Information Operations on the Battlefield

Maj. Gen. Kh.I. SAYFETDINOV (Ret.),
Doctor of Military Sciences

Abstract. The author looks close up at information operations and their relevance to the Russian Armed Forces and the country as a whole in peace and wartime; at the growing role of information operations in local wars and military conflicts; at the need to develop regulations stating the purpose, objectives, and underlying principles on which information operations are based as a system; and at their significance in the integrated government and military command and control system.

Keywords: information operations (warfare), information superiority, psychological stability, morale and psychological state, automated troops and weapons control systems.

Information operations, or information warfare, is briefly an across-the-board employment of information in whatever form to enable the user to achieve his goals on and off the battlefield. Many political and military leaders have left records of the ways in which they used information to deceive or mislead their adversaries, subvert the adversaries' will to resist, strike panic into adversary ranks, and encourage betrayal. At heart, information warfare (or operations) is conscious employment of information to enable the user to achieve his political, economic, military, or any other goals.

Interest toward information warfare has grown lately because of the rapidly expanding use of computers to control military or civilian equipment and machinery, the swelling bulk of information, and the high speed at which it is disseminated. In the late 20th and early 21st centuries, change occurred in the pattern of geopolitical competition between countries, globalization is expanding, and information is given increasingly greater weight than the traditional force of arms in confrontation between states. Operations carried out by the U.S. and its allies in Iraq (Shock and Awe and Desert Storm), and the events unfolding these days in Ukraine are examples of combined employment of sheer armed force and information operations.[1]

Back in September 2012, General Martin Dempsey, Chairman of the Joint Chiefs of Staff, signed a basic concept for the conduct of joint operations that

gives a central place to information capabilities (forces and equipment). According to this concept, globally integrated operations built and carried out around actions undertaken by the U.S. special operations and cyberspace operations forces simultaneously with or separately from general-purpose forces are to become the principal form of employment of U.S. armed forces and the forces of its allied countries in the future.

The information operations forces will be used to disrupt information exchange between military and government control agencies, reduce opportunities for the adversary to obtain authentic information through space-based intelligence capabilities, missile attack warning and space monitoring systems, to influence mass consciousness and decision makers' awareness, and to lower the Russian Armed Forces' combat potential. Targeted employment of information capabilities is, as a result, turning into a decisive factor contributing in a large measure toward victory or defeat, and is capable of preventing open armed confrontation.

The experience of the two military campaigns planned and conducted to restore the constitutional law and order in Russia's Chechen Republic in the mid-1990s and early 2000s demonstrated how little attention information operations received from the Russian military command. To remedy this flaw, the country's government and military control agencies have no more important an issue to take on than directing adequate attention at the problem still waiting finite resolution by, among many other measures, updating national laws and regulations. The Russian military academic community must give more thought to information operations practiced in peace and wartime, such as the time periods when the U.S. armed forces and their allies planned and carried out military operations against Iraq and Afghanistan.

To our mind, research in information operations must begin with setting out in precise phrases (fully new or revised, if stated inadequately previously):

- basic concepts, terms, and definitions;
- purposes and objectives of information operations in general, and in the military environment, primarily;
- principles to be followed in attaining the objectives set down in peace and wartime;
- possible forces and capabilities to be drawn upon to attain the objectives laid down; and
- effective forms and methods of information operations.

That is not all, though. It is also essential to develop specifications for future software and hardware, work out recommendations on techniques to plan and control information operations; provide answers to many more questions (such as the need to propose a theory to manage information operations), and draft interim instructions on information operations.

Information operations have been getting a fair share of attention from academics and military chiefs in recent years, evidence of which includes research undertaken in the last few years to find solutions to outstanding problems and tasks, and some aspects of information operations are addressed in rules and regulations. With whatever experience there is to draw on, and no claims to lay on what follows, we will only give a framework for the fundamental principles on which information warfare is based.

In our view, gaining and holding information superiority over adversary forces, and creating favorable conditions for getting the national Armed Forces into shape and sending them into action is the primary ***objective*** of information operations on the battlefield.

Information operations must be conducted ***constantly***, in peacetime, in the period of threats gathering around, and in wartime by committing all available forces and software and hardware potentialities to impact the opponent's information capabilities and protect our own against similar actions by the opponent.

All-around attack by friendly information operations forces and technical capabilities against adversary capabilities in close cohesion and cooperation with the friendly general-purpose forces is the principal ***condition*** for achieving the objective of the information operations.

The information operations forces and technical capabilities must be fused into a ***unified system*** and used ***in coordination*** relative to their objective, tasks, location, and time.

In ***peacetime***, information operations must be maintained to achieve objectives set by the country's political leaders in an effort to enhance the effectiveness of political, diplomatic, economic, judiciary, and military measures to maintain the security of the Russian Federation, above all, for strategic deterrence purposes. Government and military command and control agencies and all available information operations forces and capabilities must be involved in these efforts.

Information operations must reasonably be controlled and military and nonmilitary measures implemented from a central control station at the top of the military hierarchy (control station of the Armed Forces' General Staff or a national control station of the country's defense operations set up expressly for this purpose), which draws on the control centers of military districts, fleets, and territorial control stations instituted with these aims in mind.

In a ***period of threat***, the information operations system must address tasks set by the country's political and military leaders, giving consideration to the evolving situation, under plans developed (revised) in advance for an orderly entry of the country and its Armed Forces into war and for fulfilling the tasks they have been assigned and simultaneously fulfilling military and national (nonmilitary) measures.

Information operations may be directed from a unified control station headquartered at the Armed Forces' General Staff. The various agencies of the exec-

utive branch of federal government, too, must assign their own forces and capabilities for involvement in the Armed Forces' information operations.

In ***wartime***, information operations must be pursued to fulfill tasks set by the country's top political and military leaders, in particular, gaining and maintaining information superiority over the adversary for creating favorable conditions facilitating success in operations conducted by the general-purpose forces.

At the stage of preparations for, and conduct of, strategic actions (operations) by the Russian Armed Forces, information operations must be ***controlled*** by military command and control agencies in coordination with national general-purpose (nonmilitary) information operations and information measures undertaken by the control authorities set up by various government ministries and public service agencies that raise and maintain their own IO forces and facilities. When operations (combat actions) are planned and carried out, all information measures directed against adversary information centers and instituted to protect friendly forces and capabilities, and civilians in areas of military operations (conflicts) must be coordinated from a single center.

The primary ***tasks*** to be achieved by information operations may include:

- monitoring information sources, and detecting, assessing, and predicting information-related threats to the Russian Federation and its Armed Forces;
- deceiving the adversary as to own plans and intentions;
- disorganizing (disrupting) the adversary's government and military command and control over his forces;
- impairing the psychological stability of the adversary's armed forces personnel and civilian population during the preparatory stage and conduct of military actions; and
- maintaining morale and psychological state of the friendly forces' personnel at a stable level.

Protection of friendly automated troops and weapons control systems and information, information management, and other military and defense-related systems is a critical ***task*** of information operations.

The Russian Federation's Military Doctrine sets out the profiles of possible military hazards and threats, and also military conflicts that may arise out of them. A future military conflict will be a series of fast-fought operations that will require a cardinal review of all military control functions, from beginning to end. The situation on the battlefield will be assessed, decisions made and implemented, and their effectiveness evaluated in near real time. In this setting, the adversary's information operations may inhibit significantly the performance of the friendly government and military control system. To further complicate the situation, information operations will spill over into psychological warfare.

An **information operations system** must be among the future Armed Forces' basic systems responsible for information security of friendly informa-

tion capabilities and suppression (destruction) of an adversary's information capabilities. It may be structured to include several subsystems, in particular:

– attack against, and protection from, an adversary's technical information capabilities;

– software and hardware capabilities;

– reconnaissance, including electronic reconnaissance capabilities;

– electronic warfare; and

– psychological warfare against an adversary and moral and psychological support for the friendly forces.

Design and development of an information operations system must, therefore, be undertaken to enable it to fulfill the entire range of functions it is capable of, and it only remains to fit it into a proper slot within the unified government and military control system.

NOTE:

1. N. Apple, *Rossiya v virtual'noy voyne* [Russia in Virtual War], *Vedomosti*, May 8, 2014.