Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2022, Volume 54, Number 1(203), Pages 35-51
DOI: 10.5604/01.3001.0015.8025

Original article

Challenges of contemporary command and future military operations

Marek Wrzosek

Faculty of Military Studies, War Study University, Warsaw, Poland,
e-mail: m.wrzosek@akademia.mil.pl

INFORMATION

Article history:
Submited: 30 April 2019
Accepted: 06 February 2020
Published: 15 March 2022

ABSTRACT

The article aims to identify the challenges facing the command system in the context of changes that will shape future military operations. For the presentation of the cognitive results, the analysis of documents was used as well as the results of research conducted with the aid of a diagnostic survey, an interview method, as well as non-standardized observation. The structure of the article covers four main issues. The first one presents the relationship between the terms "directing – management – command" in the context of the deliberations made. The second topic focuses on the characteristics of future operations that define the challenges for command. The third one, on the other hand, explains the matters related to the modification of the command in future military operations. The issue complementing all the considerations is an attempt to resolve the problem of recommendations for the command system in the wars of the future. The content of the article uses the conclusions from the experience gained during the military conflicts in Iraq and Afghanistan.

KEYWORDS

command, military operations, future wars, information warfare, network-centric operations

Introduction

In the last years of the new 21st century, many local armed conflicts of varying intensity have been observed. With the consent of international organizations, the intervention of the armed forces of various countries was allowed to restore stability. In addition, military activities of a preventive (anticipatory) nature were carried out in regions where there was a high probability of conflict development[1]. From the observation results, it can be concluded that in command of troops, understood as the multifaceted activity of commands at all

[1] Preventive strikes are military operations aimed at anticipating possible threats by preventing them from developing. This type of operation was, for example, attacks by the Israeli Air Force on nuclear installations in Iraq (1981) and Syria (2007), the intervention of the US-led coalition in Afghanistan (2002), Iraq (2003), and Ethiopia and Somalia (2006).

organizational levels, it was important to prepare appropriate conditions for performing commanding functions, managing subordinate full-time units and temporarily formed army groups (task forces), and using effectively forces and resources at the commander's disposal.

Experience shows that effective command is a prerequisite for success in any military operation. Achieving the assumed goals, both in the period of preparation and conducting operations, depends primarily on the efficiency of operation and the development of appropriate forces in the right place and time. Effective command is therefore a basic condition that will enable the efficient preparation of a military operation involving various types of armed forces.

The presented outline of the situation shows that the issue of command in the conditions of contemporary conflicts is very extensive thematically and complicated organizationally. There is no need to convince anyone about the correctness of this statement. It is enough to analyze the past military conflicts to specify the complex scope of tasks and conditions for their implementation resulting from the use of armed forces. The problem becomes even more complex when the discussed phenomenon is considered in the context of a vision of a new type of armed forces. This is a fundamental factor that forces us to look at the broadly understood "contemporary command" differently than before. Given the fact that command, or rather the command system, constitutes a certain type of organization in the armed forces, it can be assumed that its components constitute a four-element model. In the command model perceived as an organization, one can distinguish: (1) tasks/goals (future, desired result of the organization's operation), (2) structure (a set of organizational units and positions and connections between them (including: information flows, scope and division of duties, subordination), (3) technology (command post technical equipment, information processing procedures), and (4) people (command post personnel and service). Therefore, assuming that in future armed conflicts, command will still be one of the main aspects of ensuring success in fight, it seems necessary to modify it in the light of changes in the way military operations are conducted.

Military operations conducted in the 21st century have generated the essential conditions for a future military conflict. The conclusions and experiences from the campaigns in Iraq, Afghanistan, and the wars in the eastern part of Ukraine were at the basis of attempts to work out changes in the command system. For this reason, many NATO countries are developing command organization modification programs to adapt it to the upcoming challenges. Besides, it should also be noted that combined operations are an obvious requirement of the contemporary and probably future battlefield. Accordingly, the activities undertaken are aimed at ensuring that the new organization of command of the armed forces ensures optimal conditions for joint training and operation of soldiers of all types of armed forces, while maintaining their structure and specificity.

The article is only a voice in discussion, because it is difficult to cover a rather complicated and certainly complex topic within the volume of such a small study. From the perspective of time and experience, the author had the opportunity to carry out tasks in the command structures; he also participated in the process of organizational changes in the command system. The limited volume of the article does not allow for the presentation of comprehensive research results, however, the key conditions forcing the modification of the command organization in the perspective of future military operations will be presented in a synthetic way.

The main objective of the research, the results of which are presented in this article, was to identify the challenges faced by the command system in the context of changes shaping future military operations.

The main problem was formulated in the form of the following research question: What are the challenges facing the command system in the context of future military operations? To solve the main problem, specific problems were also formulated in the form of the following research questions:

1. How is leadership perceived in terms of leadership and management?
2. What changes generating challenges for the command system occur in military operations?
3. What factors will determine the command of future military operations?

It was assumed that the changes taking place both in the concepts of conducting military operations and resulting from the experiences of past military conflicts affect the command system. Achieving the research objective and solving the accepted research problems was possible thanks to the use of analysis and synthesis as well as the survey research method. The study was a pilot study, it was carried out in a group of experts who were selected purposefully, taking into consideration three target respondent groups: commanders, educators, and command system organizers. In addition, the results of non-participant indirect observation were used in the research process.

1. Command, control, management – the conceptual apparatus

In the literature on the Armed Forces command, many publications can be indicated, in which both theorists [See: 1; 2] and practitioners [3; 4] analyzed and interpreted the concept of "command". They usually used an interdisciplinary approach, considering command through the prism of the art of war, praxeology, and organization and management theory. For this reason, the undertaken cognitive activities aimed at determining the meaning of the term "command" in the context of the commonly used terms "management" and "leadership". Therefore, when considering terminological issues in the area of broadly understood command, it is reasonable to explain the basic terms and indicate their characteristic features, as well as mutual relationships.

The conclusions from the literature review allow for the statement that "directing" [See: 5] is the original term from which "management" and "control" are derived. Generally, directing means "any deliberate interaction of one system with another in order to obtain such changes in the course of the process occurring in the subject of control or in the state of the controlled system at any given moment which are considered to be desirable" [6, p. 231]. In the considered context, directing as a concept refers to humans, animals, and machines, as well as the system (organization). As emphasized above, directing is an interaction with a specific object (human, animal, machine, system) aimed at causing the desired conduct or behavior in the expected manner. In other words, the directing should lead to the change of one highlighted state of the system into another highlighted state better suited to the controller [7, p. 49].

Directing, according to the *Encyclopedia of Organization and Management*, is one of the basic organizational concepts. In the most general terms, directing can be understood as the impact of one object (directing) on another (directed) object aimed at making the directed object behave (act or function) towards achieving the goal set before it, in the most simple and specific case – one goal [8, p. 205].

Like the authors of the cited encyclopedia, James A.F. Stoner and Ch. Wankel accepts that directing is the process of planning, organizing, leading, and controlling the activities of members of an organization, and the use of its other resources to achieve the objectives set [9, p. 23].

When considering the term “management”, one should return to the theory of organization and management, where “management is a type of directing in which the entitlement to exert influence on hierarchies and value systems, interests and aspirations as well as attitudes and organizational behaviors of the directed drives from the possession or from the fact that the manager has material and energy resources or nominal and information resources of particular importance for the functioning and development of the organization or the management’s belief that the manager has the possibility to obtain these resources” [10, p. 207]. Therefore, in the cited definition there is an indication that management is a type of directing. It follows from this statement that directing is the overriding term.

After the terminology in management and directing has been settled, the definition of “command” can be addressed. As for the term command, there are various descriptions that differ significantly from one another in the literature. This is probably a consequence of periodic needs resulting from changes that have occurred and are taking place in the art of war. The periods of operation of the Armed Forces, when different needs of entities forming the content of the definition in question were determined, had a significant impact on the diversity of the definition of command. The preferences of the authors, who took account of its various aspects when defining, were also important for defining “command”.

In the praxeological aspect, the exercise of command is primarily associated with the decision-making and planning process. In the Polish theory and practice of command, it is assumed that the general and superior term is “command system”, which consists of three components: the command organization, the command process, and the means of command [11, p. 271].

The command organization covers the general structure and the structures of its individual elements: personal, technical and organizational, as well as the appropriate transformation of these structures, with the state of functioning of the state, from time of peace to time of crisis or war, considered.

The command process, on the other hand, is treated as a repeating, informational and decision-making cycle of command activities aimed at the most effective preparation and use of subordinate troops – both organic and temporarily assigned ones. It consists in the continuous collection and compiling of information and its cyclical processing into appropriate decisions transferred to executors in the form of tasks.

The term “means of command” includes material and technical resources, technical systems, devices and procedures, and information technologies (applications, computer programs, etc.), organized into command post infrastructure, telecommunication, postal, signaling, and command support networks. The means are used in command to acquire, process, verify, distribute, collect, and display information.

The command system functions to maximally support commanders of all levels of command in terms of supplying and providing timely information necessary to perform the command functions: planning, organizing, setting tasks, and the executive part – leading and coordinating the activities (control). The conducted argument shows that the command is carried out in the information and decision-making process, which is based on personnel, technical and organizational elements, mutually dependent, designed and organized into a command system [Cf. 12, p. 99-100].

On the other hand, the *Lexicon of Defense. Command of Poland and Europe* defines command as the “process through which the commander, within his/her authority, makes decisions with the utmost rigor of feasibility, aimed at achieving the intended goal with the use of his/her forces and means" [13, p. 46].

When searching for the relationship between the terms "management", "directing" and "command", it was found that there are common areas of command, directing, and management, which, while maintaining logical result and coherence, are applicable in the command process. In this situation, it is justified to argue that from the analysis of sources and references to power relations in organizations, three main factors forming the formal basis for exercising power and three forms (types) of managing economic and non-profit organizations have been distinguished [14, p. 248].

Table 1. Relationships between factors creating power and types of management

No.	Factors forming the basis of power	Entitlement to direct	Types of directing
1.	Formal competences	Rulership	Administration, rule, supervision, command
2.	Material competences	Possessing or disposing of resources	Management
3.	Intellectual competences of the driver (features, knowledge, skills, creative activity, experience, coexistence)	Personal authority	Leadership

Source: [15, p. 14, based on: 14, p. 248].

Thus, the relations presented by L. Krzyżanowski between the factors creating power and the types of management enable the identification of command based on formal competences (or rather formal power) as one of the types of organization management [14]. The above-mentioned definitions constitute a specific interpretation of the approach to the complex problem of command in contemporary conditions.

Considering the accumulated knowledge, it can be concluded that the basic difference between command and control concerns the scope of power held by the military commander in relation to his/her subordinates. When it comes to the issues of command and control, it should be noted that the national doctrinal documents [16, p. 7] indicate that command at "the tactical levels of the Land Forces includes the process of planning, organizing, setting tasks, and controlling the operation of troops and the use of resources allocated to them to achieve specific goals related to preparation in peacetime and direct tactical operations in times of crisis and war. Planning, organizing, leading and controlling are the basic command functions, which correspond to the stages and activities of the relevant phases of the command process". The fact leads to the conclusion that command is the same in terms of scope as directing, and therefore it can be treated as a specific form of management.

2. Changes during military operations generating challenges for the command system

In the reflection on the future wars, the wars of the 21st century, one thing can be assumed with line with the view opinion, new forms of military operations will probably soon appear, as it used to be in the past (air-land battle), while the old forms will not disappear for a long time (e.g., tribal wars in Africa). Therefore, as the mentioned author concludes, there will be more forms and models of armed conflicts. Thus, next to the wars of the information age, the eras of virtual computer games will also be fought in their characteristics closer to the past than to the future. There may be more of these non-modern “archaic” armed conflicts, they can be longer and bloodier, devoid of the principles of humanism and international law. The theses presented are paragraphs taken almost entirely from books and articles cited in the text [17].

2.1. Information warfare in military operations

In the context of the considerations regarding the command system, one may wonder how important information is for the armed forces. The commander and staff need information in order to make a decision. As shown above, the process of command itself is nothing more than the acquisition, processing, and distribution of information. Thus, information provides the possibility of exercising control to coordinate and monitor the activities of troops. But what is most important in the considerations is the fact that information is the basis for generating news and building knowledge, and thus operational awareness. Finally, information is a factor that makes it possible to use means of destruction, perform a maneuver or avoid hitting the enemy. This brief statement of facts proves the information plays a vital role in the Armed Forces. Hence the great interest in information warfare [See more: 18].

In terms of the art of war, it should be emphasized that the recognition of information as a key element is an inherent feature of contemporary armed conflicts in which information is used both as a weapon and as a target. Military theorists even point to the necessity to treat the information sphere (naturally including cyberspace) as a new combat environment.

The best example illustrating the validity of the above thesis is the experience of the war in Iraq (1991). The war in Iraq was defined as the first conflict of the new century. During the war, the automated digital command systems of the allied forces used information from satellites, image, electronic and personal reconnaissance, while the Iraqi forces continued using analog links to report the position of the troops. Near real-time electronically processed data presented the operational and tactical situation of the allied forces on the monitors, while the Iraqi staffs manually mapped information from the written and graphic content of reports.

After the experience of the Iraqi war, the thesis that the information warfare, and mainly the disruption of information circulation, and the deprivation of the command and staff as the governing body of contact with information sources, seriously hampers the functioning of the command systems, does not raise any doubts. The effectiveness of information warfare is so great that the use of troops, weapons, and combat techniques may become pointless, delayed, and sometimes even impossible. Examples of this kind of activity could be seen during the First Gulf War (1991). The observation of past armed conflicts and the results of comparative analyzes prove that the armed forces conduct information warfare with the use of functional subsystems: military reconnaissance, psychological activities, disinformation, electronic warfare, and direct physical influence. Nevertheless, in many cases, the media can also be a tool of information warfare in armed conflicts. Hence, in the structure of command posts, there are press units, information operation teams, or combined reconnaissance and intelligence teams.

Therefore, taking the challenges for the future command system into consideration, it can be concluded that information warfare may lead to a general advantage that will allow the organization of the global command system and the integration of strategic, operational, and tactical command subsystems. In addition, according to experts, it will ensure the efficient operation of fire control systems by combining sensors (reconnaissance elements and fire control centers) with fire means. Also, it will enable effective disruption of the enemy communication and command systems.

2.2. Cyberwar – from theory to command practice

Throughout the nineteenth century, armed forces around the world conducted operations in one of three operational planes – land, water, and air. On the other hand, in the 20th century, for military purposes, the exploration of a new operational plane – space – began. It was in the space that reconnaissance devices and artificial satellites were installed. Another dimension of action and a new paradigm in armed conflicts was the electromagnetic spectrum, where domination was provided by an information advantage. With the advent of the 21st century, more and more armies of various countries noticed the fact that wars can also be fought in the virtual world, which is now treated as the next, sixth, operating plane next to land, air, water, space and the electromagnetic spectrum [See: 19].

Cyber conflict is commonly understood as a conflict in cyberspace perceived as a clash in computer networks involving various teams of people, techniques, processes, and information resources. The transfer of conflicts into the area of cyberspace is the result of technological changes and the impact that telecommunications has on the security systems of not only countries but also international organizations. The results of observations of the course of contemporary armed conflicts prove that technologically advanced means of combat[2], including intelligent ammunition allowing for precise strikes with limiting unnecessary losses, play an increasingly significant role. Currently, most of the world's armies are investing in modern technologies, especially information ones. For this reason, cyber conflict is no longer just a theoretical concept, it begins to function in practice. In the opinion of military experts, the potential threat resulting from the possibilities created by cyberspace is considered. It may soon turn out that launching homing missiles or the use of aircraft will not be possible, as a potential enemy will block the start codes, disable aircraft engines or limit communication using a virus program for this purpose. Probably a new type of weapon may also be an electromagnetic bomb in the future, often also called the E bomb, it causes an electromagnetic pulse of high power that immobilizes electronic devices. An explosion of an electromagnetic bomb can immobilize everything around, and it contains electronic components[3].

There is no doubt that in the military aspect cyberspace is treated as a new environment for military operations. A new environment that enables the interaction and synchronization of all information gathering, recording, processing, and distribution devices. The widespread digitization and automatic transmission of information in command and control systems makes cyberspace the main information channel and the Internet is a global area of information resources for command and staffs conducting military operations.

These conditions have led to almost every armed force taking action in the event of cyberwar. It is likely that all large countries have their own hacker groups, although few admit to them

[2] During the war with Iraq, the Americans used Tomahawk missiles with a load of specially formed carbon fiber. Graphite missiles scattered over power lines and installations caused short circuits and nuisance blackout in Baghdad.

[3] The e-bomb uses a phenomenon known since 1962, when during the detonation of a 1.4-megaton hydrogen bomb in the Central Pacific at an altitude of 30 km, satellite installations operating nearby were destroyed and radio communication in the Pacific was broken for about 30 minutes. The effect of the explosion was so great that even radio stations at the distance of 1,200 km from the site of the explosion were disrupted.

keeping the operational capabilities of their "cyber-arms" secret. Many countries are making practical preparations for cyber operations by creating units for a new kind of combat within their state structures and types of armed forces to meet new challenges [See: 20, p. 45; 21, p. 44-45]. Since 2008, NATO has regularly conducted exercises under the cryptonym "Cyber Coalition". Their aim is to improve the ability to respond during a crisis, develop cooperation between different agencies and make decisions in the context of a cyber conflict. Each year, the modified scenario of the exercise assumes a massive cyberattack on NATO installations. In addition, specialist training sessions are organized in the member states, the aim of which is to develop practical methods of disrupting and preventing the use of various information systems used by the enemy [See: 22]. At the 2018 NATO summit (11-12 July, Brussels), the final declaration also confirmed the creation of the NATO Cyber Operations Command. It also stressed that cyberattacks are becoming more frequent and more advanced and destructive. Therefore, it was declared that NATO would continue the process of preparation for operations in cyberspace where attacks are carried out by both states and non-state actors. Thus, NATO indicates that cyber defense is an integral part of the collective defense of the Alliance. Hence, the Alliance must operate in cyberspace as effectively as it does on land, air and sea. It should strengthen deterrence in virtual space soon. The presented argument aims to describe a new challenge for the command system, which in the near future will be forced to operate under the conditions of a number of not yet fully understood cyber-threats[4].

War in cyberspace is a development of the concept of information warfare. The military concept of information warfare was based on the belief that using the capabilities of information systems to weaken the enemy's defense capabilities may lead to avoiding the outbreak of a classical armed conflict. In the context of the challenges faced by the modern command system, it can be stated that the main issue will be to maintain the coherence of information resources and ensure information security.

2.3. Network-centric operations – a new environment for command

The basis of the Network Centric Warfare doctrine was the concept of obtaining an information advantage and shortening the decision cycle based on current data contained in computer servers. To achieve the intended objective, it was necessary to build a coherent and effective system of collecting, gathering processing, and distributing information in the armed forces, covering all levels of the command system. As in large commercial or service networks, it was necessary to aggregate information and ensure wide access to it for all military units.

Thus, the concept of a network-centric operation assumes an increase in combat capabilities by achieving a high degree of integration in all dimensions of the operational space and allows the number of troops to be limited thanks to precise information [23]. Since thanks to good quality information, smaller forces will have greater operational capabilities to move, detect, and destroy enemy objects.

The structural aspect is essential in the process of getting to know the specificity of the network-centric struggle. The new concept assumes that combining combat participants,

[4] In February 2017, the Minister of Defense of the Russian Federation, Sergei Shoigu, officially confirmed the creation of an information operation force. The Russian Ministry of Defense is convinced that victory not only in cyberspace, but more broadly in information warfare, in the present reality is of greater importance than success in a classic war. In the opinion of the Russian side, the information confrontation is gaining in importance due to the possibility of shaping people's minds and social awareness.

including elements of an operational group in one network, should be made in three planes, in some publications referred to as "domain" (discipline, field, area, plane, sector, industry):

1) physical,
2) information,
3) cognitive (procedural).

In the effect of developing the assumptions of the concept of network-centric warfare, it was presumed that the physical domain would include traditional military operations in which the enemy was physically eliminated. Hence, in practical implementation, its scope will include attack, defense, and maneuver perceived in all dimensions of military operations (land, sea, air, space, and electromagnetic). Command posts, weapons systems, and the entire physical information system are located in the physical domain. The main indicators for assessing the effectiveness of military operations in this domain are two basic values: destruction efficiency and resilience (ability to survive). To this day, NATO forces deal with the issues of ensuring the effectiveness of destruction while limiting unwanted losses, and the ability to survive. That demonstrates the complexity of the troop preparation process for network-centric operations.

On the other hand, the information domain covers the entire process of collecting (creating), processing and distributing, and thus sharing information resources. It was assumed that it is in the information domain that the information exchange between the participants of the operation will take place. Thus, information will be transferred between the components of the armed forces that take part in the operation, especially command centers and headquarters, and will be exchanged with institutions and organizations supporting military operations. Due to its role in the network-centric struggle, the domain has been given special protection and defense. In principle, the thesis that the information domain directly influences the increase in combat potential and operational capabilities, especially in the situation of gaining an information advantage, is not questionable.

In turn, the cognitive domain is an intangible dimension of the concept of the network-centric warfare. Because it exists only in tacit knowledge, in the minds of participants in military struggles. For this reason, it is even difficult to identify in formal terms. It is often assumed that the cognitive domain consists of non-material entities, such as leadership, morale, cohesion (unity) of a military unit (subunit), the level of training, the ability to understand the operational and tactical situation (situational awareness), and even faith, religion and public opinion. The effects of the thought process (decision-making), i.e., the strategy, combat doctrine, tactics of armed formations, procedures of conduct (operational procedures), as well as the intention to act understood as a way of playing a fight, are physically located in this domain. The above structural domains of the network-centric operation generate new challenges for the command system since it is not only about providing conditions for combat management, but also about the functional separation of information resources for executors of combat tasks.

Another way to present the structure of the network-centric operation space is its division into a three-layer ICT application, which comprises a layer of sensors (sensors), command and control centers (staffs and commands, telecommunications systems), and effectors influencing selected objects.

The concept of a network-centric operation is no longer the future, as some experts claim, but the present in contemporary military operations. It is a response of military thought to changes in today's societies and organizations, including military ones, and a change in the paradigm of contemporary threats. The fundamental change concerns the quality of the threat, as the existing armed forces of the potential enemy have been replaced by terrorist organizations, paramilitary structures, and rebel units [17]. In this context, there is a challenge for new solutions within command organization – how to organize the command system in anti-terrorist or anti-rebel operations under the conditions of network-centric operations?

The results of observations of the course of operations in Iraq and Afghanistan show that the increase in combat potential was generated by connecting sensors and combat systems into an information network, enabling decision-makers to achieve awareness of joint action, increase the speed of command and pace of operations, and increase the effectiveness of weapons. Due to operational knowledge and situational awareness, an increase in resistance to enemy strikes and in the degree of synchronization of activities at all levels was also achieved.

3. Factors determining command in future military operations

Command as an information and decision-making process is undergoing a major transformation, both in technical and organizational terms. Future command systems, thanks to network-centricity, will maintain greater coordination, interdependence, and coherence in the aspect of managing troops and means of destruction. The functional structures of the command system will probably become blurred, which means that in times of peace, crisis, and war they will be structurally identical, and only the staffing will be strengthened. Observation of the ongoing changes is the basis for the conclusion that increasingly efficient, automated elements of the command system, networks and IT systems supporting decision-making processes, as well as automated and integrated communications networks will be introduced. These requirements, in turn, generate the assumptions of a cyber-conflict.

New technical devices, ICT solutions, and the miniaturization of means of communication are currently supporting the commands of the armed forces massively. For this reason, stationary and mobile (field) headquarters and staffs already have comprehensive command systems that ensure high operational awareness. Due to the large distances between command posts, satellite communications are commonly used. The automation of information processes means that an increasingly visible tendency is to shorten the time of information flow. Currently, information aggregated into collections, obtained in real time, is transferred directly from fighting soldiers, equipped with means of communication and digital imaging of the battlefield. In many solutions it is also assumed that image reconnaissance will be carried out at the lowest command levels, where soldiers will have miniature cameras and a sensor system, which will allow to illustrate the information with the transmitted image. Examples of introducing unmanned aerial reconnaissance systems to the tactical level evidence the correctness of the presented thesis. In this respect, therefore, it is appropriate to pay attention to the possibilities that are initiated by the entire spectrum of information warfare measures, namely, disrupting the operation of both sensors and systems, introducing computer viruses or blocking the transmission of information.

The decision-making process, and therefore the timely response to events taking place on the battlefield that especially applies to events in dynamic situations, remains a new challenge for the command. The observation of changes in the conduct of military operations proves that the decision-making time is shortened, and at tactical levels there are already cases in which finding and defining targets as vital for the course of combat are a continuous process. Such a scenario is possible thanks to the network-centric architecture of the command system. It should be noted that the dynamics of the fight will increase, and hence it is necessary to adjust the current organizational solutions in the structure of the command system. Changing the command procedures, especially in the field of reconnaissance, identification, and location of targets[5], is a new challenge for the command in the wars of the future.

Already in the near future, it will be possible to observe intensive technical support for the decision-making process aimed at solving operational and tactical problems. It should be presumed that once the armed forces are equipped with computer simulation programs for the course of military operations, it will become realistic to test the adopted scenario of operations, taking account of the possible reactions of the enemy, and determining the impact of the environment on the planned fighting. Therefore, computer wars in cyberspace will be carried out at command posts, the result of which will be real orders for the armed forces.

In the wars of the future, a human will still be an irreplaceable element of the entire command system. Computer support systems provide a lot of information but do not make decisions. This is the domain of the commander who selects one of the several variants presented by the staff and implements it. "Intelligent ammunition", common on the future battlefield, will probably become the basis for direct impact, but will not determine its use. A human, his/her knowledge, skills, and competences in the field of the art of war will remain the decision-maker.

The challenge to command in the wars of the future in connection with the entire area of information warfare will be the protection of information resources. It is already difficult to overestimate the role and importance of computer networks operating in the command system. In this situation, there is no doubt that finding information of strategic importance should be an insurmountable obstacle. Unfortunately, periodic cyberspace security reports prove that breaching security systems and entering protected networks are still frequent phenomena. Therefore, it is becoming an increasingly complex challenge to secure both entire systems and the network of command posts against IT attacks.

Noting the dynamic development of the network-centric environment of operations, it should be emphasized that it will not be without influence on decisions regarding the operation of troops and the use of means of destruction. Therefore, in the future, circulating ammunition, capable of launching an attack with high-precision missiles with a controlled blast force[6], will become common. The new type of ammunition will independently find selected objects (targets) to shape the battlefield.

Given the technical and functional solutions implemented in the armed forces of other countries, it can be stated that the command organization for the needs of new military operations will change. Probably the alterations will take place in three main directions.

The first will cover the automation of command systems, including the limitation of the human role in the processes of collecting, processing, and distributing information. It can be assumed that the basic principle will be the complexity and systemic nature of solutions

[5] The described phenomenon is already a priority task of many staffs and commands, the best example of which is the modification of the targeting process.

[6] For example – the WARMATE air platform used in combat mode is intended for single use. In observation mode, it can be recovered many times. WARMATE is a fully autonomous solution that allows for the operation of a flying combat vehicle in real time based on video material received from the observation subsystem. The system is equipped with control modules allowing for full automation of most phases of flight and supporting the operator in the target guidance phase. The operator has full control and responsibility for switching to "armed" mode to perform the fire task – see: [online]. Available at: https://www.wbgroup.pl/produkt/bojowy-bezzalogowy-system-powietrzny-warmate/ [Accessed: 2009].

as well as the interconnection and complementation of individual command elements. As the result of the coordination of staff activities, it is expected to achieve greater efficiency of operation at all levels of command. Projects and experiences in this field were already undertaken in the first decade of the 21st century. The concept of information domains was developed from the collected conclusions from armed conflicts to manage information in the network-centric environment.

Due to the specificity of the armed forces, the nature of their tasks and the resulting information needs, four basic types of information domains have been distinguished, namely: hierarchical[7], specialized[8], task-related[9], and spatial[10]. Initial research indicated that the creation of appropriate information domains would allow for higher situational awareness. Therefore, it can be assumed that access to information at the domain level would allow for the resignation of the existing registration system in favor of sharing information [24, p. 41-47].

The second direction in the organization of command will concern the automation of managing the means of destruction (impact). Observing the development of new technologies, it can be concluded that the means of combat will be controlled by means of reconnaissance and detection devices ensuring the identification of air, land, surface, and underwater targets (objects). The automation process will also include the preparation of the necessary data, guiding the means of destruction and firing, after obtaining the consent of the operator – the appropriate missile. The results of observations of past conflicts enables the conclusion that reconnaissance aerial platforms have become the main element in targeting programs of high value targets. It is estimated that their number increased over 40 times in the years 2002-2010. In Afghanistan throughout 2007, a total of 74 strikes by air combat platforms were recorded, but in 2012 the figure was 33 strokes per month [25, p. 2]. During this time, the modified packages of sensors and computer software made it possible for analysts to recognize and categorize personal objects as well as infrastructure and combat equipment objects. That ensured almost full real-time surveillance and a detailed bearing of objects for targeting purposes [26, p. 72]. Unofficial evaluations suggest that over 98 percent of the targets defeated outside of the combat area of the targeting in the last decade were made using these platforms [27, p. 8].

In the years 1990-1991, during the Gulf War and the 1999 Kosovo operation, the United States significantly accelerated the introduction of various types of precision weapons and ISR (Intelligence, Surveillance and Reconnaissance). The development of resources was so dynamic that Russian general Vladimir Slipochenko described the new approach to warfare as "sixth generation combat operations"[11]. It is estimated that China and Russia have great

[7] Hierarchical domains will constitute the basic type of information domains. Their structure will be in line with the adopted structure of the armed forces. It was assumed that each unit should have its own information domain. For this reason, the lowest level of these domains, e.g., in land forces, would be a battalion (squadron). The hierarchical domains will be the primary domains in which the original information will be stored.

[8] Specialist domains will be responsible for access to information within the framework of individual types of troops, taking into account the adopted hierarchy of command and the needs of cooperation. They will be created on the basis of hierarchical domains thanks to the appropriate configuration of their system.

[9] Task domains will group information developed by units involved in the performance of a specific task.

[10] Spatial domains will contain information from units located in the selected area. These domains will be created by appropriate system reconfiguration.

[11] It should be noted that in the exercise "Zapad" conducted in 2013, the Russian Armed Forces tested the wide use of various types of unmanned aerial vehicles for the purpose of collecting data on objectives and tasks in the field of intelligence, surveillance, and reconnaissance (ISR), thus supporting the activities of

capabilities to perform precision weapon strikes and are also the owners of ISR funds. Probably also non-state actors such as Hezbollah have the ability to attack Israeli IDF (Israeli Defense Forces) corvettes, as was evidenced by the use of Chinese C-802 guided missiles [28, p. 134].

The third direction is the organizational change of command bodies. In principle, there is no doubt that the staffs together with commanders will play the main role in the command of troops in future operations. The effective use of the separate components of the armed forces will largely depend on the efficiency of the entire staff and the ability to use modern technologies supporting the command process. It can be assumed that in the future, due to the large scope of automation of many processes, it will be necessary to limit personnel and means of command.

4. Recommendations for the command system in future military operations

The assessments of military specialists in the field of command organization expressed during individual interviews provide the basis for the conclusion that in relation to armed conflicts in the future, three main problems should be considered and answered[12]:

First, *is it possible to reduce the number of levels of command?*

When observing the increasing number of combatants, it seems almost unrealistic, because the future commander (combat organizer) will not only command five directly subordinate units, but also the reinforcement units temporarily subordinate to individual levels in the organic command system. Therefore, network-centrism is the solution to many problems of the command organization. Thus, the commander will be obliged to simultaneously coordinate many activities with the staffs of the operational units from which the reinforcement units were separated. Besides, command will become increasingly complicated as each new combat system is put at disposal. Moreover, the command system will require an increased amount of information processed electronically in computer networks, and thus will be more susceptible to cyberattacks.

Second – *how many command positions are needed at each level of command?*

It can be assumed that in future armed conflicts the principle of organizing forward and main command posts at tactical levels will be maintained. Such a solution seems to be necessary and justified, if only because of the dynamics of military operations and the multidimensional threat to command positions (physical, cyber, and psychological attacks). However, when organizing main, backup, rear, and forward command posts at the same time, considerably large personnel and numerous safeguards must be considered. Therefore, to improve the organization of the command system, one should not exclude the taking over of staff functions by automatic machines working in parallel with people at backup command posts. In this situation, in the context of cyber-wars, the threat to telecommunications systems will increase and it will be necessary to have specialized IT security and trained crews of staff and command vehicles.

Third – *how mobile should the command post be?*

Observing the dynamics of actions in the past armed conflicts, it can be presumed that the requirements for maintaining constant command capacity and high mobility of main

the air and land forces. The Russians successfully used unmanned aerial vehicles to coordinate activities of land forces, including self-propelled tube and rocket artillery and missilery.

[12] The presented problems were part of the interviews conducted.

command posts must be undoubtedly respected. The ability is necessary, especially in the case of frequent changes in the SD position, in accordance with the movement of troops to maintain continuity of command. Moreover, it is conditioned by the dynamics of military operations, the conditions of operations, and the specificity of the operating environment.

Therefore, it can be assumed that the rule will probably be to develop command posts within the boundaries of urbanized areas (currently over 80% of command posts are developed in localities). However, assuming the elements of the command posts are constantly exposed to the enemy's influence, the functional elements will be located on armored vehicles, where workplaces will be organized in container cabins, protecting against radiation and securing the means of command against the cybernetic incapacitation of the enemy. The high mobility requirement will be maintained for all command levels in future operations, taking account of the full transport capacity of the vehicles. Summing up, the dynamics of future conflicts may make the mobility of command posts a condition necessary for combat effectiveness.

The presented developments in the command system obviously provoke reflection. They are the basis for generating conclusions, regardless of the type of armed forces. The collected generalizations show that there is a clear tendency towards decentralization of command positions. The possibility of conducting military operations in a cyber environment is also noticed and implies many decisions to safe and efficient use of the means of command. At the same time, the process of implementing new technical solutions supporting the command process is being observed.

Conclusion

The analysis and evaluation of the development of command structures and procedures in the North Atlantic Alliance shows that, as part of its adaptation to the new, expanded spectrum of tasks, the military structures of NATO commands and forces, as well as the political structure of command have been transformed.

Bearing in mind the need to adapt the command system to the needs of future operations, the activities undertaken should focus on:

a) increasing the lifetime of the command system due to the decentralized structure of functional subsystems and the use of mobile telecommunications elements,

b) improving the efficiency of technical equipment and communication devices resulting from the use of modern technologies for the construction of sensors, means of data transmission, and processing,

c) increasing the efficiency of information transfer in the command system due to the optimization of the use of new information technologies,

d) integration of the command systems of the components of various types of armed forces.

A new command system will be essential for the integrated information system, for which the management subsystem will be built to optimize its size and technical complexity. The integration of different command posts in future operations can be accomplished by linking individual SDs tightly with a data stream or by creating a common communications network for all users (the domains concept mentioned above).

Despite the technical development of the command means, the division of command levels will still result directly from the organizational structure of the armed forces. Currently, an organizational change is noticeable, aimed at the transition of the armed forces to universal structures, ensuring the work of the SD in times of peace, crisis, and war. The quantitative and qualitative changes in the technical equipment of command units resulted in some organizational changes. Nonetheless, it did not cause any significant changes in the scope of tasks and competences of commanders or the organization of command posts Meanwhile, the collected conclusions indicate that in future operations the number of subordinate units will be increased, which will force the commander to change command posts more often and give orders earlier. Moreover, the experiences from the conflicts in Iraq and Afghanistan prove that the increased number and variety of means of combat and the expansion of the spectrum of their impact require directing a fight carried out by many entities, both military and civilian, including private military companies. Therefore, the aim of changes in the organization of the future command system should be to fully integrate the possibilities of reconnaissance, control, and impact in the flexible concept of future task forces. Summing up, the future command system should enable a quick transition from an operational development from a conventional armed conflict against state opponents and the implementation of individualized military actions in unconventional (hybrid) war scenarios against non-state actors.

Acknowledgement

The article was financed under the research task “The process of military threat assessment using the scenario method” (code: II.3.10.0; bursary 559).

Conflict of interests

The author declared no conflict of interests.

Author contributions

The author contributed to the interpretation of results and writing of the paper. The author read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Marek Wrzosek https://orcid.org/0000-0002-1369-9434

References

1. Orzechowski J. *Dowodzenie i sztaby*. Warszawa: MON; 1974.
2. Piotrowski S. *Dowodzenie w działaniach taktycznych wojsk lądowych*. Warszawa: AON; 1995.
3. Mossor S. *Sztuka wojenna w warunkach nowoczesnej wojny*. 3rd ed. Warszawa: MON; 1986.
4. Ścibiorek Z. *Wojna czy pokój*. Wrocław: Ossolineum; 1999.
5. Wiener N. *Cybernetyka czyli Sterowanie i komunikacja w zwierzęciu i maszynie*. Warszawa: PWN; 1971.
6. Pszczołowski T. *Mała encyklopedia prakseologii i teorii organizacji*. Wrocław: Ossolineum; 1978.
7. Ścibiorek Z. *Podejmowanie decyzji*. Warszawa: Agencja Wydawnicza Ulmak; 2003.
8. *Encyklopedia organizacji i zarządzania*. Warszawa: PWE; 1981.
9. Stoner JAF, Wankel C. *Kierowanie*. Warszawa: PWE; 1992.

10. Krzyżanowski L. *Podstawy nauk o organizacji i zarządzaniu*. Warszawa: PWN; 1994.
11. *Regulamin działań taktycznych wojsk lądowych*. Warszawa; 2008.
12. Posobiec J. *Dowodzenie w środowisku sieciocentrycznym*. Warszawa: AON; 2008.
13. Huzarski M, Wołejszo J (eds.). *Leksykon obronności. Polska i Europa*. Warszawa: Bellona; 2014.
14. Krzyżanowski L. *O podstawach kierowania organizacjami inaczej: paradygmaty, metafory, modele, filozofia, metodologia, dylematy, trendy*. Warszawa: PWN; 1999.
15. Posobiec J. *Kontrola w dowodzeniu*. Warszawa: Wydawnictwo Menadżerskie PTM; 2013.
16. *Planowanie działań na szczeblu taktycznym w wojskach lądowych. DD/3.2.5*. Warszawa: Dowództwo Wojsk Lądowych; 2007.
17. Balcerowicz B. *Wojny współczesne. Wojny przyszłe*. Myśl Wojskowa. 2003;5.
18. Wrzosek M. *Wojny przyszłości. Doktryny, technika, operacje militarne*. Warszawa: Fronda; 2018.
19. Wrzosek M. *Operacje w cyberprzestrzeni. Założenia teoretyczne i praktyka*. Kwartalnik Bellona. 2016;4:42-59.
20. Czulda R. *Obrona przez atak*. Polska Zbrojna. 2009;33.
21. Rybicki R. *Prawo do cyberobrony*. Polska Zbrojna. 2009;35:44-5.
22. Rybarczyk M. *Mundur dla hakera*. Newsweek. 02.09.2007:32-5.
23. Wrzosek M. *Jakość informacji w konfliktach militarnych*. Problemy jakości. 2018;1:2-8.
24. Dela P. *Domeny informacyjne a zarządzanie informacją w środowisku sieciocentrycznym*. Przegląd Wojsk Lądowych. 2009;2(020):41-7.
25. Etzioni A. *The Great Drone Debate*. Military Review. 2013;93(2).
26. Callam A. *Drone Wars: Armed Unmanned Aerial Vehicles*. International Affairs Review. 2010;18(3).
27. Zenko M. *Reforming U.S. Drone Strike Policies*. Washington, DC: Council on Foreign Relations; 2013.
28. Paździorek P. *Wojskowa myśl operacyjna w konfliktach zbrojnych przełomu XX i XXI wieku*. Toruń: Wydawnictwo Adam Marszałek; 2016.

Biographical note

Marek Wrzosek – Col. (ret.), Prof. Dr. hab., Professor of the Military Department of the War Studies University. In 2007-2015, he was the Deputy Dean of the Faculty of Management and Command of the National Defense University in Warsaw. Then, until September 2017, Vice-Rector for Research at the National Defense University, and then the War Studies University. For many years in his professional, didactic and scientific work, he has been dealing with issues related to the military reconnaissance system, information processes, and in particular – the assessment of military and non-military threats. He is the author of numerous theoretical and practical studies. He is an implementer and participant of scientific and research works and projects, including those involving foreign entities.

Wyzwania współczesnego dowodzenia a przyszłe operacje militarne

STRESZCZENIE

Celem artykułu jest identyfikacja wyzwań przed jakimi stoi system dowodzenia w kontekście zmian kształtujących przyszłe operacje militarne. Do prezentacji wyników poznawczych wykorzystano metodę analizy badania dokumentów oraz wyniki badań prowadzonych za pomocą sondażu diagnostycznego, metodą wywiadu, jak również obserwacji niestandaryzowanej. Struktura artykułu obejmuje cztery zasadnicze zagadnienia. W pierwszym przedstawiono relacje terminów „kierowanie – zarządzanie – dowodzenie” w kontekście czynionych rozważań. Drugie zagadnienie koncentruje się na charakterystyce operacji przyszłości określających wyzwania dla dowodzenia. Natomiast trzecie zagadnienie wyjaśnia kwestie związane z modyfikacją dowodzenia w przyszłych operacjach militarnych. Zagadnieniem dopełniającym całość prowadzonych rozważań jest próba rozstrzygnięcia kwestii rekomendacji dla systemu dowodzenia w wojnach przyszłości. W treści artykułu wykorzystano wnioski z doświadczeń uzyskane w czasie konfliktów militarnych w Iraku i w Afganistanie.

SŁOWA KLUCZOWE dowodzenie, operacje militarne, wojny przyszłości, walka informacyjna, operacje sieciocentryczne

How to cite this paper

Wrzosek M. *Challenges of contemporary command and future military operations*. Scientific Journal of the Military University of Land Forces. 2022;54;1(203):35-51. DOI: 10.5604/01.3001.0015.8025.