Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space

"The source of external threat for information security of the Russian Federation is the development by a number of countries of the concepts of information wars which envision the creation of the means for dangerous effect on the information spheres of the other countries of the world, the malfunction of the information and telecommunication systems, the preservation of information resources and obtaining unauthorised access thereto"

(Information Security Doctrine of the Russian Federation approved by the President of the Russian Federation on 9 September 2000).

Introduction

The rapid development rate of the information systems for various applications, Internet-type computer networks and electronic media brought about at the turn of Millennium the formation of the global information space. Alongside the land, maritime, air and cosmic space, the information space started to be actively used by the armies of the most developed countries for solving a wide range of military tasks.

Due to the vulnerability of the information and communication systems towards radioelectronic и software/hardware effects, the information weapons that have cross-border adverse factors were created and started quickly spreading in the world, and the role of the information war has substantially grown. The Russian Federation, which is rapidly moving in the direction of the informatization of all spheres of the vital activity of the society, is currently facing a new serious threat arising from the global information space.

The extreme importance for countermeasures against the acts of aggressive information war was first emphasised in the Information Security Doctrine of the Russian Federation approved by the President of the Russian Federation on 9 September 2000. The Doctrine states that one of the priority directions in counteracting this threat is solving the tasks "for the improvement of the measures and options for strategic and operational deception, intelligence and radioelectronic combat, the methods and means for vigorously counteracting the information-and-propaganda and psychological operations of a potential enemy. Moreover, recently, due to the wide use of computer equipment in the systems of command and control of troops and weapons, this list has been supplemented by the task to protect the information infrastructure of the Armed Forces of the Russian Federation from various kinds of computer attacks.

The experience of the armed conflicts of the last decade, as well as the practice of the operational training of the troops and command staff gives the ground to state that currently the Armed Forces of the Russian Federation have formed an integral system of activities, which is intended to secure the efficient containment, prevention and resolution of military conflicts in the information space.

This Conceptual Perspective describes the main principles, rules and confidence-building measures pursuant to which the Armed Forces of the Russian Federation use the global information space for solving the tasks of defence and security.

1. Main terms and definitions

For the purposes of this document, we use the following main terms and definitions:

Military conflict in information space – a form for settlement of international or domestic differences using information weapons.

Activities of the Armed Forces in information space – use by the Armed Forces of the information resources for solving the tasks of defence and security.

Information security of the Armed Forces – state of protection of the information resources of the Armed Forces from the effect of the information weapons.

Information war – confrontation between two or more states in the information space for damaging the information systems, processes and resources, which are of critical importance, and other structures, to undermining the political, economic and social system, and massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party.

Information infrastructure – body of technical means and systems for the formation, creation, transformation, transmission, use and storage of information.

Information weapons – information technologies, means and methods used for the purposes of waging information war.

Information space – area of activity related to the formation, creation, transformation, transmission, use and storage of the information affecting *inter alia* the individual and social consciousness, information infrastructure and the information *per se*.

Information resources – information infrastructure, as well as the information *per se* and its flows.

Crisis situation – stage of conflict escalation characterised by the use of military force for its resolution.

International information security – state of international affairs precluding the breach of the global stability and creation of threats for the security of the states and global community in the information space.

System of ensuring information security of the Russian Federation – part of the system of ensuring the national security of the country which is intended for the implementation of the state policies in the sphere of the information security.

2. Principles

The activities of the Armed Forces of the Russian Federation in the information space are constructed pursuant to the combination of the following principles: legality, priority, complexity, interaction, cooperation and innovation.

2.1. Legality

Adherence to the principle of legality demands from the Armed Forces of the Russian Federation, during the activities in the information space, to invariably follow the regulations and principles of the current legislation of the Russian Federation, as well as the generally recognised regulations and principles of the international law.

In particular, pursuant to Art. 20 of the Military Doctrine of the Russian Federation, the use of the Armed Forces of the Russian Federation during the peacetime shall be implemented on the basis of the resolution of the President of the Russian Federation according to the procedure established by the federal legislation. Thus, a resolution for the use of the Armed Forces of the Russian Federation outside the territory of the Russian Federation shall be adopted by the President of the Russian Federation on the basis of a corresponding regulation of the Council of Federation of the Federal Assembly of the Russian Federation. This provision shall also be extended to the use of the Armed Forces of the Russian Federation in the information space.

As regards the international law, the Armed Forces of the Russian Federation in connection with the peculiarities of the military activity in the global information space are guided by the following regulations and principles thereof:

respect towards national sovereignty,
non-interference in internal affairs of other states,
non-use of force and threat of force,
rights for individual and collective self-defence.

In addition, the Armed Forces of the Russian Federation are guided by the regulations of the international humanitarian law (limitation of indiscriminate use of information weapons; establishment of special protection for information objects, which are potentially dangerous sources of technogenic catastrophes; prohibition of treacherous methods of waging information war).

2.2. Priority

Adherence to the principle of priority demands from the Armed Forces of the Russian Federation, during the activities in the information space, as a matter of priority to strive towards the gathering of actual and reliable information concerning the threats, its operational processing, thorough analysis and timely development of defence measures. The combination of all of the above creates favourable conditions for the efficient command and control of troops and weapons, maintaining the necessary morale of the military personnel.

The implementation of the set of measures for the protection of the information resources will allow, in the conditions of the information war, avoiding the disorientation of the bodies of military administration, the disorganisation of the system of the command and control of troops and weapons, the catastrophic destruction of the elements of logistical and transport infrastructure, and the demoralization of the military personnel and population in the area of the military operations. In the contemporary conditions, the necessity for the implementation of the aforementioned measures as a matter of priority is caused, *inter alia*, by the fact that currently hundreds of millions of people (entire countries and continents) are involved in the common global information space formed by the Internet, electronic media and systems of mobile communications.

2.3. Complexity

Adherence to the principle of complexity demands from the Armed Forces of the Russian Federation, during the activities in the information space, to use all the available forces and means for the efficient solving of the tasks they face.

As a whole, the activity in the information space includes the operations of the command staff and the actions of the troops in the sphere of intelligence, operational deception, radioelectronic combat, communications, covert and automated command and control, informational work of command staff, as well as the defence of own information systems from radioelectronic, computer and other effects.

The activity in the information space constitutes a coordinated integral system, where each component performs its tasks using the ways and means characteristic of it, and, on the other hand, by integrating in the integral system, it increases the capabilities of the entire system for the achievement of the objectives faced by the Armed Forces of the Russian Federation.

The leadership and the command staff of all levels directly participate in the organisation of the activity in the information space during the peacetime and the wartime, in the preparation and in the course of the operations (military engagement).

Each of these command and control bodies, according to their functions and responsibility, develops and plans the operations and actions of the subordinate troops united by the common concept of the operation in the information space.

2.4. Interaction

Adherence to the principle of interaction demands from the Ministry of Defence of the Russian Federation to coordinate their activity in the information space with the other federal executive bodies.

The interaction is performed in the framework of the system for ensuring the information security of the Russian Federation stipulated in the Information Security Doctrine of the Russian Federation (2000).

2.5. Cooperation

Adherence to the principle of cooperation demands the coordination of efforts with the friendly states and international organisations.

The main objective for the development of cooperation on the global level is the establishment of the international legal structure governing, *inter alia*, the military activity of the states in the global information space based on the principles and regulations of the international law.

The development of cooperation on the regional level pursues the following objectives: creation of the mechanisms for efficient collective action targeted at the detection, prevention and interdiction of the use of information and telecommunication technologies to threat the peace and security, to perform the acts of aggression; settlement and resolution of international disputes and conflict situations related to the hostile use of information and telecommunication technologies; strengthening of trust in the area of the use of the information systems of cross-border nature and ensuring the security in the use of the common information space.

2.6. Innovation

Adherence to the principle of innovation demands from the Armed Forces of the Russian Federation to use for the preparation and implementation of the activity in the information space the most advanced technologies, means and methods, and also to involve in solving the tasks of the information security the highly-qualified military personnel.

Therefore, the development and production of such means and technologies may involve the research and production capacity of the most advanced innovation centres of the Russian Federation, and the development *per se* may be performed in the framework of the national and agency-level programmes, and research and development.

The training of the specialists in the area of the organisation and implementation of the activity in the information space is performed in the educational institutions of higher vocational education of the Ministry of Defence of the Russian Federation.

In addition, the specialists who graduated from the other educational institutions of the Russian Federation may be involved in solving the tasks of information security of the Armed Forces of the Russian Federation, pursuant to the procedure established by the legislation of the Russian Federation.

3. Rules

In the course of their activity, the Armed Forces of the Russian Federation are governed by the set of the rules for the containment, prevention and resolution of military conflicts in the information space

> *"The military policies of the Russian Federation are targeted at the inadmissibility of the armaments race, and the containment and prevention of military conflicts…" (Art. 17 of the Military Doctrine of the Russian Federation approved by the Decree of the President of the Russian Federation dated 5 February 2010)*

3.1. Containment and prevention of conflicts

The Armed Forces of the Russian Federation, in their practical activity, are governed by the following rules of containment and prevention of military conflicts in the information space:

1. To develop the system for ensuring the information security of the Armed Forces of the Russian Federation envisioned for the containment and resolution of military conflicts in the information space.

2. To maintain the forces and means for ensuring the information security in constant readiness for repulsing the threats of military and political character in the information space.

3. To establish cooperation on a priority basis with the states of the Collective Security Treaty Organization, the Commonwealth of Independent States and the Shanghai Cooperation Organization, to expand the circle of partner states and to develop cooperation with these countries based on the common interests in the area of the strengthening of the international information security pursuant to the provisions of the UN Charter and other regulations of the international law.

4. To strive towards the entry, under the aegis of the UN, into a treaty for ensuring the international information security, which extends the effect of the generally recognised regulations and principles of the international law to the information space.

5. To take all possible measures for the early detection of potential military conflicts in the information space, and also for the exposure of the organisers of the conflict, its instigators and accomplices.

6. To determine the factors for the creation and escalation of the conflict and to establish control over these in order to avoid the occurrence of emergency situations.

7. To take priority measures for counteracting the development (conservation or escalation) of a conflict and its entry into such state, which materially increases the settlement price.

8. To take measures for non-admission of the spread of a conflict to adjacent spheres of international relations, which would demand additional expenses and efforts for the settlement of the consequences of the conflict.

9. To take measures for neutralizing the factors which created a conflict in order to switch the interaction between the conflicting parties onto a track of constructive cooperation.

10. To publicly, objectively and promptly explain to the global community the reasons and sources of a conflict. The formation of the necessary public opinion implies its corresponding orientation and mobilization; it provides an opportunity to create in the global information space a climate promoting the limitation of the possibility for the perpetration by the organisers of the conflict of any further escalation steps.

3.2. Resolution of conflicts

> *"The Russian Federation considers it justifiable to use the Armed Forces and other troops to repulse the acts of aggression against the country and (or) its allies, maintain (restore) peace based on a resolution of the UN Security Council or other structures of collective security, and also for securing protection of its citizens staying outside the Russian Federation pursuant to the generally recognised principles and regulations of the international law and the international treaties of the Russian Federation"*
> *(Art. 20 of the Military Doctrine of the Russian Federation approved by the Decree of the President of the Russian Federation dated 5 February 2010)*

The Armed Forces of the Russian Federation are governed by the following rules for the resolution of military conflicts in the information space:

1. The resolution of conflicts in the information space shall be primarily performed by means of negotiations, reconciliation, addressing the UN Security Council or regional bodies, or through agreement or other peaceful means.

2. In case of the aggravation of tension, to strive towards the inadmissibility of the entry of the conflict into extreme and destructive forms of confrontation, especially the forms

that can lead towards the destabilization of the international atmosphere and occurrence of crisis situation.

3. In the conditions of the escalation of a conflict in the information space and its entry into the crisis phase, to use the right for individual and collective self-defence with the implementation of any chosen options and means, which do not contradict the generally recognised regulations and principles of the international law.

4. In the interests of solving the tasks of individual and collective self-defence, to determine the necessary potential for retaliation based on the national democratic procedures taking into account the legal interests for ensuring the security of other countries, as well as the necessity to ensure the international information security and stability.

5. In the interests of individual and collective self-defence, to position own forces and means for ensuring the information security on the territory of other states pursuant to the agreements developed by these on the voluntary basis in the course of negotiations, and also pursuant to the international law.

6. In the course of the conflict, to constantly inform the domestic and international media about the developing situation and, relying on the public opinion, to efficiently influence its de-escalation development and the consolidation of the achieved results in the resolution of the conflict contradictions.

4. Confidence-building measures

The Armed Forces of the Russian Federation shall strive towards the development of the measures for confidence-building in the sphere of the military use of the information space. In particular, such measures include:

1. Exchange of national concepts for ensuring security in the information space.

2. Timely exchange of information regarding crisis events and threats in the information space and taken measures in respect to their settlement and neutralisation.

3. Consultations on the issues of activity in the information space, which may cause the parties' concern, and the cooperation regarding the settlement of any conflict situations of military character.

4.

5. Conclusion

In the contemporary conditions, the defensive potential of the Russian Federation significantly depends on the efficiency of the activity of the Armed Forces in the information space and to a great extent it is defined by their capacities in the containment, prevention and resolution of conflicts arising in the information space.

The Armed Forces of the Russian Federation intend to solve the tasks faced by them for ensuring the defence and security based on the fundamental principles and rules of the activity of the Armed Forces of the Russian Federation in the information space, and also on the confidence-building measure specified in this Conceptual Perspective.

Implementing this Conceptual Perspective, the Armed Forces of the Russian Federation shall strive towards the maximum use of the opportunities of the information space for strengthening the defensive potential of the state, the containment and prevention of military conflicts, the development of military cooperation, as well as the formation of the system of international information security in the interests of the entire global community.