The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 2 (2025)

DOI: 10.62524/msj.2025.3.2.10

Recommendations on the Implementation of Defence Planning Measures for Acquiring and Developing Capabilities by the Prospective Cyber Forces of the Armed Forces of Ukraine Based on the DOTMLPFI

Volodymyr Horbatiuk
Deputy Chief of the General Staff of the Armed Forces of Ukraine
The General Staff of the Armed Forces of Ukraine
03168, Povitrianykh Syl Avenue, 6, Kyiv, Ukraine
e-mail: gorbvol@yahoo.com
ORCID: 0009-0009-9566-3168

Vladyslav Horhulenko
Adjunct of the Scientific and Organisational Department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: vladyslavhorhulenko@gmail.com
ORCID: 0000-0001-6382-5075

Valeriia Horhulenko
Junior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: horhulenkovaleriia@gmail.com
ORCID: 0009-0009-1394-6325

Yuzef Dobrovolskyi
Candidate of Technical Sciences, Associate Professor
Deputy Chief of the Military Education Department
for the Educational Work – Chief of the Educational Unit
The National Aviation University
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: kataza@i.ua
ORCID: 0000-0002-1077-1402

Maksym Samsonenko
Educator of the Millitary Management Department
at the Institute of State Military Management of the National Defence University of Ukraine
National Defence University of Ukraine
03049, Povitrianykh Syl Avenue, 28, Kyiv, Ukraine
e-mail: samson8115@ukr.net
ORCID: 0009-0001-6264-6582

Abstract. Today, the development of the Ministry of Defence of Ukraine and its Armed Forces, in particular, is carried out based on the capabilities required, with a focus on existing and potential threats to national and military security. The experience of armed confrontation over the past decade has shown that one such threat is adversary aggression in cyberspace. Therefore, there is now

sufficient justification for establishing Cyber Forces as a separate branch of troops(Forces) within the Armed Forces of Ukraine, whose task shall be the preparation for and conduct of military measures for cyber defence. Effective execution of this task will be possible if the prospective Cyber Forces of the Armed Forces of Ukraine acquire the capabilities for conducting confrontation in cyberspace as defined in the Strategic Defence Bulletin. The aim of the article is to develop an implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine, based on DOTMLPFI – one of the advanced methods (approaches, techniques) used in NATO countries.

During the course of the research, methods of systems analysis, generalisation, and systematisation were used, which collectively enabled the development of an implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the Armed Forces of Ukraine based on DOTMLPFI. The developed model represents a description of capabilities for conducting confrontation in cyberspace for each of the eight fundamental DOTMLPFI components in the following format: the potential that can be achieved through the implementation of acquired capabilities; the current state (problem) of the capabilities; and possible measures to resolve the problem that will enable the potential to be realised. Thus, the implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the Armed Forces of Ukraine covers such capability components for conducting confrontation in cyberspace as: doctrinal foundation (D), organisation (O), training (T), materiel support (M), leadership (L), personnel (P), infrastructure (F), and interoperability (I). The practical significance of the research results is revealed in the potential of the Armed Forces of Ukraine to acquire capabilities for conducting confrontation in cyberspace through the implementation of the proposed defence planning implementation model based on DOTMLPFI.

Keywords: cyber defence, cyberspace, cybersecurity, cyber confrontation, Cyber Forces, defence planning, capabilities, DOTMLPFI.

Introduction

Defence planning activity plays a key role in ensuring state national security [1–3]. This activity requires constant dynamic development, adaptation, modernisation, and reform across the security sector, particularly within the armed forces, to maintain the state's ability to repel armed aggression. The complexity of the defence planning process lies in assessing this ability amidst uncertainty surrounding future armed aggression — including the scale of conflict, enemy weaponry, intentions, objectives, and other factors [4–6]. Accordingly, the level of readiness to repel aggression may fall short due to insufficient threat assessment, or exceed what is necessary and sufficient — leading to excessive defence spending from the state budget, which is unacceptable in countries with market economies and democratic systems. Under such conditions, a variety of defence planning approaches have emerged, including: top-down planning; resource-based; technology-based; risk-avoidance-based; sequential planning; historically driven; scenario-based; threat-oriented; and capability-based models. Ukraine currently adopts capability-based defence planning oriented towards threats. This model allows for consideration of threats to military security and their potential development scenarios, enabling the identification of tasks for Ukraine's Security and Defence Sector entities, as well as the capabilities required to fulfil them — capabilities that must be inherent in standard capability carriers [7–9].

Under the Law of Ukraine [10], the task of preparing and conducting cyber defence is assigned to the MoD of Ukraine and the General Staff of the AF of Ukraine. The Strategic Defence Bulletin [11] defines the list of components within the Security and Defence Sector of Ukraine required for capability development. Among these, the AF of Ukraine is the carrier of all the specified capabilities without exception. At the same time, the Cybersecurity Strategy of Ukraine [12] establishes the

formation of cyber troops within the system of the MoD of Ukraine. To implement this provision, a draft law [13] has been registered in the Verkhovna Rada of Ukraine, which proposes the establishment of Cyber Forces as a separate branch of troops(Forces) of the AF of Ukraine, whose main task shall be the execution of specifically military measures for the for state cyber defence. The relevance and urgency of forming Cyber Forces as a separate branch of troops(Forces) within the AF of Ukraine is further confirmed by the results of analysis and synthesis of advanced experience in conducting cyber warfare during contemporary armed conflicts [14], which indicate a threat to Ukraine's national and military security in the form of military cyber operations by the russian federation (rf) and highlight the dominance in cyberspace of states whose defence institutions include cyber troops. Under wartime conditions, the russian federation (rf) actively employs its own cyber forces, which influence the course of the war in Ukraine across the informational and cognitive dimensions. Unlike the United States, the rf has not formally declared the existence of cyber forces, but in practice they exist in the form of several structures, the main ones being: APT "Sandworm" under the Main Directorate of the General Staff of the Armed Forces of the rf, APT "Turla" under the Federal Security Service of the rf, and APT "Nobelium" under the Foreign Intelligence Service of the rf [14].

It would be entirely logical and rational for the prospective Cyber Forces to aggregate all required capabilities for conducting confrontation in cyberspace, as defined for the AF of Ukraine, with their acquisition enabling the formation of an integrated ability to conduct military measures for state cyber defence. At the same time, the use of modern methods, models, approaches, and techniques of defence planning during planning activity may significantly enhance the implementation model for capability development measures by the Cyber Forces [15–18].

The aim of the article is to develop an implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine, based on DOTMLPFI – one of the advanced methods (approaches, techniques) used in NATO countries.

Methodological Framework

The methodological basis of the research is the application of DOTMLPFI principles to the process of acquiring and developing capabilities by Ukraine's prospective Cyber Forces through the development of a capability-based defence planning implementation model.

DOTMLPFI is based on eight fundamental components used for capability decomposition, namely:

1. Doctrine (D) – doctrinal foundation.
2. Organization (O) – organisation.
3. Training (T) – training.
4. Materiel (M) – materiel support.
5. Leadership (L) – command and leadership.
6. Personnel (P) – personnel.
7. Facility (F) – military infrastructure.
8. Interoperability (I) – interoperability.

Examples of applying the DOTMLPFI method in defence institutions of leading states provide a broader understanding of the strategy for the soft integration of Cyber Forces into the system of the MoD of Ukraine.

The DOTMLPFI system is based on NATO's defence capabilities. The NATO Alliance is a global leader in the field of cyber defence due to its well-considered strategy for protecting digital space, effective coordination among allies, and advanced cybersecurity infrastructure. As early as 2008, the North Atlantic Alliance recognised cyberspace as a separate theatre of operations, and since 2016, has equated it with the traditional domains of warfare – land, sea, air, and space. This demonstrates that NATO views cyberattacks not merely as a threat but as a serious challenge that may

have critical consequences for national security. The war waged by the rf against Ukraine has clearly demonstrated the impact of cyberattacks on Ukraine's cyberspace and information domain as a whole. The need for the AF of Ukraine to acquire capabilities for state cyber defence is fully justified.

It is proposed to develop an implementation model for defence planning measures aimed at acquiring and developing capabilities by the prospective Cyber Forces of the AF of Ukraine using a capability assessment methodology consisting of four stages [19]:

1. Preparatory stage
2. Requirement analysis
3. Gap analysis
4. Solution analysis

According to this methodology, the preparatory stage involves forming a working group in line with the subject of assessment. The requirement analysis stage focuses on identifying capability requirements, taking into account task specifics, conditions, assessment indicators, standards, and so forth. These two stages shall be considered completed, resulting in a defined set of capabilities required by the AF of Ukraine for conducting confrontation in cyberspace [12]. Accordingly, based on the implementation of the third and fourth stages of this methodology within the research, an implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine will be developed using the DOTMLPFI framework.

Capabilities reflect and serve as indicators of the ability of capability carriers to achieve the desired outcome (effect) in military operations (combat actions) of troops (Forces) [1]. The following represent the capabilities of typical capability carriers of the AF of Ukraine for conducting confrontation in cyberspace (cyber defence) [11]:

the ability to conduct information measures for state defence;

creation of a cyber defence system for conducting confrontation in the information domain (including cyberspace);

the ability to ensure effective cyber protection of national information infrastructure (critical information infrastructure), conduct preventive actions to detect and respond to cyberattacks and cybersecurity incidents, eliminate their consequences under conditions of enemy cyber reconnaissance and intensive cyber influence (cyberattacks);

the ability to conduct cyber reconnaissance and cyber surveillance in information and telecommunication networks and systems of state, private, and military purpose (critical infrastructure targets) of the adversary, in order to obtain information about the adversary's cyber infrastructure, its function, location, technological processes, vulnerabilities, establish covert control, intercept and decrypt command and resource-related data and information;

the ability to prepare and carry out coordinated demonstrative cyber actions (cyber influence) in cyberspace to prevent the outbreak of armed conflicts, and to deter and repel military aggression in cyberspace;

the ability to organise training and conduct cyber actions (cyber influence, cyberattacks) using all types of cyber weapons, including seizure (disruption, takeover), infliction of damage (cascade effect), disruption of functioning of the adversary's critical and information infrastructure, while simultaneously concealing one's activity in cyberspace;

employment of cyber security hardware and software systems, cyber defence tools, and cyber weapons to fulfil cyber warfare tasks.

The process of acquiring and developing the listed capabilities by the prospective Cyber Forces of the AF of Ukraine may potentially lead to additional expenditures from the state budget. Therefore, when justifying the rationality of implementing particular defence planning measures in this area, it is proposed to use the return on investment indicator, known in English-language literature as ROI (*Return on Investment*). The P_{ROI} indicator operates with the value of potential financial loss caused by adversary actions in cyberspace and the funds spent on cyber defence:

$$P_{ROI} = \frac{P_{loss} - P_{cost}}{P_{loss}}, \quad (1)$$

where, P_{loss} – potential financial loss, UAH;

P_{cost} – funds spent on cyber defence, UAH;

$0 < P_{cost} < P_{loss}$;

$0 \leq P_{ROI} \leq 1$.

That is, spending one million hryvnias on cyber defence, which protects cyber infrastructure from adversary's destructive actions that could potentially result in a financial loss of ten million hryvnias, would yield a $P_{ROI} = 0{,}9$ value. Based on the numerical value of the P_{ROI}, indicator, and knowing the criterion for rationality in implementing cyber defence measures, it is possible to assess the appropriateness of such measures. However, the justification of this rationality criterion constitutes a separate area of research.

Results and Discussions

The situation described above demonstrates the necessity of and confirms the course set out in the Cybersecurity Strategy of Ukraine for the establishment of Cyber Forces as a separate branch of troops (Forces) within the AF of Ukraine, enabling them to acquire the capabilities required to fulfil their assigned task of preparing for and conducting state cyber defence. In order to effectively carry out this task, the Cyber Forces of the AF of Ukraine, once (or if) established, must acquire the previously outlined capabilities for conducting confrontation in cyberspace.

The situation described above proves the necessity of and confirms the course declared in the Cybersecurity Strategy of Ukraine for establishing Cyber Forces as a separate branch of troops (Forces) within the AF of Ukraine, which would enable them to acquire the capabilities required to fulfil their assigned task of preparing for and conducting state cyber defence. In order to effectively perform this task, the Cyber Forces of the AF of Ukraine, once (or if) established, must acquire the previously outlined capabilities for conducting confrontation in cyberspace.

Taking into account that the first two stages of the selected capability assessment methodology [19] have been implemented directly in the form of a list of capabilities, the implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine will be developed as the result of completing the stages of capability gap analysis and solution analysis. The implementation of these stages of the capability assessment methodology is proposed to be carried out for each of the eight fundamental components of DOTMLPFI. For this purpose, each of the eight fundamental components of the AF of Ukraine's capabilities for conducting confrontation in cyberspace will be described using the following structure:

the potential that can be achieved through the implementation of acquired capabilities;

the current state (problem) of capabilities;

measures to address the problem, which will allow the potential of capabilities to be achieved.

The structure of the implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine may be conventionally presented as shown in Fig. 1 (for each fundamental DOTMLPFI capability component).

Proceeding to the direct presentation of the core content of the implementation model for defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine for conducting confrontation in cyberspace, it should be noted that this model is not a dogma, postulate, or directive for action. The aim of developing this model is to identify problem areas that require development and propose indicative measures in these areas that may be useful for achieving the potential of acquiring the specified capabilities.

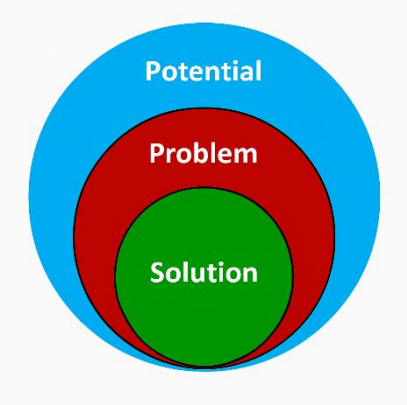


Figure 1. Structure of the implementation model for defence planning measures for each fundamental DOTMLPFI capability component

Doctrinal foundation (D). Ukraine's legislation and the doctrinal framework of the AF of Ukraine in the field of cybersecurity, cyber defence, and the conduct of military operations in cyberspace require further development (refinement) in the direction of unifying, systematising, and hierarchising the terminology, which is currently shaped by a range of legal acts and sectoral guidance documents. For today, the boundaries for the use of cyberspace for military purposes have not been clearly defined.

The definition of cyberspace provided in the Law of Ukraine [10] characterises it in a civilian context, without offering legal grounds to regard cyberspace as an operational environment. Cyber defence, for which the MoD of Ukraine and the General Staff of the AF of Ukraine are responsible in terms of preparation and execution, involves not only military but also economic, political, legal, social, and other measures. However, the mechanisms and algorithms for implementing the latter remain unclear. The doctrinal framework does not establish a link between cyber defence and cyber confrontation, despite recent studies on the relevant terminology [20] substantiating the need to introduce a clear relationship between these two concepts. Additionally, terms such as "cyber actions" and "actions in cyberspace" exist at the same level within the terminology system, although in practice they refer to the same concept. In other words, the doctrinal base contains a degree of duplication and substitution of terms.

The potential of improving and regulating the doctrinal framework lies in the ability to unambiguously interpret, describe, and classify actions in cyberspace and, as a result, to assess their effectiveness. Accordingly, the effectiveness of task execution by the prospective Cyber Forces of the AF of Ukraine, if established, will become one of the main criteria for evaluating the feasibility of this branch of troops (Forces). Without unifying the terminology in the fields of cyber defence, cybersecurity, and cyber confrontation, it is more than likely that there will be difficulties in clearly defining the tasks, authorities, and areas of responsibility within the Cyber Forces of the AF of Ukraine.

A possible solution to the problem of the doctrinal framework for realising the potential of acquiring capabilities for conducting confrontation in cyberspace by the prospective Cyber Forces of the AF of Ukraine is to carry out joint comprehensive research involving representatives from military, technical, and legal fields, at least within the scope of a research project. Such research should reformat Ukraine's doctrinal base in the part related to conducting confrontation in cyberspace and ensure clarity and unambiguity in the distribution of responsibilities among the components of the Security and Defence Sector of Ukraine regarding the provision of state cybersecurity.

Organisation (O). At present, the structure of the MoD of Ukraine includes military command bodies and military formations that perform assigned tasks related to Ukraine's cyber defence.

Specifically, these are the Main Directorate of Electronic and Cyber Warfare of the General Staff of the AF of Ukraine, the Main Directorate of Communications and Cybersecurity of the General Staff of the AF of Ukraine, and the AF of Ukraine's Communications and Cybersecurity Troops. The problem lies in the absence of a clearly defined division of tasks and responsibilities among these actors involved in ensuring state cyber defence, which creates uncertainty regarding accountability in this area of activity within the AF of Ukraine.

The potential of establishing the Cyber Forces of the AF of Ukraine as a separate branch of troops(Forces), tasked with carrying out military measures for preparing and conducting state cyber defence, lies in eliminating overlapping responsibilities among organisational structures within the MoD of Ukraine in this area, building a hierarchical cyber defence management system, and enabling scalability.

The solution to the organisational problem of the AF of Ukraine's capabilities for conducting confrontation in cyberspace is unequivocal – the formation of Cyber Forces as a separate branch of troops(Forces) within the AF of Ukraine, entrusted with the authority to carry out military measures for preparing and conducting state cyber defence.

Training (T). Training is an integral part of the system for ensuring state cyber defence. At present, the training cycle for military cybersecurity specialists and their targeted employment within the MoD of Ukraine and the AF of Ukraine remains incomplete. The leading military higher education institution that trains officers at the tactical level in the field of information technology, including cybersecurity, is the Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty. However, a common phenomenon is the assignment of graduates, upon completion of their studies and acquisition of the relevant qualification, to positions in related military occupational specialties, for example, as platoon commanders in mechanised (tank) battalions or battalion staff officers. Training for non-commissioned cybersecurity personnel exists only in a very generalised form, as the majority of specialised positions are officer roles.

At the same time, despite NATO's experience in establishing cyber ranges for simulating and modelling military operations in cyberspace, and a significant body of research in the field of cybersecurity that substantiates the relevance of introducing such experience into the training system of the AF of Ukraine, the training of military cybersecurity specialists is currently not conducted using cyber ranges. The relevance of integrating cyber ranges into the training system for cybersecurity specialists of the AF of Ukraine is reinforced by the rapid increase in the number of information and communication systems within the military command bodies of the AF of Ukraine and the complexity of their technical organisation.

The potential of establishing a closed-loop system for training military cybersecurity specialists and ensuring their targeted employment in relevant AF of Ukraine units, such as the prospective Cyber Forces of the AF of Ukraine, lies in maintaining a consistent level of unit proficiency and cohesion for conducting confrontation in cyberspace, as well as their ability to carry out assigned tasks related to the preparation for and execution of state cyber defence.

Given the persistent uncertainty of cyberspace and the processes occurring within it, military cybersecurity specialists must be trained on the basis of a creative approach to task execution, flexibility, and the ability to adapt and alter the nature of their actions depending on the operational environment. Cyber specialists of the AF of Ukraine must have fluent command of the applied information technology stack and be able to use it in practice without significant reliance on technical literature. In military higher education institutions, academic programmes in cybersecurity-related specialisations must be regularly updated to reflect emerging forms and methods of cyber confrontation and the advancement of information technologies. Cooperation with NATO in the training process is also essential, and participation in joint cyber defence exercises, such as Locked Shields and others, is necessary.

Materiel support (M). The acquisition and development of capabilities for conducting confrontation in cyberspace directly depend on the adequacy and quality of materiel support.

Currently, the existing units within the MoD of Ukraine and the AF of Ukraine responsible for preparing and conducting cyber defence possess certain types of antivirus software for combating malicious code, as well as software and hardware systems for scanning computer networks to detect and neutralise adversary intrusions into information and communication systems. At the same time, the process of equipping the AF of Ukraine with cyber weapons is at the stage of defining their tactical and technical requirements.

The potential of creating sufficient, high-quality, and technologically advanced materiel support for acquiring and developing capabilities to conduct confrontation in cyberspace by the prospective Cyber Forces of the AF of Ukraine lies in the ability to develop proprietary technologies and software solutions for cyber defence and cyber influence, engage in cyber defence cooperation with partner states, and utilise artificial intelligence technologies for attack analysis and cyber intelligence.

If a decision is made to establish Cyber Forces within the MoD of Ukraine, it will be essential to equip this branch of troops(Forces) with the most advanced equipment available on the market. In addition, considering the frequent cases of adversary intrusion into the cyber infrastructure of Ukraine's critical information infrastructure, caused by the use of software produced by non-resident companies, it is necessary to scale up Ukraine's own developments in the field of cybersecurity. The creation of domestic, internal software (or software-hardware) tools for cyber defence and cyber influence will enable the independent execution of actions or operations in cyberspace. In this regard, and to gain an advantage over the adversary in cyberspace, attention must be paid—during both the development and procurement of cyber weapons—to those systems equipped with artificial intelligence algorithms (technologies) for automated detection of enemy cyber reconnaissance (cyberattacks) and vulnerabilities within one's own cyber infrastructure. Today, the use of artificial intelligence in cybersecurity is one of the most relevant trends.

An equally important aspect of materiel support is financial provision. Since military cybersecurity specialists must have full command of the entire spectrum of applied information technologies, this makes them highly competitive on the labour market, while their financial remuneration in the AF of Ukraine does not differ significantly from that of service members in other armed services(branches) of troops(Forces)..

Leadership (L). Leadership is a driving fundamental component of any capability. Under conditions where the results of confrontation in cyberspace are directly dependent on knowledge and mastery of applied information technologies and the ability to implement them, ensuring the principles of unity of command and effective leadership becomes a complex task. This challenge is further compounded by the fact that military cybersecurity specialists are trained in military higher education institutions with a clear technical focus, while insufficient attention is paid to the development of methodological and leadership qualities necessary for command roles.

The potential of improving the leadership component within the capabilities for conducting confrontation in cyberspace by the prospective Cyber Forces of the AF of Ukraine lies in increasing the cohesion of relevant units, fostering healthy competition among personnel for career advancement, and building an effective command system for military operations in cyberspace.

At the same time, operations in cyberspace, like conventional military operations, require a clear hierarchical command structure. Therefore, a leader within the prospective Cyber Forces of the AF of Ukraine must possess both knowledge and practical skills in applying information technologies for cyber defence, as well as strong leadership qualities – to lead by example, inspire the team, and encourage top performers. A leadership-based approach presumes career advancement for the best and most motivated.

Personnel (P). The specifics of training and targeted employment of military cybersecurity specialists were considered during the analysis of the fundamental capability component "Training

(T)". However, there are certain issues related to the patriotic mindset and motivation of personnel who serve as carriers of capabilities for conducting confrontation in cyberspace. Motivation and patriotic commitment are often interrelated aspects. At the same time, such issues are present not only within the cyber defence units of the MoD of Ukraine but also in other organisational structures.

The potential of equipping the prospective Cyber Forces of the AF of Ukraine with qualified, patriotic, and motivated personnel who meet the defined requirements for capabilities to conduct confrontation in cyberspace lies in preventing a personnel shortage within this branch of troops(Forces) and ensuring that units are capable of fulfilling their designated tasks through careful candidate selection.

To realise this potential, it is necessary to select candidates for service in the prospective Cyber Forces of the AF of Ukraine based on professional competence, to maintain continuous motivation of personnel, and to strengthen the patriotism of units by creating attractive service conditions and ensuring fairness in managerial decisions.

A separate area for improving the provision of qualified personnel is the involvement of civilian cybersecurity specialists—of whom there are many in Ukraine—during a special period or under martial law, to perform tasks related to Ukraine's cyber defence as an alternative to their mobilisation on general grounds into general military formations. An example of this is the CyberGuard programme in the United States, which enables IT experts from the private sector to work with military units.

Military infrastructure (F). The level of military infrastructure for conducting confrontation in cyberspace can be assessed based on the availability and condition of facilities, individual structures and associated communications, as well as land designated for ensuring the preparation and conduct of state cyber defence, their location, suitability for supporting daily functioning and training.

The potential of providing military infrastructure is revealed in the ability to adequately prepare units and military formations to carry out state cyber defence measures and in enhancing the effectiveness of cyber weapons with which they will be equipped.

At present, the AF of Ukraine lacks a network of cyber ranges, which complicates the training process for cybersecurity specialists. In addition, to enable the acquisition and development of capabilities by the prospective Cyber Forces of the AF of Ukraine, it is necessary to expand military infrastructure for their deployment and performance of designated measures, ensuring that it meets all technical requirements of this branch of troops(Forces). Such facilities must be compatible with the weaponry of the Cyber Forces.

Ukraine is already expanding state data centres for information protection, and backup server projects have been created to safeguard state data. However, a critical issue remains the heavy dependence on civilian infrastructure (commercial cloud services).

Interoperability (I). At present, the problem of interoperability lies in the decentralisation of responsibility for Ukraine's cyber defence among military command bodies. Different tasks and responsibilities for conducting confrontation in cyberspace are assigned to various organisational structures that are not subordinated to one another. Moreover, interoperability among the entities of Ukraine's National Cybersecurity System is limited; in addition to the MoD of Ukraine, this system includes the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, and several other agencies. A separate issue is achieving interoperability between the prospective Cyber Forces of the AF of Ukraine and NATO cyber defence units, given Ukraine's course toward joining the Alliance.

The potential of enhancing interoperability in conducting confrontation in cyberspace lies in enabling the AF of Ukraine to carry out joint, coordinated, effective, and result-oriented actions aimed at achieving tactical, operational, and strategic objectives of cyber defence.

To address the issue of interoperability, Ukraine must scale up the ongoing integration into NATO's cyber network, define clear tasks and limits of authority for the prospective Cyber Forces of

the AF of Ukraine in conducting confrontation in cyberspace, and establish effective mechanisms for interaction between this branch of troops(Forces) and other organisational structures of the MoD of Ukraine whose activities involve cybersecurity, cyber protection, and cyber defence.

To fully address and summarise this issue, the key points of the implementation model for defence planning measures aimed at acquiring and developing capabilities by the prospective Cyber Forces of the AF of Ukraine should be presented in the form of Table 1.

Conclusion

Thus, the article proposed recommendations for implementing defence planning measures to acquire and develop capabilities by the prospective Cyber Forces of the AF of Ukraine based on the DOTMLPFI framework. The developed model presents a description of each of the eight fundamental capability components of the AF of Ukraine for conducting confrontation in cyberspace, following the structure: the potential that can be achieved through the implementation of acquired capabilities; the current state (problem) of capabilities; and the measures to resolve the problem that will enable the potential to be realised. The implementation and adoption of this model will constitute a significant step towards strengthening Ukraine's national security, enabling effective preparation for and conduct of cyber defence, and countering aggression in the digital domain.

Table 1. Key provisions of the implementation model for defence planning measures

	Potential	Problem	Solution
D	– clarity in the interpretation, description, classification, and evaluation of the effectiveness of actions in cyberspace; – unified terminology in the fields of cyber defence, cybersecurity, and cyber confrontation; – clear definition of tasks, authorities, and area of responsibility of the prospective Cyber Forces	– ambiguity in the terminology; – duplication of terms and substitution of concepts within the system of legal acts and guidance documents; – lack of clear distribution of tasks for preparing and conducting state cyber defence; – absence of a unified military doctrine on cyber defence; – low level of integration of cyber strategy into the overall concept of warfare	– reformatting the doctrinal framework in the part related to conducting confrontation in cyberspace to ensure clarity and unambiguity in the distribution of responsibilities among the components of the Security and Defence Sector of Ukraine regarding the provision of state cybersecurity
O	– elimination of overlapping responsibilities among organisational structures of the MoD of Ukraine in the field of cyber defence; – establishment of a hierarchical cyber defence management system and the possibility of its scalability	– lack of clearly defined distribution of tasks and responsibilities among the entities responsible for state cyber defence; – uncertainty in accountability for state cyber defence	– formation of the Cyber Forces of the AF of Ukraine as a separate branch of troops(Forces); – aggregation by the Cyber Forces of all defined capabilities for conducting confrontation in cyberspace
T	– consistent level of proficiency and cohesion among units designated for conducting confrontation in cyberspace; – capability to carry out assigned tasks for preparing and conducting state cyber defence	– incompleteness of the training cycle for military cybersecurity specialists and their targeted employment within the military education system	– high-quality training of military cybersecurity specialists based on a creative approach and adaptability; – regular updating of academic programmes in cybersecurity-related specialisations in military higher education institutions; cooperation with NATO in the training process and joint exercises

Table 1 continued. Key provisions of the implementation model for defence planning measures

M	– possibility of developing proprietary technologies and software solutions for cyber defence and cyber influence; – cooperation in the field of cyber defence with NATO partner states; – use of artificial intelligence technologies for attack analysis and cyber reconnaissance	– the process of equipping the AF of Ukraine with cyber weapons is at the stage of defining their tactical and technical requirements	– equipping the prospective Cyber Forces of the AF of Ukraine with the most advanced equipment; – scaling up Ukraine's own developments in the field of cybersecurity; – use of artificial intelligence algorithms (technologies) for automated detection of adversary cyber reconnaissance (cyberattacks) and vulnerabilities in cyber infrastructure; – adequate financial provision for military cybersecurity specialists
L	– increased cohesion among cyber defence units; – healthy competition among personnel for career advancement in the field of cyber defence; – establishment of an effective command system for military operations in cyberspace	– difficulty in ensuring the principles of unity of command and leadership in the domain of confrontation in cyberspace; – predominantly technical focus in the training of military cybersecurity specialists; – low level of methodological and leadership skills	– enhancement of leadership abilities among military cybersecurity specialists; – career advancement for the best and most motivated personnel in cyber defence units; – adoption of NATO leadership practices in cyber defence units
F	– possibility of proper preparation of units and military formations for carrying out state cyber defence measures; – increased effectiveness in the use of cyber weapons	– absence of a cyber range system for simulating and modelling confrontation in cyberspace	– expansion of military infrastructure for deployment and execution of cyber defence measures; – alignment of military infrastructure with the needs of the prospective Cyber Forces of the AF of Ukraine; – compatibility of military infrastructure facilities with Cyber Forces weaponry
I	– enabling the AF of Ukraine to conduct joint, coordinated, effective, and result-oriented actions to achieve tactical, operational, and strategic objectives of cyber defence	– decentralisation of responsibility for Ukraine's cyber defence among military command bodies; – low interoperability among the entities of Ukraine's National Cybersecurity System	– scaling up the ongoing integration into NATO's cyber network; – defining clear tasks and authorities for conducting confrontation in cyberspace; – establishing effective mechanisms of interaction with other MoD of Ukraine structures involved in cybersecurity, cyber protection, and cyber defence; – interoperability with cyber defence units of NATO member states

References

1. Deniezhkin, M. M., Nalyvaiko, A. D., & Polyayev, A. I. (2017). Features of Defense Planning in NATO Member States Based on Capabilities. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine, 2* (60), 34–38. https://doi.org/10.33099/2304-2745/2017-2-60/34-38.
2. Nalyvaiko, A. D., Polyayev, A. I., & Nalyvaiko, L. P. (2019). Theoretical Foundations of Building a Functional Model of the Defense Planning Process for Defense Forces. *Collection*

of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine, 2 (66), 35–41. https://doi.org/10.33099/2304-2745/2019-2-66/35-41.

3. Nalyvaiko, A. D., & Polyayev, A. I. (2021). Approaches to Developing a Functional Defense Management Model. *Social Development and Security, 11* (3), 20–29. https://doi.org/10.33445/sds.2021.11.3.2.
4. Pavlikovsky, A., Frolov, V., & Saghanyuk, F. (2020). *Defense Reform: A Systematic Approach to Defense Management*. (Edited by A. Syrotenko). National University of Defense of Ukraine.
5. Valtonen, I., Rautio, S., & Salmi, M. (2022). Capability Development in Hybrid Organizations: Enhancing Military Logistics with Additive Manufacturing. *Progress in Additive Manufacturing. 7*, 1037–1052. https://doi.org/10.1007/s40964-022-00280-z.
6. Korendovych, V. S., & Chirikalov, O. S. (2020). The Problem of Decentralization of Command and Control in Hybrid Warfare. *Development of Theory and Methodology, 3* (12), 32–40. https://doi.org/10.33099/2618-1614-2020-12-3-32-40.
7. Shchipansky, P. V., Saghanyuk, F. V., & Mudrak Y. M. (2021). Defense Management: Approaches to Managing the Defense Planning Process. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine*, *1* (71), 52–58. https://doi.org/10.33099/2304-2745/2021-1-71/52-58.
8. Nalyvaiko, A. D. (2024). Justification of Directions for Improving Strategic Planning in the Defense Sector. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine*, *1* (80), 27–33. https://doi.org/10.33099/2304-2745/2024-1-80/27-33.
9. Lutsyk, Y. O., Parkhomenko P. P., Demeniev O. M., & Alimov D. I. (2023). Analysis of the Defense Planning System Based on Capabilities, Considering the Leading Experience of NATO Member States. *Modern Economics*, *41*, 73–78. https://doi.org/10.31521/modecon.V41(2023)-11.
10. Law of Ukraine *"On the Basic Principles of Cybersecurity Provision in Ukraine"* No. 2163-VIII (2017, 05 Aug. 10): as of June 28, 2024. https://zakon.rada.gov.ua/laws/show/2163-19
11. President of Ukraine. (2021). *On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine"* (473/2021). https://zakon.rada.gov.ua/laws/show/473/2021#Text
12. President of Ukraine. (2021). *On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021, "On the Cybersecurity Strategy of Ukraine"* (447/2021). https://zakon.rada.gov.ua/laws/show/447/2021#Text
13. *Draft Law on Cyber Forces of the Armed Forces of Ukraine.* https://itd.rada.gov.ua/billinfo/Bills/Card/45453
14. Horhulenko, V. A. (2024). Cyber Warfare in Modern Conflicts: Advanced Experience, Trends, and Development Patterns. *Modern Information Technologies in Security and Defense*, *2* (50), 11–28. https://doi.org/10.33099/2311-7249/2024-50-2-11-28.
15. Krykun, P., Pavlenko, V., Korendovych, V., Yasenko, S., & Tkach, M. (2024). Development of the National Defense Planning System of Ukraine Based on Euro-Atlantic Principles: Military-Historical Analysis. *Social Development and Security, 14* (3), 14–32. https://doi.org/10.33445/sds.2024.14.3.2.
16. Fediienko, O. P. (2024). Modern Trends in Normative Support for Institutional Formation of Cyber Forces (Cyber Troops): The Experience of Some NATO Countries. *Information and Law, 1* (48), 150–161. https://doi.org/10.37750/2616-6798.2024.1(48).300800.
17. Nagy, J., Foltin, P., & Ondryhal, V. (2022). Use of Big Data Analysis to Identify Possible Sources of Supply Chain Disruption through the DOTMLPFI Method. *LogForum, 18* (3), 309–319. http://doi.org/10.17270/J.LOG.2021.731.

18. Llopis Sanchez, S., Sandoval Rodriguez-Bermejo, D., Daton Medenou, R., Pasqual de Riquelme, R., Torelli, F., & Maestre Vidal, J. (2022). Tackling Verification and Validation Techniques to Evaluate Cyber Situational Awareness Capabilities. *Mathematics, 10*, 2617. https://doi.org/10.3390/math10152617.
19. Tkach, M. Y., & Korendovych, S. A. (2024). *Basics of Defense Management*. National University of Defense of Ukraine.
20. Horhulenko, V. A. (2024). Military-Theoretical Justification of Recommendations for the Development of Terminological Apparatus in the Field of Cyber Warfare. *Modern Information Technologies in Security and Defense*, *3* (51). https://doi.org/10.33099/2311-7249/2024-51-3-41-50.

Рекомендації щодо реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України на основі DOTMLPFI

Володимир Горбатюк
заступник начальника Генерального штабу Збройних Сил України
Генеральний штаб Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: gorbvol@yahoo.com
ORCID: 0009-0009-9566-3168

Владислав Горгуленко
ад'юнкт науково-організаційного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: vladyslavhorhulenko@gmail.com
ORCID: 0000-0001-6382-5075

Валерія Горгуленко
молодший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: horhulenkovaleriia@gmail.com
ORCID: 0009-0009-1394-6325

Юзеф Добровольський
кандидат технічних наук, доцент
заступник начальника кафедри військової підготовки
з навчальної роботи – начальник навчальної частини
Національний авіаційний університет
03048, вулиця Медова 1, Київ, Україна
e-mail: kataza@i.ua
ORCID: 0000-0002-1077-1402

Максим Самсоненко
викладач кафедри військового управління
Інституту державного військового управління
Національного університету оборони України
Національний університет оборони України
03049, проспект Повітряних Сил, 28, м. Київ, Україна
e-mail: samson8115@ukr.net
ORCID: 0009-0001-6264-6582

Анотація. Сьогодні розвиток Міністерства оборони України та її Збройних Сил зокрема здійснюється на основі необхідних для набуття спроможностей, з орієнтуванням на існуючі та потенційні загрози національній і воєнній безпеці держави. Досвід збройного протистояння останнього десятиліття показав, що однією з таких загроз є агресія противника у кіберпросторі. Тому наразі існують достатні підстави для формування Кіберсил як окремого роду військ (сил) Збройних Сил України, завданням якого має стати підготовка та ведення військових заходів з кібероборони. Ефективне виконання покладеного завдання є можливим у разі набуття перспективними Кіберсилами Збройних Сил України визначених у Стратегічному оборонному бюлетені необхідних спроможностей з ведення протиборства у кіберпросторі.

Під час проведення дослідження було використано методи системного аналізу, узагальнення та систематизації, які за сукупністю дозволили розробити модель реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України на основі DOTMLPFI.

Метою цієї статті є розроблення моделі впровадження заходів оперативної безпеки для формування та розвитку потенціалу перспективних Кіберсил Збройних Сил України, використовуючи DOTMLPFI – передовий підхід, що застосовується в країнах-членах НАТО.

Розроблена модель являє собою опис спроможностей щодо ведення протиборства у кіберпросторі за кожним із восьми базових компонентів DOTMLPFI у формі: потенціал, якого можна досягнути, реалізувавши набуті спроможності; існуючий стан (проблема) спроможностей; можливі заходи для вирішення проблеми, які дозволять досягнути потенціалу спроможностей. Отже, модель реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України охоплює такі компоненти спроможностей з ведення протиборства у кіберпросторі як: доктринальна база (D), організація (O), підготовка (T), ресурсне забезпечення (M), управління та лідерство (L), персонал (P), інфраструктура (F), взаємосумісність (I).

Практична значимість результатів дослідження розкривається у потенціалі набуття Збройними Силами України спроможностей з ведення протиборства у кіберпросторі шляхом впровадження запропонованої моделі реалізації заходів оборонного планування на основі DOTMLPFI.

Ключові слова: кібероборона, кіберпростір, кібербезпека, кіберборотьба, Кіберсили, оборонне планування, спроможності, DOTMLPFI.