CNA

Special Issue | September 8, 2022

A biweekly newsletter on AI and autonomy developments in Russia

CNA Russia Studies Program

Translations of Russian Military Journal Articles on War, AI, and Autonomy This issue of *AI and Autonomy in Russia* features translations of several Russian military journal articles that reflect on the use of AI and autonomy. All have been written since the Russian invasion of Ukraine.

The first article, “Transforming the Content of War: Contours of Future Military Conflicts,” takes a broad look at how conflict is evolving. It gives a historical perspective, leading up to the current day, and forecasts conflicts to come. We find that it reflects much of the thinking among Russian military writers today.

The second article, “Counter-Drone Systems: A New Technical Level and Integrated Approach,” highlights the relatively recent massive introduction of UAVs on the modern battlefield, noting their use in Syria, Nagorno-Karabakh, and, finally, the Russia-Ukraine war. The article discusses the dangers to troops from the proliferation of UAVs and the difficulty in countering that threat. It offers a model for integrating various capabilities as a possible solution to threat from UAVs.

The final article, “On Legal Regulation of Artificial Intelligence Application in the Military Sphere,” surveys the application of AI to military systems in both the United States and Russia. It then argues that developments of military AI are far outpacing domestic and international regulation. Finally, it offers recommendations on possible regulatory initiatives for military AI.

THIS WEEK'S CONTENTS

TRANSFORMING THE CONTENT OF WAR: CONTOURS OF FUTURE MILITARY CONFLICTS

(Трансформация содержания войны: контуры военных
конфликтов будущего)

Lieutenant General A.V. SERGEANTOV, Doctor of Military Sciences
Major General A.V. RESIN, Candidate of Military Sciences
Reserve Colonel I.A. TERENTIEV, Candidate of Military Sciences

Voennaya Mysl, no. 6 (2022): 19-30

Abstract: The paper shows changes in the nature and content of military conflicts, the prospective model of power changing techniques, the main types of military conflicts, the novelty of future operations and the space of hostilities, classifying military conflicts of the future and their basic principles.

Keywords: Military conflicts of the future, hybrid activity, transformation, non-military measures, military activity, technologies, informational confrontation, sea-air-space, theater of operations, noncontact warfare, national security.

The ongoing global processes again call into question the relatively peaceful development of human civilization. In this regard, the question of the transformation of 21st century military conflicts is being actively discussed in scientific and research circles, which is associated with an increase in the use of non-military measures and the introduction of new technological solutions.

An analysis of the views of the military-political leadership of a number of Western countries regarding "hybrid" tools allows us to talk about their use in the development of crisis situations in their own interests. At the same time, an appearance of impartiality is created, and direct involvement in armed confrontation is hidden. The military conflicts of the future will most likely be determined by the political and economic interests of various states in the context of the struggle for resources and geopolitical dominance in strategically important regions of the world.

The formation of military policy aimed at developing the parameters of the optimal military potential of the state depends on the definition of their nature. Today, the military expert community agrees that in the foreseeable future (until 2030), the outbreak of large-scale wars is unlikely. At the same time, regional, local wars and armed conflicts with limited goals are predicted, as well as the use of military force to neutralize the threats that have arisen. Under these conditions, the views of the military-political leadership of the leading states on the use of military force and the development of armed struggle are being improved. All changes are embodied in the theoretical foundations of wars and armed conflicts, and are implemented in conceptual and doctrinal documents that define a very specific adversary.

First of all, states are identified that are likely to be encountered in defending and implementing their national interests, and the degree of their determination in achieving their goals is assessed. Their level of development of science is taken into account, which ensures the creation of new, and modernization of existing types of weapons, military and special equipment, as well as the state's economic potential. In the future, based on an analysis of trends in the changing nature of military conflicts, a scenario base is formed for unleashing and conducting military operations in the future.

However, in conditions of a certain blurring of the boundaries between peace and war, such an approach is clearly not enough. It is necessary to work out not only the conduct of wars and armed conflicts, but also the use of military force in interstate confrontation in the interests of deterring a potential aggressor from military escalation, while disrupting his efforts to achieve his goals through "hybrid" actions. In the future, the meaning and time intervals of the initial, subsequent and final periods of war and armed conflicts will change. They will be transformed. At the same time, a special role is assigned to the period preceding the start of the military conflict, which is characterized by an extreme aggravation of interstate relations in various fields, an increase in the military threat, and the emergence of conditions for the outbreak of hostilities.

During this period, economic, financial and diplomatic instruments of pressure on the enemy are actively and widely used. In the wars of the past, these measures were applied fragmentarily and often did not have a significant impact on their outcome. Today, they are being transformed at a new qualitative and technological level. First of all, this is due to the development of information technologies implemented in the virtual space in the form of behavioral, cognitive, mental and cybernetic wars. In the future, they will become of paramount importance in order to create the most favorable conditions for achieving strategic goals. The development of information warfare is manifested not only in the information and technical plan, but also in improving the methods of influencing both the armed forces and the population of the enemy country.

Its activity, scale and aggressiveness are increasing. The side that succeeds in winning and maintaining dominance in the virtual domain will create conditions for the realization of its national interests. There is a tendency to replace the period of increasing aggression with a phase of "controlled chaos", used to change the main geopolitical potential of the state—the national mentality, culture, and morale of people. As an example—the attempted coup in Kazakhstan in January 2022. In military conflicts of the future, the opposing side will seek to use military force against a weakened enemy, creating an artificial crisis. This is the only way to achieve your goals without significant losses.

To inspire crises, the use of methods of non-linear influence on political and economic processes arising from an unstable (chaotic) situation is not excluded. (Inspire—cause something by suggestion, incitement, instigation). When such a situation is "swinging", there is a high probability of using "aggravating" factors: dissatisfaction with the existing government, infringement of the rights and freedoms of citizens, social stratification of society, the imposition of "new democratic values" instead of "wrong" democracy, the use of man-made accidents and disasters, the spread of epidemics, the use of the Internet, artificial maintenance of crisis situations and others. After all, the desire of the aggressor state for world domination is not based at all on the desire to deepen freedom and democracy, rid countries of violence and poverty, but on superiority of its economy, politics and ideology, and then their complete control. Consequently, the power of world elites in this way is aimed at solving the main task of their foreign policy—the elimination of competitive states that are gaining political and economic weight. All this represents the messianism of US foreign policy, the goal of which is complete domination in the world.

At the same time, the main focus is on the use of destabilizing factors in the interests of artificially creating crisis regions with the formation of governments under control, acting in parallel with the legitimate authorities. In addition, the future model of power change technologies can combine both proven non-military measures and military solutions, including the mobilization of protest potential, "color" revolutions, actions in the "gray zone", "revolutions of social networks", the creation and use of new weapons and military strategies. Such a scenario has already been used in Libya, it was assumed in Syria and Venezuela. The forceful intervention of the United States and its allies in Libya led to the actual split of society and the destruction of state foundations.

However, the repetition of the Libyan events in Syria was disrupted by the timely appearance of the Russian Armed Forces. It is obvious that crisis situations become an element of interstate confrontation, are artificially created in the interests of achieving their interests in strategically important regions, and pursue the containment of a rival state capable of pursuing an independent foreign policy and resisting American hegemony. It is assumed that the beginning of the active phase may be due to the degree of weakening or loss of the combat potential of the enemy's armed forces. It will represent short-term stages of a massive complex and selective impact, applied simultaneously in all spheres and throughout the entire territory of the state. After all, not only physical spheres of confrontation, but other types of weapons appear, for which the priority is not the physical, but the functional defeat of the enemy.

For example, the state, which is a recognized leader in high technologies, creates on their basis a complex system of command and control of troops and weapons for conducting military operations. And the more complex the system, the more vulnerable elements in it, the destruction and suppression of which will achieve the goal.

Next. The boundaries between the strategic, operational and tactical levels are blurred, which implies the conduct of military operations by autonomous, self-sufficient inter-service groupings of troops (forces) capable of successfully operating in remote areas (zones), using the potential capabilities of forces and means in the aerospace domain, at sea and in cyberspace in order to strike at critically important objects, creating conditions for the further development of the success of the operation. At the same time, the role of special operations and special forces is increasing, and the range of tasks they perform is expanding.

In general, it can be stated that military threats to Russia in the medium and long term will grow. Russia can be drawn into military conflicts of various scales, including with the use of nuclear weapons. It is predicted that in the future any military conflict will end with the implementation of measures to restore the peaceful life of civil society, political, economic and social structures in the territory where the hostilities took place, the period of the so-called post-conflict settlement.

In future geopolitical conditions, the problem of resolving military conflicts will be incredibly difficult and will require enormous efforts by the international community. Post-conflict settlement will become an important element of the diplomacy of the leading countries and international political associations, which will consider it as an effective way to promote their national interests. The Armed Forces in the post-conflict settlement can solve a wide range of tasks—from neutralizing the sources of the threat of the resumption of the military conflict to the temporary replacement of civil society institutions (systems of state administration).

“Crisis situations become an element of interstate confrontation, artificially created in order to achieve their interests in strategically important regions and pursue the containment of a rival state capable of pursuing an independent foreign policy and resisting American hegemony.”

One of important direction is the improvement of humanitarian actions in order to provide the civilian population of the conflicting parties with food, clothing, medicines and other essentials. Another topical area is related to assistance in organizing and holding democratic elections in the interests of the population.

The stages considered (artificial crisis; active phase, including the possibility of using nuclear weapons; post-conflict settlement) in one variation or another will form the main expectation of interstate confrontation in military conflicts of the future. At the same time, the predictable nature and their content show that, despite the increasing role of non-military measures in interstate confrontation, the main thing remains the sufficient and necessary use of military force at all stages of the development of the military-political environment.

Summarizing, we can say that the change in the nature and content of the war, which determine the significant difference between the ideology of their conduct and the wars of the past in terms of declared goals, an expanded list of participants, the emergence of new areas of confrontation, the weapons and military equipment used, means and methods of confrontation, forms and methods of conducting military operations, in fact, determine the contours of military conflicts of the future.

Moreover, despite the seemingly identical nature of wars and armed conflicts, their content can and will radically differ from each other, such as by the following criteria:

- the level of development of the opposing states, its economic and, as a result, technological potential;

- the level of training and equipment of the armed forces of the opposing states with weapons and military equipment;

- goals planned to be achieved, both declared and hidden;

- the achievement of goals by the participants in the conduct of hostilities;

- the chosen strategy and methods of conducting military operations to achieve the goals.

On this occasion, back in 1926, in his work “Strategy”, A. Svechin wrote: “For each war, it is necessary to develop a special line of strategic behavior, each war is a special case requiring the establishment of a special logic... "

At the same time, it should be borne in mind that, despite such a difference, military conflicts of any type and scale will certainly be characterized by a number of common characteristics, determined by the desire of the military leadership to use the most successful methods and action in the course of hostilities based on the analysis and generalization of military experience. These features include:

- widespread use of special operations forces;

- the use of asymmetric, non-standard methods of military operations;

- active information and psychological impact on the enemy;

- active use of unmanned and robotic means;

- conducting combat operations by small autonomous mobile formations, etc.

However, despite the existence of such common characteristics, their implementation is determined, in fact, by the availability of appropriate opportunities, primarily economic, for states and other subjects participating in a military conflict. The content of military conflicts involving states that are underdeveloped economically and technologically will be based on confrontation using guerrilla, sabotage and terrorist methods. At the same time, an asymmetric approach will be widely used as the basis for the strategy of conducting a military conflict.

This kind of strategy for conducting a military conflict is being actively used at the present time and, given the existence of states that are diametrically developed (as opposed to the Western economic model) economically, which also determines their military power, it will be successfully used in future military conflicts. As possible participants in military conflicts of this kind, there can also be non-state entities (the so-called pseudo-states, such as ISIS in Syria or the Taliban in Afghanistan), which do not have a military potential equal to the military power of a developed state.

As a goal of war, such subjects of wars, as a rule, formulate political slogans, for example, the formation of a single state on a confessional approach—a world caliphate, the unification of the territories of different states for the reunification of divided peoples, the promotion and protection of their national views that are not correlated with national features of development other states, etc. Often these slogans hide other, true goals of the war, primarily economic ones. However, in a number of cases, economic goals can be ignored and not taken into account in favor of views on the national characteristics of the country's development, purely subjectively declared by the leaders of these states or associations. The main means of achieving certain goals in military conflicts of this kind will be both the regular armed forces and the rebel detachments, mercenaries, armed opposition, and religious radical fanatics in pseudo-state structures.

The number of informal military structures, as a rule, is quite small, compared with the armed forces of developed states. Heavy weapons are usually absent or available in small quantities. This also determines the strategy for their use in a conflict—actions in small autonomous mobile groups, combining the tactics of guerrilla, sabotage and terrorist warfare: attack, strike, withdrawal with dispersal, collection in a designated area. In essence, this is a land-based transformation of the naval tactics of the "wolf packs" of Admiral Doenitz in World War II.

However, this tactic also has an obvious disadvantage. The great independence of the leaders of these formations often leads to the emergence of conflict situations between them, inconsistency in actions and, as a result, low efficiency of their application. This problem can be solved if there is a sufficiently powerful authoritarian center, which should coordinate the actions of independent formations. However, on the other hand, its presence is a weak link in the control system, since the destruction of a critically important control element will lead to a complete disorganization of control and coordination of the actions of such formations. Undoubtedly, this should be taken into account by the opposing side when developing a counteraction strategy in the course of hostilities.

At the same time, it should be taken into account that the existing certain weakness in armed struggle due to the economic or political impossibility of acquiring modern and promising means of armed struggle, these states will seek to level through the use of a strategy of asymmetric actions.

Military operations involving high-tech and economically developed states will, as a rule, be based on the application of a strategy of destruction. Their basis will be non-contact actions. But even in such actions, it becomes relevant to use the advantages of new areas of confrontation, especially the information domain, actions in which, in the era of modern rapid technological breakthrough in a number of areas focused on the production of information means of confrontation, are becoming especially in demand. Their use will destroy the mental component of the opposing side, reduce the moral and psychological stability of the enemy. It cannot be argued that this kind of influence is something absolutely new in the field of war.

Even Clausewitz in his work "On War" wrote that "the destruction of the enemy armed forces should not be limited to the destruction of material forces alone, the destruction of moral forces is implied." For the moral element is the most affected and determines the stability of the army as a whole.

At the same time, the breakthrough development of information technologies has allowed actions in the information sphere to reach a fundamentally new level of their implementation and become an almost independent domain of confrontation, which, under certain conditions, can have a significant impact on the achievement of war goals.

It was these circumstances that served as the basis for the rapid development and renewal of various warfare strategies. If initially two well-known strategies dominated the world: destruction and attrition (their active supporters in our country were Tukhachevsky and Svechin, respectively), then by the beginning of the 20th century other, fundamentally new strategies for waging war appeared, based both on the use of new means of armed struggle, and on a complex combination of various types of military forces and the methods of confrontation in a war implemented in this case: a global nuclear strike, nuclear deterrence, preventive actions, indirect actions, etc.[1]

Moreover, the main goal of this kind of warfare is not to destroy as much of the enemy's military force as possible, but to create conditions when their use becomes ineffective, which ultimately leads to the defeat of the enemy state in the war as a whole. The need to implement such updated strategies will require new approaches to planning and conducting operations. Their spatial and temporal parameters, the composition of the troops (forces) involved and the distribution of functions between them will change.

The novelty of future operations will be determined primarily by the transfer of armed struggle to new spaces—real and artificially created ("gray zones", crisis regions). The concept of a theater of war will lose its exclusively geographical meaning and will be perceived as a combat space that unites land and water areas, often separated by hundreds of kilometers, the atmosphere, space, and the information environment.

The main theater of war will be aerospace and sea domains. It will be widely used for non-contact strikes and ensuring the actions of troops (forces). Without gaining superiority in air and space, it will become impossible to achieve a sustainable advantage on land and at sea. In the course of aerospace operations, the greatest damage will be inflicted on the enemy, therefore, in terms of their significance, they will begin to dominate the actions of the ground forces. Information warfare is also becoming an integral part of hostilities. Without an advantage in this area, even a militarily stronger side will face serious difficulties in organizing and conducting hostilities.

In technical terms, the destruction of the control system is considered as an important condition for inflicting defeat on the enemy. Even before the start of hostilities, complete information superiority must be won, and the main task is to achieve lightning-fast, anemic strategic and operational paralysis of enemy's command and control.

Disruption of communication lines, massive failures in the operation of computers, failures of other radio-electronic equipment will not allow the opposing side to conduct combat operations in an organized manner. First of all, enemy military-political leadership, military personnel and civilian population will be subjected to massive psychological impact in order to push them to consciously or spontaneously commit certain actions.

Active propaganda will be directed both at its own population and at the inhabitants of "third countries" in order to create favorable domestic and foreign political conditions for further conduct of the war.

[1] CNA Note: The reference to Tukhachevsky and Svechin reaches back to a debate in Russia in the 1920s between strategies that advocated for seeking a decisive destruction against an adversary versus winning through a war of attrition. For more, see Richard W. Harrison, *The Russian Way of War: Operational Art, 1904-1940* (Lawrence, KS: University Press of Kansas, 2001), 129-33.

The high effectiveness of means of destruction and the dynamics of changes in the situation in the course of armed struggle will increase the cost of managerial errors, and in some cases will not leave time and resources to correct them, so the need for proactive intelligence information will rapidly increase. To reduce the time delay between the receipt of information and its implementation, reconnaissance and destruction means will be integrated into single systems by telecommunication networks linking spatially distributed elements.

The high dynamics of military operations and the accuracy of management decisions corresponding to a complex strategic and operational situation will be ensured by systems based on artificial intelligence. This is the reality of tomorrow. There are developments that allow considering the elements of artificial intelligence of some weapon systems that can interface them with control, reconnaissance and navigation tools.

The first steps in this direction have already been taken by domestic scientists, and they are based on a modern technological base. At the same time, the sequence of defeating the enemy will change: if earlier it began with a decisive offensive against the border groupings of ground forces, then promising weapons will make it possible to disable the most important elements of the administrative and military control system, the military-industrial complex, transport and energy during the first and initial operation.

Military operations in future wars will become more difficult to classify on the basis of their belonging to the strategic, operational or tactical levels, since the activity on each of them will have a direct impact on the situation as a whole. This happened before, but now the close interconnection of events at the local, regional and global levels has become the norm.

The battlefield is transformed into a kind of strategic (operational) space, divided into small "fields". When conducting hostilities, there will be an effect of "small" battles between fully or partially autonomous groups. They can be separated by territory containing non-combatants, potential adversaries, and life support facilities for the population. As a result, the possibility and necessity of creating a continuous line of contact between troops (forces) will disappear, which will have to be in constant readiness for a contact with the enemy, a quick transition from offensive to defense and vice versa. Superiority in each specific case will be created not by the number of troops (forces), but by their mobility and the reach of weapons. Operations and systematic combat operations to block the zone of military conflict and establish an embargo regime will become widespread.

The importance of operations to ensure the security of the territory and the population from various destructive impacts on critical infrastructure facilities will increase. It is expected that such an impact will be carried out in the form of sabotage, cyber attacks and targeted strikes using high-precision weapons and weapons based on new physical principles. At the same time, the formation of promising strategies can be based on the following classification of military conflicts of the future:

- "classic"—using strategies to crush the enemy;
- "asymmetric"—using the strategy of indirect actions;
- "hybrid"—combining the use of classical and asymmetric methods.

The forms of military operations, in addition to classical combined-arms operations and battles, will be urban riots, well-prepared uprisings supported by the strategy of "controlled" chaos, terrorist acts and covert operations inspired from abroad, affecting mainly society of the enemy state. At the same time, the growing trend of moving military confrontation into the information sphere in order to manipulate public opinion and influence automated control systems and computer networks necessitates the development of information weapons capable of exerting a leading and uncompromising impact on the enemy.

A very delicate issue concerns a fundamentally new type of military conflicts—behavioral, the emergence of which has become possible only recently due to the accumulation of huge arrays of objective information about human behavior, including the behavior of social and other groups of arbitrarily large dimensions. In addition, human behavior to a large extent not only depends on our ideas, values, beliefs, but is also based on stereotypes and habits, and is also formed under the influence of formal and informal institutions.

They are based on the manipulation of the society, as well as our own biography and cultural environment, with algorithms of behavior, habits and stereotypes of activity. The toolkit of behavioral warfare is to separate the habit from the established type of activity that formed its situations and use behavioral algorithms to achieve other goals.

The behavioral weapon is the weapon of tomorrow. It is for this purpose that the super-giant center belonging to the National Security Agency exists in Utah, put into operation in terms of its information capacity, and is constantly “sharpened”, accumulating arrays of behavioral information from all countries of the world and on all continents. This classified new type of weapons is where part of the American elite's greatest hopes are in the tough confrontations of the future.

In addition to behavioral weapons, the emerging dynamics in the advanced countries in the development of technologies that implement military operations in space requires accelerating the development of space weapons that will perform both anti-missile functions and the functions of long-range high-precision weapons. Space technologies in the future, no doubt, will play the role of a factor in the strategic deterrence of a potential adversary. Thus, with a decrease in the likelihood of unleashing a large-scale war, military conflicts of the future are most likely to be associated with the fight against terrorism, the conduct of "hybrid" actions in the "gray zone", asymmetric actions, local, regional and other, as yet insufficiently studied wars and armed conflicts with a real possibility of limited use of nuclear weapons.

To achieve political and strategic goals, stakes will be placed on "non-contact" warfare, the widespread use of various systems of high-precision "smart" weapons for various reasons. At the same time, the “non-contact” nature of military operations implies the destruction or incapacitation of the enemy at long distances long before combat contact. Ideally, enemy troops should not leave their places of permanent deployment at all, or, in extreme cases, they should be destroyed on advance routes. This, of course, is possible only under the condition of absolute information awareness, first of all, about the enemy, his plans and intentions.

One of the key factors for achieving victory in a military conflict of the future is the correct distribution of priorities for influencing the enemy’s goals and objects: initially, the impact will be on the political leadership and leaders of the state, then on its life support systems, subsequently on the infrastructure, economy, population, and finally, the armed forces. In this case, the opposing sides will use various and sophisticated strategies, methods, methods, tactics and new technologies.

Promising combat (strike) systems will be able to hit the enemy by unconventional methods at ranges that significantly exceed the capabilities of existing enemy weapons, which, in turn, will expand the boundaries of the areas of operations. In general, in the medium and long term, the struggle between technologies themselves and between technologies will come to the fore. In the military conflicts of the future, the one who has the most advanced technologies and is available for mass production will win. Such technologies will make it possible to plan and implement their active use in new military strategies, forms and methods of influencing the aggressor.

Considering that the main threat to national security is no longer limited to the enemy's military aggression against the country's geographic space, it is necessary to “expand” the new concept of ensuring state security (political, economic, informational, cultural and other security). To win, you need to "go beyond"—a completely new method of conducting a future military conflict.

In this case, such a conflict may be inherent in the following basic principles:

• omnidirectionality (comprehensive assessment and combined use of all related factors);

• synchronicity (simultaneous actions in different areas);

• limited goals (compliance of goals with opportunities);

• unlimited measures (tendency towards unlimited application of measures, limited by the achievement of limited goals);

• asymmetry (search for the main site of action in the opposite direction from the symmetry equilibrium contours);

• minimum consumption (use of the smallest sufficient amount of combat resources to achieve the goal);

• comprehensive coordination (coordination and cooperation of various forces in various fields to achieve a specific goal);

• control of the entire process (use during the entire conflict of the information received for the timely introduction of changes in further actions).

The main rule of the military conflict of the future will be the absence of any rules: nothing is forbidden. The military conflict of the future will be a combination of methods implemented by force of arms or without it, as well as a diverse use of methods of interstate confrontation with the sole goal of forcing the enemy to submit to the attacker’s will.

At the same time, I would like to emphasize that the military conflicts of the future will not be limited only to the sphere of armed struggle. The implementation of confrontation along with armed struggle in other spheres will become their indispensable condition. It is this circumstance that underlies the fact that the world is entering a period of wars of a new generation, aimed not at the direct destruction of the enemy, but at creating, through the implementation of complex measures, conditions when the use of mass armies will be not only ineffective, but also inexpedient, which will allow achieving political goals without global military battles.

It is this circumstance that underlies the fundamental change in the nature of modern wars, leaving an imprint on the transformation of the content of war in its static nature.

COUNTER-DRONE SYSTEMS: A NEW TECHNICAL LEVEL AND AN INTEGRATED APPROACH

(Система борьбы с беспилотными летательными аппаратами — новый технический уровень и комплексный подход)

Lieutenant General G.V. YERYOMIN, Candidate of Military Sciences
Colonel S.N. CHORNY, Candidate of Technical Sciences

Voennaya Mysl, no. 7 (2022): 32-40

Abstract: The paper examines issues of countering small-size drones, ways of improving the means and system of combating these drones by the Ground Forces, and also actions by specialized subunits to counter use of unmanned aerial vehicles.

Keywords: Small drones, system of comprehensive fight against unmanned aerial vehicles, modes and tactical methods of actions by specialized units of combating unmanned aerial vehicles, reconnaissance, striking and electronic suppression of unmanned aerial vehicles.

The experience of recent military conflicts (Libya, Syria, Nagorno-Karabakh, Ukraine) indicates an increase in the use of unmanned aerial vehicles (UAVs) in military operations, an increase in the proportion of UAVs used as strike weapons, target designation equipment for high precision weapons (PGMs) and artillery fire correction equipment (Fig. 1).

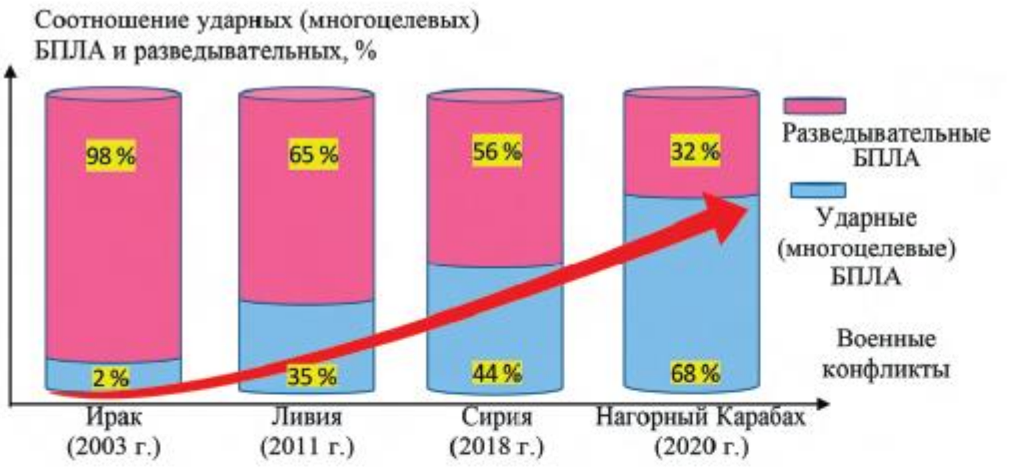


Рис. 1. Соотношение доли ударных (многоцелевых) и разведывательных БПЛА в военных конфликтах

[Fig. 1: Percussion share ratio (multi-purpose) and reconnaissance UAVs in military conflicts]

As a result, conditions are created that allow countries that do not have powerful armed forces to radically change the course of a military conflict in their favor due to the competent use of UAVs.

Considering UAVs as countermeasures used for air defense (AD), it should be noted that while the characteristics of heavy and medium UAVs are comparable to the characteristics of typical airborne targets (AT) for air defense systems, small UAVs have significant differences, including defining them as complex objects due to their low optical, infrared, radar and acoustic visibility/signature, the capability to operate at extremely low altitudes with low flight speed, as well as their use in large groups.

At the same time, these UAVs are characterized by easily detectable radiation from ground control stations (GCS) and onboard radio-electronic equipment (REE) at the stage of executing combat and special tasks; high sensitivity to the impact of organized radio interference both through control channels and through radio-navigation channels (especially those of commercial UAVs); and the vulnerability of the UAV GCS's to strike weapons (once identified).

The experience gained in military operations in recent military conflicts (primarily in Nagorno-Karabakh) and during the Russian Armed Forces' "special military operation" to protect the Donetsk and Lugansk People's Republics shows both a serious threat to the troops by reconnaissance and strike operations of UAVs, as well as the imperfection of existing approaches to organizing and conducting combat operations against them.

The factors considered above determine the relevance of ways to improve the organization and conduct of countering UAVs. It is reasonable to consider their reconnaissance capabilities, countering their use via fire and radio-electronic destruction, and the protection of Russian troops and military facilities from UAVs as the main components of the fight against unmanned aerial systems.

The analysis of the combat experience and the results of theoretical studies and practical experiments have made it possible to determine that successful fight against UAVs is possible on the basis of the comprehensive application of diverse forces and means for solving the reconnaissance of an air attack (AA) and counteracting their effective use; the improvement of methods and techniques for countering UAVs; and solving problems to reduce the effectiveness of their actions.

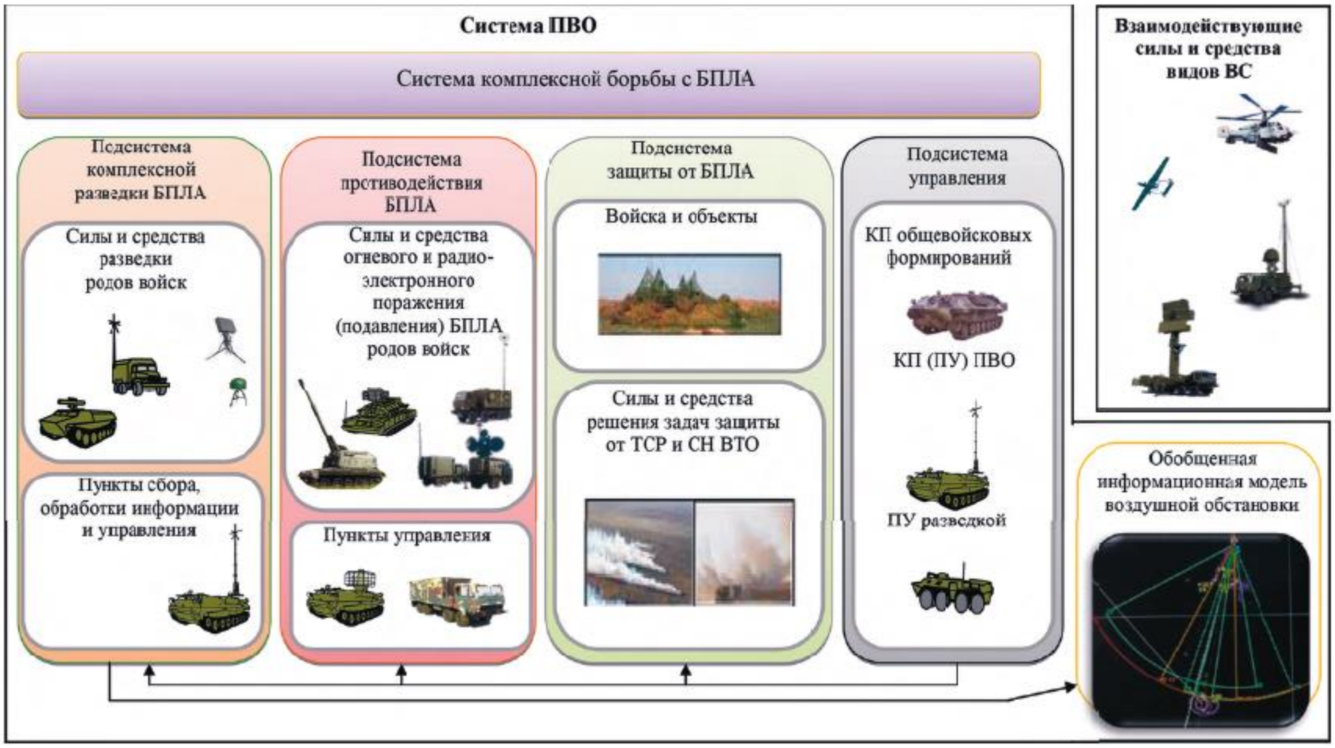
Based on the aforementioned, in order to ensure an effective fight against the UAVs, we propose to use the complex application of diverse forces and means within the framework of integrated combat against UAVs, the structure of which is shown in Figure 2.

The system under consideration should function as an element of the air defense system and include the following subsystems: integrated reconnaissance of UAVs; anti-UAV countermeasures; and protection from UAVs. At the same time, the tasks of countering UAVs, in addition to allocated air defense forces and means, should be performed by the following: specialized units for countering UAVs; specially designated general military units; electronic warfare (EW) units; radiation, chemical and biological protection (RCBP) units; and units that are part of the protection and defense of critical facilities.

The effectiveness of accomplishing the tasks assigned to the forces and means listed above is largely determined by the capabilities of the means used to combat UAVs (reconnaissance means, fires/strikes, electronic suppression, protection against technical means of detection (TMD), and targeting adversary high-precision weapons command and control.) The experience gained in combat operations as well as the results of theoretical studies and practical experiments indicate that the existing measures for combating UAVs are ineffective.

Thus, even when using the available reconnaissance means, the reliable and timely detection of small UAVs is not ensured. The main reasons for this are as follows: insufficient capabilities of existing radars to detect small-sized and low-speed, low-flying aerial targets; low visual reconnaissance capabilities, including those performed with the use of optical and optic-electronic systems; the difficulties of acoustic reconnaissance of small-sized airborne vehicles; and the imperfect methods of collecting, processing, and distributing information about the aerial situation in general.

Taking into account the characteristics of UAVs and the listed problems of combating them, it is necessary to further develop reconnaissance subsystems for the following tasks: the modernization of existing radars (implementation of modes for detecting small-sized low-speed aerial targets; the development of specialized small-size radars; equipping air defense units and specialized units being formed with radio-electronic reconnaissance equipment (RTE) and automated optical-electronic reconnaissance (OER) devices; and providing complete informational-technical compatibility of reconnaissance equipment with automation equipment at the command points (CP) of command and control bodies and air defense units, reconnaissance and artillery formations.


Система ПВО
Система комплексной борьбы с БПЛА
Подсистема комплексной разведки БПЛА
Силы и средства разведки родов войск
Пункты сбора, обработки информации и управления
Подсистема противодействия БПЛА
Силы и средства огневого и радио-электронного поражения (подавления) БПЛА родов войск
Пункты управления
Подсистема защиты от БПЛА
Войска и объекты
Силы и средства решения задач защиты от ТСР и СН ВТО
Подсистема управления
КП общевойсковых формирований
КП (ПУ) ПВО
ПУ разведкой
Взаимодействующие силы и средства видов ВС
Обобщенная информационная модель воздушной обстановки

[Fig. 2: Structure of the integrated anti-UAV system by functional slice (variant)]

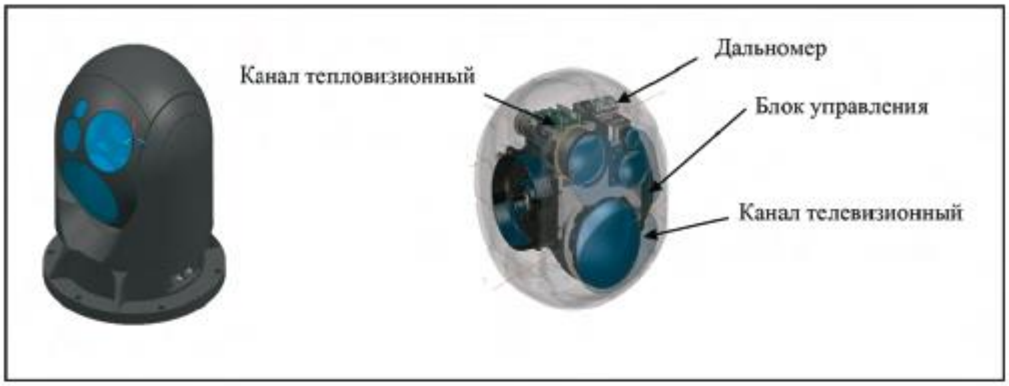
The timely detection of small UAVs using radars is possible due to the increased sensitivity of their receiving systems in the near-field zone and the adaptation of the filter parameters of the moving target selection systems to UAVs' low flight speeds.

Considering the relatively short detection ranges of micro-UAVs, it is advisable to equip both the units assigned to combat these UAVs and the units guarding critical facilities with small-sized (specialized) radars for detecting small-sized airborne targets. This ensures the avoidance of situations where non-strike UAVs and drones are used.

The use of existing and prospective radio-technical reconnaissance facilities will make it possible to reveal the directionality of UAV operations, recognize their class, type, and current nature of operations. It is also possible to reveal the position of the UAV GCS and the preparations for their launch.

To conduct optical-electronic reconnaissance of UAVs, television and infrared reconnaissance devices from automation systems can already be used at present. The advantage of these reconnaissance assets is in the capability to detect air targets in general or in a given sector, and incorporating the obtained data into the general data exchange network that is part a unified coordination system. The capabilities of these tools for detecting small-sized aerial targets are significantly inferior to promising radar and radio-electronic reconnaissance means, but they are not impacted by electronic warfare, and the information they provide can be effectively used by specialized UAV countermeasure units deployed deep in the Russian battle formations.

In the long term, the OER tools discussed above can be replaced by more advanced models. For example, samples OER devices have already been developed that are capable of detecting micro-UAVs in a timely manner. An example is the optical-electronic all-around vision station developed by the research and production enterprise "Alexander" (Fig. 3).



[Fig. 3: Optical-electronic all-around vision station]

Today, many counter-UAV engagements are carried out using air defense systems developed to combat tactical aircraft, helicopters, and cruise missiles. At the same time, combating small-sized UAVs is associated with significant problems due to: low probabilities of hitting a target with anti-aircraft artillery shells and triggering the radio fuses of anti-aircraft guided missiles; the insufficient fire performance of anti-aircraft systems when countering UAVs operating as part of a group or "swarm"; and the relative economic inexpediency of using medium-range and long-range air defense systems to combat such UAVs.

The main areas of improvement for countering UAVs should include the development of small, relatively cheap surface-to-air missiles, and improving the firing capability of anti-aircraft systems when UAVs are part of groups or "swarms."

Currently, the electronic warfare equipment in Russian service does not fully comply with the requirements for the frequency range of reconnaissance and jamming of onboard EW, their power, or their reaction time. The main directions for the development of electronic warfare measures in countering UAVs should include: the development of portable, small-sized, autonomous systems for radio-electronic destruction of small-sized aerial targets based on standard special vehicles; the creation of specialized reconnaissance means capable of identifying control and data transmission channels between the GCS and the UAV; and the development of systems for the functional destruction of UAVs.

The state of protecting troops and facilities from UAV operations is currently characterized by: insufficient effectiveness of camouflage methods, the absence on many models of weapons, military, and special equipment (WMSE) of built-in personal protective equipment against technical reconnaissance equipment (TRE) and guidance systems for high-precision weapons (GS HPW); insufficient number of means of protection against TRE and WGE; conducting a set of measures to reduce the effectiveness of HPW operations without proper reconnaissance and information support and effective management.

It is advisable to improve the protection troops and facilities from UAVs in the following directions: equipping troops with means of protection against TRE and GS HPW; and expanding the list of WMSE samples equipped with personal protective equipment against TRE and GS HPW.

A common problem in countering UAVs is the lack of effective control over the means and measures involved. The main directions for improving such control should include: the provision of information-technical interaction of the automated control systems part of the air defenses command points (CP) with the their counterparts at other armed forces' branches; the development and implementation in automated control systems (ACS) of algorithms for managing reconnaissance, fire, and electronic destruction; and the introduction into the ACS of algorithms for data analysis of UAVs' and aerial targets' reconnaissance.

We propose to determine the following for improving reconnaissance of UAVs: the implementation of the integrated nature of reconnaissance—simultaneously in several physical fields, demasking features of UAVs; ensuring that efforts are focused on the most likely areas of UAV operations; reducing the time it takes for information about detected UAVs to reach the command point (CP) to conduct countermeasures and defense means.

As part of the practical implementation of the above-raised questions, we proposed to use certain methods of conducting airborne attack reconnaissance: the "*Single Observer*" and the "*Solid Field*."

The essence of the "***Single Observer***" method lies in the fact that, in addition to designated air defense units, we involve other forces and military branches capable of detecting enemy aerial objects. In this case, the reconnaissance of the UAV will be carried out simultaneously in several physical fields (by means of several types of reconnaissance). The reconnaissance information about the UAVs should be transmitted in a single coordinate system to the air defense launchers of the general military formation and the command point of the anti-aircraft missile unit (subunit), where it is summarized.

This information can be transmitted both in a non-automated way—using tablets with a target designation grid, and in a combined way—using the capabilities of the CAE of the air defense command point (CP) by the manual input of aerial target coordinates and their semi-automatic tracking.

While using other military branches, it is advisable to involve military intelligence units equipped with Strelets-M reconnaissance and communications systems (RCS), as well as observation posts of all combined arms units; electronic intelligence units; reconnaissance radar divisions, and reconnaissance crews from combined arms and artillery units.

The "***Solid Field***" reconnaissance method is proposed in order to address the problems of creating a continuous radar field in the probable directions and altitudes of adversary UAV operations. The essence of the method is in the fact that the radar station is directed towards the most probable directions of the UAV operations, alongside the deployment of small-sized radar stations at positions maximally placed in the direction of the enemy (due to which a section of a continuous radar field is created with not less than a double overlap). Data transmission from the radar to the air defense command point (CP) is proposed to be carried out through the nearest battery command posts.

For improving the methods of countering and controlling UAVs, it is advisable to consider the following: the effective use of specialized units for countering UAVs equipped with various types of anti-aircraft systems and protecting critical facilities in the tactical defense zone; the effective use of specialized UAV countermeasure units that cover temporary combined arms formations from drones' actions; the impact on firing on UAVs in combination with electronic destruction and suppression; using the vulnerability factor from radio-electronic interference of control channels and data transmission between the NPU and the UAV, as well as on-board subscriber receivers of satellite radio navigation systems such as NAVSTAR, GLONASS, GALILEO, and BEIDOU; and increasing flexibility in the implementation of various control methods in the dynamics of hostilities—in the context of changes in the composition of specialized units to counter UAVs.

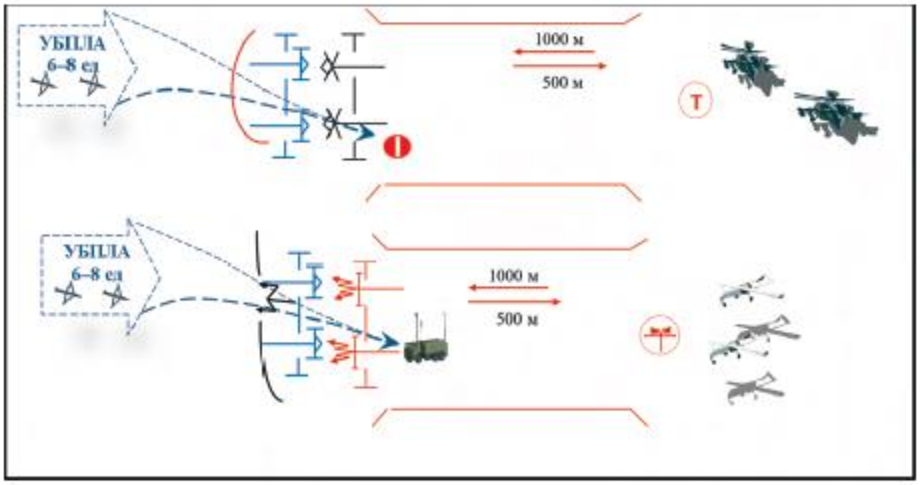
To counter the UAV, we also proposed to use the following methods: "*Air Defense-EW Barrier*", "*Air Defense—Defense KVO (Critically Important Object)*" and "*Air Defense Air Barrier*".

The "**Air Defense-EW Barrier**" method is intended to be used on a tactical level. Its essence lies in the fire and electronic destruction (suppression) of UAVs in the most probable directions of their actions, carried out by a specialized unit for countering UAVs, which is used as a mixed air defense-electronic warfare unit. The options for air defense and electronic warfare may be different, depending on the combat conditions and the availability of resources. A mixed air defense-electronic warfare unit occupies positions in the area where enemy tactical UAVs are expected to operate. When they are detected, the electronic warfare means suppress the UAVs' control and navigation channels. In case of insufficient EW impact on enemy UAVs, they are destroyed by anti-aircraft units assigned to this mixed unit.

The "**Air Defense—Defender of the KVO (Critically Important Object**)" method is advisable at the operational and tactical levels. The essence of the method is in the deployment of combined air defense units around a critically important object and the coordinated successive destruction of approaching UAVs by various anti-aircraft missile systems. At the tactical level, the integrated air defense unit is formed among the air defense forces and combined arms formation. The implementation of the "*Defender of the KVO*" method at the operational level involves the use of a full-time anti-UAV combat unit. In the future, this method can be transformed into the "**Air Defense Air Barrier**" method—the use of a highly mobile airborne anti-drone unit to fight UAVs with the implementation of situational awareness to detected threats, providing, as shown in Figure 4, the deployment of these units to the assigned UAV interception positions.

It is advisable to improve the methods of protecting troops and facilities from UAV attacks as follows: the implementation of a unified reconnaissance and information support for forces and measures that solve the above-mentioned tasks; ensuring unified management of a set of measures to reduce the effectiveness of adversary UAV operations; and the use of more effective techniques and means of camouflage against such aerial threats.

It is expedient to increase the effectiveness of protection for troops and facilities from adversary technical reconnaissance equipment (TRE) and guidance systems (GS) through the use of the "***Unified Defense***" method – reducing the effectiveness of enemy airborne operations with the implementation of a unified intelligence and information support and resource management, which involves the activation of individual and group protection, taking into account information about the adversary aerial attacks involving UAVs.



[Fig. 4: Order of battle of the unit implementing the “Air Barrier” method of air defense at the operational level”]

Based on the aerial targets’ flight parameters and their current position, the determination is made on the protective air defense equipment used, and the start time and methods of their application are then determined.

Improving the camouflage for troops and facilities should be aimed at hiding the unmasking signs of their deployment and operations, which requires constant monitoring of their timeliness and quality of camouflage using technical means of control, including those deployed on UAVs. The results of these studies have shown that the implementation of methods for protecting troops and facilities from TRE and GS can increase the likelihood of hiding and maintaining the combat capability of Russian military equipment to acceptable levels.

Thus, the obtained results in analyzing UAV operations, as well as other aerial objects for reconnaissance and countermeasures, made it possible to highlight the strengths and weaknesses of certain aerial targets’ classes, to identify the problems in countering tactical small-sized UAVs and the degree of threat from such aerial systems for ground troops, forces and means, thus potentially increasing air defenses against outlined threats.

At the same time, the presence of certain vulnerabilities in tactical UAVs, and the development of new means of reconnaissance, strike and electronic destruction of small air targets create the preconditions to bring the fight against them to a new technical level. In order to maximize the potential of promising means of combating UAVs, certain reconnaissance and countermeasures methods against UAVs were considered, largely based on the interaction of all forces and means capable of solving the problem of detecting the considered aerial targets. The implementation outlined approaches for the improvement of counter-UAV system will make it possible to solve the problems that occur in this area of military affairs.

ON LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE APPLICATION IN THE MILITARY SPHERE

(О ПРАВОВОМ РЕГУЛИРОВАНИИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ВОЕННОЙ СФЕРЕ)

Colonel of Justice E. A. GLUKHOV, Candidate of Legal Sciences

Voennaya mysl, no. 8 (2022): 73-85

Annotation: Despite the widespread introduction of automation and artificial intelligence in the military, their legal justification is currently practically absent. Gaps in the legal regulation of the use of artificial intelligence for military purposes are identified, proposals are made for the development of regulatory legal acts.

Abstract: Despite the increasing introduction of automation and artificial intelligence assets in the military, their legal justification is virtually nonexistent at the moment. The paper highlights the gaps in the legal regulation of artificial intelligence use for military purposes, offering suggestions for normative legal acts development.

Keywords: Artificial intelligence, military robot, automatic weapons, military management, decision making, means of warfare, military law.

The use of artificial intelligence (AI) in warfare in terms of scale and effectiveness can be safely compared with the revolution in military affairs that occurred with the advent of nuclear missile weapons. Systems with AI elements have already been adopted by a number of countries, starting with unmanned aerial vehicles, sentry robots and ending with systems for processing complex information.

For example, in July 2016, news about the US Air Force computer program called ALPHA became public. It allows not only for control of the flight of a fighter jet, but also to win an air duel with an experienced military pilot in a virtual battle. In other tests, neural network algorithms successfully carried out not only close maneuverable air combat, but also detected the enemy with the help of radars, and then hit the adversary with missiles.

The ground forces are also actively implementing artificial intelligence technologies. For example, at the beginning of 2019, the US Army command initiated a program to develop a virtual assistant for tank and combat vehicle crews, which are designed to increase the effectiveness of equipment and weapons in modern combat. The ATL AS virtual assistant will detect targets that people did not immediately notice, assess their danger, and also aim a gun at the target. At the same time, the ATLAS system will not only process data from its own sensors and combat vehicle devices, but also receive data from outside, which will increase the likelihood of target detection. As stated in the technical documentation of the system, it will allow detecting, identifying and hitting targets at least 3 times faster than a person is doing now.

The US Navy uses the Aegis combat information and control system, which allows receiving and processing information from ship and aircraft sensors and providing target designation to missile launchers. The decision to defeat the enemy is made by a person (operator), but the system can be configured in such a way that targets are automatically destroyed without human intervention. Moreover, according to the proposed American strategy, lethal military weapons are installed on the US Navy support ships, and the decision to use them is made remotely. In other words, on the ships themselves, where combat missiles are installed, there is no team designed to serve and launch missiles.

The U.S. Department of Defense has about 600 AI projects underway, and investments in them have grown from $600 million in 2016 to $2.5 billion in FY2021. According to the views of the top military leadership of the United States, one of the key tasks at the present stage of military development is the integration of artificial intelligence technologies into existing and new models of military equipment.

The Chairman of the Communist Party of China also repeatedly noted the importance of introducing AI into all spheres of state life, including the defense industry. The PLA spends more than $1.6 billion annually on AI-enabled systems, not counting classified developments, according to a study by American scientists.

Thus, at the present time there is another round of the arms race, but now in the information technology domain. More than 40 countries, including the USA, Russia, Great Britain, France, China, Israel, South Korea, are developing robots capable of fighting without human participation. It is planned that by 2030 the share of combat technical means with AI will be 52% of the number of crewed combat vehicles, and 30% of the total composition of combat vehicles. At the same time, according to the estimates of American military experts, the combat capabilities of these new type of units will increase by 2-2.5 times.

In Russia, developments are also underway to equip modern weapons and equipment with electronic control systems. Some samples of "smart machines" have already entered the Russian military. For example, in 2021, during the exercises, Russian Uran-9 ground-based "drones" equipped with a cannon, machine gun, anti-tank missiles and a flamethrower, as well as the Nerekhta robotic system, have successfully hit targets. The control of such machines was carried out in real time by operators located at a distance of 1.5 km. In 2022, there is a plan to conduct an experimental exercise using combat robotics—based on its results, a decision will be made on the optimal amount of delivery of such military equipment to the troops.

The President of the Russian Federation V.V. Putin drew attention to the relevance of introducing AI technologies into new models of weapons: "... artificial intelligence technologies should provide a qualitative breakthrough in improving the combat characteristics of weapons, should be more actively used in control systems, communications and data transmission, as well as high-precision missile systems. Equally important is the introduction of artificial intelligence technologies in the creation of promising robotics with a high degree of autonomy, in ensuring the control of drones, as well as deep-sea vehicles. All these priorities and tasks should be fully reflected in the state armament program through 2033." Speaking at the 2020 collegium of the Russian Ministry of Defense, the Russian President recommended "in the course of combat training, to more actively master, "run in" weapons and equipment with elements of artificial intelligence, including robotic systems, automated control systems. Such weapons significantly increase the potential of units and formations and in the near future will largely determine the outcome of the battle.

It is no coincidence that the Russian government plans to allocate 244 billion rubles for the development of AI in the country until 2024. In 2020, the Russian Ministry of Defense (MOD) has already ordered the development of an artificial intelligence system for military use. The cost of the contract, which must be completed by November 10, 2022, amounted to 387.8 million rubles. At the same time, MOD planned to allocate more than 115 million rubles for AI-related research in 2020, over 152 million rubles in 2021, and 120 million rubles in 2022.

Therefore, it was quite a natural fact that a new body was created in the Russian Ministry of Defense—the Main Directorate of Innovative Development, one of the main functions of which is the introduction of high-tech products for military and special purposes in the interests of defense.

Central media report that no later than 2035, the Russian military will switch to the creation of fully autonomous drones and military systems' groups. The introduction of new generation automatic target recognition systems will not only increase the effectiveness of reconnaissance aircraft, but also drastically reduce their potential combat losses.

All of the above examples testify to the relevance and urgency of closer scientific consideration of the development and implementation of new weapons and equipment systems that use AI technologies. Moreover, the legal regulation of this process, as usual, lags behind the actual achievements. Yes, the legislation of the country more or less regulates civil relations related to the production and sale of weapons and military equipment. The Russian state describes in more detail the procedure for using handguns. But the use of smart machines, the use of AI for military purposes is regulated extremely weakly, all the more so by open (non-secret) regulatory legal acts accessible to the public. Currently, there is no special regulation in the Russian Federation that takes into account the specifics of using artificial intelligence and robotics technologies. Meanwhile, the indicated legal problem in such a dangerous, but important for the defense and integrity of the state area, is hardly justified and can lead to critical consequences.

It can be confidently asserted that technological progress has once again overtaken the legal regulation of social relations in creating technical innovations. By the way, a similar legal uncertainty exists regarding the admission of unmanned vehicles on public roads. In both cases, we are talking not just about the use of a new device or a machine, but about the operation of devices capable of independently (that is, without human participation) receiving information, analyze it, make decisions and implement them. Thus, independent actions of such devices (both under the control of the operator and without his control) will give rise to legal consequences for individuals.

I would like to draw special attention to a very important point. AI systems cannot be identified simply with robots or automated control systems that operate strictly according to a given program. Professor V. M. Burenok, in particular, points out the danger of substitution of concepts, saying that although artificial intelligence is a computer phenomenon, and does not have the intellectual abilities of a person, it is no longer limited in its decisions by some rigid algorithm, and is able to go out in its own actions outside of this algorithm. Automation of management processes with the help of computers is not identical to the work of the AI system. In the first case, we are talking about computers equipped with a set of information processing algorithms, which is then used as a system of initial data for solving problems using formalized methods. The main differences between intellectualization and automation are the realization of the computer's ability to make decisions in conditions of significant uncertainty, based on heterogeneous and incomplete information, frequently changing situations, including those outside the programmed algorithms. We can say that AI is the ability of a computer to make decisions in a variety of, and in rapidly changing situations in a similar way to a human.

The key point here is the independence of actions in a technical device, expressed in the ability to analyze, make decisions and implement them without agreeing with a human, whether it be an operator, owner or a programmer. A device endowed with AI is much more independent than just a simple technical device, even if it works according to a complex program. And the most important thing is the independence of such a computer system, its ability to draw conclusions and make decisions depending on the results of data analysis, and even its creative functions. When using military robots with AI, the operator only sets the final goal, and not specific steps to achieve it.

Moreover, AI has another important quality—it is capable of self-learning and adaptation to various conditions, i.e., to change the algorithms of its actions or even structure in order to achieve an optimal state when external conditions change. Such a technical device under the control of artificial intelligence is capable, on the basis of previous experience and new information, of independently changing and improving the software originally embedded in it, carrying out self-programming (changing and supplementing its programming), and therefore solving problems that were not foreseen during the initial creation of this device. Therefore, it is extremely important, based on these characteristics, to improve the system of legislation in using systems with AI.

In the Russian legislation, the conceptual and terminological apparatus of regulating artificial intelligence is laid down by Decree of the President of the Russian Federation of October 10, 2019 N 490 "On the development of artificial intelligence in the Russian Federation", which approved the "National Strategy for the Development of Artificial Intelligence for the period up to 2030". In this document, the following definition of “artificial intelligence” is given—it is a set of technological solutions that allow simulating human cognitive functions (including self-learning and finding solutions without a predetermined algorithm), and obtaining results when performing specific tasks that are at least comparable to the results of human intellectual activity.

Thus, at the level of the normative Russian legal acts, the provision on self-learning and self-development of a computer program is fixed. Therefore, such a computer program embedded in a technical device (for example, a robot or a server) will change after some time and will differ from the original program—and this change will occur without the participation of third parties.

The above-mentioned Ai Strategy provides for the phased creation of a regulatory framework capable of ensuring the formation and functioning of an integrated system for regulating social relations arising in connection with the development and use of AI technologies. By 2024, the necessary legal conditions should be created to solve the problems and implement the measures provided for by the Strategy, and by 2030, a flexible legal regulation system in artificial intelligence, including guaranteeing the safety of the population and stimulating the development of AI technologies, should be created.

At the same time, it should be recognized that this AI Strategy refers to the development of a legislation system, primarily in civil law. In other words, it declares the development of legislation regarding exclusive rights to products with AI elements, rules for the circulation of such products, liability for possible harm as a result of its operation and designates entities that will have to compensate for this harm. Legal scholars are seriously discussing the possibility of endowing AI with a certain legal personality in the future, making transactions and imposing civil liability for its actions.

However, in domestic legal science, the legal aspects of using military force by artificial intelligence (and the use of artificial intelligence by military structures) have practically not been developed; the legislation lacks relevant rules of law that establish a framework for the use of AI in military service. Moreover, the criteria for classifying employees of military organizations as subjects of criminal liability for causing harm by military robots have not been defined.

There are only general rules on the use of weapons and military equipment, as well as general provisions on liability for causing harm. However, the existing legal norms do not take into account the specifics of AI presence (in such systems), and do not take into account the specifics of military legal relations. In addition, the lack of legal norms on the procedure for using technical means with AI also means that they cannot be violated, and without violating the norms of law, the offense itself is impossible, as well as legal liability. The Constitution of the Russian Federation enshrined the principle that no one can be held responsible for an act that was not recognized as an offense at the time it was committed (Article 54).

The problem is that the boundaries and the very subject of legal regulation regarding the use of military artificial intelligence systems are not completely clear. Legislative acts regulating these legal relations have not been created; the regulation of this issue is extremely sparingly represented in the military departments. This problem is stated in the Concept for the development of regulation of relations in artificial intelligence technologies and robotics until 2024. At the same time, as mentioned above, the technical means with AI elements already exist.

In the foreign legal literature for the past several decades, the so-called "robolaw" or "law of robots" has been quite consistently formed as an independent subject area of research. First of all, the problems of responsibility, legal personality, controllability of AI systems, problems of copyright and patent law, and many others are considered.

However, firstly, the above studies of foreign scientists cannot be applied to the Russian reality due to the difference in legislation, the discrepancy between the levels of technical and economic development, the mentality of the population and the principles of state policy. Russian science has yet to study this issue. As stated in the Program of Fundamental Scientific Research in Russia for 2021-2030, "the focus will remain on the issues ... of the legal and information space. Interdisciplinary research is needed in the legal regulation of the development of robotics, clarification of the legal status of AI."

And secondly, the military legislation has significant specifics. Unlike, for example, the Tesla unmanned vehicle, whose function is to move people and goods with the least possible harm, robotic systems used in the interests of Russian national defense have as its main function to precisely cause harm to enemy personnel and equipment, or another specified goal. Or they are indirectly related to the above function of causing harm. The harm caused by them, as a rule, does not occur accidentally, not as a result of "force majeure", but purposefully as a result of their intended use. For these purposes, AI systems have the ability to use weapons, intelligence activities, analyze information (including personal data), destroy objects, cause harm to human life and health, etc. Therefore, in the military, systems endowed with AI are potentially much more dangerous.

International humanitarian law has for many years been developing a regulatory framework regarding the prohibition on the use of certain means and methods of warfare. Under the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, the right of belligerents to choose methods or means of warfare is not unrestricted. The use in armed conflicts of weapons, projectiles, substances and methods of warfare that are likely to cause major injury or cause unnecessary suffering is prohibited.

Thus, the following means of warfare fall under the ban:

* explosive and incendiary bullets; bullets that easily unfold or flatten in the human body; asphyxiating, poisonous or other similar gases and bacteriological agents;

* bacteriological (biological) and toxic weapons, specific types of conventional weapons (undetectable fragments in the human body, some types of mines, incendiary weapons and weapons of mass destruction—in relation to the civilian population), means of influencing the natural environment, chemical weapons;

* blinding laser weapons.

As you can see, the international conventions do not directly provide for a ban on the use of systems with AI, and these international acts themselves were adopted even before the implementation of such technical systems. But here it is appropriate to make an important reservation: not all military equipment with AI elements is actually a weapon. Many types of military equipment, including ground and aerial drones, were created not as weapons, but as auxiliary and maintenance systems. AI can also exist in computer networks, performing an intellectual function, helping to make decisions for the command or participating in a cyber war with the enemy. In this case, no chassis, no firearms, no other technical device is required.

In modern realities, the line between weapons and other technical military products is blurred. For example, you can harm an enemy not only by firing from a firearm, but also by disabling his control systems, or by switching control over to yourself, destroying life support systems through computer viruses, DDoS attacks, acting by sound, light, magnetic radiation, spreading disinformation, giving false commands, etc.

For example, voice artificial intelligence can accurately model the voice of any person. Imagine what will happen when, during combat, you receive commands by radio or telephone given by the "voice of the commander" (actually—given by the enemy)? Will their execution by subordinates lead to disorganization of control and defeat in battle? The answer is obvious: significant damage will be done to the enemy, it is quite possible that people will die, and the troops will be in a disadvantageous position.

The conduct of modern wars does not provide for long and bloody battles, but at the same time, technical combat means continue to be improved, as a result of which the enemy will be inflicted irreparable harm precisely in a specific and critical place/time/location. This may be the financial or energy sector, the activities of government bodies, and the like.

At the same time, many armies are also armed with military robots, which have military weapons as a constituent element, which are designed to hit the enemy's manpower. Yes, any weapon is produced in order to warn the aggressor and, if necessary, harm him. Therefore, the free circulation of weapons is limited by law, and their intended use must be carried out strictly on the basis of the law according to the established procedures

AI systems may not be “weapons”. For example, they are used for navigation, communications, reconnaissance, surveillance, demining, logistics, maintenance of weapons and equipment, information warfare, electronic warfare, training, control, automatic target recognition, preparation of management decisions, programmatic disabling of electrical and telecommunications enemy networks. The development of weapons systems and the acceleration of the pace of hostilities forces the military command to automate the control of forces as much as possible, because the human brain is inferior to a computer in the speed of processing such an amount of information.

But even without being a weapon (in the usual sense of the word), AI systems in the military are still designed to increase the combat capability of their forces and inflict damage on the enemy. Thus, unmanned aerial vehicles can carry out ramming even without firearms, i.e., they are still capable of causing harm, including killing a person. The situation is further complicated by the fact that they can bring harm without the direct command of a person. It should be noted that neither in international law nor in Russian legislation is there a requirement for the mandatory participation of a person when a robot implements its deadly action (i.e. "pulling the trigger" or approving a decision).

To date, three types of military robots have developed: with an initially rigid program of actions, controlled by a human operator, with artificial intelligence. In Western classification it looks like this:

* "man-in-the-control-system" (human-in-the-loop)—robots are able to independently detect targets and carry out their selection, however, the decision to destroy them (or take other actions) is made only by the human operator;

* "human-on-the-loop"—this category includes systems that can independently detect and select targets, as well as make decisions regarding them, but the human operator, who acts as an observer, may intervene at any time and correct or block this decision;

* "human-out-of-the-loop"—this category includes robots that can detect, select and destroy targets on their own, without human intervention.

A fully autonomous system is able to make decisions and perform actions in the absence of human control. This level of autonomy is to be distinguished from systems that either "interact" with a human or are subject to some form of human control.

Thus, it should be stated that modern autonomous weapons systems can operate completely independently, without operator intervention: from searching for a target to making a decision and depriving a person of life, even if this human is not in military uniform. And such cases have already been recorded. In 2020, Turkish Kargu 2 drones, using "swarm tactics", tracked down and attacked rebels in Libya. And they did it on their own, without human intervention. Another case—in November 2020, nuclear scientist M. Fakhrizadeh, head of the research center in the Iranian Ministry of Defense, was killed in Iran. The shots were fired from a machine gun controlled by a computer system, without human intervention.

In Russia, in the summer of 2021, changes were made to the Federal Law "On Weapons". In particular, it was clarified that weapons are a source of increased danger. And although only a small part of the weapons used by the Russian Armed Forces and other military departments falls under the regulation of this law, the legislator clearly defined the vector of legal regulation in legal relations under consideration. After all, if the legislator attributed combat hand-held small arms and edged weapons to sources of increased danger, then much more deadly tanks, cannons, flamethrowers, torpedoes, etc., are such a source. As indicated in the legal literature, a source of increased danger for military purposes is characterized by certain specific features: increased harmfulness, scale of harm. Such military systems are capable of causing harm, despite the most complete human control over them.

As a general rule, the higher the risk for violation of human rights or causing harm, the more stringent the legal regulation in this area of relations should be. Accordingly, areas associated with particularly high risks, such as national defense, law enforcement, the use of weapons or sources of increased danger, should be regulated in the most detailed way. However, in reality this is not the case. Scholars recognize the absence of even international treaties on the use of new technologies for conducting military operations, although their development and the possibility of using them in armed conflicts should not take place in a legal vacuum.

In this regard, I would like to support Elon Musk in his statement that artificial intelligence is much more dangerous than nuclear weapons. Artificial intelligence is that rare case when it is necessary to take the initiative in regulation, and not try to respond to its activities after the fact.

Of course, the development of algorithms implemented as part of the software in robotic systems is carried out according to the technical specifications and requirements of the Russian government. But still, it is impossible to replace legal regulation, which is mandatory for all subjects and is provided by coercion of the state, with technical regulation, which determines only the desirable parameters of the objects produced.

Within the framework of this publication, of course, it is impossible to give a qualitative legal assessment of all aspects of using AI systems in the military domain. It is necessary to begin to develop a concept for the use of AI systems in the military sphere today, in particular, to consider the following problematic issues:

Determine those areas of military activity in which the use of systems with AI is acceptable. In particular, the question requires legal regulation: "Are AI systems entitled to obtain, process and store information about personal data of citizens, other information protected by law, information containing state secrets?" Also today it is necessary to set a normative list of situations when making significant decisions should be done by a person.

Identify those types of weapons that cannot be equipped with AI systems, since only a person can pull the trigger in such deadly weapons.

Regulate the rights, duties and responsibilities of military officials who use AI systems in order to prevent them from committing crimes prohibited by international humanitarian law. Otherwise, there is a possibility that such a deadly and intelligent weapon will become simply a means to achieve criminal goals, a means of causing death at a distance.

Determine when the AI has the right to make decisions on its own without waiting for the approval of the operator, for example, in cases where it is necessary to protect against an enemy attack (the decision to destroy a missile or a drone approaching the command center). The issue of AI making independent decisions in offensive operations (i.e., the use of weapons not for defense), as well as making decisions regarding the use of cyber weapons, also requires clarification.

Clarify the balance of authority and responsibility between a person and an AI system in cases when artificial intelligence prepares a solution for further approval by a human. In the context of the transience of modern military operations and the significant advance of the computational and analytical abilities of a computer compared to a person, any delay in decision-making can lead to defeat. At the same time, the role of a human cannot be reduced to pressing any button that the AI recommends, that is, to the role of Pavlov's dog, but only with a weapon. It is desirable to determine those parameters in the presence of which the operator has the right, without negative legal consequences for himself, to disagree with the solution proposed by AI.

There is a need for legal regulation for exercising control over the activities of AI and providing objective information to its owner, or regulatory and supervisory authorities.

Determine situations when AI systems should stop the execution of the program to destroy/harm people (white flag raised by the enemy or hands raised up, target classification as non-combatant, wounded soldier, etc.).

Define the entities that have the right to own and use military-grade AI technologies. It is unacceptable that such military systems could fall into the hands of terrorists or criminals.

The most important issue in the regulation of AI and robotics is the question of responsibility: who is responsible for the actions of a robot, especially a military one? Therefore, it is necessary to clearly regulate the balance of responsibility of the state, the military command, and the manufacturer of AI systems to third parties for the harm caused during the use of military robots. As independent areas of legislative activity, it is necessary to clarify liability for harm caused not by weapons, but by cyber attacks, as well as liability for harm caused as a result of a technical failure in the operation of AI systems, i.e. without a causal relationship with the actions of the operator. It is quite possible that it will be necessary to adjust the legislation on compulsory civil liability insurance in relation to the operation of AI systems.

A separate consideration is the question of who should be responsible for the actions of an AI that has the ability to self-learn? After all, AI is able to independently make a decision on the commission of illegal actions or inaction, which will entail the onset of harm. If the algorithm of the program is modifiable, then the developer cannot be responsible for the use of the robotic system after modifying what he has developed, and the person operating it cannot fully manage and control the system with rules of behavior unknown to him.

Undoubtedly, an autonomous system that calculates numbers, searches for a large amount of data and sorts it, quickly responding to urgent tasks, with the ability to simultaneously perform several tasks, including complex ones, surpasses human abilities. However, only a human can reflect, show mercy, apply existing experience to new emerging challenges, make meaningful decisions and bear legal responsibility for them.

Conclusion: the state that wins the race to create AI will receive a critical and possibly undeniable military advantage, but this process must necessarily take place strictly in accordance with legal norms.

This report is a special issue in a series of biweekly updates as part of an effort by CNA to provide timely, accurate, and relevant information and analysis of the field of civilian and military artificial intelligence (AI) in Russia and, in particular, how Russia is applying AI to its military capabilities. It relies on Russian-language open-source material.

Approved by September 2022: Michael Kofman, Research Program Director
Russia Studies Program / Division Name

This work was performed under Federal Government Contract No. N00014-22-D-7001.

DISTRIBUTION STATEMENT A. Cleared for Public Release.

Public Release

This document contains the best opinion of CNA at the time of issue. The views, opinions, and findings contained in this report should not be construed as representing the official position of the Department of the Navy.

This report may contain hyperlinks to websites and servers maintained by third parties. CNA does not control, evaluate, endorse, or guarantee content found in those sites. We do not assume any responsibility or liability for the actions, products, services, and content of those sites or the parties that operate them

CNA is a nonprofit research and analysis organization dedicated to the safety and security of the nation. It operates the Center for Naval Analyses—the only federally funded research and development center serving the Department of the Navy—as well as the Institute for Public Research. CNA is dedicated to developing actionable solutions to complex problems of national importance.

DNL-2022-U-033442-Final

Link to Russia AI and Autonomy Newsletter Archive