McCabe, R., Palmer, A. (2023). Ukrainian Innovation in a War of Attrition. Center of Strategic and International Studies (CSIS).
9. Kasapoglu, C. (2020). ANALYSIS - Five key military takeaways from Azerbaijani-Armenian war. https://www.aa.com.tr/en/analysis/analysis-five-key-military-takeaways-from-azerbaijani-armenian-war/2024430#, Accessed March 10, 2024.
10. Kaushal, S., Bronk, J., Watling, J. (2023). Pathways Towards Multi-Domain Integration for UK Robotic and Autonomous Systems, RUSI, Occasional Papers.
11. Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine, Contemporary Security Policy, 44:4, 576-591, DOI: 10.1080/13523260.2023.2262792
12. Lichtman, M., Rao, R., Marojevic, V., Reed, J., Jover, R. P. (2018). 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation. In 2018 IEEE international conference on communications workshops (ICC Workshops). 1-6. IEEE.
13. Moon, T., Fewell, S., Reynolds, H. (2008). The what, why, when and how of interoperability. Defence & Security Analysis, 24(1), 5-17.

14. Rinaldi, F., Raschellà, A., Pizzi, S. (2021). 5G NR system design: a concise survey of key features and capabilities. Wireless Networks 27, 5173–5188. https://doi.org/10.1007/s11276-021-02811-y
15. Roslin, A. (2023). Wild Hornets: Ukraine's Tiny Armor-Busting, Trench-Clearing Secret Weapon, Kyiv Post, July 8, 2023, https://www.kyivpost.com/post/19227, Accessed March 10, 2024.
16. Sadler, B. D. (2023). Applying Lessons of the Naval War in Ukraine for a Potential War with China. Backgrounder 3743, 1-13.
17. Soare, S. R., Singh, P., Nouwens, M. (2023). Software-defined Defence: Algorithms at War. The International Institute for Strategic Studies.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.05

Realising Ukraine's military potential in the Space Domain

Frank Ledwidge
PhD, FRHS,
Senior Lecturer in War Studies at the University of Portsmouth,
Senior instructor in Space Power at the
Royal Air Force College, United Kingdom
e-mail: frank.ledwidge@port.ac.uk

Abstract. Whilst conventional assistance (such as artillery, tanks, fighter jets etc) has been widely discussed, the most indispensable asset has gone largely unrecognised even whilst it shapes all of Ukraine's operations. From the essential communications role of Starlink to the 'space-powered targeting information and processes underpinning Ukraine's strike capabilities, space is the decisive supporting element. During the current war, the leverage provided by the west's decisively superior space capabilities has proved to be vital in allowing Ukraine to resist an ostensibly more powerful force. However, both the need for and potential of Ukraine's own sovereign space power is evident. Ukraine has the history and resources to be a leading space power in Europe and worldwide.

In order to further this aim, once there is the conceptual space to do so, Ukraine must begin the process of renewing and developing a National Space Strategy. This should be followed by, or be concurrent to the development of formal space doctrine. There are many excellent examples of national space strategies which provide much food for thought. These ae resources from which to draw. Ukraine like all countries has a unique set of resources and experiences which must be reflected in such strategy and doctrine. The process of drafting this guidance itself promotes thinking and planning and the product can and must be a guide to all military officers as to what the space domain can offer. It can also promote and drive essential co-operation.

Keywords: space domain, scientific and industrial enterprise, NATO, defense space strategy, Ukraine's military potential.

Introduction

Since the beginning of the space age in 1957, space has been an arena of military activity, offering military and political leaders access to the 'ultimate high-ground'. Space activities were also used to promote ideology, demonstrating the superiority of the US or indeed USSR. All of these factors a still the case, and indeed it is certain that access to space and the use thereof is more important than ever and its importance will only increase. As French defence Minister Florence Parly said in 2021 'If space was the new frontier in the 1960s, there is no doubt that today it is a new front on the battlefield' (French Defence Minister, 2021). The key importance of space activities was confirmed when NATO added it as its fifth combat domain in 2019 (NATO, 2023) and outlined its approach to that new domain. Civilian life in most contexts today, certainly in Europe, relies upon satellites for every major function of life. As in the military world, the importance of – for example – GPS systems in governing bank transactions, supply chains, weather forecasting, agricultural surveying and planning or the use of the internet is rarely considered. Space is absolutely vital however in all of those and many, any more contexts. There are tens of thousands of satellites now in orbit of all sizes

This article will not discus in detail contemporary space operations, partly because such matters are rightly claissified, and partly because they take place – as far as is known – at the tactical level, whereas this brief study is concerned largely strategic and policy matter. However, in general we can state with confidence that space has been an absolutely vital domain in Ukraine's successful efforts

to resist Russia's invasion. Currently, today, the US is by far the dominant space power. There is no Premier League of Space Powers, there is the United States and – in various degrees – everyone else. However, the US is seriously concerned about the rise of China which is placing vast investments into its military space programme. The significant of this for Ukraine may not be immediately apparent, but it is nonetheless great. If Ukraine, or indeed any other allied power is to be sure of gaining the advantages of 'the ultimate high ground' there must be no complacency. Retaining the west's edge is a matter of urgency. As former Commander of US Space Command Lt General Stephen Kwast has put it 'China is on a ten-year journey to operationalise space, we're on fifty years journey' (CNBC, 2017). Ukraine has a major part, if it wants it, to play in helping our side. This short paper outlines how Ukraine may begin, or as we will see, continue to do so. On the way, we will look at the basics of space power, its role in the Ukraine war, Ukraine's role as a leader in space power the importance of strategy and doctrine and finally what partnerships Ukraine can utilise into the future.

The First essential requirement is building awareness at all levels of military operations – beginning by ensuring that all officers are trained in the basics of space power. In turn Ukraine's approach needs to be based upon a sound, NATO compatible doctrine and above all a considered, well-planned and realistic strategy. Second is building Ukraine's already formidable military space skillset. Finally, by leveraging existing skills, knowledge and infrastructure, Ukraine is well-placed to become a leader in European space infrastructure and operations.

Space and its vital role in Defence

Generally, during civilian life or indeed military operations, despite the centrality of space its importance is usually forgotten as an individual gets on with his task. However, almost all military operations have a space element to them. In deed very many would be impossible without them. Most basic space manuals outline the five main tasks and roles fulfilled by space. NATO's 'Approach to Space' (NATO, 2023) outlines them: they are

1 Positioning, Navigation and timing (in English 'PNT'). Of all the functions of space, this is the most founds all others, including communications. The main role of GPS (USA), Galileo (Europe), Glonas (Russia) and Baidou (China) is PNT. The purpose for which GPS was designed and deployed in the 1980s was to assist targeting, and this allowed the development and use of precision-guided weaponry. The direction and protection of these assets is a major role of all space forces.

2 Early warning; this is probably the most strategically vital function after PNT. It allows for the detection of enemy missile launches. Equally importantly it can also determine whether missiles have NOT been launched or prepared for launch and therefore can act in reducing tension. Accordingly, access to space can act as a major factor in threat reduction and assurance

3 Environmental monitoring, extremely useful of course in civilian roles for agricultural and scientific work of various kinds. These kind of applications can, for example, be used for meteorology and therefore mission planning for air forces.

4 Secure satellite communications are absolutely vital for armed forces of all kinds, particularly those deployed worldwide. So for example the UK – not a major space power – has forces globally and has developed the Skynet system (now into its sixth generation) to ensure security of all forms of communications. At the more local level, Starlink – which very different in design and concept from the large older-format communications space craft has proved to be decisive in Ukraine for the same purpose.

5 Intelligence, Surveillance and reconnaissance. All of these functions are of course critical for situational awareness, mission planning and decision making at tactical, operational and strategic levels. Because of its strategic importance, the space domain, as NATO puts it is 'congested,

contested and competitive – the last two imply conflict. Consequently, military space forces are now, for major military powers that can afford or have the expertise to operate or exploit space assets vital component of defence forces. It must be stressed that a power need not have spacecraft in orbit to exploit what space can offer as a vital enabler of military operations. The ability to exploit space is just as important as the ability to build or operate satellites. In deed the latter is useless without the former. Much, indeed some might argue most space technology might be termed 'dual-use'. That is to say that they can be used for civilian or military use. The most obvious example of this is imagery, which can be sued, to take one of hundreds of examples, the assessment of agricultural plantation or the identification and targeting of military formations. As we saw above, GPS and its Chinese, Russian and European equivalents are as much – if not more – useful for civilian applications than military (Defence). Indeed, it is certainly the case that it is *civilian* technological investment and research that drivees military development now. Of course there are many roles of satellites that are entirely military in nature, notably the crucial role of missile defence, where satellites identify the launch of missiles by adversary powers. All of these applications, civilian and military require vast amounts of analytic capability. This role is a crucial aspect of space power (Maxar, 2023).

Significance to the Ukraine war

Whilst all of the roles of space power played a part in the Ukraine war, the key, perhaps even decisive role of space in the Ukraine war, was first appreciated in the early days of the war. This was particularly true concerning its contribution to the Intelligence Surveillance and Reconnaissance picture. This was most publicly visible when pictures of the 'traffic jams' of Russian army vehicles were released. These were produced and delivered to a large extent by the commercial company Maxar. In deed even before the war, the elements of transparency available due to extensive commercial surveillance made it far more difficult for Russian disinformation to develop any degree of credibility. Even ten, and certainly twenty years ago this kind of imagery was available only to those with the highest security clearance. In deed your author recalls using such imagery in planning operations in Iraq when fairly primitive (by today's standards) pictures used for target identification required extensive justification. Now, images of a far higher degree of clarity and resolution are available on anyone's computer or indeed telephone. This ability to access civilian applications which work at or around military specifications highlights what the current commander of the US Space Force calls 'the commercial augmentation of space capabilities' (Breakingdefense, 2023).

No platform demonstrated this more than Starlink, which whilst it started as what amounted to a ex tempore gift from Elon Musk to replace some of the benefits of the communications systems lost to Russian cyber attack, become a crucial enabler – perhaps the only true crucial enabler in Ukraine's arsenal. Whilst there have been controversies over its deployment and use, this remains a vital part of the connective tissue holding Ukraine's Command and Control systems together at the operational and tactical level. It has largely (not entirely) proved resilient to Russian attack (Connell, 2023) and is likely to remain so now that Starlink over Ukraine has now evidently come to some extent under the responsibility of US Space Command (Defenseone, 2023). The various controversies over Starlink, as well as the undoubted decisive edge that it provided highlights the need to caution over the military outsourcing of communications or other space technology.

Clearly products of NATO and especially US space assets are being extensively used to assist Ukraine. Much of this use is rightly classified and only history will be able to tell us what difference it made. One might speculate tht this was particularly useful in the Intelligence, Surveillance and Situational Awareness roles, but confirmation must wait until long after the war.

In addition to services and functions leased or donated by foreign states or companies it is important to recall that Ukraine has also been highly active in its own right in space. Its own 'Sich' Erth observation satellite. Further here is evidence that it has leased services from the Finnish

company ICEYE which has a constellation of synthetic aperture radar satellites (Mike Wall, 2022). Ukraine ahs been successful in conducting cyber attacks against Russian satellite communications (Connell, Michael, 2023). We do know, from extensive open sourcing, that the access to commercial imagery from such companies as Maxar, PlanetLabs and Blacksky have given Ukraine 'a select advantage in the space domain', particularly in the imagery intelligence aspect.

Against the background of the Soviet Union's impressive performance during the Cold War it is important to realise that Russia is most certainly not the power it once was. To put this into context as of May 2022, Russia had 172 operational satellites. Chona had 451 – making it the second space power. Overwhelmingly the leading space power is the United States with 3433 operational satellites in orbit. The situation for Russia is even worse than it initially seems, since many of its spacecraft are coming to the end of their lifetimes. This lack of numbers and presence placed Russia at a significant disadvantage relative to the assets deployed by Ukraine's allies. The military demands of Russia's space assets 'significantly exceeded the supply'. The situation is such as Russia's civilian space agency, Roskosmos, has been required to supply imagery at – by modern standards – very low resolution and low revisit-rate Resurs and Kanopus family of satellites (Connell, Michael, 2023). The practical result of this is that Russia is losing the war in space and until Russia can access some Chinese commercial (or more unlikely military) satellite imagery for targeting and other intelligence purposes, it will remain at a significant disadvantage. It is worth mentioning that a Chinese firm Spacety was sanctioned by the US for providing imagery to the Wagner mercenary organization (Connell, Michael, 2023).

In summary, as Connell puts it 'the performance of the KV in Ukraine significant gaps remain in its capabilities, especially in the areas of earth imaging and reconnaissance (Euspa). In the medium and longer term, there is no doubt that Russia will continue on its trajectory as a declining space power. Its launch services will no longer be attractive or-due to sanctions-legally viable to US and European interests. In the commercial sector there is equally no doubt that Ukraine will be well placed to full part of the gap left by that country. Fortunately, Ukraine has a history and space culture that places it in Europe's first division of space-faring nations.

Ukraine as a spacefaring nation past and future

It is often forgotten, not appreciated or ignored that Ukraine is one of the major European spacefaring nations. This is not the place for a recital of why this is, its deep historical heritage or a detailed survey of its contributions to the exploration and exploitation of orbital space. It is sufficient to state that during the Soviet Union, Ukraine was the heartland of rocket and satellite engineering of all kinds. This industry was centred, and will again be centred in the 'Rocket-city' of Dniepro where the rocket and design facilities of Yuznoye and Yuzmash were based. Ukraine's pre-eminence was still, indeed even more the case before the large-scale invasion in 2022. Indeed, an argument can be made that aside from France, Ukraine was the pre-eminent space-industrial power in Europe aside from France. It constructed and deployed major elements of US and other national space systems, notably the highly successful Zenit, Cyclon (both derived from ICBM designs) and Antares rockets and rocket structures (Nkau).

'Ukraine a country of engineers' and Ukraine's pre-eminence in space-engineering only reinforces this precept. The design, construction and operation of spacecraft may be described as the pinnacle of engineering skills, given the environmental extremes and temperatures within which they operate. Many opportunities for startups like Israel. The applications are not of course confined to the public or state sector. Ukraine has many fine space companies, many of which are adjusting to the needs of the war (Tereza Pultarova, 2023).

All of this demonstrates the potential inherent in this aspect of Ukraine's scientific and industrial enterprise. There is clearly vast potential for investment and development, to assist in the reconstruction of the country's economy. However, the potential does not stop there. There is also

the prospect of leveraging all of this experience, knowledge and infrastructure into the wider and at least equally vital field of military space. As Ukraine further develops as a space power, building on its fine history and current skills and experience it will be vital to get the political and organisational basics right. This implies a number of factors. First, Ukrainian military leaders and space experts will need to establish what its assets and potential in space are, and how that potential might be applied to its military power. There fore a military space strategy will need to be developed. The next section will deal with why this is and what elements it should contain.

Planning the future – Strategy and military doctrine

Serious space powers need a number of institutional basics. First, is a strategy. Ideally a strategy for space security and defence should be subordinate to an overall national space strategy. This is certainly the approach of some countries such as the United Kingdom an ambitious and growing space power, if at the moment somewhat underfunded (see below).

The second, which should follow and be subordinate to a military space strategy, is workable doctrine. As we will see, doctrine is a driver of thinking but also informs operators and allows them a common frame of reference.

Crucially, Ukraine already has defined its ambitions for integration into European and western security structures, the European Union and NATO. Ukraine's future contribution in these areas will be subordinate to their approaches and strategies. NATO has no strategy for space as such. This is as it should be, as it leaves it open to member states how they approach the issue by reference to national priorities. However, NATO does have what it calls its 'Approach to Space' (NATO, 2023) and which is itself subordinate to the NATO 2022 Strategic Concept. The 'Approach to Space' outlines the development of some NATO organic capabilities such as what it calls the 3SAS (Strategic Space Situational Awareness System) be based in Luxembourg and a virtual constellation of national satellites to provide faster data-integration and therefore intelligence. This will be called 'Aquila'. All of this will, it is supposed, be overseen by the NATO Space Centre in Ramstein.

As matters stand, there is no 'common approach' to space strategy. This is currently the responsibility of individual nations; chief amongst them is of course the United States.

United States Space Strategy

The US has of course been developing strategies for its defence activities in space for six decades, and a vast amount of thought goes into each one. It is of course in this respect, as in so many others, in a class of its own. It has a vast space defence system, and each of its now six services have operational contributions and requirements involving the space domain. As matters stand the overrising strategy is the US Defense Space Strategy of 2020 (Defence, 2023). Most of it is classified but a public summary declares that it sets out 'four priority lines of effort to achieve the desired conditions while addressing identified threats, opportunities, and challenges:

1) Build a comprehensive military advantage in space.

2) Integrate military spacepower into national, joint, and combined operations.

3) Shape the strategic environment.

4) Cooperate with allies, partners, industry, and other U.S. Government departments and agencies' (Spacecom, 2020).

From Ukraine's perspective It is worth noting the latter priority of co-operation with allies and partners. It must be stressed once again that the US is in a class of its own. As we saw above it is not only peerless with respect not only to its thinking and experience, but also to its capabilities and number of platforms. It is worth stating her that the US Defense establishment now has its eyes firmly directed to the nation it regards as its 'pacing threat' which is China.

Of more use to any senior military official concerned with thinking about space strategy from a practical perspective, it may be worth looking at how two similarly sized European nations have looked at the development of their space strategies, Europe's current leader in space which is France, and a rather less ambitious United Kingdom.

France's Space Strategy

France has certainly the the most significant space industry and expertise in Europe. In terms of its experience France is in some ways comparable to Ukraine in its long history and focus on the space domain in both its civil and military contexts. Indeed, reflecting its European pre-eminence in space France was the first country in Europe to rename its air force the 'Air and Space Force' ('Armee de l'air et de l'espace') in 2019 if one excepts Russia (VKS renamed in 2015). France in space, as it does in nuclear weaponry and indeed across its military capabilities, prioritises strategic autonomy. Indeed, this is explicitly and firmly dealt with in its Space Defence Strategy (Gouvernement, 2020) which is well-written and is clearly the fruit of extensive and detailed consultation and consideration. It is a model national space strategy, brief (only 36 pages) to the point and clear. I Its space ambitions as described in the Strategy are modified by a realistic assessment of its capabilities. These are considerable, it is important to recall that France is essentially at the centre of the European space industry. which whilst considerable may not be compared to the major space powers. He area around Toulouse is the powerhouse of European and French aerospace activities and ESA has its main launch facilities in the territory of French Guyana, which is a part of metropolitan France. This is reflected in its strategy which sets out an ambitious but achievable set of policies and investments.

The Strategy describes the challenges and opportunities offered by military space, and vitally from the perspective of Ukraine (i.e., as an example of how Ukraine might set out its ambitions) sets out a useful roadmap delineating how France will achieve its strategic objectives. This includes relevant objectives for the development of defined capabilities and indeed equipment, complete with timelines with the overall and overriding objectives of France's wider plans set out in its Military Planning Act. The importance of partnerships is stressed, with clear descriptions of how France sees the contribution other states such as Japan, Germany, the UK, Italy and of course the United States can make to the achievement of its overall strategy. Importantly, it outlines explicitly that the next stage is the formation of doctrine, incorporating the technological and scientific developments with the following principles at their heart: autonomous assessment and decision-taking; France as a driver of the space sector in Europe and developing the means to defend our capabilities and ensure compliance with international law, including self-defence. All of these, and a great deal more within the strategy provides clear guidance for those developing the doctrine for how France does and will operatioalise its space capabilities.

The United Kingdom Space Defence Strategy

In the words of one leading UK space expert, the UK has a lot of catching up to do with its allies' (Juliana Seuss, 2022) UK Space Strategy – less impressive and comprehensive than either France or of course the US – lacks specificity save for budget which is unimpressive for comparison France spent 646million Euros in 2022 (Defensenews, 2022) alone on the space domain. The UK aspires in its space defence strategy – which rightly followed the Space Strategy - to £1.4 billion spread over this decade (although a previously committed 5 billion to the main UK communications satellite system should also be taken into account (RUSI, 2022). Priorities are far less ambitious than France's aspirations focussing first on SATCOM and second on Space Domain awareness, leveraging already existing platforms and facilities on the ground. Various other data support and surveillance satellite constellations are planned (notably the ISTARI system of low earth orbit spacecraft. However, there is an evident lack of specificity and – frankly – ambition in the document and it compares unfavourably to that of France.

The European Union's Space Defence Strategy

The nature of the military alliances and relationships, matters such as security guarantees, NATO membership and so forth are all matters of extensive debate and discussion. Huwever one relationship which will certainly exist and expand is that with the European Union. In the area of humanitarian support from space, the EU has already at least one initiative the '#EUSpace 4Ukraine, the idea of which is to match innovators with humanitarian requirements. This has proposed a number

of applications invoilving the ESA's Copernicus and Galileo systems in humanitarian tasks such as agricultural surveys and EHNSS enabled drones for search and rescue (Euspa). It is worth saying that earth observation and ENSS-enabled drones are potentially dual-use.

However, dual-use or not, there is a significant difference between an ad hoc series of projects and a strategic and operational co-operation between partners for the purpose of defence and security. What then is the EU approach to the space domain and its security implications? Clearly the Ukraine war triggered off some thinking in the EU Commission.

In order to exploit the lessons offered by Starlink, the EU is planning to develop a megaconstellation called Iris (Politico, 2024) which of course will have predominantly civil use, but equally obviously will have a dual-ue. EU now see space as a significant priority and there is no doubt at all that this new sense of urgency was driven by the Ukraine War.

Accordingly, the EU have made a start in becoming active as a player in the space defence world. They have drafted a military space strategy (Eur-lex, 2023). This is similar in some respects to other strategies it sets out to take 'action to protect its space assets, defend its interests, deter hostile activities in space and strengthen its strategic posture and autonomy'.by laying out a shared understanding of space threats', resilience and protection of space systems, Responding to space threats, the use of space for security and defence and most importantly for Ukraine, partnering both with multilateral bodies, close allies such as the US and 'likeminded third countries'…

Over all the EU Strategy is rather more descriptive than prescriptive and so may struggle to be seen as a true strategy. This view may be reinforced by its advocacy of 'exploring synergies' and 'modalities' and unlikely ambitions for ensuring that 'all available EU tools can rapidly e mobilised thereby improving its space response architecture' All of this and more seems somewhat unlikely and rather bureaucratic in nature. Given that this is the EU Commission, this is not surprising. It is an organisation not built for rapid action. Huwever it is blunt that the EU and the Commission lack expertise in space. This is certainly not true overall the EU contains excellent expertise if one defines it as composed as states. As a quasi-state itself, certainly less so. Nonetheless, there is a stress on education and training which is essential in any spacefaring polity. Its lack of specificity in some respects has its advantages from Ukraine's perspective as it may allow for Ukraine to take the initiative whilst being compliant with the strategy, especially aas Ukraine moves towards the EU.

Operationalising Strategy – Military Doctrine

At the same time, as developing strategy. military space experts, once they have established the nature and extent of Ukraine's capabilities now and into the future, will need to decide upon and draft a military space doctrine.

The development of doctrine has several roles. It forces thinking, coheres approaches and provides common standards, A good simple and clear definition of military doctrine is as follows:

'The principle purpose of military doctrine therefore, is to provide the armed forces with a framework of guidance for the conduct of operations. It steers military forces in their actions while also situating the context in which those actions will be taken (UK Army Doctrine Primer, 2011). From that, it should be clear that space operations lend themselves to the development of a common understanding of what they do.

The Role and Function of Military Space Doctrine

The country which has applied by far the most thought to the use of space in military operations is the United States. A close second, is Russia. US Space Readiness and Training Command (STARCOM) set out the function of space doctrine as; establishing a common frame of reference on the best way to plan and deploy space forces as part of a broader joint force'. The US has produced a hierarchy of doctrine publications which taken together provide a comprehensive introduction and guide to military space operations (Starcom).

These are divided into three levels. First there is the 'Capstone' composed of one doctrine note'. This sets out the fundamentals of pace power. Subordinate to that are seven other 'keystone' doctrine publications, at the operational level. These deal respectively with Personnel, Operations, Training, Sustainment, Planning and Mission Command (Starcom). Space Situational Awareness, space battle

management and Joint All-domain Operations sit under the Operations heading.

Finally, there are the documents comprising the tactical element. Below is a diagram of US space doctrine (Ibid).

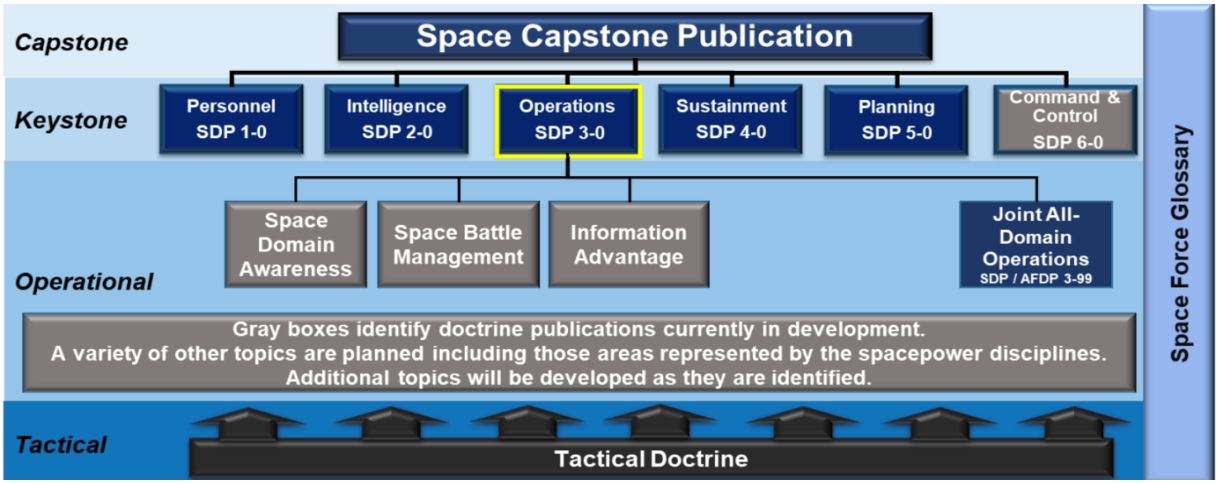


Figure 1. Space Force doctrine hierarchy

These documents et out definitions of terms as understood by the relevant military authorities, competencies and roles, the 'why, how and who' of each of them, the various relationships at the institutional level s that are desirable to build and above al how and with what assets various tasks are carried out. The threats to space assets, in orbit and on the ground as well as in the various electromagnetic spectra are also described with information as to how to counter them. As well as requirements for training and sustainment of on-orbit equipment there are also indications as to the legal and other constraints which apply to space operations.

All of this requires a good understanding of what resources are available or might become available. In the context of space operations these documents also serve as a primer or introduction to how military space assets work within the context of the relevant country. In deed the STARCOM publications provide a comprehensive outline of how the US does space operations. Importantly, it must be stated and recognise that this is the gold standard for space doctrine produced by a state whose space assets are, as observed above, in a league of their own. No other country will match the US in the comprehensiveness of its doctrine and it would be counterproductive to attempt to do so. The importance for Ukraine of these documents is simply that they contain the full spectrum of space operations from which much practical advice can be drawn.

However, is this full systematisation of space power useful to a country with the limited resources of Ukraine? As Ukraine moves towards building and systematising its military space it is important to realise that hat matters most is not the equipment one has, but how one uses it. The last two years of war have demonstrated this principle as a continuing reality. US doctrine is a repository of best practice drawn from many decades of experience and development. For an example of the doctrine of a smaller, experienced but significantly less resourced space power it is worth looking at the United Kingdom.

The United Kingdom' military space doctrine

As we saw above, the UK has a far more limited military space programme than the US or indeed France. However, it has closely followed best practice in developing its strategy alongside its doctrine. Until 2022, UK space doctrine was always published as a component of air operations (UK Ministry of Defence, 2017). In 2022 the first separate UK Space Power doctrine was produced (UK Space Power, 2022). Clear and relatively brief (at just over 104 pages) it is well constructed, well-written and provides a clear account of how the UK sees space operations, particularly with its stress on seeing it as part of an integrated approach. Like all good doctrine, it also provides a very sound introduction to how space power work in the military context. It also provides a clear direction on

how partners inside government and UK industry, echoing the UK National Space Strategy; as it says 'This strategy is about more than capabilities; it is about partnerships; government working as one with industry and international allies' (Ibid). There is also emphasis on academic partnerships.

Conclusions and recommendations

The following simple recommendations require a minimal outlay of any funds, save for the time of the participants for consideration. Both are vital preconditions for the development of Ukraine's potential as a significant space power. Ukraine will require the drafting of a space defence strategy and in due course space doctrine. An essential prerequisite for both of these activities is extensive discussion amongst military space commanders, other commanders, political leaders and diplomats as to the shape of Ukraine's space defence approach. The way other European countries have approached this will provide excellent guidance. The process itself of developing strategy and doctrine is as important as the product. In deed a process without the product of a defence space strategy is far more constructive than the production of a poor strategy without a process.

Those who are convinced of the importance of space to Ukraine need to be conscious that very many people either do not understand or indeed have little or no idea of the importance of military space capabilities. There fore awareness raising is essential. This has been a struggle for many western countries, both for civilian leaders as much as for senior military officials. Convincing decision-makers of the centrality of space to defence is a prerequisite to decisions concerning procurement of investment. Equally important is the necessity of educating more junior officials not only of the centrality of space to defence but how practically it can help them in their day to day work; answering the question so space is important; so what? Ukraine should consider developing a programme of education both for senior officials – military and civilian, and a series of courses for operational officers. At the very least, good doctrine provides the basis for the provision of currucula for such courses.

References

1. French Defence Minister 'Shifting from a new frontier to a new front'. (2021). *Defense News.* December 6. Available at https://www.defensenews.com/outlook/2021/12/06/french-defense-minister-shifting-from-a-new-frontier-to-a-new-front/
2. NATO's approach to space 23rd May (2023) available at https://www.nato.int/cps/en/natohq/topics_175419.htm.
3. URL : https://www.cnbc.com/2017/11/10/usaf-general-steve-kwast-china-in-space-five-times-faster-than-us.html.
4. NATO's Approach to Space available at https://www.nato.int/cps/en/natohq/topics_175419.html.
5. There is an excellent video primer on military GP functions here: https://www.defense.gov/Multimedia/Videos/videoid/906449/
6. See for example https://blog.maxar.com/earth-intelligence/2023/the-game-changing-role-of-commercial-satellite-imagery-and-analytics-in-ukraine.
7. Interview with General Chance Saltzmann Breaking Defense 13th January (2023). Available at https://breakingdefense.com/2023/01/ukraine-spotlights-criticality-of-space-in-conflict-saltzman/
8. Michael Connell; 'The Role of Space in Russia's Operations in Ukraine'. (2023). (Center for Naval Analysis – CAN, November 2023) available at https://www.cna.org/reports/2023/11/Role-of-Space-in-Russias-Operations-in-Ukraine.pdf. at p. 9.
9. 'Pentagon buying Musk's Starlink for Ukraine; *Defense One*. June 1 2023. available at https://www.defenseone.com/policy/2023/06/pentagon-buying-musks-starlink-ukraine/387022/
10. Mike Wall; 'Ukrainian Charity buys radar satellite service sto help fight Russian invasion' (2022). (Space.com 19 August) Available at https://www.space.com/ukraine-radar-satellite-services-russian-invasion.
11. Connell, Michael. 'The Role of Space in Russia's Operations in Ukraine' (2023). Center for

Naval Analysis – (CAN), November. available at https://www.cna.org/reports/2023/11/Role-of-Space-in-Russias-Operations-in-Ukraine.pdf at p. 15.
12. Connell; p. 9.
13. Connell; p. 11.
14. Ibid p. 25.
15. For more information see https://www.nkau.gov.ua/ua/launches-of-ukrainian-lv-ua/
16. For more see Tereza Pultarova 'Ujraine's space start-ups recalibrate to adjust to the challenges of the war'. (2023). (via Satellite 23 November) available at https://interactive.satellitetoday.com/via/december-2023/ukraines-space-startups-recalibrate-to-meet-the-challenges-of-the-war/
17. 'NATO's Approach to Space'; last updated 23rd May (2023) available at https://www.nato.int/cps/en/natohq/topics_175419.html.
18. An unclassified summary (2023) is available here: https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_ DEFENSE_SPACE_STRATEGY_SUMMARY.pdf.
19. US Space Command Press release June, 17 (2020) available at https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2223891/department-of-defense-releases-defense-space-strategy/
20. 'Armee de l'air et de l'espace'
21. See 'Defence Space Strategy; Report of the Space Working Group' (2020). available at https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2020/08/france_-_space_defence_strategy_2019.pdf.
22. Juliana Seuss; 'The UK Defence Space Strategy' RUSI February (2022) available at https://www.rusi.org/explore-our-research/publications/commentary/uk-defence-space-strategy.
23. https://www.defensenews.com/global/europe/2021/09/22/next-gen-tech-investments-platform-upgrades-lead-frances-2022-defense-budget/
24. 'The UK Defence Space Strategy' (2022). RUSI, February. Available at https://www.rusi.org/explore-our-research/publications/commentary/uk-defence-space-strategy.
25. See https://www.euspa.europa.eu/euspace4Ukraine#:~:text=Country%3A%20Ukraine&text=Their%20key%20objective%20is%20to,Tech%20Hub%20in%20Eastern%20Europe.
26. Spac Wars; Europe's mater plan to counter Elon Musks Starlink' *Politico* January, 25, (2024). available at https://www.politico.eu/article/space-wars-europe-masterplan-counter-elon-musk-starlink/#:~:text=But%20there%20are%20problems%20with,Volodymyr%20Zelenskyy's%20calls%20for%20aid.
27. Full text (2023). available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0009.
28. UK Army Doctrine Primer (2011) available at https://assets.publishing. service.gov.uk/media/5a79b6c540f0b63d72fc7eac/20110519ADP_Army_Doctrine_Primerpdf.pdf.
29. See Space Doctrine Publication 4-0 'Sustainment' available at https://www.starcom.spaceforce.mil/Portals/2/SDP%204-0%20Sustainment%20(Signed).pdf?ver=jFc_4BiAkDjJdc49LmESgg%3D%3D#:~:text=United%20States%20Space%20Force%20(USSF,of%20a%20broader%20joint%20force. At p. 3.
30. See STARCOM wire diagram and linked publications at https://www.starcom.spaceforce.mil/Resources/Digital-Library/
31. Ibid.
32. See for example JDP 0-30 'UK Air and Space Power (UK Ministry of Defence 2017) available at https://assets.publishing.service.gov.uk/media/5a8238bd40f0b62305b9320c/doctrine_uk_air_space_power_jdp_0_30.pdf.
33. UK Space Power (September 2022) available at https://www.gov.uk/government/publications/uk-space-power-jdp-0-40.
34. Ibid p. 56.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.06

A conceptual approach to improving the information support of the prospective Armed Forces of Ukraine

Oleksandr Peredrii
Candidate of Military Sciences, Senior Researcher
Head of the Research Department of the Center for Military and Strategic Studies
of the National Defense University of Ukraine,
03049, 28 Povitroflotskyi prospect, Kyiv, Ukraine,
ORCID: 0000-0003-2877-4959

Petro Snitsarenko
Doctor of Technical Sciences, Senior Researcher,
Leading Researcher of the Center for Military and Strategic Research
of the National Defense University of Ukraine,
03049, 28 Povitroflotskyi Prospect, Kyiv, Ukraine,
ORCID: 0000-0002-6525-7064

Yurii Sarychev
Candidate of Technical Sciences, Senior Researcher,
Leading Researcher of the Center for Military and Strategic Research
of the National Defense University of Ukraine,
28 Povitroflotskyi Prospect, 03049, Kyiv, Ukraine,
ORCID: 0000-0003-1380-4959

Viktor Zubkov
Senior Researcher of the Center for Military and Strategic Research
of the National Defense University of Ukraine,
28 Povitroflotskyi Prospect, 03049, Kyiv, Ukraine,
ORCID: 0009-0008-5755-2339

Abstract. The relevance of this article is due to the fact that modern armed conflicts lead to a change in the nature of military operations, which increasingly acquire an informational and technological nature, which forces the leadership of the leading countries of the world to review the theory and practice of the military construction in order to implement the concept of "network-centric war". This approach involves considering the control bodies, units, planes, ships, communications, and intelligence of the armed forces as objects connected to a single information and communication network. The capabilities of such a network-centric system of conducting military operations are determined by the capabilities of the entire group of objects connected to the network (synergistic effect). In the implementation of this concept, a key role belongs to the information support of objects of a single network, which has a number of components that need to be implemented in a network-centric system of conducting military operations. The requirement for high operational efficiency of information support necessitates the widespread introduction of automated control systems (ACS) in such a system. At the same time, the information support of the objects of the unified network is the main purpose of the ACS, the means of which in automatic mode allow you to quickly display the situation, assess the terrain, the state of the enemy, your troops (forces), model the development of combat operations, develop options for solutions, draft combat documents, prove tasks to

subordinates, control their execution.

The article analyzes the experience of implementing information systems for managing the armed forces of leading countries, the peculiarities of their organization and implementation in the armies of NATO member states. Based on the results of this analysis, approaches to determining ways to improve the information support of the control systems of the Armed Forces of Ukraine are proposed. One of the main tasks of the Armed Forces of Ukraine (Defence Forces) on the way to NATO membership is the creation of a network-centric military control system, which should be equipped with ACS and compatible with the Alliance's military control systems. Meanwhile, according to foreign publications, the level of automation of the control systems of the defense forces of Ukraine today is 2-2.5% compared to the armed forces of the leading countries in the world, in which ACS ensure the level of automation of C4ISR management functions (command, control, communication, informatization, intelligence, etc.). For this reason, at present, the state of information support for the management processes of the Armed Forces of Ukraine (Defense Forces) cannot be called satisfactory. Therefore, the implementation of C-shaped ACS (taking into account the experience of the Russian-Ukrainian war) is a necessary condition for the implementation of reliable and sufficient for the implementation of network-centric principles of conducting operations (combat operations) in the prospective structure of the Armed Forces of Ukraine.

Thus, the realization of such a conceptual approach to the implementation of information support (by its main types) in the C-shaped ACS will contribute to increasing the combat capabilities of the troops (forces) of the Armed Forces of Ukraine (Defense Forces) in the modern conditions of conducting military operations.

The materials of the article can be useful for the higher command staff of the Armed Forces of Ukraine (Defence Forces), as well as scientists and researchers in the field of information support and development of the defense sphere of the state.

Keywords: Information Systems; Control Systems; ACS, Network-Centric Warfare.

Introduction

The analysis of the publications shows that today the issue of forming the future outline of the Armed Forces of Ukraine (AF of Ukraine) is being actively researched, taking into account the experience of the leading countries of the world. The content of the concepts of the construction and development of the armed forces of the countries of the world convincingly shows that the priority areas include the improvement of the military (force) control system (Ilyashov, 2009), (Pashchetnyk, 2015), (Zagorka, Koval, Tyurin, Malyuga, Zagorka, 2016). At the same time, the experience of the participation of the armed forces of the leading countries in the operations of the late 20th and early 21st centuries determined the development and implementation of the concept of *Net-Centric Warfare* (*NCW*) as the main trend in the development of the theory and practice of military management (Savin, 2011), (Kondratiev, 2009), (Baulin, Kondratiev, 2009), (Makarenko, Ivanov, 2018), (Oproschenko, 2018), (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020), (Nor, Borokhvostov, Solomytskyi, 2023). These publications claim that a network-centric war is a war in which the achievement of success is ensured on the basis of information superiority over the enemy by means of combining military objects into a single information network (US military doctrine, 2020), (Gavrilov, 2010), (Balakhontsev, Kondratyev, 2011).

The above publications mainly explore the fundamental tasks of building automated control systems (ACS) for the implementation of the concept of network-centric wars. At the same time, they do not pay enough attention to the information support of such systems. Without up-to-date information, any automated system cannot perform its intended functional tasks. At the same time, the information advantage can be achieved by timely information support of the decision-making

process and actions at all levels of the military (force) control system. Therefore, the issue of information support of modern control systems in the military sphere is of the utmost importance.

The purpose of the article is to justify conceptual approaches to determining the directions (ways) of improving the information support of the control system of the Armed Forces of Ukraine based on the experience of building and using information systems for managing the armed forces of the leading countries of the world. In this article, only the main contours of the development of control systems in the conditions of fundamentally new wars of the 21st century are marked.

Presenting the main material. The war of the future is not only a high-tech war, but primarily a "network" war. It requires the unification of all participants in the hostilities, the support of accurate and timely data on the situation on the battlefield in real time to ensure preemptive damage to enemy objects (Makarenko, Ivanov, 2018), (Oproschenko, 2018), (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020).

The reform of the armed forces of the leading countries of the world is carried out, first of all, by introducing new approaches to the management and conduct of hostilities. They are based on the network principle of providing troops (forces) with accurate and timely information, provided by the promising "network-centric" concept (Gatsenko, 2015).

Today, the concept of information has many definitions. For the military sphere, it is reasonable to consider that in general, *information* is processed and understood data, their content, meaning (essence), knowledge or conclusions obtained on their basis, regardless of the form of presentation (Central Department of Metrology and Standardization of the Armed Forces of Ukraine, 2014). At the same time, the value of information is determined by its usefulness and its ability to provide a certain subject with the necessary conditions to achieve the goal.

It should be noted that according to the laws of cybernetics (Wiener, 1968), any control function in systems is implemented exclusively through information. This means that the process of any management, and especially in the military sphere, requires the implementation of a number of information processes that have an impact on all elements of the control mechanism. The set of these information processes is actually united by the information support definition, which permeates the closed loop of management. Its essence consists, on the one hand, in the formation of tasks and their delivery from the control body to the subjects of the system, and on the other hand, in the possibility of the control body receiving feedback to control the management process and adjust the information impact. The above is summarized by the following relevant definitions given in the Military Standard (Central Department of Metrology and Standardization of the Armed Forces of Ukraine, 2014).

Information support (in the military sphere) is a set of measures of military administration bodies of all levels, actions of troops (forces) and other subjects of information activity with the aim of creating (forming) and using in the information space of the military sphere the necessary information resources for the implementation of management processes in the state defense interests.

The information space of the military sphere is a part of the information space of the state: an environment in which information processes and information relations regarding the creation, collection, receipt, storage, use, distribution, security and protection of information (information products, information resources) of a military nature take place.

Integral components of the information environment are information resources, information infrastructure and information technologies, which constitute the essence of the national information potential.

An information resource is data and knowledge, the distinguishing and integral characteristic of which is their pragmatic value, which is determined by practical needs in the interests of solving certain tasks.

Information infrastructure is a set of various information (automated) systems, information resources, telecommunication networks and data transmission channels, means of communication

and control of information flows, as well as organizational and technical structures, mechanisms that ensure their functioning.

Today, it is the level of information potential which is based on the information resource produced by the elements of the information infrastructure, and the possibility of its effective, in particular automated, use, that to a greater extent determines the high efficiency and quality of decision-making. In addition, it also determines the necessary structure and characteristics of control bodies, weapons samples, assessment of their sufficiency level, in general – with a high probability determines the outcome of an armed confrontation.

On the basis of scientific research (Sarychev, 2016), a complete list of information functions, which implement the components of information support of the control system in the military sphere, was formed. Such components should at least include the following main types:

Condition monitoring is a set of activities that implements a continuous process of obtaining information of a military nature based on data of all types of military intelligence, with the aim of assessing and forecasting the development of the operational and tactical situation, as well as highlighting threatening actions in space, air, land, surface, underwater and information spaces.

Information-analytical support is a set of activities that implements the processes of creating information products based on the use of information resources, conducting calculations, modeling situations, analyzing data and information in order to support decision-making by military control bodies.

Organization-administrative support is a set of organizational and administrative measures that are implemented by military control bodies, commanders (supervisors) through document circulation for the purpose of preparing and making informed decisions, communicating tasks to subordinates, organizing execution and control.

Protection of information resources is a set of legal, administrative, organizational, technical and other measures that ensure the preservation and integrity of information (information resources) and the proper order of access to it (them).

Moral-psychological support is a set of measures that are carried out with the aim of forming, maintaining and renewing the moral-combat and psychological qualities, moral-psychological state of troops (forces) in the personnel of military formations at the level necessary for the successful performance of assigned tasks.

Image support is a set of activities carried out to highlight the activities of the Defense Forces, with the aim of forming a positive public opinion in society and at the international level, as well as promoting the growth of the prestige of the military service in the national society and beyond.

Disinformation support is a set of measures to mislead the enemy by means of distracting demonstrative actions, imitation, concealment of one's main actions and dissemination of false information.

Information-psychological influence is a purposeful informational intervention in the consciousness (subconsciousness) of the leadership and personnel of the enemy's troops with the aim of introducing changes in behavior and (or) worldview that undermine their moral-psychological state.

Information-technical impact is a set of actions and attacks that implement purposeful destructive electronic interference in the process of functioning of the enemy's information infrastructure objects.

Radio-electronic protection is a set of measures to guarantee the stability of the operation of radio-electronic components of information means, information systems and other media of information resources in conditions of radio countermeasures by the enemy and mutual electromagnetic influence.

Navigational support is a set of measures aimed at constant and objective acquisition of information by military facilities about their own location in real time for the effective conduct of operations (combat operations) and the use of weapons and military equipment.

Topo-geodetic (geo-informational) support is a set of measures for the preparation and delivery of all levels of topographic and special maps (including electronic ones), photo documents of the area,

as well as astronomical-geodetic and gravimetric data to the military control bodies for the implementation of spatial synchronization in the control of troops (forces) and weapons in the course of performing the tasks set by them.

Hydrometeorological support is a set of measures to collect, analyze and deliver information about the hydrological and meteorological situation to the troops (forces).

The specified types constitute the basic list of components of the complete process of information support of the control system in the military sphere, which implements management functions according to the target purpose.

In the modern era of the "information age" (Digital Age, Computer Age), new information technologies come to the fore. Their implementation in the military sphere is also aimed at increasing the combat capabilities of formations. However, not only due to the improvement of intelligence, fire, maneuverability and other characteristics of individual samples (platforms), but, first of all, due to the availability of better information support and the possibility of shortening the cycle of combat control in operations (battle) (Kondratyev, 2008).

The concept of "network-centric war", or "conducting hostilities in a single information and communication space", considers elements of the armed forces as devices connected to the network. Depending on the choice of network architecture and its type, the means of the network can be military units and subdivisions, ships, aircraft, weapons, control, communications, intelligence, and a combination of both. The capabilities of such combat units are determined not so much by individual characteristics, but by the capabilities of the entire group of networked assets as a whole.

According to specialists' calculations, the automation of the processes of collection, processing, generalization, transmission (reception), use of information can contribute to increasing the combat capabilities of troops (forces) by 15-20% and, at the same time, reduce the time spent by military control bodies of all levels by 50% on making decisions and bringing tasks to subordinates (Frolov, 2012).

Ensuring comprehensive integration, increasing the level of interaction due to the implementation of the principles of new network-centric concepts and the integration of control, communication, intelligence and defeat systems is becoming an increasingly urgent and priority direction of reforming the armed forces of most countries of the world.

Measures for the implementation of network-centric concepts are mainly carried out in three key areas (Snitsarenko, Sarychev, Tkachenko, Zubkov, 2021):

development of information acquisition, processing, analysis and distribution systems using unified tools for its processing and transmission formats;

optimization of organizational structures of control bodies, information processing and analysis, personnel training and review of doctrinal documents;

deployment of modern communication and data transmission systems.

It is known that NATO implements the concept of "Complex network capabilities" (NATO *Network Enabled Capabilities - NNEC*), which is intended to organize the interaction of high-tech formations of national armed forces in armed conflicts (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020), (Molitvin, 2008), (Adams, Ben-Ari, Logsdon, Williamson, 2004). Its implementation will enable effective information support of operations of the entire possible spectrum, starting from peacekeeping operations to establish peace to large-scale combat operations of high intensity. At the same time, NATO military experts emphasize that NNEC is not only the integration of control and communication systems, but also an opportunity to increase the level of information interaction of all participants in the operation (combat operations), including weapons, bodies and logistical points software.

In the USA, the essence of the concept of "network-centric war", "conducting hostilities in a single information and communication space", based on the experience of using troops (forces) in modern conflicts, has acquired the greatest practical content in the unified system of intelligence and

information support and combat control of the US Armed Forces - "*Network Centric Warfare*" (*NCW*) (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020), (Molitvin, 2008), (Adams, Ben-Ari, Logsdon, Williamson, 2004), (Thomas, 2005).

Great Britain (*Network Enabled Capability*), France (*Guerre Infocentre*), Germany (*Infanterist der Zukunft*) and together with the Netherlands ("*Tactical Edge Networking*") (Adams, Ben-Ari, Logsdon, Williamson, 2004), Australia (*Network Centric Warfare*) (Adams, Ben-Ari, Logsdon, Williamson, 2004), China have similar systems (*Integrated Network-Electronic Warfare - INEW*) (Thomas, 2005), and Israel considers the implementation of information technologies as an integral and mandatory attribute of modern and future operations (Adams, Ben-Ari, Logsdon, Williamson, 2004).

It is obvious that the main principles of the implementation of measures for the wide introduction of information components in the military sphere within the framework of the network-centric operations concept are:

ensuring real information unity of groups;

application of open architecture and modular construction of modern systems and complexes of armed struggle;

implementation of vertical and horizontal information integration and interaction of all participants of the operation (combat operations).

Analysts claim (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020) that the wars of the next generation are, above all, wars of intelligence, where having the necessary information about the enemy is the key to success in such wars. In modern conditions, in the leading countries of the world, a steady trend can be seen to emphasize the acquisition and integration of various information about the state of political, economic, social, military, scientific, scientific and technical, informational, legal, organizational, and other relations between states, groups of states and in the world as a whole.

Therefore, such a type of information support as enemy monitoring, which is based on the process of comprehensive intelligence, is dominant in the general information support system of troops (forces). At the same time, any network-centric system cannot be used as intended without up-to-date information in real time. Depending on the level, the network-centric system, based on the presence of useful, reliable, complete, timely intelligence information, is able to visually display the situation, assess the terrain, the state of the enemy and its troops (forces), and simulate the development of combat operations. At the same time, the system is able to produce recommendations, options for solutions, drafts of combat documents, deliver tasks to subordinate control points and the ability to control all information processes.

Reliability is the ability of information to reflect real objects (processes, phenomena) with the required accuracy within a certain level of probability of the case being displayed.

Sufficiency (completeness) is the minimal, but sufficient composition of the information product for making a decision.

Timeliness of information means that it is exactly what is needed at the moment, essential, important at this time.

The need (usefulness) of information is determined in view of the tasks that can be solved with its help.

Along with the advantages of the network-centric concept of conducting hostilities, a number of problems regarding its implementation have been identified. In particular, the issue of rational distribution and processing of large volumes of information received by consumers is acute. For a better understanding of this problem, we consider it expedient to dwell on the distribution of classes of network-centric systems depending on the degree of automation of controlled processes and information flows that circulate in them.

The experience of development, implementation and operation of network-centric systems in

the USA shows (Zagorka, Pavlikovsky, Koretskyi, Kyrychenko, Zagorka, 2020), (American ACS) that modern automated control systems, which are informational in nature, are divided into several classes. According to the functions performed by the systems, command, control, communications, computers (informatization), general intelligence, surveillance, real-time intelligence (*Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance*) are distinguished.

At the same time, the systems differ in the degree of automation of controlled processes in accordance with this classification. Each system belongs to a specific class according to the level of automation of management functions. So, if the control system in the automated mode has only two functions, for example, command and control (*Command and Control*), then it will correspond to the "CC" class (C2). If four functions are automated in the system - command, control, communication, communication (*Command, Control, Communications, Computers*), then such a system is classified as "CCCC" (C4). At the same time, functions starting with the letter "C" are used as basic, and others are additional.

From the point of view of automated management functions (tasks), the control system, which contains more letters "C" in its abbreviation, is more perfect. Thus, the C2SR (*Command, Control, Surveillance, Reconnaissance*) class system will be inferior to the C4 class system in terms of the range of tasks used in automated mode.

Systems in which *Command and Control* (C2) functions are automated solve the following tasks:

display and transmission of combat tasks to subordinate control bodies (control objects) in a formalized text and graphic format using a single network;

determination of the positions of own control objects and notification of their control bodies and neighbors about their location with display on electronic maps;

display on electronic maps and data exchange about detected enemy objects, infrastructure elements on the battlefield;

selection and calculation of traffic routes based on known data about the road network and display of the route traveled.

The C2 system only allows the commander to quickly convey the decision to subordinates and control the progress of its implementation. At the same time, the function of assessing the situation and making a decision is fully dependent on the person. Some systems belonging to the C2 class can perform mutual recognition of objects located in the system according to the principle of "friends-or-foes". In addition, they can also perform target identification and provide automatic target designations to the means of fire damage included in the system. Control systems in which such functions are automated have additional letters "SR" (*Surveillance, Reconnaissance*) and are designated as C2SR (or C2+). At the same time, computers used in C2 class systems are considered only as means of primary processing and display of information. Although C2 systems include personal computers, they do not have the word "*Computers*" and the corresponding letter in the abbreviation of their class. In general, the C2-class system only helps commanders communicate the task to subordinates, collect and display current information about the enemy and the state of their control objects. At the same time, there is still no talk of intellectual support for decision-making and the development of options for combat decisions and their simulation.

Such tasks as the automatic organization of communication and local computer networks are already a distinction of the system, which has the abbreviation of the word *Communications* (C3) in the name of its class. The tactical link systems in service with foreign countries belong to the C2 or C2+ class and differ from each other only by a small expansion of the spectrum of the solved tasks. At the same time, all systems of tactical purpose do not even reach the C3 class in principle.

The presence of the fourth letter "C" (*Computers*) and the letter "I" (*Intelligence*) in the abbreviation of the system class means, firstly, full automatic processing of the data obtained during the implementation of the first two "C" - *Command and Control*, secondly, on the basis of the primary

data processing the development of a variant of the commander's situational decision and its presentation in the most convenient form for a person, respectively.

C4 class systems (in addition to performing the functions implemented in C2 and C3 class systems) must be able to solve the following tasks:

full automation of information collection and processing;

informational support for the development of decision options by the commander (availability of "Sketch in the decision" type programs - the intention of the decision);

simulation of combat operations based on selected options for performing combat tasks with a graphic display of their progress and results on electronic maps, including using means of a three-dimensional display of the battlefield;

informational support for the development of planning documents ("Sketch in the plan" program, which transforms graphic and audio materials into planning documents;

informational support for decision-making during a combat mission (updating assessments and conclusions based on information received during combat).

The fundamental difference between the C4I class systems and the C2 class is a higher degree of automation of information and control tasks.

In the armed forces of even technologically developed countries, C4I and C4SR class systems belong to the operational or operational-strategic link systems according to the level of control. According to military experts (Adams, Ben-Ari, Logsdon, Williamson, 2004), the main obstacles to the development of tactical link systems from class C2 to class C3 and C4 are:

the absence of mathematically correct algorithms for evaluating the actions of the troops at the tactical level, taking into account the huge variety of methods and techniques used by them to perform combat tasks;

the difficulty of creating an automated system for collecting and evaluating data on the tactical situation, given the wide variety of its parameters and the rapidity of changes (compared to the operational control chain);

the need to process a large amount of data per unit of time, the volume of which currently exceeds the capabilities of the machine support used in the tactical control chain;

the difficulty of creating communication networks and reliable local networks (data transmission systems) between a large number of highly mobile control objects.

At present, significant development of C+ class systems in the interests of implementing the concept of network-centric operations has been received in the USA.

The most famous of all the existing systems of the tactical link is the American system of the "C2SR" class FBCB2 - Force XXI Battle Command Brigade and Below ("*System of managing the brigade and subordinate units in the battle (battle) of the twenty-first century*") - one of the main components of the automated control system US ground forces ABCS (*Army Battle Command System*), which played a key role in the operations in Iraq and Afghanistan (Thomas, 2005).

During the last 30 years, the military-political leadership of Ukraine, realizing the need for the development of military control systems, paid attention to the process of creating automated military control systems of various levels. Thus, in order to solve the problems of the management of the Armed Forces of Ukraine as a whole, the concept of the functioning and development of such systems was developed, starting with the Unified Automated Control System of the Armed Forces of Ukraine (UAMS of the Armed Forces of Ukraine), which was supposed to be integrated with other state ACS. Within the framework of the creation of the UAMS of the Armed Forces of Ukraine, the development of special and other ACS of various levels of military control bodies (tactical, operational, operational-strategic) was foreseen: ACS of the "Dnipro", "Karpaty", "Oreanda", "Nika", "Borsuk", "Space" and others. At the same time, special emphasis was placed on the introduction of modern information technologies in the management of troops, military equipment and weapons during the creation of the UAMS of the Armed Forces of Ukraine.

During this time, more than 100 scientific research works and more than 40 research and design works were carried out on the subject of UAMS of the Armed Forces of Ukraine. The experience of carrying out such works has proven their low efficiency. Thus, only about 20% of works reached the stage of production of prototypes, experimental operation and state tests. And about 80% of them did not find their implementation, so they were suspended at various stages of work: sketch and technical design (40%), development of design documentation (40%) (Pastukhov). According to experts, the imperfection of research works was influenced by many problems of a general nature. One of the main ones is the lack of adequate experience in the development of complex, multi-branched automated systems for military purposes in the majority of Ukrainian development organizations.

Nevertheless, today the main idea of the creation of the UAMS of the Armed Forces of Ukraine – the automation of the necessary types of activities of the military control bodies – has already been implemented in general. During this time, separate components of ACS of various levels were developed (information and analytical systems for supporting the control of the organizational and personnel structure and personnel; monitoring and planning of defense resources; modeling of prospective military formations and organizational measures for the implementation of directives; creation and development of weapons and military equipment) and they actually function in a protected mode at the facilities of the Armed Forces of Ukraine.

However, it should be noted that at this stage of the development of the Armed Forces of Ukraine, the state of automation of management processes cannot be called satisfactory. According to (Gatsenko, 2015), the automation of the activities of military administration bodies is only 10-30% of the needs. The available means do not make up complete systems, the existing information and calculation resources meet the needs of control bodies by only 12-15%. At the same time, the level of informatization of the control systems of state defense entities compared to the armed forces of the leading countries of the world is 2-2.5%. At the same time, the presence of large screens with icons of different colors on the electronic topographic map at the control point is not a sign of a high level of automation of the troop control system. In addition, before the start of the armed aggression, despite a number of attempts, the construction of an automated combat control system for troops (forces, weapons) was not completed in the Armed Forces of Ukraine (Galagan, Polishko, Bondarchuk, 2019). It turned out that such a task became too difficult.

At the same time, in this context, the top military leadership of Ukraine defined a vision for the development of the military (force) control system (Mil, 2020): "... It is necessary to build a reliable system of communication, automation, intelligence and surveillance (C4ISR) in the Armed Forces of Ukraine, resistant to external influences, protected from means of electronic warfare (EW), which will have alternative communication channels. The means of communication must be combined with the means of communication of the partner countries. It is necessary to create an information network in the interests of the security and defense sector of the state, which will ensure the acquisition of information capabilities for receiving, processing, storing, transmitting, controlling and providing information at the request of commanders and headquarters (tactical, operational, strategic levels) of the United forces".

With the beginning of the armed aggression of the Russian Federation against Ukraine in 2014, the highest military and political leadership of Ukraine paid special attention to the issue of the development of the ACS by troops (forces, weapons). The result of this, already after the full-scale invasion of the armed forces of the Russian Federation into Ukraine, is the adoption by the Armed Forces of Ukraine in 2022 of the "Dzvin-AS" ACS - a highly integrated automated combat control system of troops (forces) of the strategic, operational and partially tactical level. It is believed that it enables (Mil):

to generate combat control documents in semi-automatic and automatic modes;

to receive available intelligence on the enemy's troops, their current and prospective support;

to create and monitor cartographic information;

to receive comprehensive data on own troops;

to carry out calculations of the ratio of forces and means, the optimality of their use in various scenarios.

In addition, with the start of the hostilities in 2014 in the East of Ukraine, the combat control system of the "Kropyva" ("Nettle") tactical unit was successfully operational in a short period of time. This is a battle-tested system designed to automate individual control tasks at the level of a battalion - company - platoon - a separate unit of equipment (cannon). Currently, the "Kropyva" ACS can be used by various units of the ground forces: artillery, infantry, tank units, joint military intelligence, air defense units of the Graund Forses, sapper units, etc. At the same time, a protected Delta situational awareness information system was implemented for the military control bodies of the Ukrainian Armed Forces. It allows collection, processing and display of the situation in real time, and also provides support for decision-making by the commander.

In our opinion, making an attempt to immediately create a C4ISR system is a task that does not correspond to the resource capabilities of the state. As an example, a special NCOIC consortium (96 companies from 32 countries, 26 of which are NATO members) was formed to optimize the implementation of the NATO concept *Network Enabled Capabilities* (NNEC). It is intended to ensure the unity of information processing protocols and the coordination of industry efforts in fulfilling the requirements for achieving the necessary level of interaction and integration of prospective systems in order to ensure the implementation of network-centric principles of military formation management.

At the same time, according to the conclusions of American analysts, none of the European allies is likely to be able to create a fully networked army in the near future. The biggest challenge for European investment in C4ISR is the general limitations of defense budgets, not the lack of adequate technology (Adams, Ben-Ari, Logsdon, Williamson, 2004).

In this matter, it is advisable to borrow the experience of China as well. Its military experts realize that they will not be able to create a network-centric system adequate to the American one, despite the presence of a significant military budget, in the near future. Therefore, the bet is placed on the creation of forces, systems and means that provide an asymmetric effect on the enemy. It means the fire and electronic defeat of elements of information structures (command posts, communication nodes, orbital grouping of intelligence and control satellites, etc.) (Thomas, 2005).

In view of the above, it is advisable to start the development of the C-shaped system in Ukraine from the C2+ level, with its subsequent evolutionary increase to C3 and higher, based on the results of tests, operational experience and resource capabilities. At the same time, it should be remembered that information support of control bodies is a priority task - without information, any control system works inefficiently. Only with the availability of relevant information the system can perform functional tasks as intended.

In our opinion, the level of information support of troops (forces) in the interests of reliable operational management should ensure:

for the tactical level (platoon, company, battalion, brigade) - using the C2+ type system, solving the following tasks:

exchange of information about the position, detected objects of the enemy and their actions in an automated mode in real time with display on electronic maps from top to bottom and from bottom to top;

determination of the positions of own control objects and notification of their control bodies and neighbors about their location with display on electronic maps;

transmission of combat tasks to subordinates in a formalized text and graphic format and control of their progress;

mutual recognition of objects located in the system according to the principle of "friends-or-foes";

identification of targets and providing in an automated mode targeting of means of fire damage;

for operational and strategic levels - using a system of the C3 type (in the future - C4 with applications), which must be able to solve the following tasks:

full automation of the collection and processing of information in a real (close to real) time scale about the enemy, the position and condition of own troops (forces);

informational support for the development of decision options for the use of the Armed Forces, troops (forces), formations and military units;

simulation of operations (combat operations) according to the selected options with a graphic display of their progress and results on electronic maps, including using three-dimensional display tools;

information support for the development of planning documents, conversion of graphic and audio materials into planning documents;

informational support for clarifying decisions during operations (combat operations).

Results

Thus, the experience of the world's leading countries convincingly shows that when implementing a network-centric concept for the control systems of the Armed Forces of Ukraine, the main attention should be focused on the issues of collection, processing, analysis, identification and security of information to support decision-making by managers at all levels. At the same time, the support of timely, up-to-date, reliable (relevant) information for military assignment control systems becomes the main task in the general process of information support of the Armed Forces of Ukraine.

The conducted analysis shows that the activities related to the construction and use of information systems for the control of the armed forces of the leading countries of the world, first of all, the experience of the NATO member states, causes an urgent need to further search for approaches to the improvement of the information support of the control systems of Ukrainian Armed Forces. The network war can be won only by network means, adapting to one's own conditions and effective technologies.

Conclusion

1. The concept of network-centric wars is a system of views on the conduct of hostilities and military-technical support in the conditions of full computerization of forces and means of armed struggle. At the same time, the interoperability of automated intelligence systems, control of troops and weapons, as well as ensuring sustainable interaction between them are considered as key components. They are necessary to achieve an informational advantage and, as a result, an advantage in decision-making in order to decisively anticipate the enemy throughout the entire cycle of combat control (according to the principle: "the first to see - the first to shoot").

2. Information support of network structures becomes the main and necessary condition for the effective functioning of control systems. In order to create such a structure and a single information space for users in a real (close to real) time scale, it is necessary to combine all forces and means of obtaining and generating information by automated systems.

3. Proper and timely information support of military control systems is a necessary condition for the implementation of network-centric principles of combat operations. It can be implemented in the Armed Forces of Ukraine by introducing a C-shaped automated control system through its evolutionary development, starting with the construction of a C2+ class system. In this case, taking into account the great experience gained by the US armed forces in the development of informatization of the military sphere, the implementation of the theory of network-centric operations into practice, as well as the fact that Ukraine is in a state of war, we consider it appropriate:

to take as an example for implementation in the Armed Forces of Ukraine the existing American automated control system of the tactical link of the C2SR class - Force XXI Battle Command Brigade and Below (FBCB2) or another similar prospective automated control system of foreign production;

at the first stage, as an urgent measure, consider the issue of obtaining (purchasing) a brigade set of an automated tactical link control system for testing in the conditions of conducting real combat operations to determine the feasibility of further implementation in the Ukrainian Armed Forces;

in the case of obtaining positive results, raise the issue of gradually equipping military units and units of the Ground Forces of the Ukrainian Armed Forces with prospective automated tactical control systems of foreign production;

at the same time, to direct the acquired experience to the development of domestic (taking into account the capabilities of science and industry of Ukraine) C-shaped prospective adaptive control systems of various levels, compatible with the automated control systems of the armed forces of NATO member countries.

Recommendations

It is advisable to direct further research to the development of information support of the Ukrainian Armed Forces by more clearly defining the composition, structure and volume of information flows. They circulate in control systems, substantiating the functional components of the information process in such systems, which will allow optimizing the list of tasks that must be performed at each stage of the control cycle.

The materials of the article can be useful for the higher command staff of the Ukrainian Armed Forces (Defence Forces), as well as scientists and researchers in the field of information support and development of the defense sphere of the state.

References

1. Ilyashov, O. A. Trends in the development of armed struggle in the wars of the fourth - sixth generations. (2009). *Science and defense*. No. 3. P.43–48.
2. Pashchetnyk, O. D. Analysis of global trends in the development of automated systems for the management of troops and weapons. (2015). *Science and technology of the Air Force of the Armed Forces of Ukraine*. No. 2 (19). P.64–68.
3. Peculiarities and principles of building a network-centric management system of a group of troops (forces). (2016). O.M. Zagorka, V.V. Koval, V.V. Tyurin, V.G. Malyuga, I.O. Zagorka. *Collection of Scientific Papers of Kharkiv Air Force University*. Issue 3(48). P. 7–11.
4. Savin, L. V. Network-centric and network warfare. Introduction to the concept. (2011). Moskov: Eurasian Movement. 130 p. Access mode: https://www.geopolitica.ru/sites/default/files/ ncw.pdf.
5. Kondratiev, A. Implementation of the concept of "Network-centric warfare" in the US Air Force. (2009). *Foreign Military Review*. No. 5. P.44–49. Access mode: http://pentagonus.ru/publ/ 24-1-0-1159.
6. Baulin, V., Kondratiev, A. Implementation of the concept of "Network-centric warfare" in the US Navy. (2009). *Foreign Military Review*. No. 6. P. 61-67. Access mode: http://pentagonus.ru/publ/26-1-0-811.
7. Makarenko, S. I., Ivanov, M. S. *Network-centric warfare – principles, technologies, examples and prospects*. (2018). SPb: High technology, 898 p.
8. Oproschenko, Yu. O. Network-centric war: main features, peculiarities and principles of conduct. (2018). *Social and political studies*. Scientific almanac. Works of young scientists. No. 2. P. 7-11.
9. Theoretical foundations of managing a group of troops (forces) in modern conditions of armed struggle (2020). Monograph. Zagorka, O. M., Pavlikovsky, A. K., Koretskyi, A. A., Kyrychenko, S. O., Zagorka, I. O. In general ed. Russian, I. S. Kyiv: NUOU named after Ivan Chernyakhovsky. 248 p.
10. Nor, P. I., Borokhvostov I. V., Solomytskyi O. I. The main trends in the development of forms and methods of armed struggle. *Science and defense*. 2023. No. 1. P. 20-27.
11. US military doctrine "Joint Vision 2020". (2020). Access mode: http://pentagonus.ru/doc/ JV2020.pdf.

12. Gavrilov, A. Automated system for collecting, processing and distributing intelligence information of the US Army DCGS-A. (2010). *Foreign Military Review*. No. 7. P.32–40. Access mode: http://pentagonus.ru/publ/122-1-0-1596.
13. Balakhontsev, Y., Kondratyev, A. The influence of the "network-centric war" concept on the effectiveness of intelligence support for the US Armed Forces. (2011). *Foreign Military Review*. No. 2. P.14–20.
14. Gatsenko, S. S. Analysis could be used for military management systems and their improvements. (2015). *Collection of scientific works of the CVSD NUOU*. No. 2. P. 85–90.
15. Military standard VST 01.004.004 – 2014 (01) "Information security of the state in the military sphere. Terms and meaning" (2014). [confirmed by the order of the head of the Central Department of Metrology and Standardization of the Armed Forces of Ukraine - the chief metrologist of the Armed Forces of Ukraine dated 02/27/2014. No. 1].
16. Wiener, N. *Cybernetics or control and communication in animals and machines*. (1968). Moskov. Soviet Radio. 328 p.
17. Sarychev, Yu. O. Analysis of approaches to determining the modern role and place of information support in the state administration system. (2016). *Bulletin of the NADU under the President of Ukraine*. In general ed. Kovbasyuk, Yu. V. Issue 3 (82). P. 138–143.
18. Sarychev, Yu. O. Theoretical approach to information support in the system of state administration in the military sphere. (2016). *Bulletin of the NADU under the President of Ukraine* (Series "State Administration"). In general ed. Sausage, Yu. V. Issue 4 (83). P.153–160.
19. Kondratyev, A. E. General characteristics of network architectures used in the implementation of promising network-centric concepts of leading foreign countries. (2008). *Military Thought*. No. 12. P. 63–73.
20. Frolov, V. S. Structural and logical scheme of the Unified automated control system of the Armed Forces of Ukraine. (2012). *Science and defense*. No. 1. P. 15.
21. Snitsarenko, P. M., Sarychev, Yu. O., Tkachenko, V. A., Zubkov, V. P. The experience of the armed forces of the leading countries of the world in the interests of improving the information support of the Armed Forces of Ukraine. (2021). *Collection of Scientific Papers of the TsVSD NUOU named after I. Chernyakhovskyi*. No. 2 (72). P.40-50.
22. Molitvin, A. On the implementation of the concept of a single NATO information space. (2008). *Foreign Military Review*. No. 1. P. 23–27. http://pentagonus.ru/publ/3-1-0-565.
23. Adams, G., Ben-Ari, G., Logsdon, J., Williamson, R. (2004). European C4ISR Capabilities and Transatlantic Interoperability. The George Washington University.
24. Thomas, T. L. (2005). Chinese and American network warfare. *Joint Force Quarterly*. July.
25. American ACS troops FBCB2. Access mode: http://dragon-first-ru.livejournal.com/33339.html; http://defense-update.com.
26. Pastukhov, A. ACS of the Armed Forces of Ukraine. Technologies. Access mode: https://mil.in.ua/uk/d0-b0-d1-81-d1-83-d0-b7-d0-b1-d1-80-d0-be-d0-b9-d0-bd-d0-b8-d1-85-d1-81-d0-b8-d0-bb/#google_vignette.
27. Galagan, V. I., Polishko, S. V., Bondarchuk, S. V. Proposals for improving the process of introducing information systems of foreign production into the activities of the Armed Forces of Ukraine. (2019). *Collection of Scientific Papers of the TsVSD NUOU named after I. Chernyakhovskyi*. No. 2. P. 62–68.
28. The Vision of the General Staff of the Armed Forces of Ukraine regarding the development of the Armed Forces of Ukraine for the next 10 years. (2020). https://www.mil.gov.ua/news/2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi – 10 - rokiv.
29. The "Dzvin-AS" management system has been adopted by Ukraine. Access mode: https://mil.in.ua/uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.07

An access to innovation program to enhance the technological capabilities of the armed forces

Marie-Pierre Raymond
MEng, CD (LCol Ret'd)
Defence Research & Development Canada (DRDC)
Ottawa, Ontario, Canada
e-mail: marie-pierre.raymond@forces.gc.ca

Eric Fournier
e-mail: eric.fournier@forces.gc.ca

Abstract. As part of "Strong, Secure, Engaged: Canada's Defence Policy" (Department of National Defence (2017) Strong, Secure, Engaged) released in 2017, the Canadian Department of National Defence (DND) announced the creation and implementation of an access to innovation program to be called the "Innovation for Defence Excellence and Security (IDEaS)" Program. The IDEaS Program was introduced to support, increase, and sustain science and technology (S&T) community capacity external to DND that can generate new ideas and formulate solutions to Canada's current and future defence and security innovation challenges. This paper will explore the design of this new business model through the delivery of the first proof of concept to have gone through the whole IDEaS cycle, in order to showcase the validity of this concept and processes. It also demonstrates that IDEaS has allowed a closer relationship with innovators and firms that had never worked with the defence industry, as well as the identification of novel solutions to a host of problems/challenges facing defence and security.

Keywords: technological capabilities, IDEaS, innovations, SOAR, defence capability.

Introduction

Accessing innovative solutions to support defence and security needs is crucial for Canada to stay technologically advanced, enhancing security capabilities, and addressing the dynamic threats landscape. It is essential to stimulates the development of cutting-edge solutions, promote strategic advancements, and ensure Canada maintains a competitive edge in the ever-changing landscape of defence requirements and security needs. In response to this complex environment, Canada launched the Innovation for Defence Excellence & Security (IDEaS) program, with the goal of augmenting the Department of National Defence (DND) and the Canadian Armed Forces (CAF) capabilities. Several allied nations have initiated comparable innovation programs to encourage non-traditional defence innovators to actively engage and provide their technologies for defence applications. These programs, such as the Defence Innovation Unit (DIU) and SOFWERX in the US, the Defence and Security Accelerator (DASA) in the UK, and the Defence Innovation Hub in Australia, use a very similar general business model than the IDEaS program but with various specificities in their applications. The IDEaS program represents an investment in access to Canadians innovators to enable Canada's military to tap into the nation talent pool more efficiently. IDEaS is built on three fundamental pillars: recruiting innovators (connect), supporting development (develop), and maturing innovative solutions toward adoption (evaluate).

IDEaS was announced in the Fall of 2017 in Strong, Secure, Engaged (SSE), Canada's defence policy. The program officially launched on April 9th, 2018. This innovation program has been given $1.6B CAD over 20 years to deliver on its mandate and advance defence capabilities. The goal is to continuously tap Canadian innovators for their solutions through various calls for proposals

launched on a regular basis. IDEaS is for all Canadian innovators, from defence primes to academia, small and medium sized enterprises to not-for-profits, municipal / provincial / territorial entities to individuals.

Program design

This novel program acts as a facilitator between the DND/CAF capability requirements and the Canadian innovation ecosystem. Any organization within DND/CAF can generate and submit a priority/challenge to the IDEaS team, from the Army to the Air Force, to Space, to Cyber and all the other organizations of the department. Following a prioritization of the DND/CAF priorities received by the program (a prioritization process is required as too many priorities are received from DND/CAF), the IDEaS team turns each priority into a challenge to be released to the innovation community.

The program is intended to help foster solutions at any stage of development that have potential defence and security focus and align with DND/CAF priorities. From early research and development to prototyping and testing novel concepts generated by innovators, the program exists to advance technology. DND will access the extraordinary talent and ingenuity of innovators across Canada, including non-traditional players, seeking to leverage and integrate their expertise. Innovators, in turn, will gain DND's support through funding and guidance to help create capability and capacity for defence and security.

Each challenge released by IDEaS represents a genuine and current need from a number of Canadian defence and security stakeholders. Challenges are written with broad language intentionally to encourage a higher volume of submissions, as it is expected that this will lead to the discovery of novel and unexpected proposals. It should be noted that since the launch of the program in April 2018, the program has addressed more than 75 challenging problems spanning various defence and security domains, including electronic warfare, counter-UAS, communications in denied environments, ISR, human performance, cybersecurity, transition from military to civilian life, as well as quantum technologies, artificial intelligence based-technologies and many more.

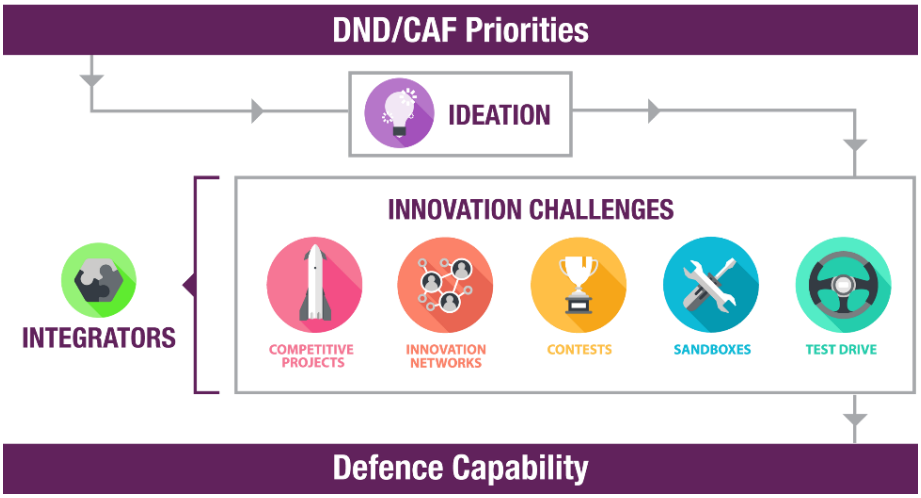


Figure 1: IDEaS Elements that enable the search of new capabilities for DND/CAF

IDEaS Elements

IDEaS leverage 5 different elements to access innovation depending on the technical readiness level of the solution and the types of outcomes sought by the DND/CAF partner.

Competitive Projects – This element was the first one developed under the program, and it

is still the work horse of the program: more than 75% of all the challenges launched by IDEaS so far have been with this tool. The Competitive Projects element funds projects fast. It advances promising technology quickly through a phased approach, which can quickly move technology ahead. Projects that show promise are considered for additional phases of funding.

Contests – Contests are a competitive means of finding innovative solutions and awarding prizes to the best solutions derived from the innovation community. Whether it is a hackathon, a pitch event in front of military experts, or an amazing race, Contests will bring innovators face-to-face with the competition. Depending on the challenge, Contests could entertain solutions at various Technology Readiness Levels, but it is expected that most of the actual events are going to be directed at higher Technological Readiness Level (TRL) (NASA (2023) Technology Readiness Levels) solutions.

Innovation Networks – Innovation Networks are an opportunity to create new networks (or support existing networks) of understanding, stimulate collaboration and allow for the free flow of ideas critical to innovation. They usually occur at lower TRL level, so to allow fully creative solutions to be generated by the participants and support basic and applied research, analysis, technology development and knowledge transfer leading to innovative solutions.

Sandboxes – A Sandbox is an opportunity for innovators to test and demonstrate their prototype solutions to National Defence military users and science experts for a specific IDEaS advertised challenge. The IDEaS team also provides on-site military and science experts, as well as other government safety and security potential users, to give innovators observational feedback on their solutions.

Test Drive – Test Drives takes an innovative solution through the final stage of the innovation journey towards commercialization. The IDEaS Team acquires a solution so that DND/CAF can assess the readiness of the product in a real-world environment for a military audience. Innovators will receive feedback on their technology following the testing.

In addition to these 5 "access" elements, another very important element for the innovator community is called "**Integrators**". Although not directly linked to the call for proposals process, like the previous five elements, it is really an enabler for the innovators. This element has been developed to provide constant support and oversight to the innovators, by providing scientific and operational experts for every challenge launched. These experts come from DRDC and DND/CAF and are experts in the specific domains of each challenge. Their role is to provide guidance to the innovators, without orienting their work towards specific solutions as the role of the program is to allow innovators to develop their own novel and innovative solutions.

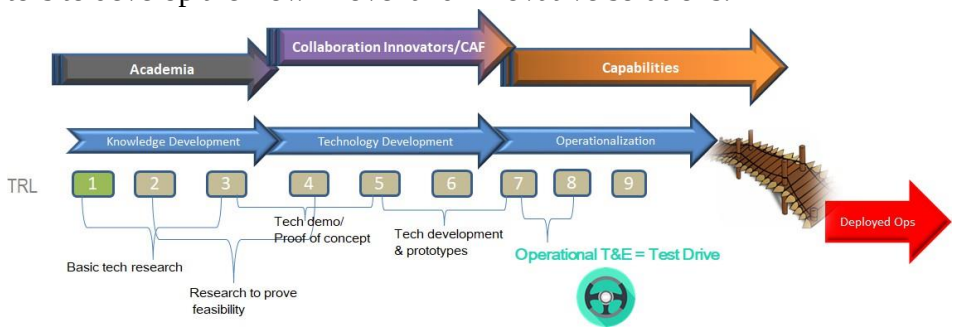


Figure 2. IDEaS innovation pipeline to transform innovation into new capabilities for DND/CAF.

Finally, IDEaS innovation champion, called **Challenge Managers**, are assigned to every challenge launched by the program. These defence scientists are responsible for organizing and

overseeing CAF innovation challenges as they move through the IDEaS innovation pipeline. Their role is to create an environment conducive to innovation supporting the innovators and the CAF stakeholder. They provide guidance, support, and expertise to individuals and teams.

IDEaS PROOF OF CONCEPT

In April 2018, the IDEaS program, and members of the CAF Director General Information Capabilities Force Development (DGICFD) organization collaborated on one of the first challenges launched by the program. They worked on the formulation of the challenge statement of a cybersecurity hard problem that was titled "**Cyber Attribution for the Defence of Canada**".

A. Challenge Development

The Challenge scoping was done with subject matter experts from the organization that submitted the Challenge and defence scientists supporting the organization. It was a collaborative endeavor aimed at defining and refining the parameters, objectives and boundaries of the challenge/hard problem that needed to be addressed. The process involved brainstorming, discussion, analysis to ensure that the challenge was well-defined, aligned with the goals of the organization and of course actionable by the innovator. "Attribution" is one of the most challenging problems in cyberspace. The decentralized, dynamic, and open architecture of the internet enables a perpetrator to easily hide his or her tracks and operate with varying degrees of anonymity.

Following the challenge development process, the Challenge Statement was written as:

The Department of National Defence (DND) is looking for innovative approaches to access, interpret, and compare all available evidence (e.g., technical, all-source intelligence) on how current cyberspace activities get attributed. This will assist in assessing the current cyberspace environment to improve methods on how to obtain secure cyberspace attribution in a timely manner.

The desired outcome of this research effort is to demonstrate methodological approaches and confidence metrics as well as identify challenges and issues (for e.g., technical, regulatory, etc.) with cyber activity attribution that would advance shared understanding of cyberspace and promote national cybersecurity.

B. Calls for Proposals.

An innovation call for proposals (CFP) was the next steps in the process. It was conducted through a structured process to solicit ideas and solutions from Canadian innovators. Following the reception of the proposals, a review, evaluation, and selection process was completed to identify the best proposals for funding. Criteria such as Merit, Novel & Innovation, Impact, Feasibility, Operational Investment and Advancement of the solution were used throughout this process. A total of 24 proposals were received for this CFP, which allowed 7 of these to be selected for the initial phase of funding under Competitive Projects. This original phase of funding has for objectives to establish the merit, innovativeness, and impact of the solutions to address the specific defence and security challenge stated above.

C. Progress through Competitive Projects

Moving along the IDEaS process, one proposal (one out of the 7 chosen for the first phase of funding) was selected for the next phase of funding – only one proposal was selected by the Stakeholders to move forward and receive further funding, and it was the proposal from Sapper Labs (a small & medium enterprise). The solution was to address both strategic issues and next-generation operational solutions. Sapper Labs was proposing to build a next-generation cyber threat hunting system with accelerated detection, attribution and active cyber defence through automated playbooks, Security Orchestration, Automation and Response (SOAR) on forward deployed networks in conflict zones. It offered an innovative way to hunt down bad actors and confidently assign attribution for their actions which was never done before. It was therefore selected to continue its development under the second phase of funding of Competitive Projects.

D. Test Drive

After successfully delivering under the Competitive Projects development phase, Sapper Labs were granted a $7.5M CAD contract for the program's first "**Test Drive''**, the last component of the IDEaS innovation pipeline. In using the funding received from the Competitive Projects, Sapper Labs were able to develop a cyberprotection platform capable of identifying the perpetrators of sophisticated cyber threats. Therefore, the objective of the Test Drive was to validate their cyber attribution capability in a DND/CAF operational setting to accelerate the detection of advanced threats against Canadian assets and led to the development of the Canadian Active Cyber Defence Platform (CACDP) tool to the CAF. The Test Drive in CAF operations lasted 18 months and was broken-down into four phases:

Phase 1 – Initialization and Implementation of the CACDP; Phase 2 – Systems Integration, Tuning and Training analysts;

Phase 3 – Conduct of Cyber and Intelligence Operations and Testing; and Phase 4 – Cognitive Warfare Proof-of-Concept.

Operationalizing the designs and methodologies in this project was critical to achieve the cyber objectives of the Strong, Secure, and Engaged Canadian Defence Policy. During the Test Drive, the following activities were planned to be performed on an operational network or forward-deployed deception network at scale:

- Automate/accelerate attribution of advanced persistent threats and launching of active defence (using AI/ML);
- Integrate/fuse cyber threat intelligence (CTI), Open Source Intelligence (OSINT) and Commercial Sourced Intelligence with real time network sensing to support attribution; and
- Orchestrate threat hunting, intelligence production and active cyber defence. Development of targeting packages and demonstrating the ability to take action based upon playbooks.

Sapper labs accommodated a substantial number of feature requests from the operators during the live operations part of the experiment. Innovator flexibility was critical to address end-users evolving needs as the Test Drive progressed and the real-time threats evolved. At the same time, Sapper Labs, being the first innovator to reach this Test Drive milestone, had to overcome many unforeseen situations including security issues, approbations periods, etc.…

Sophisticated threat actors blended offensive cyber–cognitive campaigns as part of an informationized warfare strategy. In the course of this project, CAF operators using Sapper Labs Active Cyber Defence Platform (CACDP) detected cyber and cognitive attacks against the CAF attributed to Russia - specifically, APT28 Fancy Bear, STRONTIUM Russian cyber espionage group associated with the Russian military intelligence agency GRU Unit 26165 and Unit 74455, as well as the Internet Research Agency (IRA). Sapper Labs discovered direct threats to CAF attributed to these entities (this information can be found in Sapper Labs final report and is open source).

E. Follow-Up and Opportunity from working with IDEaS

Participating to this challenge and working closely with the CAF opened additional opportunities for Sapper Labs to collaborate with other advanced innovators working in the cyber domain. In June 2021, NATO, in partnership with IDEaS and the Canadian Special Operation Forces Command, released an Innovation Challenge looking for innovative concepts and/or tools for countering cognitive warfare. The goal of the challenge was to look for technics and tools to identify, assess, and protect against attacks on the cognitive domain of NATO forces and their allies. This pitch style event invited non-traditional thinkers from across all 30 NATO member nations to showcase ways of securing the cognitive domain against attacks. Following the NATO competition, Sapper Labs collaborated with the overall winner, the US innovator Veriphix (NatSec technology that directly tracks population level belief using a low signature active and ethical data collection) and the recipient of the best Canadian-made solution BMU (Counter-Disinformation Intelligent Solution (CDIS) focusing on the Sense – Augmented Intelligence platform) to initiate a research project focused on countering Russia disinformation and cognitive warfare tactics. The development

and trial of this Cognitive Warfare phase lasted approximatively 4 months.

Cognitive warfare, intelligence and targeting of private military contractors became highly-relevant to this challenge (Cyber Attribution Sophisticated Threat Actors in the Defence of Canada). Hence, they represent a significant part of this project using the Proof-of-Concept for Cognitive Warfare.

Intelligence analysis showed that adversaries transition seamlessly from cyber and cognitive domains. In fact, it is no longer possible to separate cyber and cognitive warfare. Nation-state actors like Russia outsource development and operations to a vast network of security companies, dis-information centres and Private Military Contractors. Target systems analysis revealed direct connections between these entities and blended cyber-cognitive operations against Canada.

In partnership and embedded with military operational units, Sapper Labs delivered an advanced, innovative and effective cyber defence, cognitive warfare, intelligence and targeting solution to CAF. All objectives of the IDEaS Operational Test were fully met. Additionally, several other remarkable and important achievements were accomplished through the execution of this program related to cyber defence, strategic intelligence, operational intelligence and cognitive warfare.

Conclusions

IDEaS does work. After more than 5 years using the Innovation for Defence Excellence and Security (IDEaS) program and tools, DND/CAF deciders and staff can confirm that this business model can work. IDEaS has allowed a closer relationship with innovators and firms that had never worked with the defence industry, as well as the identification of novel solutions to a host of problems/challenges. The experience of IDEaS, with over 75 challenges since the beginning of the program in 2018, covers all of the most defence/security domains of work, such as protection, electronic warfare, communications, human performance, transition from a military career to civilian life, quantum and AI, and many more. Novel solutions are being generated in many of these domains of work.

The success of the IDEaS Challenge “Cyber Attribution for the Defence of Canada” can be attributed to three observations:

- Effective innovation program – IDEaS is a critical CAF program for both innovation and capability development, at speed, particularly in cyber, cognitive warfare and intelligence domains. It is a great program for positive Canadian outcomes;
- Operational outcomes - The relationship between Sapper Labs, CAF operators and IDEaS management was relentlessly focused on timely mission outcomes, despite challenges; and
- Collaboration breeds better innovation - through execution, Sapper Labs and CAF became more capable innovators and operators. They became allies in meeting complex challenges and realities for operational missions – from policy, to doctrine, operational planning, execution, and training. Successful technology adoption was directly correlated to mutual knowledge transfer.

References

1. Department of National Defence (2017) Strong, Secure, Engaged: Canada’s Defence Policy. Retrieved 8 December 2023. Strong, Secure, Engaged: Canada's Defence Policy - Canada.ca DND/CAF
2. NASA (2023) Technology Readiness Levels. Retrieved 12 February 2024. https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/ Manning, Catherine.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.08

The impact of the russian-ukrainian war on economic processes in russia: analysis and forecasting

Maryna Sliusarenko
PhD (Engineering), Senior Researcher
Central Research Institute of the Armed Forces of Ukraine
28B, Povitroflotskyi Ave. 03049, Kyiv, Ukraine
e-mail: slusarenko@gmail.com
ORCID: 0000-0003-4165-3908

Serhii Baranov
Head of the Main Directorate of Missile Forces,
Artillery and Unmanned Systems General Staff of the Armed Forces of Ukraine
03168, Povitroflotskyi prospect, 6, Kyiv, Ukraine
e-mail: sharada3699@gmail.com
ORCID: 0000-0002-3306-943X

Roman Voytsehovskiy
Postgraduate of the Department of Millitary Management of the Institute of State Military Management of the the National Defense University of Ukraine
28B, Povitroflotskyi Ave. 03049, Kyiv, Ukraine
e-mail: voytsehovskiy31@gmail.com
ORCID: 0009-0000-6408-9620

Abstract. In this article, the author examines the impact of the war in Ukraine on the Russian economy, analyzes and forecasts some of the main factors. The relevance of the issue under consideration is due to the fact that the economic situation in Russia directly affects Russia's ability to continue the war in Ukraine. Therefore, the purpose of the article is to analyze and forecast the impact of the Russian-Ukrainian war on economic processes in Russia. Despite the fact that official statistics are mostly classified or distorted by Rosstat, the analysis shows that the economic situation in Russia is getting worse. For the past six years, the Russian economy has been experiencing strong inflation, and in the current environment, inflationary processes have intensified significantly. Eventually, the Kremlin will face a problem: either to continue fighting in Ukraine, or to boost the economy, or to move to a large-scale money issue, which will lead to even higher prices. The National Welfare Fund has shrunk by almost a third and continues to shrink. That is, without additional investments of foreign capital, Russia will not be able to raise the economy and conduct military operations.

The key policy rate was forecasted using neural networks based on the method of group consideration of arguments using the GMDH Shell program. The forecast shows that in 2023 the key policy rate may increase to 23%.

The article shows how the national welfare fund of Russia has been reduced, and the federal budget expenditures are analyzed. The author gives the estimated expenditures of the Russian Federation for the first year of the war and the budget deficit. According to experts' estimates, an approximate figure of the need for funds to support combat operations in the current conditions is provided. The materials of the article are of practical value for analysts, economists and anyone who studies the Russian-Ukrainian war from the point of view of the economic component.

Keywords: Russian-Ukrainian war, economic processes, National Welfare Fund, key rate, inflation, military spending, budget.

Introduction

The Russian-Ukrainian war has a negative impact on economic processes in the Russian Federation, which, in the absence of external support and investment, as well as the closure of foreign markets, has devastating consequences for the Russian economy and, ultimately, the socio-economic situation of the country. According to experts, 88% of the Russian Federation budget for 2023 was spent in January-February (2.6 trillion rubles, or $ 0.31 trillion). This resulted in its deficit at the end of the year (2.9 trillion rubles, which is about 1.5% of GDP according to Rosstat) and increased destructive processes in the economy. Due to exorbitant costs that the military and political leadership of the Russian Federation failed to forecast, the country is now falling into a "deficit hole". This is also due to a drop in almost half of revenues from oil and gas exports. Currently, according to analysts, the Russian Federation is losing about $500 million per day (Melov V., 07.03.2023, Melov V., 31.12.2023). Since these destructive processes directly affect Russia's ability to continue the war, the study of issues related to the decline of the Russian economy is relevant.

Many experts from all over the world, including economists, financiers, demographers, and political scientists, are engaged in analyzing and forecasting the impact of the Russian-Ukrainian war on economic processes in Russia. The authors of *The Economist* analyze how the Russian economy is withstanding the war ("The Russian Economy Can Withstand ...", 2023; "The Russian economy is dangerously overheated...", 2023). How the costs of the war affect Russian citizens is investigated in ("Russia's expenses for the war in Ukraine...", 2023). How the fall of the ruble affects the ability of the Russian Federation to conduct hostilities in Ukraine is covered in ("What does the fall of the ruble mean...", 2023). Experts of the Center for Countering Disinformation study issues related to the impact of the Russian banking crisis on the ability to conduct hostilities in Ukraine ("How the banking crisis in Russia...", 2023). Experts from the International Research Institute for Food Policy (Aizenman N., 2022 and Bloomberg (Bloomberg, 2022) consider scenarios for the development of the economy, including the Russian one, during the war in Ukraine. How the war affects the banking system in the Russian Federation and the International Monetary Fund is investigated in (The Worldwide Effects of Russia's Invasion of Ukraine, 2022). Russia’s military actions against Ukraine affect not only the industry of the Russian Federation itself, but also global food security (Glauber J., 2022). The global socio-economic consequences of the Russian-Ukrainian war are explored in (Chaliuk Y. O., 2022). The processes of degradation of the Russian economy and the inevitability of the crisis are considered in (Kovalenko E., 2023). War, mobilization, sanctions, and the mass exodus of Russians abroad have undermined many people's sense of confidence in the future. According to (Enikolopov R., 2023), its absence will determine the development of the economy for the coming years.

However, when analyzing the impact of the Russian-Ukrainian war on the economy of the Russian Federation, only certain indicators are mostly considered, while the forecasts provided are empirical in nature without an attempt to make an analytical description of the processes under study.

Materials and Methods

According to the analysis by the Center for Strategic and International Studies CSIS (Russia lost in Ukraine..., 2023), in the first year of the war in Ukraine, Russia suffered more losses than in all wars and conflicts in which it has participated since World War II. The average number of Russian soldiers killed per month is 25 times higher than in Chechnya and 35 times higher than in Afghanistan. But the question arises: how do such large losses affect the economic situation of the Russian Federation and what indicators can be assessed for this? (Development Analysis..., 2022) have already considered such indicators as changes in the exchange rate of the Russian ruble, changes in

military spending, and the demographic aspect. The author believes that the main indicators that most clearly reflect the real state of Russia's economy extend to military spending, including funds that the Russian Federation spent during the one year of the war in Ukraine; changes in the National Welfare Fund (NWF); the industrial production index; inflation; a drop in industrial production in 2022; Russia's oil and gas and non-oil revenues; changes in the price of URALS oil in 2022 ($ per barrel); freight turnover of transport in the Russian Federation in 2022; unemployment rate; and the key rate of the Central Bank of the Russian Federation. As part of this study, let us look into some of them. Key rate forecasting is carried out using neural networks based on the Group Method of Data Handling applying GMDH Shell.

Results and Discussions

The NWF was created as part of the mechanism of pension provision for citizens for the long term. That is, one of the functions of this fund is to ensure the balance (covering the deficit) of the budget of the pension fund of the Russian Federation. However, due to the fact that the war against Ukraine is protracting, many expenditure items that have not been taken into account have been added, so the NWF is inevitably being spent. The fund cut down during 2022 is shown in Fig. 1.

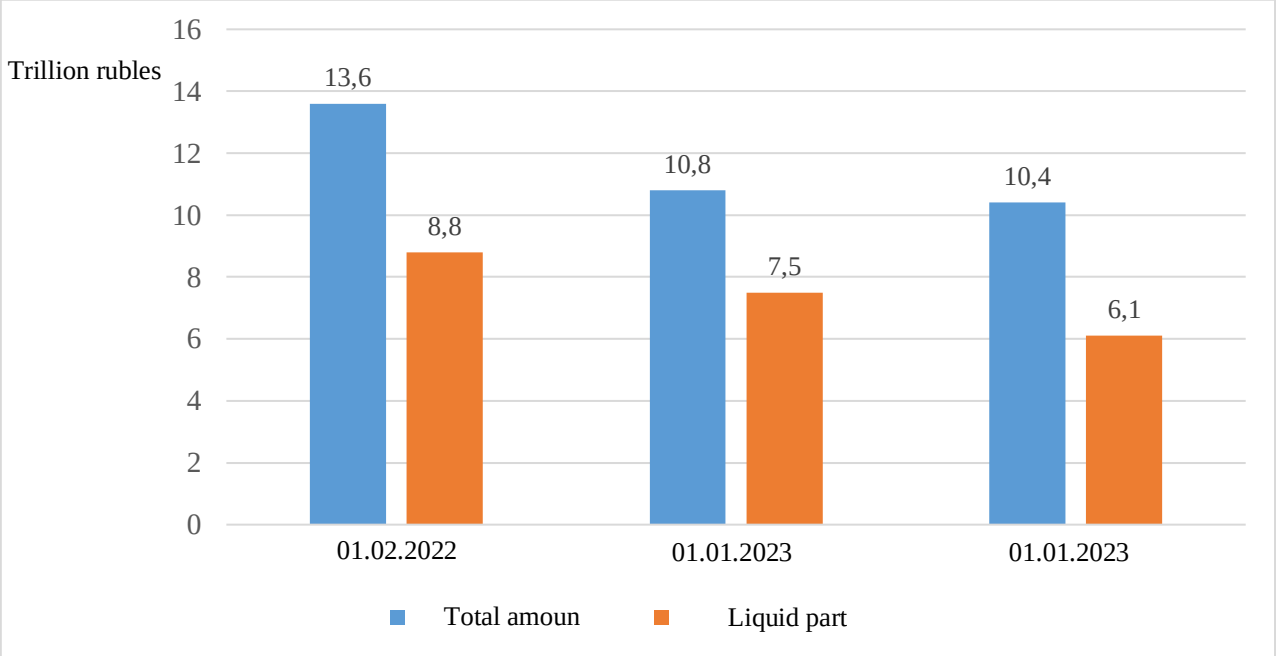


Figure 1. Changes in the NWF of the Russian Federation, 01.02.2022 - 01.01.2023

As can be seen in Fig.1, in the first year of the war, the NWF decreased by almost the same amount, making 3.2 trillion rubles ($0.038 trillion). In the first quarter of 2023, the budget deficit amounted to 2.4 trillion rubles, with expenditures reaching 28% of the annual plan. This is 83% of the planned annual deficit. Therefore, it can be argued that, according to the forecast, the total volume of the NWF and its liquid part will continue to fall, and this is the issue of financing the war in Ukraine. (The liquid part is the government's money in bank accounts.)

Consider the distribution of *expenditures of the federal budget of the Russian Federation* in 2022 (Fig. 2) (Melov V., 06.04.2023).

As already noted, the budget deficit of the Russian Federation in 2022 amounted to almost 3.3 trillion rubles, judging by the distribution of the federal budget expenditures, this is the amount spent on defense.

Russia's military expenditures are shown in Fig. 3.

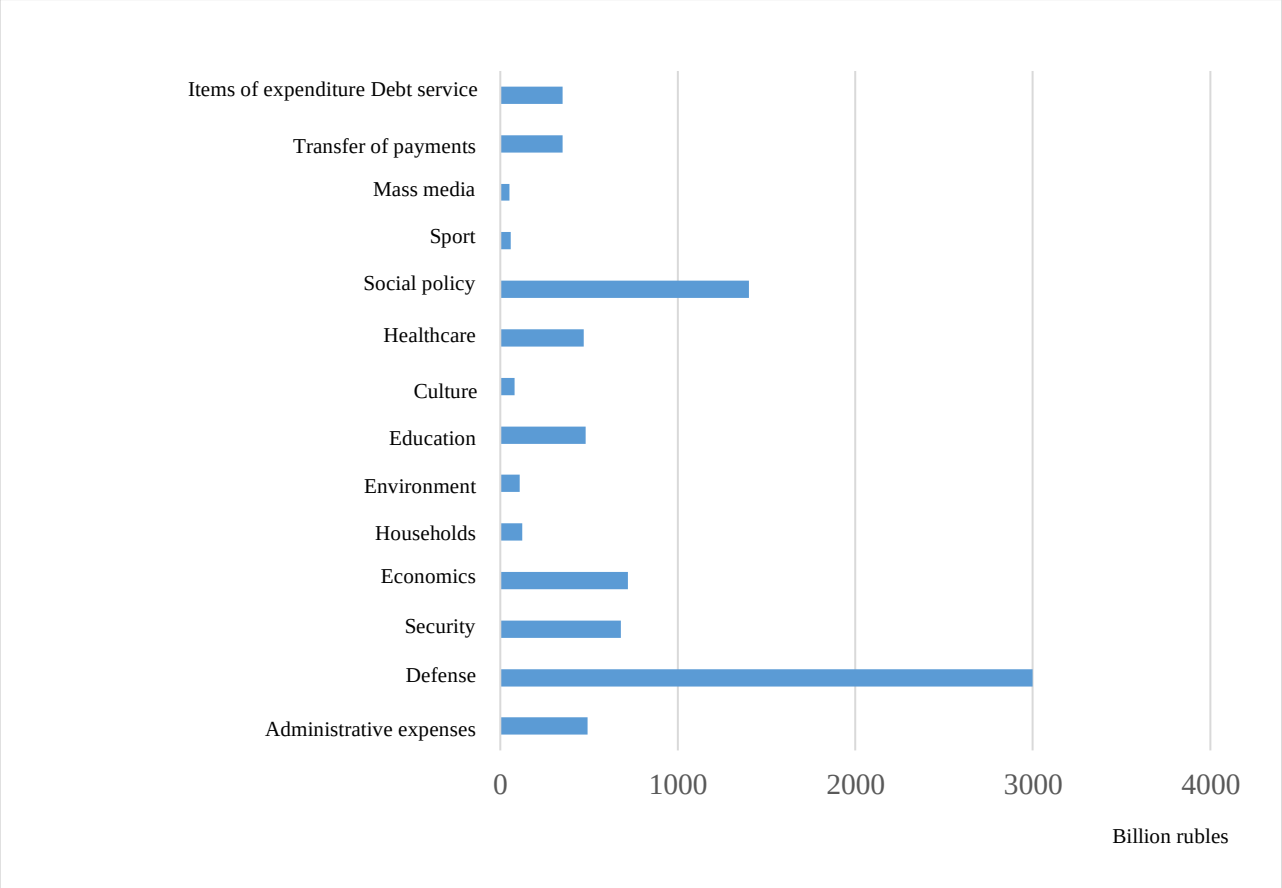


Figure 2. Expenditures of the federal budget of the Russian Federation as of 28.03.2023, billion rubles for 2022

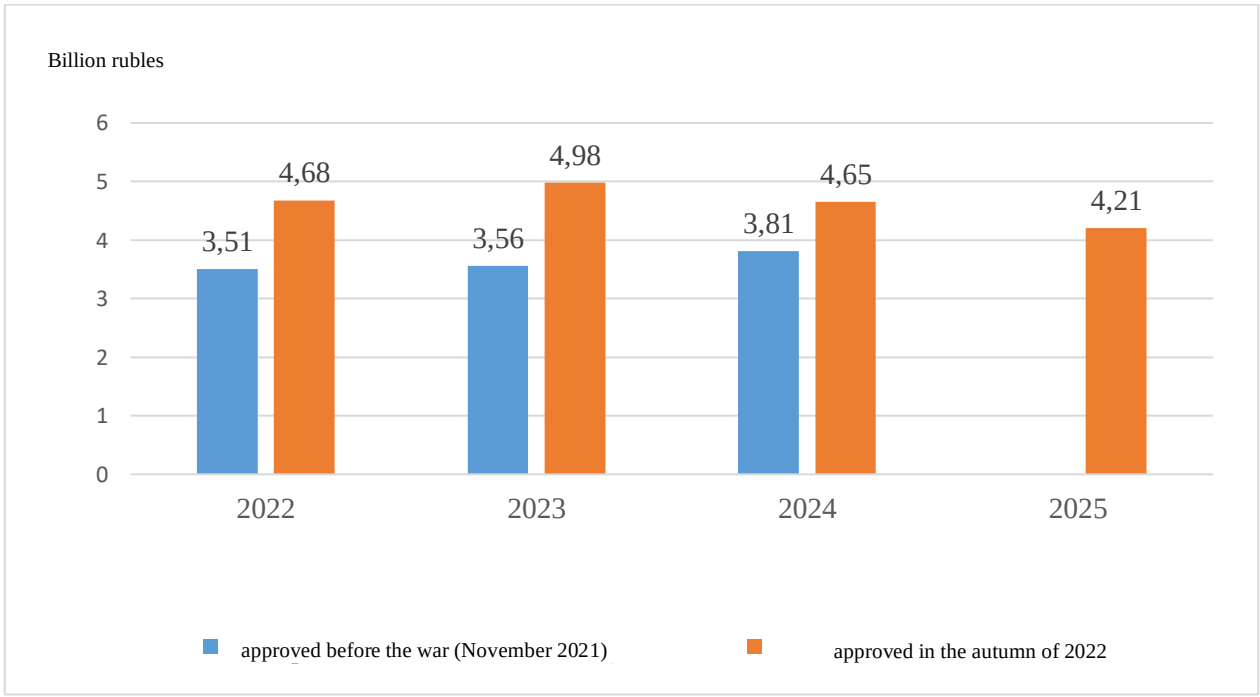


Figure 3. Military expenditures in the budget of the Russian Federation for 2022–2025 (trillion rubles)

Recently, there has been a tendency for the Russians to conceal real defense spending. Thus, at the end of 2021, part of classified expenses amounted to 15.2%. In the first half of 2022, the non-public part increased to 18.6%. Since the beginning of 2023, 32% of the Russian budget has been classified (except for open data on defense and security) (Bloomberg 2023). As of 24.03.2023, this makes $31 billion. According to analysts, this indicates that all these costs go to the war in Ukraine. According to experts, at least 10-15 trillion rubles are required ($1 = $84.32) per year to sustain combat operations in the current conditions. The most expensive for the federal budget was the provision of the army – about $36 billion per year of the war. And the amount of compensation that the Russian government has to pay to the killed and wounded even exceeds the amount of salaries – $29.1 billion. The families of each killed Russian soldier (175160 as of 03.04.2023) should be paid compensation of 7.4 million rubles (approximately $110,000). That is, the total amount of compensation for the killed Russians in the first year of the war exceeds 1 trillion rubles. The wounded will receive 3 million rubles compensation from the Russian Federation. However, there are usually twice as many seriously wounded as killed, that is, the expenditure for this item is not much less. At the same time, despite the increase in defense spending, the Russian Federation is significantly inferior to the United States and European NATO countries in this regard.

The values of GDP, military expenditures of the Russian Federation, the United States and European NATO countries are shown in Table 1.

Table 1. GDP of the Russian Federation, the United States and European NATO countries

Countries	*GDP, $ trillion*	*Military expenditures, $ trillion*	*% of GDP*
RF	1.7	0.0356	2.09
USA	23	0.7777	3.38
European NATO countries	23	0.345	1.5

Although Russia avoided economic collapse after the start of a full-scale war against Ukraine, it is slowly plunging into crisis. According to Bloomberg Economics, the Russian economy could lose $190 billion in GDP (8%) by 2026. This is equivalent to the annual GDP of such countries such as Hungary or Kuwait. During a year of the war, the Russian Federation spent a third of all revenues of the Russian budget for 2021 (Table 2, Fig. 4) (Datsenko V., 2023).

Russia's expenditures for a year of the war in Ukraine

As shown in the graph (Fig. 4), Russia's spending on compensation to the families of the killed and compensation for the wounded will increase in 2023.

Russia spent $114.4 billion on the war in just one year (almost $10 billion per month). This amount includes only direct costs of the war and does not take into account economic and indirect losses suffered by the Russian Federation from sanctions and economic isolation.

The dynamics of Russia's expenditures during a year of the war on financial support and compensation to military personnel is shown in Table. 3 and in Fig. 5.

Table 2. Russia's estimated expenditures for a year of the war in Ukraine

Total military salaries and compensation costs	$53.8 bn
Expenses for the provision of the army	$36.1 bn
Cost of lost equipment	$24.5 bn
Total	$114.4 bn

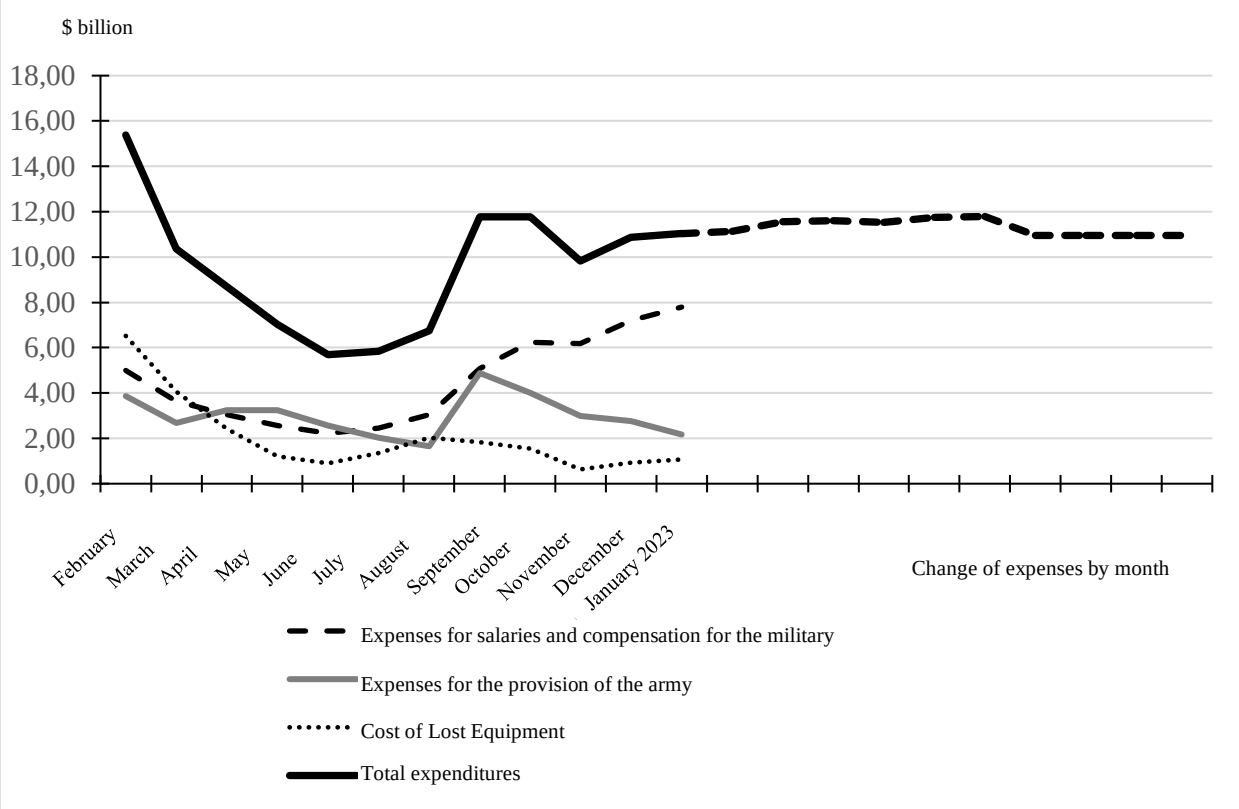


Figure 4. Dynamics of changes in Russia's estimated expenditures in the first year of the war in Ukraine by items

Table 3. Total expenditures of the Russian Federation during a year of war on financial support and compensation to military personnel

Items	Amount, $bn
Total expenditures of the Russian Federation for a year of the war on financial support for military personnel	24.7
Total expenditures of the Russian Federation for a year of the war to compensate the families of the killed	16
Total expenditures of the Russian Federation for the year of the war to compensate the wounded	13.1
The total amount of expenditures of the Russian Federation	53.8

Whilst they are trying to increase the cost of providing the army and maintaining military personnel, there is a big problem with equipment. The estimated cost of weapons and military equipment that the Russian Federation is losing during the war is $10-11 billion per month. It is quite clear that Russia is unable to compensate for these costs in the medium term. The above graph (Fig. 4) presents the total costs, a forecast for 2023 is based on them. Forecasting is carried out using neural networks based on the Group Method of Data Handling applying GMDH Shell. At the same time, the coefficient of determination of the obtained forecasts ranges from 0.85 to 0.97, and the forecast corridors did not exceed 15%, which indicates their high accuracy on the selected horizon.

The cost of equipment lost by Russia during a year of the war.

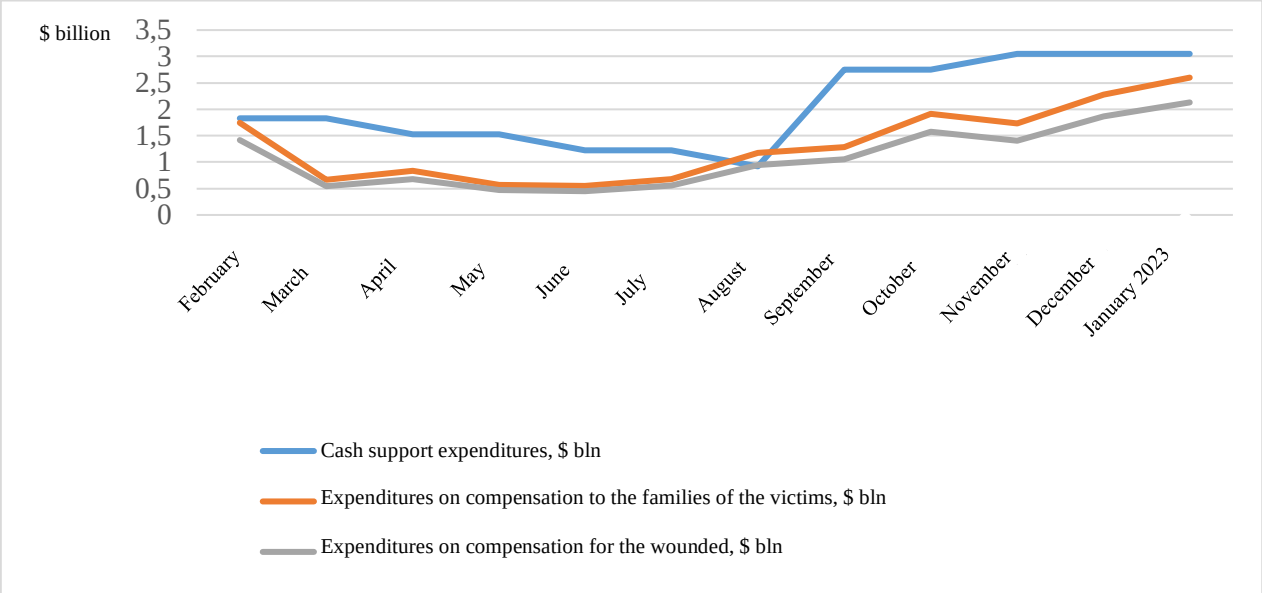


Figure 5. Dynamics of Russia's expenditures on financial support and compensation to military personnel in the first year of the war

It is estimated that the value of the equipment alone lost by Russia reaches $25 billion. The cost of equipment by type, which the Russian Federation lost during one year of the war in Ukraine, is shown in Fig. 6.

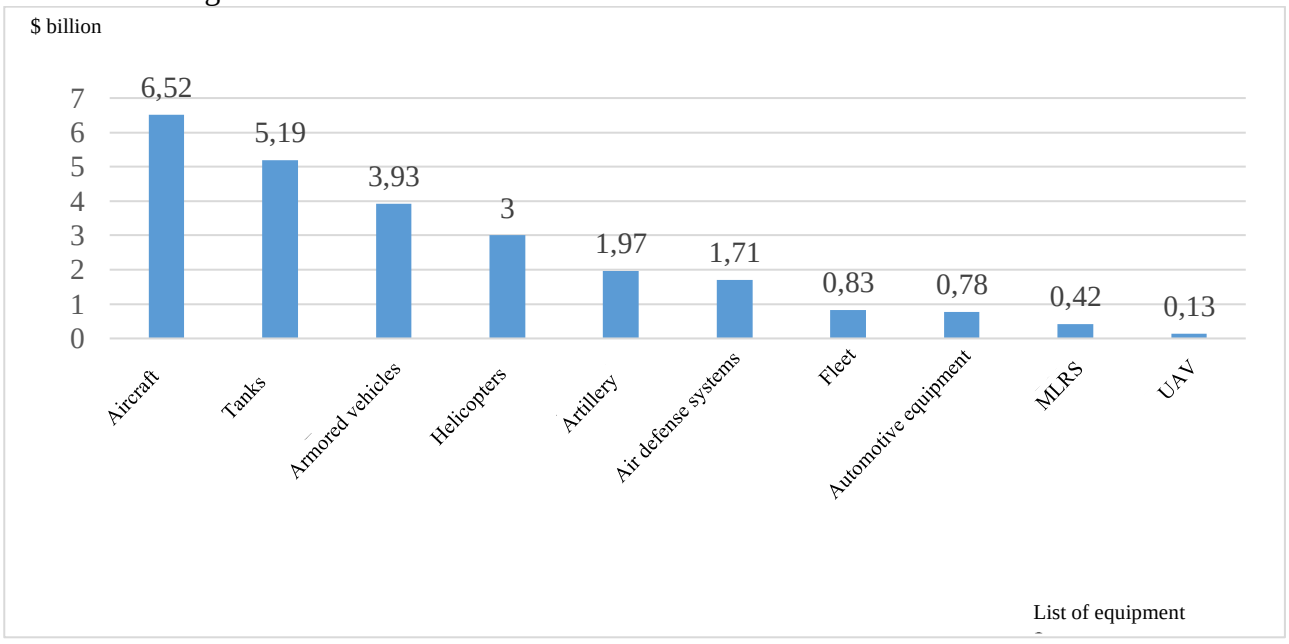


Figure 6. The cost of equipment that the Russian Federation lost during one year of war in Ukraine

Apparently, the most costly for the Russians are the losses of aviation (about $6.52 billion), despite the fact that aviation does not play such an important role in the war in Ukraine. At the same time, the restoration of the fleet is the most complex and costly process. The destroyed helicopters cost Russia about $3 billion. The total cost of equipment that the Russian Federation lost during one year of the war in Ukraine will increase in 2023. For the Russian Federation, the restoration of

weapons and military equipment will be problematic, especially when it comes to high-tech one, due to the relatively large number of foreign-made components to which there is currently no access, the indivisible production potential and the acute shortage of technical personnel. For example, the promising T-14 Armata main tank, the development of which began in 1971, was supposed to be put into service in 2015, but it has not yet passed state tests, the start of serial production is constantly being postponed, the volume of orders is decreasing (from 2300 samples in 2018 to 132 in 2021), and according to the latest information, the production of the T-14 has been stopped due to Western sanctions (Russia refuses, 2022).

A similar situation has developed with the fifth-generation Su-57 (T-50) aircraft, which is based on Soviet developments, and has been actively developed since the early 2000s. So far, only 3 serial models and 7 test models have been produced, but, according to experts, it is already obsolete and inferior in basic characteristics even to the F-15 and F-16, which were created in the mid-70s of the last century (more than 6000 samples were produced in total) (Against the backdrop of outright stagnation, 2022).

Expenditures of the Russian Federation on the provision of the army in 2022-2023 are shown in Fig. 7.

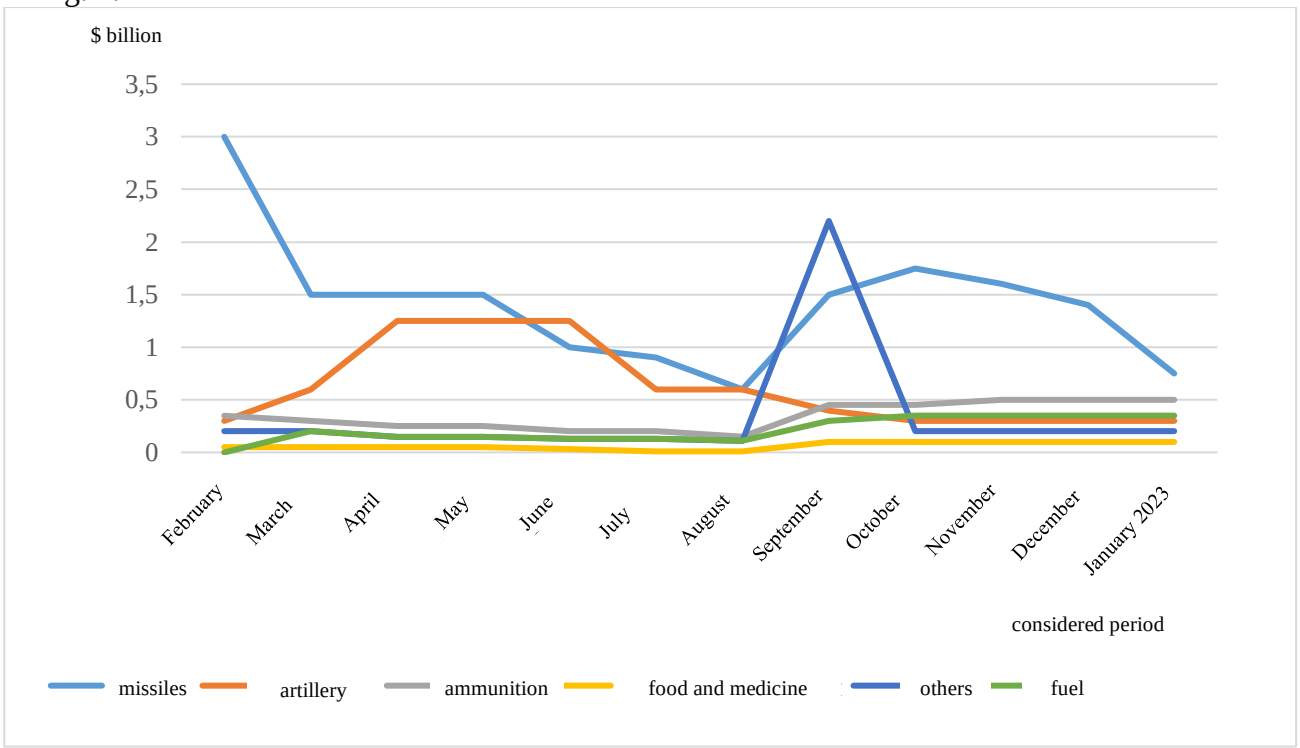


Figure 7. Dynamics of Russia's expenditures on the provision of the army

According to estimates, the cost of provision of the Russian army per month ranges from $1.2 to $2 billion, which creates an additional burden on the budget.

Inflation

The war against Ukraine, together with sanctions, has had a significant impact on the economy of the Russian Federation. Thus, over the past six years, the Russian economy has been experiencing inflation, and in the current conditions, inflationary processes have accelerated significantly (Fig. 8).

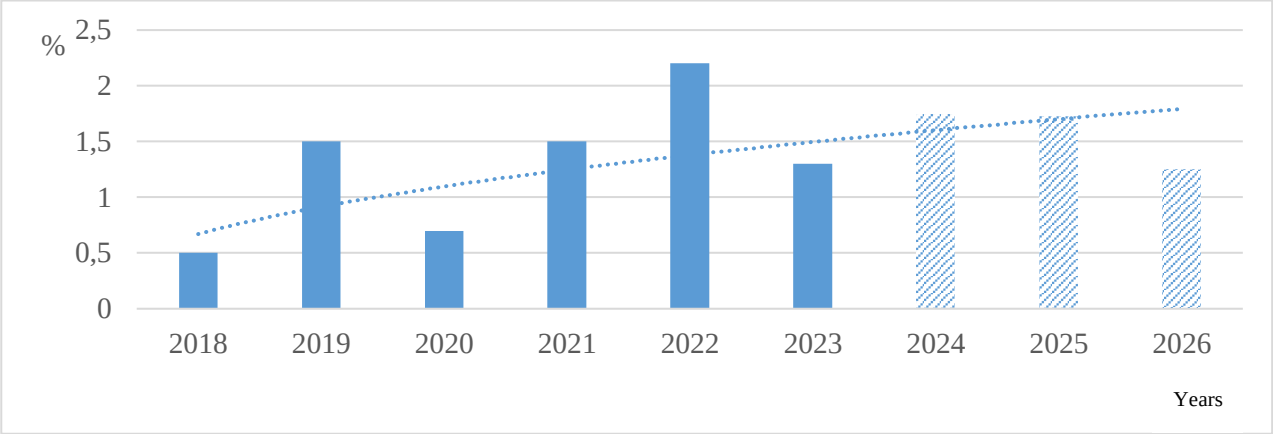


Figure 8. Inflation in 2018–2023, January–December, % compared to December of the previous year

That is, inflation has a steady upward trend.

National currency exchange rate

An important indicator that reflects both the real economic situation and the state's efforts to stabilize it is the exchange rate of the national currency (Fig. 9, 10). Thus, inflation targeting is an important element of monetary policy, the ultimate goal of which is price stability (Inflation Targeting, 2023). At the same time, the Central Bank of the Russian Federation noted that annual inflation, after falling below the target of 4% in March-April 2023, would gradually begin to grow in May-June. The inflation forecast of 5–7% for the end of 2023 remains unchanged (Zabotkin A., 2023).

Tough economic sanctions against the banking system and fear of new restrictions are eroding Russian stability. In order to somehow even out the situation, the Central Bank adopted a package of currency restrictions: on the sale of cash in $ and Euro; withdrawal of money from accounts opened in foreign currency; for international money transfers, etc. However, exchange rates continue to rise.

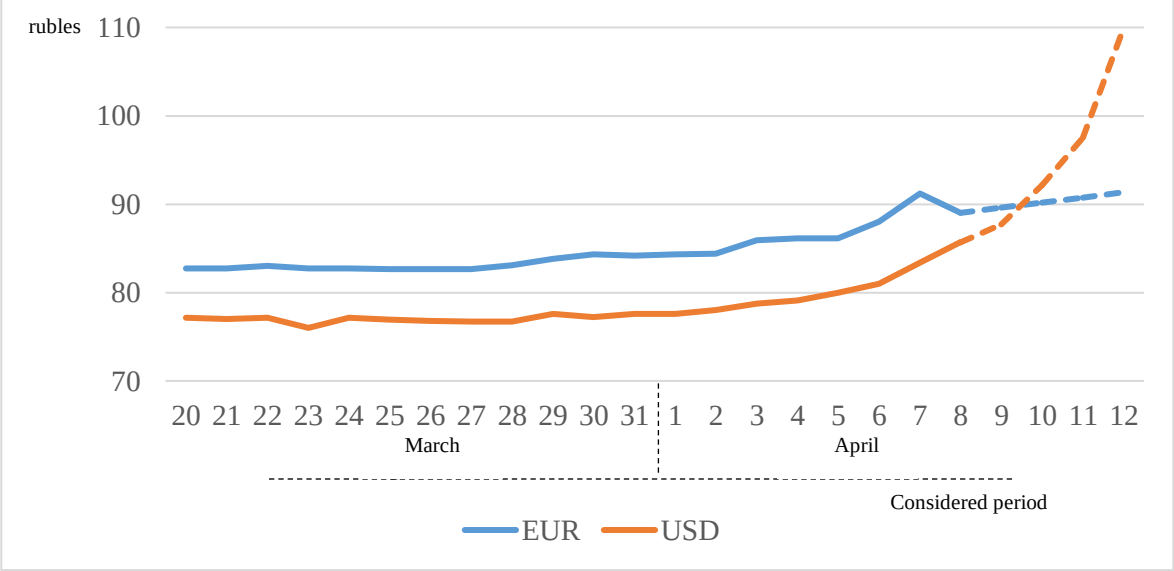


Figure 9. Dynamics of changes in the exchange rate of the dollar and Euro against the ruble, March–April 2023

Retrospective analysis shows that the outbreak of armed conflicts has a negative impact on the ruble exchange rate (Fig. 10).

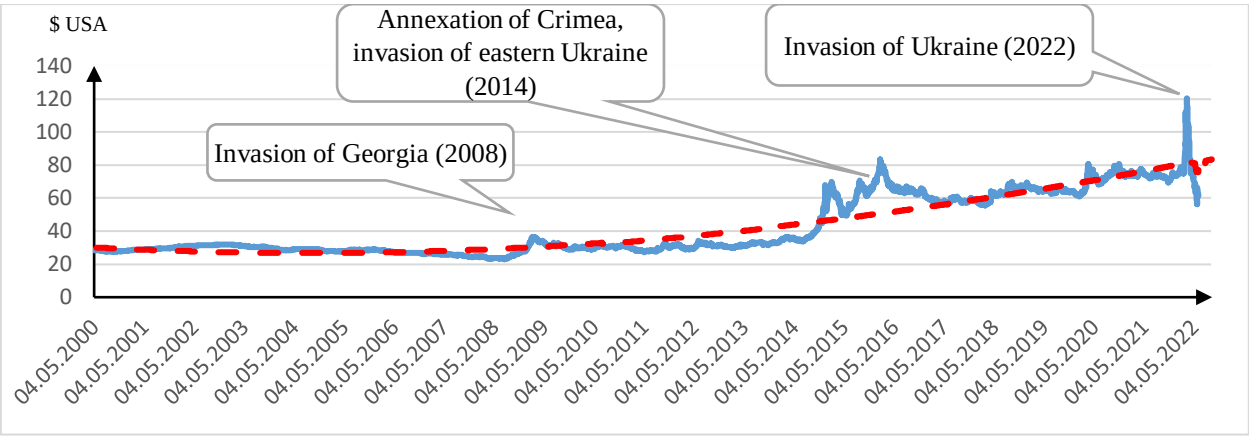


Figure 10. Changes in the ruble exchange rate against $ in 2000–2022

Key rate

Another important indicator is the key rate. This is the minimum interest rate at which the Central Bank issues loans to commercial banks. The key rate is one of the instruments of monetary policy to support the economy in a downturn. Since the end of 2020, the key rate had been 4.5 % and remained at this level until March 2021 (Fig. 11). In the second half of 2023, the Board of Directors of the Central Bank of Russia raised the key rate five times, the last one – on 15.12.2023 to 16 % (Ilchenko L., 2023). Currently, the Central Bank has stopped the reduction of the rate, freezing it for an indefinite period. The government of the Russian Federation assures the market that under such circumstances, high rates will remain for a long time. Fig. 11 presents a forecast for changes in the key rate by the end of 2023 and at the beginning of 2024. If the current trends continue, it is expected to grow to 17 %.

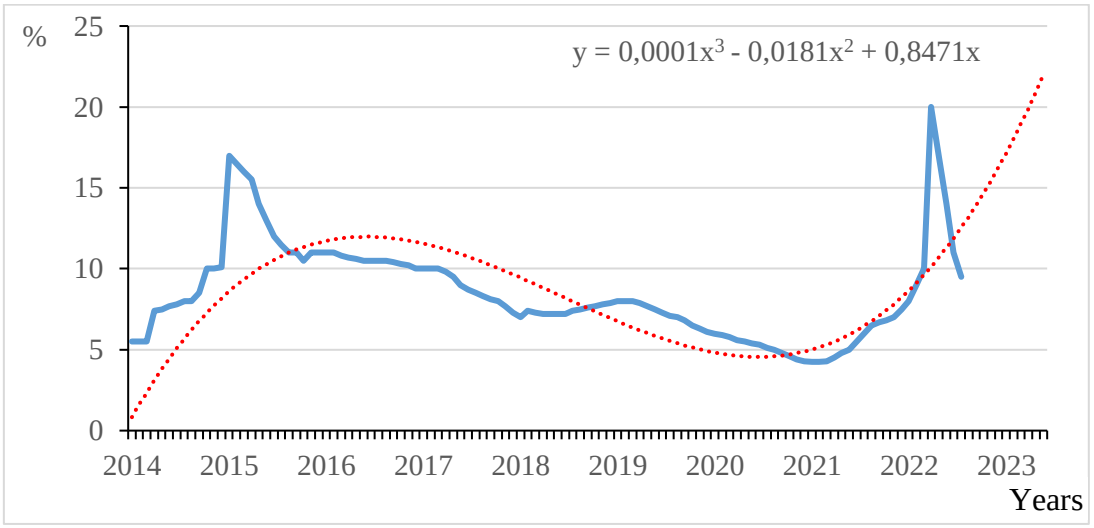


Figure 11. Change in the key rate of the Russian Federation, % (where x is the value of the key rate in the previous step)

Approximation is rather accurate, without taking into account " unloadings". The unloading is the real nature (reaction) of the process, and the decrease that occurs after is the reaction of the Central Bank, which is due to its purposeful activity. Preliminary accounting of "emissions unloadings" was

not carried out due to the overall smoothness (harmony) of the process and the specifics of the software used. Therefore, there was no decrease in the key rate in 2023 and it is not expected in the first half of 2024.

At the same time, there is every reason to believe that the situation is worse than that presented by the official data of Rosstat. Thus, the Central Bank of the Russian Federation admitted that the blow to the economy is very strong, and it is unknown how long it will last. In addition, the Central Bank classified bank statements.

Oil and gas revenues

The main source of filling the budget of the Russian Federation is oil and gas revenues. On 05.12.2022, almost a year after Russia's invasion of Ukraine, the West imposed an almost complete embargo on Russian oil exports According to IEA (International Energy Agency), due to the embargo, the Kremlin will lose about one trillion dollars in export revenues by 2030, and Russia's share in the global energy market will decrease to 13% from 20%. At the same time, the situation is worsening due to the rapid reduction in the price of Russian oil. The markets lost to the Russian Federation will be occupied by the United States and the countries of the Middle East (Kalmykov O., 2023). Russia's revenues will fall by at least 40% in 2023. changes in the price of URALS oil during 2022 are shown in Fig. 12.

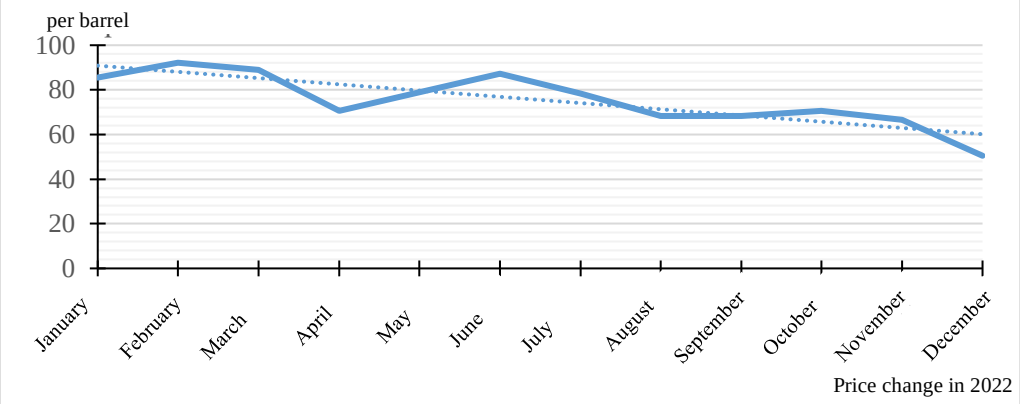


Figure 12. Changes in the price of URALS oil in 2022, $ per barrel

In March 2023, the average price of URALS oil was $47.85 per barrel. There was no increase in the price of oil due to a decrease in its production.

Gas exports from the Russian Federation fell by 46%. That is, one can say that the budget of the Russian Federation will not see large revenues from oil and gas, since the situation with oil is not improving. As a result, we should expect an even larger budget deficit, which depends on the sale of oil and gas, by 40%, and this is the issue of financing the war in Ukraine. As a result, there is a further expenditure of the NWF.

Conclusion

Thus, the article analyzes and forecasts the impact of the Russian-Ukrainian war on economic processes in Russia. In the first year of the war, the NWF shrank by 3.2 trillion rubles ($0.038 trillion), in 2022 their budget deficit was almost 3.3 rubles ($0.039 trillion). Defense spending is the largest part in the expenditures of the federal budget of the Russian Federation for 2023 (3000 billion rubles, or $ 35.577 billion). The key goal of the budget policy of the Russian Federation is to finance the war. For 2024, 11 trillion rubles have been allocated. for military expenditures. Russia spent $114.4 billion on the war in a year (almost $10 billion per month). According to experts, at least 10-15 trillion rubles are needed. ($0.12 trillion – $0.18 trillion) per year to sustain hostilities in the current

conditions. Now the enemy has put its economy on a war footing, but due to Western sanctions, it is not able to quickly produce modern weapons. Since there is not enough money, the Russian Federation will revise its federal budget and increase military spending. This will put additional pressure on the deficit, and falling revenues and high spending have already created it.

Over the past six years, the Russian economy has been experiencing strong inflation, and in the current conditions, inflationary processes have accelerated significantly. The forecast suggests that the key rate may rise to 17% in 2023. Eventually, the Kremlin will face a problem: either to continue hostilities in Ukraine, or to raise the economy, or to move to large-scale monetary emission, which will lead to an even greater increase in prices. The NWF has shrunk by almost a third, and this process continues. That is, without additional investment of foreign capital, the Russian Federation will not be able to raise the economy and conduct hostilities.

The subject of further research may be the study of the impact of mobilization on the economic processes of Russia.

Recommendations

The materials of the article are of practical value for analysts, economists and all those who study the Russian-Ukrainian war from the point of view of the economic component.

References

1. Melov, V. Money is running out. Russia's budget deficit is growing. (2023). https://youtube/HOtsOmgh00k (accessed 07.03.2023).
2. Melov, V. Price growth cannot be stopped. (2023). https://youtube/HOtsOmgh00k (accessed 31.12.2023).
3. Russian economy can withstand a long war, but not an intense one. (2023). *The Economist*. 2023.04.25. https://texty.org.ua.
4. Russian economy is dangerously overheated due to the war. (2023). *The Economist*. 2023.12.11. https://texty.org.ua.
5. Russia's spending on the war in Ukraine is about to hit the Russians hard. (2023). *The Economist.* 2023.10.02. https://texty.org.ua.
6. What the fall of the ruble means for Russia's ability to wage war. (2023). *The Economist*. 2023.08.15. https://texty.org.ua.
7. How does the banking crisis in Russia affect the war in Ukraine? (2023). Center for Countering Disinformation. 18.08.2023. https://cpd.gov.ua/main/yak-bankivska-kryza-rosiyi-vpiyvaye-na-vijnu-v-ukrayini/.
8. Aizenman, N. Russia’s war on Ukraine is dire for world hunger. But there are solutions. (2022). https://www.npr.org/sections/goatsandsoda/2022/03/061083769798/russias-war-on-ukraine-in-dire-for-world-hunjer-butthere-are-solutions.
9. How War in Ukraine Threatens the World’s EconomicRecovery. (2022). *Bloomberg*. https://www.bloomberg.com/news/features/2022-02-25/war-in-ukraine-russia-conflict-could-impact-the-global-economy.
10. The Worldwide Effects of Russia’s Invasion of Ukraine. URL: https://learningenglish.voanews.com/a/the-worldwide-effects-of-russia-s-invasion-of-ukraine/6468531.html.
11. Glauber, J., Laborde, D. How will Russia’s invasion of Ukraine affect global food security? https://www.ifpri.org/blog/how- will-russias-ukraine-affect-global-security.
12. Chaliuk, Yu. O. Global socio-economic consequences of the Russian-Ukrainian war. (2022). *Economy and society*. Kyiv. № 37. https://economyandsociety.in.ua.
13. Kovalenko, Ye. Putin has finally finished the Russian economy. (2023). https://www.unian.net/economics/finansy (accessed 10.01.2023).

14. Yenikolopov, R. People do not eat tanks. How the Russian economy was affected by war and mobilization. (2023). https://rus.postimees.rus/ (accessed 27.02.2023).
15. Russia has lost more soldiers in Ukraine than in all wars since World War II. (2023). CSIS, Washington, DC. https://interfax.com.ua (accessed 06.03.2023).
16. Sliusarenko, M. O. Analysis of the development of the economic and demographic situation of the Russian Federation in view of the Russian-Ukrainian war. (2022). *Bulletin of Kremenchuk Mykhailo Ostrohradskyi National University*. Kremenchuk. Issue 4 (135). C. 8-44.
17. Preliminary assessment of the execution of the federal budget for January-December 2022. (2023). URL: https://minfin.gov.ru/ru/press-center/?id_4=38343 (accessed 18.01.2023).
18. Melov, V. Dollar 80, Euro 90. Banks are sounding the alarm. (2023). https://youtube/HOtsOmgh00k (accessed 06.04.2023).
19. Bloomberg reported on "unprecedented" classification of Russia's budget spending. (2023). Forbes.ru/finansy/478481-bloomberg-soobsil-o-besprecendentno-zasekreciavanii-reshodov-budzeta-rossii (дата звернення: 06.04.2023).
20. Datsenko, V. (2023). https://Forbes.ua (accessed 2023 April 06).
21. Russia is abandoning the production of new tanks, including the T-90 and T-14 Armata. https://mil.in.ua/uk/news/v-rosiyi-vidmovlyayutsya-vid-vyrobnytstva-novyh-tankiv-v-tomu-chysli-t-90-ta-t-14-armata-gur-mo/.
22. Against the backdrop of outright stagnation of the aircraft industry in Russia, there is talk of another "unparalleled" fighter jet. https://defence-ua.com/weapon_and_tech/pislja_provalu_z_su_57_v_rosiji_zamahnulis_na_stvorennja_vlasnogo_f_35_zapiznilij_start_nerealnih_bazhan-3802.html.
23. Inflation Targeting. (2023). https://uk.m.wikipedia.org (accessed 06.04.2023).
24. Zabotkin, A. Economics. (2023). http://Interfax.Ru. (accessed 03.04.2023).
25. Ilchenko, L. In Russia, the discount rate was raised for the fifth time in six months. *Ekonomichna pravda*. https://www.epravda.com.ua.
26. Kalmykov, O. (2023). https://www.ddc.com (accessed 05.02.2023).

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.09

The systematic review of variety of military, weapon, combat and warfare system-of-systems wuth their new classification and ontology depiction for further concept and design development for the Armed Forces of Ukraine

Volodymyr Tymchuk
candidate of technical sciences, senior researcher
doctorate researcher
Hetman Petro Sahaidachnyi National Army Academy
79026, Lviv, 32 Heroyiv Maydanu
email: voljuty@gmail.com
ORCID: 0000-0002-3549-2813

Vasyl Trysnyuk
doctor of technical sciences, professor
head of department of environment research
Institute of Telecommunications and Global Information Space
of the National Academy of Sciences of Ukraine
03186, Kyiv, 25 Chokolivskiy bulv., ap. 13.
email: trysnyuk@ukr.net
ORCID: 0000-0001-9920-4879

Abstract. A system-of-systems is a special complex structure in which new capabilities arise from interacting independent pieces that are controlled by multiple operators. One special kind of similar structure are military, or weapon, system-of-systems. The architecture of weapon SoS consists of the constituent systems (pieces), of interfaces and IT, of communication and exchanges occurring between the systems. The architecture of the SoS is always in a state of flux, but in warfare the demands to change the structure of weapon SoS are emphasized. To save lives and to win both in close battles and long war is the main mission of HQ, common combat forces and supporting efforts.

In the article the architecture of created SoS in different countries (mainly in U. S., but also in NATO and P. R. C.) are presented – their schemes, components, purposes and key peculiarities. These features allow to get the ontology for typical variant of SoS – they all were divided into five classes. So, we suppose that SoS may by differed by their creation, or evolution, or transition, or combination, or due to attaching to non-SoS.

In general, the development planning of the military or weapon SoS is a challenging strategic analysis work because it involves various aspects, such as mission tasks, capability requirements, weapon effectiveness, and economic benefits. But in demands of lifesaving in warfare the expectable replacing soldiers via an autonomous vehicle SoS are straightforward, so it is need to understand the concept and main features of SoS.

Keywords: military system-of-systems, command and control, design concept, ontology, Zbroini syly Ukrainy.

Introduction

In the modern warfare the military system-of-systems (SoS) is a highly complex system which contains all the common combat forces (land forces, navy, air forces, special forces, etc.), aerospace forces, nuclear triad, C^4ISR (command, control, communication, computer, intelligence, surveillance,

reconnaissance), cyber-space forces, electro-magnetic warfare, supply & support, etc. That's why there are a lot of domains where military SoS (MSoS) are investigated for a long time, but in recent years the interest hasn't decreased.

For example, to develop a military SoS, Liu et al. (2023) focused on the strategic, operational, services and resources layers of a MSoS, following a top-down design process, and got the Unified Architecture Framework, which is designed for the modeling of a SoS. The authors got a "vision-goal-mission-capability-operation-service-resource" logic chain, which can lead to a solution-seeking as well as a warfare system-of-systems construction in order to meet the needs of the stake-holders of the SoS. Using a modularized architecture, the described domain meta-model can provide a flexibility of changing different layers in order to better find solutions. With an implementation of measurements from strategic layer down to the resources layer, the SoS model can finally leads to the requirements of the future generation equipment and the system level solution.

Yang et al. (2023) proposed a model-driven human-in-loop architecture design method for weapon systems (WS) based on the challenges and difficulties brought by system complexity and emergence that cannot be solved by traditional document-based architecture design methods. The method drives the SysML model of Magicdraw and the equipment entity model in UE4 (The Unreal Engine 4 landscape building function). The virtual battlefield environment was constructed and a communication server was developed to perform visual simulation of interoperability between WS.

Under the guidance of capability-based planning, Hu et al. (2023) addressed the generation and trade-off problem of weapon SoS (WSoS) development and planning under the double uncertainty of the scene and the key weapon system attributes using a multiobjective network-based optimization method combined with fuzzy set theory as a hybrid solution approach.

By investigating the effectiveness of air forces, Gao et al. (2022) proposed the concept of the SoS influence degree and conducted a scientific quantitative evaluation to quantitatively measure the effect of aviation equipment as the key to affecting the overall search and rescue action that are an important part of joint operations and one of the key supports for ensuring combat effectiveness.

There is an important problem for unmanned aerial vehicles (UAV) action in a hostile environment where no GPS is used. It is known that one of the main challenges of the perception component is the simultaneous localization and mapping (SLAM). So, in the context of multi-robot system and more generally for technological SoS, Mahdoui et al. (2019) proposed a multi-UAV framework for SLAM-based cooperative exploration under limited communication bandwidth.

How to integrate WS on a single platform and what will be the further enhancing the integration of multiple killing means—components of SoS are shown by Li et al. (2023). The authors also gave the brief analysis of the development direction of the combined artillery and weapon.

As we see all research fields are different completely and have unique planning and design methods. The immaturity of the researches in this area (no security aspects), the lack of citations of existing works and a lack of consensus on how the SoS architecture is described were the main features for the SoS interest mushrooming (Axelsson, 2015; Guessi, 2015).

That's why Barachini and Stary (2022, 77) underlines that applying SoS thinking is considered an effective way of handling complex adaptive systems with their self-regulation, self-management and self-organization.

Because of there are a lot of complex WS during Russian-Ukrainian war it is supposed to create a basis for analysis of systems and weapon equipment that have the key features of SoS. The mentioned sphere is absolutely new in Ukraine, so our aim is to initiate the discussions about military SoS and further development directions.

For this first stage of our research, we will use the traditional document-based analysis to systemize the key content in the field of SoS and propose the ontology for specific kinds of SoS. It is also the definitions and terms that are varies from multiple sources will be explained.

On the second stage the Ukrainian variants of SoS are expected for the analysis.

Literature review

The best way to initiate the discussion is to start with some official statements.

So, there is a following definition for SoS in International Standard (ISO/IEC/IEEE, 2019) – "Set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on its own." The such systems are man-made and are configured with one or more of the following: hardware, software, humans, procedures and facilities. It is mentioned that there is a wide variety of systems in terms of their purpose, domain of application, complexity, size, novelty, adaptability, quantities, locations, life spans and evolution.

Such wide variety allows alternative definitions with proper explanation even in later papers. From Introduction it is easy to notice both military SoS and weapon SoS, but some authors used also warfare SoS, combat SoS and autonomous vehicle SoS. As we see, the definition and next difficulties are caused (and enforced too) by the facts that: (1) the SoS are designed to wide spectrum of entities (for National level leaders, for coalitions of partners or for Multi-National Forces (MNF), for organizations (for national systems in sphere of defense and/or security, for combat forces—from Army to warfighters); (2) there are investigations in different countries and the main purpose for them is to use the results in military systems/warfare that are protected by some secrets.

Naturally that first researches in future sphere of SoS were in Army, some of them, without any doubts, were started during WWII. Kammhuber Line (Halenko, 2023) or Mid-Ocean Escort Force (Hague, 2000) had the "hardware, software, humans, procedures and facilities".

The "system-of-systems" paradigm has been defined in different ways and domains by different authors since as far back as the 1950s—research work in Bell Labs (Kelly, 1950), in the Radio Corporation of America Labs (Engstrom, 1957), in the Survey Research Center at the University of Michigan (Boulding, 1956) and other that were summarized by Goode and Machol (Goode, 1957).

And the serious practice results were obtained in space or defense (National Research Council, 1967). For example, U. S. Ballistic Missile (BM) defense efforts can be traced to the World War II years, in an attempt to respond to the German V-2 missile, which was a threat for European allies (1st result—US guided missile test, 1960). The program has received different names during the years of the Antiballistic Missile Treaty (1972–2002). U. S. Navy also was on a top of achievements for complex adaptive systems planning in the 1990s own future. Further, at the end of 20th c., focusing on the construction of weapons and equipment systems, the U. S. military successively formulated the "NASA Technology Roadmaps", "Unmanned Systems Integrated Roadmap", "Army Unified Network Plan", etc. Judging by the implementation effect, U. S. military planning has undoubtedly played a positive role in promoting the construction of weapon highly complex system that got the name of the SoS sooner—in 2015 U. S. researchers had the predominant participation in this topic (Axelsson, 2015).

The birth of the term "System of systems" is referred to Mark Maier (Maier, 1998), who proposed a unifying definition of SoS in computer science, leveraging the features that characterize the concept in this domain. He first postulated five distinguishing traits (operational and managerial independence, evolutionary and emergent behavior, and geographic distribution) and later he explained that operational independence means that each of the constituent systems (CSs) of the SoS is capable of independent operation, even when isolated from the other CSs; managerial independence means that each of the CSs can be managed independently from other CSs, that is, multiple decision-making authorities can be present (Maier, 2005).

The fact that the term emerged in computer science instead of military science sphere is evidencable because of with the evolution of warfare in the direction of networking, informatization, and intelligence, greater challenges have arisen for the planning and construction of "a collection of independent systems as parts of a larger and more complex system that delivers certain capabilities" (Boardman, 2006). So, the concept of SoS suited well to the application of a large number of distributed platforms, sensors, weapons and networks.

Materials and Methods. Methodological Framework

Due to historical evolution of Systems Engineering nowadays there are a lot of methods for modern research the SoS.

Klein and van Vliet analyzed almost 200 studies and provided an overview of the SoS architecture in this systematic review (Klein, 2013). They showed that the known approaches developed solutions for specific SoS problems but did not provide a general perspective suitable for widespread adoption.

The openness of SoS for new operational concepts and disruptive technology make the future – not only far but close even – battlefield more difficult to predict.

To cope deeper with uncertainty in planning the future design of WSoS, the U. S. Department of Defense (DoD) proposed capability-based planning (CBP) (Davis, 2002), which focuses on capacity development rather than direct measure.

There are other approaches to understand all is possible in the whole variety of SoS. A method process for collecting and organizing existing studies in a research field to respond to a series of research questions that is known as Systematic Mapping Studies (SMSs) (Budgen, 2006) was often used. For example, Axelsson in his SMS tried to structure scientific developments in SoS studying nearly 3000 articles dedicated mostly to SoS architecture, modeling and simulation (Axelsson, 2015). Some reviews were dedicated to SoS architecture (Guessi, 2015) or such quality attributes of SoS as security, performance, and interoperability (Bianchi, 2015). Olivero et al. used SMS to capture a broader range of studies and to draw a map of the research area, possibly identifying existing gaps. One of the gaps was closed by exploring the state of the art in security, privacy, and trust in SoS (Olivero, 2023). The classification of SoS according to their purpose using the identified SoS characteristics to identify new research lines was published by Nielsen et al. (Nielsen, 2015).

It is necessary to mention that SoS have a prominent piece of information technology (IT), which is based on a combination of discrete and componentized pieces of software that are loosely coupled and communicated through standard web protocols, cloud computing and infrastructure. The key approach for SoS design here is service computing and software engineering that was originated from service-oriented architecture (Papazoglou et al., 2007).

Because of such widespread SoS, we decided to restrict the number for several classes using the such distinguishing criteria as evolvability of SoS. With this restriction, the materials for our research are military, or weapon, or warfare, or combat SoS depicted in accessed works. The main focus is for U. S. DoD programs—Brigade Combat Team Modernization Program (BCT), Ballistic Missile Defense System (BMDS), Defense Information Systems Agency (DISA), for some simulations SoS and for nascency of SoS in Ukraine as a first results of warfare since 2022.

To characterize the SoS we will propose five classes that can demonstrate how the SoS was transited during its action.

Our methodological framework is an ontology approach with the distinguishing criteria.

Results

I. Abbreviations and definitions

Some definitions and abbreviations are important part of our research so we should begin with explanations.

So, $\tilde{\mathcal{A}}$ is a symbol for SoS that has some architecture (state) combined different $\mathcal{A}_i$ components of SoS (constituent systems and supporting efforts) with certain purpose.

First of all, to differ the kinds of SoS we use the following “units of measure”:

[pcs] = pieces—components of SoS, each of them was created during the separate program;

[SME] = single module for evolvability, it means that each piece of SoS can be upgraded as a separate module and upgrades of some modules in parallel are possible;

[CSs] = constituent systems of a weapon;

[SEs] = supporting efforts for uncountable components (entities, IT);
[ICS] = integrated combat system that consists of CSs that could be modernized.

Some abbreviations are depicted in the article when they are mentioned at first, but common abbreviations (that are linked with SoS in general) are below:

BMS Battle Management System;
C2 Command and Control (so C2BMS means "C2 + BMS", C2SIM means "C2 + SIM", C2S is the C2 System, C2ISR is the C2 Intelligence, Surveillance, Reconnaissance);
CN communication networks;
~IS information system (so CIS is the computer IS, GIS is the geographic IS, etc.);
JIE joint information environment;
RESE rapidly evolving security environment;
SIM training model, or system for simulations.

II. The basic principles and terms

A military SoS is typically a directed SoS, in which the "component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose" (DoD, 2008), therefore SoS is "a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities".

Such SoS can be researched through three domains: physical domain, information domain and cognitive domain (Albert, 2000).

The physical domain includes personnel, equipments, environments, and so on, and is the domain that the strikes are expanded in the circumstances of land, sea, sky and outer space, that is the domain composed of the physical platforms, and the CN linking these physical platforms.

The information domain is the domain that the information exists, in which the information is generated, collected, processed, and shared. The information existed in the information domain perhaps reflects the real things, also maybe not.

The cognitive domain exists in the consciousness of man, in which senses, recognitions, comprehensions, persuasion and worthiness are placed, and is the domain that the decision making must be made through reasoning.

Three features are general for Military SoS, they: (1) are social technical systems, (2) are purposeful systems, and (3) linked together ("cobbled together" from erstwhile previously independent pieces, or designed from scratch with specific properties) (see Table 1).

Table 1. The features of Military SoS with explanations, examples and consequences

Feature of SOS	Explanation	Examples	Consequences
sociotechnical (in physical domain)	possess some observable structure	BMDS, combat entities (HQ, BDE, BN)[1], CN, CIS	the human element provides many of the emergent capabilities and the technical elements augment, facilitate, or otherwise promote these emergent capabilities
purposeful (mission SoS)	all elements have an aim, must derive their activity from their knowledge of the SoS purpose, and their role in achieving it	to win, to intercept BM	SoS are not static structures, but dynamic entities that must drive to a desired end state that emerges from their collected purposeful activity
linked together	there is a defined and purposeful relationship among all elements of SoS	information flow models and IS models (*in information domain*), C2S and decision models (*in cognitive domain*)	it is organized a server-based architecture for SoS that allows each its component to be used (or to be tested) in physical and/or information domain individually without being in touch with all other CSs

Notes: [1]HQ—headquarters, BDE—brigades, BN—battalions.
Source: created by authors.

Military SoS design concept includes key peculiarities. Some of them are below:

- operating in dynamic and interconnected world and in a RESE (a SoS should operate in contexts for which it was not originally intended);
- being an important form in the information-based warfare and having some non-fix architecture (or state) $\tilde{\mathcal{A}}$ allowing to be transited to architecture (or state) $\tilde{\mathcal{B}}$ ($\tilde{\mathcal{C}}$, $\tilde{\mathcal{D}}$, ...);
- corresponding to the concept of evolvability (having an ability of the architecture to support possible future capabilities) to respond quickly to changing warfighter needs (see fig. 1);
- realizing C2 or other warfare principles;
- forming the whole system from interacting components that make possible control by multiple independent operators;
- investigating the best design for SoS that demands powerful IT for simulations and all possible kinds of analysis (course of action (COA) for combat applications, prediction using machine learning and deep learning etc.).

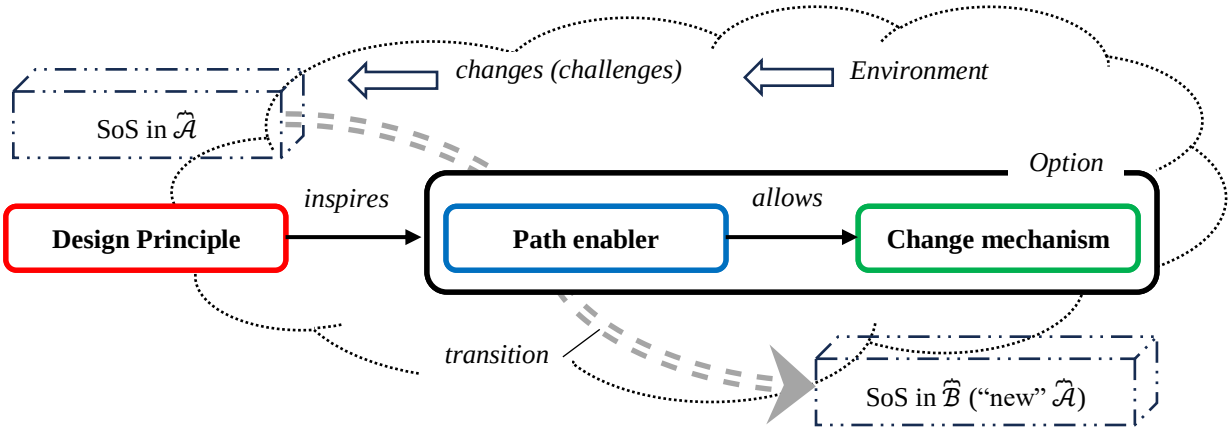


Figure 1. The diagram showing an option of SoS transition from $\tilde{\mathcal{A}}$ to $\tilde{\mathcal{B}}$ for an evolution event, where the design principle is a known term from systems engineering, the path enabler is a physical object, an action or a decision that is a key for executing of the change and the change mechanism is the method through which a SoS goes from $\tilde{\mathcal{A}}$ to $\tilde{\mathcal{B}}$

Source: created by authors from Ricci (2014) with additional elements.

Naturally, new state $\tilde{\mathcal{B}}$ (or $\tilde{\mathcal{C}}$, $\tilde{\mathcal{D}}$, ...) becomes a main state of current SoS "transforming" in $\tilde{\mathcal{A}}$.

III. The depictions of classes for military SoS and how they have transformed

There is a lot number of designed and created SoS. We have analyzed them and decided to represent all of them in five common classes. They are:

- created SoS,
- existed and transited SoS,
- combined SoS,
- evolved SoS,
- attached SoS.

We have collected some examples of SoS and systemized the key features for each of them in the Table 2.

Table 2. The variants of Military SoS with some aspects of its creation or evolution

Country(ies), institution(s)	Title, year, class	Declared target	Change of the current SoS to new architecture
P. R. C., Commanding Communications Academy, Wuhan	SoS combat SIM, 2011 (*created SoS*)	to construct a SoS (as a CN), which suppresses, breaks, destroys or controls enemies SoS	it had been just a system before evolution and became a SoS after upgrading
MNF coalition: U. S. & UK Armies; DARPA; NATO, NCI Agency; Sweden, Saab; France, Thales; Spain, GMV; Denmark, Systematic	C2SIM, 2014 (*created SoS & evolved SoS*)	to perform training, COA analysis, and mission rehearsal, working through their own C2 systems to access the SIM	a basis (a generic, consistent approach to interoperability) is the Battle Management Language; as regular, IT (software for JIE) has next evolution, for example instead of JADOCS is used JTIC2S —Joint Targeting Integrated Command and Coordination Suite
U. S., DoD	BMDS, 2004–2018, as a mission SoS (*existed and transited SoS*)	to enable a robust, layered defense against BM in all phases of flight	in 2008 due to C2BMC the THAAD interceptor battery was added
			sea-based sensors mounted on the ship has spread the possibilities to intercept BM
			land-based sensors on new terrains
U. S., DoD	BCT, 2009, as a platform SoS (*combined SoS*)	to respond quickly to changing warfighter needs in a RESE	by modularizing the structure of the BCT, interdependencies are reduced, and it is simpler to implement an evolution increment
U. S., DoD	DISA IT-SoS, 2014, with ⟨capability⟩ $\tilde{\mathcal{A}} \ni 1{,}5 \cdot 10^3$ [users] (*evolved SoS*)	to provide IT and communication support to all entities	JIE Mobile Solutions, a central information sharing solution, is designed to take the separate networks (was a reason of low efficiency for information sharing) and collect these into a shared architecture (upd. 2016–2020), $\left(\tilde{\mathcal{B}} \to \tilde{\mathcal{A}}\right) \ni 10^5$ [users]
Air Forces of Ukraine; France-UK, MBDA	Su-24M, 2023 (*attached SoS*)	to arm the Su-24M with Storm Shadow / SCALP-EG	Su-24M has become a carrier for SoS missiles that designated to operate in RESE (using C2S, GIS and other IS)

Let's show the structure of known or guessed military SoS and give the ontologies for them.

1. SoS combat SIM was created as a combination of combat entities, CIS, and CN to create the SIM on network-centric architecture (Hua Tian, 2011). For this class of created SoS the ontology is next (with units of measure:

$$\tilde{\mathcal{A}} \ni \overline{\mathcal{A}} \wedge \mathcal{A}_i \text{ [pcs]} \cup \text{[SMEs]}, \tag{1}$$

where $\overline{\mathcal{A}}$ shows that the system wasn't a SoS, so the including $\mathcal{A}_i$ into it made $\tilde{\mathcal{A}}$ as a SoS.

2. C2SIM SoS for MNF is IT to enable an environment where national C2SIM can exchange information freely and each nation's military operations can be represented accurately, each operating their own SIMs (Pullen, 2016). It is also a created SoS (that can be easily evolved SoS by changing the set of components of SoS), so the ontology is as:

$$\tilde{\mathcal{A}} \ni \wedge_{i=1}^{N} \mathcal{A}_i = \tilde{\mathcal{A}} \ni \{\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \ldots \wedge \mathcal{A}_i \wedge \ldots \wedge \mathcal{A}_N\} \text{ [pcs]} \cup \text{[SMEs]} \cup \text{[SEs]}. \tag{2}$$

C2SIM SoS, that was designed and tested according MSG-085 Standardization for C2-Simulation Interoperation (ended in 2014), was a process of maturing the technical (Technical Readiness Level (TRL)) and operational (Coalition BML) basis for MNF use of standardized C2SIM.

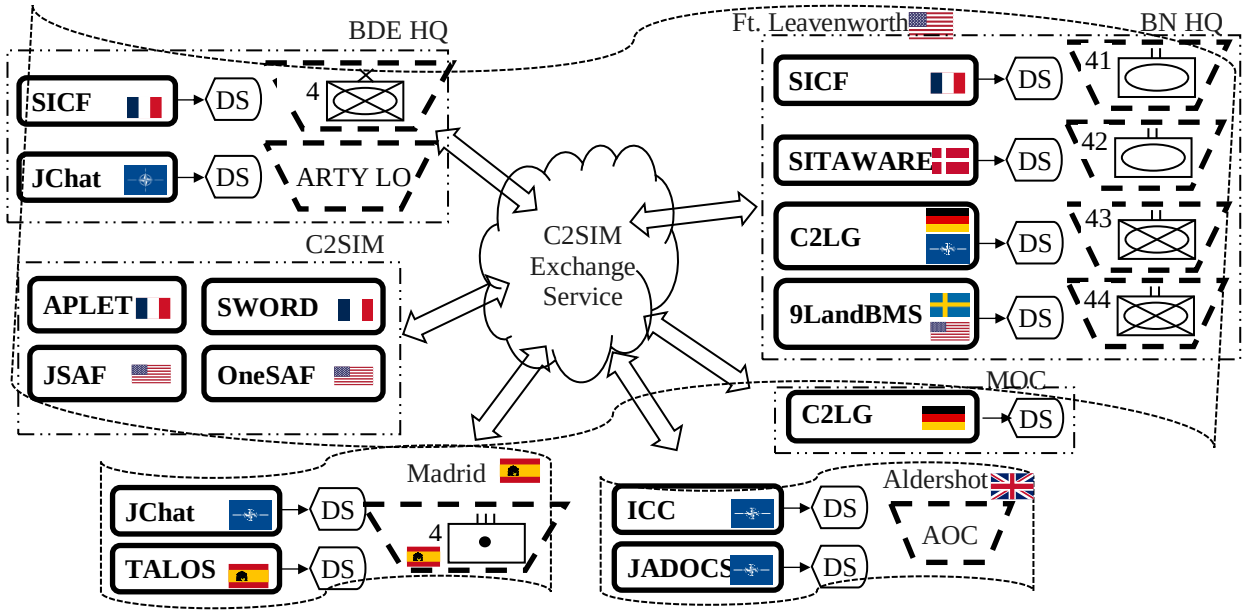


Figure 2. The SoS according to MSG-085

Notes: [1]we use thick lines for separate systems as components of SoS, thin lines for a system with determined process, f.e. to display smth (orders, reports, situation) as DS—display systems; dash for uncertain (in cognitive domain) SoS which unite platform SoS, separate systems, supporting efforts (HQs, units, warfighters), IT etc., where the humans have a key role);
[2]SoS architecture included: a set of BMS (SICF by Thales Communications, SITAWARE by Systematic, C2LG by Fraunhofer Institute for Communication, Information Processing and Ergonomics, 9LandBMS by Saab) and C2S (TALOS by GMV), a set of C2SIM (APLET, OneSAF, SWORD, JSAF), a set of IT (both JChat and ICC from NCI Agency, JADOCS from DARPA, C2SIM Exchange Service), supporting efforts (BDE HQ, BN HQs, Arty LO—artillery liaison officer, AOC—Air Operations Centre)).
Source: updated by authors using Pullen's base scheme (2016).

3. The BMDS SoS architecture included: networked sensors (space-based, ground-based and sea-based radars for target detection and tracking); ground-based and sea-based interceptor missiles for destroying a BM using either direct collision ("hit-to-kill") technology, or an explosive warhead; command, control, battle management, and CN providing the operational commanders with the needed links between the sensors and interceptor missiles (Ricci, 2014).

Architecture $\tilde{\mathcal{A}}$ (in 2004) included five long-range Ground-based Midcourse Defense (GMD) interceptors (at Fort Greely, Alaska), the Aegis SM-3 interceptors for medium-range defense of the terminal segment (near US territory), PAC-3 interceptors for short-range defense.

In Architecture $\tilde{\mathcal{B}}$ (in 2008) there were the inclusion of the Terminal High Altitude Area Defense (THAAD) interceptor battery instead of GMD interceptors to provide the BMDS with additional capability to intercept and destroy BM inside or outside the atmosphere and it was a new change mechanism (the method) through which a SoS went from $\tilde{\mathcal{A}}$ to $\tilde{\mathcal{B}}$. The path enabler for executing the change mechanism was the C2BMC, which provided the communication and data-management backbone for easily integrating THAAD within the current C2 nodes of the SoS.

The ontology is similar to (2), just the "units of measure" due to evolution increment for some pieces of existed SoS are inner.

At first there was a SoS architecture as:

$$\tilde{\mathcal{A}} \ni \bigwedge_{i=1}^{N} \mathcal{A}_i = \tilde{\mathcal{A}} \ni \{\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \ldots \wedge \mathcal{A}_i \wedge \ldots \wedge \mathcal{A}_N\} \text{ [pcs]}, \quad (4)$$

and an evolution event causes the transiting SoS to its new architecture:

$$\left(\tilde{\mathcal{B}} \to \tilde{\mathcal{A}}\right) \ni \{(\wedge_{i=1}^{N} \mathcal{A}_i \setminus \mathcal{A}_j) \wedge \mathcal{B}_j\} \text{ [pcs]}, \quad (5)$$

where $\mathcal{A}_j \notin \tilde{\mathcal{A}} = (\mathcal{A} \setminus \mathcal{A}_j)$.

Due to evolution event, it is possible to combine two or more existed SoS in a new SoS.

So, in Architecture $\tilde{\mathcal{C}}$ (Phase Adaptive Approach (PAA) initiative, 2009) there were the combination of highly mobile Aegis BMD ships (guided-missile USS Monterey ship equipped with a sophisticated Aegis radar system) in the Mediterranean Sea (since 2011) and a forward-based X-band radar on European land (in Turkey, since 2011).

The ontology looks like:

$$\left(\tilde{\mathcal{B}} \to \tilde{\mathcal{A}}\right) \ni \wedge_{i=1}^{N} \tilde{\mathcal{A}}_i = \left(\tilde{\mathcal{B}} \to \tilde{\mathcal{A}}\right) \ni \left\{\tilde{\mathcal{A}}_1 \wedge \ldots \wedge \tilde{\mathcal{A}}_i \wedge \ldots \wedge \tilde{\mathcal{A}}_N\right\} \text{ [SoS]}. \quad (6)$$

Fig. 3 shows the results of evolution events on SoS transformation (SoS evolution) where according to mentioned approach (see Fig. 1) there are "red" design principles that are well-known in system design that make capable the evolution of any system and there are "blue-and-green" options to realize the capability using a path that ensure an effect or a change.

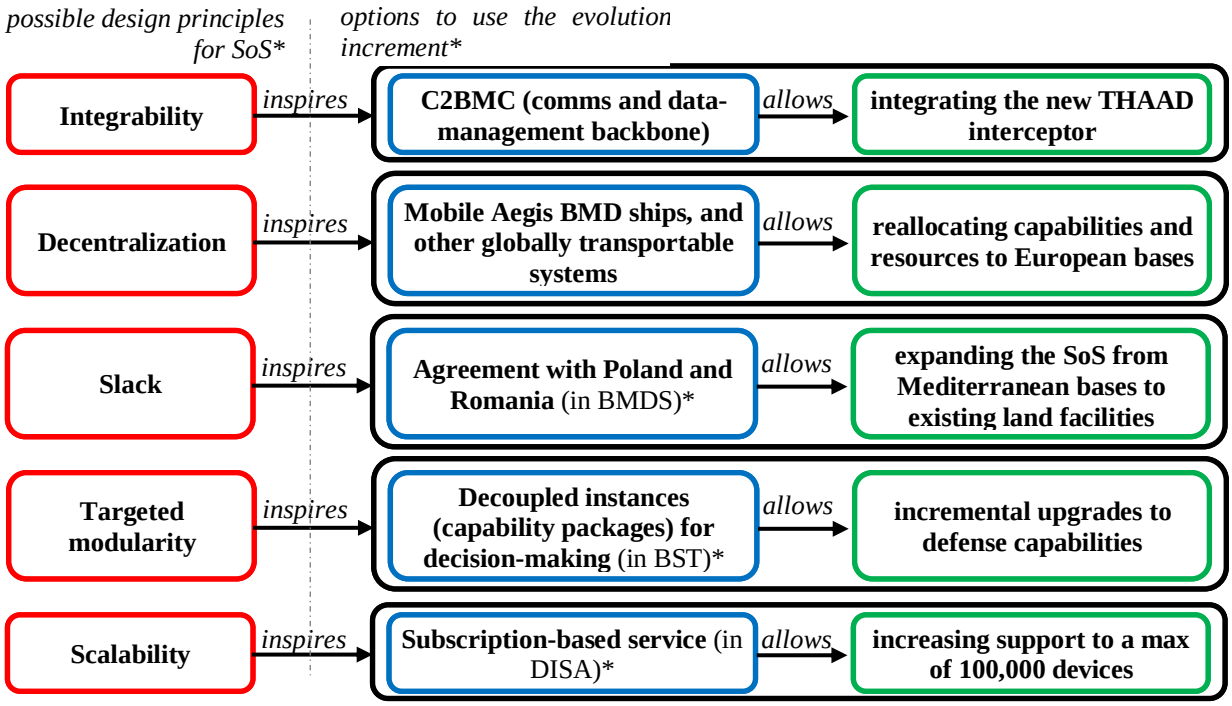


Figure 3. The examples how different SoS are transited to ensure the its evolution
Source: created by combining from using Ricci (2014) by authors, symbol (*) shows added elements.

4. The BCT (Headquarters, 2021) was announced in 2009 to replace the Future Combat System (FCS) program, 2003, which was cancelled due to cost and schedule overruns.

Similar to (4) at first there was a SoS architecture for BST as:

$$\tilde{\mathcal{A}} \ni \{\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \ldots \wedge \mathcal{A}_i \wedge \ldots \wedge \mathcal{A}_N\} \text{ [SMEs]}. \quad (7)$$

The ontology with some evolution increment (see also Fig. 3) is as:

$$\left(\tilde{\mathcal{B}} \to \tilde{\mathcal{A}}\right) \ni \{(\mathcal{A}_1 \vee \mathcal{B}_1) \wedge (\mathcal{A}_2 \vee \mathcal{B}_2) \wedge \ldots \wedge (\mathcal{A}_i \vee \mathcal{B}_i) \wedge \ldots \wedge (\mathcal{A}_N \vee \mathcal{B}_N)\} \text{ [SMEs]}. \quad (8)$$

5. The DISA IT-SoS architecture (DISA, 2014) includes CN, JIE (including the Mobile Device Management system, the Mobile Application Store, etc. IT software) and users' infrastructures (mobile devices, apps, email and other functions, and wireless networks) for securely operating and rapidly adaptation to changing technology and increasing numbers of users (to allow a diversity of current and future devices to be integrated into the SoS).

To realize the evolution demand (see Table 2) it is necessary to change some specifications in DISA IT-SoS, so the ontology looks like:

$$\mathcal{B}_i\begin{bmatrix} \cdots \\ \vdots \quad \ddots \quad \vdots \\ \cdots \end{bmatrix} = \mathcal{A}_i\begin{bmatrix} \cdots \\ \vdots \quad \ddots \quad \vdots \\ \cdots \end{bmatrix} \times K_i\begin{bmatrix} \cdots \\ \vdots \quad \ddots \quad \vdots \\ \cdots \end{bmatrix} [\text{SME}], \tag{9}$$

where $K_i[\ \ ]$ presents some "coefficients" to improve the SME (updating) according to evolution event (here the operational capability is the improving specification of SoS, see Table 2).

The second stage of the SoS evolution is (8).

6. The attached SoS means that existed integrated combat system of higher level has obtained some changes due to attached SoS that are subordinated to this ICS not becoming a SoS.

The such situations took place in Ukraine since 2022 for Zbroini syly Ukrainy (ZSU).

First of all, we underline three prerequisites for our following statements: (1) key peculiarities of SoS design concept mentioned above are justified for our examples; (2) simple weapons can also emerge through interactive collaboration (Di Pietro, 2021); (3) each AV forms an independent system that can serve a purpose on its own but, when massed together or partnered with pre-existing military formations, AVs form an SoS with the potential for emergent behavior (Klingensmith, 2018).

Using the prerequisites let's show two examples of SoS.

At first, the adaption of SCALP-EG cruise missile to Su-24M bomber of Air Forces of ZSU is an example for an attached SoS. Due to missile's specifications (TERCOM system, GPS and other sensors) it is a component of some Defense SoS. For this case the ontology would be as:

$$\left(\overline{\mathcal{C}} \to \overline{\mathcal{A}}\right) \ni \overline{\mathcal{A}} \wedge \widehat{\overline{\mathcal{B}}}\ [\text{ICS}], \tag{10}$$

where $\overline{\mathcal{A}} \ni \{\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \ldots \wedge \mathcal{A}_i \wedge \ldots \wedge \mathcal{A}_N\}$ [ICS], although $\widehat{\overline{\mathcal{B}}}$ corresponds (2).

When we also take a look on general features for military (see Table 1) we can notice how combat use of UAV and unmanned surface vehicles (USV) (such as MAGURA V5, Sea Baby) made an effect on warfare. The principles and options for SoS creation in Ukraine is shown below.

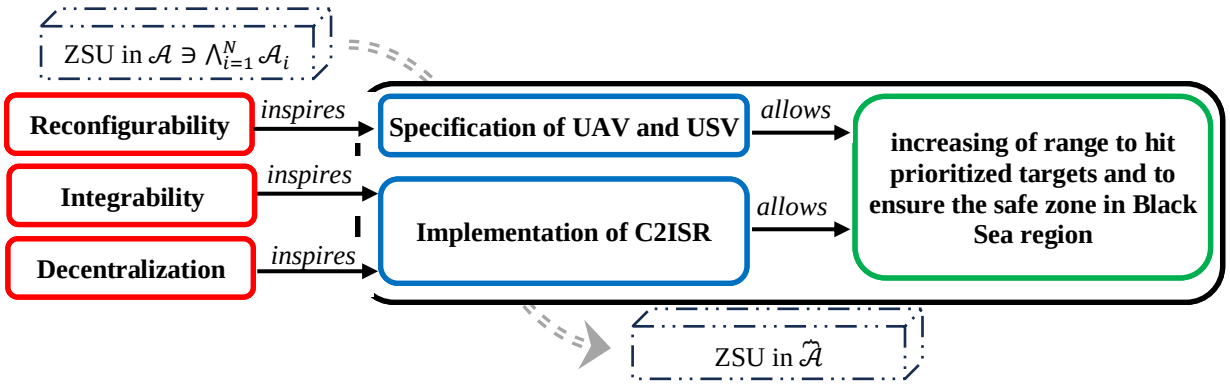


Figure 4. The emergence of SoS in ZSU (since 2022)

Source: created by authors.

For the such SoS in ZSU the ontology is following (including everything for warfare):

$$\left(\mathcal{A} \to \tilde{\mathcal{A}}\right) \ni \overline{\mathcal{A}} \wedge \tilde{\mathcal{A}} \text{ [pcs]} \cup \text{[SMEs]} \cup \text{[SEs]} \cup \text{[ICS]} \cup \text{[CSs]}. \quad (11)$$

To compare the effect is very simply, just should look at two maps—what ceasefire violations took place in Ukrainian east in 2021 (OBSE, 2022) on Fig. 5 and which tendency take place in Russia concerning secure and insecure areas for russian army of occupation (RAO). So, Russian territory that is under the strikes from ZSU in two years after 2022-03-24 (Sarcastosaurus, 2024) is on Fig. 6.

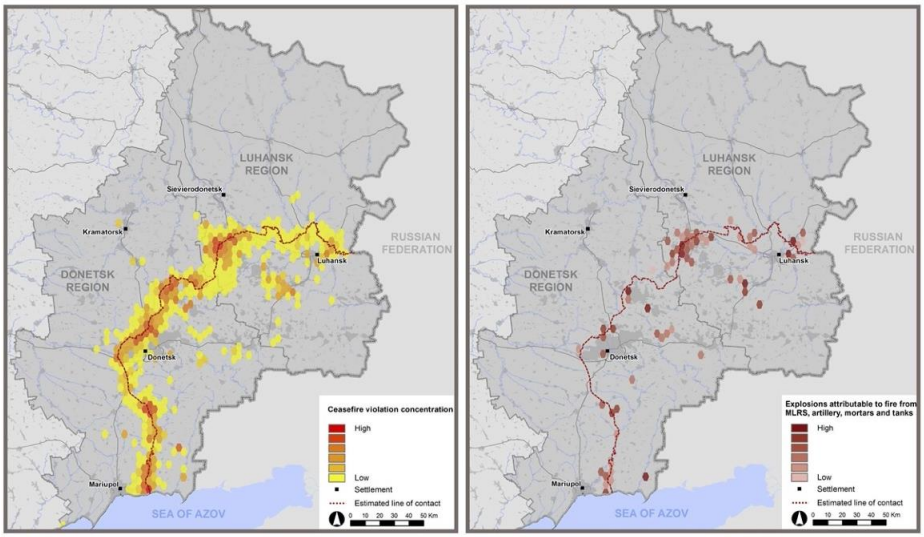


Figure 5. Insecure area on The temporarily occupied territory of Ukraine with ceasefire violations (on the left) and long-range WS use (on the right) during 2021
Source: used only a fragment of the 2021 Trends and observations sheet (OSCE, 2022).

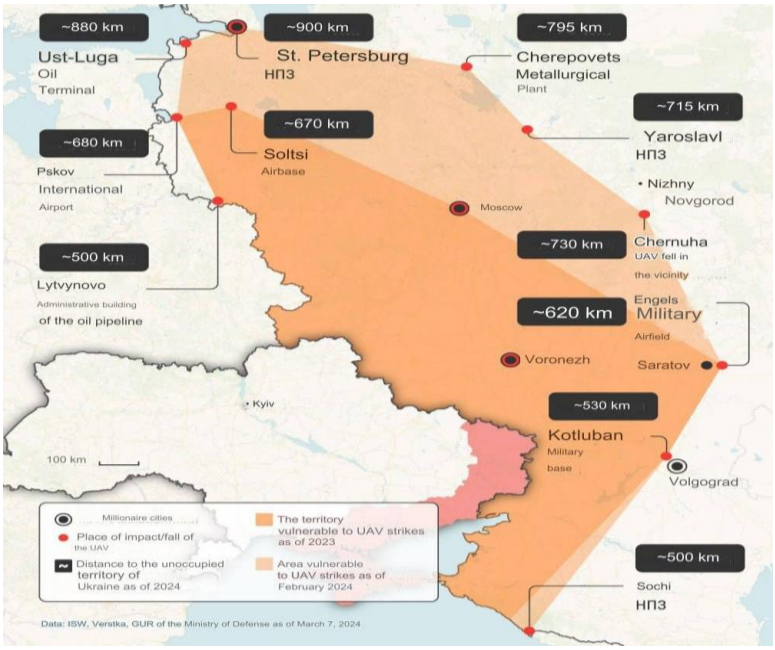


Figure 6. "Cotton belt of Russia"—the territory of Russia vulnerable to ZSU strikes
Source: probably The New Voice of Ukraine, but the map is taken from Sarcastosaurus (2024)

Second example of SoS is potential C2ISR for artillery of Ground forces of ZSU. The modern structure of artillery reconnaissance control point (Tymchuk, 2024) allows the additional processing of signals, information and data using sensors such as radar, UAV cameras, hostile artillery locator, CIS, GIS, machine learning system (MLS) and other pieces (Tymchuk, in press). The structure of C4ISR SoS is shown on Fig. 7, any CIS is an optional piece for SoS if it is possible to solve additional mission in JIE supporting such feature of SoS as purposeful one.

The ontology for such SoS is the same as (2).

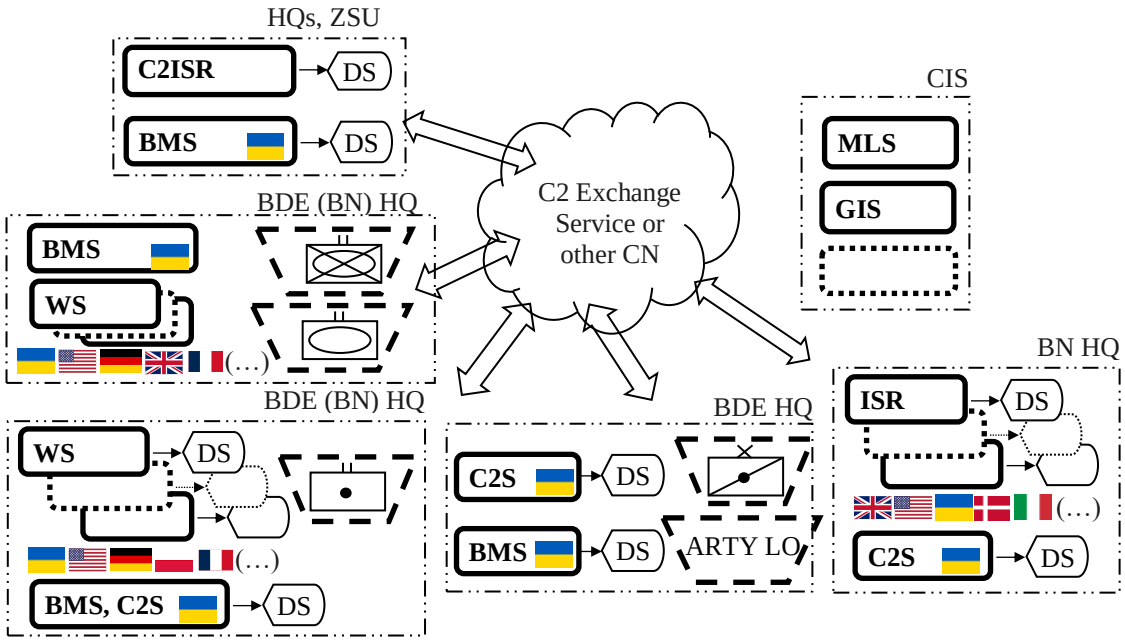


Figure 7. The probable C4ISR SoS in Ground forces of ZSU on the brigade level

Notes: SoS architecture included: BMS ("Delta" is a situational awareness and BMS) and C2S ("Kropyva" by Logika), a set of C2SIM (APLET, OneSAF, SWORD, JSAF), a variety of WS (main battle tanks, AHS Krab with Topaz artillery fire control system, AS-90 with Turret Control Computer, CAESAR with its autonomous systems, etc.), ISR (systems and sensors, f.e. 1L220UK Zoopark-3, AN/TPQ-37, AN/TPQ-37, ARTHUR, HALO, RQ-35 Heidrun, …), supporting efforts (BDE HQ, BN (division) HQs, Arty LO = artillery reconnaissance control point)).

Source: created by authors.

Discussions

The results of systematic review for military, or weapon, or combat, or warfare, or autonomous vehicles SoS allows us to divide them on five classes depending on the evolution stage of SoS – created ones, evolved ones, existed & transited ones, combined ones, and attached ones.

Such classification will be useful for next development planning of the military or weapon SoS when analyzing the key issues demanded for the best action of SoS during warfare, estimating resource allocation and time process for the design, construction and control.

Conclusion

The operation application of the weapon SoS can determine the success of a war. Ukrainian reality of war with a purpose to stop Russian military aggression and occupation have demonstrated the key and turn effects of evaluated weapon and tactics that cause the creation and action the such phenomena as SoS.

The systematic review for the main SoS in military sphere is done. The examples of SoS that are observed in ZSU are added too. It was possible to make due to unique approach of systematization SoS according to such main feature as its evolvability. The ontology for different classes that were

proposed by authors are prepared.

So, the concept of SoS will be useful for Ukrainian militarists and scientists.

A systematic review for engineering methods, processes, and tools that are used in SoS design is an important direction for further research. It is also necessary to describe the relationships of the elements in the SoS to solve the problem of complexity of a weapon or military SoS. Additional direction for further research is ways search for improvement of operational capabilities in created, combined and attached SoS in ZSU.

Recommendations

The construction of the WSoS emphasizes the interconnection and interoperability between weapons, so it's necessary to study the concept of SoS by commanders and military scientists of ZSU.

The initial steps in military SoS design should be mission tasks, capability requirements, weapon effectiveness, and economic benefits.

Acknowledgments

We thank to Main Library of Ivan Franko National University of Lviv (UAFNU) as a borrower from world-wide for access to the references used in the systematic review.

References

1. Albert, D. S., Garstka, J. J., Stein, F. P. (2000). Network centric warfare: developing and leveraging information superiority. CCRP Library of Congress Cataloging 2 in 2 Publication Data, Washington, DC.
2. Axelsson, J. A systematic mapping of the research literature on system-of-systems engineering. (2015) In: *10th System of Systems Engineering Conference* (SoSE), pp. 18–23.
3. Barachini, F., Stary, C., From digital twins to digital selves and beyond. (2022). https://doi.org/10.1007/978-3-030-96412-2_9.
4. Bianchi, T., Santos, D. S., Felizardo, K. R.: Quality attributes of systems-of-systems: a systematic literature review. (2015). In: *Proc. of the 3rd Int Workshop on Software Engineering for Systems-of-Systems*, SESoS 2015, pp. 23–30, https://doi.org/10.1109/SESoS.2015.12
5. Boardman, J. & Sauser, B. "System of Systems - the meaning of of," (2006). In 2006 IEEE/SMC *International Conference on System of Systems Engineering*, Los Angeles, California, USA, 2006, pp. 118–123. https://doi.org/10.1109/SYSOSE.2006.1652284.
6. Boulding, K. E.: General systems theory – the skeleton of science. Manage. (1956) *Science*. 2 (3), pp. 197–208.
7. Budgen, D., Brereton, P.: Performing systematic literature reviews in software engineering. (2006) In: Proc. of the *28th Int. Conf. on Software Engineering* – ICSE'06, sn, P. 1051. https://doi.org/10.1145/1134285.1134500
8. Davis, P. K. *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation*. (2002). RAND Corporation, Santa Monica.
9. Di Pietro, R., Raponi, S., Caprolu, M., Cresci, S. New Dimensions of Information Warfare. (2021). pp. 1–4. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-60618-3_1.
10. DISA, Enabling The Joint Information Environment (JIE) (2014). 5 May. https://disa.mil/-/media/Files/DISA/About/JIE101_000.pdf.
11. Engstrom, E. W. "Systems engineering: A growing concept" (1957). In *Electrical Engineering*, Vol. 76, No. 2, pp. 113-116, Feb. 1957, doi:10.1109/EE.1957.6442968.
12. Gao, Y., H. Liu, F. Niu, Y. Tian, J. Wang & W. Cheng. Search and rescue system-of-systems influence degree evaluation of aviation equipment based on simulation. Scientific Reports.

(2022) 12:22384. 20 pgs. https://doi.org/10.1038/s41598-022-26098-x
13. Goode, H. and Machol, R. (1957). Systems Engineering: An Introduction to the Design of Large-Scale Systems. 551 pp, McGraw-Hill book co, Inc. New York.
14. Guessi, M., Neto, V. V. G., Bianchi, T., Felizardo, K. R., Oquendo, F., Nakagawa, E. Y. A systematic literature review on the description of software architectures for systems of systems. (2015). In: *Proc. of the ACM symp. on applied computing*, Vol. 13–17-April, No. V, pp. 1433–1440. https://doi.org/10.1145/2695664.2695795.
15. Hague, A. (2000). The Allied Convoy System 1939–1945. Naval Institute Press.
16. Halenko, I., Tymchuk, O., Tymchuk, V. Kammhuber Line as a prototype for a consolidation information system. In Ukrainian Army: modern and historical aspects. (2023). 30 Nov. Ukraine, Kyiv, National Defense University of Ukraine. *Proc. of 4th Int Conf.*, Kyiv, 2023. P. 332 [in Ukrainian].
17. Headquarters, Department of the Army. FM 3-96. Brigade Combat Team (2021). 460 p.
18. Hu, C., X. Wang, M. Li, and J. Jiang. Navigating uncertainty in weapon system-of-systems planning: a hybrid multiobjective network-based optimization and fuzzy set approach. International journal of computational intelligence systems (2023) 16:136. 21 pgs. https://doi.org/10.1007/s44196-023-00313-7.
19. Hua Tian, and Zhi-chun Gan (2011). A Network-Centric Architecture for Combat System-of-Systems Model. In L. Qi (Ed.): Information and Automation: International Symposium, ISIA 2010, Guangzhou, China, Nov. 10-11, 2010, CCIS 86, pp. 411-417, 2011 [from Springer-Verlag Berlin Heidelberg 2011] [from www.archive.org].
20. ISO/IEC/IEEE, "ISO/IEC/IEEE 21839:2019." ISO/IEC JTC 1/SC 7 Systems and software engineering – System of systems (SoS) considerations in life cycle stages of a system. IEEE, (2019). Accessed: Feb. 24, 2024. [Online]. Available: https://www.iso.org/standard/71955.html
21. Kelly, M. J. (1950). The Bell Telephone Laboratories-An Example of an Institute of Creative Technology. Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, 203(1074), 287–301. http://www.jstor.org/stable/98407.
22. Klein, J., van Vliet, H.: A systematic review of system-of-systems architecture. (2013). In: QoSA 2013 – *Proc. of the 9th Int. ACM Sigsoft conf. on the Quality of Software Architectures*, pp. 13–21. https://doi.org/10.1145/2465478.24.
23. Klingensmith, K., Madni, A. M. Resilience Concepts for Architecting an Autonomous Military Vehicle System-of-Systems. In A.M. Madni et al. (eds.) (2018). Disciplinary Convergence in Systems Engineering Research, Springer International Publishing AG. https://doi.org/10.1007/978-3-319-62217-0_6.
24. Li T., H. Chen, L. Kong, J. Li, and Y. Yang. The development of the combined weapon of light and high maneuvering artillery from the view of the warfare object. (2023). In S. Long and B. S. Dhillon (Eds.): *Man-machine-environment system engineering: Proc. of the 23rd int. conf. on MMESE*, Lecture Notes in Electrical Engineering, 1069, pp. 303–308. https://doi.org/10.1007/978-981-99-4882-6_43.
25. Liu N., J. Wang, Y. Zhang, D. Li, and M. Ju. Top-down military system-of-systems design using MBSE based on UAF: A Case Study. (2023). In D. Krob et al. (Eds.): CSD&M 2023, LNEE 1085, pp. 210–219. https://doi.org/10.1007/978-981-99-6511-3_19
26. Mahdoui, N., V. Frémont, E. Natalizio. Communicating multi-UAV system for cooperative SLAM-based exploration. (2020) *Journal of Intelligent & Robotic Systems*. 98:325–343. https://doi.org/10.1007/s10846-019-01062-6.
27. Maier, M. "Architecting principles for system-of-systems," (1998). Syst. Eng., Vol. 1, No. 4, pp. 267–284, 1998. https://doi.org/10.1002/(SICI)1520-6858(1998)1:4%3C267::AID-SYS3%3E3.0. CO;2-D.

28. Maier, M. W. Research challenges for systems-of-systems context: collaborative systems. (2005). In: Aerospace Corporation, pp. 1–6. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1571630&isnumber=33257.
29. National Research Council (1967). Applied Science and Technological Progress: A Report to the Committee on Science and Astronautics, U.S. House of Representatives. Washington, DC: The National Academies Press. https://doi.org/10.17226/21281.
30. Nielsen, C. B., Larsen, P. G., Fitzgerald, J., Woodcock, J., Peleska, J. Systems of systems engineering: basic concepts, model-based techniques, and research directions. (2015). *ACM Comput. Surv*. 48(2), 1–41. https://doi.org/10.1145/2794381.
31. Olivero, M. A., A. Bertolino, F. J. Dominguez-Mayo, M. J. Escalona, I. Matteucci. A systematic mapping study on security for systems of systems. (2023). Int J of Information Security, 31 pgs. https://doi.org/10.1007/s10207-023-00757-0.
32. OSCE - Organization for Security and Co-operation in Europe, (2021). Trends and observations from the Special Monitoring Mission to Ukraine, 4 February 2022, https://www.osce.org/special-monitoring-mission-to-ukraine/511327.
33. Papazoglou, M. P., Traverso P., Dustdar S. Leymann F. (2007). Service-oriented computing: State of the art and research challenges. *Computer*, 40 (11), 38–45.
34. Pullen, J. M. (2015). Enabling Military Coalition Command and Control with Interoperating Simulations as a System of Systems, In Simulation and Modeling Methodologies, Technologies and Applications: International Conference, SIMULTECH 2015 Colmar, France, July 21-23, 2015, In Advances in Intelligent Systems and Computing, 442, M.S. Obaidat et al. (eds.), Springer International Publishing, Switzerland, 2016, pp. 157–174, DOI: 10.1007/978-3-319-31295-8_10.
35. Ricci, N., D. H. Rhodes, A. M. Ross (2014), Evolvability-Related Options in Military Systems of Systems, In Procedia Computer Science, 28, pp. 314–321, from Conference on Systems Engineering Research (CSER 2014), CA, March 21-22, 2014, doi: 10.1016/j.procs.2014.03.039
36. Sarcastosaurus, Ukraine War. (2024). 13 March: Me and my Questions..., https://xxtomcooperxx.substack.com/p/ukraine-war-13-march-2024-me-and?utm_source=post-email-title&publication_id=1535927&post_id=142570636&utm_campaign=email-post-title&isFreemail=true&r=1sg7kk&triedRedirect=true&utm_medium=email.
37. Tymchuk, V. The structural and parametric synthesis of combat control system (on the example of the artillery reconnaissance control point) in the conditions of asymmetrical forces distribution for two-loop optimization. (2024). *Trudy universytetu*. 5(180) (in Ukrainian).
38. Tymchuk, V., “Methodology for processing of data reductance in hostile artillery locator system,” in Modern Information Technologies in the Sphere of Security and Defence, in press.
39. Yang H., Zhun Xia, Yanqing Chen, Linqun Zhu, Luohao Dai, Ruotian Xu, Gui Ying Sun, Hongyang Yu, Wenting Xu (2023). Research on visual simulation for complex weapon equipment interoperability based on MBSE. *Multimedia Tools and Applications*. 2024. 83:13463–13482. https://doi.org/10.1007/s11042-023-15950-5.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.10

Methodological approach to determining the nomenclature of mobile assets for acomplishment the tasks of nuclear threat detection and assessment

Kostiantyn Furmanov
PhD in Military Science, senior staff scientist
Chief of scientific-research derectorate
The Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitroflotskyi Avenue, Kyiv, Ukraine
e-mail: k.furmanov16@gmal.com
ORCID: 0000-0002-0049-8959

Oleh Hutchenko
PhD in Military Science, senior staff scientist
Chief of scientific-research branch
The Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitroflotskyi Avenue, Kyiv, Ukraine
e-mail: gutchenko.oleg@gmail.com
ORCID: 0000-0002-1724-6918

Kateryna Hutchenko
PhD in medicine
Scientist
The Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitroflotskyi Avenue, Kyiv, Ukraine
e-mail: dr.gutches@ukr.net
ORCID: 0009-0008-6377-7745

Abstract. The relevance of the article is due to the fact that in the context of countering large-scale aggression, Ukraine's actions to de-occupy the captured territories and implementing its strategic course to join the European community and NATO, there are potential threats from the russian federation. Continuing its hostile rhetoric, terrorising Ukraine with missile strikes, the russian leadership threatens to use nuclear weapons, which poses the highest level of danger and can lead to large-scale radiation contamination (Lessons of the russian-Ukrainian war 2022: military aspects, 2022).

Taking into consideration this state of the security environment, it is necessary to respond effectively to nuclear threats and ensure reliable protection of troops, which, in their turn, should be ready to act in radiation contamination conditions. This requires the Armed Forces of Ukraine to effectively train military units of chemical, biological, radiological and nuclear defence capable of performing their assigned tasks and, in the further future, to be ready to detect and assess nuclear threats in joint actions (operations) with the units of NATO member states. All this requires solving problematic issues related to the nomenclature of chemical, biological, radiological and nuclear defence equipment of the Armed Forces of Ukraine to ensure the required level of protection of troops. Especially challenging tasks in the current environment are the detection and assessment of the chemical, biological and radiological situation of the movement routes and areas of troops' concentration, the covering of troops and facilities of the Armed Forces of Ukraine from reconnaissance and destruction by modern precision weapons, and the liquidation of the chemical,

biological and radiological contamination consequences. To a large extent, the maximum reduction of troop losses during actions in conditions of chemical, biological and radiological contamination is ensured by the application of existing and prospective assets of chemical, biological, radiological and nuclear defence However, it is impossible to make reasonable decisions on the nomenclature of mobile chemical, biological, radiological and nuclear defence equipment without determining the amount of losses of chemical, biological, radiological and nuclear defence equipment during the conduct of tasks in the operations of the Armed Forces of Ukraine in accordance with the trends in the development of the Armed Forces of Ukraine, forms and methods of warfare, and assets of combat actions.

To solve this problematic issue, we propose a methodological approach to determining the nomenclature on the example of mobile assets to fulfil the scope of tasks for detecting and assessing nuclear threats.

The methodological approach will allow to formulate substantiated practical recommendations regarding the procedure for determining the nomenclature of chemical, biological, radiological and nuclear protection assets. The article presents the nomenclature of nuclear threat detection and assessment, which depends on the scope of detection and assessment tasks and the capabilities of assets used to accomplish these tasks. The materials of the article may be useful for officials of military command and control bodies involved in planning chemical, biological, radiological and nuclear (CBRN) defence during combat actions..

Keywords: nuclear threats, assets, scope of tasks, capabilities, nomenclature, characteristics.

Introduction

The adoption of the Treaty on the Non-Proliferation of Nuclear Weapons in 1970 divided the world into those countries that were the official possessors of nuclear weapons and the rest of the states. About 90% of the world's nuclear arsenals are approximately equally distributed among two of these countries - russia and the United States.

At this time, russian federation's nuclear arsenal is part of the nonstrategic nuclear forces (NSNF) (land, air, and sea components), which include units of the land forces, the air space forces, and the navy, which are equipped with operational-tactical (tactical) nuclear weapons.

The russian armed forces have about 2,000 non-strategic nuclear warheads in their arsenal, and 760 warhead can be mounted on cruise, anti-submarine and anti-aircraft missiles, torpedoes and submarine depth charges, aircraft carriers, cruisers, destroyers, frigates, corvettes, aircraft and naval aviation helicopters, 570 warhead on aircraft, including Tu-22M3, Su-24M and Su-34 aircraft. All of these aircraft can carry free-fall nuclear bombs, and the Tu-22M3 can also carry the X-22 Burya.

The targets of the russian federation's nuclear weapons can be defence areas in enemy breakthrough areas, cities that are conducting circular defence, and buildings of the state administration (defence forces), with the aim of breaking through the defence, impairing control and destroying the state leadership.

russian NSNF have on their armament:

nuclear artillery ammunition – a supplement to conventional artillery, capable of qualitatively increasing its capabilities and effectiveness against enemy defensive formations, rear area objects, as well as in counterbattery combat;

tactical missiles (operational-tactical missiles), which form the basis of the tactical nuclear weapons arsenal.

The most dangerous is the use of tactical nuclear ammunition that can be mounted on ballistic and cruise missiles such as Iskader-M, Tochka-U, Kinzhal and Kalibr-PL (NK) with a yield of more than 10 kt in TNT equivalent, which can lead to the total destruction of structures within a radius of up to 1 km, damage to up to 80% of personnel and the population not in shelters, as well as failure of

radio-electronic and electrotechnical equipment within a radius of up to 2.5 km (Methodology for Assessing the Situation in Technogenic and Natural Emergencies, 2018).

This testifies to the relevance and importance of detecting and assessing nuclear threats to troops in order to create favourable conditions for successful training and combat actions.

The detection and assessment of nuclear threats is organised and conducted to timely inform troops about the factors of destruction, in particular radioactive contamination at command posts, travel routes, supply routes, evacuation routes, in areas of concentration and operations of troops. (Doctrine on Chemical, Biological, Radiological and Nuclear Protection of Troops (Forces), 2020). The task is conducted by regular and specially trained non-staff chemical, biological, radiological intelligence units by collecting data on the chemical, biological, radiological (CBR) situation along the routes of advance, areas and directions of troops' actions.

Despite the possible scale of nuclear threat consequences and their negative impact on military operations, currently that the Armed Forces of Ukraine (AFU) have a full nomenclature of nuclear threat detection and assessment capabilities assets to perform the full scope these tasks requires clarification.

This affects the completeness of nuclear threat detection and assessment to support decision-making by military command and control bodies. Thus, it is obvious that the detection and assessment of nuclear threats in the current conditions of combat actions is of special importance.

Thus, in order to increase the provision of the Armed Forces of Ukraine with the full nomenclature of protection assets against nuclear threats, there appears a necessity to resolve the task of determining the number of assets for detecting and assessing nuclear threats of the *i*-type, taking into account the current peculiarities of the conditions for performing these tasks in an operation (combat actions). For this It is proposed to expand the list of indicators for assessing the functioning of nuclear threat detection and assessment assets by implementing additional time indicators and completeness of nuclear threat detection and assessment tasks (on the example of chemical, biological, radiological intelligence), and to improve the method of determining the capabilities of these assets using the importancy coefficients of individual samples of assets. This will allow to determine their nomenclature for performing the scope of tasks in conditions of a high level of threat of use of nuclear weapons by the enemy.

Materials and Methods

As part of the methodological approach to determining the nomenclature of nuclear threat detection and assessment assets, the indicators and criteria for determining the nomenclature and number of these assets were selected and substantiated.

As the criteria, the minimum cost of the c_i i -type CBRN protection asset is adopted, which characterises the degree of goal achievement, which is to perform tasks on detection and assessment of nuclear threats in a timely manner and in a full scope.

The methodological approach to determining the nomenclature of CBRN protection assets, in particular nuclear threat detection and assessment assets, involves four stages of calculations.

At the 1st stage, the initial data required for calculations are generated, in particular: the nuclear threat detection and assessment tasks to be performed; operational force grouping (OFG) total operational square, *S*, km2; cost of one machine for detection and assessment of nuclear threats c_i , *i*-type, UAH; given time for detection and assessment of nuclear threats, T_{det}, hours; value of nuclear threat detection and assessment machines' relative losses per one hour of functioning, k_{loss}.

For determining the degree of compliance capabilities of nuclear threat detection and assessment equipment vailable nomenclature with the scope of tasks assigned to them (on the example of CBR reconnaissance tasks), the approximate capabilities of the available CBR reconnaissance units of the CBRN Defence Battalion (bCBRNd) of the operational force

grouping (OFG) and the required scope of CBR reconnaissance tasks during combat operations were determined (Tactical calculations of service tasks CBRN Defence, 2017):

the capabilities of CBR intelligence units of the bCBRNd OFG are: $S_{розвід}^{можл} = 6100\ км^2$;

the approximate scope of CBRN reconnaissance tasks (square of radiation reconnaissance of OFG combat areas) where as a result of tactical nuclear weapons use is accepted $S_{розвід}^{потр} = 8640\ км^2$.

Table 1 shows an example of radioactive contamination zones' average values size resulting from explosions of tactical nuclear weapons of the 3VB4 (3VB11) type with a yield of 2 kT in TNT equivalent by deploying 240 mm 2S4 Tulip self-propelled mortar. The 2S4 Tulip self-propelled mortar has a 20-round ammunition capacity.

Table 1. Sizes of radioactive contamination zones as a consequence of tactical nuclear weapons type 3B4 (3B11) explosions with a yield of 2 kT in TNT equivalent (example)

Conditions	Average size value of the radioactive contamination zone as a result of a nuclear explosion, km^2			
	Zone A (moderate contamination)	Zone B (highly contaminated)	Zone C (dangerous contamination)	Zone D (extremely dangerous contamination)
Contamination at wind speeds of 3-5, m/s	up to 14 km in length, up to 9.3 km in width, with a total area of up to 44.1 km^2	up to 4.8 km in length, up to 4.5 km in width, with a total area of up to 15.1 km^2	up to 2.4 km in length, up to 2.3 km in width, with a total area of up to 7.5 km^2	up to 1.2 km in length, up to 1.3 km in width, with a total area of up to 3.5 km^2
Radiation doses that personnel may receive in the case of open location on the ground, Rad	23	245	410	1300

At the 2nd stage, "Capabilities determination of nuclear threat detection and assessment assets and scope of tasks" is conducted:

in block 2.1, where the capabilities of available nomenclature and number of assets for detection and assessment of the *i*-type $\left(i = \overline{1,5}\right)$ nuclear threats are calculated:

$$S_{розвід\ i}^{можл} = v_{i\ розвід} \cdot x_{i\ розвід} \cdot (1 - k_{втр}) \cdot T_{розвід}\ , \qquad (1)$$

where $S_{розвід\ i}^{можл}$ – is an area's size to be reconnoitered by the available assets for detecting and assessing nuclear threats of the *i*-type; $v_{i\ розвід}$ – is capability of detecting and assessing nuclear threats with a one *i*-type CBR reconnaissance vehicle, km^2/hour; $x_{i\ розвід}$ – is an *i*-type CBR reconnaissance vehicles' available number, units; $k_{втр}$ – is a value of relative losses CBR reconnaissance vehicles per hour of nuclear threats detection and assessment; $T_{розвід}$ – is the set time for CBR reconnaissance, hours;

in block 2.2, where the necessary area of reconnaissance *i*-type CBR's areas (the scope of nuclear threat detection and assessment tasks) in the area of combat actions of the OFG is calculated:

$$S^{потр}_{розвід\ i} = \sum_{\alpha=1}^{k} S_{розвід\ \alpha i}, \quad (2)$$

where $\sum_{\alpha=1}^{k} S_{розвід\ \alpha i}$ – is areas' sum of k-operational areas of OFG units (components), km^2; $\left(\alpha = \overline{1,k}\right)$.

Further, the value of the necessary scope of tasks for detecting and assessing nuclear threats $S^{потр}_{розвід\ i}$ is compared with the capabilities' value $S^{можл}_{розвід\ i}$ of the i-th type available number of assets. If the accepted conditions $S^{можл}_{розвід\ i} \geq S^{потр}_{розвід\ i}$ correspond, it is considered that the capabilities of the available nomenclature and number of i-type nuclear threat detection and assessment assets to ensure OFG are sufficient.

If the mentioned condition is not fulfilled, we determine the nomenclature and nuclear threat detection and assessment assets' number that are capable of fulfilling the scope of nuclear threat detection and assessment tasks, for which purpose, at the **3rd stage**, we conduct "Importance coefficients' determination of of nuclear threat detection and assessment assets according to their indicative tactical and technical characteristics (TTC) by the taxonomy method" (example) by using CBR reconnaissance vehicles TTC (Table 2) (Zahorka, 2004).

Table 2. Value matrix α_{ij} of *i*-type CBR reconnaissance vehicles

CBR reconnaissance vehicle's type, i, $\left(i = \overline{1,5}\right)$	j-vehicle's TTC, $\left(j = \overline{1,5}\right)$				
	Radiological situation control radius, km	Capabilities for detecting the radiological situation in the areas, km^2	Capabilities to assess the radiological situation, areas, km^2	Power reserve, km	Engine power, HP
RKhM-4-01	$\alpha_{11}=2$	$\alpha_{12}=30$	$\alpha_{13}=9$	$\alpha_{14}=500$	$\alpha_{15}=250$
RKhM-4	$\alpha_{21}=3$	$\alpha_{22}=32$	$\alpha_{23}=10$	$\alpha_{24}=600$	$\alpha_{25}=260$
RKhM-1K	$\alpha_{31}=1$	$\alpha_{32}=36$	$\alpha_{33}=11$	$\alpha_{34}=400$	$\alpha_{35}=240$
BRDM-2cbr	$\alpha_{41}=4$	$\alpha_{42}=40$	$\alpha_{43}=12$	$\alpha_{44}=750$	$\alpha_{45}=140$
Kozak-2M1	$\alpha_{51}=6$	$\alpha_{52}=50$	$\alpha_{53}=20$	$\alpha_{54}=650$	$\alpha_{55}=300$

Since the matrix elements have different units of measurement, they are brought to a standardised (normalised) form using the formula:

$$\alpha^{*}_{ij} = \frac{\alpha_{ij} - \alpha_{j\eta\theta}}{\sigma_j}, \quad (3)$$

where is the arithmetic average of the matrix *j*-column elements according to Table 1:

$$\alpha_{j\eta\theta} = \frac{\sum_{i=1}^{5} \alpha_{ij}}{5}; \quad (4)$$

unbiased estimate of the average square deviation (dispersion) from arithmetic average of these elements (TTX) of matrix each column, Table 1:

$$\overline{\sigma}_j^2 = \frac{\sum_{i=1}^{5} \left(\alpha_{ij} - \alpha_{j\eta\theta}\right)^2}{5}. \quad (5)$$

Results of reducing to a standardised form the technical characteristics of a OFG CBR reconnaissance vehicle (assets) by using formula (3) are summarised in Table 3. The noted results indicate that after centring $\alpha_{ij} - \alpha_{j\eta\theta}$ and normalisation ($\overset{*}{\alpha}_{ij}$) obtained elements α^*_{ij} the obtained elements can already be compared with each other, in contrast to the initial comparability of element values α_{ij}.

Table 3. Normalised values α^*_{ij} of CBR reconnaissance vehicle (asset) technical characteristics

CBR reconnaissance vehicle's type, *i*, $\left(i=\overline{1,5}\right)$	*j*- vehicle's TTC, $\left(j=\overline{1,5}\right)$				
	1	*2*	*3*	*4*	*5*
RKhM-4-01	$\alpha^*_{11}=0,62$	$\alpha^*_{12}=0,95$	$\alpha^*_{13}=0,77$	$\alpha^*_{14}=0,59$	$\alpha^*_{15}=0,20$
RKhM-4	$\alpha^*_{21}=0,10$	$\alpha^*_{22}=0,70$	$\alpha^*_{23}=0,54$	$\alpha^*_{24}=0,14$	$\alpha^*_{25}=0,37$
RKhM-1K	$\alpha^*_{31}=1,14$	$\alpha^*_{32}=0,20$	$\alpha^*_{33}=0,31$	$\alpha^*_{34}=1,33$	$\alpha^*_{35}=0,03$
BRDM-2cbr	$\alpha^*_{41}=0,41$	$\alpha^*_{42}=0,30$	$\alpha^*_{43}=0,09$	$\alpha^*_{44}=1,25$	$\alpha^*_{45}=1,65$
Kozak-2M1	$\alpha^*_{51}=1,45$	$\alpha^*_{52}=1,56$	$\alpha^*_{53}=1,72$	$\alpha^*_{54}=0,51$	$\alpha^*_{55}=1,04$

After using formula (3), a normalised matrix with dimensionless elements is formed:

$$A^* = \left\| \begin{matrix} \alpha^*_{11}\alpha^*_{12}\alpha^*_{13}\alpha^*_{14}\alpha^*_{15} \\ \alpha^*_{21}\alpha^*_{22}\alpha^*_{23}\alpha^*_{24}\alpha^*_{25} \\ \alpha^*_{31}\alpha^*_{32}\alpha^*_{33}\alpha^*_{34}\alpha^*_{35} \\ \alpha^*_{41}\alpha^*_{42}\alpha^*_{43}\alpha^*_{44}\alpha^*_{45} \\ \alpha^*_{51}\alpha^*_{52}\alpha^*_{53}\alpha^*_{54}\alpha^*_{55} \end{matrix} \right\| = \left\| \begin{matrix} 0{,}62\ 0{,}95\ 0{,}77\ 0{,}59\ 0{,}20 \\ 0{,}10\ 0{,}70\ 0{,}54\ 0{,}14\ 0{,}37 \\ 1{,}14\ 0{,}20\ 0{,}31\ 1{,}33\ 0{,}03 \\ 0{,}41\ 0{,}30\ 0{,}09\ 1{,}25\ 1{,}65 \\ 1{,}45\ 1{,}56\ 1{,}72\ 0{,}51\ 1{,}04 \end{matrix} \right\|. \quad (6)$$

Further, at this stage, the importance coefficients of the respective TTC each OFG CBR reconnaissance vehicle (assets) by using the method of expert survey were determined . The set of these importance coefficients could be reflected by a matrix of the such form:

$$B = \left\| \begin{matrix} B_1 0..0..0..0 \\ 0..B_2 0..0..0 \\ 0..0..B_3 0..0 \\ 0..0..0..B_4 0 \\ 0..0..0..0..B_5 \end{matrix} \right\| = \left\| \begin{matrix} 0,1..0..0..0..0 \\ 0..0,3..0..0..0 \\ 0..0..0,2..0..0 \\ 0..0..0..0,1..0 \\ 0..0..0..0..0,3 \end{matrix} \right\|, \quad (7)$$

where B_j – "weight " *j*-их TTC of analysed CBRN reconnaissance vehicle, in this case:

$$\sum_{j=1}^{5} B_j = 1. \tag{8}$$

Further, the task is reduced to multiplying the normalised A^* (6) and diagonal B (7) matrices, while the matrix colums' number A^* should be equal to the matrix rows' number B. After multiplying the normalised A^* and diagonal B matrices, the "weighted" matrix A^z is obtained:

$$A^z = \begin{Vmatrix} \alpha^z_{11} \alpha^z_{12} \alpha^z_{13} \alpha^z_{14} \alpha^z_{15} \\ \alpha^z_{21} \alpha^z_{22} \alpha^z_{23} \alpha^z_{24} \alpha^z_{25} \\ \alpha^z_{31} \alpha^z_{32} \alpha^z_{33} \alpha^z_{34} \alpha^z_{35} \\ \alpha^z_{41} \alpha^z_{42} \alpha^z_{43} \alpha^z_{44} \alpha^z_{45} \\ \alpha^z_{51} \alpha^z_{52} \alpha^z_{53} \alpha^z_{54} \alpha^z_{55} \end{Vmatrix}, \tag{9}$$

where the element of the "weighted" matrix $\alpha^z_{ij} = \alpha^*_{ij} \cdot B_j$ is equal to the scalar product of matrix A^* (6) *i*-vector-row by *j*-vector-column of diagonal matrix B (7).

The results of multiplying the normalised A^* and diagonal matrix B are summarised in Table 4.

Table 4. CBR reconnaissance vehicle (assets) coefficients α^z_{ij}

CBR reconnaissance vehicle's type, *i*, $(i = \overline{1,5})$	*j*- vehicle's TTC, $(j = \overline{1,5})$				
	1	*2*	*3*	*4*	*5*
RKhM-4-01	*0,062*	*0,285*	*0,154*	*0,059*	*0,06*
RKhM-4	*0,01*	*0,21*	*0,108*	*0,014*	*0,042*
RKhM-1K	*0,114*	*0,06*	*0,062*	*0,133*	*0,396*
BRDM-2cbr	*0,041*	*0,09*	*0,018*	*0,125*	*0,495*
Kozak-2M1	*0,145*	*0,468*	*0,344*	*0,051*	*0,312*

After "rolling up" the TTC importance coefficients α^z_{ij}, the complex indicators A^z_i of *i*- type CBRN reconnaissance vehicle (assets) are obtained:

$$A^z{}_{i\ розвід} = \sqrt{\left(\alpha^z{}_{11}\right)^2 + \left(\alpha^z{}_{12}\right)^2 + \ldots + \left(\alpha^z{}_{ij}\right)^2 + \ldots + \left(\alpha^z{}_{i5}\right)^2}. \tag{10}$$

Further, for each type of the above-mentioned CBR reconnaissance vehicle (assets), their importance coefficients are determined $K_{i\ розвід} = \frac{A^z_{i\ розвід}}{\sum_i^5 A^z_{i\ розвід}}$.

At the 4th stage, "Nomenclature and movable vehicles' number determination of OFG CBR reconnaissance" is performed by solving the optimisation problem of integer linear programming through the use of importance coefficients K_i of these vehicles (assets). Taking into account that there are five *i*-types of vehicles (assets) to conduct a certain CBR reconnaissance task, each of them has capabilities v_i and required time T . It is necessary to determine the nomenclature and the number X_i of these vehicles (assets), which will allow to perform the necessary scope of tasks in condition minimising the cost of all vehicles (assets).

Obviously, the total cost of the vehicles (assets) should be equal:

$$min\sum_{i=1}^{5} c_i \cdot X_i \qquad (11)$$

on condition that the required scope of CBR intelligence tasks are completed::

$$\sum_{i=1}^{5} v_{i\ розвід} \cdot K_{i\ розвід} \cdot X_{i\ розвід} \cdot T_{розвід} \geq \sum_{i=1}^{5} S_{розвід\ i}^{потр}, \qquad (12)$$

where $S_{розвід\ i}^{потр}$ determined according to (2).

Based on the results of solving the optimisation task, non-negative values variables X_i, are selected for which the objective function reaches a minimum.

The calculation results are shown in Table 5.

Table 5. Nomenclature of nuclear threat detection and assessment assets (on CBR reconnaissance assets example) of the OFG CBRN battalion

Indicators name		CBR reconnaissance vehicles names			
		RKhM-4-01	RKhM-4	Kozak-2M1	BRDM-2CBR
CBR vehicle capabilities for area reconnaissance, km²/hours, $v_{i\ reccon}$		*80*	*70*	*90*	*60*
Time for CBR reconnaissance, hours, $T_{розвід}^{опер}$		*10*	*10*	*10*	*10*
Vehicle importance ratio, $K_{i\ reccon}$		*0,15*	*0,11*	*0,19*	*0,23*
Scope of activities required, km², $S_{розвід}^{потр}$		*8640*			
CBR reconnaissance assets' nomenclature available, units $x_{i\ reccon}$		-	-	-	*18*
Variants of the CBR reconnaissance assets' nomenclature, units. $x_{i\ reccon}$	1	*4*	*6*	*4*	*9*
	2	*5*	*5*	*6*	*8*
	3	*4*	*6*	*7*	*7*
	4	*5*	*6*	*5*	*8*
A rational variant of the CBR intelligence assets nomenclature is determined, од., $x_{i\ reccon}$	5	*6*	*4*	*6*	*7*

Based on the analysis of the obtained results, it was determined that 20 to 24 CBR reconnaissance vehicles (assets) as components of OFG CBRN brigade's are necessary to perform the required scope of CBR reconnaissance tasks $S_{розвід}^{потр} = 8640\ км^2$, taking into account losses (see Table 4, Fig. 1).

Thus, the nomenclature and number of mobile assets for detecting and assessing nuclear threats (on the example of *i*-type CBR reconnaissance assets) are determineding.

At this point, the task of determining the nomenclature of mobile assets to conduct the scope of nuclear threat detection and assessment tasks is considered to be completed.

Prospects for further research are the development of software to reduce the time of headquarters and services' work.

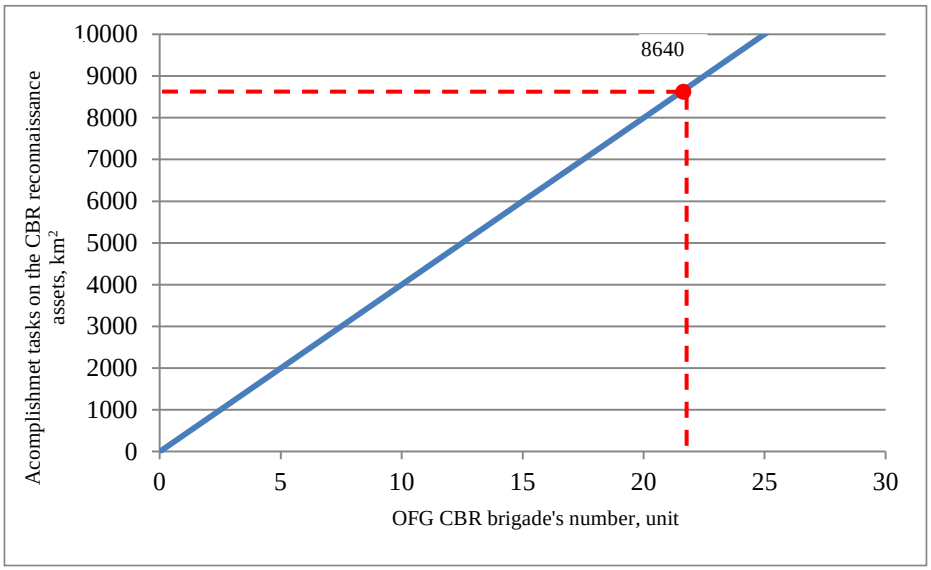


Figure 1. Scope dependence of nuclear threat detection and assessment (CBR reconnaissance) acomplishmet tasks on the CBR reconnaissance assets in OFG CBR brigade's number

Results and Discussions

Thus, by expanding the list of indicators for assessing the functioning of nuclear threat detection and assessment capabilities by introduction of additional time indicators and task completeness for detection and assessment of the situation (CBR reconnaissance), improving the means for determining the capabilities of these assets by using the importance coefficients of assets' individual samples, their nomenclature for performing the scope of tasks under conditions of a high level of threat of nuclear weapons use by the enemy was determined.

This definition means that the results of the assessment of the functioning of nuclear threat detection and assessment assets depend on the level of assets losses that affect their ability to conduct the scope of tasks during combat actions in conditions of the use of nuclear weapons by the enemy, the nomenclature and number of detection and assessment assets (CBR) and their tactical and TTC.

The results of the research and publications analysis showed that a number of studies paid attention to matters related to the troops' protection against nuclear threats organisation and conduct, in particular, detection and assessment of the CBR situation. These are, for example, general questions regarding the CBR reconnaissance organisation and conduct operations (Units' Chemical, Biological, Radiation Protection, 2007), radiation, chemical, biological protection troops' tactics in relation to the conduct CBR reconnaissance activities, tactical calculations substantiation for the conduct of CBR protection tasks and activities, including CBR reconnaissance activities (Hutchenko, Hyshko, Prokofiev, 2017). However, the nomenclature of movable assets for performing the scope of tasks of detecting and assessing nuclear threats, taking into account the loss of these assets and their importance, was not considered in these researches and publications.

The russian-Ukrainian war experience convinces that during the conduct of combat actions in the conditions of threat level escalation, the scope of tasks for detecting and assessing nuclear threats will increase, and the capabilities for their accomplishment will change. In consideration of the above, it is necessary to determine the nuclear threat detection and assessment assets nomenclature by assessing their characteristics, which will allow to evaluate their capabilities and importance in a complex radiological situation, which was done in the article using the proposed methodological approach.

Conclusion

Thus, the presented extended list of indicators for assessing the nuclear threat detection and assessment assets functioning by introducing additional time indicators and tasks completeness of situation detection and assessment (CBR intelligence), improving the method of determining these assets' capabilities through the use of individual assets samples' importance coefficients made it possible to determine the nomenclature of these assets to perform tasks' scope in a high level of nuclear weapons use threats by the enemy conditions .

The research has shown that the results of the assessment of nuclear threat detection and assessment assets functioning depend on the level of assets losses that affect their ability to accomplish the scope of tasks during combat actions in the enemy use of nuclear weapons' conditions, the nomenclature and number of detection and assessment assets of situation (CBR intelligence) and their tactical and technical characteristics.

Prospects for further research in this area are research on the tasks of defence against CBR and nuclear threats, as well as software development to reduce the time of military command and control bodies with this purpose.

Recommendations

The materials in this publication may be useful for military command and control officials involved in CBRN planning for troop protection during combat actions. The results of these calculations will allow determining the nomenclature of assets to perform the scope of nuclear threat detection and assessment tasks.

References

1. Hutchenko, A., Hyshko, V., Prokofiev, V. Tactical calculations on the CBRN protection service's tasks: methodological manual. (2017). Kharkiv. Kharkiv National University of Air Force named after I. Kozhedub. P. 48.
2. Doctrine on Chemical, Biological, Radiological and Nuclear Protection of Troops (Forces). Support Forces Command of the Armed Forces of Ukraine: (2020). VKP 5(3)-00(03).01 of 26.10.2020. Kyiv. P. 35.
3. Zahorka, O. Comparative assessment of weapons samples (complexes and systems) using the taxonomic method. (2004). Scientific Proceedings of the Central Research Institute of the Armed Forces of Ukraine. Kyiv. № 3 (28). P. 96-102.
4. Instruction "Chemical, Biological, Radiological and Nuclear Protection in NATO Operations". Support Forces Command of the Armed Forces of Ukraine: (2023). PTKP 10-25(263). Kyiv. P. 433.
5. Fact Sheet of the US Department of State. (2009). https://2001-2009.state.gov/t/vci/rls/prsrl/2008/ 102844. htm (accessed 15.10.2022).
6. Information sheet. (2022). https://www.washingtonpost.com/world/2022/10/05/russia-nuclear-weapons-military-arsenal/ (accessed 08.10.2022).
7. Koval, V. Methodical approach to assessing the effectiveness of the automatisation assets' integration into the work of radiation, chemical and biological defence in troops' (forces') command and control bodies. (2008). Modern information technologies in the field of security and defence. Kyiv. № 3 (3). P. 28-30.
8. Blekot, O., Romaniuk, V., Nikitin, A., Kotsiuruba, V. Methodology for assessing the situation in emergency situations of technogenic and natural character: a study guide. (2018). Kyiv. National Defence University of Ukraine. P. 12.
9. Meshcheriakov, I., Kurtseitov, T. CBR defence units' action modes formation based on the experience of russian military aggression against Ukraine. (2023). Problematic issues of

organising support activities of the troops (forces) of the Armed Forces of Ukraine in the counteracting course the large-scale armed aggression of the russian federation against Ukraine (taking into account the experience of the joint forces operation). *Scientific and practical seminars materials' collection* (Kyiv, 27 April). Kyiv. National Defence University of Ukraine. P. 38-42.

10. Nikitin, A., Vysotskyi, P. CBRN planning experience analysis for the protection of military facilities and the use of CBRN defence units in the counteracting course of russian federation against Ukraine armed aggression. (2023). Problematic issues of organising support activities of the troops (forces) of the Armed Forces of Ukraine in the counteracting course the large-scale armed aggression of the russian federation against Ukraine (taking into account the experience of the joint forces operation). *Scientific and practical seminars materials' collection* (Kyiv. 27 April). Kyiv. National Defence University of Ukraine. P. 23-24.
11. Regarding the Instruction on the Functioning of the System of Prevention and Warning of Chemical, Biological, Radiological and Nuclear Threats (Incidents) in the System of the Ministry of Defence of Ukraine's Approval. (2023). Decree of the Ministry of Defence of Ukraine of 22.03.2023 No. 152/nm. Kyiv. P. 43.
12. Strategic Missile Forces of the russian federation. (2022). https://uk.wikipedia.org/wiki (accessed 08.10.2022).
13. Slobodianyk, V., Sevostianov, I., Shvets, O. & Dolhalenko, O. (2023). Methodology for Assessing the Military-Technical Level and Prospects for the Development of Radiation, Chemical, and Biological Reconnaissance Devices. *Scientific Proceedings of the Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine*. Kyiv. № 1 (75). P. 152-158.
14. Teploukhov, B. Weapons of mass destruction and protection against them: methodological guide. (2008). Kyiv. Military Institute of Taras Shevchenko National University of Kyiv. P. 100.
15. Lessons of the russian-Ukrainian War of 2022: Military Aspects (2022). (Information and Analytical Report No. 19). Experience of using the units and subdivisions of the Support Forces of the Armed Forces of Ukraine in the context of the russian federation's large-scale aggression against Ukraine. Kyiv. Central Research Institute of the Armed Forces of Ukraine. Inv. no. 18339. P. 132.
16. Completeness of radiation survey is a criterion for the quality of actual radiation situation in modern conditions' detection. (2015). Actual problems of modelling risks and threats of emergencies at critical infrastructure facilities. Proceedings of the International Scientific and Practical Conference (Kyiv, 20-21 April). Kyiv. Ukrainian Research Institute of Civil Defence. P. 35-36.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.11

Methodological aspects of justifying the specialists training duration of the armed forces branches of a formation (unit)

Serhii Godz
Doctor of Military Sciences, Senior Researcher
Leading Researcher
Central Research Institute of the Armed Forces of Ukraine
28B, Povitroflotskyi Avenue. Kyiv, 03049, Ukraine
e-mail: sergiigodz1968@ukr.net
ORCID: 0000-0002-7860-2330

Oleksii Taran
Chief of the J7 of the General Staff of the Armed Forces of Ukraine
Main Directorate of Doctrine and Training of the General Staff of the Armed Forces of Ukraine
6, Povitroflotskyi Avenue, Kyiv, 03168, Ukraine
e-mail: zs507076@gmail.com

Abstract. In the study, the duration of training of specialists in the branches of the armed forces of a formation (unit) refers to the amount of training time or the number of training hours required to achieve the required level of training of specialists in the relevant categories (profiles), primarily those that determine the combat capability of the formation (unit).

The current conditions of armed struggle place increased demands on the level of training of troops (forces). At the same time, during a special period, this training can be carried out under conditions of significant resource, including time, constraints, which requires military command and control bodies (commanders) to take a balanced and comprehensively justified approach to planning training and building the training process of troops (forces). Thus, the experience of combat operations once again confirms the need to address one of the most important and problematic issues - to ensure that the amount of training time allocated for the training of specialists in formations (units) and in training centres (schools) meets real needs. Failure to address this issue has a negative impact on the development of the knowledge, skills, physical and psychological qualities required in a combat situation, and thus on the combat capability of the unit.

At present, in units and training centres (schools), the amount of training time required for certain military specialities (positions) is determined mainly based on military experience, by comparing different forms and methods of training, and without the necessary analytical justification. Therefore, the relevance of this study is precisely due to the need to scientifically substantiate the amount of training time that would ensure both the required level of training of specialists in the relevant categories (profiles) and the appropriate level of training and combat capability of units of the branches of the military and the formation (unit) as a whole.

The purpose of the article is to outline the methodological aspects of substantiating the duration of training of specialists in the branches of the military forces of a formation (unit).

With the help of the above methodological aspects, it is possible to analytically express the process of training specialists of any category (profile) through a function of the type, which characterises the dependence of the achieved level of training of these specialists on the number of training hours during which servicemen learn a certain amount of information - acquire the necessary knowledge, skills and abilities. Graphically, the function can be represented as a -shaped curve that characterises the dynamics of the educational process - the initial and main periods of training. Based on the results of the study of the behaviour of the -shaped curve and the position of its inflection point,

the law of change in the level of training (training effectiveness) of specialists of a certain i-th category (profile) is formulated, depending on the number of training hours during which they acquire the necessary knowledge, skills and abilities, and the values of the parameters and, which most appropriately reflect the dynamics of the educational process of specialists of any category (profile). The presented law makes it possible to unambiguously determine the required number of training hours to achieve the desired level of training of specialists in the branches of the military forces of a formation (unit), and the dynamics of its behaviour is like the continuous Weibull-Gnidenko probability distribution.

The materials of the article are of theoretical value for further scientific research on the problem, as well as practical value - aimed at maintaining (developing) the typical group of capabilities FDR-3 (Training of Military Command and Control Bodies and Troops (Forces)). The practical use of the above methodological aspects will contribute to improving the quality of planning and building the process of training troops (forces), and thus to increasing their combat capability and ability to effectively counter the enemy on the battlefield.

Keywords: combat capability; training of troops (forces); individual training; training; knowledge, skills, abilities; military accounting speciality; training planning; structure of the educational process.

Introduction

The basis of the training of troops (forces) is the individual training of servicemen, and the level of training achieved by specialists of the relevant categories (profiles) is a crucial element of the coherence of units, units, and formations. The results of individual training should achieve the main goal of the educational process - the formation of a serviceman as a specialist, the development of knowledge, skills, physical and psychological qualities necessary in a combat situation. It is also important to consider that the process of individual training of personnel is inseparable from the process of combat coordination of squads (crews, services), platoons, companies (batteries), battalions (divisions).

Training is the level of preparation for performing assigned tasks of units, units, formations - one of the main indicators by which their combat capability is assessed - a state that determines the ability of military formations (MF) to implement their combat capabilities, conduct combat operations in any conditions of the situation and perform assigned tasks. At the same time, the effectiveness (level) of combat training of a formation (unit) is assessed by the following indicators: training – the level of individual training of servicemen of all categories; the level of training (cohesion) of command-and-control bodies (headquarters); the level of training (cohesion) of units of a formation (unit).

The rapidity of modern operations (combat actions), the growing capabilities of intelligence and firepower, the increasing role of maneuvers, the safety of the use and protection of troops (forces), the adoption of new models of weapons and military equipment (WME) place increased demands on the level of training of individual servicemen and units. At the same time, in a special period, this training can be carried out under conditions of significant resource, in particular time, constraints, which requires military command and control bodies (commanders) to take a balanced and comprehensively justified approach to planning training and building the training process of troops (forces). Thus, the experience of combat operations once again confirms the need to address one of the most important and problematic issues - to ensure that the amount of training time allocated for training specialists in formations (units) and in training centres (TCs) (schools) meets real needs. Failure to address this issue negatively affects the development of knowledge, skills, physical and psychological qualities required in a combat situation, and thus the combat capability of the unit. Therefore, despite resource constraints, military command and control bodies (commanders) take

certain measures to ensure that the duration of personnel training, primarily in military specialties (MS) (positions) that determine combat capability, is sufficient for successful combat operations. In particular, the long-term domestic and foreign experience of training troops (forces) is considered, which shows that for a serviceman to be able to perform duties in his specialty (position) independently and as part of a crew (service), the unit needs to have a training period of 4 to 6 months. At the same time, the amount of training time should be from 600 to 800 academic hours (6-8 academic hours per day for a 6-day academic week or 156-208 academic hours per month). First, this applies to the positions for which a specialist class qualification is awarded, for example, commanders of combat vehicles (guns), gunner-operators (gunners), driver mechanics (drivers), senior gunners (aimer), anti-aircraft gunners (gunners), etc. It is also considered that a reduction (in a special period) of the overall training period for personnel and an increase in the intensity of the training process - the number of training hours per day (considering the physiological capabilities of a person) - may have a negative impact on the result of training. For example, the experience of training personnel in specialized training centres - "Afghan training schools" for the Soviet troops in Afghanistan (the 40th Combined Arms Army) - is important. Thus, since 1982, training in the "sergeant's school" has lasted five to five and a half months (about 780-860 training hours), while in the "soldier's school" - two months (about 312-416 training hours). By the spring of 1984, it became clear that a two-month training period for "soldier's training", even with a rich curriculum, was not enough. It was decided to extend the training period up to 3 months (468-624 training hours) for personnel trained in the "rifleman" specialty. For servicemen who were assigned to more complex military specialties, such as gunner-operator, tank gunner (loader), machine gunner, gunner, gunner's number, driver, grenade launcher, etc., the training period was extended to five months (800 training hours). Since May 1985, all new recruits to the 40th Army have been trained under a five-month program.

At present, in units (units), in educational centres (schools), the amount of training time required for certain military occupational specialties (positions) is determined mainly on the basis of military experience, by comparing different forms and methods of training and without the necessary analytical justification. Therefore, the relevance of this study is due to the need to scientifically substantiate the amount of training time that would ensure the required level of training (proficiency) of both specialists of the relevant categories (profile) and units of the branches of the armed forces and formations (units) in general.

The purpose of the article is to outline the methodological aspects of substantiating the duration of training for specialists of the branches of the military in a formation (unit).

Methodological Framework

The proposed methodological aspects make it possible to analytically express the process of training specialists of a certain category (profile) through a type function $E(x)$, that characterizes the dependence of the achieved level of training E of these specialists on the number of training hours x during which servicemen learn a certain amount of information - acquire the necessary knowledge, skills and abilities. The function $E(x)$ is a display for which the scope of the definition of this function - the set x - the number of training hours from 0 to the planned $x_{план} \approx 600 - 800 \approx$ 700 hours $(0 \le x \le x_{план})$ ones is matched, the set of function values - the numerical range $(0 \le E(x) \le 1)$ - all the function values $E(x)$ from 0 to 1, - the achieved level of training of specialists of a certain category, where the argument is the number x of study hours. It is believed that the process of training specialists of any category is continuous, and its dynamics are similar in content. Conventionally, the educational process can be divided into two periods: initial - mainly theoretical training and main - during which the practical component of training for a certain MS (position) dominates.

Graphically, the function $E(x)$ can have the form of a S -like curve with asymmetric branches,

and therefore there must be a special point - an inflection point with abscissa x_1 dividing this curve into two parts - concave (initial period of preparation) and convex (main period of preparation) (Fig. 1).

The transition from the concave part of the *S*-shaped function $E(x)$ curve to the convex part is a sufficient condition for the existence of a certain inflection point. The presence of an inflection points in the behaviour of the function $E(x)$ in this case qualitatively reflects (underlines) the dynamics of the educational process, and its position will be determined by a specific type of function $E(x)$ that describes the educational process in one or another specialty.

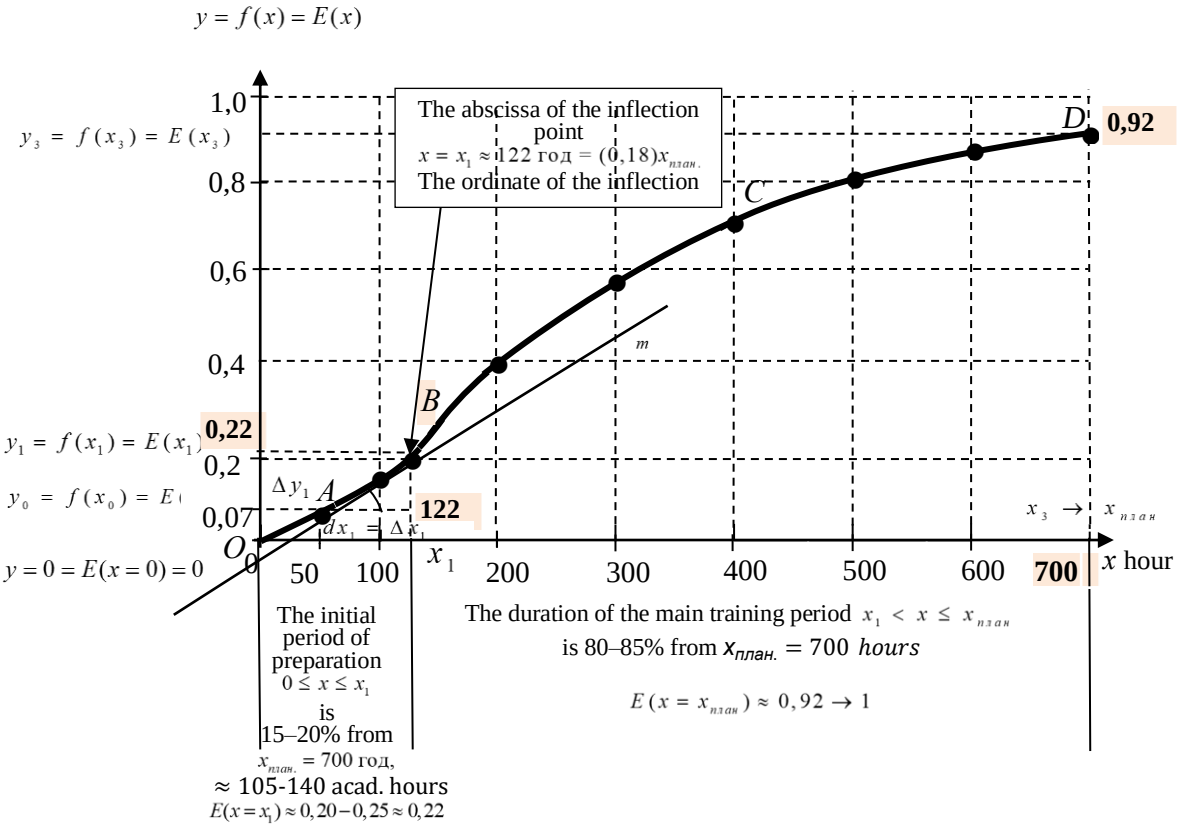


Figure 1. A possible graph of the function $y = f(x) = E(x)$

On the example of the training of specialists (sergeants, soldiers) of the main units (mechanized, tank, artillery, anti-aircraft) of a separate mechanized brigade (unit) in national centres (schools) and directly in compounds (units), we will consider the dynamics of their educational process (behaviour of a S -like curve), namely: the dependence of the achieved level of training $E(x)$ of these specialists on the number of training hours (x) planned for a certain period of training. In accordance with the requirements of the governing documents, the general level of training and overall combat capability of the armed forces is assessed based on the level of training of these specialists (units) of the military branches.

S -like curve $E(x)$ reflects two main periods of the educational process. Each of these periods corresponds to its own dynamics of behaviour S -like curve similar to that in fig. 1 is conventionally shown by currents *O, A, B, C, D.*

The first training period (initial)

At the beginning of the educational process S-like curve $E(x)$ starts from point O with coordinates $x=0$, $E(x=0)=0$ – the initial training period begins with a duration $x=0\le x\le x_1$, of 15–20% of the planned $x=x_{план.}\approx 700$ hours, or $x=x_1=105-140$ hours. Military servicemen get acquainted with the future specialty, they develop the necessary theoretical knowledge, practical skills, and primary skills. The curve is slowly but gradually increasing. In fig. 1 the initial period of training is reflected by the concave part of the S-like curve $E(x)$. During this period, about 80% of the amount of training time is devoted to theoretical classes in the specialty, and the achieved level of training will correspond to the value $E(x=x_1)\approx(0,20-0,25)$, which is assumed to be approximately the same for specialists of any profile. At a certain point in time, the level of training of military personnel allows you to move to the second, main, period of training, during which the personnel acquire the necessary practical skills and skills for the corresponding MS (position). The level of learning achieved during the initial training period $E(x_1)$ is limited by the inflection point *B*, which separates the concave part of the S-like curve from the convex part. If we take the average value of the abscissa of the inflection point *B* $x=x_1\approx 122$ hours $=0,18$, and the corresponding average value of its ordinate, $E(x=x_1\approx 122$ hours$)\approx 0,22$, then the second (main) period of preparation begins from this moment.

Second training period (main)

After the inflection point *B* the training process is intensified, the main period of training of military personnel in accordance with the MS (positions) with a duration of $o\le x\le x_1$. A gradual build-up of the necessary practical skills and skills in the personnel is observed. S - like curve grows more rapidly and passes, for example, through point *C*. The duration of the main training period is about (80–85%) $x_{план.}$, i.e. $(x_1\approx(0,15-0,20)<x\approx(0,80-0,85)\le x_{план}\to 1)$, at the same time, the level of achieved education is $E(x=x_{осн})\to E_{потр}$.. About 80% of the training time of this period is devoted to conducting practical classes in the specialty. At the end of the main period of training there is some slowing down of the pace of the educational process and assimilation of the educational material by military personnel, the curve becomes gentler. The dynamics of increasing the level of training of specialists is somewhat slowing down. In fig. 1, the slowing down of the educational process and its end is characterized by point *D* with coordinates $x\to x_{план}$, $E(x_3)\to E(x_{потр})\to 1$ $(e^{-\lambda\cdot x^{\kappa}}\to 0)$.

Since the process of training specialists of different categories is continuous, the function $y=f(x)=E(x)$, which graphically displays the educational process in the form of a S-like curve, is continuous, and it must be differentiated twice. If the function $E(x)$ is differentiable, that is, it has a derivative at every point of some interval *OD*, then the function is differentiable on this interval. If the derivative of the first order at each point S-like curve characterizes the speed with which the function $E(x)$ changes, then in order to find the position - the coordinates $(x_1;\ y_1)$ of the inflection point B, it is necessary and sufficient to find the second derivative at this point and equate it to 0. The derivative of the second order at the inflection point $B(x_1;\ y_1)$ characterizes the acceleration of the level of learning $E(x)$ of the individual achieved at a certain time composition or the rate at which the rate of growth of this level of learning changes relative to time. The acceleration determined by the inflection point characterizes the transition to the main training period, which is indicated by the convex part of the S-like curve. The convexity of the curve indicates that the second derivative of the function $E(x)$ at the inflection point is positive (>0), the tangent at this point passes through quadrants 1 and 3, and the tangent of its slope angle is positive, which indicates a transition to the convex part of the *S*-like curve.

Dependence, when the S-like graph corresponds to the functional dependence $E(x)$, is displayed analytically similar to the continuous Weibull-Hnidenko probability distribution. The Weibull-Hnidenko continuous probability distribution function is two-parametric and has the form:

$$E(x) = 1 - e^{-\lambda \cdot x^{\kappa}}, \quad (1)$$

where $x \geq 0$; $\lambda > 0$ is the first parameter of the distribution – some constant, scale factor (scale of distribution), which characterizes the intensity of the distribution and affects the shape of the curve $E(x)$. The larger the scale factor, the more widespread the distribution. The parameter λ is a dimensionless value. In the study, the physical content of this coefficient can characterize the amount of information learned by military personnel per unit of time (for example, for 1 training hour) or for a specified (on the abscissa) number of training hours. The value of this coefficient depends on the general educational level of personnel training, training in the amount of the general military minimum, the previously achieved level of training, the state and order of use of the educational material and technical base, etc.; $\kappa > 0$ - the second parameter of the distribution is the shape coefficient, the exponent (integer or fractional), which determines the shape of the graph. In the study, the physical meaning of this coefficient can characterize the growth of the level of education per unit of time. The type of Weibull-Hnidenko continuous probability distribution function depends on the value of the coefficient κ. For example, for a $\kappa = 1$ continuous probability distribution, the Weibull-Hnidenko coincides with the exponential one; for $\kappa = 2$ – turns into a Rayleigh distribution; for $\kappa > 3,5$ – practically coincides with the normal distribution law (Gaussian). The parameter κ, like λ, is a dimensionless value.

Acceptable parameter values κ and λ were determined in the study to emphasize the peculiarities of the behaviour of the function $E(x)$. In particular, the influence of parameters κ and λ on the position of the inflection point and on the behaviour of the S-like curve at the inflection point was investigated. To find the coordinates (abscissa $x = x_1$ and ordinate $y_1 = E(x_1)$) of the inflection point of the *S*-like curve, it is necessary and sufficient to find the second derivative of the function at the inflection point and equate it to 0. Thanks to the calculation of the second-order derivative $(\frac{d^2E(x)}{dx^2} = 0)$, the expression is obtained:

$$x^{\kappa} = \frac{\kappa - 1}{\kappa \cdot \lambda}, \quad (2)$$

from where the abscissa of the inflection point is determined by the values κ and λ:

$$x = x_1 = \kappa\sqrt{\frac{\kappa - 1}{\kappa \cdot \lambda}} = \left(\frac{\kappa - 1}{\kappa - \lambda}\right)^{\frac{1}{\kappa}}, \quad (3)$$

and the ordinate of the function $E(x)$ at the inflection point, considering (2), will be calculated as:

$$E(x = x_1) = 1 - e^{-\lambda \cdot x^{\kappa}} = 1 - e^{-\lambda \cdot \frac{\kappa - 1}{\kappa \cdot \lambda}} = 1 - e^{-\frac{\kappa - 1}{\kappa}}, \quad (4)$$

and does not depend on the value of the parameter λ, but is determined only by the value of κ.

The functional dependence (1) can be expressed as:

$$E(x) = 1 - e^{-\lambda \cdot x^{\kappa}} \geq E(x)_{nomp}. \quad (5)$$

From (5), necessary for achieving $E(x)$ the required number of training hours x can be determined as follows:

$$e^{-\lambda \cdot x^{\kappa}} = 1 - E(x); \qquad \ln e^{-\lambda \cdot x^{\kappa}} = \left[\ln\left(1 - E(x)\right)\right]; \qquad -\lambda \cdot x^{\kappa} = \left[\ln\left(1 - E(x)\right)\right];$$

$$x^{\kappa} = -\frac{\left[\ln\left(1-E(x)\right)\right]}{\lambda}; \qquad x = \left[-\frac{\ln\left(1-E(x)\right)}{\lambda}\right]^{\frac{1}{\kappa}},$$

if $E(x) = E_{потр}$, then:

$$x \geq x_{план.} = \left[-\frac{\ln\left(1-E_{потр}\right)}{\lambda}\right]^{\frac{1}{\kappa}} \quad (6)$$

By condition, the number of training hours allocated for the training of military personnel in one or another specialty is taken at the level $x = x_{план} = 700$ hours per training period. Thus (6) can be written as:

$$x = x_{план} = 700 \geq \left[\frac{\ln\left(1-E_{потр}\right)}{\lambda}\right]^{\frac{1}{\kappa}}, \quad (7)$$

from where the function $E(x)$ (1) parameter λ can be determined:

$$\lambda \geq -\frac{\ln\left(1-E_{потр}\right)}{700^{\kappa}}. \quad (8)$$

From equations (2), (3), considering x_1 (the abscissa of the inflection point), the parameter λ is calculated:

$$\lambda = \frac{\kappa-1}{\kappa \cdot x_1^{\kappa}}. \quad (9)$$

Combining equations (8), (9), we get the transcendental equation:

$$\frac{\kappa-1}{\kappa \cdot x_1^{\kappa}} = -\frac{\ln\left(1-E_{потр}\right)}{700^{\kappa}}, \quad (10)$$

from where the value of the parameter κ can be determined.

If the abscissa of the inflection point is $x = x_1 \approx 122$ год, we will receive:

$$\frac{700^{\kappa}}{122^{\kappa}} = \frac{700^{\kappa}}{\kappa \cdot 122^{\kappa}} - \ln\left(1-E_{потр}\right) \cdot \quad (11)$$

The transcendental equation (11) with respect to the value κ is solved graphically or numerically. To solve it graphically, the transcendental equation (11) can be written in the form of equations that are expressed through the same function y:

$$y = \frac{700^{\kappa}}{122^{\kappa}}; \qquad y = \frac{700^{\kappa}}{\kappa \cdot 122^{\kappa}} - \ln\left(1-E_{потр}\right); \quad (12)$$

the joint solution of these equations graphically will allow to determine the value κ by calculating the values of y given in the table. 1 and 2.

Table 1. Calculation of values $y = \frac{700^{\kappa}}{122^{\kappa}}$

Possible values κ						
1	1,2	1,3	**1,4**	1,6	1,8	**2**
Calculated values y						
5,74	8,13	9,68	**11,55**	16,36	23,21	**32,92**

Table 2. Calculation of values $y = \frac{700^{\kappa}}{\kappa \cdot 122^{\kappa}} - \ln(1 - E_{потр})$

Possible values $E_{потр}$	Possible values κ						
	1	1,2	1,3	1,4	1,6	1,8	**2**
	Calculated values y						
0	5,74	6,78	7,45	8,25	10,23	12,89	16,46
0,2	5,96	7,00	7,67	8,47	10,45	13,11	16.68
0,4	6.25	7,29	7,96	8,76	10,74	13,40	16,97
0,6	6,66	7,70	8,37	9,17	11,15	13,81	17,38
0,8	7,35	8,39	9,06	9,86	11,84	14,50	18,07
0,95	8,74	9,78	10,45	11,25	13,23	15,89	**19,46**

An approximate value is determined from the intersection of the curves $y = \frac{700^{\kappa}}{122^{\kappa}}$ and $y = \frac{700^{\kappa}}{\kappa \cdot 122^{\kappa}} - \ln(1 - E_{потр})$, for example, by $E_{потр} = 0,95$:

$$\kappa \approx 1,3. \quad (13)$$

If we take the average value of the abscissa of the inflection point corresponding to and the corresponding average value of the ordinate of the inflection point $x = x_1 \approx 122 \text{ год} = 0,18$, then the function (4) or the ordinate of the inflection point can be written as a function $E(x = x_1) = 1 - e^{-\frac{\kappa - 1}{\kappa}} = 0,22$, from where more accurate compared to (13) the value of the parameter (exponent of the degree) of the function (1) will correspond:

$$\kappa \approx 1,33. \quad (14)$$

Then, taking into account (3), (9), if $x = x_1 = (\frac{\kappa - 1}{\kappa - \lambda})^{\frac{1}{\kappa}} \approx 122 \text{ год}$, and $\kappa \approx 1,33$ we get the second parameter of function (1):

$$\lambda = \frac{\kappa - 1}{\kappa \cdot x_1^{\kappa}} = \frac{1,33 - 1}{1,33 \cdot 122^{\kappa}} = 0,00042. \quad (15)$$

For a more in-depth analysis of the behaviour of function (1) for different values of quantities x within, for example, 0 ÷ 700 hours and the found values κ = 1.33, λ = 0.00042, the values of this function are calculated (Table 3).

Table 3. Calculation of function values $E(x) = 1 - e^{-\lambda \cdot x^{\kappa}}$

Possible values x (hours)														
0	50	100	**122**	150	200	250	300	350	400	500	550	600	650	**700**
Calculated values $E(x) = 1 - e^{-\lambda \cdot x^{\kappa}}$														
0	0,07	0,17	**0,22**	0,28	0,38	0,48	0,56	0,64	0,70	0,80	0,84	0,88	0,90	**0,92**

Considering the value of table. 3, it can be assumed that the function $E(x)$ (1) satisfies the requirements for the parameters of the educational process and with the same values for all specialties κ = 1.33 (3), (14), λ = 0.00042 (8), (15) acquires, unlike from (1), of the form:

$$E(x) = 1 - e^{-\lambda \cdot x^{\kappa}} = 1 - e^{-0,00042 \cdot x^{1,33}}. \quad (16)$$

For different values κ, λ, the behaviour of the function $E(x) = 1 - e^{-\lambda \cdot x^{\kappa}}$ for $x = x_{план} =$ 700 hours is presented in the table. 4 and Fig. 2.

Conclusions about the parameter λ

From fig. 2 and (3). , that is, as κ the parameter λ (8), (9), (15) (increasing the amount of

information successfully learned per unit of time) decreasing the value of abscissa $x = x_1$ of the inflection point (3), there is a shift of the inflection point and the curves to the left, i.e., as the parameter λ increases, the graph of function (1) (curves) shifts to the left to the ordinate axis, which is normal. And vice versa, from fig. 2 and (3) it follows that for a given κ parameter with decreasing the parameter λ (i.e. decreasing the amount of successfully assimilated information per unit of time) value of the abscissa $x = x_1$ increases of the inflection point (3), the inflection point and curves $E(x)$ shift to the right, i.e., as the parameter λ decreases, the graph of the function (curves) shifts to the right of the ordinate axis. At the same time, the number of training hours required for the training of military personnel x needs to be increased (which may indicate an insufficient level of personnel training). So, the parameter λ characterizes the displacement of the abscissa $x = x_1$ of the inflection point (horizontally – to the left or right) and determines the value of the abscissa of the inflection point at an unchanged value of its ordinate. Thus, with a change in the parameter λ, and therefore with a change in the abscissa of the inflection point $x = x_1 \approx 122$ hours $\approx 0{,}18$, for one and the same κ value, the values of the function $E(x = x_1)$ at the inflection point remain unchanged (4), since they are determined only by the values $\kappa \geq 1$ and do not depend on the parameter $\lambda > 0$. And of the ordinate of the inflection point, that is, the achievable the level of training $y_1 = f(x_1) = E(x_1)$ of specialists in the initial period of training (4) depending on the number of training hours x, is determined by the value of the parameter x.

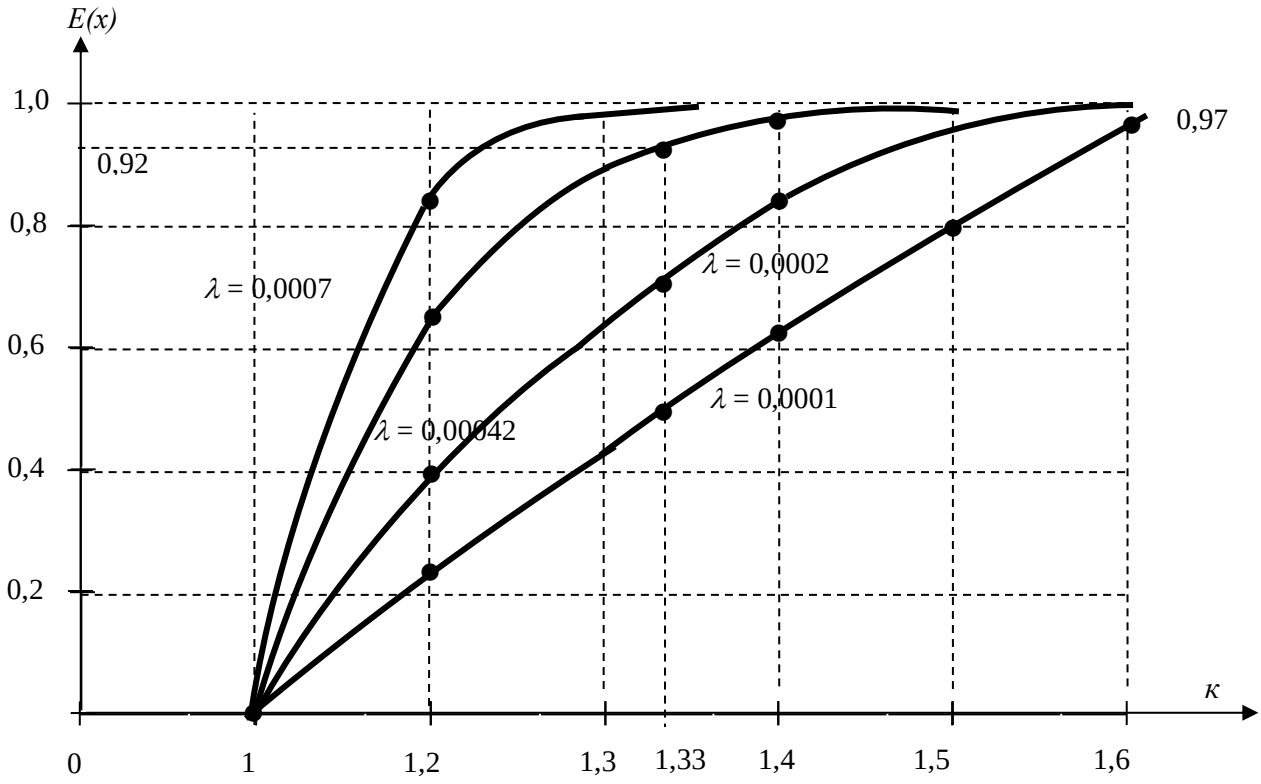


Figure 2. Behaviour of the function $E(x) = 1 - e^{-\lambda \cdot x^{\kappa}}$ at different values κ, λ, for $x = x_{план} = 700$ год

Table 4. Function behaviour $E(x)=1-e^{-\lambda \cdot x^{\kappa}}$ for $x = x_{план} = 700$ год

Possible values κ	Possible values λ						
	0,0001	**0,0002**	0,0003	**0,00042**	0,0005	0,0006	**0,0007**
	Calculated values $E(x)=1-e^{-\lambda \cdot x^{\kappa}}$						
1,0	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
1,2	0,23	0,40	0,54	0,66	0,73	0,79	0,84
1,33	**0,46**	**0,70**	0,84	**0,92**	0,95	0,97	**0,99**
1,4	0,62	0,85	0,94	0,98	0,99	0,999	≈ 1
1,6	0,97	≈ 1	≈ 1	≈ 1	≈ 1	≈ 1	≈ 1

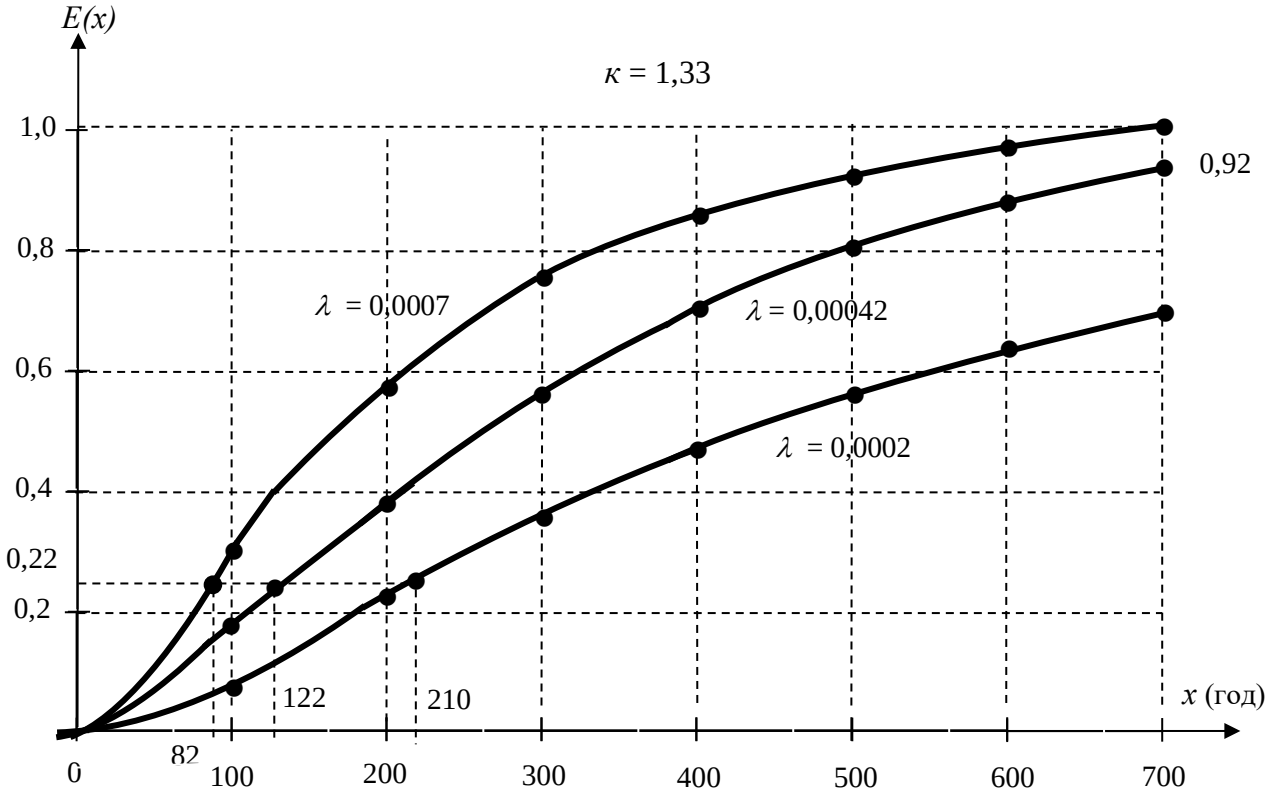


Figure 3. Graphs $E(x)=1-e^{-\lambda \cdot x^{1,33}}$ за $\lambda =$ 0,0002, 0,00042, 0,0007

A decrease in the duration of the initial training period (3) with an increase in parameter λ (9) can characterize (underline) the influence of the general educational level of training or training in the amount of the combined military minimum, which is observed in the personnel before the beginning of the training process, and also allows determining the duration of the initial training period $x = 0 \le x \le x_1$. In fig. 3 according to data, for example, table. 4, graphs of the behaviour of the function $E(x)=1-e^{-\lambda \cdot x^{\kappa}}$ for $x = x_{план} = 700$ год, for different parameter values κ, λ,, in particular for $\lambda = 0.0002, 0.00042, 0.0007$, are shown. In fig. it can be seen that as parameters λ (8), (15) increase, the value (abscissa) of x_1 the inflection point decreases, this point shifts to the left, the curves $E(x)$ shift to the left to the ordinate axis. In the case of a change in the position of the inflection point x_1 and for the same value κ, the values of the function $E(x = x_1)$ at the inflection point remain

unchanged (4), since they are determined only by values $\kappa \geq 1$ and do not depend on the parameter $\lambda > 0$. If, according to the experience of military training, the duration of the initial period of training $x = 0 \leq x \leq x_1$ is 105–140 academic hours, and the average value of the abscissa x_1 of the inflection point corresponds to $x = x_1 \approx 122$ год $\approx 0{,}18$, the corresponding average value of the ordinate of the inflection point will correspond to the achieved level of education $E(x = x_1 \approx 122 \text{ год}) = 0{,}22$, which is assumed to be approximately the same for specialists of any profile.

Conclusions about the parameter κ

The selected value of the parameter κ affects the position of the inflection point, i.e. determines its ordinate or the achievable level of education of specialists $E(x)$ of a certain category in the initial period of their training (4) depending on the number x_1 of training hours during which the information was learned. So, the value of the parameter κ characterizes the movement of the inflection point along the ordinate axis (vertically) and determines the value of the ordinate $y_1 = f(x_1) = E(x_1)$ of the inflection point. As the parameter κ increases, the value of the ordinate of the inflection point increases, and the value of the achieved level of learning (4) at the inflection point increases. As the parameter κ decreases, the value of the ordinate of the inflection point decreases, and the value of the achieved level of learning (4) at the inflection point decreases. The above confirms the presence of an inflection point in the *S*-like curve, as well as the fact that at the inflection point the level of training $E(x = x_1) = 1 - e^{-\frac{\kappa - 1}{\kappa}}$ of military personnel does not depend on the value of the parameter λ, but is determined only by the value of the exponent κ. Considering the fact that the value $E(x = x_1)$ at the inflection point is determined only by the value κ, and the initial period of training and the corresponding level of education are approximately the same for specialists of any i-th category, the results of the calculations made it possible to obtain the values of the parameters $\kappa \approx 1.33$ and $\lambda = 0,\ 00042$, which most appropriately ($x = x_1 \approx 122$ год $= 0{,}18$ – abscissa and $E(x = x_1) \approx 0{,}22$ – ordinate of the inflection point) characterize the behaviour of a S-like curve, which is presented in the form of a function $E(x)$ with a variable x and reflects the dynamics of the educational process of these specialists. Therefore, the coordinates of the inflection point coincide with the data of the initial training period. Thus, the function of changing the level of education of specialists of a certain category (profile) depending on the number x of training hours during which they learn a certain amount of information, for different values of the abscissa of the inflection point x_1, and therefore, for different values of parameter λ (8), (15), unlike from $E(x) = 1 - e^{-\lambda \cdot x^{\kappa}}$, should be written as $E(x_i) = 1 - e^{-\lambda_i \cdot x_i^{\kappa}}$, where λ_i is the parameter of the function $E(x_i)$ for the corresponding i-th specialty ($i = \overline{1,\ 4}$) (the main branches of troops (units)).

The results of the analysis of the behaviour of the curve $E(x)$, shown in fig. 2, as well as in table. 4, allow us to conclude that the obtained parameters $\kappa \approx 1.33$, $\lambda_i = 0.00042$ most appropriately reflect the dynamics of the educational process of specialists of any category (profile). This makes it possible to formulate the law of changes in the level of training (effectiveness of training) $E(x_i)$ of specialists of the i-th category (profile) depending on the number x_i of training hours during which they acquire the necessary knowledge, abilities and skills, and the parameter values $\kappa \approx 1.33$, $\lambda_i = 0.00042$, which are the most adequately reflect the dynamics of the educational process of specialists of any category (profile).

Unlike (16), this law can be written as:

$$E(x_i) = 1 - e^{-\lambda_i \cdot x_i^{\kappa}} = 1 - e^{-0{,}00042 \cdot x_i^{1{,}33}}, \quad (17)$$

where λ_i is the parameter of $E(x_i)$, which in this case, like the parameter κ, is assumed to be the same for any i-th specialty $(i = \overline{1,\ 4})$. Such a law meets the requirements for the function $E(x_i)$, and the dynamics of its behaviour does not differ from the continuous Weibull-Hnidenko probability distribution (16). Therefore, the number x_i of training hours required for achievement $E(x_i)$ can be determined as follows:

$$e^{-\lambda_i \cdot x_i^{\kappa}} = 1 - E(x_i); \qquad \ln e^{-\lambda_i \cdot x_i^{\kappa}} = \left[\ln\left(1 - E(x_i)\right)\right]; \qquad -\lambda_i \cdot x_i^{\kappa} = \left[\ln\left(1 - E(x_i)\right)\right];$$

$$x_i^{\kappa} = -\frac{\left[\ln\left(1 - E(x_i)\right)\right]}{\lambda_i}; \qquad x_i = \left[-\frac{\ln\left(1 - E(x_i)\right)}{\lambda_i}\right]^{\frac{1}{\kappa}},$$

if marked $E(x_i) = E_i$, we will write it down as:

$$x_i \geq x_{i\,план} = \left[-\frac{\ln(1 - E_i)}{\lambda_i}\right]^{\frac{1}{\kappa}}. \quad (18)$$

Results

According to (17), (18) it is possible to calculate the number of training hours x_i that will allow to achieve the required level of training $E(x_i)$ of specialists of any i-th category (profile). For example, for the given value $E(x_i) = E_i = 0{,}9$ of κ = 1,33, λ = 0,00042, the number of training hours required for training the i-th category of specialists will be calculated as follows:

$$x_i = \left[-\frac{\ln(1 - E_i)}{\lambda_i}\right]^{\frac{1}{\kappa}} = \left[-\frac{\ln(1 - 0{,}9)}{0{,}00042}\right]^{\frac{1}{1{,}3}} = \left[-\frac{\ln 0{,}1}{0{,}00042}\right]^{0{,}752} = \left[-\frac{2{,}30258}{0{,}00042}\right]^{0{,}752} = 5483^{0{,}752} = 648 \text{ год.}$$

Given the given value $E(x_i) = E_i = 0{,}85$ of κ = 1,33, λ = 0,00042, the number of training hours x_i required for training the i-th category of specialists will be calculated as follows:

$$x_i = \left[-\frac{\ln(1 - E_i)}{\lambda_i}\right]^{\frac{1}{\kappa}} = \left[-\frac{\ln(1 - 0{,}85)}{0{,}00042}\right]^{\frac{1}{1{,}3}} = \left[-\frac{\ln 0{,}15}{0{,}00042}\right]^{0{,}752} = 560 \text{ год.}$$

The calculated learning time resource is within the planned limits.

Discussions

The study of problematic issues related to the training of troops (forces) and the development of scientifically based recommendations on ways to solve them is an important component of the development of the theory of military training and education as a branch of military science, as well as one of the main tasks of scientific (research) institutions and military command and control bodies of the Armed Forces of Ukraine.

At the same time, the results of the analysis of recent publications in the field of research, in particular, existing methods for assessing the level of training of specialists (units) of branches of the armed forces, formations (units) and justification of the amount of training time required for their training (Nesterov A. G., 2001; Malkov M. I., 2001; Pichugin M. F., 2002; Gorda M. Y., Zhernakov Y. V., 2004; Molokov O. V., 2005; Chabanenko P. P., 2012; Sidash V. V., 2013; Kovch V. Yu, 2020; Sakovskyi H.

A., 2020; Tymkiv O. A., 2021; Pekhota S. G., 2021; Zaluzhnyi V. F., Moisiuk E. G., Shaptala S. O., 2022; Zaluzhnyi V. F., Zabrodskyi M. V., 2023; Chornomaz O. O., 2023), allow us to draw the following conclusions:

– in the work of command-and-control bodies (headquarters), empirical models are usually used in planning training and building the educational process of troops (forces), which are reflected in planning and policy documents, methods and training programs. However, these models do not always accurately reflect the dynamics of the educational process, in particular, the dependence of the achieved level of training of specialists (units) of the branches of the armed forces on the number of training hours allocated for their training (Godz S.V., 2021), (Mozharovskyi, V. M., Godz, S. V., Sakovskyi, H. A., 2019);

– most of the papers combine deterministic and stochastic models. For example, (Malkov, M. I., 2001) describes a methodology for assessing the effectiveness of the combat training system of combined arms formations (units) of permanent readiness; (Sidash, V. V., 2013) – an improved methodology for planning flight training of aviation brigade crews, taking into account resource constraints and opportunities for implementing planned activities; (Molokov, O. V., 2005) – a methodology for assessing the effectiveness of individual fire training of personnel of the Armed Forces units; (Harabara, V. I., 2020) – an improved comprehensive methodology for assessing the effectiveness of combat training of a tank brigade during the resumption of combat;

– a number of papers use the exponential distribution of the level of training over time ((Pichuhin M. F., 2002) – substantiation of recommendations for improving the training system for junior specialists for anti-aircraft missile forces in the NC; (Hrom, V. A., 2017) – improved methodology for assessing the effectiveness of combat training of units and subunits of engineering troops);

– in some works, in particular (Dyenyezhkin, M. M., 2019) – (Mozharovskyi, V. M., 2018), indicators are used to assess the combat capability of the MF, which characterize their staffing, provision of basic types of anti-aircraft weapons and expendable logistic support. At the same time, the indicators characterizing the level of training of the personnel and the military personnel and MF are not taken into account or are taken into account as limitations;

– there are studies, in particular (Tymkiv, O. A., 2021), (Zaluzhnyi, V. F.), which highlight the experience of combat operations and raise problematic issues of training personnel, units, and units in the context of repelling the armed aggression of the Russian Federation against Ukraine. These works are important for further study of the issues of training of the Armed Forces and the Defence Forces in general.

At the same time, in the presented methods for evaluating the level of training of personnel and MF indicators of time costs (required number of training hours) are chosen mainly on the basis of military experience, by comparing different forms and methods of training and without the necessary analytical justification. These methods do not provide an opportunity to substantiate the required number of training hours to achieve the required level of training of specialists (units) of the troops (units); use different methods (ways, methods) of researching the process of distribution of education level over time; do not provide for a comprehensive approach to the organization and evaluation of the effectiveness of combat training of a unit taking into account resource limitations. The above confirms the relevance of this study, which is due to the need for scientific substantiation of the amount of training time, which would ensure both the required level of training of specialists of the relevant categories (profile), and the required level of training and combat capability of units of military branches and formations (units) as a whole.

Conclusion

The methodical aspects described in the article make it possible to formulate the law of changes in the level of training (effectiveness of training) $E(x_i)$ of specialists of the i-th category (profile) depending on the number of training hours x_i during which they acquire the necessary knowledge, skills and abilities, and the values of the parameters $\kappa \approx 1{,}33$, $\lambda_i = 0{,}00042$, which most appropriately

reflect the dynamics of the educational process of specialists of any category (profile): $E(x_i)=1-e^{-\lambda_i \cdot x_i^{\kappa}}=1-e^{-0{,}00042 \cdot x_i^{1{,}33}}$ (17), where λ_i is the $E(x_i)$ parameter, which in this case, like the parameter κ, is assumed to be the same for any i-th specialty $(i=\overline{1,\ 4})$.

The given law makes it possible to unambiguously determine the amount of training time necessary to achieve the required level of training of specialists of the military branches of the troops (units).

Recommendations

The number of training hours obtained as a result of the calculations makes it possible to achieve the required level of training of servicemen for the MS (positions) for which the class qualification of a specialist is assigned (are the most difficult), for example, for commanders of combat vehicles (cannons), gunners-operators (cannon gunners), mechanics -drivers (drivers), senior gunners (gunners) of guns, operators (gunners) of anti-aircraft installations, etc.

For the training of military personnel for the MS, who do not require the assignment of specialist class qualifications, for example, riflemen, machine gunners, grenade launchers, the number of training hours may be reduced depending on the level of their acquisition of practical skills and abilities. At the same time, practice shows that the minimum period of training of specialists for MS (positions) that determine the combat capability of units (parts) should be at least three months (468–624 study hours). It should also be taken into account that during a special period, the reduction of the general terms of training (for example, from three to one month) and at the same time an increase in the intensity of the educational process (the number of educational hours per day from 8 to 10) can negatively affect the final result of training.

The methodological aspects presented in the article are aimed at maintaining (developing) the typical FDR-3 capability group (Training of military authorities and troops (forces)) of the FDR functional capability group (Planning the development and ensuring the readiness of troops (forces)). The practical use of the presented methodical aspects will contribute to the improvement of the quality of planning and construction of the process of training troops (forces), and therefore to the growth of their combat capability and ability to effectively oppose the enemy on the battlefield.

Prospects for further research. Given the fact that the methodical aspects considered above do not provide for any restrictions, except for the duration of the training process, in practice there may be a need to distribute training hours between the units of the troops of the unit (unit), taking into account the financial resources allocated for combat training. In this regard, the perspective of further research may be to formulate and solve an optimization problem that, given the given levels of training $E(x_i)$ of specialists (units) of the troops of the unit (unit) and taking into account the importance (contribution) a_i of one or another unit of the unit to the combat capability of the unit (units), as well as the financial resources C allocated for combat training (for the training period), made it possible to determine the resource of training time $x_i(i=\overline{1,4})$, necessary to achieve the given level of training $E(x_i)$ of the main divisions of the military branches and the maximum level of training $\max E(x)$ of the unit (unit) as a whole (Godz, S. V., Taran, O. V., 2019), (Godz, S. V., 2020).

The level of training of the military reserve of human resources is of great importance, in particular conscripts (reservists), who in peacetime are on military registration in territorial recruitment centres, and in a special period are subject to mobilization, and, as specialists under certain MS, arrive for assembly of troops (units) of the Defense Forces. At the same time, it is important to consider the fact that conscripts lose some part of the information (acquired knowledge, abilities, skills) that they have acquired before for a certain period. Under the same conditions, the rate of loss of this information, and therefore the current level of education of conscripts, can be

different. In one case, significant average annual losses of information from memory are observed, in the second case, these losses are insignificant, which is related to the peculiarities of each person's memory and its main properties - memorization and forgetting (memory is a psychological process that characterizes the ability of military personnel (conscripts) to store and reproduce in the mind the information previously acquired during military training). One of the main ways to restore partially lost information in the memory of servicemen (military conscripts) is to periodically conduct military training events with them, for example, training meetings or classes during mobilization events. In this regard, the perspective of further research may also be to substantiate the periodicity and duration of training events with this category of personnel (Godz, S. V., 2020).

References

1. Godz, S. V. Analysis of factors influencing the combat training of military formations of the State Defence Forces, in particular, formations (units) of the Armed Forces of Ukraine. (2021). *Collection of scientific articles of the Central Research Institute of the Armed Forces of Ukraine*. Kyiv. № 1 (96). P. 52-62.
2. Mozharovskyi, V. M., Godz, S. V., Sakovskyi, H. A. Analysis of existing methods for assessing the effectiveness of combat training planning and the level of training of military formations of the state defence forces. (2019). *Collection of scientific articles of the Central Research Institute of the Armed Forces of Ukraine*. Kyiv. № 3 (89). P. 18-29.
3. Malkov, M. I. Substantiation of recommendations for improving the effectiveness of the combat training system of combined arms units and formations of permanent combat readiness. (2001). Dissertation ... Candidate of Military Sciences: 20.01.05. Kyiv. Central Research Institute of the Armed Forces of Ukraine. 181 p.
4. Sidash, V. V. Substantiation of recommendations for improving the process of flight training of aviation brigade crews, taking into account the capabilities of the brigade and resource constraints. (2013). Dissertation ... Candidate of Military Sciences: 20.01.05. Kyiv. Central Research Institute of the Armed Forces of Ukraine. 184 p.
5. Molokov, O. V. Substantiation of recommendations for improving the effectiveness of individual fire training of the personnel of the units of the Land Forces of the Armed Forces of Ukraine. (2005). PhD thesis ... Candidate of Military Sciences: 20.01.05: 20.01.05. Kyiv. Central Research Institute of the Armed Forces of Ukraine. 20 p.
6. Harabara, V. I. Substantiation of Recommendations for Improving the Effectiveness of Combat Training of a Tank Brigade in the Course of Restoring Combat Capability. (2020). PhD thesis ... Candidate of Military Sciences: 20.01.05. Kyiv. 18 p.
7. Pichuhin M. F. Substantiation of recommendations for improving the system of training junior military specialists for air defence systems in training centres. (2002). Dissertation ... Candidate of Military Sciences: 20.01.05. Kyiv. Central Research Institute of the Armed Forces of Ukraine. 219 p.
8. Hrom, V. A. Substantiation of recommendations for improving the effectiveness of combat training of units and subunits of the engineering troops of the Armed Forces of Ukraine. (2017). Dissertation ... Candidate of Military Sciences: 20.01.05. Kyiv. Central Research Institute of the Armed Forces of Ukraine. 203 p.
9. Dyenyezhkin, M. M. Methodological bases of substantiation of measures for the development of the Armed Forces of Ukraine to ensure a given level of their combat capability. (2019). Dissertation ... Doctor of Military Sciences: 20.01.05. Kyiv. Central Research Institute of the Armed Forces of Ukraine. 443 p.
10. Mozharovskyi, V. M. Methodological bases of substantiation of the combat composition of the Armed Forces of Ukraine to ensure the required level of their combat capability. (2018).

Dissertation ... doctor of military sciences: 20.01.05. Kyiv. Central Research Institute of the Armed Forces of Ukraine. 476 p.

11. Tymkiv, O. A. Substantiation of recommendations for improving the combat capabilities of military formations through the modernisation of major types of weapons and military equipment. (2021). PhD thesis ... Candidate of Military Sciences: 20.01.05. Kyiv. 20 p.
12. Zaluzhnyi, V. F., Zabrodskyi, M. V. Prospects for ensuring the military campaign of 2023: Ukrainian view. (2022). https://ukrinform.ua. 07.09.2022.
13. Zaluzhnyi, V. F. Modern positional warfare and how to win it. https://www.liga.net/ua/politics/articles/yak-peremohty-u-pozytsiinii-viini-pereklad-povnoi-versii-statti-henerala-zaluzhnoho.
14. Zaluzhnyi, V. F., Moisiuk, E. G., Shaptala, S. O. et al. (2022). TKP 7-000 (162) 01.03. Collection No. 3 of materials for studying the combat experience of the Russian-Ukrainian war of 2022. Kyiv. Doctrine and Training Department of the General Staff of the Armed Forces of Ukraine. Scientific and research institutions of the Armed Forces of Ukraine. 336 p.
15. Godz, S. V., Taran, O. V. Functional dependence of the level of training of a formation (unit) on the number of training hours allocated for combat training and their distribution among specialists (units) of the branches of the armed forces. (2019). Joint actions of military formations and law enforcement agencies of the state: problems and prospects. *Collection of materials of the international scientific and practical conference* (Odesa, 12-13 September). Odesa. Military Academy. P. 90.
16. Godz, S. V. Optimisation problem of distribution of training hours of the Comprehensive Combat Training Programme between specialists (units) of the branches of the armed forces to achieve a given level of training of a formation (unit). (2020). *Collection of scientific articles of the Central Research Institute of the Armed Forces of Ukraine*. Kyiv. № 3 (94). C. 50-61.
17. Godz, S. V. Substantiation of the frequency of training sessions with persons liable for military service, taking into account the linear and nonlinear dependence of the rate of loss of previously acquired knowledge, skills and abilities. (2020). Proceedings of the University. *Collection of scientific papers of NDU of Ukraine*. Kyiv. № 1 (157). P. 125-142.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.12

Complex modeling of complicated processes: analytical model parameters adaptation in solving qualimetric problems

Olexander Mashkin
Doctor of Engineering, senior staff scientist
Chief of scientific-research branch
The Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitroflotskyi Avenue, Kyiv, Ukraine
e-mail: alexlen@meta.ua
ORCID: 0000-0002-3094-9984

Svitlana Maslenko
senior staff scientist of scientific-research branch
The Central Research Institute of the Armed Forces of Ukraine
03049, 28B Povitroflotskyi Avenue, Kyiv, Ukraine
e-mail: Sveta0213@i.ua
ORCID: 0000-0002-9673-3844

Abstract. The relevance of the study is due to the fact that despite the sustainable development of methods and technologies for creating models of various classes and purposes, the tasks of managing their quality (the so-called inverse problems of theoretical qualimetry) are often neglected. For example, in the field of information technology, much more attention is paid to assessing the quality of software products, which is reflected in the corresponding standards. These tasks become especially relevant when models reflect a complex process (CP), and such processes may be unique, and obtaining complete objective data on such CPs prior to modeling is difficult or impossible (accidents and disasters models, military operations, natural disasters, and others like that). The article's main purpose is to consider the issues of solving the inverse qualimetric problem by parametric adaptation of analytical models to unpredictable possible changes in the complex processes' nature. The solution to this problem is based on the combined (analytical and simulation) modeling of unique processes. Theoretical qualimetry involves a quantitative assessment of any product's qualitative properties; to ensure the adequacy level of analytical models (based on the results of their parametric adaptation), it is planned to evaluate with the use of well-known metrology principles regarding relative measurement deviations. In this case, detailed simulation modelling results are used as a reference for combined modelling. The complexity of the processes conditiond by the expediency of their polymodel description in order to mutually compensate for the objective deficiencies of heterogeneous models, as well as the use of simulation capabilities to adjust the parameters of analytical models in cases where the use of the latter is due to strict time constraints on obtaining calculation results and developing control actions based on them. A variant of the formalized statement of the problem of parametric adaptation of analytical models is presented. A presented example that considers the adaptation of parameters of the Lanchester-type analytical model conducted on simulation data. The adaptation of parameters could be carried out in different ways, and the expediency of choosing a certain one is determined by the assessment of mutual deviations of the results of heterogeneous modeling. The results of the calculations witnesses that parametric adaptation can be an effective element in solving one of the key tasks of model qualimetry, namely, ensuring their required qualitative properties. The prospect of further research is to consider the issues of structural adaptation of simulation models to the given conditions for displaying complex processes.

Keywords: simulation and analytical modeling; model qualimetry; Lanchester-type models; parametric model adaptation.

Introduction

In the modern world, a large number of methods and techniques are used for quantifying and assessing the various types of products' quality. The science that studies and combines these methods and techniques, systematizes and develops them is called qualimetrics (from the Latin word qualitas – quality, property and the ancient Greek metreon – to measure). Qualimetrics is a scientific discipline within the framework of which the methodology and problematic issues of complex, quantitative assessment of object quality are studied (Kuts, Stoliarchuk, Druziuk, 2012), (Tsyba, 1997), (Bozhenko, 2003). E. Hevorkian (2022) gave the following definition: qualimetry is a scientific field that studies and develops principles and methods of quantitative quality assessment; establishes quantitative regularities formation of various product quality indicators in design projecting, manufacturing and exploitation fields; discloses objective links between the costs of creating products or articles and the beneficial effect achieved as a result of these costs. The term "qualimetry" concisely and accurately conveys the meaning of the concept of "quality measurement" (Shapoval, 2002). In qualimetrics, two main concepts are used - measurement and evaluation. Measurement is understood as finding the value of a physical quantity by means of research methods with the help of special technical means. Evaluation in qualimetry is used both differential (single) and complex, depending on the need.

Theoretical qualimetry involves for the distinction between direct and inverse tasks, which are understood as, respectively, the tasks of direct assessment of quality properties (direct) and the tasks of quality management in order to ensure the required properties of products for any purpose (inverse). The structure of a comprehensive simulation model quality assessment is presented in the article by B. Butvin, M. Mashkin, O. Sobolev etc. (2022). Since the models themselves are created both for the purpose of analyzing existing original objects and for the purpose of their synthesis, the inverse tasks play a major role in model qualimetry. According to the fair statement of the authors B. Sokolov, R. Yusupov (2004), B. Sokolov, R. Yusupov, S. Mikoni (2014, 2018), despite the sustainable methods development and technologies for creating models of various classes and purposes, such tasks often remain beyond attention. These tasks become especially relevant when the models reflect a complex (unique) process (CP), and obtaining complete objective data on such CP's prior to modeling is difficult or impossible. A characteristic manifestation of the process complexity from the cybernetic point of view, according to S. Mikoni, B. Sokolov, R. Yusupov (2018), M. Moiseiev (1981), is considered to be the necessity of its polymodel description, involvement of heterogeneous models based on different methodological frameworks. The use of heterogeneous models combined into a complex will not only increase substantiation of assumptions about the probable nature of the complex process's course, but also provide additional opportunities for solving qualimetry model inverse problems. Among the two main types of modeling – analytical and simulation – simulation models (SM) have much broader capabilities to reflect key factors of complex random processes. At the same time, despite the rapid development of distributed computing technologies, SM remains the main processor time consumers. Analytical models (AM) provide much higher efficiency in calculations, but conceding to SM in terms of adequacy of the CP display. In conditions when the calculations efficiency is a priority requirement for modeling, parametric adaptation of AM (adjustment, parameters correction to the variable conditions of CP simulating) is an effective way to increase the models' adequacy while maintaining the calculations' efficiency. Solving the inverse qualimetric tasks in this way is a relevant practical task, which led to the article's topic choice.

Materials and Methods

To avoid terminological divergences in the quality of model adequacy definition, the following is accepted (Moiseiev, 1981), (Ahrem, 2007), (Rumiantsev, 2010): it is the ability of the model to take into account the most significant factors that affect the course of the CP. The SM essence implies the rationality of reflecting all stages of the modeled process while maintaining the logical sequence of their course in time, and taking into account random, difficult to formalise factors using pseudo-random variables with appropriate laws of their distribution. Along with the possibility of using almost the entire arsenal of analytical modeling methods in SM, this ensures CP' sufficient description detailization and potentially high adequacy of such models (of course, they must pass all verification stages). In the absence of real data on the course of the CP, the simulation modelling results can serve as a reference, a benchmark in relation to the AM. In this case, with the comprehensive use of AM and SM, a possible variant of the AM parametric adaptation task is presented as follows.

The article considers a poly-model complex (PMC) designed to predict probable variants of the CP's course and developing controlling influences (CI) based on the calculations results. The PMC includes a reference simulation model (IM_e) and analytical models' plurals $\{AM_a\}$, $a = \overline{1,A}$ with a simplified process description, which provide the necessary efficiency of modeling and obtaining the entire set of calculated indicators $(\bar{Y})$ required for the CI production. If it is necessary to develop the CI as a response to changes in the CP' course, time restrictions are imposed on the time of obtaining the $(\bar{Y})$ indicators. Such limitations determine the possibility of using IM_e only at the stage of preliminary forecast calculations of possible options for the CP development, with its beginning and, if necessary, in response to changes in its course, the capabilities of the complex set $\{AM_a\}$ are used exclusively. In order to ensure the AM' adaptation to changes in the conditions of CP modeling, it is necessary:

1) to determine, with regard to the entire set of l parameters $\bar{P}_l^{(a)}$ of each a-th analytical model of the PMC, the appropriate order of their coordination with similar parameters obtained by simulation modeling $(\bar{P}_l^{(e)})$. The use of agreed parameters in AM should minimize the current deviation (absolute or relative, ΔY) between the results of analytical and simulation modeling, while such deviation cannot exceed some established limit value (ΔY_D):

$$\begin{gathered}\Delta Y_{min}\left[AM_a\left(\bar{P}_l^{(a)}\right); IM_e\left(\bar{P}_l^{(e)}\right)\right] \le \Delta Y_D; \\ \overline{P_h}^{(a,e)} = \left\{P_1^{(a)}, \dots, P_l^{(a)};\ P_1^{(e)}, \dots, P_l^{(e)}\right\},\ \ l = \overline{1,L}.\end{gathered} \tag{1}$$

2) to numerically assess the possibility of ensuring the AM adequacy to the changes in simulated CP conditions by matching the analytical models' parameters with the reference SM parameters.

Based on the results of the required runs number IM_e, the parameters $(\bar{P}_l^{(e)})$ will be obtained in the statistical data form. The adjusted parameters $(\bar{P}_l^{(a)})$ can be presented in the form of mathematical expectations' estimates (based on the statistical data processing results) and as variable values. Depending on the analytical models' class included in the PMC, the use of the obtained distributions makes it possible to use them to refine the AM parameters in various ways. To illustrate, let's assume that the indicators' analytical calculation $(\bar{Y})$ is carried out by means of differential equation systems. In this case, the totality of parameters $(\bar{P}_l^{(a)})$ the coefficients on the variables and the free terms of the equations will be acting. An explanation regarding the refintment order for clarifying the AM parameters can be demonstrated in the following example.

Let that with help of the PMC, the course and results of combat actions are been modelled, and one of the necessary totality indicators $(\bar{Y})$ is the number of opposing groupings at certain moments

of time, which are analytically determined by modifying analytical Lanchester models (Fursenko and Chernovol, 2020). Let's also assume that, under tasks conditions, such an AM should take into account the recovery of parties' numbers (instead of the lost ones) and has the form the following equations system:

$$\begin{cases} \frac{dx}{dt} = (-c - b)y + d[x(0) - x]; \\ \frac{dy}{dt} = (-g - f)x + h[y(0) - y], \end{cases} \quad (2)$$

where x, y are the numbers of opposing groupings at time t ≥ 0;

x(0), y(0) – initial conditions of the groupings' number at the action starting moment (t = 0);

c, g, b, f – intensity of the parties' losses due to the impact of different types of armaments;

d, h – the intensity of the parties' numbers recovery.

Despite the uniqueness of each combat plans implementation, the general trends in such a joint venture development, proceeding, in particular, on previous experience in similar conditions, are approximately known. That is, some averaged values of the AM parameters are also known, assuming, for example, that the parameters *c*, *g* and *b*, *f* characterise losses from the effects of planar and point means of destruction, respectively. A variant of such parameters can take the following values (Table 1):

Table 1. Variant of the averaged (based on the AM results) parameters' values $\overline{P_l}^{(a)}$ of the equations system (2)

x side	***c***	***b***	***d***
	0,0087	0,0121	0,0179
y side	***g***	***f***	***h***
	0,0107	0,0058	0,0264

For combat actions' particularised conditions and for the purpose of AM type parametric adaptation (2), based on simulation modelling results obtained the mentioned parameters distributions and the CP sought indicator values (in this case, the number of opposing parties x_{IM_e} and y_{IM_e} at a combat actions' certain moment of time). In accordance with the assigned task, it is necessary to minimize the discrepancy between the CP indicators obtained by analytical and simulation way, with simultaneous compliance with the condition $\Delta Y \leq \Delta Y_D$. It can be concidered that for the type of model under consideration, the permissible deviation limits are about 15 % ($\Delta Y_D \approx$ 15 %). The deviation, i.e., ΔY, could be estimated using a well-known expression to determine the calculations' relative error (regarding the defined indicators):

$$\delta_x^* = \frac{|x_{IM_e} - x_{AM}^*|}{x_{IM_e}} \cdot 100; \quad \delta_y^* = \frac{|y_{IM_e} - y_{AM}^*|}{y_{IM_e}} \cdot 100, \quad (3)$$

where x_{AM}^*, y_{AM}^* - the numbers of parties' opposing groupsings at a certain moment of time, established by the results of analytical modeling with adjusted parameters; deviations for AM with averaged parameters are determined in the same way (denoted by $\delta_{x,y}$, respectively).

In fact, expression (3) can serve to numerically evaluate the level of analytical modeling adequacy to simulation in the CP complex modeling.

The choice of parameters' form that can be used as corrected parameters in the ($\overline{P_l}^{(a)}$), is is determined by the look of the obtained statistical distributions and the results of the relative deviations assessment $\delta_{x,y}$. In view of the above, mathematical expectation estimates (MEE) of the obtained

data ($\tilde{m}[\, x_{IM_e};\, y_{IM_e}]$), are used as refined parameters, i.e. model (2) will appear as a system of linear non-homogeneous equations. Let us assume that, based on the results of simulating the CP specific conditions, the following assessments MEE of the system parameters' statistical data (2) were obtained, Table 2:

x side	***c***	***b***	***D***
	0,0141	0,0152	0,0302
y side	***g***	***f***	***H***
	0,0137	0,0078	0,0264

For certainty, let us assume that the analysis of actions is carried out on a time interval up to t = 5 (days) with arbitrarily taken initial conditions x(0) = 30000; y(0) = 25000. The indicators' values obtained by IM_e, are: $\tilde{m}[\, x_{IM_e}(5)] = 23173$; $\tilde{m}[y_{IM_e}(5)] = 19051$. Comparative estimates of the system numerical integration results (2) for the certain initial conditions are shown in Fig. 1 It is also clear that changing (adjustment) the parameters of such an AM type determines the necessity of assessing the stability (in the Liapunov sense) of the decicions obtained. For the parameters of Table 2 and the type system (2), the determinant is represented as:

$$\begin{bmatrix} -0{,}0302 - k & -0{,}0293 \\ -0{,}0215 & -0{,}0264 - k \end{bmatrix}, \tag{4}$$

respectively, the characteristic equation:

$$k^2 + 0{,}0566k + 0{,}000167 = 0, \tag{5}$$

roots: k_1=-0,0031,k_2=-0,0535.

The roots type meets the conditions for the stable decicions existence.

The established constraint assessment carried out in accordance with (2), let us affirm that the use of the refined parameters ensures a reduction in the deviation of the simulation and analytical modeling results to the permissible difference, from δ_x=19,23 % and δ_y=19,56 % to δ_x^*=15,68 % to δ_y^*=16,27 %, see Fig. 1.

The CP physical essence and the simulation results indicate the nececity to take into account the influence of a random factors' plurals, the reflection of some CP factors is possible in the AM form as stochastic differential equations (SDE) systems (Debrabant, Roessler, 2008), (Clauden, 1992). Thus, for the considered conditional variant, the parameters' statistical series (in the form of histograms) are presented in Fig. 2. An example of a simulation, given, let us suppose, for the parameters *b* and *d*, is obtained from the results of 40 independent runs IM_e and grouped into 10 digits of their values (I_i).

Histograms view of the statistical series indicates that the obtained parameter b values are grouped around the statistical average, while the parameter d values have a pronounced character of small fluctuations over the entire interval of their possible values. Under the condition that similar character will be seen in other equivalent parameters of system (2), such a model can be represented in the form of a stochastic differential equations (SDEs) system (Byram, Partal, and Buyukoz, 2018), (Allen, 2007), (Wang, 2016) with multiplicative Wiener noise. In this case, taking into account the Table 2 data, the system of SDEs is presented as follows:

$$\begin{cases} \frac{dx}{dt} = -0{,}0293y + 0{,}0302[x(0) - x]dw; \\ \frac{dy}{dt} = -0{,}0215x + 0{,}0264[y(0) - y]dw, \end{cases} \quad (6)$$

dw – random Wiener process implemented as: $dw = \varepsilon\sqrt{dt}$, $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n), \varepsilon_i \sim N(0,1)$ – normal distribution with zero average and unit variance.

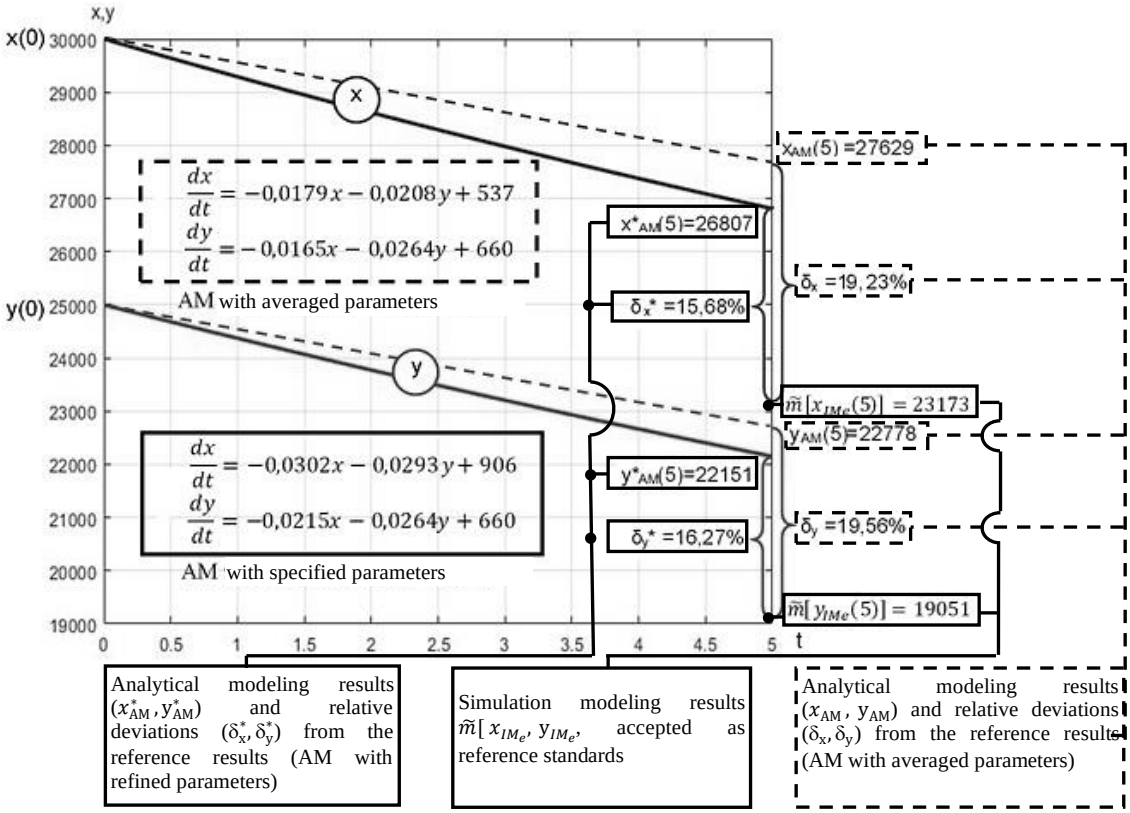


Figure 1. Simulation results and analytical modeling comparison; system solution (2) for the initial conditions with the parameters of Tables 1 and 2

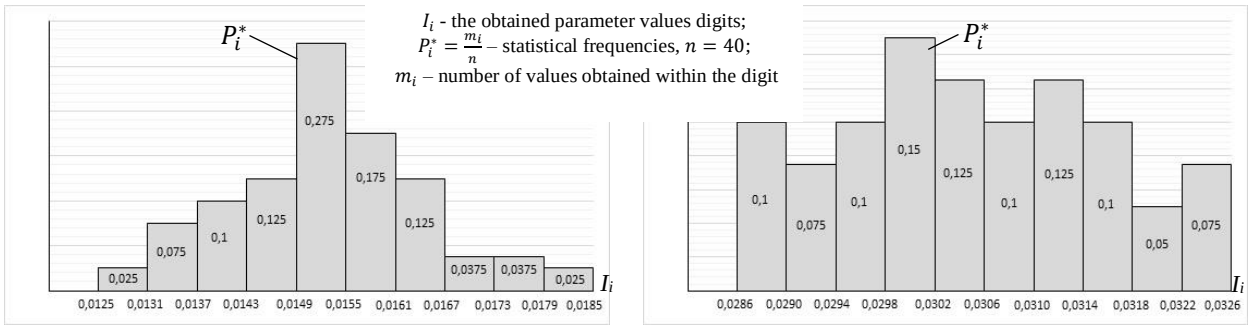


Figure 2. Histograms of system parameters statistical series (2):
a) parameter *b*; b) parameter *d*

The use for the purpose of solving system (6) of specialised methods of PDE numerical integration (Lukshin and Smirnov, 1990), (Averina and Artemev, 2005), (Tocino and Ardanui, 2002) allows to obtain results in the form of both approximate strong and approximate weak decisions.

Weak decisions are used to find the probability distributions of the desired values, at the same time, individual realisations are not crucial. In the context of the AM parameter adaptation task (based on simulation calculations), the obtained probability distributions for weak solutions are of greater interest. The results of numerical solution system (6) by the Milstein method (in the weak sense) are presented in Fig. 3.

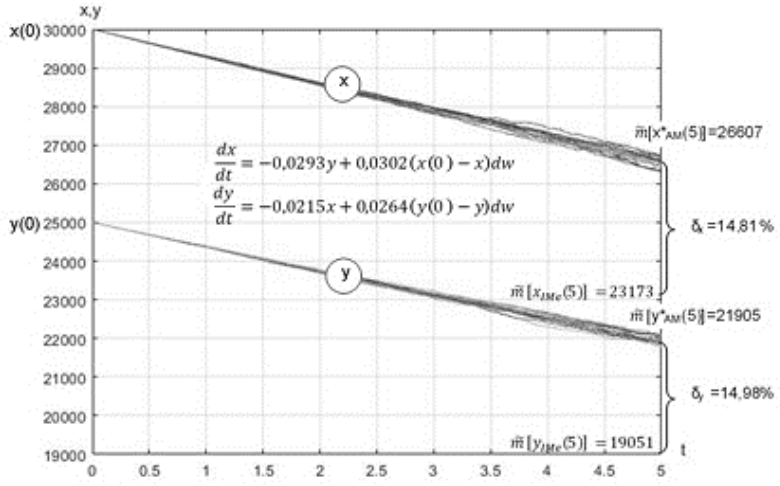


Figure 3. The system solution's results (2) for the defined initial conditions by the Milstein method (fragment for 20 trajectories)

Assessing the solution's stability, as in the ordinary differential equations' case, is an important model's qualitative characteristic (6), but in the case of using SDE, the stability concept has a somewhat broader interpretation, in particular it is related to the methods of solving the such equations (Lukshyn and Smyrnov, 1990), (Averina and Artemev, 2005), (Carletti and Berraj, 2004). Taking into account the statements by Lukshyn and Smyrnov (1990), Mao (2007), and Averyna and Artemiev (2005), as well as the confirmed stability of the deterministic basic system (Fig. 2), the results of solving (6) are considered stable. For their type shown in Fig. 3, the relative deviations of the selected indicators (δ_x та δ_y), calculated from the MEE distributions for 10,000 system realizations (6) are δ_x = 14,81 %; δ_y = 14,98 %. In other words, the condition $\Delta Y \leq \Delta Y_D$ is met in this case, which indicates that the AM is satisfactory level of adequancy.

Result

The given simplistic example demonstrates the necessity for a reasonable choice of the refined parameters application form, as a result of the all the data analysis of the CP simulation modeling. Similarly, the parameters' form is refined in the case of a significantly non-stationary process (O. Mashkin, 2020), i.e., an of AM form example (2) will reflect the process as a system of linear non-stationary equations (or combined, as a system of non-stationary SDE). If the reasonable use of the refined parameters established forms does not ensure the fulfillment of the condition $\Delta Y \leq \Delta Y_D$, this will indicate the necessity to adjust the type or class of the AM itself, not just its parameters. So, only when the detailed simulation and analytical modelling results of unique CP achieve convergence (within certain bounds), we can talk about the possibility of elaborating a CI based on the analytical calculation results.

In addition, practical calculations have confirmed that increasing the number of simulation runs (with further AM parameters refinement in the manner considered) also contributes to ensuring the consistency of the heterogeneous modeling results, and, accordingly, to increasing the AM adequacy.

Discussions

Models' parametric and structural adaptation are covered in thematic publications (in particular, S. Mikoni, B. Sokolov, R. Yusupov (2018), B. Sokolov, R. Yusupov (2004), M. Moiseiev (1981)) as appropriate methods for ensuring the necessary models' qualitative properties. However, the recommendations in these sources are mostly a general theoretical nature and are limited to models of real-world objects-originals. Besides, the absence of a well-established terminology base in the field under consideration adds certain difficulties in solving this problem. Discrepancies in the understanding of the concept of model adequacy, different opinions on the principal possibility and methods of quantifying the adequacy of SP unique models do not contribute to the unambiguous establishment of such a qualitative characteristic from the qualimetric point of view. According to the right remark of the authors S. Mikoni, B. Sokolov, R. Yusupov (2018), summarising the results of applied research in the area under consideration should become the basis for further development of this promising scientific and practical direction.

Conclusion

The solution of the inverse qualimetric problem in the combined display of unique SPs through AM parametric adaptation will require, first of all, the formation of a PMC as part of coordinated CP analytical and simulation models, in which at least one (or a single) simulation model should serve to obtain reference results. Thus, the appropriate course of action regarding adapting the AM parameters is presented in the following sequence:

- Identification of the analytical models' most important parameters are in need to be refined by simulation;

- determining the distributions of parameters by runs of reference AM for the most predictable variants of the CP' course;

- use of the parameters refined by simulation in analytical models in the form determined by the simulation results analysis (the form of the statistical data set), the class of analytical models used and the peculiarities of their software implementation;

- assessing the mutual deviation of analytical and simulation modelling results, adjusting (combining), if necessary, the forms of the refined parameters applied. In the case inability to comply with the requirement for consistency of heterogeneous modelling results, the type of analytical models used will be needed to be clarified.

That is, analytical models' parametric adaptation can be considered an effective element of solving one of the key tasks of model qualimetry, that is, ensuring their necessary qualitative properties in the complex application of complex processes heterogeneous models.

The further research prospect is to consider the questions of SM structural adaptation to determine the necessary data for the parametric adaptation of AM.

References

1. Averina, T. A., Artemev, S. S. (2005). Numerical solution of stochastic differential equations with increasing dispersion (in russian) // Siberian Journal of Computational Mathematics. Novosibirsk: Siberian Dept. RAS and IVMiMG, Vol. 8, No. 1. P. 1-10.
2. Allen E. (2007). Modeling with stochastic Ito differential equations. Mathematical modeling: theory and application. Issue 22.
3. Ahrem A. A. (2007). Mathematical methods for analyzing the adequacy of complex technical objects' models. *Proceedings of the ISA RAS*. T. 29. P. 245-264.
4. Bayram Mustafa, Partal Tugcem, Buyukoz Gülsen Orukova (2018). Numerical methods for modeling stochastic differential equations.
5. Bozhenko, L. I.; ed. Kryuchkevich, L. I. (2003). Standardization, metrology and qualimetry in mechanical engineering: [textbook for universities]. Lviv: Svit. 328 p.

6. Butvin, B. I., Mashkin, O. O., Sobolev, O. M., Mykhalevych, V. E., Open'ko, P. V., Maslenko, S. V. (2022). Parametric Adaptation as an Element of Mathematical Models Qualimetry of Complex Processes. *Advances in Military Technology*, Vol. 17, No. 2. P. 427-437.
7. Gevorgyan, E. S. (2022). Fundamentals of qualimetry: Lecture notes. Kharkiv: UkrDUZT, 84 p.
8. Carletti, M., Berraj, K. (2004). Numerical modeling of stochastic ordinary differential equations in biomathematical modeling. *Math. comput. simul*. T.64(2). P. 271-277.
9. Cloden, Peter E. and Platten, Eckhard (1992). Applications of stochastic differential equations. In: *Applications of Mathematics* (SMAP). T.23. P.253-275.
10. Kuts, V. R., Stoliarchuk, P. G., Druziuk, V. M. (2012). Qualimetry. Ministry of Education and Science, Youth and Sports of Ukraine, Lviv Polytechnic National University. Lviv: Lviv Polytechnic Publishing House. 256 p.
11. Lukshin, A. V., Smirnov, S. N. (1990). Numerical methods for solving stochastic differential equations (in Russian). *Mathematical modeling: journal*. Moscow: Keldysh Institute of Applied Mathematics of the Russian Academy of Sciences. T. 2, № 11. P. 108-121.
12. Mao, X. (2007). Stochastic Differential Equations and Applicatios. 2nd edition. Elsevier, 9, 12, 13, 17.
13. Mashkin, O. O. (2020). Features of the numerical solution of Lanchester-type models differential equations in a stochastic formulation. *Information Processing Systems*: scientific and technical journal: KhNUPS named after I. Kozhedub. Kharkiv. № 1 (160). P. 67-72.
14. Mikoni, S. V., Sokolov, B. V., Yusupov, R. M. (2018). Qualimetry of models and polymodel complexes: monograph: RAS. 314 p.
15. Moiseiev, N. N. (1981). Mathematical problems of system analysis. Moscow: Nauka. Main edition of physical and mathematical literature. 488 p.
16. Rumiaantsev, M. I. (2010). On the issue of assessing the adequacy of simulation models of banking business processes. *Modern problems and ways of their solution in science, transport, production and education*: a collection of scientific papers on the material of the international scientific and practical conference (Odesa, 19th of November). Odesa: Black Sea. VOL. 15, PP. 84-93.
17. Sokolov, B. V., Yusupov, R. M. (2004). Conceptual and methodological bases of qualimetry of models and polymodel complexes (in Russian). *Proceedings of SPIRAN*. Issue 2, Vol. 1. P. 10-35.
18. Sokolov, B. V., Yusupov, R. M., Mikoni, S. V. (2014). Qualimetry of models and polymodel complexes: state of research and prospects for development. Sankt-Petersburg: TsNII Elektropribor. P. 44-53.
19. Sokolov, B. V., Yusupov, R. M. (2004). Conceptual foundations for evaluating and analyzing the quality of models and polymodel complexes (in Russian). *Theory and systems of management*. Moscow. № 6. P. 5-16.
20. Tochino, A., Ardanui, R. (2002). Runge-Kutta methods for numerical solution of stochastic differential equations. *Journal Computational Mathematics*. No 138 (2). P. 219-241.
21. Fursenko, O. K., Chernovol, N. M. (2020). Lanchester models of combat operations. *Collection of scientific works of Kharkiv National University of the Air Force*. №4(66). P.85-91.
22. Tsyba, V. T. (1997). Fundamentals of the theory of qualimetry. *Study guide*. Kyiv: Institute of Content and Methods of Education of the Ministry of Defense of Ukraine. 160 p.
23. Shapoval, M. I. (2002). Quality management: a textbook. Kyiv: Znannia.
24. Debrabant, K. and A. Roessler (2008). Classification of Stochastic Runge-Kutta Methods for the Weak Approximation of Stochastic Differential Equations. *Mathematics and Computers in Simulation*, 77(4), pp. 408-420.
25. Wang, Liguo (2016). Numerical Solutions of Stochastic Differential Equations. PhD diss., University of Tennessee. https://trace.tennessee.edu/utk.graddiss/3974.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.13

The sufficiency of the State's economic capabilities to ensure the necessary level of defense needs forecasting improving method

Oleh Semenenko
Doctor of Military Sciences, Professor
Head of Department
Central Research Institute of the Armed Forces of Ukraine
03049, Air Force of Ukraine Avenue, 28 B, Kyiv, Ukraine
e-mail: aosemenenko@ukr.net
ORCID: 0000-0001-6477-3414

Maryna Abramova
Philosophy Doctor in Economy, Senior Researcher
Central Research Institute of the Armed Forces of Ukraine
03049, Air Force of Ukraine Avenue, 28 B, Kyiv, Ukraine
e-mail: Elaira3@gmail.com
ORCID: 0000-0001-7644-9988

Maria Yarmolchik
Head of the research laboratory
Department of Military Training of the National Aviation University
Kyiv, Ukraine

Abstract. The concept of sufficiency is closely related to the economic forecasting ability to set realistic and achievable goals for the economy as a whole development. Forecasting opportunities is a critically important tool that takes into account the current State of the economy, sets goals for future development, and also determines the necessary tools of State regulation to achieve them. Ultimately, the adequacy of economic opportunity can be assessed using these forecasting approaches because they aim to balance what is realistically achievable against the current State of the economy. The initial step in this process involves the formation of conceptual approaches that pave the way to the creation of a comprehensive system of forecasting the economic capabilities of the State to ensure the necessary level of defense needs. The article presents the results of the assessment of the individual economic capabilities of such countries as Norway, France, Finland, the USA, Sweden, Great Britain and Israel, taking into account the level of economic stability of the countries and the coefficients of stability of changes. By means of an expert survey, a list of possible threats and scope of implementation of different levels of protection was determined, taking into account the dependence of defense needs on the stability of funding and the stability of its changes. The averaged values of the limits of the corresponding levels of defense needs until 2033 inclusive are also determined. To predict the sufficiency of the State's economic capabilities ensuring the necessary level of defense needs, the Lagrange interpolation method was used, with the help of which 5 possible directions of the development of the situation were identified. The results of using the appropriate method were the provision of recommendations based on the following characteristics: for countries that do not meet the selection criteria (Lithuania, Latvia, Estonia, Germany, Hungary and Poland); for countries with a "wave-like" trend, which characterizes the instability of State policy (France and Finland); for countries with a "wave-like" trend and a high potential for self-sufficiency and characterized by the instability of State policy (Norway); for countries that have the potential for gradual growth, using their own economic opportunities; may be characterized by over Stated defense needs (USA, Sweden and Great Britain); for countries with a high potential of their own capabilities (Israel). Thanks to this distribution, it is

possible to examine potential future trends in the development of economic capabilities of countries and compare them with the determined levels of defense needs.

Keywords: capabilities, forecasting, sufficiency, defense need, threat.

Introduction

Ensuring adequate funding for national defense is a critical aspect of ensuring the country's stability and security. In this context, improving the methods of forecasting the sufficiency of the State's economic capabilities to ensure the necessary level of defense needs can not only help to accumulate resources, but also be the basis for developing an effective long-term policy.

Accurate forecasting depends on the availability of reliable information and the use of appropriate analytical methods (Freiman, 2017). However, in many cases the data required for this is either absent or insufficient, leading to inaccurate predictions. Rapid changes in economic and political conditions can significantly affect defense needs and the resources needed to meet them (Hnatenko, 2021). In addition, rapidly developing technologies such as artificial intelligence also create uncertainty in the defense landscape (Koval, 2023). Due to uncertainty about future threats and military needs, it is much more difficult to predict the sufficiency of the State's economic capabilities to meet defense needs, and with the development of global security threats, it becomes increasingly difficult to predict the exact nature and scale of future military needs (Sarana, 2010).

To overcome this uncertainty, it is advisable to focus on improving the understanding of potential future threats and develop comprehensive strategies for responding to a wide range of scenarios (Chambers, Satinder, 2016), which currently do not take into account some modern features of the formation of initial data.

Methodological Framework

The analysis of historical data and trends is an important aspect of forecasting the adequacy of the State's economic capabilities (Everett, 2021). This method involves studying past economic indicators and identifying patterns that can provide valuable information concerning the future prospects (Ritis, 2017). To detect deviations, time series methods may be used, in particular, taking into account seasonal pulses, level shifts and time trends.

The study of the current economic conditions and policies is another important component of forecasting the adequacy of the State's economic capabilities (Gompert, Oliker). This involves assessing the current state of the economy, examining various economic indicators and evaluating the effectiveness of existing policies. And the development of future scenarios and forecasts is the final stage of forecasting the sufficiency of the State's economic capabilities (Market Research Methods for Economic Forecasting, 2021). This process involves the creation of various possible economic scenarios based on historical trends, current conditions and expected changes in the future (Hatcher, 1994).

Threat and risk assessment plays a critical role in meeting defense needs. Threat modeling, for example, is a proactive strategy for determining their impact on cyber security, which involves identifying potential threats and developing appropriate countermeasures (Nicastro, 2023). Another important approach is to use updated threat and risk assessment guidelines that offer resources and strategies for security professionals (Yoder, 2023). In the context of national security, SWOT analysis (Strengths and Weaknesses, Opportunities and Threats) is often used, although open sources do not provide a generally accepted risk assessment methodology for national security strategy (Petropulps, 2022). These methods help identify and understand various threats that may affect the country's defense needs. One approach to addressing this issue is security risk assessment, which identifies, evaluates, and implements key security controls with a focus on preventing flaws (Kvin, 2016). Ultimately, understanding defense needs is essential to developing and implementing an effective defense strategy, which involves analyzing different alternatives and determining the best

course of action.

Therefore, there is a need for long-term provision of the necessary level of defense needs, which is difficult to provide without sufficient economic capabilities of the State, and their assessment and search for ways to increase is the key to more reliable forecasting and planning.

Results

The importance of the economic capabilities of the State for defense needs forecasting cannot be overestimated. Ensuring that a nation has the necessary economic capacity to meet its defense needs is a critical component of national security and planning. Therefore, a competent implementation of the corresponding forecast allows for a more efficient allocation of resources, prioritization of defense-related investments, and maintenance of a strong and stable defense-industrial base capable of responding to new threats and challenges. For example, one of them is the need to substantiate the annual defense budget and develop medium- and long-term defense planning, which requires a deep understanding of the functioning of the defense planning system as well as the military-economic justification of programs, and this is impossible without a clear understanding of economic opportunities.

Therefore, the provision of sufficient economic capabilities for defense needs is of prime importance for the defense of the State, especially in times of conflict. A well-funded defense system plays a critical role in maintaining national security and maintaining stability. For this, it is important to have a method of forecasting the sufficiency of the State's economic capabilities to ensure the necessary level of defense needs, the results of which can most accurately reflect the future possible state of the State's economic capabilities.

The first feature the method given in this work is the use of the following key factors that should be taken into account when forecasting the sufficiency of the State's economic capabilities to ensure the necessary level of defense needs: determining the volume of the Gross Domestic Product (GDP), the level of employment, the availability of labor, taking into account income inequality and the size of the gap poverty (Fig. 1), etc.

The second feature there is an individual consideration of each State, without taking into account their bloc affiliation, and therefore the goal that have been set - the possibility of achieving the necessary level of economic opportunities only by the of one's own economy powers. (To compare the results, statistical data from the following countries were also used: Lithuania, Latvia, Estonia, Norway, Sweden, Finland, Germany, France, Hungary, the USA, Poland, Israel and Great Britain).

The third feature is taking into account the dependence of economic opportunities on the economic stability of the country (SC) and the stability of changes (SCh) within the economy. These indicators were calculated for all components of Block 1 "Assessment of the adequacy of the State's economic capabilities" (Fig. 1) and, taking them into account, the corresponding coefficients were determined. calculated by taking into account the standard deviation over a specified period of time, which is a measure of the variability or dispersion of a data set, and in this context it is used to estimate the variation of a country's indicator over time. To calculate the standard deviation, you first need to find the mean) value for the same time period, and then determine the difference between each individual item value and the mean. These differences are squared, and the mean value of these squared differences is found. Finally, the square root of this mean is taken to obtain the standard deviation.$SC^n SCh^n SC^n$

With the help of this calculation, you can better understand the consistency and predictability of the country's economic indicators. After calculating the standard deviation, the last step is to divide the standard deviation by the average value for the same time period to obtain the coefficient (Table 1).SC^n

The calculation can be extremely useful for predicting future trends and making informed decisions about the direction of development:$C3^n$

$$SC^n = \bar{x}^m \Big/ \sqrt{\frac{\sum((x^{n1}-x^{n0})-\bar{x}^m)+\cdots+(x^{n14}-x^{n13})-\bar{x}^m))^2}{n-1}},$$

where x^n – the statistical data of the elements of Block 1 (for the years 2010-2023), and $\bar{x}^m$ – the average value of the sample for each group separately (1.1; 1.2; 1.3; 1.4 or 1.5).

However, the results of the calculation of the coefficient of sufficiency of economic capabilities of the State (taking into account the level of economic stability of the State (SC) and the stability of changes (SCh)) made it possible to single out States that have a sufficient reserve (potential) of economic capabilities to ensure the necessary level of defense needs in the future, where the value reflects percentage of possible financial needs of Block 2 "Assessment of the necessary level of defense needs" (Table 2) (Fig. 1?).$SC^n SCh^n NLDN_{HP}$

Table 1. Generalized calculations of the coefficient of sufficiency of the economic capabilities of the State according to $SECL^n \sum \bar{x}^m$

Countries	$SECL^n$ (beginning of 2024)	Countries	$SECL^n$ (beginning of 2024)
Lithuania	-0.0776	France	0.0023
Latvia	-0.1070	Hungary	-0.0973
Estonia	-0.0408	USA	0.0135
Norway	0.0473	Poland	-0.0858
Sweden	0.0455	Israel	0.0301
Finland	0.0018	United Kingdom	0.0204
Germany	-0.1032		

Source: calculated by the authors.

The coefficient of financial dependence proposed for calculation (k) is proposed to be calculated by finding the results of the ratio of the amount of debt to free assets (Table 2).DN_{HP}

Table 2. Generalized calculations of the coefficients of the required level of the State's defense needs for $DN_{HP} \sum \bar{x}^m$(calculated by the author)

Countries	$\boldsymbol{DN}_{HP}$ (beginning of 2024)
Lithuania	0.7259
Latvia	0.7779
Estonia	0.4007
Norway	0.5918
Sweden	0.2664
Finland	0.1400
Germany	0.3492
France	0.3418
Hungary	0.3200
USA	0.3980
Poland	0.4869
Israel	0.4362
United Kingdom	0.1519

Source: calculated by the authors.

Therefore, when assessing the adequacy of the State's economic capabilities, the first priority is the assessment of GDP volumes, which is one of the most important economic indicators used in forecasting methods to assess the adequacy of the State's economic capabilities to ensure the required level of defense needs. And long-term forecasts of a country's GDP can provide valuable information about its overall economic growth and potential for allocating resources to defense spending.

The assessment of the level of employment is important when determining the sufficiency of the economic capabilities of the State to ensure the necessary level of defense needs. A comparison of the structure of employment by types of economic activity and professional groups shows the prevalence of destructive shifts and catastrophic consequences for the economy.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

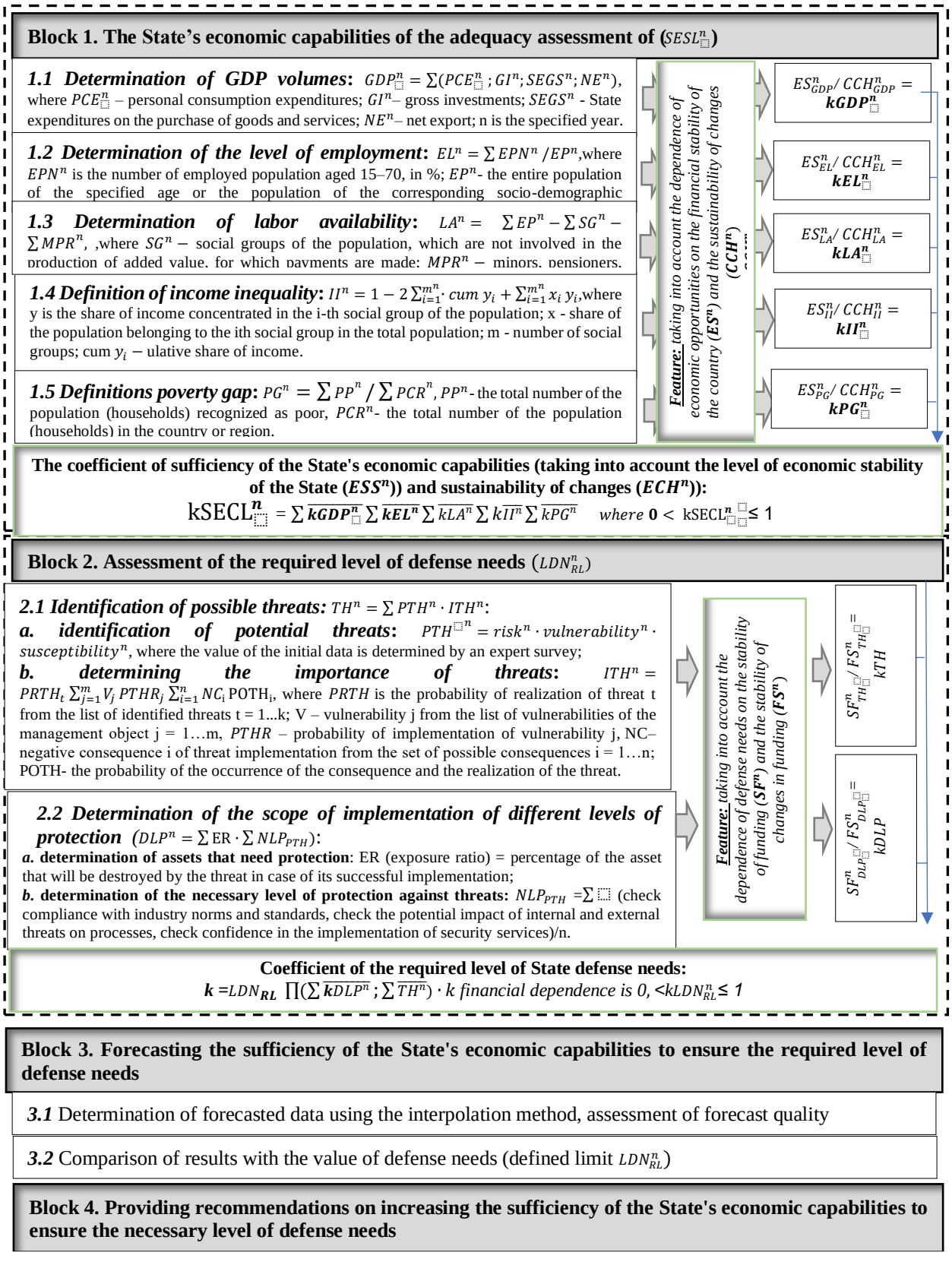


Figure 1. The forecasting method of the sufficiency of the economic capabilities of the State to ensure the necessary level of defense needs stages, without considering the coalition factor schematic representation

Source: suggestions of the authors.

The role of labor availability in the development of economic opportunities is one of the crucial aspects. A strong workforce contributes significantly to economic growth by providing the necessary resources and skills for various industries and sectors. Having a highly skilled and productive workforce can lead to increased productivity, innovation and competitiveness, ultimately strengthening a country's economic status. In addition, its availability helps maintain a stable and prosperous economy by supporting business, generating tax revenue and contributing to economic resilience in times of crisis.

Understanding the use of income inequality as a measure of economic opportunity is critical to assessing a country's economic opportunity (Figure 2). Income inequality refers to the distribution of income among different groups in the population, with greater inequality reflecting large differences between the rich and the poor. This indicator can provide insight into the effectiveness of a country's economic policies and whether they promote growth and equal opportunities for all citizens.

Estimating the poverty gap is a crucial indicator for understanding the scale of a country's economic opportunities (Fig. 3). Its rise can limit human development, ignite large-scale social and political conflicts, and threaten the unity of societies. In addition, economic growth in most developing countries has stalled in recent years, falling from 6% to 4% for the first time in two decades. This stagnation further emphasizes the need to address the problem of poverty and its consequences for the economic capabilities of the State.

Comparing projected economic opportunities with defense needs is essential for a nation's economy to adequately support its defense policy. In Block 2 “Assessing the Necessary Level of Defense Needs”, understanding the scale of potential threats is critical to assessing defense needs, as the growing openness of the international system creates new opportunities and challenges. The reliability of these estimates is vital to the defense analysis process, as it plays an important role in justifying the annual defense budget and ensuring the efficient allocation of resources.

In order to determine the necessary level of defense needs, it is extremely important to first determine potential threats and the probability of their occurrence (in this work, the initial values were obtained by an expert method). This involves analyzing various factors that may pose a threat to national security or organizational stability. For example, you can consider the possibility of disclosure of State secrets, which requires regular checks of personnel to minimize risks. By assessing the likelihood that potential threats will become real, decision makers can prioritize which areas of protection require the most attention and resources.

After determining the potential threats and the probability of their occurrence, the next step is to assess the importance of the threat (in this paper, the initial values are obtained by the expert method). This may include modeling the development of potential threats into actual threats and investigating the negative consequences they may cause. In addition to considering direct effects, it is important to consider indirect effects, such as the weakening of other institutions as a result of the strengthening of one institution. This comprehensive assessment of potential threats and their consequences allows decision-makers to better understand the overall defense landscape and develop strategies to effectively address these challenges.

After determining the potential threats and their impact, it is necessary to determine the cost of implementing different levels of protection (in this work, the initial values are obtained by the expert method). This involves assessing the cost of each proposed measure to eliminate or mitigate adverse safety impacts. In addition, it is critical to identify the parties responsible for implementing these measures, as well as the resources required to achieve the minimum required level of defense objectives. By carefully evaluating the costs and resource requirements associated with different levels of protection, decision makers can make informed choices about the most appropriate and cost-effective protection strategies to implement.

To predict the sufficiency of the State's economic capabilities to ensure the necessary level of defense needs, the method of interpolation of the Lagrange polynomial ($P_n(x)$), which is usually used in

theoretical research (during proving theorems, analytical problem solving, etc.), was used.$P_n(x)$

$$P_n(x) = \sum_{i=o}^{n} y_i \cdot L_n(x),$$

where $L_n(x)$ is the Lagrange multiplier, x −the corresponding variables

$$L_n(x) = \frac{(x-x_0)\dots(x-x_{i-1})(x-x_{i-1})\dots(x-x_n)}{(x_i-x_0)\dots(x_i-x_{i-1})(x_i-x_{i-1})\dots(x_i-x_n)}$$

$$P_n(x) = y_0\frac{(x-x_1)(x-x_2)\dots(x-x_n)}{(x_i-x_1)(x_0-x_2)\dots(x_0-x_n)} + y_1\frac{(x-x_0)(x-x_2)\dots(x-x_n)}{(x_1-x_0)(x_1-x_2)\dots(x_1-x_n)}$$
$$+ y_n\frac{(x-x_0)(x-x_1)(x-x_2)\dots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)(x_n-x_2)\dots(x_n-x_{n-1})}$$

This mathematical method is used to estimate unknown values in a known data set using known values surrounding the unknown value. However, it is also worth noting that, unlike some other interpolation formulas, Lagrange's formula does not require that the points in the set be equidistant from each other. In the context of the economy, it can be used to determine trends and forecast future economic conditions, which, in turn, can inform decision-making processes related to defense needs (Fig. 3 (there is no such figure) shows the forecast of the economic capabilities of States according to conditions $\mathrm{SNEN}^n > 0$, until 2033 inclusive).

The fourth feature of the proposed model is the determination of the limit value of the need for defense sufficiency (Fig. 2 and Fig. 2), which is compared with the financial equivalent: Norway (; Sweden (; Finland (; France (; USA (; Israel (; (from the general dynamics of the calculated values for 2010-2023 (Table 2).$0{,}59 \cdot 100 = 59\%)0{,}26 \cdot 100 = 26\%)0{,}14 \cdot 100 = 14\%)0{,}34 \cdot 100 = 34\%)0{,}39 \cdot 100 = 39\%)0{,}43 \cdot 100 = 43\%)0{,}15 \cdot 100 = 15\%)$ −

To assess the quality of information regarding indicators obtained from forecasting results, an indicator of the size of the sampling error was used. It determines the limits of the confidence intervals of the possible values of the indicator based on the sample survey data. The estimate of the indicator for which the value of the sampling error is significant compared to the value of the estimate itself cannot be used in the analysis of the survey results:

$$\text{Standart error} = {}^{\mathrm{D}^2}/_{\text{Value of the estimate}},$$

where D– dispersion.

The value of the marginal error of the sample determines the limits of the confidence interval for the estimation of the indicator and is calculated according to the formula:

$$\text{Marginal error} = \mathrm{t} \cdot \text{standart error}$$

where t −a confidence number that determines the ratio of the marginal and standard error for this probability.

The marginal sampling error is used to construct confidence limits of estimates (limits of confidence intervals - Fig. 2 and Fig. 3), namely:

$$\bar{y}_{\text{lower}} = \bar{y} - \text{Marginal error};\ \bar{y}_{\text{upper}} = \bar{y} + \text{Marginal error},$$

where $\bar{y}_{lower}$ −the lower confidence limit of the interval estimate of the mean value; the upper confidence limit of the interval estimate of the mean value.$\bar{y}_{upper}$ −

In this paper, the coefficient of variation was used to assess the suitability of the data.

$$k\text{Variation} = {}^{\text{Standart error}}/_{\bar{y}} \cdot 100\%.$$

In our case, the estimates are considered reliable because $k\text{Variation} \leq 5\%$.

So, above is a brief description of the importance of taking into account the elements of Block 1 "Assessment of the sufficiency of the State's economic capabilities", and in fig. 2 and fig. 3 presents the results of calculations of the relevant coefficients. Therefore, the following observations can be made regarding the assessment of the sufficiency of the economic capabilities of the studied States, namely, it is important:

- taking into account the physical size of countries, which depends on the amount of free resources;
- the direction of social policy development aimed at improving human resources and contributing to the improvement of the demographic situation;
- to understand the balance of the policy of long-term development planning of countries with its capabilities;
- Norway (0.0473), Sweden (0.0455) and Israel (0.0301) are currently in the most favorable position;
- such countries as Lithuania, Latvia, Estonia, Germany, Hungary and Poland have insufficient stock of economic opportunities to independently (without the help of the coalition countries) provide for their planned defense needs, therefore it is expedient to develop a coalition action plan (table 2).DN_{HP}

Therefore, the analysis of the results of data interpolation calculations up to and including 2033 made it possible to distinguish four groups of countries:

1 defense needs are partially met by their economic capabilities (Norway); 2 countries whose defense needs are not met by their gradually decreasing economic opportunities (France, Finland); 3 countries whose defense needs are not met by their gradually increasing economic capabilities (USA, Sweden, Great Britain); 4 countries whose defense needs are met by their economic capabilities (Israel).

Therefore, when formulating recommendations on increasing the sufficiency of the State's economic capabilities to ensure the necessary level of defense needs, all five scenarios should be considered (including countries whose initial data did not pass the limitations of the proposed method).

The data forecast for Israel (Fig. 3) is indicative, reflecting the possible accumulated potential of the State's economic opportunities.

According to the obtained results, Block 4 "Providing recommendations on increasing the sufficiency of the economic capabilities of the State to ensure the necessary level of defense needs" can be considered in the above 5 directions:

Recommendations 1 (for countries that do not meet the selection criteria$0 < SNEN^n; DN_{HP}^n < 1$): regarding increasing the sufficiency of the economic capabilities of Lithuania, Latvia, Estonia, Germany, Hungary, and Poland to ensure the necessary level of defense needs (provided that they intend to develop economic capabilities without taking into account the subsidies of countries that are members of blocs, associations, and alliances):

- for Lithuania, Latvia, Estonia and Germany, investment in infrastructure and technology is a priority. As the largest drop in GDP in 2024 is predicted for Estonia, Ireland, Hungary, it becomes important for these countries to focus on developing their infrastructure and technological capabilities. In the case of Lithuania, Estonia and Latvia, there is significant potential for growth due to the development of export investments. Encouraging entrepreneurship and innovation and workforce development is another effective strategy for increasing GDP;
- encouraging foreign investment and trade, as well as improving infrastructure and transport networks, is crucial for Hungary and Poland.

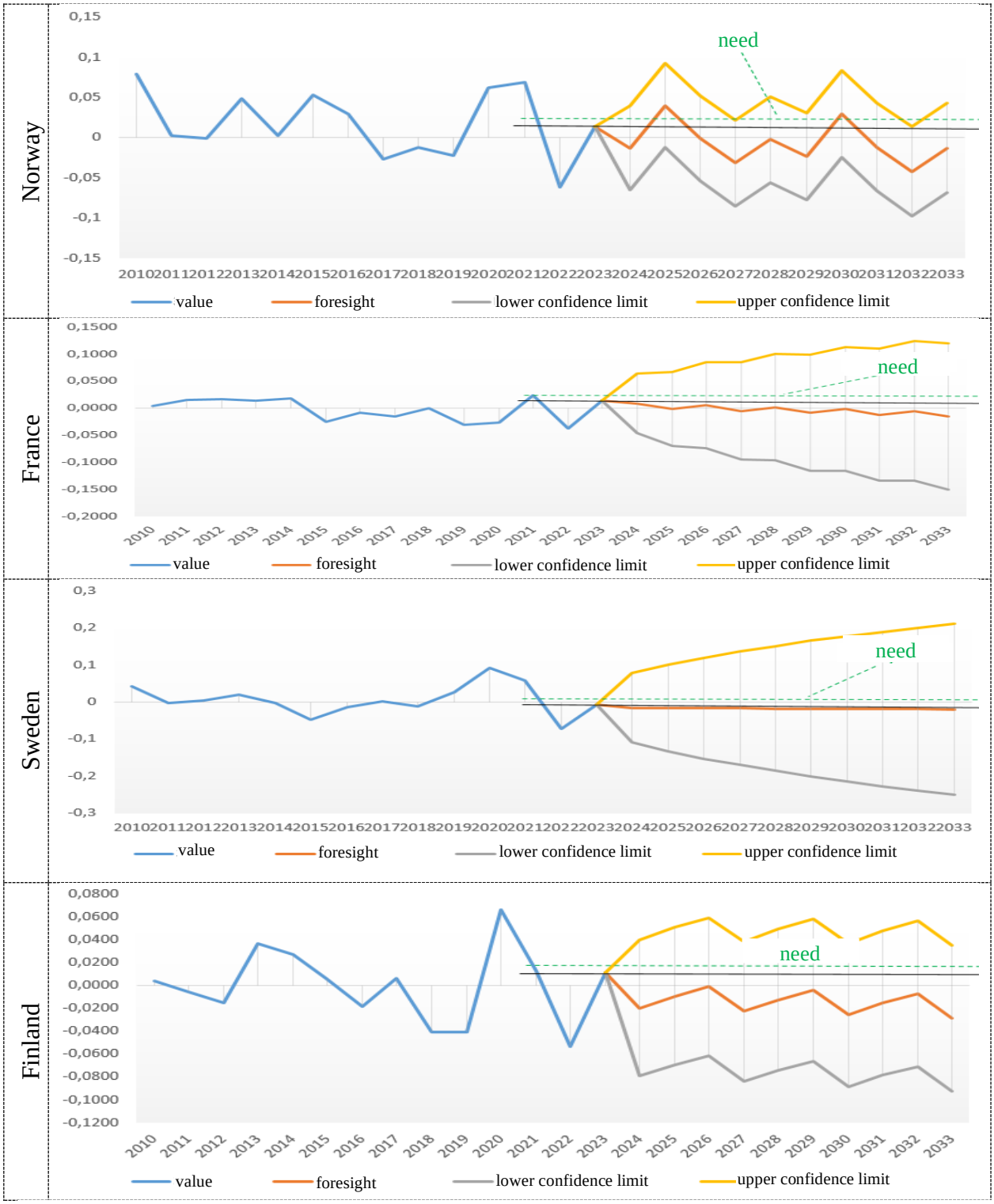


Figure 2. The coefficients of Block 3 "Forecasting the sufficiency of the economic capabilities of the State to provide necessary level of defense needs" calculations results

Source: suggestions of the authors.



Figure 3. Block 3 calculations results for the "Forecasting the sufficiency of the State's economic capabilities to ensure the required level of defense needs" coefficients

Source: suggestions of the authors.

Recommendation 2 (for countries that have a "wave-like" trend, which characterizes the instability of State policy):regarding increasing the sufficiency of the economic capabilities of France and Finland (provided that they intend to develop economic capabilities without taking into account the subsidies of countries that are members of blocs, associations, and alliances):investment in education and professional training programs; encouragement of entrepreneurship and innovation; strengthening international trade and partnership.

Recommendation 3 (for countries with a "wave-like" trend and a high potential for self-sufficiency and characterized by the instability of State policy):regarding the preservation of the sustainability of Norway's economic capabilities (provided the intentions of developing economic capabilities without taking into account subsidies from countries that are members of blocs, associations, and alliances):development and implementation of sustainable business practices; investments in renewable energy sources and clean technologies; promotion of sustainable tourism and travel.

Recommendation 4 (for countries with the potential for gradual growth using their own economic capabilities; may be characterized by over stated defense needs):regarding increasing the economic capabilities of the USA, Sweden, and Great Britain (provided that they intend to develop economic capabilities without taking into account subsidies from countries that are members of blocs, associations, and alliances):support of small and medium-sized enterprises (SMEs) and startups; encouragement of entrepreneurship and innovation; development of renewable energy sources.

Recommendation 5 (for countries with a high potential of their own capabilities): regarding the preservation of the stability of Israel's economic capabilities (provided the intentions of developing economic capabilities without taking into account subsidies from countries - members of blocs, associations, alliances): investments in renewable energy sources; promoting sustainable business practices; reducing the level of threats.

Therefore, the use of an improved method of forecasting the sufficiency of the State's economic capabilities to ensure the necessary level of defense needs makes it possible to determine the current capabilities of countries' economies, interpolate them and evaluate them taking into account defense needs, without taking into account bloc cooperation (support).

Discussions

When studying various scientific works, publications and methodical documents on forecasting the sufficiency of the State's economic capabilities to ensure the required level of defense needs, which are publicly available, no full-fledged appropriate calculation method was highlighted. Instead, L. Nicastro (2023) takes the position that the analysis of economic trends and defense needs is an important step in forecasting the sufficiency of economic opportunities to meet the required level of defense needs. Yoder N. (2021) believes that the national defense strategy serves as a plan for the development of defense capabilities in the present and future and strengthens the economy, and Petropoulos F. (2021) is of the opinion that in order to make informed decisions about defense investments and capabilities, politicians should take into account various factors such as industrial potential, technological progress and the State of the State's economic capabilities. By examining these factors in the context of economic trends, decision makers can gain valuable information about the potential challenges and opportunities facing the defense industry and the economy as a whole.

Over the past 15 years, progress in the theory and practice of forecasting has led to the creation of various models and methods of forecasting economic trends (Poledna S. (2022)). One such example is the agent-oriented model (AOM), which has demonstrated its ability to compete with benchmark VAR and DSGE models in out-of-sample forecasting of macro variables. These models can be applied to specific industries, such as high-tech sectors, to provide valuable information and guidance for economic forecasting.

According to Bezrukova T. (2014), using the most modern models and methods, researchers and politicians can more accurately forecast economic opportunities and challenges, which allows them to make informed decisions about defense investments and potential. And assessing the sufficiency of economic opportunities to meet defense needs requires a comprehensive understanding of both the current State of the economy and future trends (Hicks H. (2022)). This involves evaluating a wide range of indicators and using modern forecasting models to predict the future economic landscape. Based on such assessments, appropriate recommendations can be developed.

Conclusions

The imperfection of the researched approaches to forecasting the sufficiency of the State's economic capabilities to ensure the necessary level of defense needs requires the use of additional factors to correct the obtained results. The method proposed by the authors takes into account the following features: GDP volume, employment rate, labor availability, income inequality, poverty gap, level of potential threats, opportunities to protect against them, etc.

It is innovative to consider the coefficients of the country's economic stability and stability of changes, as well as taking into account the dependence of defense needs on the stability and stability of funding changes when determining the results of the sufficiency of the State's economic capabilities. A valuable stage for researchers of this issue is the identification of countries (in accordance with the specified conditions), potential opportunities for raising the level of economies that are unlikely without considering the coalition factor (Lithuania, Latvia, Estonia, Germany, Hungary, Poland).

The proposed method made it possible to assess the capabilities of the economies of the studied countries until 2033 inclusive. Based on this, proposals were made for countries that adhere to the "wave-like" model of State policy, for example, France and Finland; Norway, whose economy is characterized by a high degree of self-sufficiency.

In addition, the recommendations refer to countries that have demonstrated the ability to grow at a slow pace while maintaining their own economic capabilities, which are potential candidates for increased defense spending (eg, the United States, Sweden, and the United Kingdom). Finally, countries with a high potential for self-sufficiency, such as Israel, were also considered. This distribution of ratings made it easier to study the potential future growth of economic capabilities of these countries and helped to compare these potential defense levels with the currently determined levels of defense needs.

A further area of research is forecasting the sufficiency of the State's economic capabilities, considering a larger number of factors that can have a potentially significant impact on the level of the State's defense needs.

Recommendations

The results of the above material will be of interest to researchers who are engaged in methods of increasing the potential of the State, ensuring the long-term economic capabilities of the State, increasing the levels of defense capabilities, assessing the ratio of the volumes of defense needs and the actual capabilities of economies.

References

1. Freiman, C. (2017). Economic Sufficiency. P. 55–74. https://doi.org/10.4324/9781315210759-5
2. Hnatenko, V. (2021). Key factors of the State's economic security. No. 1. P. 61–66. https://doi.org/10.36690/2674-5216-2021-1-61
3. Koval, M. (2023). Prediction of the State's ability to repel armed aggression. *Science and Defense*, No. 3, 25–32. https://doi.org/10.33099/2618-1614-2023-22-3-25-32
4. Sarana, O. Yu. (2010). Complication of the economic functions of the State in the conditions of global development of transformational economies. *Formation of market relations in Ukraine*, 2 (105), 40–44.
5. Chambers, J. & Satinder, M. (2016). How to Choose the Right Forecasting Technique. https://hbr.org/1971/07/how-to-choose-the-right-forecasting-technique
6. Everett, R. (2021). Economic forecasting. https://www.britannica.com/money/topic/economic-forecasting
7. Ritis, C. (2017). Economic Scenarios: What's Reasonable and Supportable? https://www.moodysanalytics.com/articles/2017/economic-scenarios-whats-reasonable
8. Gompert, D. & Oliker, O. Defense Development. https://www.rand.org/pubs/research_briefs/RB9040.html
9. Market Research Methods For Economic Forecasting. (2021). https://fastercapital.com/topics/market-research-methods-for-economic-forecasting.html
10. Hatcher, P. L. Economic earthquakes: Converting defense cuts to economic opportunities. (1994). Berkeley, M. Institute of Governmental Studies Press, University of California, 221 p.

11. Nicastro, L. (2023). The Defense Industrial Base. https://crsreports.congress.gov/product/pdf/R/R47751
12. Yoder, N. (2023). DOD Strategic Management Plan FY 2022–2026. https://media.defense.gov/2023/Mar/13/2003178168/-1/-1/1/DOD-STRATEGIC-MGMT-PLAN-2023.PDF
13. Petropulps, F. (2022). Forecasting: theory and practice. https://doi.org/10.1016/j.ijforecast.2021.11.001
14. Kvin, D. (2016). Technological Forecasting. Foresight in Organizations. P. 100–128. https://doi.org/10.4324/9781315728513-11
15. Poledna, S. (2022). Economic forecasting with an agent-based model. https://doi.org/10.1016/j.euroecorev.2022.104306
16. Bezrukova, T. (2014). Use of the multisigmoidal method of approximation when forecasting economic indicators. Vol. 2, no. 5. P. 195–201. https://doi.org/10.12737/6381
17. Hics, H. Securing Defense-Critical Supply Chains. https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.pdf UDC 355/359.07

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.14

Methodological principles of forming the "image of the enemy" in the minds of ukrainian servicemen during the russian-ukrainian war

Olena Kholokh
Candidate of Philosophical Sciences
Leading researcher
Research Center for Humanitarian Problems of the Armed Forces of Ukraine
30, Air Force Avenue, Kyiv, Ukraine, 03186
e-mail: kholokh.lena@ukr.net
ORCID: 0000-0001-6916-5450

Abstract. The relevance of the study is due to the development of scientific and practical knowledge regarding the moral and psychological aspects of war, one of which is the socio-psychological phenomenon "the image of the enemy" as a component of the social consciousness of war participants. Its formation depends on the readiness of Ukrainian servicemen to destroy the enemy and the appropriate moral and psychological state in general to perform combat tasks.

The purpose of the article is to determine the theoretical and methodological principles of identifying the formation of the "enemy image" in the minds of Ukrainian servicemen in the process of communication and its formation if necessary.

In the research process, general scientific methods were used: analysis, synthesis, comparison, and generalization. And special methods: model of neurological levels of R. Dilts for determining markers in communication and logical levels of the formation of the "image of the enemy" in the minds of Ukrainian servicemen, as well as for the formation of the "image of the enemy" if necessary. The method of interpretation is used to reveal the meaning of the statements of military personnel. The interdisciplinary approach made it possible to combine the development of a few humanitarian sciences, namely: philosophies of war, social psychology, social communications, and neuro-linguistic programming.

The main results of the study consist in the identification of markers in communication and logical levels of formation of the "image of the enemy" in the minds of Ukrainian servicemen during the Russian-Ukrainian war. According to R. Dilts' pyramid of logical levels, which are manifested in communication at the following levels: environment, behavior, strategies, values, and identity. And at the mission level, the "image of the enemy" acquires its final formation and completion. In addition, a toolkit has been developed for officers in internal communication work to identify the logical levels of formation of the "image of the enemy" in the minds of servicemen and its correction or formation in the process of communication.

The materials of the article are of practical value for the military administration that organizes and manages internal communication work in the Armed Forces of Ukraine and for officers who conduct it with their personnel. The theoretical significance of the conducted research lies in the expansion of the humanitarian discourse of military science based on an interdisciplinary approach, which made it possible to involve effective methods, principles, and approaches of other humanitarian sciences to solve the actual tasks of military science.

Keywords: "image of the enemy" as a component of the social consciousness of war participants; formation of the "image of the enemy"; model of neurological levels by R. Dilts; internal communication work in the Armed Forces of Ukraine.

Introduction

Russia's ongoing armed aggression against Ukraine has necessitated a rethinking of the place and role of the socio-psychological phenomenon of the "enemy image" in the minds of military personnel and the Ukrainian population during the war. Prior to the beginning of the Russian-Ukrainian war, the problem of forming an "enemy image" was studied mainly in the discourse of such humanities as imagology, history, political science, psychology, military anthropology, and indirectly in philosophical studies. However, with the outbreak of war, research on this issue has become more relevant, not only theoretical but also applied, aimed at realizing a specific goal: the formation of an "enemy image" in the minds of Ukrainian military personnel. This largely affects the moral and psychological readiness to destroy the enemy in battle, the cohesion of military units and the proper level of moral and psychological state to perform combat missions.

The "image of the enemy" constitutes a dehumanized representation of one social entity within the collective consciousness of another. This socio-psychological phenomenon integrates into the public consciousness of the peoples involved in conflict, serving several pivotal functions: firstly, fostering a sense of moral and psychological superiority over the adversary; secondly, circumventing moral and ethical inhibitions against harming fellow humans (symbolically stripping the enemy of human attributes within public perception, thereby channeling resultant aggression towards the physical elimination of the enemy); and thirdly, fostering societal cohesion in a shared endeavor against the common foe.

Hence, the issue of cultivating an "enemy image" among military personnel amid the Russian-Ukrainian conflict remains pertinent. Addressing this necessitates research employing humanities methodologies and approaches, enabling the identification of the presence or absence, as well as the logical level, of the "enemy image" within servicemen's minds during communication. Furthermore, it facilitates the exploration of the nuances surrounding its formation in communication processes, particularly when deemed necessary.

Literature review

The issue of constructing an "enemy image" has been extensively explored within the interdisciplinary framework of the humanities. Psychological research has delved into the underlying causes of human hostility towards others. According to social learning theory, the prevalence of high or low levels of hostility within society is attributed to the process of socialization and the acquisition of behaviors through social learning (Bandura, 2000). Some theories posit that hostility stems from inherent human characteristics driven by competition for survival, resources, and power (Androshchuk & Oleksienko, 2019). K. Lorenz further suggests that aggression is innate to human nature (Lorenz, 2002). Within the intersection of psychology and philosophy, scholars have examined the socio-psychological mechanisms involved in the formation of an "enemy image" of Ukraine by the Russian media during the Russian-Ukrainian conflict, as well as potential strategies for altering this socio-psychological phenomenon within the Russian public consciousness (Kholokh, Skryabin, 2023).

The construction and alteration of the "enemy image" within public consciousness have been examined through the lens of philosophical inquiry. This entails a binary mode of human cognition wherein the perception of one social entity as "Us" is juxtaposed against the categorization of another as "They," "Aliens," or "enemies." In essence, the perception within the public consciousness shifts from a state of friendliness or neutrality towards a potentially perilous (Aliens) or hostile (enemies) stance, and vice versa. These dynamics, particularly within an information-driven society, are largely mediated by mass communication channels (Kholokh, 2022). Furthermore, the "enemy image" has been analyzed as a component influencing the formation of Ukrainian national identity (Kryvda, Storozhuk, 2020).

Historians have significantly contributed to the exploration of the "enemy image," identifying

both general characteristics and specific manifestations inherent in diverse historical contexts. They have elucidated its evolution during times of war, influenced by frontline events, territorial occupation, and liberation (Mayevsky, 2013, 2015, 2019). Furthermore, historians have analyzed the various forms and mechanisms employed to construct the "enemy image" across different historical epochs (Hrynevych, 2014). Their investigations extend beyond wartime, encompassing the post-conflict period and examining the emergence of new iterations of the "enemy image" and the mechanisms underlying its formation, including the classification of external and internal adversaries (Fateev, 1996). Ukrainian scholars have explored the transformation of Cold War-era narratives surrounding the "enemy image" into discourses of understanding and friendship between the United States and the Soviet Union (Nekrasova, 2011). Within the realm of historical research on the formation of the "enemy image," the methodology of J. Werch's narrative templates has been employed. This method involves reconstructing historically entrenched and perpetually reproduced narratives rooted in the collective memory of a society (Kotova, 2019). By utilizing narrative templates, researchers can identify deep-seated mental stereotypes and mythologies within specific national communities, essential for comprehending the foundations upon which one state constructs its "enemy image" of another. Furthermore, within the context of historical imagology—the study of how images and perceptions of one people are formed by another—the essence and structure of the "enemy image" within public consciousness have been illuminated. Additionally, an imagological research method has been developed to delve into this issue (Senyavsky and Senyavskaya, 2006).

Ukrainian linguists have delved into the linguistic dimensions of "enemy image" formation since the outset of the Russian-Ukrainian conflict (Hnatiuk, 2015; Kyryliuk, 2020; Matsyshina, 2022). Their research reveals that the lexical makeup of Russians' "hate speech" directed towards Ukraine and Ukrainians within the discourse of the Russian-Ukrainian information war is largely rooted in ethnostereotypes (Hnatiuk, 2015). Furthermore, this "hate speech" is replete with figurative and symbolic linguistic devices—such as metaphors, metonymies, analogies, and synecdoches—rendering it manipulative in its ability to shape public opinion (Kyryliuk, 2020). Mythological epithets used to depict adversaries, such as "orcs," negatively impact the perception of the enemy by Ukrainians by stripping them of genuine subjectivity and imbuing them with mythic attributes divorced from reality (Matsyshina, 2022).

In the realm of political science research, the article scrutinizes the content of the "enemy image," characterized as an evaluative construct shaped within the public consciousness. This construct encompasses objective information, subjective interpretations, emotional elements, social stereotypes, myths, and prejudices. The formation of a particular "enemy image" within the public consciousness of a given social entity is facilitated through mass communication channels (Levchenko, Rakcheieva, 2016).

In the Western discourse within the humanities, the formation of the "enemy image" within public consciousness has been investigated from various perspectives. Scholars such as J. D. Frank and A. Y. Melville have examined the evolution of the "enemy image" initially cultivated in the minds of the populations of the United States and the USSR during the Cold War, which eventually transitioned into the concept of the "image of the Other" towards the end of the conflict (Frank, Melville, 1988). P. Madder, B.B. Fisher, S. Shpiro, and others have scrutinized how intelligence agencies in nations like the United States, the United Kingdom, Israel, and Pakistan gather and interpret data concerning potential adversaries, thereby shaping the "enemy image" and influencing subsequent state policies (Madder, 2015). H. Burgess has highlighted the detrimental effects of entrenched "enemy images" within various segments of a society or between nations during times of peace. The author proposes strategies to mitigate negative stereotypes within public consciousness and foster positive ones that foster unity among societies and nations (Burgess, 2003). Additionally, researchers M. G. Bartoszewich and M. Pruckova have analyzed how the Czech and Estonian republics construct an "enemy image" of Russia within their security discourses, and how this

perception influences their policy-making. The formation of the "enemy image" in the context of potential future conflicts is intricately linked to the security strategies of states, ranging from preparations for potential direct confrontations with a significantly stronger adversary to strategies aimed at deterrence or reconciliation (Bartoszewich and Pruckova, 2023).

The model of neurological levels developed by R. Dilts in 1980 serves as a valuable tool for identifying an interlocutor's beliefs about a particular issue, the significance of their actions, and for shaping necessary beliefs and influencing their behavior. This model also aids in pinpointing obstacles that impede the formation of specific beliefs in interlocutors, which in turn affect their actions. Moreover, R. Dilts' model offers guidance on resolving problems that arise at various neurological levels during communication (Dilts, 2004; Zelenin, 2015). This tool has demonstrated its effectiveness across various fields such as coaching, business, and marketing over the years. Nonetheless, it remains underutilized in the realm of internal communication within the Armed Forces of Ukraine, particularly in identifying markers of the "enemy image" and shaping it if deemed necessary during wartime communication among military personnel.

Therefore, the aim of this study is to establish the theoretical and methodological underpinnings for identifying markers of the "enemy image" within the internal communication processes among Ukrainian servicemen, as well as to develop strategies for its formation by internal communication officers in instances where it is insufficiently developed. This will be accomplished through the utilization of R. Dilts' model of the pyramid of neurological levels.

Methodological Framework

The methodological framework of this study is structured to align with the problem and purpose at hand. General scientific theoretical methods such as analysis, synthesis, comparison, and generalization were employed. Additionally, a specialized approach utilizing R. Dilts' model of neurological levels was adopted to identify communication markers and logical levels associated with the "enemy image" among Ukrainian military personnel, as well as to facilitate its formation when necessary. Furthermore, the method of interpretation was utilized to discern the significance of statements made by military personnel. An interdisciplinary approach was integral to this study, allowing for the integration of insights from various humanities disciplines including the philosophy of war, social psychology, social communications, and neuro-linguistic programming, thereby enriching the research findings.

Results and Discussions

The "enemy image" stands as a fundamental component of the public consciousness among servicemen during times of war or heightened conflict, wielding significant influence over the moral and psychological dimensions of warfare success. Servicemen's perceptions of the enemy, categorized as the "Other" or the "enemy," are evident across cognitive, affective, and behavioral domains. This construction of the "enemy image" follows a binary mode of thinking, characterized by mutually exclusive opposition. Binary categorization serves as a primary means of comprehending the world and human cognition. Within this framework, the "enemy image" is diametrically opposed to the "image of one's own," which is endowed solely with positive connotations, while the "enemy image" is imbued exclusively with negative ones. Markers of the "enemy image" are palpable within language, as language and thought are intricately intertwined components of a unified system. Consequently, the discourse of military personnel serves as a focal point for analysis, assessing the presence of the "enemy image" within their consciousness and discerning the logical levels of its formation or absence.

To gauge the extent of the "enemy image" formation within servicemen's minds, we have devised primary criteria for evaluating indicators of its development, drawing upon R. Dilts' pyramid of neurological levels (Zelenin, 2015). The model delineates six hierarchical levels observable in

communication, reflecting servicemen's attitudes and experiences, while also indicating the presence of specific beliefs within their minds.

1. Level of Environment. At this logical level, communication reflects the circumstances and conditions to which servicemen must respond or adapt. This encompasses external factors (context) influencing individual servicemen, the personnel of the Armed Forces of Ukraine, the state of Ukraine, and the Ukrainian population at large, thereby shaping the state of public consciousness. These factors may include: peaceful peacetime conditions; confrontations within the context of information-psychological, information-semantic, or hybrid warfare; anticipation of war in physical space; defense and repulsion in military-political conflicts or full-scale wars; internal unity or disunity among Ukrainians; international support or refusal of support, among others.

Positive markers of the current state of affairs at this level include: strong cohesion among military units, the population, and the military-political leadership of the state; an ample supply of reliable weapons; an adequate provision of high-quality military uniforms and ammunition; satisfactory food provisions; sufficient financial support for military personnel; and effective social and other forms of support for military personnel. These indicators suggest the absence of significant issues that could impede the formation of the "enemy image" in the minds of the troops. Conversely, negative markers of the current state of affairs may include: lack of cohesion within military units; distrust towards the military and political leadership; inadequate or poor-quality military weapons and ammunition; substandard food provisions; low salaries for military personnel, among others. The presence of these negative markers indicates potential obstacles in the process of forming the "enemy image" among the military. Therefore, at this level of communication, the overall context in which military personnel operate is expressed, which may either facilitate or hinder the ongoing formation of the "enemy image."

It is pertinent to note that if servicemen have already formulated an "image of the enemy" in their minds, it will manifest at this level of communication through a juxtaposition of our servicemen's context with that of the enemy. Our context will typically be associated with positive connotations, whereas the enemy's context will be depicted with negative connotations. For instance: "Our weapons are modern and reliable, whereas the enemy troops are equipped with decommissioned Soviet-era weapons that are often malfunctioning"; "We currently receive adequate financial support, whereas the Russians are promised payments for participation in combat operations, but in reality, they receive very little compensation," and so forth.

2. Behavioral Level. At this logical level, communication pertains to the specific actions undertaken by military personnel within a given environment. These actions and deeds may include: participation in service activities and combat training, both in peacetime and during wartime; the level of activity or passivity among military reservists during conscription amidst declared mobilization efforts; the level of engagement or disengagement exhibited by military personnel during training exercises; the degree of cohesion or disunity, as well as the level of perseverance, resilience, or passivity demonstrated by military personnel during coordination and combat operations, among others.

The presence of positive markers in communication regarding specific actions and deeds of military personnel signifies the absence of significant issues at the neurological level of behavior that could hinder the formation of an "enemy image" at higher neurological levels. Conversely, the presence of negative markers, such as statements depicting problematic behaviors or shortcomings among military personnel, suggests the absence of an "enemy image" in their minds and indicates unresolved issues at this neurological level. Furthermore, the likelihood of encountering obstacles to the formation of an "enemy image" at higher neurological levels increases. For instance, positive markers like "We receive comprehensive training from seasoned instructors under conditions closely resembling combat scenarios, enhancing our chances of survival," juxtaposed with negative markers like "Meanwhile, the mobilized Russians indulge in alcohol during training and subsequently perish

in combat," indirectly hint at the formation of an "enemy image" among Ukrainian servicemen.

3. Level of Strategies (Abilities/Capabilities) – This logical level of communication encompasses the experiences wherein the skills, abilities, and mental strategies guiding the behavior of servicemen are manifested. It also pertains to the formation of strategies based on specific behaviors, abilities, skills, and capabilities that are interconnected, as well as the execution of these strategies in appropriate conditions (contexts).

This level of communication can indirectly indicate the formation of an "enemy image" in the minds of military personnel when they consciously and persistently hone their skills and master techniques to accomplish complex objectives in combat situations, with the intention of defeating the enemy during military training and in actual combat. In other words, military personnel cultivate their professional attributes not solely to adhere to military standards, but also to gain an edge over the enemy in combat scenarios and effectively neutralize them.

Markers indicating the formation of an "enemy image" in the minds of Ukrainian military personnel at the level of communication abilities and strategies may include statements such as: "We diligently study and master new Western military equipment to employ it effectively in enemy engagements," or "Our unit undergoes rigorous combat training to ensure our survival in battle, coordinate our actions, accomplish missions successfully, and bring us closer to victory over the enemy." Conversely, markers indicating the absence of an "enemy image" in the minds of servicemen at this level of communication may include statements like: "I fail to comprehend why we exert ourselves so much during combat training," or "Mobilized individuals cannot sufficiently acquire a particular military specialty within the short training period." When military personnel express motivation to develop their skills, abilities, and strategies not merely to fulfill their military duties but to effectively engage and neutralize the enemy in combat, these serve as markers for the formation of an "enemy image" in their minds. Conversely, expressions of limiting beliefs questioning the necessity of learning and developing skills, abilities, and strategies for physical survival, proficiency with weapons and equipment, teamwork, etc., indicate the absence of an "enemy image" in the minds of servicemen. Furthermore, such negative markers suggest the presence of unresolved issues at higher neurological levels, specifically at the levels of beliefs and values, identity and mission, and spirituality. Human behavior, skills, and strategies are inherently influenced and guided by these neurological levels, which essentially constitute one's worldview. Thus, the beliefs, values, identity, and mission of military personnel not only shape their experiences but also fundamentally determine them.

4. Beliefs and Values Level – This logical level of communication encapsulates the judgments, beliefs, and knowledge upon which service members rely, thereby enhancing their capabilities. Furthermore, it serves as the level of communication wherein the beliefs and values of the military are articulated, motivating, facilitating, or constraining the development and deployment of various pertinent capabilities. Hence, this level of communication does not merely convey experiences but rather the internal worldview and perspective of the serviceman. It is at this neurological level that the "image of the enemy" begins to take shape in the minds of servicemen as a juxtaposition of mutually exclusive judgments, beliefs, knowledge, and intentions articulated in the narratives of both our military and our adversaries.

When something is perceived as unfavorable to one's interests, it is often regarded as hostile, creating a sense of threat or danger that necessitates distancing oneself from it. This opposition is further intensified on an axiological basis, wherein one's own values are considered the only correct ones, and hostile values are viewed as threats to one's existence. In such a scenario, one's own existence is seen as the sole viable option, inherently incompatible with the existence of the enemy. The notion of mutual perspectives or a neutral outlook on the future becomes untenable, as accepting the enemy's perspective is perceived as a relinquishment of one's own identity. This axiological escalation culminates in the release of aggression, directed towards the enemy. The readiness to

physically eliminate the enemy is cultivated through internal communication efforts with military personnel. Consequently, communication and propaganda technologies are employed to dehumanize the enemy, stripping them of their human attributes and eradicating any moral, ethical, social, and religious inhibitions against killing fellow beings. Further discussion on markers of dehumanization will be explored in the subsequent neurological level of identity.

Markers indicating the formation of an "enemy image" in the minds of servicemen at the level of beliefs and values in communication may manifest as contrasting values depicted in narratives, such as: "We, as Ukrainians, are defending our homeland in the ongoing war, safeguarding our loved ones, and fighting for our freedom and independence, whereas Russians are perishing disgracefully on foreign soil due to their minds being manipulated by propaganda"; "Ukraine is a European nation with over a millennium of history and culture, while Russia originated within the Golden Horde, inheriting corresponding values and culture, and only gained independence from its control in the early eighteenth century. Consequently, Ukrainians and Russians possess fundamentally distinct values, histories, cultures, and aspirations," and so forth.

Thus, communication at the level of values and beliefs serves as evidence of the formation of an "enemy image" in the minds of servicemen. In cases where such an image is absent and there is a need to cultivate it, the "enemy image" is established at this neurological level through the juxtaposition of the values and beliefs held by our military (Ukrainian population) with those of the enemy (Russian military and population), highlighting their inherent opposition.

5. The identity level is the logical level of communication that deals with who people perceive themselves to be and how they (or others) are called. It is a sense of self that is associated with beliefs, values, abilities, and appropriate behavior in different contexts.

At this logical level of communication, the formation of the "enemy image" is also evident, manifested as a juxtaposition of names, titles, and designations associated with the "image of the own" - namely, the Ukrainian military, population, and state leadership - in contrast to those of the enemy. For instance, in the ongoing Russian-Ukrainian war, our military is referred to in communication as "defense forces," "our soldiers," "Ukrainian soldiers," "our heroes," "defenders," "unconquered," "brothers and sisters," and so forth, contrasting with designations for the enemy such as "rashists" (Russians adhering to fascist ideology), "non-humans," "pigs," "occupiers," "orcs" (depicting a barbaric army conquering through sheer numbers, possessing low intelligence, and lacking comfort in living), "terrorists," "invaders," "looters," "murderers," "rapists," and so on. Additionally, profanity is often employed in interpersonal communication when referring to the enemy, serving as another marker of the formation of an "enemy image" in the minds of Ukrainian military personnel. The redefinition of names, titles, and designations towards devaluation and humiliation constitutes a communicative strategy aimed at dehumanizing the enemy through linguistic means.

Furthermore, within Ukrainian media discourse during a full-scale war, official authorities and media outlets often depict Russia and its capital with lowercase letters - "Russia" and "Moscow." Similarly, names of the Russian president, other politicians, propagandists, and all Russian opinion leaders who support the war against Ukraine are also presented in lowercase. Such deviations from grammatical norms serve to convey contempt for the enemy and underscore its humiliation. Additionally, the term "Russian Federation" is frequently subjected to communicative "redefinition," being referred to as "Muscovy," "rashka," "orkestan," "zaporebereya," "zalessia," among others. Through this linguistic approach, Russia is dehumanized and its perceived backwardness is accentuated. Consequently, this communication strategy diminishes the status of the Russian state within the Ukrainian value system.

Hence, when Ukrainian servicemen employ mocking, insulting, and humiliating terms, including foul language, in their communication at the identity level, directed towards the enemy military, population, state leadership, opinion leaders, and the state itself, it signifies the formation of

an "enemy image" in their minds. Moreover, the degree of emotional intensity conveyed by these terms reflects the level of aggression and fury directed towards the enemy. Conversely, the absence of such vocabulary in wartime communication necessitates the formation of the "enemy image" through internal communication efforts, utilizing negative semantics and relevant narratives about the enemy.

6. Spirituality and Mission Level – This logical level of communication encapsulates perspectives on the world, the essence and purpose of human life, as well as the community's, group's, or nation's awareness of its role in the world and its envisioned future development. It encompasses a sense of connection with a higher power, intelligence, or ancestral heritage that transcends individual existence and guides collective endeavors.

At this neurological level, the overarching national ideology, the essence and purpose of the people's and the state's existence are articulated. It embodies the potent energy of inspiration for the nation's self-realization and provides answers to questions concerning the raison d'être of the state, culture, and people in the world. At this logical level, patriotism finds expression, alongside the mission of soldiers, units, and the state in times of war, as well as concepts such as the "image of Victory," the "image of the Motherland," and the "image of the future of our state," among others. It is here that the aggressor nation begins to construct an "image of the enemy" of the country and its people, against whom premeditated aggression is planned. To achieve this, strategic narratives are disseminated in the information domain, outlining specific goals for future development, the state's role, and the tasks entrusted to the people. These strategic narratives regarding the mission are juxtaposed against those of states targeted for assimilation or aggression.

For instance, in Russia during the late 1990s, the imperial vision of the "Russian world" was conceived, positioning Russia in opposition to the collective West. Advocates of this project asserted that Russia's influence transcended mere territorial boundaries, extending wherever the Russian language was spoken, irrespective of nationality or citizenship, and even without the consent of Russian-speaking individuals in neighboring countries. Under Putin's presidency, the implementation of the "Russian world" commenced through propaganda campaigns within Russia and its neighboring states. This propaganda campaign began at the neurological level of spirituality and mission before permeating lower neurological levels, where Russia coerced neighboring states into embracing the "Russian world" through gas, economic, and trade pressures, alongside aggressive activities culminating in the conflicts with Georgia, the annexation of Crimea, and the escalation of the war in eastern Ukraine from 2014 onwards, eventually escalating into full-scale armed aggression against Ukraine in 2022. At this neurological level, the adversary disseminates its ideologies and launches an information and semantic campaign aimed at eroding the national identity, historical memory, language, and culture of target populations. The consequences of this information and semantic influence are particularly devastating at this level.

Indeed, the constructive information and semantic influence on the consciousness of Ukrainian servicemen at the level of spirituality and mission can yield significant outcomes, such as the cultivation of a deeper meaning and purpose behind their actions amidst the ongoing Russian-Ukrainian conflict. It aims to address fundamental existential questions, providing clarity on the rationale and significance of their endeavors. Constructive narratives may encapsulate sentiments like: "We are combating the adversary to secure a tranquil future for our offspring within a liberated and sovereign Ukraine, characterized by European standards of living, rights, freedoms, and democratic principles." Such narratives, when articulated by servicemen, serve as indicators of their commitment, conscious resolve, and alignment with higher ideals transcending personal interests. Conversely, the repercussions of the enemy's deleterious information and semantic influence at this level can manifest in narratives expressing doubt, confusion, or apathy among Ukrainian servicemen amidst the conflict. Phrases like "I fail to comprehend my purpose here," "What cause are we championing?" or "Why does the choice of my residing state matter to me?" may signify a deficiency

in the formation or erosion of national and civic identity, consequently leading to a loss of the overarching significance inherent in safeguarding their homeland from the adversary's aggression.

Absolutely, at the level of spirituality and mission, servicemen grasp the utmost significance of their endeavors, comprehending the essence and purpose underlying their actions. This level of communication enables the realization of the profound meaning inherent in their military service, fostering unwavering loyalty and dedication to their cause. Servicemen develop a conscious understanding of the ideals they are defending, acknowledging the potential sacrifices they may face, including the ultimate sacrifice of laying down their lives. It is at this pinnacle level of communication that the intrinsic valor and commitment of servicemen shine forth, embodying the noblest aspirations and convictions of their nation.

Thus, the "image of the enemy" in the minds of military personnel is primarily formed at the level of values and identity, which is realized at the experiential levels - strategies, behavior and environment - in specific actions and strategies aimed at destroying the enemy. And at the level of mission and spirituality, the formed "image of the enemy" acquires its final meaning and completeness.

The formed "image of the enemy" in the minds of servicemen manifests itself: at the cognitive level - as a set of knowledge and beliefs about the enemy, mutually exclusive opposition of "own" and "enemy" values, identities and missions in the ongoing war; at the affective level - as the experience of feelings and emotions: distrust, anger, aggressiveness, condemnation, thirst for revenge, disrespect, hatred, rage and, least of all, fear. These emotions form the appropriate attitude towards the enemy - the desire to inflict psychological and physical harm (destruction) on the enemy; at the behavioral level - as a willingness to destroy the enemy, or as a real experience of its destruction.

The insufficiently formed or absent "image of the enemy" in the minds of servicemen manifests itself at the cognitive level - as a tolerant attitude to the values and mission (aspirations) of the enemy, and at the level of identity, i.e., in the process of nominating the enemy, there will be no offensive and humiliating vocabulary; at the affective level - as apathy, or fear and anxiety, which form the appropriate attitude towards the enemy - the desire to withdraw and avoid participation in the war to retake the temporarily occupied territories and destroy the enemy; at the behavioral level - as unwillingness to destroy the enemy, which can manifest itself as an attempt to avoid mobilization, as well as constant complaints about training and lack of combat experience, dissatisfaction with various types of support, combat conditions, actions of commanders, etc.

According to the pyramid of neurological levels by R. Diltz's pyramid of neural levels, the cognitive level of formation or absence of an "enemy image" in the minds of servicemen is manifested in communication at the levels of values, identity, mission and spirituality; the affective level of formation or absence of an "enemy image" of servicemen is manifested as emotional communication using profanity and hate speech against the enemy, or its absence in case of insufficient formation or absence of an "enemy image" in servicemen. Efficiency in communication can be manifested at all levels of R. Dilts' pyramid of neurological levels - environment, behavior, strategies, values, identity, mission and spirituality; the behavioral level of formation or absence of an "enemy image" in servicemen is manifested in communication at the levels of: behavior and strategies according to R. Dilts' pyramid of neurological levels. If servicemen are unwilling to destroy the enemy, then according to the methodology of R. Dilts' neurological levels, the formation of this readiness, that is, the "enemy image" in the minds of servicemen should take place at higher neurological levels - values, identity, mission and spirituality.

Conclusion

As a result of the study, the theoretical and methodological foundations for the formation of the "enemy image" in the minds of Ukrainian servicemen during the Russian-Ukrainian war have been developed. They consist of:

- defining the essence and content of the socio-psychological phenomenon of the "enemy image" as a component of the public consciousness of military personnel (war participants);

- principles of forming an "enemy image" (binary opposition and 6-stage gradation of logical levels of knowledge acquisition and formation of levels of beliefs in a person);

- markers in communication that express the presence of an "enemy image" at a certain logical level according to R. Diltz's pyramid;

- communicative techniques for forming an "enemy image" in the minds of Ukrainian military personnel.

The theoretical value of this study is to expand the humanitarian discourse of military science on the basis of an interdisciplinary approach that allowed to involve effective models, methods, principles, approaches and tools of the humanities to solve the actual problems of military science.

The practical value of this study is the creation of a communication model to identify the formation of the "enemy image" in the minds of Ukrainian military personnel, as well as to form it if necessary. This tool will be useful for military command and control bodies that organize and manage internal communication work in the Armed Forces of Ukraine and for officers who carry it out with personnel.

Recommendations

The results of the study will be useful for internal communication officers in the Armed Forces of Ukraine, military command and control bodies that organize and manage internal communication, as well as in the process of training internal communication officers.

References

1. Bandura, A. (2000). Teoryia sotsyalnoho nauchenyia.
2. Androshchuk, O., Oleksiienko, S. (2019). Psykholohichni osoblyvosti formuvannia obrazu voroha yak skladovoi hibrydnoi viiny Rosiiskoi Federatsii proty Ukrainy. *Zbirnyk naukovykh prats Natsionalnoi akademii prykordonnoi sluzhby Ukrainy*. Seriia: psykholohichni nauky. 2 (13), 182–198.
3. Lorenz, K. (2002). On Aggression.
4. Kholokh, O. (2022). Antropolohichne osmyslennia obraziv “Svoho”, “Chuzhoho”, “Inshoho” ta “voroha” yak skladovykh suspilnoi svidomosti. *Hileia*: naukovyi visnyk, 8 (175), 49–54.
5. Kryvda, N., Storozhuk, S. (2020). Image of an “Enemy” as a Factor of Constructing the Ukrainian National Identity. *Ideas Philosophical Journal Special Scientific Issues*, (1 (15) –2 (16)), pp. 57–66.
6. Kholokh, O., Skriabin, O. (2023). Sotsialno-psykholohichni mekhanizmy formuvannia “obrazu voroha” z Ukrainy rosiiskymy zasobamy masovoi komunikatsii pid chas rosiisko-ukrainskoi viiny. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*. Viiskovo-spetsialni nauky, 3 (55), 34–40.
7. Maievskyi, O. (2019). Konstruiuvannia ikonografichnoho obrazu spivrobitnykiv NKVD u natsystskii propahandi Raikhu naperedodni ta u roky Druhoi svitovoi viiny. Z arkhiviv VUChK–HPU–NKVD–KHB. № 1 (51), 264–285.
8. Maievskyi, O. (2013). Obraz zovnishnoho voroha kriz pryzmu plakatnoi produktsii SRSR. *Storinky voiennoi istorii Ukrainy*: zbirnyk naukovykh statei, (16), 207–217.
9. Maievskyi, O. (2015). Obraz nimetskoho viiskovosluzhbovtsia u zobrazhuvalnii propahandystskii produktsii Radianskoho Soiuzu na terytorii Ukrainy. *Druha svitova viina i Ukraina: aktualni istoryko-pravovi problem*y: zbirnyk materialiv kruhloho stolu (Kyiv, 28 kvit. 2015 r.), 28–36.
10. Hrynevych, L. (2014). Mekhanizmy masovoho narodovbyvstva: konstruiuvannia “obrazu voroha” v radianskii politychnii karykaturi (druha polovyna 1929 – pochatok 1930 rr.). *Storinky*

istorii: zbirnyk naukovykh prats, 47–64.
11. Fateev, A. (1996). Kak sozdavalsya obraz vraga: u istokov kholodnoi voini. Istoriya. Yezhenedelnoe prilozhenie k gazete "*Pervoe sentyabrya*", 3, 7–12.
12. Nekrasova, V. (2011). Obraz "voroha" ta "druha" v ideolohichnomu protystoianni chasiv zavershennia "Kholodnoi viiny". *Rozpad Radianskoho Soiuzu ta mizhnarodni interpretatsii zavershennia Kholodnoi viiny: 20 rokiv potomu*: materialy mizhnarodnoi naukovo-praktychnoi konferentsii (Zaporizhzhia, 2–4 lystopada 2011 r.), 43–47.
13. Kotova, S. (2019). "Obraz voroha" v sotsiohumanitarnomu dyskursi Velykoi Brytanii, Nimechchyny ta Rosii periodu Pershoi svitovoi viiny (1914–1918) : dys. … kand. istor. nauk: 07.00.06. / Dniprovskyi natsionalnyi universytet imeni Olesia Honchara, 213.
14. Senyavskii, A., Senyavskaya, Ye. (2006). Istoricheskaya imagologiya i problema formirovaniya "obraza vraga". *Vestnik RUDN*. Seriya "Istoriya Rossii", 2 (6), 54–72.
15. Hnatiuk, V. (2015). "Mova vorozhnechi" v rosiisko-ukrainskii viini 2014–2015 rokiv ta natsionalna samosvidomist ukraintsiv. *Istoryko-kulturni studii*, 2 (1), 47–52.
16. Kyryliuk, O. (2020). Movni zasoby tvorennia obrazu voroha v umovakh informatsiinoi viiny. *Naukovi zapysky*. Seriia: filolohichni nauky, 187, 45–50.
17. Matsyshyna, I. (2022). Homo Sacer ta vyklyk subiektyvnosti "voroha" v umovakh rosiisko-ukrainskoi viiny. *Politychne zhyttia*, 2, 15–22.
18. Levchenko, L., Rakcheieva, S. (2016). Tekhnolohii formuvannia zovnishnoho voroha u demokratychnykh ta nedemokratychnykh rezhymakh. *Naukovi pratsi Chornomorskoho derzhavnoho universytetu imeni Petra Mohyly kompleksu "Kyievo-Mohylianska akademiia"*. Seriia: Politolohiia. T. 273, 261, 74–78.
19. Frank, J. D., Melville, A. Y, (1988). The Image of the Enemy and the Process of Change In Breakthrough: Emerging New Thinking: Soviet and Western Scholars Issue a Challenge to Build a World Beyond War.
20. The Image of the Enemy. Intelligence analysis of adversaries since 1945. (2015).
21. Burgess, Heidi. (2003). "Enemy Images" Beyond Intractability. http://www.beyondintractability.org/essay/enemy-image.
22. Bartoszewicz, M. G., Pruckova, M. (2023). Enemy Image? A comparative analysis of the Russian federation`s role and position in the leading national security documents of Estonia and Czech Republic. *Journal of contemporary European studies*. Published online: 14 jun. 2023.
23. Dylts, R. (2004). Kouchyng s pomoshchiu NLP.
24. Zelenin, V. (2015). Po toi bik pravdy: neirolinhvistychne prohramuvannia yak zbroia informatsiino-propahandystskoi viiny: navch. posib. Tom 1. NLP – XX stolittia.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.15

Implementation of the emerging and disruptive technologies as the key to technological superiority in modern warfare

Kostiantyn Kulahin
PhD in engineering, senior researcher
senior researcher
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska Street, 77/79, Kharkiv, Ukraine
e-mail: k.kulagin@ukr.net
ORCID: 0000-0003-1189-5623

Ivan Nos
PhD in engineering
head of scientific research department
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska Street, 77/79, Kharkiv, Ukraine
e-mail: 171a16@gmail.com
ORCID: 0000-0003-1501-0503

Oleksiy Solonets
PhD in engineering, senior researcher
leading researcher
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska Street, 77/79, Kharkiv, Ukraine
e-mail: alex_solonez@ukr.net
ORCID: 0000-0001-6223-5022

Kostiantyn Kvitkin
researcher
Ivan Kozhedub Kharkiv National Air Force University
61023, Sumska Street, 77/79, Kharkiv, Ukraine
e-mail: kosta_kit@ukr.net
ORCID: 0000-0002-8330-5023

Abstract. The relevance of article is due to the fact that in the conditions of confrontation between countries different in terms of resources, strength of the army and number of weapons, military superiority over the enemy are achieved by using asymmetric and hybrid actions with using innovative high-tech weapons and C4ISR. The search for innovative approaches to the management of troops, new methods of using both traditional types of weapons and new ones created on unconventional physical principles, the introduction of the emerging technologies is an urgent need for the development of the Ukraine defense capabilities - the key to technological superiority in modern warfare. Today, most of the developed countries pay considerable attention to scientific research on the emerging and disruptive technologies, strive to maintain advantages in this field. Based on this, the research of promising scientific and technical trends and determining the potential of their application in military affairs is an important scientific and practical tasks that must be solved. The leading approach to solving this problematic issue is the use of the results of the analysis of scientific publications, reports of leading international security institutions, the use of statistical

methods of scientometric and patent analysis, as well as the assessment of the level of attention or expectations. The article presents the results of a systematic analysis of existing technological trends, the most significant new and breakthrough technologies, as well as an assessment of their impact on the sphere of security and defense. A certain author's view on the possibilities of using such technologies is offered. The materials of the article are of practical significance for specialists who are responsible for the formation of directions of scientific and scientific-technical activity, the introduction of innovations and the emerging technologies in the activities of the defense-industrial complex.

Keywords: innovation, emerging and disruptive technologies, artificial intelligence, robotic and autonomous systems, novel materials, defense capabilities

Introduction

Currently, humanity is facing a dangerous, unpredictable and unstable world with non-traditional challenges and threats, such as asymmetric and hybrid wars, space militarization, international terrorism, cyber threats, information and psychological operations, climate change and bioterrorism. The ability to respond promptly to current and future challenges can be improved through the active and driving role of emerging and disruptive technologies (EDTs), which can be implemented within the next 10-20 years and will have a significant impact on the economic, socio-political and, of course, defense capabilities of those countries or security associations of countries that will timely and correctly assess the potential of such technologies and take a leading position in their practical application.

Under the newest (emerging) technology we will understand a radically new innovative technology characterized by relatively rapid development and a certain degree of consistency that has been maintained for a long time, the technical and value potential of which is largely uncertain, ambiguous and not fully realized, but which is assessed as having a significant impact on the socio-economic, military-technical and other spheres of society in the future. Such technologies will reach maturity and find implementation within 10-20 years, and, as of today, they are not widely used or their impact on defense, security and industry is not sufficiently analyzed and fully understood. A breakthrough technology is a relatively new innovative technology, the degree of development of which allows us to assess its technical and value potential as unequivocally capable of quickly and radically changing existing norms and processes in certain areas of life or in society as a whole, destroying established business models, traditional markets and relationships between governance entities, institutions and consumers, to dramatically displace old technologies, products or services by overcoming technical barriers, applying new ways of solving problems and meeting needs that were not previously available or underdeveloped, significantly reduce costs, improve productivity and increase accessibility to a wider audience, changing the demand for goods and services and consumer preferences.

Emerging and disruptive technologies have several generalized characteristics that help experts identify and categorize them promptly, including innovation, synergistic potential, ability to develop, impact on the future, and ability to change traditional business models. These characteristics help to identify the latest and most disruptive technologies, and understand their future potential and likely impact on various areas.

Often, emerging and potentially disruptive technologies present opportunities for integration with each other and with other existing established technologies, which can lead to more complex and powerful technological solutions called convergent technologies. They are defined as innovative technologies that combine several technologies in a certain way to create a synergistic effect.

Over time, the latest, breakthrough and convergent technologies may become critical for the state - technologies that require protection and guaranteed preservation, are of fundamental

importance for sustainable economic development, ensuring economic and national security and defense of the state, maintaining existing and acquiring new defense capabilities, creating high-tech competitive energy-efficient and environmentally friendly products. When compiling a list of critical technologies, each country relies on the specifics of its own goals, needs, capabilities, and ambitions.

The driver of EDT implementation in the military sphere is NATO. Within its structure, the NATO Science & Technology Organization (STO) is active, and several specialized bodies, agencies and working groups have been established, including the NATO Advisory Group on Emerging and Disruptive Technologies (AGEDT), NATO's Data and Artificial Intelligence Review Board (DARB), The Defense Innovation Accelerator for the North Atlantic (DIANA), which cooperate with public and private defense sector, international organizations, including the European Union (EU) and the United Nations (UN), academia and civil society to develop and, most importantly, implement EDT and establish international principles for the responsible use of these technologies.

EDTs and other innovative technologies will be used in the military sphere, regardless of where and why they were created. At the same time, they may create entirely new operational domains (e.g., cyberspace) or re-apply traditional ones. Rapid changes in the technological landscape are driving the Fourth Industrial Revolution “Industry 4.0”, and the seventh-generation military revolution.

German economist Klaus Schwab is considered to be the developer and ideologist of the Fourth Industrial Revolution concept. He outlined his vision of “Industry 4.0” in his books “The Fourth Industrial Revolution” (2017) and “Technologies of the Fourth Industrial Revolution” (2018). The main technological driver of this revolution is considered to be disruptive innovation and its synthesis in three main areas: physical, digital, and biological. And this, in the author's opinion, determines the fundamental difference between the Fourth Industrial Revolution and all previous industrial revolutions. The ability of innovative technologies to breakthrough (critical change) sustainable technologies was first discussed by Clayton Christensen in his book "The Innovator's Dilemma: How New Technologies Kill Strong Companies" (2004), and breakthrough innovations and corresponding breakthrough innovative technologies were identified as the main catalyst for changes in consumer values in the market and sustainable business processes.

In recent years, experts from various fields have explored the essence and prospects of the latest and most disruptive technologies. In particular, (Rotolo, Hicks, Martin, 2015) discusses terminological aspects in detail, (Küfeoğlu, 2022) reveals the essence and principles of organization of the most well-known emerging technologies at the moment, (Mariette, Bernard, Meyerson, 2023) analyzes the top 10 emerging technologies of 2023 and considers the methodology for assessing their impact on society and the economy. Armstrong (2017) considers various concepts, methodologies, tools and areas of application of disruptive technologies, Manners-Bell and Lyon (2022) describes the peculiarities of the application of disruptive technologies in the field of logistics and supply chain management, and Slyusar, Sotnyk, Kupchyn, 2020) proposed a definition of critical and breakthrough technologies, as well as an approach to their structuring, as well as a conceptual approach to structuring the most important critical and breakthrough technologies for the state defense sector using a decision-making model based on fuzzy logic. Aspects of the selection and application of critical technologies in the defense sector are discussed in (Slyusar, Sotnyk, Kupchyn, 2020), (Sotnyk, Rastryhin, Kupchyn, 2020), and the study of the potential and possibilities of introducing convergent technologies in Ukraine is discussed in (Matyushenko, 2016). Some publications present the results of applying statistical methods of scientometric and patent analysis to study global technological and scientific trends (Pysarenko and Kvasha, 2021), assessing the level of attention of scientific and technical communities, defense companies, and individual countries to new, disruptive, and critical technologies (Pysarenko and Kvasha, 2020).

By far the most significant source for EDT analysis is the NATO Science & Technology Organization (STO) report "Science & Technology Trends 2020-2040" (Reding, Eaton, 2020) and the 2023 report "Science & Technology Trends 2023-2043. Across the Physical, Biological, and

Information Domains" in two parts (Reding, Lucia, Blanco, Regan, Bayliss, 2023), in which NATO experts identified the main strategic priorities in the development of weapons and military equipment, which should be based on ten closely interrelated EDTs, which are considered to be the main strategic disruptors over the next 20 years. Other important documents are two reports prepared by AGEDT, with advice on how to optimize their innovation efforts. The first one (Chana, 2020), published in March 2021, provided four main initial tips for NATO: improve technological literacy, create an effective network of innovation centers; develop and facilitate new mechanisms for financing innovation with the participation of private sector actors, and create innovative partnership initiatives with external stakeholders. In its second annual report (Chana, 2021), published in April 2022, the group reviewed three critical ongoing areas of work to ensure that NATO and Allies can rapidly adopt new technologies and maintain technological advantage through the DIANA project, the NATO Innovation Fund, and the Human Capital Innovation Policy, which provides guidance to NATO on how to attract, retain, and develop talented people with technical skills and innovative thinking. Since June 2020, Ukraine, as a NATO Enhanced Opportunities Partner, has been able to participate in almost all initiatives and studies conducted by NATO working groups, organizations, and agencies.

An analysis of publications shows a sharp increase in the interest of scientists and defense program (project) managers in the tools for identifying EDT and assessing (predicting) the results of their implementation, both on the positive side and taking into account the negative risks of their use. Most publications are devoted to economic, transport and logistics, information, technical, and environmental aspects, and only a small share of works is devoted to defense and technical aspects, which makes this study relevant.

Therefore, the purpose of this article is to define the essence of EDTs and the potential for their use to acquire new defense capabilities in the context of the war with the Russian Federation and possible future hybrid and asymmetric wars, to systematize the identified technological trends, to focus the attention of the scientific community on the need for accelerated analysis of potential technological advantages that EDTs can provide, especially in the security and defense sector of the state, to expand the discussion around urgent technological needs to acquire the necessary equipment for the troops to win.

Methodological Framework

According to the results of studies (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023), (Chana, 2020), (Chana, 2021) conducted by NATO experts, it is believed that by 2043, four main characteristics will determine the emergence and implementation of the latest and most disruptive technologies in the military sphere:

intelligence (ensured by the use of symbiotic artificial intelligence, its integration at all levels using machine learning technologies, and analytics of large amounts of structured and unstructured data);

interconnectedness (ensured by the use of a distributed network of primary sources of information (virtual and physical) using new encryption methods and Distributed Ledger Technology (DLT));

distributed (ensured by large-scale decentralized and ubiquitous use of various sensors and sensors, collection and processing of large amounts of data);

digitalization (ensured by the digital combination of human, physical and information domains to create breakthrough effects).

The implementation of EDT should ensure the implementation of the five main imperatives of the NATO Warfighting Capstone Concept (NWCC) (2023): cognitive superiority, multilevel resilience, sustained impact and demonstration of power, cross-domain command and control, and integrated multilayer defense in five operational environments (domains), including space and cyberspace.

As of the end of 2023, NATO experts have identified 10 main groups of advanced and disruptive technologies:

1) technologies for processing and advanced analytics of large data sets (Big Data and Advanced Analytics, BDAA) and information and communication technologies (ICT))
2) artificial intelligence technologies (Artificial Intelligence, AI);
3) Robotics & Autonomous Systems (RAS);
4) Space Technologies (ST);
5) Hypersonic Technologies (HT);
6) Quantum Technologies (QT);
7) Biotechnology and Human Enhancement Technologies (BHET);
8) Novel Materials & Advanced Manufacturing;
9) energy and advanced energy propulsion (Energy & Propulsion);
10) electronic and electromagnetic technologies (Electronic & Electromagnetic, E&EM).

The main defining characteristics of these technologies are: the symbiosis of human and artificial intelligence, interconnectedness (combination) of virtual and physical dimensions, distributed storage and processing of large data sets, global digitalization of physical, human and information spaces.

Technological developments in the areas of artificial intelligence, autonomy, space, some areas of big data, energy, electrical engineering and electromagnetic effects are considered by NATO experts to be predominantly (but not exclusively) disruptive, as developments in these areas are based on a long history of support for scientific and technological development. Activities in these areas are centered around their effective implementation and impact on other technologies. Thus, a significant or revolutionary disruption of military capabilities is either already underway or will have a significant effect within the next 5-10 years. New developments in quantum technologies, biotechnology, materials with new properties, and some aspects of data analytics (e.g., next-generation 6G communication networks) are assessed as emerging technologies because previous development cycles have had a significant impact on previous technological revolutions. They will require significantly longer development time (10-20 years) before their disruptive nature is fully realized into a specific technological or military capability.

Results and Discussions

Let's analyze the main 10 groups of the latest and most disruptive technologies in more detail.

The "BDAA & ICT" technology group provides advanced analytical tools for analyzing data that is large in volume, variety, structured, reliable, timely, and visualized, and accelerated digitalization, the proliferation of new sensors, new modes of communication, smart things technologies, and the virtualization of social and cognitive spaces greatly contribute to the development of advanced analytics of large distributed data sets. The most well-known new technologies for processing large data sets (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023) are: Advanced Computing & Methods (advanced computing technologies and methods of high-performance computing); Novel Applications & Decision Making (new software and algorithmic applications for decision support with improved interface and visualization and methods of multi-criteria group decision making); Distributed Ledger Technologies (distributed ledger technologies that provide simultaneous access, verification and updating of records in a network database); Advanced Networks (advanced fault-tolerant and cyber-resilient data transmission networks that integrate satellite, cellular, wired and wireless communication channels into a single network); Networked Sensors & Sensing (sensor network and network sensing technologies that allow collecting and analyzing information from various traditional and advanced sensors connected to the network in all operating environments); Data Storage (new data storage technologies); Cyber & Cyberphysical Systems (cyber resilience and cyber defense technologies).

The introduction of BDAA technologies will increase the efficiency of military structures, reduce costs, improve logistics, real-time monitoring of resources and predictive assessments of plans and programs. At the same time, it will generate much greater situational awareness at the strategic, operational, tactical, and defense-industrial levels.

It should be noted that to operate with big data and use it effectively, it is necessary to use faster, more reliable and distributed new-generation communication and data transmission networks. In this area of innovation, the development of mobile broadband networks is becoming increasingly important, allowing for continuous communication and combat control functions during high-speed maneuver operations in wide theaters of war. The required highly efficient and secure military communications can be provided by the latest commercial fifth (5G) and sixth-generation (6G) mobile technologies, which continue to evolve rapidly due to improved technologies and new cellular models (Keller, 2020). Key advances over previous generations include multi-interface access, spectrum expansion, network software based on Network Function Virtualization (NFV), Software-Defined Networking (SDN), and Internet of Things (IoT) features.

The introduction of next-generation military communications technology will ensure high-performance mobility, flexibility and adaptability, data security, cognitive control of bandwidth, frequency, and speed of information transmission to ensure reliable and uninterrupted communication in congested and complex electromagnetic environments, invulnerability to jamming, attacks on fiber-optic cables and satellite communication channels, resistance to cyber attacks on radio software and to electromagnetic pulses caused by electromagnetic munitions or a nuclear explosion at high altitude. To ensure high defense capabilities, military communication systems must become smaller, and lighter, cover multiple operating radio wave bands, and be capable of transmitting any data, including geospatial and video data.

The BDAA & ICT technology group is the core technology group for all EDTs and is central to their use for the development of military operational capabilities, which should be defined in the defense planning process (Slyusar and Kulagin, 2019). However, the greatest synergistic effect is obtained through the combination of these digital technologies with intelligent technologies, in particular artificial intelligence.

The group of technologies "Artificial Intelligence (AI)" is a technology that provides human-made intelligent systems (machines) with the ability to act and perform tasks in a physical or digital environment that usually require human intelligence (e.g., recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action), taking into account a complex goal and choosing the best actions (according to predefined parameters and algorithms), and that need to be performed to achieve the goal based on the perception of its operating environment, interpretation of collected structured or unstructured data, justification of knowledge gained from this data, analysis and selection of possible action strategies that may rely on learning or adaptation to the environment (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023). AI has been called the most influential technology ever invented and is expected to play a significant disruptive role in defense and security.

There are two generalized types of artificial intelligence: "weak" or narrow artificial intelligence (Artificial Narrow Intelligence, ANI) and "strong" artificial intelligence, which consists of general artificial intelligence (AGI) and artificial super intelligence (ASI). ANI is a type of artificial intelligence for solving a certain specialized group of tasks that makes decisions only based on the limited data used for its training. Examples of such systems are: Natural Language Processing (NLP) systems, object or face recognition systems, chatbots, conversational or recommendation assistants, powerful lexicographic systems, machine translation programs and electronic dictionaries, Predictive Maintenance (PdM) models, specialized autonomous platforms, etc. AGI can learn and reason based on experience, solve problems and communicate by imitating generalized human-level intelligent behavior. In addition, it can plan any task. ASI is a type of artificial intelligence that is expected to

exceed the intelligence and abilities of the human brain.

Artificial intelligence is based on Machine Learning (ML) and Deep Learning technologies. ML is a type of artificial intelligence that uses big data and statistical methods of processing it, capable of recoding itself in accordance with constantly growing new data. DL is a subclass of machine learning algorithms based on artificial neural networks (e.g., Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Residual Neural Network (ResNet), Quaternion-Valued Neural Networks (QVNN)), with Long Short-Term Memory (LSTM), both algorithmic and biological (Disentangling AI, Machine Learning, and Deep Learning, 2021), and uses a multi-layer filter system for hierarchical extraction of useful features.

A separate class of RAS is the Lethal Autonomous Weapon System (LAWS), which selects and engages targets that meet certain predefined criteria without human intervention, after a human decision to deploy the weapon with the understanding that the attack, once initiated, cannot be stopped by human intervention (Robotic and Autonomous Systems in a Military Context, 2021).

The ultimate goal of integrating robotic and autonomous systems into military activities is to combine humans and RAS into a powerful, well-coordinated team, allowing RAS to perform boring, dirty, dangerous and expensive tasks while utilizing the unique talents, experience and intuition of humans.

NATO experts have grouped the areas of RAS development into four broad areas (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023): Advanced RAS, RAS Application, Counter-RAS, and RAS Man-Machine Teaming (combining human, robotic, and autonomous systems into a working team).

The widespread introduction of RAS, especially those with artificial intelligence, in the military sphere creates significant moral and ethical challenges, but also opens up new opportunities to increase the efficiency, effectiveness and flexibility of the armed forces by

the speed of decision-making and prioritization of threats, much higher than the human reaction time, which allows to significantly reduce the cycle of observation, orientation, decision-making and implementation of appropriate actions - the OODA cycle (Observe, Orient, Decide, Act)

high reliability and efficiency in performing specific tasks;

accuracy of image recognition and sensory perception of RAS that exceeds the level of human capabilities;

increased range and endurance, ability to control swarming and self-healing of the swarm structure in case of failure of individual elements;

Increased resistance to weather and climatic conditions, pollution, intentional and unintentional mechanical and electromagnetic factors, and combat damage;

reducing the cost of production of mechanical, electronic and software components and services, especially through additive manufacturing;

Increased time of functioning as intended (RAS can perform tedious and repetitive high-level monitoring tasks 24/7 without the need for "rest", logistics planning can be solved efficiently, and the limits of human multitasking can be quickly exceeded);

increasing the flexibility and adaptability of RAS throughout the system's life cycle through scalability, functionality expansion, component and software upgrades, AI training and self-improvement, etc.)

Robotic and autonomous systems represent a transformation of forces and capabilities in the military sphere. They provide a significant military potential to expand the quality, coverage, efficiency and security of military operations and change the forms and methods of armed struggle in future wars and conflicts.

Space Technologies (ST) - technologies developed through space exploration sciences and space vehicles created by the aerospace industry, which necessarily take into account the unique and extreme characteristics of near-Earth, middle and deep space.

Over the past decade, interest in the use of space and space technologies for military purposes has grown significantly, driven by two interrelated trends:

First, over the past few years, the share of commercial space programs has increased significantly, private financial assets have radically changed the directions and intensity of space exploration and contributed to changes in the forms and methods of armed struggle (for example, the use of commercial satellite communications by Starlink (USA), satellite imagery from private American companies Maxar Technologies Ltd, Planet Lab, and BlackSky Technology Inc. as well as Argentine Satellogic, Spanish Deimos Space, and Finnish ICEYE by the Armed Forces of Ukraine in the war against the Russian Federation has significantly increased situational awareness and decision-making support). In addition, the global commercial space industry continues to lead the way in drastically reducing launch costs, new options for deploying space assets, and commercial availability of high-quality space-based information;

second, new technologies and production methods have changed the nature, availability and cost of space utilization (e.g., new propulsion options such as advanced solar-powered electric propulsion systems (Advanced Electric Propulsion System, AEPS) (Peterson, 2021), electromagnetic acceleration technologies for moving payloads into space (SpinLaunch) (Jeffrey, 2022), on-board AI, advanced robotics, remote maintenance of satellites in orbit, reduction of size, weight, power consumption, and cost (SWaP-C) of systems, advanced and new sensors, 3D printing, improved energy storage and efficiency, and next-generation encryption technologies. As a result, outer space is becoming a strategic driver of technological development and geostrategic competition.

In 2019, NATO foreign ministers recognized space as the fifth operational domain of military activities, in January 2022, NATO's Overarching Space Policy (2022) was published, and at the Brussels Summit in 2021, it was recognized that harmful activities in space could lead to the application of Article 5 of the North Atlantic Treaty (Brunner, 2021). Therefore, the use of space in the interests of the system of operational (combat) command and control, communications, computerization - intelligence, surveillance and reconnaissance (Command, Control, Communications, Computers - Intelligence, Surveillance, Reconnaissance, C4ISR), as well as navigation and defense against threats in and from space, are central to many of NATO's existing defense capabilities, and it is the basis on which NATO is building a technological edge that partner countries can join.

Thus, we can confidently expect an increase in the number of space programs, the use of space technologies and the amount of data received from space over the next 20 years. In combination with BDAA & ICT, AI and RAS technologies, space technologies can significantly improve situational awareness at all levels, space-based support for operations, protection of space-based military and commercial infrastructure, reliable missile and space defense, and operational effectiveness of military and humanitarian missions around the world. However, the issue of sustainability of space assets and systems is becoming no less relevant than the benefits provided by such systems.

The Hypersonic Technologies (HT) group of technologies is the technology that enables advanced hypersonic weapons systems (HWS) (missiles, gliders, aircraft, cruise missiles, maneuverable warheads) to reach and maintain a speed of more than Mach 5 (6125 km/h) in the Earth's atmosphere or at its boundary, and to maneuver at such speeds. These systems are particularly strategically disruptive given the reduced reaction time available for Integrated Tactical Warning/Attack Assessment (ITWAA), maneuverability, reduced time to target, difficulty in developing countermeasures, and the threat they pose to critical targets individually or en masse (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023). Systems of this origin can rely on the kinetic effect of use alone or on the use of various types of warheads, including nuclear ones. Countermeasures against such hypersonic systems are particularly challenging due to their speed, maneuverability, and altitude.

The main advantages of HWS are: limited time for detection and warning of use, due to the

high speed and specific flight profile of hypersonic weapons; rapid response to the need to quickly reach and guarantee the destruction of a critical target, especially a moving one or one with temporary vulnerability; high ability to overcome enemy missile defense, due to the combination of high speed, low altitude, maneuverability and stealth; unpredictability for enemy assessment, due to the difficulty of predicting the trajectory of the missile. The main challenges in the design of HWS are the selection of materials that can withstand extreme loads and temperatures, as well as control systems that can operate in extreme conditions, in particular, due to the plasma created around the object moving at hypersonic speeds through dense layers of the atmosphere and isolating the aircraft from signals from the outside. However, new materials, improved modeling and simulation, and more efficient propulsion devices (jet engines) have contributed to certain technological breakthroughs in hypersonic research and significantly increased the likelihood of their widespread operational use (Tirpak, 2018).

Currently, China, Russia, the United States, the United Kingdom, France, India, Iran, Japan, and Australia have openly recognized the research, testing, and experimental use of hypersonic systems (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023), (Speier, Nacouzi, Lee, Moore, 2017), (Mizokami, 2019), (Bernstein, Hancock, 2021), (Hypersonic Weapons, 2024), and the Armed Forces of Ukraine destroyed modern Russian hypersonic missiles X-47M2 Kinzhal and 3M22 Zircon for the first time with the MIM-104 Patriot anti-aircraft missile system during their combat use in the capital of Ukraine in 2022-2024 (Lendon, 2024).

The Quantum Technologies (QT) group of technologies is a group of technologies that use quantum physics and related phenomena at the atomic and subatomic levels, in particular quantum entanglement and superposition (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023), (Amerongen, 2021), (Krelina, 2021). These effects support significant technological advances primarily in cryptography and unbreakable encryption systems, quantum computing, precise navigation and time synchronization, sensing using ultra-sensitive sensors and sophisticated visualization, communication, and the creation of new materials. Quantum phenomena underpin modern technologies, including the transistor, nuclear energy, electron microscopes, superconductivity, photoelectric detectors, medical imaging (functional magnetic resonance and positron emission tomography), lasers, and solid-state devices. Such technologies use the rules of quantum behavior of matter on the atomic scale (less than 10 nm), strong encryption and communication, and hitherto impossible levels of computing power (for some classes of problems).

Quantum technologies can be grouped into five main overlapping groups:

Quantum computing - a type of computing that does not operate according to standard mathematical algorithms, but takes advantage of quantum mechanical phenomena such as superposition, quantum entanglement, and interference (Amerongen, 2021), (Krelina, 2021);

Quantum communication - communication that uses subatomic particles, such as photons, to transmit data using the principles of quantum mechanics, provides the use of secure or cryptographic communication methods using quantum properties, Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) (2023). The Quantum Internet can also be considered part of this field of research, defined as a (theoretical) network built through entangled quantum communication networks and computers;

Quantum sensing and metrology is a field of knowledge about the use of quantum systems, quantum properties or phenomena to measure physical quantities with high accuracy (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023), (Krelina, 2021). For example, the measurement of magnetic or gravitational fields using quantum sensing technologies is used for precise positioning, navigation, and timing synchronization in inertial high-precision navigation systems in combat platforms where the use of global satellite navigation systems such as GPS is impossible or difficult;

quantum materials - materials whose properties can be explained only with reference to

quantum phenomena. Two-dimensional materials, such as graphene or graphene, are often referred to as quantum materials, as are quantum topological materials, whose electronic structures are different (and much more complex) than those of metals or insulators.

Quantum optics - technologies for applying quantum mechanics to understand and exploit the interaction of light with matter. This applies to a variety of applications such as interferometry, photonics, quantum computing, communications, sensing, etc.

Today, three groups of quantum technologies are already considered by military experts as having the potential to revolutionize military operations (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023).

First of all, these are quantum sensors. The use of ultra-sensitive gravimetric, magnetic, or acoustic sensors will significantly increase the effectiveness of underwater warfare capabilities, potentially making the oceans transparent (Roblin, 2019). Quantum radar (O'Donnel, 2019) could make stealth technologies obsolete, provide more accurate target identification, and allow for covert detection and surveillance. Precision clocks will allow for the development of (accurate) PNT systems for use in places inaccessible to GPS (e.g., under ice).

Second, there is quantum computing, potentially the most disruptive quantum technology of all, which could make classical computing tasks that were previously unattainable viable in areas such as optimization, BDAA&ICT, AI, and simulation and testing. This computational advantage can greatly enhance the decision-making and operational effectiveness of any armed force, and for the first time make the most robust modern encryption methods and encrypted data possible to break and steal.

Thirdly, quantum communication and cryptography technologies are used to create ultra-secure communications with a high degree of intrusion detection and low probability of interception. Achievements in quantum communications are considered essential for the development of efficient next-generation wireless communication technologies such as 6G.

Although new quantum technologies have the potential to revolutionize military operations (missions), most of them are still in the early stages of development, and significant technical challenges remain to be addressed before real operational systems can be developed.

The BHET group of technologies includes biotechnologies that use organisms, tissues, cells, or molecular components derived from living things to affect living things or to affect the functioning of cells or molecular components of cells, including their genetic material, and human enhancement technologies that apply biomedical interventions to the human body that improve physical fitness or cognitive, physiological, sensory, or social functions beyond baseline. These technologies cover the spectrum of biological technologies such as genetic manipulation (e.g. CRISPR) for the development of new pathogens or medical countermeasures, manufacturing methods using biological processes, human enhancement technologies using integrated robotics (e.g. exoskeletons, artificial limbs or internal organs), neurointerfaces, vision enhancement technologies, socio-technical symbiosis with AI and RAS, pharmacological approaches to cognitive and physical enhancement, increased virtualization of the socio-cognitive environment that supports the development of new social, information

NATO experts have grouped breakthrough areas of BHET technology research into eight groups (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023), (Ladisch, 2001):

Biowarfare and Heath (biological warfare and military health) - technologies for identifying pathogens, slowing or stopping the pathophysiological processes of bioagents, creating new classes of drugs, means for the prevention and prophylaxis of diseases, biometrics, wound care and tissue regeneration.

Genetics and Microbiology – technologies for gene editing and means to mitigate accidental or intentional misuse of gene editing, development of personalized medicines and therapeutic/prophylactic treatments for military personnel, as well as discovery of genome-based

medical and biotechnological applications.

Bioengineering is a technology that applies engineering principles of design and analysis (with the support of AI/ML technologies) to biological systems and biomedical technologies, their operation (e.g., biomanufacturing) and problem solving in the interaction of such systems. Over the next twenty years, bioengineering is expected to become much easier and cheaper, thanks to new developments that will reduce the cost of biotechnology for reading, writing, and editing genes. In addition, new research efforts are improving and expanding the ability to create complex multicellular systems for enhanced capabilities and functional materials with integrated biological functions. This includes 3D bioprinting, AI/ML-enabled bioengineering, hybrid materials, synthetic biomimetic materials, smart materials, and organoids ("brain balls").

Systems Biology and Bioinformatics – technologies that study complex biological systems through large-scale quantitative analysis of dynamic interactions between multiple components of a biological system. Areas of particular interest include novel chemical, biological, radiological and nuclear biological sensors and computational biology.

Cognitive Enhancement - technologies for improving human cognitive abilities, monitoring and manipulating neural activity in the brain to improve cognitive performance and neurological and psychiatric care in military medicine, as well as for creating new methods and technologies for the treatment of brain injuries, neurodegenerative diseases and certain mental illnesses, including the treatment of post-traumatic stress disorder.

Social Enhancement – technologies for studying social networks, analyzing, modeling and simulating their dynamics, as well as the corresponding social behavior of individuals, certain social groups and society as a whole. The research is being conducted in two directions: predicting new properties of social networks and targeting social consequences, such as disinformation, cognitive and hybrid warfare campaigns, and using "virtual reality" to expand and improve social interaction.

Physical Performancet - technologies for increasing human physical performance and the efficiency of individual biological systems of the body (e.g., strength, endurance, tolerance to pain or fatigue).

Human-Machine Symbiosis – technologies for increasing human productivity with the help of mechanical or electronic means, the use of artificial intelligence, computer vision, augmented reality and human-machine interfaces. Improving SWaP-C characteristics will facilitate the use and eventual development of sensory and motor augmentation capabilities, such as virtual reality contact lenses or exoskeletons.

BHET technologies are expected to become available within the next 20 years. The most breakthrough scientific and technical areas of BHET that should be of interest to the military are: bioinformatics and biosensors, the use of genetic modifications, pharmacological agents, electromechanical devices or neurological interfaces to improve human physiological and neurological performance, medical countermeasures and technologies, synthetic biology, etc.

The Novel Materials & Advanced Manufacturing group of technologies combines technologies for creating artificial materials with unique and novel properties that can be produced using nanotechnology or synthetic biology methods, as well as technologies focused on the design, development, assembly and optimization of manufacturing processes required to create such materials and microelectronics.

Modern advances in BDAA, AI, ST, QT, BHET and new discoveries in materials science (e.g., graphene, one of the thinnest, strongest, stiffest and most extensible crystalline materials (The wonder material graphene may have found its killer app, 2022) have significantly influenced the technological field of creating extremely heat-resistant, high-strength materials for combat platforms, stealth coatings, or coatings capable of collecting and storing energy, superconducting materials, 2-D materials, and topological materials. Interesting research is being conducted on new 2D materials (e.g., graphite, a multilayer allotropic modification of carbon), new polymers, nanomaterials, and

meta-materials (Yiming, 2022). Recently, eight new materials have been discovered that have a structure similar to graphene (Reding, Eaton, 2020): antimonene, arsenene (a single-layer bent honeycomb structure of arsenic), bismuth, boron, borophane, boronene, fagraffen, phosphoren, and stannene. Other similar two-dimensional materials, such as ferromagnetic chromium triiodide, rhenium disulfide, titanium carbides, and molybdenum ditelluride, have unique optical, ferromagnetic, physical, or electrical properties. Polymeric materials are an integral part of the modern economy and military. There are several notable areas of research (Young, 2021): the creation of complex topological structures, functional polymeric materials, sustainable materials, biopolymers, and self-healing polymers. Nanomaterials are nanoscale (one billionth of a meter) materials that exhibit unique optical, electronic, biological, or mechanical properties. Two critical areas of research are (Hecht, 2022): bionanomaterials and quantum dots.

Additive manufacturing, often used synonymously with three-dimensional printing (3D printing) (Additive Manufacturing Research Group, 2018), is the process of creating an almost arbitrary three-dimensional solid object from a digital model by adding materials in layers. Additive manufacturing can be used for: rapid prototyping; rapid production and repair in the field; and the production of precision, customized, or unique parts.

Advanced manufacturing methods encompass many techniques, but two of them deserve special attention because of their potentially disruptive impact on military capabilities: 3D/4D printing and biomanufacturing (reproduction of biological structures using 3D printing for rapid aid to the wounded and their rehabilitation). Unlike 3D printing, 4D printing transforms materials under the influence of changing environmental stimuli, such as pressure, heat, pH, light, humidity, or temperature. Such materials are promising for new structures or sensors, especially in biomedical applications such as biomedical robots, tissue engineering, or bioscaffolds (two- or three-layer tissue-cell structures grown in vitro on the basis of a vascular scaffold that serves as a support for layering cellular structures).

While additive manufacturing methods such as 3D/4D printing continue to evolve, new nano- and microfabrication techniques are being explored to synthesize, assemble, and create materials from the atomic to macro-scale with potential applications in energy, optics, electronics, therapeutics, and genetic engineering (Bechelany, 2022).

Technologies for creating new materials can significantly increase the efficiency and sustainability of combat platforms, provide new more powerful, reliable and safe equipment for military personnel, equip the army with state-of-the-art compact means of communication, reconnaissance and navigation, ensure the creation of protective coatings and stealth coatings, materials for space and hypersonic flights, and additive manufacturing technologies will allow to organize the production of unique parts and structures, rapid restoration and repair of equipment in the field.

Energy & Propulsion Technology Group – technologies for creating new ways to generate energy and store it, as well as building efficient power units (engines).

Social and political interest in combating the effects of anthropogenic climate change, transition to the concept of sustainable economic development, active implementation of green energy technologies, research in the field of renewable energy, environmentally friendly engines, and clean energy generation methods are of significant commercial, social and military interest. In particular, research for NATO defense is focused on four areas (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023): creation of new batteries and energy storage devices (Batteries and Energy Storage); new power generation technologies (Power Generation); search for new ways of energy transmission (Power Transmission); new propulsion systems (Propulsion).

In the field of creating efficient energy storage devices for military needs, work is underway to optimize the traditional technology of lithium-ion batteries and introduce new technologies of potassium-ion and zinc-ion batteries, as well as to study new technologies based on double carbon,

lithium-carbon, lithium-iron-phosphate, sodium-iron, magnesium-sulfur, etc. Some of these technologies are focused on large-scale energy storage, while others are targeted for use in transportation platforms.

Another option for energy storage with significant advantages in weight, safety, lifetime, energy density, charging speed, and toxicity is provided by supercapacitors or ultracapacitors that do not rely on electrochemical storage, or hybrid systems that combine electrochemical energy storage with supercapacitors (Reding, Eaton, 2020), (McFadden, 2020).

Research on clean energy technologies is important to support the climate policy of NATO and European countries. First of all, these are renewable energy sources based on solar energy storage or the use of environmentally friendly biofuels with neutral carbon emissions (e.g., bioethanol, biodiesel, and biobutanol) or hydrogen. Another promising area is the creation of compact (on-site) nuclear power plants based on safer and more environmentally friendly nuclear fuel, such as thorium (David, 2023), (Barry, Santoso, 2022).

Two promising areas are being considered in the field of energy transmission: Wireless Power Transmission (WPT) (for short distances, power is transmitted by magnetic fields using inductive coupling or by electric fields using capacitive coupling, and for long distances, by narrowly focused electromagnetic radiation) and localized power grids (Microgrids) of military camps or ships that can be disconnected from large power grids, thereby increasing the sustainability and localization of power generation.

The development and widespread deployment of efficient propulsion systems or powering military vehicles is a major technical challenge that is being explored in three main areas: electrification of combat platforms, new aerospace engines, and environmental operations.

Examples of the electrification of combat platforms include the replacement of traditional fossil fuel engines with electric or hybrid propulsion systems on aircraft, ships, tanks, and other combat and transportation platforms, and the transition to low-carbon fuels. At the same time, new propulsion systems and fuels should be unified with civilian standards and be compatible with the commercial production sector. For example, the Tactical Vehicle Electrification Kits (TVEK) developed for the U.S. Army's ground forces reduce average fuel consumption by 25%. The first prototype of an all-electric light reconnaissance vehicle, the Electric Light Reconnaissance Vehicle (eLRV), is being tested, and the full transition of military and transport equipment to hybrid powerplants is planned by 2035, and to all-electric ones by 2050 (Kulagin, Solonets, Kvitkin, Medved, Gubareva, 2023).

E&EM Technologies Group – technologies for the creation of microelectronic and microelectromechanical devices and other electronic component base, search for new circuitry solutions and new architecture of integrated circuit crystals, improvement of semiconductor technologies and materials, as well as creation of devices for generating and emitting powerful pulses of electromagnetic radiation, powerful pulsed power supplies with high specific energy density, development of new approaches to generating powerful microwaves.

Technological progress and the implementation of EDT technologies depend heavily on the development of new microelectronics and electromagnetic spectrum management. However, the constant scaling of the silicon-based electronic component base, according to NATO experts (Reding, Eaton, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023), will face severe physical limitations over the next ten years. This will require new approaches to electronic systems that use new materials, designs, architectures (combining memory and computing), physics (magnetic states, electron spin properties, topological insulators, phase-shifting materials, trapped ions, and photonic quantum circuits), photonics, artificial intelligence-enabled design tools, and neuromorphic chip designs (Budget Estimates Justification Book, 2022). The electromagnetic spectrum is becoming an increasingly competitive and congested area. Therefore, research is constantly underway to maximize

and optimize it (e.g., cognitive radios and frequency management) while taking into account the challenges of electronic warfare.

It is expected (Reding, Lucia, Blanco, Regan, Bayliss, 2023) that over the next 20 years, development will occur in the following areas:

Advanced Electronics and Electromagnetics – technologies for creating new microelectronics based on traditional and innovative materials. A significant part of this research is grouped into three broad categories (Reding, Lucia, Blanco, Regan, Bayliss, 2023), (Budget Estimates Justification Book, 2022): Materials (new silicon-free compounds (e.g., gallium, gallium arsenide or nitride, silicon carbide, etc.) and 2D materials), Architecture (rethinking the architecture of silicon-based microchips and boards, specialized circuits built with artificial intelligence, circuits for biomimetic, neuromorphic, and hyperdimensional computing), and Design (improving chip performance, design, and layout using AI/ML technologies);

Antennas (new antenna designs) – technologies for creating new antenna designs and sensor systems with improved SWaP-C characteristics and performance, as well as long-distance wireless communication systems, including underground and underwater. Promising research is in the following areas: antennas with mechanical control of magnetic/electric fields at ultra-low frequency (ULF), from 0.3 to 3 kHz, and ultra-low frequency (VLF), from 3 to 30 kHz, for long-range wireless communications, as well as underwater and underground communication channels antennas for ultra-wideband emitters and receivers to provide reliable and secure communication channels that are resistant to electronic warfare; 4D antenna arrays for multi-channel transmission and intelligent electromagnetic beamforming;

Photonics and Lasers – technologies for manipulating electrons and photons for information transmission, signal processing, spectroscopic sensing and imaging, as well as for the development of microchips modeled on the basis of neural processes (neuromorphic photonics), ideal for AI/ML applications. In addition, the development of silicon chips for light control and nanolasers on a chip allows us to move to quantum computing;

Spectrum (electromagnetic spectrum) – technologies for the efficient use of the available electromagnetic spectrum, its control and counteracting access to such spectrum by hostile parties. Promising research is focused on three areas: Adaptive camouflage (developments aimed at adapting the optical and near-optical signatures of humans, transport platforms or objects to the existing background or environment), high-frequency high-power redundant matching (development of powerful amplifiers designed to organize communication at high-frequency millimeter-wave waves to provide high-speed communication, increased sensitivity and increased sensor resolution) and adaptive spectrum management (development of cognitive radios or sensors using

Directed Energy Weapons (DEW) – technologies for creating laser, microwave, beam and sound weapons to blind the sensors of combat platforms and satellites, suppress the functioning or physical destruction of an enemy target (manpower, missiles, aircraft, unmanned platforms, vehicles, etc.

The most promising DEW developments are the High-Energy Laser (HEL) and High-Powered Microwave (HPM) weapons, which have the potential to generate effects over a wider area, disabling any electronics within their electromagnetic cone than laser weapons. While hardly a new technology, directed energy weapons (DEWs) have evolved and demand for them has increased dramatically around the world. These lasers and high-powered microwave weapons are already a devastating force on the battlefield, and are expected to be used even more widely over the next few years.

The current global DEW market is estimated to be worth USD 14.3 billion and will grow to USD 72.1 billion by 2028 (Global Directed Energy Weapons Industry, 2022). This growth is largely driven by improvements in energy storage systems, AI/ML and new material technologies. Many

DEW systems have been commissioned or have a very high level of technological readiness (Reding, Lucia, Blanco, Regan, Bayliss, 2023), (Kelley, Feickert, O'Rourke, 2023), (Hoffman, 2021), (Klontsak, Kamalov, Stetsyura, 2022).

The combination of these technologies and new mechanisms of interaction between them allow for the creation of new convergent technologies that may later become breakthroughs. For example, the synergistic combination of big data analytics and artificial intelligence technologies using intelligent, widespread and cheap sensors together with autonomy technologies should provide a potential military strategic and operational advantage, the addition of quantum technologies will expand the capabilities of data collection, processing and use (C4ISR) by significantly increasing the capabilities of sensors, secure communication and computing, the addition of new materials creation technologies will facilitate the development of materials with unconventional In turn, the development of exotic materials, new structures, miniaturization, new ways of generating and storing energy, additive manufacturing methods, and improved powertrain and engine designs will contribute to the full utilization of all five operating environments, including cyberspace and space, by reducing costs, increasing reliability, improving performance, and facilitating production.

To understand the status and pace of development of EDTs or combinations of EDTs, the importance and prospects of each technology group, certain evaluation criteria are used: potential military impact, the level of attention or excitement surrounding a particular technology or scientific field, the current level of technological readiness, the time horizon in which the science or technology is expected to be fully mature, the fit with defined operational capabilities, and the areas of science and technology that are significantly impacted by the introduction of EDT technologies.

The first step is to assess the potential probable impact of the introduction of a technology or several technologies on changing the defining characteristics of defense capabilities or carriers of these capabilities (military organizational structures, models (complexes, systems) of weapons and military equipment), such as speed, range, accuracy, lethality, survivability, availability, etc. This impact can be moderate (10-50%), high (50-100%) or revolutionary (a fundamental change in the characteristics of existing capabilities or the acquisition of completely new capabilities that were previously unattainable or underestimated).

The second stage assesses the level of attention and enthusiasm for the technology, as well as the ability of the technology to go through all the stages of integration into a sustainable technological environment. At this stage, experts should analyze many different factors that reflect the level of attention to the technology, its innovation potential and investment attractiveness: the list of countries that pay attention to a particular technology, their military potential rating and the dynamics of revenues from the sale of military technologies; inclusion of research on a particular technology in overall defense spending; the level of investment in technology development and the demand for training and qualification of personnel; the number of scientific publications and patents; the results of the risk analysis of the reassessment of the technology; and the inclusion of research on a particular technology in total defense spending; the level of investment in technology development and the demand for training and qualification of personnel; the number of scientific publications and patents; the results of the analysis of the risks of overestimating or underestimating the potential of technology and many other factors.

An interesting tool introduced by the American company Gartner, Inc, the so-called "Hype Cycle for Emerging Technologies" – a cycle that shows how a potentially successful new technology goes through five key phases (Slyusar, Sotnyk, Kupchin, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023): trigger of innovation, peak of high expectations, disappointment, enlightenment, and plateau of performance. A unique aspect of this tool is its ability to summarize information from a variety of technologies that Gartner, Inc. annually reviews, identifying only the most transformative

ones that analysts predict will revolutionize certain industries within 10 years. For example, Figure 1 shows the Gartner cycle for 2023.

Technologies do not always progress from the beginning to the end of such a cycle, many areas of science or technological discoveries never create breakthroughs for innovation, or they disappear from public consciousness after the initial fascination as unproductive areas of development, or they may appear later as new convergent developments that give rise to an old idea. The development of most new technologies can be predicted only with a certain degree of probability, but the evolutionary process built on creative failures and mistakes is essential for scientific and technological progress, as lessons learned and fantastic ideas lead to entirely new areas of research, discovery and innovation. Balancing the peak of high expectations with the low point of the disillusionment problem is a critical task in making decisions about investments and long-term capabilities. The Gartner cycle is useful for this purpose, but there are notable shortcomings in its use as a tool for evaluation and decision-making, in particular, the placement of a technology on the Gartner curve is determined by the level of expectations (hype) assessed by experts, rather than by quantitative indicators of technology development.

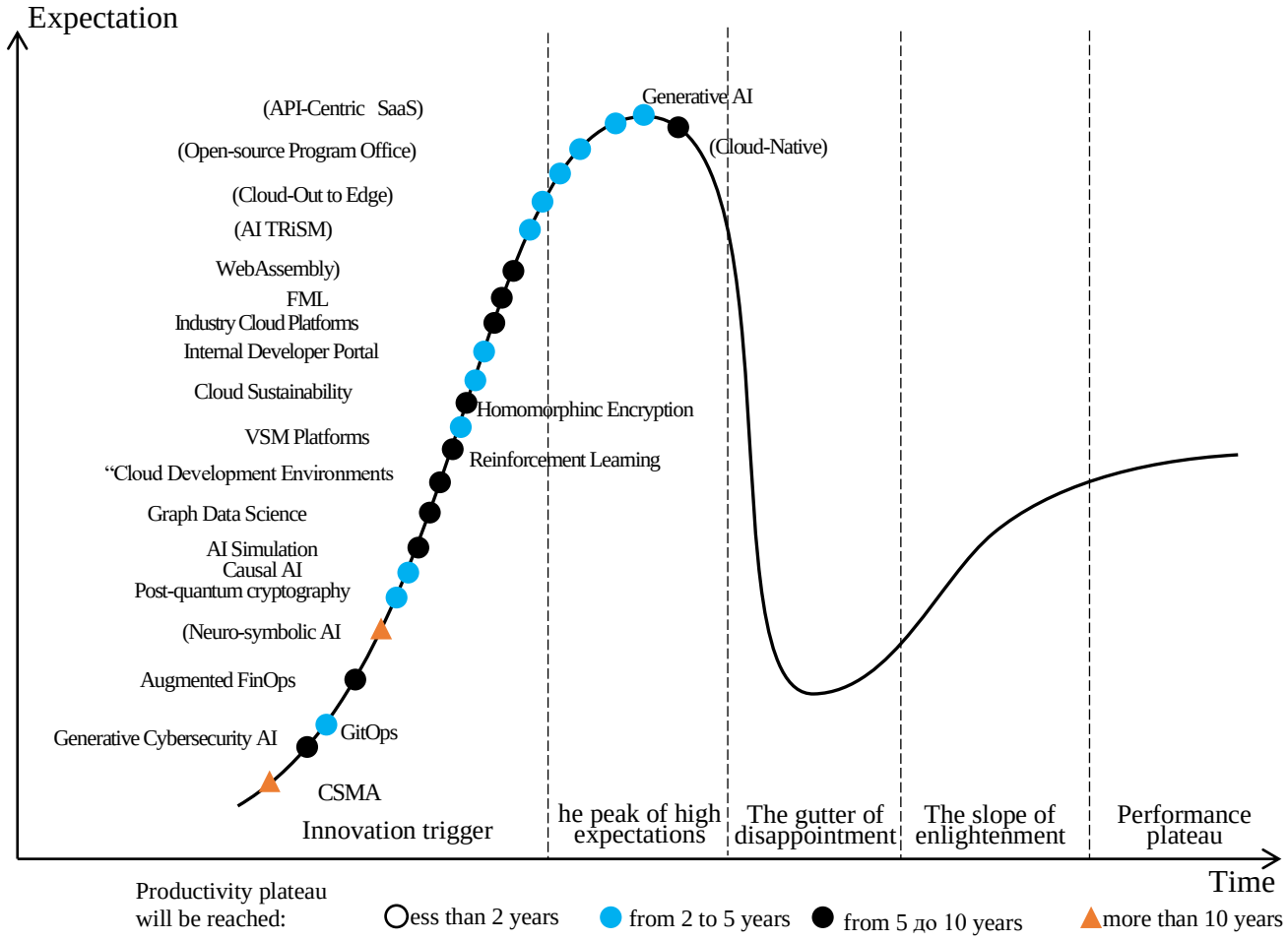


Figure 1. Gartner cycle for the latest (emerging) technologies for 2023

The third stage is the assessment of the technology's maturity level (Technology Readiness Level, TRL). The assessment system is based on a scale of nine levels, where 1 is the lowest, basic level of readiness, and 9 is the highest. There are 9 levels of technology readiness in total. The US National Aerospace Agency (NASA) first proposed such an assessment scale, and later the European Commission advised EU-funded research and innovation projects to adopt this scale (From the lab to

commercialization: the path of knowledge-intensive products through the levels of technological readiness. Innovation Cases, 2023).

At the lowest level of maturity (TRL1), scientific research is transformed into applied research and development, the basic principles of the technology are developed and described, research results are published and peer-reviewed, but the technology exists only "on paper". At TRL2, the principles of the technology have been studied, the concept of the technology has been formulated, and the initial results can be applied in practice, the practical application has been identified, but it is of a general nature. At the stage of reaching TRL3, active research and development, both analytical and experimental studies, begin to verify the viability of the technology, experimental proof of concept and its readiness for further development. After a successful proof of concept at TRL3, the main components of the technology must be integrated to ensure that the individual elements can work together successfully, the technology is tested in the laboratory, and test results are documented to demonstrate compliance with analytical predictions. At the TRL5 stage, testing prototypes of the technology allows us to predict the tasks for the next stages of development. A fully functional prototype or representative model is demonstrated and operated in an appropriate use environment at TRL6. TRL7 level - demonstrates the operation of a real prototype of the technology in the working environment and its performance in real operating conditions. The demonstration should be a prototype of a real-world application. If it is a physical prototype, it is a high-precision engineering unit that adequately addresses all critical scaling issues, built and operated in an appropriate environment to demonstrate performance in a real-world operating environment and platform (land, sea, air or space), and if it is software, there is a prototype with all key functions available for demonstration and testing. All technologies used in real systems go through TRL 8. In almost all cases, this level is the final stage of technology development. At this level, the final product in its final configuration has been successfully demonstrated through testing and analysis for a defined operating environment and the corresponding platform. All software is debugged and fully integrated with all existing hardware and software systems. All user documentation, training and maintenance documentation is complete. The TRL9 level in almost all cases is the final correction of bugs and major aspects of operation in real conditions. It can also be about integrating a new technology into an existing system. At this level, the technology can be used by customers, ongoing technical support has been established, and the technology or product is ready for mass production.

Figure 2 summarizes the levels of technological maturity of the main groups of new and disruptive technologies discussed above.

The fourth stage assesses the time horizon for reaching the level of technological maturity (TRL8-TRL9). This is a rather important time indicator, especially for investors. The time horizon for technology maturity is estimated in various foresight studies (Slyusar, Sotnyk, Kupchyn, 2020), (Reding, Lucia, Blanco, Regan, Bayliss, 2023).

At the fifth stage, the impact on current and future defense capabilities is assessed and proposals are formulated as part of the defense planning process (Slyusar and Kulagin, 2019). Each technology is assessed for its potential impact (low, medium or high). Almost all of the technology groups reviewed were assessed by NATO experts as having a high or even revolutionary level of impact on the Alliance's defense capabilities.

Defense science is divided into three broad areas, covering research in the human (including biological), information and physical domains of science and technology. Therefore, the sixth stage links EDT to these three major research areas, which helps to ensure a holistic approach to EDT research, development and exploitation.

Assessing the potential impact of emerging or disruptive technologies is therefore not a straightforward process. It requires consideration of the threat environment (current and future), legal and policy constraints, political factors, investment decisions, and an assessment of economic and entrepreneurial potential, risk tolerance and willingness.

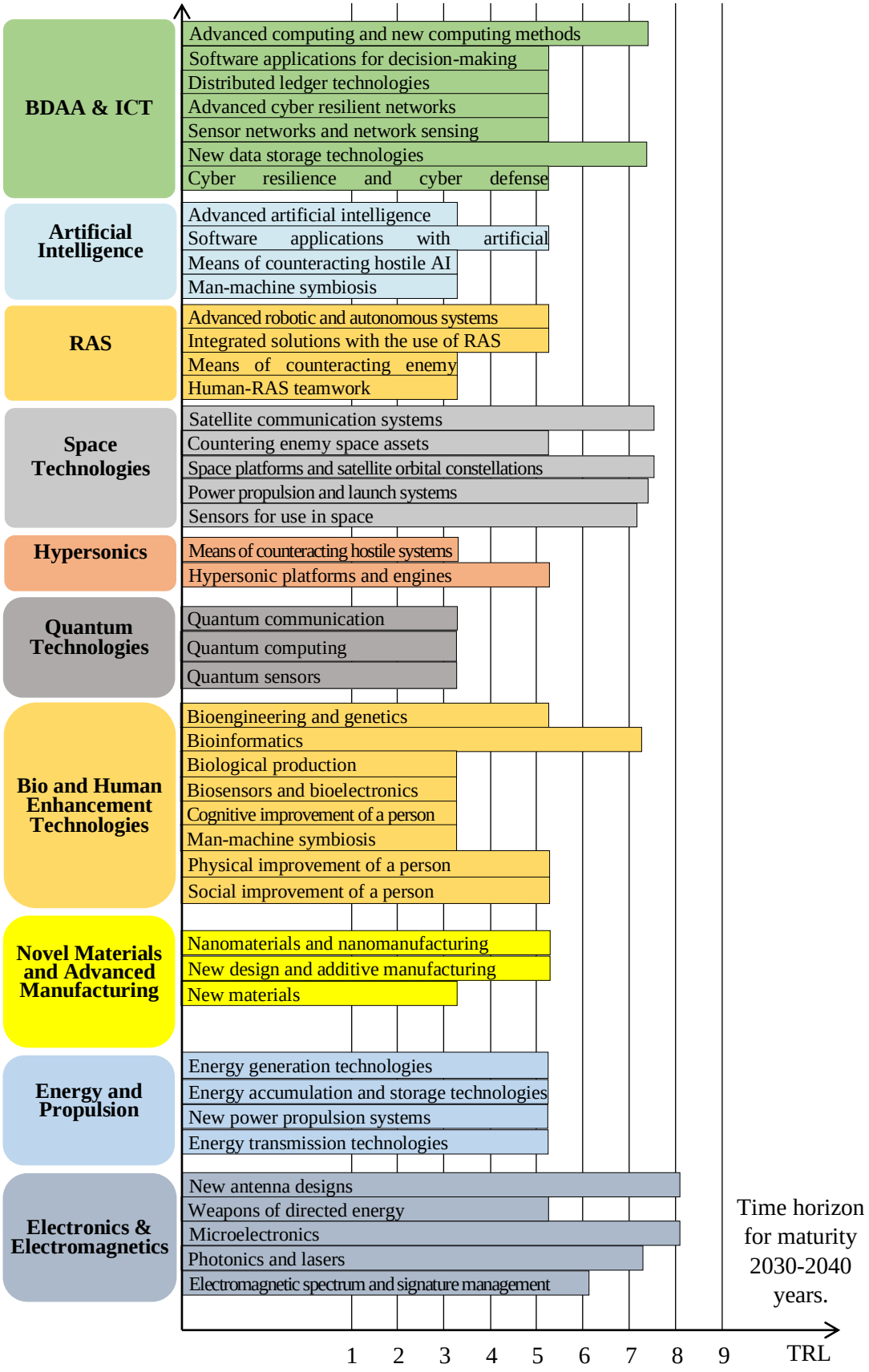


Figure 2. Summarizing the levels of technological maturity of the main groups of new and disruptive technologies discussed above

Conclusion

This article examines how new and disruptive technologies can enable or influence military capabilities in a timeframe of up to 20 years. Individually or in combination, they define the technological frontier necessary for the effectiveness of operational and organizational forces in the security and defense sector. How quickly, in what order, and ultimately how successful these technologies will be, or what risks they will pose, is not yet fully understood. The range of potential military operational domains is constantly expanding and evolving, just as the geopolitical, military, economic, social, climate, and technological landscapes are changing. However, long-term forecasts of military experts, in particular from NATO countries, provide useful information and professional advice on prioritizing new opportunities and technological investments, provide a basis for selecting promising areas for further research in the field of economic security and national defense, and contribute to technological awareness and preparedness for effective investment policy and development of the defense industry.

The systematic analysis of the ten main groups of new and breakthrough technologies recognized by NATO experts, which are expected to reach technological maturity in the next 15-20 years and significantly affect the defense capabilities of NATO member states and, accordingly, partner countries, can be useful for specialists who formulate the military-technical and defense-industrial policy of the state.

In order to develop military capabilities that meet current and future geostrategic challenges, countries must be at the forefront of innovation, science and technology, design and production of the most modern and technologically advanced weapons and military equipment. This also requires a sound assessment of the potential security environment in the future, especially with regard to military challenges and security threats arising from new scientific and technological discoveries and the implementation of breakthrough technologies in an open globalized world.

Continuous monitoring of scientific and technological trends, determination of their breakthrough military potential, and the risks of both overestimation and financial miscalculations, as well as underestimation and expected vulnerability of the security and defense system, is one of the tools for increasing the defense technological advantage or at least maintaining military-technological parity with an equal adversary, and it also accelerates the introduction of innovations, new and breakthrough technologies in the defense industry.

The results obtained will allow to focus the attention of the scientific community on the main innovation trends in the defense sector and to involve the widest possible range of experts in discussing and justifying promising and priority areas for Ukraine to introduce the latest and most disruptive technologies, risk analysis and reasonable selection of technologies that have the potential to become critical for the state.

Recommendations

The materials of the article are recommended for use by the scientific and scientific-pedagogical staff of scientific institutions and higher educational institutions of the Armed Forces of Ukraine and the Ministry of Defense of Ukraine, experts of other ministries that support the security and defense sector, and specialists of the defense industry.

In the future, it is advisable to focus on a more detailed definition of the list of the latest and most breakthrough technologies that have the potential to be implemented in Ukraine independently or with the support of partner countries, their deeper analysis and evaluation, in particular, the degree of criticality for the national security of the state and technological superiority to bring victory in the aggressive war unleashed by the Russian Federation.

References

1. Schwab, K. (2017). The fourth industrial revolution. Exmo. http://loveread.ec/

contents.php?id=66348.
2. Schwab, K. (2018). Technologies of the Fourth Industrial Revolution. Exmo. http://loveread.ec/view_global.php?id=73865.
3. Christensen, K. M. (2004). The innovator's dilemma. How strong companies die because of new technologies. Alpina Business Books.
4. Rotolo, D., Hicks, D., Martin, B. (2015). *What is an emerging technology?* University of Sussex. (Version 1). https://hdl.handle.net/10779/uos.23420075.v1.
5. Küfeoğlu, S. (2022). Emerging Technologies. *Sustainable Development Goals Series.* Springer, Cham. 11-21. https://doi.org/10.1007/978-3-031-07127-0_2.
6. Mariette, D., Meyerson, S.B. (2023). *Top 10 Emerging Technologies of 2023, Flagship Report, Centre for Fourth Industrial Revolution*. World Economic Forum. https://www.weforum.org/publications/top-10-emerging-technologies-of-2023/.
7. Armstrong, P. (2017). *Disruptive Technologies. Understand, evaluate, respond*. Kogan Page Publishers.
8. Manners-Bell, J., Lyon, K. (2022). *Logistics and supply chain innovation. A practical guide to disruptive technologies and new business model*. Kogan Page Publishers.
9. Slyusar, V. I., Sotnyk, V. V., Kupchyn, A. V. (2020). Breakthrough technologies in the defense sphere of Ukraine. *Armament and military equipment*, Kyiv. 4 (28). 13-23.
10. Sotnyk, V. V., Rasstrygin, O. O., Kupchyn, A. V. (2020). Methodology of selection of critical technologies. *Modern information technologies in the field of security and defense*. 1(37). 67-76. http://doi.org/10.33099/2311-7249/2020-37-1-67-76.
11. Matyushenko, I. Yu. (2016). Development and implementation of convergent technologies in Ukraine in the conditions of the new industrial revolution: organization of state support. FOP Alexandrova K. M.
12. Pisarenko, T., Kvasha, T., Havrys, T. (2021). Analysis of global technological trends in the military sphere. UkrINTEI. http://doi.org/10.35668/978-966-479-127-1.
13. Pisarenko, T., Kvasha, T. (2020). Global technological trends in the field of weapons and military equipment. UkrINTEI. http://doi.org/10.35668/978-966-479-117-2.
14. Reding, D. F., Eaton, J. (2020). *Science & Technology Trends 2020-2040. Exploring the S&T Edge*. March, 2020. NATO Science & Technology Organization, Office of the Chief Scientist, Brussels. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.
15. Reding, D. F., Lucia, A. D., Blanco, A. M, Regan, L. A., Bayliss, D. (2023). *Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains. Overview.* 1. NATO Science & Technology Organization, Office of the Chief Scientist. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf.
16. Reding, D. F., Lucia, A. D., Blanco, A. M, Regan, L. A., Bayliss, D. (2023). *Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains. Analysis.* 2. NATO Science & Technology Organization, Office of the Chief Scientist. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf.
17. Chana, Deeph. (2020). *NATO Advisory Group on Emerging and Disruptive Technologies. Annual report.* North Atlantic Treaty Organization. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf.
18. Chana, Deeph. (2021). *NATO Advisory Group on Emerging and Disruptive Technologies. Annual report.* North Atlantic Treaty Organization. https://www.nato.int/nato_static_fl2014/

assets/pdf/2022/7/pdf/220715-EDT-adv-grp-annual-report-2021.pdf.
19. *NATO Warfighting Capstone Concept.* (2023). Allied command transformation NATO'S Strategic Warfare Development Command. https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf.
20. Keller, J. (2020). What 5G means to the military. *The Military & Aerospace Electronics*. December 2. https://www.militaryaerospace.com/rf-analog/article/14188341/military-5g-communications.
21. Slyusar, V. I., Kulagin, K. K. (2019). Peculiarities of NATO's defense planning process. Science and technology of the Air Force of Ukraine. 3(36). 47-59. http://dx.doi.org/10.30748/nitps.2019.36.06.
22. *Disentangling AI, Machine Learning, and Deep Learning.* (2021). April 5. Exxact Corporation. https://www.exxactcorp.com/blog/Deep-Learning/difference-between-ai-machine-learning-and-deep-learning?gclid=Cj0KCQiA47GNBhDrARIsAKfZ2rALRgE7vtm XoqQx_-fWly40_XMl_Q-esKbaEzfx5Rbw5M2mVRwIk0QaArYaEALw_wcB.
23. Robotic and Autonomous Systems in a Military Context. (2021). Jstor.org. https://www.jstor.org/stable/pdf/resrep29554.3.pdf.
24. Peterson, P. (2021). September 26. *Advanced Electric Propulsion System (AEPS) Enabling a Sustainable Return to the Lunar Surface through NASA Gateway. 74th Annual Gaseous Electronics Conference*. NTRS – NASA Technical Reports Server https://ntrs.nasa.gov/citations/20210022011.
25. Jeffrey, C. (2022). *Here's what it looks like to get flung from a centrifuge at 1,000 mph.* Techspot. May 4. https://www.techspot.com/news/94466-here-what-looks-like-get-flung-centrifuge-1000.html.
26. *NATO's overarching Space Policy.* (2022). North Atlantic Treaty Organization. January 17. https://www.nato.int/cps/en/natohq/official_texts_190862.htm.
27. Brunner, Karl-Heinz. (2021). *Space and Security – NATO'S Role. Preliminary Draft Special Report.* October 10. https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/025%20STC%2021%20E%20-%20SPACE%20AND%20SECURITY%20-%20BRUNNER_2.pdf.
28. Tirpak, J.A. (2018). The Great Hypersonic Race. *The Great Hypersonic Race – Air Force Magazine*. June 27. https://www.airandspaceforces.com/article/the-great-hypersonic-race/.
29. Speier, R. H., Nacouzi G., Carrie Lee and Moore, R. (2017). *Hypersonic Missile Nonproliferation: Hindering the Spread of a New Class of Weapons*. CA: RAND Corporation. June 27. https://www.rand.org/pubs/research_reports/RR2137.html.
30. Mizokami, Kyle. (2019). Russia's New Hypersonic Weapon Flies at Mach 27. *Popular Mechanics*. Dec. 30. https://www.popularmechanics.com/military/weapons/a30346798/russia-new-hypersonic-weapon-mach-27/.
31. Bernstein, P., Hancock, D. (2021). China's Hypersonic Weapons. *Georgetown Journal of International Affairs*. January 27. https://gjia.georgetown.edu/2021/01/27/chinas-hypersonic-weapons/.
32. Hypersonic weapons. (2024). *Deep State*. Vanguard. Feb. 20. https://deepstateua.com/hypersonic_missiles/.
33. Mizokami, K. (2022). Russia Is Using Hypersonic Weapons to 'Put Fear Into the Hearts of Ukrainians. *Popular Mechanics*. Apr. 05. https://www.popularmechanics.com/military/weapons/a39600945/why-russia-is-using-hypersonic-weapons-in-ukraine/.

34. Lendon, Brad. (2024). Russia used an advanced hypersonic missile for the first time in recent strike, Ukraine claims. *CNN Business*. Feb. 13. https://edition.cnn.com/2024/02/13/europe/ukraine-russia-zircon-hypersonic-missile-intl-hnk-ml/index.htm.
35. Amerongen, M. (2021). Quantum technologies in defense and security. June 03. https://www.nato.int/docu/review/uk/articles/2021/06/03/kvantov-tehnolog-v-oboron-bezpets/index.html.
36. Krelina, M. (2021). Quantum technology for military Applications. *EPJ Quantum Technology*. https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-021-00113-y.
37. Post-Quantum Cryptography. (2023). National Institute of Standards and Technology. Computer Security Resource Center. 22nd of November. https://csrc.nist.gov/projects/post-quantum-cryptography.
38. Roblin, S. (2019). No More "Stealth" Submarines: Could Quantum "Radar" Make Submarines Easy to Track (And Kill)? *The National Interest*. 27th of April. https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547.
39. Wes O'Donnel. (2019). Quantum Radar a Game Changer for Offensive Stealth Operations. American Military University EDGE. Sept. 11. https://amuedge.com/quantum-radar-a-game-changer-for-offensive-stealth-operations/.
40. Ladisch, M. (2001). *Opportunities in Biotechnology for Future Army Applications*. National Academies Press. June 11. https://doi.org/10.17226/10142.
41. The wonder material graphene may have found its killer app. (2022). *The Economist*. May. https://www.economist.com/science-and-technology/2022/05/18/the-wonder-material-graphene-may-have-found-its-killer-app.
42. Yiming, Hu. (2022). Synthesis of γ-graphyne using dynamic covalent chemistry *Nature Synthesis.* 1. 449–454. May 09. https://www.nature.com/articles/s44160-022-00068-7.
43. Young, J. (2021). *What are the most important areas in polymer research?* https://www.hindawi.com/post/what-are-most-important-areas-polymer-research/.
44. Hecht, J. (2022). Nanomaterials pave the way for the next computing generation. *Nature 608.7922*. Aug. 10. https://www.nature.com/articles/d41586-022-02147-3.
45. *Additive Manufacturing Research Group* (AMRG). (2018) The 7 categories of Additive Manufacturing, Additive Manufacturing Research Group, Loughborough University. Loughborough University. https://www.lboro.ac.uk/research/amrg/about/the7categoriesofadditivemanufacturing/.
46. Bechelany, M. (2022). Nanofabrication and Nanomanufacturing. *Nanomaterials 12*(3). https://www.researchgate.net/publication/358202961_Nanofabrication_and_Nanomanufacturing.
47. McFadden, C. (2020). Could Ultracapacitors Replace Batteries in Future Electric Vehicles? June 6. https://interestingengineering.com/science/could-ultracapacitors-replace-batteries-in-future-electric-vehicles.
48. David, E. (2023). Power Electronics Handbook by Muhammad H. Rashid. *Cosmic Journal of Phisics. 2*(1). 38-60. https://www.researchgate.net/publication/375598117_Power_Electronics_Handbook_by.
49. Barry, N., Santoso, S. (2022). Modernizing Tactical Military Microgrids to Keep Pace with the Electrification of Warfare. *Military Review*. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/ND-22/Barry/Barry%20November-December-

UA.pdf.

50. Kulagin, K. K., Solonets, O. I., Kvitkin, K. P., Vedmid, O. I., Gubareva, O. P. (2023). Impact of climate change on the safety of military operations and the life cycle of weapons and military equipment. *Systems of Arms and Military Equipment.* 2 (74). https://doi.org/10.30748/soivt.2023.74.06.
51. Budget Estimates Justification Book. (2022). Defense Advanced Research Projects Agency. Department of Defense Fiscal Year. https://www.darpa.mil/attachments/U_RDTE_MJB_DARPA_PB_2023_APR_2022_FINAL.pdf.
52. *Global Directed Energy Weapons Industry*. (2022). ReportLinker. October. https://www.reportlinker.com/p05798382/Global-Directed-Energy-Weapons-Industry.html?utm_source=GNW.
53. Kelley, M., Feickert, A., O'Rourke, R. (2023). Background and Issues for Congress. August 22. https://sgp.fas.org/crs/weapons/R46925.pdf.
54. Hoffman, R. (2021). High Power Microwaves High Power Microwave (HPM) 6.1 Programs. *NVAL Science & Technology*. https://www.nre.navy.mil/media/document/directed-energy-weapons-dew-high-power-microwave-hpm-61-programs-fy21-annual-report.
55. Klontsak, M.Ya., Kamalov, E.V., Stetsyura, I.R. (2022). Prospects for equipping the Armed Forces of Ukraine with directed energy weapons. *Collection of scientific works of the Center for Military and Strategic Studies of the National Defense University of Ukraine named after Ivan Chernyakhovsky*. 3(76). http://znp-cvsd.nuou.org.ua/article/view/274787/269951.
56. *From the laboratory to commercialization: the path of science-intensive products through the levels of technological readiness. Innovative cases*. (2023). NEF (New Economy of Ivano-Frankivsk). September 10. https://neweconomy.if.ua/innovations/innovation-cases/z-laboratoriyi-do-komerczializacziyi-shlyah-naukoyemnyh-produktiv-kriz-rivni-tehnologichnoyi-gotovnosti/.

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.16

Artificial intelligence in the sphere of cybersecurity: innovations, challenges, and development prospects

Roman Pantiushenko
Leading Researcher of the Research and Testing Section
Central Research Institute of the Armed Forces of Ukraine
03049, Povitroflotskyi Ave., 28 B, Kyiv, Ukraine
e-mail: prvm79@gmail.com
ORCID: 0000-0002-9301-9389

Yuliia Chaika
Head of Research Section
Central Research Institute of the Armed Forces of Ukraine
03049, Povitroflotskyi Ave., 28 B, Kyiv, Ukraine
e-mail: jul.seagull@gmail.com
ORCID: 0009-0002-4342-3313

Abstract. The relevance of the study is due to the need for effective protection of information systems in the face of ever-growing cyber threats. In the modern digital world, where cyberattacks are becoming increasingly complex and widespread, the use of artificial intelligence in cybersecurity is extremely relevant. The problem of cybersecurity is becoming increasingly important and conducting relevant research is becoming a necessary aspect of ensuring security in the digital space.

In this context, we propose an article that examines the role of artificial intelligence, innovations, challenges, and prospects of its development in the sphere of cybersecurity. Additionally, it explores the utilization of artificial intelligence for automating processes of detecting, analysing, and responding to cyber threats, and its practical significance for enhancing security levels in the digital space and the effectiveness of cyber threat protection.

The main approaches for this study are trend analysis and expert assessments, which allow for a comprehensive review of the directions of artificial intelligence development in the field of cybersecurity, the benefits and challenges of its implementation, as well as potential opportunities and threats to information security.

The article discusses advanced security information and event management systems designed to collect, analyse and respond to cyber threats and other systems aimed at specific aspects of protection and expanding automation capabilities to improve the security level of information systems.

The materials of the article are of theoretical value for further scientific research on the use of artificial intelligence in the sphere of cybersecurity and reflect important features of its influence on this area. This research can contribute not only to deepening the understanding of the theoretical aspects of the use of artificial intelligence in cybersecurity but also to identifying specific practical applications and innovations that will help improve protection against cyber threats in the future.

Keywords: artificial intelligence, cyberspace, big data, Security Information and Event Management.

Introduction

The rapid and unrestrained development of digital technologies has led to cybersecurity becoming one of our time's most pressing and urgent issues (Hryshchuk, Zhovnovatiuk, Nosova,

2019). In a world where cybercrime is spreading faster than ever (Kogut, 2022), protecting against cyberattacks is a priority for all organisations and individuals operating in cyberspace. In this context, artificial intelligence (AI) is becoming increasingly important and relevant (Onyshchenko, Kalancha, Geldt, 2023) as a tool for detecting, countering and preventing cyber threats.

This article discusses the role and benefits of using AI in cybersecurity (Gurzhiy, 2023) and the challenges and prospects for further development.

Focusing on innovative methods and technologies, the research was conducted on the impact of AI on the efficiency and reliability of cybersecurity and the possibilities for further improvement (Ustymenko, Olishevskyi, 2022) in this area to ensure security in the digital space were considered.

Methodological Framework

The study examined Security Information and Event Management (SIEM) systems intended to collect, analyse and respond to cyber threats (Yushko and Shevchuk, 2020). These technologies provide real-time monitoring and analysis of events occurring in networks and other components of information systems. The obtained data was used to identify the main trends, challenges, and prospects for the development of AI in cybersecurity.

Modern SIEM systems are actively using AI to improve the efficiency of cyber threat detection. The use of AI helps to automate the collection, and analysis of big data (BD) and detection of anomalies, significantly increasing the efficiency of responding to potential threats. The AI-based approach allows us to effectively identify unusual patterns in system and user behaviour that may indicate potential threats.

Consequently, the use of AI in SIEM systems helps to increase the efficiency and speed of cyber threat detection, as well as reduce incident response time, which in turn increases the overall level of cybersecurity.

Results and Discussions

In the modern world, where cyber threats are becoming increasingly complex and sophisticated, the use of AI in the sphere of cybersecurity is extremely important and necessary. Innovative methods and technologies based on the use of AI play a key role in the continuous improvement of cyber security.

AI is widely used in cybersecurity to automate the process of detecting and analysing potential cyber threats, analysing information from event logs, detecting anomalies in user behaviour, recognising new and unknown threats, and developing predictive models to help predict possible attacks. According to research, the use of AI in cybersecurity can reduce the time for detection and recovery from an incident by up to 25% and reduce the number of false alarms by up to 50%. These capabilities can significantly improve the efficiency and speed of response to cyber threats, ensuring a higher level of security in the digital space.

An example of the use of AI in cybersecurity can be SIEM systems that integrate it into their structure to automate the analysis of BD and identify potential threats and anomalies in the network, ensuring effective response to cyber incidents and reducing response time.

A SIEM system is a comprehensive information and analytical infrastructure that combines software and hardware, network solutions, management methods and processes aimed at ensuring the security of information systems and is designed to collect, analyse, detect and respond to security events that occur in computer systems, networks and software applications.

SIEM systems widely use AI to solve cybersecurity management tasks, including detecting, analysing and responding to cyber threats. This helps to reduce false alarms and increase the effectiveness of information system protection in the current environment of ever-growing cyber threats.

As a result of the research conducted by the world's leading research and consulting company

Gartner, Inc., the Magic Quadrant for SIEM systems was created, which is the result of an analysis of the information technology security market. This quadrant (Figure 1) provides an objective view of the leaders in this field (Inci, 2023) and helps to select the best technological solutions.



Figure 1. The magic quadrant for SIEM

Based on this, a number of leading companies in this area are identified that should be considered when choosing SIEM systems, namely:

1. Splunk Enterprise Security
2. IBM Security QRadar
3. LogRhythm
4. Securonix
5. Micro Focus ArcSight
6. RSA NetWitness Platform
7. Exabeam
8. Elastic
9. SolarWinds Security Event Manager
10. AT&T Cybersecurity (AlienVault)

Figure 2 shows the interface of the IBM Security QRadar SIEM system, which includes an intuitive user interface for monitoring and analysing security events.

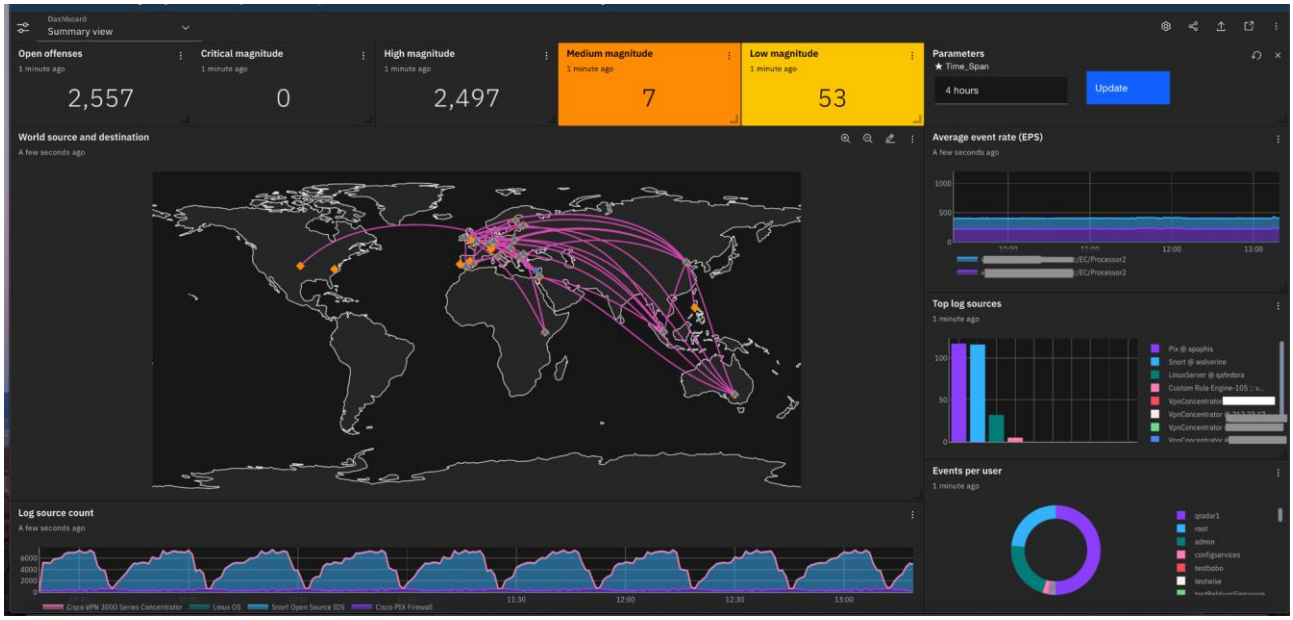


Figure 2. Interface of the IBM Security QRadar SIEM system

This interface provides operators with the ability to monitor data flows, detect anomalous activity, analyse vulnerabilities, and respond to potential threats in real-time. In addition, it can display reports and statistics on security measures, helping administrators make informed decisions about measures to improve the security of the information infrastructure.

Figure 3 shows the current and projected spending on SIEM systems by companies worldwide, illustrating the stable trend of increasing financial investments in this segment of cybersecurity, as well as the constant demand for such technological solutions.

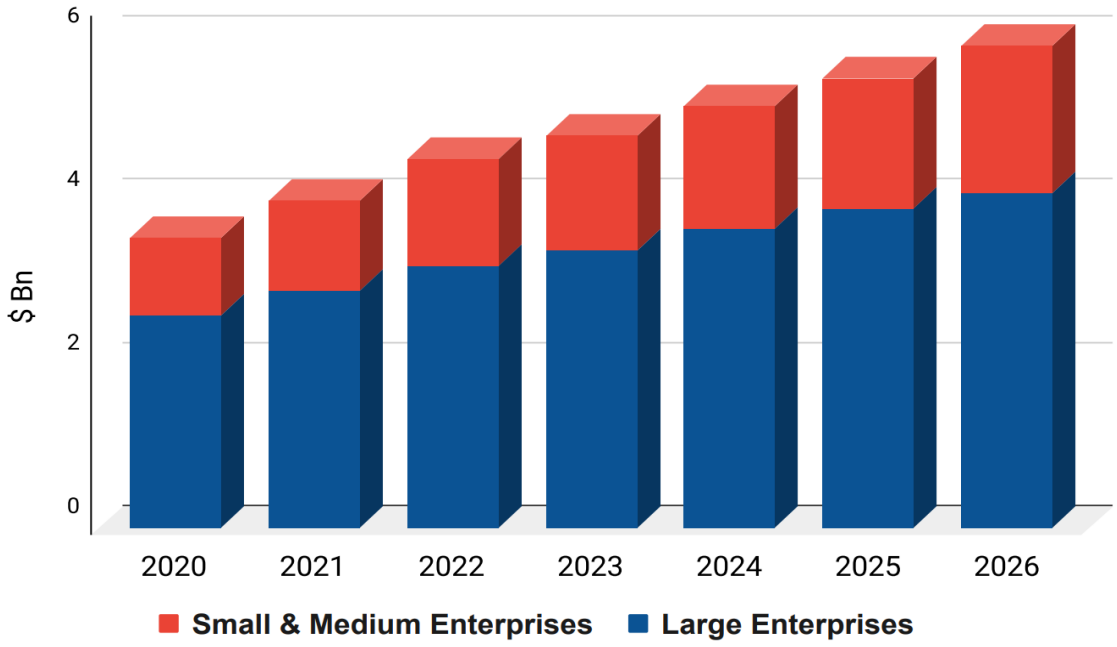


Figure 3. Existing and projected enterprise spending on SIEM from 2020 to 2026

Beyond these SIEM systems, there are other important cybersecurity tools that extend this approach to protection and use AI to improve the security of information systems. Their main difference is a focus on specific aspects of protection and advanced automation capabilities to improve the security of information systems. Among them are:

Security Orchestration, Automation, and Response (SOAR). This is a system that combines coordination, automation and response to events in the sphere of cybersecurity, which helps to increase the efficiency of threat response and optimise security processes.

Endpoint Detection and Response (EDR). This is a security system aimed at detecting and responding to threats at the level of endpoints in the network, such as computers, laptops, servers and other devices, by detecting and analysing anomalous activity.

User and Entity Behaviour Analytics (UEBA). This is a system used to analyse the behaviour of users and entities in information systems to detect anomalies in their activity to identify potential cyber threats.

These systems complement SIEM capabilities by expanding the range of tools for detecting, analysing and responding to cyber threats in various aspects of information security. They extend security management capabilities by providing additional functionality such as detecting anomalous network activity, automating routine processes, and using AI to detect complex threats. This combination of tools creates an effective and advanced security architecture that provides a high level of protection against cyberattacks in the modern cyberspace.

Having considered these systems, we can conclude that the use of AI is widely used and is a necessary component of modern technological solutions in the sphere of cybersecurity.

Despite the advantages of using AI in cybersecurity, its development is accompanied by a number of challenges and difficulties that we may potentially face in this area. Let us consider some of them.

Lack of accuracy can lead to underestimation or overestimation of threats, as well as an increase in false alarms, which affects the work of analysts and threatens the effectiveness of the system.

Uncertainty in threat behaviour makes it difficult to detect and counter cybercriminals, who are constantly developing new methods and techniques to circumvent defences.

The lack of access to relevant data can complicate training and reduce its effectiveness, while the increasing use of AI may lead to system dependence on its operation, thereby increasing their vulnerability to attacks.

Ethical and privacy issues, in particular in relation to the collection and processing of users' personal data, also need to be addressed and resolved.

When considering the role of AI in cybersecurity, it is important to note that it plays a dual role in the future of the industry. On the one hand, it undoubtedly contributes to the improvement of defence systems by providing more effective detection and prevention of attacks. On the other hand, the growing number of attacks using AI and issues related to confidentiality also pose serious challenges for cybersecurity. In this regard, all these aspects require careful analysis and development of appropriate strategies to address them in order to ensure effective and reliable security in cyberspace.

The prospects for development in the sphere of cybersecurity using AI are promising. With the development of technology and continuous improvement of its level, we can expect further development of more accurate and faster methods of detecting cyber threats, which will help increase the effectiveness of security systems.

One of the main prospects is the development of autonomous intelligent protection systems that can adapt to new types of threats and attacks without direct intervention from operators. Such systems will be able to respond faster and more effectively to changes in cyberspace and prevent

potential attacks.

Another perspective is to increase the integration of AI with other cybersecurity technologies, such as quantum computing and blockchain. This will create more comprehensive and reliable security systems that can effectively respond to current and future cybersecurity challenges.

In addition, the development of cybersecurity standards and regulations is an important prospect, which will stimulate innovation and ensure a high level of security in the Internet of Things (IoT), cloud services and other modern technological spheres.

The introduction of AI into the activities of the Armed Forces of Ukraine opens up prospects for increasing their readiness and efficiency in modern military conflicts. This innovative technology makes it possible to optimise the planning and conduct of military operations, ensuring the accuracy in making relevant decisions and instant response to sudden changes in the operational situation. Also, the use of AI contributes to strengthening the cybersecurity of the Armed Forces of Ukraine, protecting their critical information resources from cyberattacks and ensuring the stability of military communication systems. In addition, efficiency can be increased through the use of AI of cyber exercises and simulations to prepare the military for various crisis situations and cyber threats. Thus, the use of AI in the Armed Forces of Ukraine has the potential to increase their readiness and effectiveness in the modern military environment.

All in all, AI has the potential to transform the way we approach cybersecurity, providing more adaptive, intelligent and effective defence systems that can cope with the growing threats in the digital world.

Conclusion

The development of AI in the sphere of cybersecurity opens up significant potential for increasing the effectiveness of information protection in both the civilian and military sectors. Through the application of AI, cyber threats can be detected, analysed, and responded more quickly and effectively, ensuring a high level of protection against modern cyber attacks. The integration of AI into cybersecurity also increases the security and ability to respond to the challenges of the modern digital environment.

Therefore, the integration of AI in the sphere of cybersecurity opens up new opportunities to provide effective and comprehensive protection against cyber threats in the modern digital world, which is becoming a key factor in ensuring cybersecurity in the future.

Recommendations

Further research should be focused on enhancing the effectiveness of AI into cybersecurity for accurate detection and analysing of cyber threats, development of adaptive security systems, and exploration of forecasting capabilities for future threats and the development of prevention strategies.

Acknowledgments

The authors declare that they have no competing interests in the subject matter of the article.

References

1. Hryshchuk, R., Zhovnovatiuk, R., & Nosova, H. (2019). Hybrid threats in cyberspace: factors influencing the nature of emergence. *Modern Information Technologies in the Sphere of Security and Defence, 36(3)*, 53–58.
2. Kohut, Y. I. (2022). *Cyberwarfare, cyberterrorism, cybercrime (concepts, strategies, technologies)*. Sidcon Consulting Company.
3. Barabash, O. V., Hryshchuk, R. V., Molodetska-Grynchuk, K. V., & Molodetska-Grynchuk, K. V. (2018). *Identification of threats to the information security of the state in the content of*

textual content of social Internet services.
4. Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In *Countering cyber attacks and preserving the integrity and availability of critical systems* (pp. 170-192). IGI Global.
5. Onishchenko, Y. M., Kalancha, A. A., & Geldt, S. V. (2023). Application of artificial intelligence in the field of cybersecurity. In *The 8th International scientific and practical conference "Trends, theories and ways of improving science" (February 28–March 03, 2023) Madrid, Spain. International Science Group. 2023*. 565 p. (p. 544).
6. Gurzhiy, S. (2023). Features of the use of artificial intelligence in cybersecurity issues. *Information and Law*, 4 (47), 207–216.
7. Golubenko, O. I., Lemeshko, A. V., Polischuk, A. R., Kuzmenko, M. V. & Degtyarev, E. O. (2023). Research of the application of artificial intelligence in cybersecurity. *ITSynergy, (2)*, 71–81.
8. Ustymenko, V. O., & Olishevskyi, I. G. (2022). *Prospects for the application of artificial intelligence technologies in the field of cybersecurity*.
9. Opirskyi, I., Susukailo, V., & Vasylyshyn, S. (2023). Investigation of the possibilities of using artificial intelligence chatbots for the study of event logs. *Information Protection*, 24(4), 177–183.
10. Soldatova, M. O., Vityuk, A. E., Martyniuk, A. S., & Chernoborodyuk, V. D. (2022). In *The 9th International scientific and practical conference "Innovations and prospects of world science"* (April 28-30, 2022) Perfect Publishing, Vancouver, Canada. *2022*. April. P. 256.
11. Inci, S. (2023). The Best 10 SIEM Tools for 2023. *Medium*. 5 May. https://medium.com/@sedatinci1001/the-most-popular-10-siem-tools-b36f86d9fc7a
12. Yushko, A. V., & Shevchuk, R. P. (2020). *Analysis of information security event management systems*.

The Central Research institute
of the Armed Forces of Ukraine
Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.17

Вирішення задачі забезпечення справності парку авіаційної техніки Збройних Сил України в умовах особливого періоду

Михайло Сушак
кандидат технічних наук, старший науковий співробітник,
начальник науково-дослідного відділу
Державний науково-дослідний інститут авіації
01135, вулиця Григорія Андрющенка, 6в, Київ , Україна
e-mail: sushak_m@ukr.net
ORCID:0000-0001-7747-2303

Юрій Братусь
кандидат технічних наук
заступник начальника науково-дослідного відділу
Державний науково-дослідний інститут авіації
01135, вулиця Григорія Андрющенка, 6в, Київ , Україна
e-mail: 0673678791@ukr.net
ORCID:0009-0003-4947-9083

Микола Васянович
кандидат військових наук, старший дослідник
начальник центру
Центральний науково-дослідний інститут Збройних Сил України
03049, 28Б, просп. Повітрофлотський, Київ, Україна
e-mail: m.o.vasianovych@post.mil.gov.ua
ORCID: 0000-0002-8409-4774

Анотація. Технічний стан всього парку авіації Повітряних Сил Збройних Сил України характеризується вичерпанням установленого ресурсу (строку служби). Особливе значення для прогнозованого планування заходів інженерно-авіаційного забезпечення є аналіз післяремонтної надійності авіаційної техніки при виконанні заходів заводського ремонту. Аналіз діяльності авіа ремонтних підприємств України свідчить про існування низки проблемних питань, які негативно впливають на поточний стан авіаремонтної бази та перспективи розвитку. Характерні особливості існуючого стану більшості авіа ремонтних підприємств визначають доцільність формування управлінських рішень щодо заводського ремонту та технічної експлуатації авіаційної техніки державної авіації з позицій мінімізації потенційних ризиків. Програма технічного обслуговування та ремонту всіх типів літальних апаратів Повітряних Сил Збройних Сил України може розглядатись як сукупність програм більш низького рівня. Система забезпечення справності авіаційної техніки державної авіації є складною багатофакторною істотно нелінійною та нестаціонарною системою, тому одним із доцільних підходів щодо оцінки впливу ризикоутворювальних чинників на забезпечення заданого рівня справності парку авіаційної техніки є розгляд аналогій для системи адекватної складності. В якості такої системи можливо розглядати систему авіа ремонтних підприємств при виконанні заходів імпортозаміщення з відповідними ризиками. Авторами запропоновано алгоритм формування плану ремонту авіаційної техніки шляхом ітераційного процесу, при якому досягається мінімальний ризик забезпечення заданого рівня справності парку авіаційної

техніки державної авіації. Для кожного зі сценаріїв особливого періоду розглядається окремий варіант плану ремонту авіаційної техніки. Для зменшення ризику критичної залежності від одного приватного виробника необхідних для ремонту та експлуатації авіаційної техніки комплектувальних виробів, аналогічних штатним, доцільнім є розвиток державної системи економічного стимулювання (надання преференцій, державної підтримки) вітчизняних підприємств, що задіяні в процесі імпортозаміщення. Для цього, доцільним є ініціювання питання практичної реалізації державної підтримки вітчизняних підприємств, які задіяні в процесі імпортозаміщення в галузі державної авіації з виділенням на це відповідного фінансового ресурсу з Державного бюджету України. Таким чином, задача забезпечення справності парку авіаційної техніки Збройних Силах України в умовах особливого періоду з урахуванням реальних виробничих можливостей авіаремонтної галузі має вирішуватися шляхом мінімізації ризиків імпортозаміщення процесів заводського ремонту. Для теоретичного моделювання розподілу випадкових величин, які характеризують надійність, найбільш прийнятними є біноміальний та Пуассона – для дискретних величин; експоненціальний, Вейбулла та нормальний – для неперервних величин.

Ключові слова: інженерно-технічне забезпечення авіаційної техніки, забезпечення заданого рівня справності авіаційної техніки, мінімізація ризиків, забезпечення достатнього рівня надійності авіаційної техніки.

Вступ (Introduction)

Аналіз питання щодо забезпечення заданого рівня справності парку авіаційної техніки Повітряних Сил Збройних Сил України (далі – ПС ЗС України) в особливий період показує, що на озброєнні ПС ЗС України перебуває військова авіаційна техніка (далі – АТ) іноземної розробки та виробництва (окрім літаків розробником яких є державне підприємство “Антонов” та вертольотів Мі-8МСБВ, Мі-2МСБВ розробником яких є акціонерне товариство “Мотор Січ”), яка позбавлена авторського нагляду в процесі експлуатації.

Технічний стан всього парку авіації ПС ЗС України характеризується вичерпанням установленого ресурсу (строку служби). Відновлення справного стану АТ згідно з діючим методом експлуатації “за ресурсом” та експлуатації за технічним станом шляхом виконання контрольно-відновних робіт після багатоетапного продовження призначених ресурсних показників (кожен етап – на 3 місяці або на 50 годин) можливо виключно шляхом виконання капітально-відновлювальних ремонтів в умовах авіаремонтних підприємств (далі – АРП) із встановленням міжремонтних показників з відповідним продовженням призначеного строку служби. Тому особливе значення для прогнозованого планування заходів інженерно-авіаційного забезпечення є аналіз післяремонтної надійності АТ при виконанні заходів заводського ремонту, де мають бути досліджені та відповідно оцінені ризики реалізації цих заходів.

Аналіз діяльності АРП України свідчить про існування низки проблемних питань, які негативно впливають на поточний стан авіаремонтної бази та перспективи розвитку, що потребує невідкладного вжиття відповідних заходів. При цьому, характерними особливостями існуючого стану більшості АРП є:

фактичне вичерпання попередніх напрацювань, технологічних можливостей і виробничого потенціалу більшості підприємств для налагодження виготовлення запасних частин, комплектувальних виробів;

потреба в значних капіталовкладеннях для реалізації імпортозаміщення процесів заводського ремонту зразків військової АТ;

великі часові терміни освоєння нових виробництв та ремонтних робіт;

практична відсутність у підприємств досвіду, необхідного обладнання, підготовленого персоналу, конструкторської (технологічної) документації для виготовлення нової номенклатури запасних частин до АТ;

дрібносерійне й тому нерентабельне виробництво;

відсутність конкуренції, об'єктивне звуження кола підприємств, що мають необхідні ресурси для освоєння нових виробництв (ремонтних робіт) та підтримання їх на належному рівні якості (Сушак, Борохвостов, Рябець, 2019), (Reliability Engineering and Risk Analysis, 2016), (Міщенко, Сушак, Василенко, 2020), (Сушак, Грицюк, 2022).

Зазначені особливості визначають доцільність формування управлінських рішень щодо заводського ремонту та технічної експлуатації авіаційної техніки державної авіації з позицій мінімізації потенційних ризиків. При цьому необхідно враховувати наступні умови:

нагальна потреба у відновленні та створенні перспективних виробничих потужностей для забезпечення заданого рівня справності парку АТ з урахуванням розвитку можливих сценаріїв особливого періоду;

невідкладність створення нових кооперацийних зв'язків і каналів постачання матеріалів, вузлів і комплектуючих як всередині країни, так і ззовні (диверсифікація), для забезпечення ремонту та відновлення АТ, яка перебуває на озброєнні ЗС України, вирішення проблеми імпортозаміщення;

необхідність організації раніше нетрадиційного для України виду військово-технічного співробітництва з іноземними державами – імпорту вузлів і комплектуючих (запасних частин) в умовах відсутності сталих каналів постачання та політичних обмежень з боку низки країн Європейського Союзу та інших країн щодо продажу (надання матеріально-технічної допомоги) Україні необхідних товарів;

невідповідність нормативно-правової бази, що врегульовує порядок ввезення, легалізації вузлів і комплектуючих (запасних частин), отриманих за імпортом та створеного в умовах особливого періоду, невідкладним потребам оборони держави, що потребує внесення відповідних змін до законодавства в частині спрощення процедур закупівлі (постачання).

Методологічна основа (Methodological Framework)

Вирішення проблеми забезпечення справності парку АТ ЗС України в умовах особливого періоду з урахуванням реальних виробничих можливостей авіаремонтної галузі. Розробка та обґрунтування рекомендацій щодо мінімізації ризиків імпортозаміщення процесів заводського ремонту військової АТ.

В умовах сьогодення прийняття рішення з питань збільшення ресурсу, продовження строку служби авіаційної техніки державної авіації, за якою не здійснюється авторський нагляд, та яку в особливий період дозволено експлуатувати без сертифікатів льотної придатності, здійснюється командувачами видів Збройних Сил України, керівниками авіації інших центральних органів виконавчої влади за її належністю.

Пунктом 2 статті 7 Повітряного кодексу України встановлено, якщо розробник, виробник не виконує своїх обов'язків із супроводження експлуатації виробів АТ, компонентів та обладнання, підтримання їх льотної придатності, Міністерство оборони України вживає необхідних заходів для забезпечення безпеки польотів та підтримання льотної придатності державних повітряних суден згідно вимог нормативних документів, які регламентують порядок підтримання льотної придатності АТ державної авіації за якою не здійснюється авторський нагляд.

Програма технічного обслуговування та ремонту всіх типів ЛА ПС ЗС України може розглядатись як сукупність програм більш низького рівня. В залежності від методів технічного обслуговування та ремонту, що використовуються, розрізняються наступні програми

технічного обслуговування та ремонту: за наробітком, за технічним станом із контролем параметрів (з контролем рівня надійності).

За ознаками режимів технічного обслуговування та ремонту (об'єм та періодичність виконаних робіт), які використовуються, програми технічного обслуговування та ремонту розрізняються за оперативною, періодичною та ремонтною формами. З урахуванням конструктивних особливостей складових частин ЛА слід розрізняти програми технічного обслуговування та ремонту: планеру, авіадвигунів, функціональних систем (гідравлічна, паливна, керування та інші). Програма технічного обслуговування та ремонтна документація на кожний тип АТ були сформовані розробниками/виробниками ще на етапі проектуванні ЛА у відповідності з технічними вимогами (Risk Theory, 2022).

На практиці забезпечення справності парку авіаційної техніки ПС ЗС України з урахуванням об'єктивних можливостей авіаційно-ремонтних підприємств щодо гарантійного обслуговування зразків АТ, які експлуатуються за межами попередньо встановлених ресурсних показників невід'ємно залежить від фінансового ресурсу, який фактично виділяється на це.

Проблемним питанням діяльності підприємств вітчизняної авіаремонтної галузі, яке не дозволило на сьогодні забезпечити існуючі потреби ЗС України у справних зразках АТ є те, що окремі договори (контракти) про надання послуг з ремонту зразків АТ укладаються з приватними підприємствами, які мають недостатні виробничі спроможності. Так, до виконання оборонних замовлень все частіше залучаються невеликі приватні компанії, які не завжди здатні забезпечити в короткі терміни належну якість робіт і подальше гарантоване технічне супроводження відремонтованої АТ у міжремонтний період.

Система забезпечення справності АТ державної авіації є складною багатофакторною істотно нелінійною та нестаціонарною системою, тому одним із доцільних підходів щодо оцінки впливу ризикоутворювальних чинників на забезпечення заданого рівня справності парку АТ є розгляд аналогій для системи адекватної складності (Aircraft Reliability and Reliability Centred Maintenance, 2021), (Risk Theory, 2017), (Barlov, Hunter, 1960).

В якості такої системи можливо розглядати систему АРП при виконанні заходів імпортозаміщення з відповідними ризиками. На теперішній час, найбільш вагомими перепонами з реалізації заходів імпортозаміщення процесів заводського ремонту АТ державної авіації, за якою не здійснюється авторський нагляд, є ризики:

неосвоєння в рамках імпортозаміщення нових (зазвичай високотехнологічних) виробництв та ремонтних робіт (наприклад виробництво (ремонт) лопатей несучого та рульового гвинта до військових вертольотів), комплектуючих деталей основних стійок шасі літаків типу Су-27, козирка кабіни льотчика літака типу МиГ-29 інше;

незабезпечення необхідної якості виготовлення директивних запасних частин й комплектувальних виробів (ремонту) (наприклад виготовлення підшипників до авіаційних двигунів, редукторів, робочих лопаток, дисків турбін, плунжерних пар паливних насосів до авіаційних двигунів, силових елементів основних стійок шасі інше);

критичної залежності від одного виробника (часто приватного) (постачання гальмівних дисків коліс, трубопроводів, шлангів високого тиску, клеїв, герметиків, гумових сумішей інше);

неефективного використання державних коштів на реалізацію заходів імпортозаміщення.

Зазначені ризики є прямими аналогами ризиків забезпечення справності АТ при капітально-відновлювальному ремонті, тому, масштаб та наслідки їх впливу розглядається як "орієнтир" для оцінки можливого масштабу впливу та наслідків щодо системи заводського ремонту АТ в цілому.

Ризик зриву освоєння в рамках імпортозаміщення нових виробництв та ремонтних робіт ґрунтується на існуванні високого рівня ймовірності недосягнення встановлених цілей запланованих заходів імпортозаміщення. Джерелом виникнення даного ризику є невідповідність інтересів замовника освоєння та підприємства-виконавця і обмежена можливість економічного стимулювання виконавця з боку замовника, яка обмежена виключно умовами укладеного договору (контракту) (Сушак, Борохвостов, Рябець, 2019), (Reliability Engineering and Risk Analysis, 2016).

Для кількісного оцінювання ризику існують різні методи, серед яких найпоширенішими є: статистичний (у тому числі, метод статистичних випробувань і метод Монте-Карло); аналітичний; поєднання дерева рішень та імовірнісного підходу; оцінювання фінансової стійкості або оцінювання доцільності витрат; експертних оцінок; нормативний; аналізу чутливості; використання аналогів тощо. Кожний з цих методів має переваги та недоліки і використовується у конкретних ситуаціях, а універсального методу, прийнятного для всіх випадків, в тому числі, і при оцінці ризиків реалізації заходів планування процесів заводського ремонту та технічної експлуатації АТ, не існує (Asif Mostafa, 2020), (Safety and Risk Assessment of Civil Aircraft during Operation, 2020).

Результати і обговорення (Results and Discussions)

Алгоритм формування плану ремонту АТ шляхом ітераційного процесу, при якому досягається мінімальний ризик забезпечення заданого рівня справності парку АТ державної авіації наведено на рисунку нижче. Для кожного зі сценаріїв особливого періоду розглядається окремий варіант плану ремонту АТ.

Закони розподілу відмов є випадковими величинами, та мають велике значення для теорії і практики робіт щодо забезпечення надійності виробів АТ. Знання цих законів дозволяє розраховувати та прогнозувати надійність виробів, особливо велике значення ці закони мають при оцінці правильності встановлення та продовження ресурсу зразків АТ (Іленко, Сушак, Стешенко, 2018), (Смирнов, Ицкович, Загребельный, 1972), (Масягін, Сушак, Бездєльний, 2021), (Смирнов, Ицкович, Чинючин, 1978), (Сушак, Грень, Клобукова, Чернозубкін, 2021), (Митчелл, 2002), (Rausand, Хойланд, 2004), (Modarres, Каминский, Кривцов, 2010).

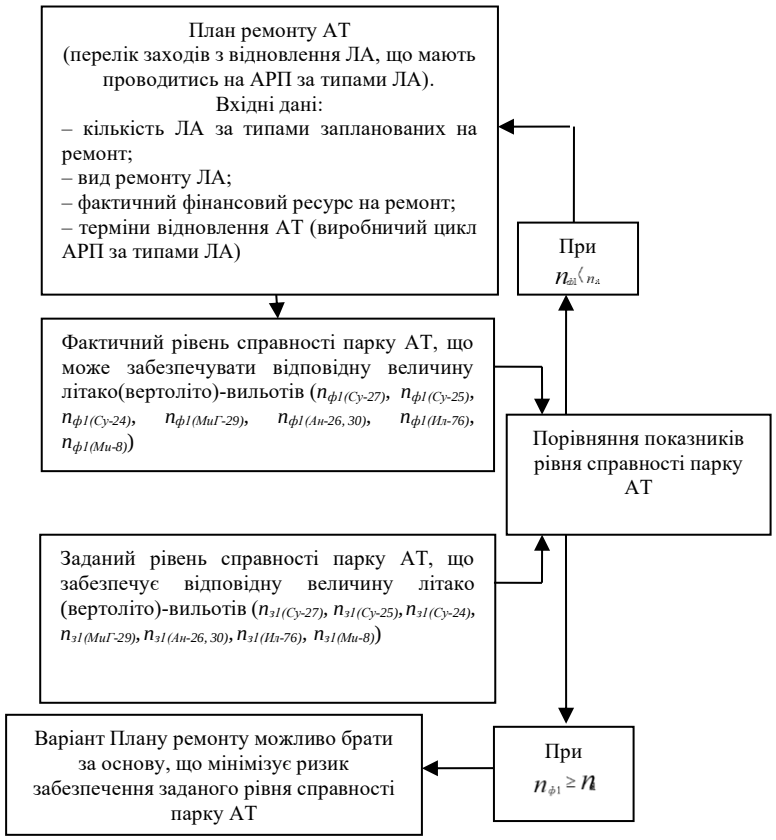
При використанні методу технічного обслуговування та ремонту за ресурсом задача забезпечення безпеки польотів (заданого рівня справності АТ) вирішується призначенням “безпечного” ресурсу виробу. При використанні метода технічного обслуговування та ремонту з контролем параметрів, задача забезпечення безпеки польотів вирішується шляхом визначення випереджувальних допусків та періодичності контролю технічного стану виробу, що забезпечує з заданою ймовірністю виявлення його передвідмовного стану. Метод технічного обслуговування та ремонту з контролем рівня надійності передбачає “безпечну” відмову виробу АТ. За характером прояву відмови елементів функціональної системи ЛА розподіляються на поступові та раптові. З великої кількості різноманіття законів розподілу випадкових величин, розроблених в теорії ймовірностей, найбільше значення для надійності мають біноміальний та Пуассона – для дискретних величин; експоненціальний, Вейбулла та нормальний – для неперервних величин (Risk Theory, 2022), (Aircraft Reliability and Reliability Centred Maintenance, 2021).

Для розрахунку експоненційного розподілу використовуються наступні формули:

$$f_i(t) = \frac{1}{T} e^{\frac{-t_{i+1}}{T}}; \quad (1)$$

$$\lambda_i(t) = \frac{1}{T}; \quad (2)$$

$$q_i(t) = \int_{t_i}^{t_{i+1}} \frac{1}{T} e^{\frac{-t_{i+1}}{T}}. \quad (3)$$



де $n_{ф1}$ – фактична кількість справних ЛА за типами;
$n_{ф1}$ – задана кількість справних ЛА за типами.

Рисунок 1. Алгоритм формування плану ремонту АТ, за якого досягається мінімальний ризик забезпечення заданого рівня справності парку державної авіації для кожного з можливих сценаріїв особливого періоду

Для розподілу Вейбулла:

$$f_i(t) = \frac{m}{t_0} t_i^{m+1} e^{\frac{-t^m}{t}}; \quad (4)$$

$$\lambda_i(t) = \frac{m}{t_0} t_i^{m-1}; \quad (5)$$

$$q_i(t) = \int_{t_i}^{t_{i+1}} \frac{m}{t_0} t_i^{m-1} e^{\frac{-t^m}{t}}. \quad (6)$$

Визначаючись із математичною моделлю визначення ймовірнісних властивостей процесу гарантійного обслуговування зразків АТ, які експлуатуються за межами попередньо встановлених ресурсних показників, слід мати на увазі, що експоненційний закон доцільно використовувати тільки стосовно виробів АТ, які не підлягають старінню або зношенню під час роботи, або у яких цей процес проходить дуже повільно. Цей закон, в основному, використовується для розподілу раптових відмов, які випадковим чином виникають при експлуатації АТ в міжремонтний період. Він розповсюджується тільки на позитивні безперервні випадкові величини.

Слід також враховувати, що експоненційний розподіл – це єдиний розподіл випадкових величин, де використовується припущення, що, якщо пристрій має експоненційний розподіл

часу до відмови, то попереднє використання пристрою ніяким чином не впливає на послідуючий час його роботи. Тобто, якщо пристрій ще не відмовив до моменту часу *t*, то розподіл його часу безвідмовної роботи буде таким же, нібито в цей момент часу почав використовуватись абсолютно новий пристрій. Це, безумовно, протирічить багатьом природнім уявленням. Експоненційний розподіл є єдиним розподілом, який має подібну властивість (Барлоу, Прошан, 1969), (Feller, 1957). Для прикладу використання експоненційного розподілу уявимо, що процес, який досліджується має пікові викиди, та що саме ці пікові зміни зовнішніх умов можуть впливати на пристрій, що розглядається, тобто пристрій може відмовити лише в момент указаного пікового викиду. Якщо потік викидів є пуассонівським, то розподіл відмов даного пристрою є експоненційним, і в цих умовах дійсно попереднє використання пристрою не відобразиться на подальшій тривалості безвідмовної роботи.

Однак зрозуміло, що зазначена властивість експоненційного розподілу не дозволяє використовувати цей розподіл для описання пристроїв, які в процесі нормальної експлуатації знаходяться під впливом факторів, які негативним чином відображаються на тривалості їх безвідмовної роботи.

Виключенням з цього правила є складні системи, елементи яких відновлюються в процесі функціонування. Для таких систем розподіл часу між відмовами може бути прийнято наближено експоненційним. У (Dais, 1952) розподіл Вейбулла (Weibull, 1939) характеризує зростаюча інтенсивність відмов при $m>1$, де m – змінний параметр, що має різні значення для окремих типів виробів (підбирається за результатом обробки експериментальних даних). Цей розподіл названо асиметричним розподілом третього типу для екстремальних значень (14). Розподіл Вейбулла (Weibull, 1939) доцільно використовувати для описання втомлювальних відмов, відмов вакуумних приладів (сильфонних вузлів агрегатів систем літаків, чутливих елементів агрегатів паливної автоматики авіаційних двигунів) та підшипників (Сушак, Грень, Клобукова, Чернозубкін, 2021), (Митчелл, 2002), (Rausand, Хойланд, 2004).

Для безперервної випадкової величини (час напрацювання) t щільність розподілу за Вейбуллом виражається формулою

$$f(t) = \frac{m}{t_0} t^{m-1} e^{-\frac{t_m}{t_0}}, \quad (7)$$

де m – змінній параметр, який має різні значення для окремих типів виробів (підбирається в результаті обробки експериментальних даних). Принаймні, якщо $m=1$, маємо експоненційний розподіл: при $m<1$ зі зростанням t величина $\lambda(t)$ зменшується; при $m>1$ зі зростанням t величина $\lambda(t)$ збільшується; t_0 – параметр, що зв'язаний з середнім напрацюванням до відмови рівнянням:

$$t_{\text{ср}} = b_m t_0^{\frac{1}{m}} \text{ або } t_0 = \left(\frac{t_{\text{ср}}}{b_m}\right)^m, \quad (8)$$

де b_m=Г(1+$\frac{1}{m}$) – гамма-функція.

Гамма–функція від аргументу m є функція:

$$\Gamma(m) = \int_0^\infty x^{m-1} e^{-x} dx \quad (9)$$

Основною особливістю нормального розподілу (нормальний закон розподілу Гаусса) є те, що він є граничним розподілом, до якого наближаються інші закони розподілу (Gumbel, 1958).

Сума достатньо великого числа незалежних випадкових величин, що характеризуються різними законами розподілу, наближено підпорядковуються нормальному закону розподілу, причому тим точніше, чим більша кількість випадкових величин підсумовується.

Основне обмеження, що накладається на підсумовування випадкових величин, полягає в тому, щоб всі величини в загальній сумі мали відносно мале значення (до таких випадкових величин відносяться, наприклад, похибки вимірювань, помилки методичного порядку тощо). Якщо ця умова не виконується, та одне з випадкових значень різко перевищує в сумі від всіх інших, то це впливає на суму та визначає, в основному, її закон розподілу.

На відміну від експоненційного розподілу та розподілу Вейбулла, що використовуються тільки для позитивних безперервних випадкових величин, нормальний розподіл може використовуватись для безперервних випадкових величин, які можуть приймати як позитивні, так і негативні значення від $-\infty$ до $+\infty$.

Щільність нормального розподілу визначається формулою:

$$f(x) = \frac{1}{\sigma_x\sqrt{2\pi}} e^{-\frac{(x-m_x)^2}{2\sigma_x^2}} \quad (10)$$

Враховуючи те, що зразки авіаційної техніки є складними виробами (агрегатами), що включають в себе різноманітні складові елементи, методичною основою визначення імовірнісних властивостей процесу їх гарантійного обслуговування є поєднання (композиція) різних розподілів, які притаманні окремим елементам цих зразків авіаційної техніки (Weibull, 1939), (Kao, 1958), (Leiblein, Zelen, 1956).

Моделювання процесу визначення імовірнісних властивостей гарантійного обслуговування зразків авіаційної техніки державної авіації України, які експлуатуються за межами попередньо встановлених ресурсних показників дозволяє теоретично визначити основні кількісні показники надійності цих зразків після їх ремонту.

Використання запропонованих математичних моделей та методики визначення імовірнісних властивостей процесу гарантійного обслуговування зразків авіаційної техніки державної авіації України, які експлуатуються за межами попередньо встановлених ресурсних показників, дають можливість в певній мірі уникнути відмов, які не пов’язані з проведенням ремонту на авіаційно-ремонтному підприємстві, а є наслідком конструктивних недоліків, та/або тривалого терміну експлуатації.

Для практичної реалізації заходів щодо забезпечення справності парку авіаційної техніки Повітряних Сил Збройних Сил України, згідно з розробленим в роботі алгоритмом процесу гарантійного обслуговування відремонтованих зразків авіаційної техніки, які експлуатуються за межами попередньо встановлених ресурсних показників, мають здійснюватися наступні заходи:

усунення недоліків, виявлених під час гарантійного обслуговування авіаційно-ремонтним підприємством відповідно до умов договору (контракту) на ремонт;

внесення змін та доповнень до ремонтної документації авіаційно-ремонтного підприємством, що передбачає заміну (ремонт) вузлів та деталей виробу авіаційної техніки, які відмовили, та врахування цього в специфікації послуг послідуючих договорів на ремонт однотипних зразків авіаційної техніки;

внесення змін до діючої нормативно-правової бази гарантійного обслуговування відремонтованих зразків авіаційної техніки, які експлуатуються за межами попередньо встановлених ресурсних показників.

Висновки (Conclusion)

Для зменшення ризику критичної залежності від одного приватного виробника необхідних для ремонту та експлуатації АТ комплектувальних виробів, аналогічних штатним,

доцільнім є розвиток державної системи економічного стимулювання (надання преференцій, державної підтримки) вітчизняних підприємств, що задіяні в процесі імпортозаміщення. Для цього, доцільним є ініціювання питання практичної реалізації державної підтримки вітчизняних підприємств, які задіяні в процесі імпортозаміщення в галузі державної авіації з виділенням на це відповідного фінансового ресурсу з Державного бюджету України.

Таким чином, задача забезпечення справності парку АТ ЗС України в умовах особливого періоду з урахуванням реальних виробничих можливостей авіаремонтної галузі має вирішуватися шляхом мінімізації ризиків імпортозаміщення процесів заводського ремонту. Для теоретичного моделювання розподілу випадкових величин, які характеризують надійність, найбільш прийнятними є біноміальний та Пуассона – для дискретних величин; експоненціальний, Вейбулла та нормальний – для неперервних величин.

Рекомендації (Recommendations)

Матеріали публікації становитимуть інтерес для фахівців експлуатуючих частин, яким необхідно проводити постійний моніторинг процесів забезпечення достатнього рівня післяремонтної надійності кожного типу АТ для своєчасного виявлення слабких місць та для оперативної підготовки (спільно з підприємствами) відповідних заходів щодо ефективного усунення недоліків та їх запобігання.

Посилання

1. Сушак, М. Б., Борохвостов, В. К., Рябець, О. М. (2019) Оцінка ефективності та проблемні фінансові, економічні та виробничо-технологічні питання впровадження на підприємствах України імпортозаміщення під час заводського ремонту авіаційної техніки. *Зб. наук. пр. ЦНДІ ОВТ ЗС України*. № 2 (73). С. 71–79.
2. Reliability Engineering and Risk Analysis (2016) A Practical Guide, 3rd Edition. Modarres, M., Kaminskiy, M. P., Krivtsov, V. Maryland. CRC Press. 522 p.
3. Міщенко, В. Б., Сушак, М. Б., Василенко, О. А. (2020) Проблемні питання матеріального забезпечення заходів бойової підготовки у військових частинах та шляхи їх вирішення. *Актуальні проблеми застосування ЗС України, управління ними, їх оперативного та логістичного забезпечення*. Зб. мат. наук.-практич. конф., 4 листопада 2020 року. Київ. ЦНДІ ЗС України. С. 164–168.
4. Сушак, М. Б., Грицюк, Ю. Д. (2022) Аналіз технічних аспектів проблем якості ремонту військової авіаційної техніки. *Проблеми якості оборонної продукції: організаційні, технічні а фінансово-економічні аспекти*. Тези доповідей IV Всеукраїнської наук.-практич. конф., 30 червня 2022 року. Київ. НУОУ ім. Івана Черняховського. С. 150–163.
5. Risk Theory (2022) (Rational Decision in the Face of Chance, Uncertainty, and Risk) Rescher Nicholas. 1st Edition. SpringerBriefs. 80 p.
6. Aircraft Reliability and Reliability Centred Maintenance (2021) A Practical Guide for Aircraft Reliability Engineers Daniel Olufisan. 226 p.
7. Risk Theory (2017): A Heavy Tail Approach. Konstantinides, D. G. 508 p.
8. Barlov, R. E., Hunter, L. C. (1960) Mathematical models for system reliability. The Sylvania Technologist, v. XIII, № 1, 2.
9. Asif, M. (2020). Safety and Risk Assessment of Civil Aircraft during Operation. Open access peer-reviewed edited volume. Academic Published 23 December 2020. 210 p. DOI 10.5772/intechopen.90993. PRINT ISBN 978-1-78984-792-5.
10. Safety and Risk Assessment of Civil Aircraft during Operation (2020) Longbiao, Li. IntechOpen, 210 p.

11. Іленко, Є. Ю, Сушак, М. Б., Стешенко, П. М. (2018) Визначення міжремонтного ресурсу авіаційних двигунів в процесі імпортозаміщення комплектуючих виробів. *Зб. наук. пр. Харківського університету Повітряних Сил ім. Івана Кожедуба.* № 4 (56). С. 00–000.
12. Смирнов, Н. И., Ицкович, А. А., Загребельный, В. И. (1972) О применении технической диагностики для определения сроков замены самолётных агрегатов. Москва. Наука. С. 69–73. (Тр. 1-го Всесоюзного совещания).
13. Масягін, В. І., Сушак, М. Б., Бездєльний, В. В. (2021) Визначення ймовірних властивостей процессу гарантійного обслуговування зразків авіаційної техніки, які експлуатуютьс за межами попередньо встановлених ресурсних показників. *Зб. наук. праць Національного університету "Полтавська політехніка ім. Юрія Кондратюка"*. № 2 (64). С. 21–26.
14. Смирнов, Н.И., Ицкович, А.А., Чинючин, Ю.М. (1978) Иерархическая структура показателей эффективности процесса эксплуатации летательных аппаратов. *Техническое обслуживание и ремонт авиационной техники*. Москва. ЦНТИ ГА. Вып. 2. С. 1–7.
15. Сушак, М. Б., Грень, В. М., Клобукова, Н. В., Чернозубкін, І. О. (2021) Методичний підхід щодо визначення основних показників надійності зразків авіаційної техніки в міжремонтний період експлуатації. *Зб. наук. праць ДНДІА*. № 17 (24). С. 80–88.
16. Митчелл, М. Дж. (2002). "Приблизительное среднее время наработки на отказ при периодическом обслуживании системы". (PDF). *Транзакции IEEE о надёжности. Июнь 2002 г. № 51 (2). С. 166–167.* DOI 10.1109 / TR.2002.1011521.
17. Rausand, M., Хойланд, А. (2004). Теория надёжности системы. Модели, статистические методы и приложения. Нью-Йорк: Джон Вили и сыновья. ISBN 047147133X.
18. Modarres, M., Каминский, М., Кривцов, В. (2010). Разработка надёжности и анализ рисков. Практическое руководство (2-е изд.). ISBN 9780849392474.
19. Барлоу, Р., Прошан, Ф. (1969) Математическая теория надежности. Пер. с англ. под ред. Гнеденко, Б. В. Москва. Сов. радио. 488 с.
20. Feller, W. (1957) An Introduction to Probability Theory and Its Applications, v.1, 2 nd ed., John Wiley and Sons, New York.
21. Dais, D. J. (1952) An Analysis of failure data, J. Amer. Statist. Assoc., v. 47, № 258, p. 113–150.
22. Gumbel, E. J. (1958) Statistics of Extremes, Columbia University Press, New York.
23. Weibull, W. (1939) A statistical theory of the strength of materials. Ing. Vetenskaps Akad. Handl, №151.
24. Kao, J. H. K. (1958) Computer methods for estimating Weibull parameters in reliability studies, IRE Transactions on Reliability and Quality Control, PGRQC-13, p. 15–22.
25. Leiblein, J., Zelen, M. (1956) Statistical investigation of the fatigue life of deep-groove ball bearings, Res, J., Nat. Bureau Stand., v. 57, p. 273–316.

References

1. Sushak, M. B., Borokhvostov, V. K., Ryabets, O. M. (2019) Evaluation of efficiency and problematic financial, economic and production-technological issues of the introduction of import substitution at Ukrainian enterprises during the factory repair of aviation equipment. Coll., *Sci., etc., Central Research Institute of Weapons and Military Equipment of the Armed Forces of Ukraine.* № 2 (73). Pp. 71–79.
2. Reliability Engineering and Risk Analysis (2016) A Practical Guide, 3rd Edition.Modarres, M., Kaminskiy, M. P., Krivtsov, V. Maryland. CRC Press. 522 p.
3. Mishchenko, V. B., Sushak, M. B., Vasylenko, O. A. (2020) Problematic issues of material support of combat training activities in military units and ways to solve them. *Actual problems of the use of the Armed Forces of Ukraine, their management, their operational and logistical*

support. Coll. Math. Scientific and Practical Conf., November 4, 2020. Kyiv. Central Research Institute of the Armed Forces of Ukraine. pp. 164–168.

4. Sushak, M. B., Hrytsiuk, Y. D. (2022) Analysis of technical aspects of quality problems of repair of military aviation equipment. *Problems of quality of defense products: organizational, technical, financial and economic aspects*. Abstracts of reports of the I V All-Ukrainian Scientific and Practical Conference. conf., June 30, 2022. Kyiv. NUOU them. Ivan Chernyakhovskyi. pp. 150–163.
5. Risk Theory (2022) (Rational Decision in the Face of Chance, Uncertainty, and Risk) Rescher Nicholas. 1st Edition. SpringerBriefs. 80 p.
6. Aircraft Reliability and Reliability Centred Maintenance (2021) A Practical Guide for Aircraft Reliability Engineers Daniel Olufisan. 226 p.
7. Risk Theory (2017): A Heavy Tail Approach. Konstantinides, D. G. 508 p.
8. Barlov, R. E., Hunter, L. C. (1960) Mathematical models for system reliability. The Sylvania Technologist, v. XIII, № 1, 2.
9. Asif, M. (2020). Safety and Risk Assessment of Civil Aircraft during Operation. Open access peer-reviewed edited volume. Academic Published 23 December 2020. 210 p. DOI 10.5772/intechopen.90993. PRINT ISBN 978-1-78984-792-5.
10. Safety and Risk Assessment of Civil Aircraft during Operation (2020) Longbiao, Li. IntechOpen, 210 p.
11. Ilenko, E. Y., Sushak, M. B., Steshenko, P. M. (2018) Determination of the overhaul life of aircraft engines in the process of import substitution of components. *Coll., Sci., pr., Kharkiv University of the Air Force. Ivan Kozhedub.* No 4 (56). P. 00–000.
12. Smirnov, N. I., Itskovich, A. A., Zagrebelny, V. I. (1972) On the use of technical diagnostics to determine the timing of the replacement of aircraft units. Moscow. Science. pp. 69–73. (Tr. of the 1st All-Union Conference).
13. Masyagin, V. I., Sushak, M. B., Bezdelnyi, V. V. (2021) Determination of the probable properties of the warranty service process for aircraft samples operated beyond the pre-established resource indicators. Coll. of *Sciences, Proceedings of the National University "Poltava Polytechnic. Yuri Kondratyuk".* No 2 (64). pp. 21–26.
14. Smirnov, N.I., Itskovich, A.A., Chinyuchin, Y.M. (1978) Hierarchical structure of performance indicators of the process of operation of aircraft. *Maintenance and repair* of aviation equipment. Moscow. CSTI CA. Vyp. 2, pp. 1–7.
15. Sushak, M. B., Gren, V. M., Klobukova, N. V., Chernozubkin, I. O. (2021) Methodical approach to determining the main indicators of reliability of aircraft samples in the overhaul period of operation. Coll. of *Sci. Proceedings of the State Research Institute of Historical Research.* № 17 (24). pp. 80–88.
16. Mitchell, M. J. S. Miller, Es (2002). "Approximate Mean Time Between Failures of Periodic System Maintenance". (PDF). *IEEE* Transactions *on Reliability. June 2002 No. 51 (2). pp. 166–167.* DOI 10.1109 / TR.2002.1011521.
17. Rausand, M., XOyland, A. (2004). System Reliability Theory. Models, statistical methods, and applications. New York: John Wiley & Sons. ISBN 047147133X.
18. Modarres, M., Kaminsky, M., Krivtsov, V. (2010). Reliability development and risk analysis. A Practical Guide (2nd ed.). ISBN 9780849392474.
19. Barlow, R., Proshan, F. (1969) Mathematical Theory of Reliability. Lane. Ed. by Gnedenko, B. V. Moscow. Sov. radio. 488 p. (in Russian).
20. Feller, W. (1957) An Introduction to Probability Theory and Its Applications, v.1, 2 nd ed., John Wiley and Sons, New York.
21. Dais, D. J. (1952) An Analysis of failure data, J. Amer. Statist. Assoc., v. 47, № 258, p. 113–150.

22. Gumbel, E. J. (1958) Statistics of Extremes, Columbia University Press, New York.
23. Weibull, W. (1939) A statistical theory of the strength of materials. Ing. Vetenskaps Akad. Handl, №151.
24. Kao, J. H. K. (1958) Computer methods for estimating Weibull parameters in reliability studies, IRE Transactions on Reliability and Quality Control, PGRQC-13, p. 15–22.
25. Leiblein, J., Zelen, M. (1956) Statistical investigation of the fatigue life of deep-groove ball bearings, Res, J., Nat. Bureau Stand., v. 57, p. 273–316.

Solving the problem of ensuring the serviceability of the fleet of aviation equipment of the Armed Forces of Ukraine in the conditions of a special period

Myhailo Sushak
Candidate of Technical Sciences, Senior Researcher
Head of R&D Department
State Research Institute of Aviation
01135, Hryhoriya Andryushchenko Street, 6v, Kyiv, Ukraine
e-mail: sushak_m@ukr.net
ORCID: 0000-0001-7747-2303

Yuriy Bratus
Candidate of Technical Sciences
Deputy Head of the Research Department
State Research Institute of Aviation
01135, Hryhoriya Andryushchenko Street, 6v, Kyiv, Ukraine
e-mail: 0673678791@ukr.net
ORCID:0009-0003-4947-9083

Mykola Vasianovych
candidate of military sciences, senior researcher
head of the center
Central Research Institute of the Armed Forces of Ukraine
03049, 28B, ave. Povitroflotskyi, Kyiv, Ukraine
e-mail: m.o.vasianovych@post.mil.gov.ua
ORCID: 0000-0002-8409-4774

Abstract. The technical condition of the entire aviation fleet of the Air Force of the Armed Forces of Ukraine is characterized by the exhaustion of the established resource (service life). Of particular importance for the predictive planning of engineering and aviation support measures is the analysis of the post-repair reliability of aircraft during the implementation of factory repair measures. Analysis of the activities of aircraft repair enterprises Ukraine testifies to the existence of a number of problematic issues that negatively affect the current state of the aircraft repair base and development prospects. The characteristic features of the current state of the majority of aircraft repair enterprises determine the expediency of forming management decisions on the factory repair and technical operation of aviation equipment of state aviation from the standpoint of minimizing potential risks. Program of maintenance and repair of all types of aircraft of the Air Force of the Armed Forces Ukraine can be considered as a set of lower-level programs. The system for ensuring the serviceability of state aviation equipment is a complex multifactorial, essentially non-linear and non-stationary system, therefore, one of the expedient approaches to assessing the impact of risk-

forming factors on ensuring a given level of serviceability of the fleet of aviation equipment is to consider analogies for a system of adequate complexity. As such a system, it is possible to consider the system of aircraft repair enterprises in the implementation of import substitution measures with appropriate risks. The authors propose an algorithm for the formation of a plan for the repair of aviation equipment through an iterative process, in which the minimum risk of ensuring a given level of serviceability of the fleet of state aviation equipment is achieved. For each of the scenarios of the special period, a separate version of the plan for the repair of the aircraft is considered. technique. In order to reduce the risk of critical dependence on one private manufacturer of components necessary for the repair and operation of aviationequipment, similar to the standard ones, it is expedient to develop a state system of economic incentives (provision of preferences, state support) of domestic enterprises involved in the process of import substitution. To this end, it is expedient to initiate the issue of practical implementation of state support for domestic enterprises involved in the process of import substitution in the field of state aviation with the allocation of appropriate financial resources from the State Budget of Ukraine. Thus, the task of ensuring the serviceability of the fleet of aircraft of the Armed Forces of Ukraine in the conditions of a special period, taking into account the real production capabilities of the aircraft repair industry, should be solved by minimizing the risks of import substitution of factory repair processes. For theoretical modeling of the distribution of random variables that characterize reliability, the most acceptable are binomial and Poisson for discrete variables; exponential, Weibull, and normal – for continuous quantities.

Keywords: engineering and technical support of aviation equipment, ensuring a given level of serviceability of aviation equipment, minimizing risks, ensuring a sufficient level of reliability of aviation equipment.

Наукове видання

Центральний науково-дослідний інститут
Збройних Сил України

Міжнародний науковий журнал
“Military Science”

Редактор Васянович М.
Коректор Котляр Т.
Комп’ютерне верстання Шнукало А.

Підп. до друку 14.05.2024. Формат 60x84/16
Папір офсетний. Друк цифровий.
Ум. друк. арк. 17,88. Зам. №. 1405-24/4.
Наклад 50 прим.

Видавець і виготовлювач ТОВ «7БЦ»
03067, м. Київ, вул. Олекси Тихого, 84
e-mail: 7bc@ukr.net, тел: (044) 592-00-80
Свідоцтво суб’єкта видавничої справи ДК №5329 від 11.04.2017