(1)

RUSSIAN VIEWS ON ELECTRONIC AND INFORMATION WARFARE:

VOLUME I

By

Mary C. FitzGerald
Research Fellow

December 1996

SUBMITTED IN PARTIAL FULFILLMENT
OF CONTRACT #DASW01-94-C-0075

1015 18th Street, N.W. • Suite 300 • Washington, D.C. 20036 • 202-223-7770 • FAX 202-223-8537

Hudson Institute

Herman Kahn Center • P.O. Box 26-919 • Indianapolis, Indiana 46226 • 317-545-1000 • FAX 317-545-9639

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the early 1980s, the Soviet military was perhaps the first to argue that a new "revolution" was occurring in military affairs. Today the Russian military argues that precision-guided, non-nuclear, deep-strike weapons and the systems used to integrate them are revolutionizing all aspects of military art and force structure -- and elevating combat capabilities on the order of 10^6. According to the Russian military, superiority in the new Revolution in Military Affairs (RMA) proceeds from superiority in C^4ISR systems: 1) reconnaissance, surveillance, and target acquisition (RSTA) systems, and 2) "intelligent" command-and-control systems. Information technologies are now said to be "the most formidable weapons of the 21st century" -- and comparable in effects to weapons of mass destruction. Indeed they constitute the essence of the new, 4th RMA. The Russian politico-military leadership is therefore engineering a dramatic shift away from material-intensive systems and toward science-intensive systems: away from ballistic missiles, submarines, heavy bombers, tanks, and artillery and toward advanced C^4ISR and EW systems.

Under conditions of parity in nuclear and conventional weapons, superiority in reconnaissance, command and control, and electronic warfare is said to be the main factor in raising the qualitative indices of weapons and military equipment, which will have a "decisive" effect on the course and outcome of combat operations. Under all circumstances the side that has advantages in these areas will always possess greater capabilities, even if the other side has definite advantages in nuclear and, even more so, conventional weapons.

The Russian military now argues that, as the most dramatic force multipliers, advanced C^4ISR and EW systems must govern the allocation of scarce defense resources. Civilians such as President Yel'tsin and Deputy Defense Minister A. Kokoshin -- head of the Military-Technical Policy Council -- have repeatedly echoed this assessment. These systems represent the most cost-effective way to increase combat capabilities without increasing the quantity or even quality of weapons systems. They must also be included in any equations involving combat potential in all future arms control negotiations; the crushing weight of these systems has negated the quantitative paradigm that formerly constituted the heart of such calculations. Warfare has indeed shifted from being a duel of strike systems to being a duel of information systems.

The Russian military hierarchy clearly understands the strategic and tactical implications of the new RMA, and has developed a detailed planning framework for generating appropriate responses. The need to spend a disproportionate share of scarce military resources on developing such responses is recognized by all senior military officers. Notwithstanding the high priority assigned to the RMA, Russia is unlikely to possess the economic and technological resources to match the U.S. in advanced military technologies for at least 10-15 years. This deficiency may force the General Staff to continue relying on more territorial, "brute-force" solutions to military challenges, most notably the employment of nuclear weapons.

But the current strategy of selective investment coupled with careful analysis of U.S. vulnerabilities could enable Russia to compete with and even surpass U.S. forces in specific operational niches -- such as information/electronic warfare -- long before the RMA is generalized throughout the Russian military. Current U.S. military doctrine refers to such niche threats as "asymmetrical warfare." The U.S. vulnerabilities that Russia has chosen to exploit are technological, doctrinal, organizational, and cultural. Even when the vulnerabilities in question are not technological (e.g., American aversion to casualties), Russia may be able to use emerging military technologies to more fully exploit them. Over the longer term, a restoration of economic vitality may enable the Russian military to "leapfrog" U.S. capabilities because many of the technologies in question involve dual-use applications that are readily available in global commerce.

Serious military reforms are more likely now that General Rodionov is defense minister. His radical reform plan includes slashing the Ground Troops, altering defense budget priorities in favor of information and emerging technologies, and significantly delaying planned weapons procurement in order to expand the R&D base. Unlike his predecessor, he is convinced that there is no alternative to radical reforms, and his acceptance of Russia's economic limitations will allow a better working relationship with other government officials. While he faces an uphill battle, his planned reforms create the basis for a gradual increase in Russian military capabilities over the next decade.

Russian military scientists note that they have fully developed the theory of information warfare, as well as the methodological foundations for conducting a future "reconnaissance-strike operation." But "the pragmatic Americans," they say, "have undertaken the resolution of individual issues without having resolved general issues." Indeed the U.S. government currently views Russia as a Third World country -- albeit

with massive nuclear megatonnage. This research provides a basis for a more prescient vision of the nature and capabilities of the Russian Armed Forces in the 21st century -- especially in the sphere of information warfare.

INTRODUCTION

> *"The high effectiveness of 'information warfare' systems, in combination with highly accurate weapons and 'non-military means of influence,' make it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population. In other words, the effect of using these means is comparable with the damage resulting from the effect of weapons of mass destruction."* (General Viktor Samsonov, Chief of the Russian General Staff, 23 December 1996)

Many Western analysts assume that during the next 15 years, only the United States has the capability to implement the new revolution in military affairs (RMA) -- that only the U.S. military will be able to integrate all of its elements into a cohesive whole. The question of what specific aspects of it other nations might obtain, when they might do so, and what implications that would hold for U.S. forces is an important one. As a result, U.S. policy-makers can only benefit from analyzing the long-term vision of military powers such as Russia.

In the early 1980s, the Soviet military was perhaps the first to argue that a new "revolution" was occurring in military affairs. Today the Russians argue that precision-guided, non-nuclear, deep-strike weapons and the systems used to integrate them are revolutionizing all aspects of military art and force structure -- and elevating combat capabilities on the order of 10^6. Russia's first official military doctrine, approved by President Yel'tsin and the Security Council in November 1993, clearly reflects the ongoing civil-military consensus on the nature and requirements of the new RMA. The document directs that R&D efforts focus above all on the development of the new deep-strike weapons and advanced C^4ISR/electronic warfare (EW) assets.

Despite the ongoing economic chaos in Russia, the Russian General Staff continues to plan for a future "air-space war." For the short term, they have explored sophisticated technical and operational countermeasures to the new technologies of the "air-space war." For the long term, they have oriented much of their limited resources toward creating an infrastructure that ensures "rapid surge production" of these technologies as the situation warrants. For the transitional period between the two, they have resurrected nuclear war-fighting to cope with a variety of worst-case scenarios. Both civilian and military leaders agree that military-technical potential for competing in the RMA represents Russia's main guarantee for preserving its hard-won superpower status.

According to the Russian military, superiority in the RMA proceeds from superiority in "information warfare (IW)": 1) reconnaissance, surveillance, and target acquisition (RSTA) systems, and 2) "intelligent" command-and-control systems. There has clearly appeared a specific field -- information -- the gaining and holding of superiority in which can play the decisive role in the achievement of success by one of the opposing sides. The "formula for success" in the modern battle or operation is approximately thus: First gain superiority on the air waves, then in the air, and only then by troop operations. This is compared with the fact that in World War II success depended largely on how successfully air superiority was gained, and in World War I on how effectively the fire resources of the troops themselves, and especially of the artillery, were used.

Thus, armed conflict today can be viewed as the aggregate of two components, electronic-fire and information, each of which has only the objects, resources, and

methods inherent to it. By the electronic-fire component of armed conflict the Russians mean that field which is defined by the capabilities of means of fire destruction and electronic warfare; i.e., of means capable of having a direct effect on enemy equipment and personnel. The information component is understood to be the field defined by the capabilities of resources that provide for acquiring information (reconnaissance) and using it (command and control) in the interest of increasing the combat potential of the resources that have a direct effect on the enemy (fire destruction and electronic warfare resources).

Under conditions of parity in nuclear and conventional weapons, superiority in reconnaissance, command and control, and electronic warfare is said to be the main factor in raising the qualitative indices of weapons and military equipment, which will have a "decisive" effect on the course and outcome of combat operations. Under all circumstances the side that has advantages in these areas will always possess greater capabilities, even if the other side has definite advantages in nuclear and, even more so, conventional weapons.

In the Russian view, the contribution to armed conflict of the information component, and of the main means of combatting it -- electronic warfare -- is becoming more and more important. The idea about the appearance, along with conflict on land, at sea, and in the air and space, of a fourth realm -- information, to which all categories, concepts, and methods of military art extend -- is more and more taking shape. The concept of "information warfare" is obtaining ever greater "citizenship rights," and gaining superiority in it is becoming a factor that determines the military-technical superiority of one side over the other.

These circumstances require that the capabilities of reconnaissance, command and control, and electronic warfare be taken into account in the generalized potentials of groupings of troops (forces, weapons, combat equipment) and, consequently, also be taken into account at disarmament negotiations, in determining parity of the sides. Finally, determination of the military budget as a whole, as well as its distribution among individual directions for developing weapons and military equipment, must take into account the correlation of the combat potentials of the sides that is taking shape, and the contribution of each of the means of waging armed conflict to the generalized combat potential of troops (forces). In the Russian view, the experience of exercises and local wars has demonstrated that the most advisable way of increasing combat capabilities (according to the cost-effectiveness criterion) is not increased numerical strength or kill capability of arms and military equipment, but their information support (outfitting with electronic systems and computers), above all for weapons and for EW, intelligence, and command-and-control systems and equipment.

An analysis of the Gulf War is said to demonstrate that owing to "intellectualization" of the precision weapons systems employed in this war -- i.e., giving them elements of "logical deduction" -- an opportunity appeared to make decisions essentially in real time. Because of sharply reduced time for the cycle of command and control both of weapons and personnel (excluding man as an intermediate element in evaluation-calculation operations of preparing variants of decisions and of command and control), this considerably increased their effectiveness and reduced the number of servicemen. Confirmation of this is said to be the rather effective battle, demonstrated for the first time, of Patriot surface-to-air missile systems against Scud missiles, which today forces one to take a quite different look at the

significance of ABM defense. Various automated combat support equipment, complexes, and systems managed to be integrated into a common intelligence and command-and-control system in this war, also thanks to "intellectualization." Its high combat capabilities were convincingly proven by the successes of Desert Storm.

In short, Russian experts argue that the development and adoption of intelligent command-and-control systems elevate command and control of forces and weapons to a new level both in peacetime as well as war. They will be economical and will permit finding necessary solutions and determining necessary personnel and equipment for achieving objectives without an actual costly, multi-variant practical check. In the Russian view, swift expansion of work on this problem is extremely necessary in view of the reduction in defense expenditures and can contribute to the development of new, highly effective technical equipment and technologies.

The Russian military argues that EW has become a form of the offense against precision weapons and advanced C⁴ISR systems. It is capable of achieving surprise by "blinding" the electronic equipment of reconnaissance and air defense systems. It is also capable of thwarting the enemy's surprise because it acts instantaneously over great distances; i.e., earlier than enemy firepower. Finally, EW can decrease the effectiveness of deep strikes during air-land operations by disrupting both the control of missile systems and the coordination between ground forces and aviation. In the Russian view, EW training has become a necessary element at all levels of military art, and it is now legitimate to speak of the creation of a new combat arm -- the EW Troops.

The Russian military now argues that, as the most dramatic force multipliers, advanced C^{4}ISR and EW systems must govern the allocation of scarce defense resources. Civilians such as President Yel'tsin and Deputy Defense Minister A. Kokoshin -- head of the Military-Technical Policy Council -- have repeatedly echoed this assessment. These systems represent the most cost-effective way to increase combat capabilities without increasing the quantity or even quality of weapons systems. They must also be included in any equations involving combat potential in all future arms control negotiations; the crushing weight of these systems has negated the quantitative paradigm that formerly constituted the heart of such calculations. Warfare has indeed shifted from being a duel of strike systems to being a duel of information systems.

The Russian military hierarchy clearly understands the strategic and tactical implications of the new RMA, and has developed a detailed planning framework for generating appropriate responses. The need to spend a disproportionate share of scarce military resources on developing such responses is recognized by all senior military officers. Notwithstanding the high priority assigned to the RMA, Russia is unlikely to possess the economic and technological resources to match the U.S. in advanced military technologies for at least 10-15 years. This deficiency may force the General Staff to continue relying on more territorial, "brute-force" solutions to military challenges, most notably the employment of nuclear weapons.

But the current strategy of selective investment coupled with careful analysis of U.S. vulnerabilities could enable Russia to compete with and even surpass U.S. forces in specific operational niches -- such as information/electronic warfare -- long before

the RMA is generalized throughout the Russian military. Current U.S. military doctrine refers to such niche threats as "asymmetrical warfare." The U.S. vulnerabilities that Russia has chosen to exploit are technological, doctrinal, organizational, and cultural. Even when the vulnerabilities in question are not technological (e.g., American aversion to casualties), Russia may be able to use emerging military technologies to more fully exploit them. Over the longer term, a restoration of economic vitality may enable the Russian military to "leapfrog" U.S. capabilities because many of the technologies in question involve dual-use applications that are readily available in global commerce.

Serious military reforms are more likely now that General Rodionov is defense minister. His radical reform plan includes slashing the Ground Troops, altering defense budget priorities in favor of information and emerging technologies, and significantly delaying planned weapons procurement in order to expand the R&D base. Unlike his predecessor, he is convinced that there is no alternative to radical reforms, and his acceptance of Russia's economic limitations will allow a better working relationship with other government officials. While he faces an uphill battle, his planned reforms create the basis for a gradual increase in Russian military capabilities over the next decade.

The U.S. government currently views Russia as a Third World country -- albeit with massive nuclear megatonnage. This research provides a basis for a more prescient vision of the nature and capabilities of the Russian Armed Forces in the 21st century -- especially in the sphere of information warfare.

KEY RESEARCH FINDINGS

NATURE OF INFORMATION WARFARE (IW)

Russian military scientists assert that IW has three components that encompass the totality of actions which ensure victory over the opponent in the information sphere. The first component is the complex of measures for acquiring information on the opponent and the conditions of the conflict (radioelectronic, meteorological, the engineering situation, etc.); the collection of information on his troops; and the processing of information and its exchange between command-and-control organs (points) in order to organize and conduct combat actions. Information must be reliable, precise, and complete, and its transmission must be selective and timely. A logical name for these tasks is "information support of troop and weapon control."

The second component of IW is opposition to the information support of the opponent's troop and weapon control ("information opposition"). It includes measures to block the acquisition, processing, and exchange of information as well as the insertion of disinformation at all levels of the information support of the opponent's troop and weapon control.

The third component consists of measures to defend against the opponent's information opposition ("information defense"), which includes actions to unblock information required for fulfilling the tasks of control, and to block disinformation disseminated and inserted into the control system. Information defense enhances the effectiveness of information support under conditions of the opponent's information opposition (see Figure 1).

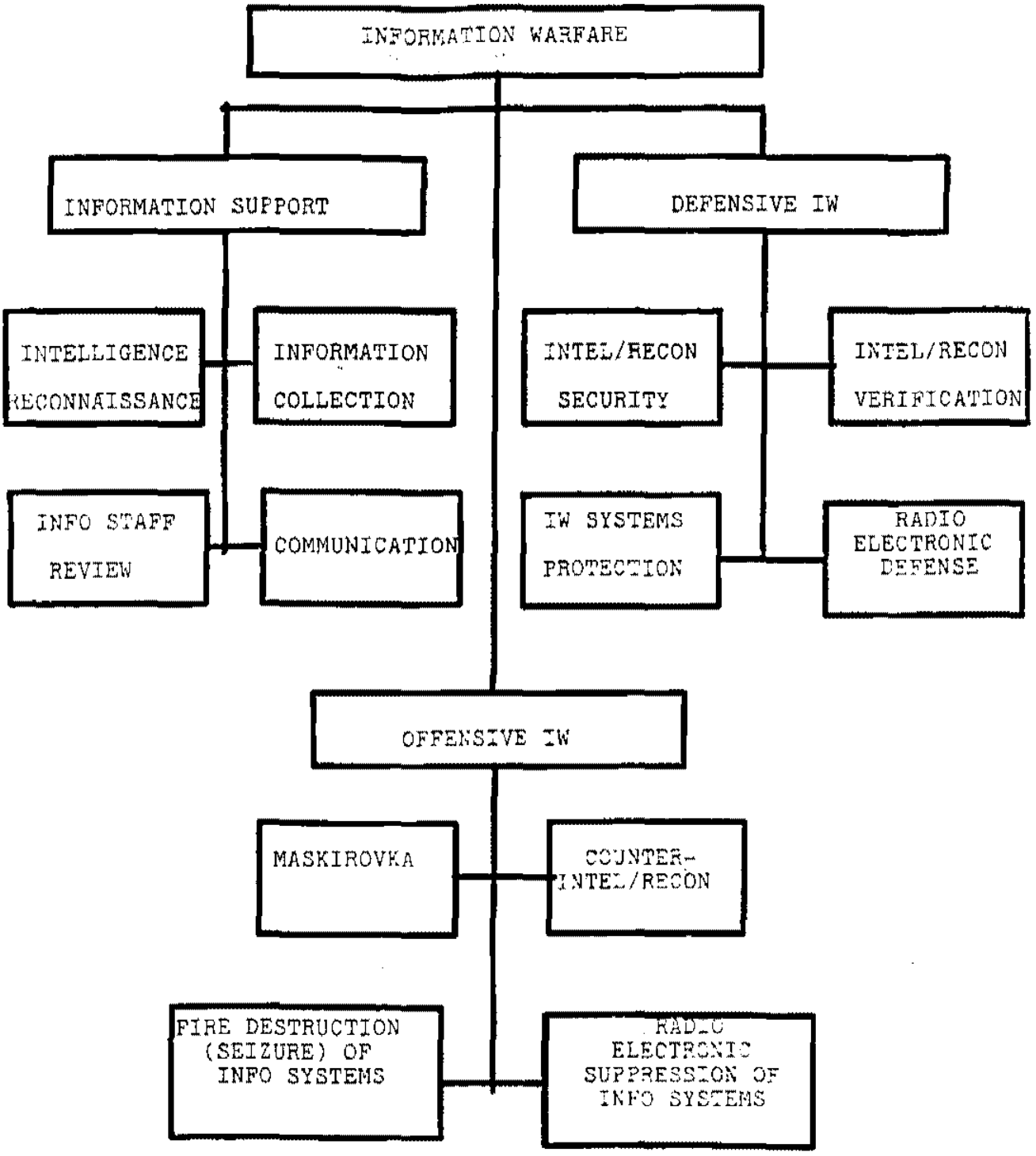
INFORMATION WARFARE
INFORMATION SUPPORT
DEFENSIVE IW
INTELLIGENCE RECONNAISSANCE
INFORMATION COLLECTION
INTEL/RECON SECURITY
INTEL/RECON VERIFICATION
INFO STAFF REVIEW
COMMUNICATION
IW SYSTEMS PROTECTION
RADIO ELECTRONIC DEFENSE
OFFENSIVE IW
MASKIROVKA
COUNTER-INTEL/RECON
FIRE DESTRUCTION (SEIZURE) OF INFO SYSTEMS
RADIO ELECTRONIC SUPPRESSION OF INFO SYSTEMS

FIGURE 1

The ultimate objective of IW is to achieve information dominance over the opponent; i.e., a situation wherein the information quotient of one's own troop and weapon control organs is more complete, precise, reliable, and timely than that of the opponent's corresponding control organs. Thus, the Russians define information warfare as a complex of measures for information support, information opposition, and information defense conducted according to a single concept and plan in order to seize and maintain information dominance over the opponent in the preparation and course of combat actions.

According to Russian military scientists, the essence of the new, 4th RMA is victory in information warfare. The United States calls this component different things: information struggle, information war, warfare against enemy command-and-control entities, etc. It is based on use of existing U.S. superiority in the spheres of communications, cybernetics, and information science; in modern methods of collecting, gathering, and analyzing intelligence; in processing and transmitting data at a high rate; and in the methodology of modeling; i.e., on superiority in information systems, which permits destroying the enemy battle management system architecture while preserving their own battle management systems. Russian experts thus argue that information weapons are a 21st-century weapon capable of replacing today's weapons of mass destruction.

The ideas and material foundations of information weapons were formed simultaneously with the development of society's information environment. Computerization of various spheres of public life, electronic communications, databases and data banks, the latest information technologies, and the transformation of

programming into a prestigious and mass specialty created the basic scientific, technological, and economic prerequisites for the emergence of a new type of information weapon, and at the same time made command and control, communications, power engineering, transportation facilities, and the banking system quite vulnerable with regard to the information effect. "American experts" list the following information effect attack systems:

a) computer viruses that can multiply and attach themselves to programs, be transmitted via communications lines and data-transmission networks, and penetrate electronic telephone exchanges and command-and-control systems and disable them;

b) logic bombs, so-called applications software that have previously been introduced into the information and command-and-control centers of the military and civilian infrastructure that are activated according to a signal or at a prescribed time and destroy or distort information or disrupt the operation of hardware or software systems. One of the varieties of this bomb -- the "Trojan Horse" -- is a program that permits one to carry out hidden unsanctioned access to enemy information resources to extract intelligence information;

c) systems to suppress the exchange of information in telecommunications networks, its falsification, and the transmission of needed information (from the position of the opposing side) via state and military command-and-control channels, and also via mass media channels; and

d) techniques and systems that permit the introduction of computer viruses and logic bombs into state and corporate information networks and systems and their remote control (from the introduction of microprocessors and other components into electronic devices sold on the world market to international information networks and systems that are managed by NATO and the United States).

The facilities that are most vulnerable to these systems are those that must maintain an uninterrupted capacity to operate or function in real time. Based upon the assessments of "foreign experts," the probability of the restoration of automated air-space attack early-warning systems, anti-ballistic missile command-and-control systems, and other strategic systems is sufficiently low so that the results of purposeful interference in their operation could be catastrophic in nature and comparable in possible damage with the consequences of the employment of nuclear weapons.

A sober assessment is needed of today's situation and of the specific features and prospects for the development of information weapons and the techniques for their employment. That assessment is the basic prerequisite for the development of Russia's foreign and domestic policy, the military and military-technical components of which could prevent or counter threats that have arisen and reliably guarantee the country's security. In the process, it is important to understand that the threat of information warfare in a broad context is a factor of latent military-political pressure and, possibly, intimidation, a factor that is capable of disrupting strategic parity and undermining the balance of the two great powers that has taken shape on the world political scene. That is why monitoring threats of the employment of information weapons and the permanent assessment of the effectiveness of the functioning of systems to counteract these weapons must be carried out on such a broad scale.

A natural reaction to the appearance of a new high-technology weapon is the development of adequate countermeasures. This must be a question not only of technologies for the detection of the effects of information weapons but also some kind of "early-warning systems." Further, Russia must provide for the continuous

improvement and development of hardware and software methods to prevent the loss, damage, destruction, distortion, or interception of information, including the exclusion of unsanctioned access to it and cryptographic information protection systems during transmission via communications channels. In general, it is possible to directly counter the effect of information weapons using hardware and software methods. These methods must be supplemented by information weapons counter-control methods and also by varied legal and organizational-economic measures directed at the protection of state information resources.

The experts also assert that Russia needs to intensify the development of its own information weapons as an integral part of weapons and military equipment. The security of the state requires the leveling of the correlation of forces for information weapons: the probable enemy must know that he himself is vulnerable.

And, according to the Russians, this is only the beginning. The possibilities of information war are increasing in response to the improvement and spread of micro-processors, high-speed data-receiving and processing systems, and sophisticated sensors -- powerful weapons in the hands of those who know how to use them. Various specific means will be used actively in information war, above all software products -- computer viruses, logic bombs, computer "chips" -- which, installed in weapons supplied to a probable enemy, will make them ineffective while appearing reliable outwardly. It is also proposed to use explosive devices producing a powerful EMP (such devices, the size of an ordinary suitcase, already have been created at Los Alamos National Laboratory), and even biological agents, particularly a special kind of microbes capable of destroying electronic circuits and insulating materials. Although

information war may precede or replace combat operations, the methods and equipment used in its course significantly increase troop capabilities and compensate for a shortage of conventional forces and arms.

Soviet/Russian experts stress that the enhanced effectiveness of weaponry resulting from its "intellectualization" underlies many of the current, revolutionary changes in military affairs. The very first phase of "intellectualization" should lead to a radical transformation of weapons systems and methods of their use. The next phase, in which automation encompasses the decision-making processes involved in using weapons, could generate radical changes in the organizational principles of armed forces. It will robotize the battlefield and dramatically lower the numerical requirements of armed forces while dictating much higher training requirements. Changes in the structure and functions of different branches of the armed forces will probably occur during this phase.

In the "intellectualization" arms race, competition might not take the form of the quantitative accumulation of arsenals, but of the augmentation of the possible varieties of programmed behavior in weapons systems; i.e., the accumulation of intellectual potential "isolated" in a programmed product. The arms race is moving into the sphere of software: the richer the variety of possible forms of behavior by self-contained systems or of premeditated alternative decisions, the more effectively the warring army can use its resources. As a result, the incorporation of information sciences into the military sphere will not merely change the specifications and performance characteristics of weapons, but will create a new military-political situation differing

radically from that which existed when the "intellectualization" of weapons had just begun.

According to the Russian military, superiority in the RMA proceeds from superiority in C⁴ISR systems: 1) reconnaissance, surveillance, and target acquisition (RSTA) systems, and 2) "intelligent" command-and-control systems. The "formula for success" in the modern battle or operation is approximately thus: First gain superiority on the air waves, then in the air, and only then by troop operations. This is compared with the fact that in World War II success depended largely on how successfully air superiority was gained, and in World War I on how effectively the fire resources of the troops themselves, and especially of the artillery, were used.

Thus, armed conflict today can be viewed as the aggregate of two components, electronic-fire and information, each of which has only the objects, resources, and methods inherent to it. By the electronic-fire component of armed conflict they mean the field which is defined by the capabilities of means of fire destruction and electronic warfare; i.e., of means capable of having a direct effect on enemy equipment and personnel. The information component is understood to be the field defined by the capabilities of resources that provide for acquiring information (reconnaissance) and using it (command and control) in the interest of increasing the combat potential of the resources that have a direct effect on the enemy (fire destruction and electronic warfare resources).

Under conditions of parity in nuclear and conventional weapons, superiority in reconnaissance, command and control, and electronic warfare is today the main factor

in raising the qualitative indices of weapons and military equipment, which can have a "decisive" effect on the course and outcome of combat operations. Under all circumstances the side that has advantages in reconnaissance, command and control, and electronic warfare will always possess greater capabilities, even if the other side has definite advantages in nuclear and, even more so, conventional weapons.

These circumstances require that the capabilities of reconnaissance, command and control, and electronic warfare be taken into account in the generalized potentials of groupings of troops (forces, weapons, combat equipment) and, consequently, also be taken into account at disarmament negotiations, in determining parity of the sides. Finally, determination of the military budget as a whole, as well as its distribution among individual directions for developing weapons and military equipment, must take into account the correlation of the combat potentials of the sides that is taking shape, and the contribution of each of the means of waging armed conflict to the generalized combat potential of troops (forces). The experience of exercises and local wars has demonstrated that the most advisable way of increasing combat capabilities (according to the cost-effectiveness criterion) is not increased numerical strength or kill capability of arms and military equipment, but their information support (outfitting with electronic systems and computers), above all for weapons and for EW, intelligence, and command-and-control systems and equipment.

A new power deterrence factor -- the threat of inflicting irreparable damage on a particular country's information resources -- is therefore forming in the system of confrontation of new geopolitical associations of states. This can be done overtly or covertly, in the form of information opposition. The most complicated form of such

aggression is to control the decision-making process in state structures under the effect of specific information or disinformation. The following types of information subversion can occur: disrupting the information exchange procedure and illegally using and collecting information; having unsanctioned access to information resources; manipulating information (disinformation, its concealment or its distortion); illegal copying of data from information systems; and theft of information from data bases and banks.

For sides possessing more developed information resources, the losses also will be more appreciable in case of large-scale use of means of special software damage. This is why, in assessing the possibilities of deterring a probable aggressor with the threat of retaliatory nuclear and conventional damage, the possibilities of information damage; i.e., of a special software engineering effect on the enemy, also must be borne in mind. It is this factor that may become a deterrent to the initiation both of a nuclear as well as of an information war. Thus, the development of information means of warfare becomes an additional guarantee of peace and of development of cooperation among countries for strengthening military-strategic stability. But this in no way means that the military threat has been eliminated. This is why, in developing the Russian military reform concept, it is also necessary to take into account new methods of waging a quiet (information) war.

Achievements in the spheres of communications, cybernetics, and information science as applied to new methods of collecting, processing, and rapidly communicating intelligence to forces; in the methodology and methods of computerized simulation of the situation and operations; in the field of crypto-analysis and so on have

generated such new concepts in modern military affairs as "information war." The concept of information war is to show a potential enemy superiority in intelligence and in the capability of blinding, deafening, demoralizing, and decapitating the command-and-control system of its armed forces and of the state as a whole, and in the ability to neutralize his computer equipment and communications assets, disrupt information processes, and destroy information systems and resources "at global distances and with the speed of light." This is supposed to induce a probable enemy to reject war, having understood its lack of prospect for himself. If intimidation does not work, use all available means en masse for victory. In other words, achieve your goals:

- in peacetime by electronic intimidation;
- in a period of threat by a use of electronic means against military and civilian information and command-and-control structures that is selective in terms of targets but massive in terms of intensity; and
- during a military conflict by massive use both of electronic as well as of fire-delivery means against all systems of the aforementioned targets.

A particular kind of information war is the destruction by "nonlethal weapons" (electronic weapons) of the most important elements of military industry and the civilian regional infrastructure by disabling, for example, power supply, communications, transportation, and other installations. But information warfare, and above all warfare against command-and-control systems (IW/C^2W), has two main goals:

- offensive -- to deceive, disorganize, or destroy the enemy information infrastructure; to confuse, disorganize, or totally disrupt the process of operational command and control of his forces and assets for rapid neutralization of resistance;

- defensive -- to protect the friendly information infrastructure and the command-and-control process against enemy effect.

Making simultaneous and maximum possible use of all means and methods of warfare in their close interaction for achieving the highest results and concentrating main efforts on destroying the most important vulnerable links of the enemy information infrastructure and command-and-control system are a guarantee of success here. Radars, surveillance and reconnaissance equipment, communications centers and lines, transmitting and receiving components of communications centers, radio-relay stations, fixed navigational equipment, television and radio broadcasting stations, and so on can be included among vulnerable links of the information infrastructure. Other vulnerable links are elements of the support infrastructure -- electrical power stations, power supply lines, and so on.

Critically important vulnerable links include the most important components of the command-and-control system, the destruction or annihilation of which will entail an immediate decrease in capabilities for command and control of troops and forces and for effective conduct of combat operations. They include military and civilian command-and-control entities at all levels with their electronic equipment (electronic computers, automated control systems, electronic data bases communications systems, situation display systems, and so on), and satellite surveillance, reconnaissance, communications, and navigation systems. Imagine the chaos that would arise as a result of a shutdown of computers and technical and information systems serving, for example, a city's municipal economy.

The Russians describe five aspects of IW/C²W. Deception is an element of stratagem which "controls" the enemy by creating a false impression in him of the actual situation and status of forces opposing him and about the concept, time periods, and nature of their operations, forcing him to act in a predictable manner unfavorable to himself.

Operations security is a disruption of enemy efforts to diminish the effectiveness of operations by opposing forces. Added here to various methods of protecting friendly information systems are measures for countering enemy intelligence, maskirovka, secrecy of the operational concept, electronic countermeasures, delivery of fire, and so on. Methods of psychological operations in information warfare include praising one's own way of life; intimidating servicemen and the population of the enemy country by the might of one's war machine; undermining their faith in their own military and civilian leaders; sowing dissatisfaction and psychosis; inciting disobedience, desertion, and surrender; and fanning defeatist and capitulationist sentiments.

The final aspect of IW/C²W is destruction. By 2000 one can expect the appearance of a so-called remote virus weapon against computers. This computer virus, such as in the form of automatic and controlled software inserts and interference, will be introduced via radio channels and laser communications links between central computers and user terminals. One hardly can overestimate the danger of a remote virus weapon to automated control systems and above all to command and control of strategic missile complexes. While destruction is achieved now basically by fire-delivery weapons, in the near future it will be done more and more with electronic means.

The Russians also assert that SHF-generators ("microwave weapons"), intended for disabling space-based, airborne, ground-based, and sea-based electronic gear by means of a powerful, directed-effect electromagnetic pulse, will become a new means of warfare against command-and-control, communications, computer support, and intelligence systems by 2005-2010. Depending on type and location, the effective casualty zone of such generators will vary from several hundreds of meters for a cruise missile to several tens of kilometers for heavier platforms. Figuratively speaking, such selective and massive electronic and fire strikes will achieve paralysis of the enemy nervous system -- his brain, nerves, and organs of sense; i.e., the command-and-control, communications, computer support, and intelligence systems.

The Russians argue that information war occupies a position between a "cold" war, which includes in particular economic war, and a "hot" war. In contrast to an economic war, the result of an information war is actual disrupted functioning of elements of the enemy infrastructure (command-and-control facilities, missile and launch positions, airfields, ports, communications systems, depots, and so on. In contrast to a "hot" war with the use of conventional and/or mass destruction weapons, it is aimed not at material, but at "theoretical" objects, symbolic systems, or their physical media. At the same time, such objects and systems can be destroyed while their material basis is preserved.

INFORMATION SECURITY

According to Russian military scientists, the following substantial groups of information and technical dangers can be singled out. The first group is related to the rapid development of a new class of weapons -- information weapons -- which are

capable of effectively influencing both people's consciousness and psychology and also the informational and technical infrastructure of society and the army. At the present time many new means have been created to produce an impact on people's minds and to manipulate their behavior. According to foreign sources, no methods have yet been found to exercise a steady and predictable direction of people's collective behavior. Yet such research programs are being conducted. Periodically reports appear in the press about the U.S. MK-Ultra program and also analogous programs in France, Japan, and other countries. Achievements in this field are such that it is already possible to talk about the effectiveness of "zombifying" (programming the behavior and activity of) particular individuals. For this purpose not only pharmacological means but also psychotropic generators have been created and are being used.

According to Russian military scientists, states with a well-developed information science sphere are preparing for a computer war and developing and testing methods of affecting computer systems. There is no question that the effectiveness of computer counteraction will be fairly high. This is evidenced by the fact that Iraq could not use the air defense systems bought in France against the MNF. Their software contained logic bombs that were activated with the start of hostilities. The use of such a bomb or a virus will apparently be capable of producing the same results as conventional bombing of a state administrative body or a combat control post (center). Therefore attempts will be made to mine all state administration and military computer systems (primarily all valuable systems and networks) with logic bombs and infect them with viruses waiting for their ultimate hour. Information terrorism is also bound to appear. It is therefore necessary that Russia make special preparations for all of this and provide for countermeasures.

Along similar lines, Rossiyskaya gazeta announced in 1995 that Russia is turning into a state which is utterly defenseless in the face of the use of "information weapons": imported technology and foreign-made communications systems in state-run and financial-and-industrial entities pose a real threat to the country's security. In order to get out of the situation, the Russian government has decided to reduce to the minimum the import of communications systems and combine the efforts of Russia's competent agencies.

The growing role of information-technology warfare is rapidly lowering the barrier between war and peace. The armed forces of likely adversaries are in a state of constant information warfare, and military informatics works to accomplish tasks characteristic of war even in peacetime. Electronic warfare is being waged continuously. A war of computer networks is now beginning. An exchange of information strikes is becoming increasingly dangerous for the fate of peace, since the effectiveness of such strikes is rapidly increasing and it is extremely difficult to identify their sources.

Sources of information threats are divided into natural sources (objective sources that are not dependent on human will) and intentional. Intentional information effects are caused deliberately and with specific purposes in mind. This often involves the use of electronic news media, electronic warfare, special programs, computer "bombs," and so on. These techniques are so effective that one can speak of a new class of weapons -- information weapons.

The second type of information threat involves the introduction and input of false data. Information security in this field is provided by special structures that are charged with waging information-technology warfare and that neutralize disinformation-technology, foil attempts to manipulate public opinion, counter electronic warfare, and eliminate the effects of computer attacks.

Computer viruses can be divided into several types, depending on how they operate. The "Trojan horse virus" is introduced in the "victim" system, remains idle for a certain period of time, and then causes catastrophic destruction of the system (for example, a missile guidance system) or network into which it has been introduced.

The "forced quarantine" virus is introduced into a network and knocks out the program of the unit into which it was planted. In order to prevent the destruction of the entire system, its components have to be separated. Consequently, if an automated communication link network is attacked, it is immediately destroyed, and communication between its components is disrupted.

As concerns the "overload" virus, the clinical picture is different. This "virus" quickly spreads throughout the entire system and gradually slows its operation. The "sensor" virus penetrates a preplanned sector of a computer's data-storage area and, at a critical moment, destroys the data bank and its information.

According to Russian military experts, information security in automated control systems is acquiring paramount importance at the present time. Laws "On Legal Security of Computer Programs and Data Bases" and "On Copyright and Related

Rights" adopted by the State Duma unfortunately only partially solve the problem of protection against "computer piracy," and they especially do not guard against unsanctioned access to information in military computer networks.

INFORMATION WARFARE LESSONS FROM DESERT STORM

Russian experts stress above all the use of electronic warfare systems in MNF combat operations in Iraq. They remain awestruck by the duration of the electronic phase, the quantity of systems employed, the simultaneity of effect on Iraqi C^2 at all levels, and the synergism of EW and fire strikes. It was the availability of powerful electronic warfare means, as well as their effective usage against Iraqi electronic means, that reliably ensured MNF operations in the air and on the ground. In practice the MNF conducted combat operations against an enemy whose control systems had been effectively disorganized. Suffice it to say that spectral hardness of intended interference in some cases reached 4000 w/me and more, which excluded the use of Iraqi air defense radars and ultra-short wave communication systems.

The Russians come to the following tentative conclusions regarding the Gulf War:

1. The modern "electronic-fire" concept of combat operations was demonstrated once again. Operations aimed at ensuring superiority over the enemy in reconnaissance, control, and electronic warfare constituted its basis. Radical changes in the nature of the armed struggle are becoming more and more obvious. During this struggle the superiority in information of one side over another becomes the indispensable factor ensuring victory. The concept "information war" increasingly

acquires real meaning. One can trace a historic law of ensuring success in combat operations. In World War I it was achieved by superiority in fire means of troops (forces), first of all in artillery ("fire superiority"). In World War II, as well as in the local wars of the fifties and beginning of the sixties (Vietnam, Korea) it was achieved by superiority in the means of air attack (gaining of "air supremacy"). Today's reality is actions aimed at gaining superiority over the enemy by disabling control systems and means, or "gaining of radio and electronic superiority", because now the basis of armaments and military equipment is electronic means and systems.

Thus, in order to succeed in modern combat operations, it is necessary above all to gain "radio and electronic superiority" during fighting, then to obtain "air superiority" and "fire superiority", and after that to engage troops to seize the enemy's territory. Taking into account the destructive capabilities of modern weapons, combat operations without these measures will always be characterized by heavy losses in personnel and materiel.

2. The success of the MNF in many respects was achieved by the effectiveness of disorganizing the enemy's control of troops and weapons, which was conditioned by punctual organization of a complex employment of reconnaissance forces, main attack forces, and electronic warfare means based upon a wide-scale use of automated control systems. Today actions against the enemy's reconnaissance and control of troops and weapons, as well as protection of one's own troops against the enemy's high-precision weapons and radio interference are becoming the most important tasks of forces.

3. The primary importance of electronic warfare forces and means in the armed struggle -- as the main component of the struggle for superiority over the enemy -- proved correct. This principle manifested itself particularly in the struggle between air forces and air defense, which was the essence of combat operations in the initial period of the war. The availability of a large number of different types of electronic warfare means required punctual coordination between them in the interest of ensuring their massive use in the decisive stage of combat operations. The corroboration of this is the coordination of the operations of electronic warfare means of the MNF ground and air force groupings in time, place, and object of actions, which ensured reliable neutralization of the electronic means of Iraqi air defense systems.

4. The level of electronic countermeasures of air defense EW means becomes the factor that will determine their combat stability and combat employment effectiveness. Special importance is attached to such air defense countermeasures as multifrequency of the employed electronic means; the capability to counteract the enemy's interference; the availability and organization of reconnaissance and destructive means based on the use of various physical principles; and the integration of electronic warfare units into air defense groupings, their rational deployment and use in operational formations of air defense forces, etc.

NEW C^{4}ISR SYSTEMS AND CONCEPTS

According to Soviet/Russian military scientists, the new RMA dictated a re-examination of C^{3}I systems, and a quest to develop an automated "control system" that will optimize the employment of forces according to the projected nature of future war. The logical result will be changes in the methods of armed combat. Soviet experts

predicted that forms of forcible confrontation and pressure will be replaced by flexible and maneuverable forms and a return to the "blitzkrieg" concept. The "intellectualization" of weapons will magnify the ability of warring armies to concentrate their forces in certain maneuvers or to use them selectively and with the highest precision. This ability will be achieved by the "intellectualization" of all levels of command and control -- from self-contained weapons systems to decision-making systems on all levels. The increase in artificial intelligence (controllability) allows relatively small forces to achieve their objectives.

Information technologies have become one of the main criteria for the modernity of armed forces. They are acquiring special significance because an intense struggle for more effective information support is being waged in the sphere of command-and-control systems. The struggle is bloodless at first glance, primarily in the spheres of equipping troops with technical C^3I systems and improving organizational structures and personnel training of command-and-control posts. In fact, however, judging by the Persian Gulf conflict, lagging behind in the sphere of command and control in modern war is fraught with great losses.

According to the Russian military, warfare has shifted from being a duel of strike systems to being a duel of information systems. As a result, military experts have repeatedly discussed current possibilities for developing "intelligent" C^3I systems in order to elevate the combat potential of the post-Soviet Air Force and Air Defense Troops. Along with the development of offensive air-space weapons which are being created with new technologies, the United States and NATO are said to be paying special attention to systems for command and control of forces and weapons. Mass

production of precision weapons leads to intensification of instability and the temptation, in case of war, to use them to destroy strategic nuclear forces and other very important installations by a preemptive mass attack using only conventional weapons. The time factor acquires decisive importance under these conditions, which is especially important in connection with the fact that it is proposed to involve essentially all branches of the armed forces and combat arms in modern strategic operations. This in turn requires appropriate processing and transmission of an enormous volume of various data in extremely limited time periods exceeding the capabilities of existing command-and-control systems.

According to Russian military scientists, modern conditions are characterized by a significant growth in the extent and content of command-and-control missions and consequently also of information support to command-and-control systems. In addition, there is a persistent striving to achieve information dominance over the enemy by creating reconnaissance, command-and-control, and information systems based on the latest information technologies. This tendency is especially pertinent under present conditions, when the struggle against battle management systems becomes one of the priority missions in warfare. In this connection a new concept -- "information weapon" -- has appeared in military terminology, the essence of which is the effect not only on military, but also on state command-and-control system information flows to disrupt stability of command and control.

The principal problem in organizing information support to modern command-and-control systems is to resolve the contradiction between the increased volume of necessary information and the constant demand to reduce its processing time. This is

what determines tendencies in the development of these systems, including automated systems.

Military specialists now give ever-greater attention to "electronization" of command-and-control systems and outfitting them with mutually tied-in technical complexes intended for assisting commanders and other officials in accomplishing command-and-control and combat missions. Command-and-control systems more and more are becoming "man-machine" systems, since some functions are placed fully on technical equipment. The form of the information medium essentially is changing and missions are arising connected with the following: determining the limits of the information space in which a command-and-control system is operating; classifying and optimizing it; and developing forms and methods of its description and presentation necessary for the subsequent creation of automated and even conventional information systems.

For the purpose of making a detailed measurement of the effectiveness (MOE) of the command and control of troops, it is important to find out the essence of particular requirements ensuring its high effectiveness. The main requirements include stability, promptness, continuity, and undetectability. At the same time it is taken for granted that command and control must, of course, be of high quality. These requirements are sometimes interpreted as qualities of command-and-control systems.

Traditionally, command-and-control MOEs are divided into combat (external) and inherent (internal) ones. The combat MOEs are based on the use of combat effectiveness indicators of troop activities that are determined by mathematical models.

Since the effectiveness of combat operations depends on the strength of the sides' troops and the effectiveness of their command and control, the following technique is usually applied in order to find out which of the methods of command and control employed within one command-and-control pattern or system has greater advantages: by assessing the command-and-control method used by the enemy troops it is possible to determine their strength and missions and, subsequently, the MOEs of combat operations that are in line with various command-and-control methods or systems are compared. For instance, if a mathematical model of a frontal offensive or counteroffensive operation shows that by the 10th day of the operation the advance movement of the front troops was 260 km under an automated command-and-control system and 200 km without it, by comparing these figures one may draw a conclusion that the introduction of an automated command-and-control system in this particular example helped raise the effectiveness of combat operations by 30 percent. These calculations have been fairly widespread in the Air Defense Troops and other branches.

Without denying the usefulness of such approaches, Russian military scientists note that they point to a relative influence of efforts to perfect the command-and-control system while making it impossible to assess its essence; that is, to establish to what degree it corresponds to its missions. What is used for this purpose are measures of one's own effectiveness of command and control of troops. At the same time, the main measure of effectiveness of command and control of troops in operations should be interpreted as the degree of utilization by a command-and-control system of troop combat capabilities. This MOE can materialize only by using the appropriate models of combat actions and carefully taking into account the role that the command-and-control systems of the two sides have to play.

Disruption is now one of the most important operational tasks of troops. It is a mandatory condition for scoring success in a defensive (offensive) operation, especially in the initial period of war. The experience of local wars and military conflicts of recent times (primarily in the Persian Gulf zone) attest to the fact that a modern war on any scale begins by solving the task of disrupting state and military control. It is unequalled for its combat effectiveness and contributes in a big way to reducing enemy combat capabilities. This success is, however, temporary (it lasts as long as it takes to restore the command and control). Therefore it is necessary to strike blows at troops to consolidate it and to thereby change the correlation of forces in one's own favor.

These circumstances predetermine the general scenario for a possible development of war, especially of its initial period. It starts with an active struggle by the sides to win superiority in command and control through, among other things, launching a special disruption operation or massive delivery of fire or electronic attacks. The winning of supremacy in the air (outer space) will amount in this struggle to exploiting success, and only then will fighting start on land and sea.

Russian experts stress that information warfare is now assuming a priority importance that necessitates research and practical measures to create intellectual command-and-control systems (ICCS) on various levels that are capable of ensuring support for making a decision in real time. Analysis of combat operations by the MNF in the Gulf area gives one ground to conclude that the "intellectualization" of reconnaissance-strike systems (RSS), automated control systems (ACS), and combat support systems have made it possible first, to make decisions practically in real time; and second, to integrate them into a single reconnaissance, command, and engagement

system. The experience of that local war has shown that the existence of reconnaissance-strike systems, which carry out in-depth effective engagement and broad maneuvers of strikes, is the main factor making a difference between success and failure in the struggle for gaining and maintaining fire superiority over the enemy.

In contemporary operations, the immediate destruction of targets as they are spotted is becoming the sole acceptable method of combatting such facilities as offensive nuclear weapons, land-based elements of RSS, self-propelled artillery batteries, columns of armored vehicles, and individual priority facilities of enemy forces. Within the framework of the Missile and Artillery Troops of the Ground Troops, it is planned that this mission will be assigned to integrated reconnaissance-strike systems (IRSS) that ensure an autonomous reconnaissance of the above and other targets, target allocation, and the delivery of missile or rocket strikes at them with a full or partial automation of the command and control of all subsystems and their functions.

The attainment of a greater effectiveness of troop and weapons command-and-control systems requires a switch from automation to "intellectualization." Thanks to this an opportunity will arise to make decisions effectively in real time; the promptness and quality of command and control will considerably increase, while the overall number of servicemen involved in this process will decrease; and means of reconnaissance, command and control, effective engagement, and combat support operations will be integrated into a single system. The development and introduction of ICSs will ensure the achievement of a new level of command and control of troops and weapons, particularly the IRSS of the Ground Troops. Their use will make it possible to organize an optimum process of providing support for decision-making and

to estimate the forces and weapons required to fulfill missions assigned to them. The conduct of research in this area is indispensable since its results could help develop new, highly effective means of warfare and technologies.

Computerization of military command and control should eliminate current shortcomings and should also ensure a unified information base for existing and future command-and-control systems and the wide-scale introduction of new information technologies including artificial intelligence systems, military knowledge database systems, and technologies and hardware for designing specialized mathematical, programming, and information-linguistic backup. This is why at present the Ministry of Defense (the Chief of Communications of the Russian Federation Armed Forces Directorate), jointly with industry, is engaged in development work on the creation of a Ministry of Defense telecommunications network which is intended to provide, in conjunction with the state information-telecommunications network, information collaboration with state and local organs of power.

The Ministry of Defense telecommunications network is being built with due consideration for the command-and-control structure of the Russian Federation Armed Forces and consequently allows for the development of large-scale topology across Russia's entire territory, ensuring the exchange of data between territorial communications systems with stage-by-stage development of information systems at the regional level. The Ministry of Defense telecommunications network is also intended to ensure exchange of information in the interests of defense industry enterprises. It has virtually no limitations as regards expansion possibilities to provide access and service to subscriber facilities and is a distributive structure functioning on

the principles of packet switch networks. As far as subscribers are concerned, the Ministry of Defense telecommunications network is an open-type network whose architecture conforms with the internal seven-level standard model of open system interface.

In parallel with the development of its telecommunications network, the Ministry of Defense is also engaged in extensive research and development in the assimilation and utilization of the latest information technologies. These technologies are being used as a basis for the development of systems for the command and control of troops, weapons, reconnaissance, and combat support. In this work the Ministry of Defense gives preference to Russian industry and orders computer hardware, local area networks, software, and network equipment from Russian industrial enterprises.

Russian military scientists assert that forms of information and psychological opposition are being improved more and more. As a result, a breakthrough in electronic technologies at the beginning of the 21st century will permit the creation of computers based on atoms which will surpass the destructive capabilities of nuclear weapons in importance by several orders of magnitude. Thus the Cold War has not ended; it is merely acquiring a new form. This is why, in beginning to develop a military reform concept, it is impossible not to take into account the actual capabilities of information and psychological means of warfare. But for this a concept of information and psychological opposition is needed. It is even more necessary for the Russian Armed Forces to develop countermeasures in information and psychological opposition as quickly as possible.

The neurocomputers being developed in Russia may cause a revolution in military and financial spheres, according to a Russian defense industry official. Yuriy Glybin, deputy head of the State Committee for Defense Industry, said that neurocomputers (NPCs) use technologies based on artificial neurons which are similar to human neurons. Such computers are cheaper and smaller in size, but operate 1,000 times faster than traditional computers. Speaking at the 2nd Russian conference "Neurocomputers and Their Application" that opened in Moscow on 14 February 1996, Glybin said that NPCs can be used to develop state-of-the-art high-precision weapons, military equipment, optic devices to detect missiles, as well as in ABM programs, dual technologies, etc.

PSYCHOLOGICAL OPERATIONS

According to Russian military scientists, new weapons will appear according to dominant law-governed patterns. The appearance of new weapons will exert a deep influence not only on the methods of conducting war, but also on the definition of its ultimate objectives and the definition of victory itself. In both the past and present, victory has meant the results of employing armed forces on the battlefield to achieve the physical destruction of the opponent and the seizure and occupation of his territory. The use of new weapons or threat thereof will be directed above all at achieving the most important political and economic objectives without the direct contact of opposing forces and without combat actions as we traditionally know them.

For example, slow-acting means that exert a concealed influence on the opponent's armed forces and population may appear in place of traditional weapons. These means can be designed to undermine immune systems, destroy the life-sustaining

elements of the human organism and human society, and seriously limit or destroy the population's ability to survive.

Indeed, say the Russians, the most important objective of military conflicts in the near-term future may become affecting the psychology of the opponent -- individual, collective, and mass. The results of using several types of psychological weapons can either be direct and occur immediately after their use, or indirect and occur only after many years. Such weapons can be designed to destroy state and societal institutions, create mass disorder, degrade the functioning of society, and ultimately cause the collapse of the state. To achieve real victory in such a war, it is necessary to acquire a deep knowledge not only of the opponent's armed forces, but also of his state and political system, the most important decision-making processes and mechanisms of the military-political leadership, and in general how leadership functions are performed. The selectivity of the destructive capabilities of new weapons can result in the destruction of only the opponent's troops and population with no feedback effect on one's own troops and population.

The new nature of warfare has led to the emergence of special subunits involved in preparing and conducting psychological operations (PSYOPs) in the armed forces of a number of countries. Under combat conditions these subunits are reinforced by the actions of sabotage and reconnaissance subunits, military intelligence, public information services, and others. The organization of such operations is regulated by special directives and manuals, which are developed for the armed forces of individual countries, as well as for their blocs, alliances, and pacts. For example, on a NATO-

wide scale there is in effect a single directive on "Principles for Planning and Conducting Psychological Operations."

The system of psychological operations, which are subordinate to overall strategic goals, comprises psychological war, whose framework is significantly broader than the period of the combat operations themselves. The widespread use of forces and means of PSYOPs in the course of the Korean War, in Vietnam, and in the recent war in the Persian Gulf advanced this type of support of combat operations into the list of priority trends exerting influence on an enemy in the preparatory period of combat operations.

Depending on their level, psychological operations are subdivided into strategic, operational, and tactical. Psychological operations on a strategic level are planned and conducted to achieve long-term goals. The target of influence is the populace, the armed forces, and the government of the subject countries. The performance of such operations requires coordinated actions by both the military and various governmental structures.

Psychological operations on the operational level support the deployment of armed forces, as well as the initiation and successful execution of combat operations by large groups of forces. The basic features of propaganda and psychological actions carried out within the framework of operations at this level are that they directly or indirectly foster the defeat of enemy forces by evoking in the enemy lack of faith in the possibility of winning, and also prepare the populace of a country for the waging of

combat operations on its territory and provide for lowering its participation in the conflict.

Psychological operations on the tactical level are planned and carried out in the interests of achieving immediate and short-term goals in order to provide direct support to combat units and subunits. They are conducted with the idea of influencing enemy civilians and military personnel in the zone of responsibility of the commander of the tactical echelon.

A most important condition for the successful execution of psychological operations is considered to be constantly maintaining the offensive and holding the "psychological initiative." Calls for certain actions should only be made when the situation requires this and the target of influence is in a position to understand them and carry them out. The armies of various countries use almost identical technical means for conducting psychological operations:

- duplicating and printing facilities;
- a system of loudspeakers;
- means of distributing leaflets by artillery, aircraft, etc.;
- radio programs, television programs, and motion pictures made by the appropriate services; and
- systems for broadcasting radio and television which are mounted on ships, tanks, vehicles, helicopters, etc.

Russian military scientists note that it is important to clearly define information-and-propaganda support of operations. They propose that it should be understood as a system of information-and-propaganda (information-psychological) activities,

coordinated and interrelated in their objectives, tasks, targets, place, and time. They should be conducted by the commander, staffs, other command-and-control agencies, and special units according to a single concept and plan designed to shape a positive public opinion about troop activity, neutralize (weaken the consequences of) the negative informational-psychological impacts, boost the servicemen's morale, strengthen the psychological endurance of the civilian population, and create favorable conditions for executing the missions assigned to the troops.

The special formations responsible for the direct organization of information-and-propaganda support are public relations (press centers, public relations centers, and so forth), educational, and psychological operations (operational information, psychological defense, and so forth) agencies. Experience shows that such a triad of special agencies should be created in the Russian Armed Forces as soon as possible. Yet before creating any structures, it is important to develop a concept for information-and-propaganda support of forces -- not only in operations but also in routine activities, during the aggravation of the external or internal situation, in special military operations, and in times of war. In some activities, signal troops can be used (for instance, for a prompt transmission of reports by media workers to their offices), EW troops, and also military counterintelligence agencies.

Russian general officers stress that in order to achieve success in an operation it is necessary to keep the entire process of warfare under control, with control being extended not only to one's own troops but also, to a certain extent, to enemy troops. The kind of control which is primarily targeted at the morale of the opposing decision-making commander and which is of a reflexive character is called reflexive control. Its

basic objective is to place the enemy under difficult conditions if it chooses to continue fighting, or to force it into making decisions objectively leading to its defeat.

The enemy can be forced into making decisions desirable for the "controlling" side by "being intimidated with the threat of damage" (real or imagined) or by "being lured with advantage" (real or imagined). In this respect disinformation, concealment, and deception per se are merely particular methods to this end. "Coercion" is all the more effective, the more it is complex and elaborate; i.e., the enemy should make the conclusion about the reality of the threat of damage or the prospects of advantage based on the entire information received.

The difficulty of reflexive control lies in the fact that on the one hand it is necessary to constantly "nudge" the enemy toward achieving the desired result by "feeding" him logical information and, on the other hand, to keep an eye on its dosage, otherwise he will lose confidence. As a term, reflexive control of the enemy lays no claim to originality inasmuch as it implies the use of already familiar procedures. However, considering them as primary missions of maskirovka will permit reinterpreting one of the difficult and developing spheres of the command element's command-and-control activity.

PSYCHOLOGICAL WEAPONS

SHF Weapons. According to Russian military scientists, the mechanisms of SHF emission on the human body can be divided arbitrarily into energy and information mechanisms. The thermal effect of relatively large SHF emission power fluxes has been studied the most. Depending on frequency and power, radio-frequency emissions

disturb brain and central nervous system operation, temporarily disable, cause a feeling of noise and whistling difficult to endure, and damage internal organs. In the latter instance there is the likelihood of a fatal outcome. At the same time, some "foreign experts" believe that creation of such non-lethal weapons is very problematical (difficulty of obtaining requisite outputs with acceptable dimensions and cost of the unit, and the short effective range).

SHF generators can be used to disable electronic gear, but there are relatively simple methods for the latter's protection. "Foreign specialists" deem use of super-powerful SHF generators to be more acceptable as a means of EW power; i.e., means that do not disable gear, but create heavy interference for it by penetrating through defensive filters, along "parasite" receiving channels, through unshielded openings and slits of the gear, and so on.

Infrasonic Weapons. Russian military experts charge that the influence of infrasonic oscillations on the human body and mind was studied intensively in the United States during the 1960s and 1970s, including for police purposes and as weapons. This work demonstrated the possibility of infrasound affecting a person's sensory as well as internal organs and disabling him in the presence of a certain combination of conditions. One well-known project is the development of a massive sonic generator that can generate several infrasonic vibrations per second. Infrasonic waves can exert a powerful destructive effect on the human organism. These vibrations are capable of causing alarm, desperation, and even horror. According to some specialists, the effect of these vibrations can cause such dysfunctions as epilepsy. They can also destroy various organs and physiological systems, and cause a mass onset of

myocardial infarction among the enemy's troops and population. Infrasonic weapons can penetrate concrete and metal structures, thereby affecting personnel in shelters and inside combat equipment.

Psychotronic Weapons. Russian military scientists also note that throughout the 1980s, abroad and above all in the United States, there was an increase in the activity of certain military and civilian scientists in studying problems of bioenergy associated with so-called paranormal human capabilities. The division of research devoted to the study of paranormal phenomena has been given the name parapsychology. It examines methods of receiving and transmitting information without using the normal organs of sense and also mechanisms of man's influence on physical objects and phenomena without muscular efforts. The term psychotronics is widespread -- the creation of various technical devices based on energy from a bio-field, that is, a specific physical field existing around a living organism. This is how the concept of psychotronic weapons, created based on using paranormal properties of the human organism, entered military terminology.

Presently, one can single out four basic directions of military-applied research in the field of bio-energy. First, elaboration of methods of intentionally influencing a person's psychic activities. The second direction includes an in-depth study of paranormal phenomena that are of greatest interest from the standpoint of possible military use -- clairvoyance, telekinesis, telepathic hypnosis, and so forth.

The framework of this phenomenon is quite broad: on a strategic scale, it is possible to penetrate the enemy's main command-and-control facilities to become

familiar with his classified documents; on the tactical level, reconnaissance can be conducted on the battlefield and in the enemy's rear area (the "clairvoyant-scout" will always be located at a safe place). However, problems do exist -- the number of individuals possessing these abilities is limited, and the data received cannot be checked.

According to Russian military experts, using psychokinesis to destroy command-and-control systems and disrupt the functioning of strategic arms is already feasible. The ability of a human organism to emit a certain type of energy has been confirmed by photography of a radiation field known as the Kirlian effect. Psychokinesis is explained by the subject's generation of an electromagnetic force capable of moving or destroying some object. Studies of objects destroyed as a result of experiments conducted have shown a different form of breakage than under the effect of physical force.

Discovering the mechanisms of controlling telepathic hypnosis will make it possible to conduct a direct transfer of thoughts from one person or group of people (telepathic subjects) to a selected audience. It is important here that the subjects not be aware that thoughts are being implanted from an external source. They must think that these are their own thoughts. For example, personnel of an enemy formation executing a sudden breakthrough of defenses, instead of exploiting the success, will try to consolidate on the line achieved or even return to the starting line.

The third direction is studying the effect of bio-emissions on command-and-control systems, communications systems, and armament, especially electronic

equipment, and also development of artificial bio-energy generators and plants for affecting enemy troops and population in order to create anomalous psychic conditions in them. The fourth and last direction includes developing systems for detecting and monitoring artificial and natural dangerous bio-emissions and also methods of active and passive protection against them.

Many "Western experts," including military analysts, assume that the country making the first decisive breakthrough in this field will gain a superiority over its enemy that is comparable only with the monopoly of nuclear weapons. In the future, these types of weapons may become the cause of illness or death of an object (person), and without any risk to the life of the operator (person emitting the command). Psychotronic weapons are silent, difficult to detect, and require the efforts of one or several operators as a source of power. Therefore, scientific and military circles abroad are very concerned over a possible "psychic invasion" and note the need to begin work on taking corresponding countermeasures.

The term "biological electronic device" (BED) has entered Russian military usage. It involves:

- A fifth-generation computer -- in other words, a computer which communicates in ordinary human language rather than in machine language;
- An artificial biological field generator;
- A bio-electronic transceiver;
- Electronic or SHF radiation sources; and
- A holographic laser.

Research has shown that a BED is capable of sensing the specifics of biological radiation from diseased human organs, of influencing the physical and chemical processes taking place within the organism, and of revealing the connections between the cortex and subcortex of the brain,. A BED detects a diseased organ, receives its signal, boosts it many times over, and creates a field of the given type of radiation with a large effective range. A BED as it were lifts human biofield imprints. Each person has their own "fingerprint," which can be recorded in a computer. And each person can be identified even from part of this "fingerprint."

But the psychotronic device with the greatest applications at the moment is the electronic monitoring device. The baggage examination machine at airports is quite a close analogy. Without opening a suitcase the controller can see everything inside. The principle is based on illuminating the suitcase with electromagnetic waves of a certain band and transforming the reflected signal into a visual display. An apartment, home, office, district, or street could become just such a "suitcase." The force of the impact on the organism is comparable to exposure to radioactivity. The same kind of structure as is used in the baggage examination device is used for this "illumination." There is a radiation generator, a receiver, and a device to transform the reflected signals. A generator designed for a single apartment or office would be the size of a tape recorder, and the radiation source could be an electrical fitting, wiring, or heating or water pipes. The VHF receiver could be an incandescent lamp or a telephone wire.

NATURE OF ELECTRONIC WARFARE (EW)

Just as "motorization" changed the appearance of armies and nature of warfare in the 1920s and 1930s, say the Russians, so now one can expect a corresponding

result in connection with the constantly growing scale to which troops are being outfitted with electronics, which increases demands on their readiness to operate in a difficult electronic environment. Further development of electronic equipment functioning in various weapon, reconnaissance, and command-and-control systems demands an improvement in the art of its use. "Electronic training" is becoming a necessary element of the theoretical and practical training of all military cadres.

According to the Russian military, EW has become a weapon equal to "fire strikes" in combat effectiveness. As a result, there has been a revision of views on tactical employment of electronic systems on the battlefield. For example, the U.S. Air Force is said to have developed large-scale conceptual provisions for employing electronic equipment in support of modern military operations. In accordance with these views, EW is now categorized as a priority combat mission of aviation in air operations. At the same time it goes beyond the scope only of a supporting mission and in the near future will have the nature of an independent combat mission along with winning air superiority, interdicting a combat operations area, and providing close air support. This is explained not only by the obvious importance of EW, but also by changes in its specific content. In addition to "electronic warfare" measures, EW envisages a set of measures for suppression of enemy air defense and is an element of the fight against his battle management systems (command, control, and communications countermeasures.)

In the views of "NATO specialists," the purpose of EW should be to prevent the operation of enemy equipment within certain sectors of the electromagnetic emissions spectrum and to take effective advantage of them in one's own interests. The following

measures are taken for this purpose: arranging to monitor specific sectors of the spectrum of radio-band frequency emissions during the necessary period of time; using radar signatures and emissions of enemy electronic equipment to collect intelligence; depriving him of an opportunity to operate in this spectrum of electromagnetic energy emissions; preserving an opportunity for effective use of electromagnetic spectrum emissions in support of friendly missions under conditions of intensive [illegible] and the enemy's use of weapons; and ensuring security and decisive operations of friendly forces.

The Russian military was awestruck by the way U.S. aviation conducted electronic warfare in the combat operations in the Persian Gulf. Whereas the allies lost 34 aircraft (1.92 percent) out of 1,763 aircraft sorties during the raids on Cologne in 1944, and Israeli aviation lost 46 aircraft (1.23 percent) in 3,729 sorties in the Six-Day War in 1967, American aviation lost just 27 aircraft and helicopters in 103,000 sorties (0.26 percent) during the combat operations in the Persian Gulf. These extraordinarily low losses were achieved, first of all, thanks to the most intensive application of means of electronic warfare in the history of war.

EW thus goes beyond the bounds of supporting the combat operations of aviation in air operations. It is more and more assuming the nature of an independent combat mission in the winning of air superiority. EW has two areas of principal application as an independent type of combat operations and special combat mission -- fighting enemy systems of combat command and control, and suppressing his AD systems.

According to Russian military scientists, the results of simulation and the experience of the war in the Persian Gulf indicate that electronic warfare equipment accounts, on the average, for one-third and more of the reduced combat potential in the disruption of enemy command and control. The effectiveness of fire delivery is largely determined by the effectiveness of the jamming of the enemy's command-and-control electronic gear. A massive delivery of fire on the enemy should be preceded and accompanied by a massive employment of electronic warfare gear. This is dictated by the fact that the high potentials of weapons and hardware are largely as efficient as their electronic elements and systems. Therefore, any operational mission will involve an impact on the enemy's electronic facilities both by weapons and electronic warfare gear. The objective will be to disrupt the command-and-control systems, to render the reconnaissance and air defense systems blind, and to disable the most important elements controlling high-precision weapon systems of the enemy. This sharply raises the effectiveness of a massive delivery of fire.

Thus, an increased role of electronic warfare facilities in operations is dictated by the following things. Electronic warfare makes it possible to reduce the element of surprise of an enemy's attack because its forces and assets are capable of acting virtually momentarily over a great distance; i.e., earlier than the main sources of fire-power. Electronic warfare gear reduces the effectiveness of the enemy's deep strikes during air-land operations by disrupting control of its missile systems (guided-missile complexes), by employing offensive force groupings and aviation and artillery supporting them, and by disruption of cooperation between the ground troops and aviation. A concerted impact by weapons and means of electronic countermeasures upon enemy forces, reconnaissance resources, and electronic warfare gear, as well as

the implementation of a set of coordinated measures to ensure electromagnetic compatibility of the electronic equipment in the groupings of friendly troops will produce higher stability of command and control of troops (forces) in all operations. There may be changes in the very nature of organization and conduct of electronic countermeasures as new tasks crop up. For example, it may become necessary to counter enemy ABM defense by taking the war into outer space in order to facilitate the operation of space-based forces and of all armed services engaged in operations.

Russian military scientists stress that the revolutionary nature of the Gulf War was manifested in the fact that it marked the origin of certain new forms and methods of operational and tactical actions such as the electronic-fire engagement, remote-controlled battle, air-assault raids, and deep mobile operations. The electronic-fire engagement played a special role in Desert Storm as the aggregate of massive, lengthy air-space, missile, naval, and electronic strikes. It was the principal content of the operation and predetermined its successful outcome. In this case the novelty lay in the fact that electronic countermeasures acted as a special weapon that was equivalent to fire strikes in effectiveness.

First, Desert Storm was characterized by the significant duration of the electronic-fire phase (38 days), which surpassed the ground operations phase (4 days) by many times (ninefold). Second, a large amount of the latest EW equipment, airborne early-warning and control aircraft, and radar systems for aerial reconnaissance of ground targets and strike delivery control took part in the engagement. The employment of EW equipment previously unknown to the enemy ensured surprise in its use. Third, all the most important enemy targets were continuously subjected to

electronic-fire pressure to the full depth of the operational alignment, which disrupted the command-and-control and communications system simultaneously at all command echelons from tactical to strategic. Fourth, electronic and fire strikes were precisely coordinated by objective, place, and time. By being combined, they mutually supplemented and reinforced each other. Fifth, the Air Force played an especially important role in fire destruction. The intensity of its strikes (in some phases up to 2,000-3,000 sorties per day) had no precedent in any previous war.

All this together dictated the exceptionally high effectiveness of electronic-fire engagement of the enemy and the winning of the fire initiative and air superiority. Before the beginning of the ground phase of combat operations it became obvious that the opposing Iraqi force grouping had lost almost all combat effectiveness. The personnel were psychologically paralyzed. This considerably eased the task for the attacking mechanized and armored formations, which completed the enemy's defeat without encountering organized resistance. Therefore, one of the characteristic features of a "technological war" is that its objectives can be achieved under certain conditions even without ground troops invading enemy territory -- by conducting an electronic-fire engagement alone. This confirms the previous conclusion that, in the future, large masses of ground troops will not be required as part of an attack grouping.

The Russian military therefore argues that the effectiveness of information systems has led "developed countries" to acknowledge the dominant role of the "electronic-fire" concept of waging war. In force structure and equipment, this concept manifests itself not in competing for numerical superiority in motorized rifle (tank) formations for conducting ground battles, but in using industrial and technological

advantages to create high-precision sea- and air-space-based weapons and global C^2 systems that facilitate "surprise first and subsequent massed radioelectronic and fire strikes that decide the outcome of the war without the invasion of ground forces." A war's main objective is shifting away from seizure of the opponent's territory and toward 1) "neutralizing his political or military-economic potential -- eliminating a 'competitor'," and 2) "ensuring the victor's supremacy in the political arena or in raw materials and sales markets." The primacy of this concept has generated a new form of utilizing armed forces: the "electronic-fire operation."

This operation will typically begin with a surprise air attack rather than an invasion by deployed ground forces, which permits not only seizure of the strategic initiative but also disruption of the opponent's strategic deployment by striking a series of his most important targets with a first strike. In addition, losses of personnel are significantly lowered since ground troops are used only after achieving space and air superiority -- which guarantees their success. Parity thus requires calculations of not only the fire component of combat but especially the "information component" -- which must govern the allocation of scarce defense resources.

COUNTERING C^4ISR/EW SYSTEMS

According to General Staff analyses, a classification of possible measures for protecting the Russian Armed Forces against the new technologies of the RMA consists of the following:

- ACTIVE WARFARE
  -Destruction of platforms, command-and-control equipment, and weapons elements by SAM complexes (systems)
  -Electronic and electro-optical suppression of weapons systems by EW equipment

- PASSIVE PROTECTION
  -Reduction of own signature (radar, optical) and of emitted signals
  -Use of diversionary means
  -Mobility, armoring

- SYSTEMS PROTECTION
  -Creation of integrated air defense systems realizing the integration of air defense and EW assets
  -Creation of alert radar field at high, medium, and low altitudes; support of information communications with reconnaissance systems of other branches of the Armed Forces

Russian military scientists have also examined the following specific counters to a variety of systems:

COUNTERS: AGAINST RECONNAISSANCE-STRIKE COMPLEXES

- Fighters Against "Airborne Elements" (Reconnaissance and Communications Relay Aircraft)
- "Front Air Operation" Against "Ground Elements"

COUNTERS: AGAINST STEALTH

- Detection: Radar, Acoustic, Laser Sensors
  -Multi-Positional and Multi-Frequency Radars
  -Over-the-Horizon Radars
  -Holographic Radars

-Air- and Space-Based Radars
-EM, Infrared Systems, etc.
-Solid Radar Field

- Destruction: SAMs and Fighter Aircraft (S-300, BUK SAMs and MIG-31, SU-27, and Follow-ons)

COUNTERS: AGAINST "NEW PHYSICAL PRINCIPLES"

- Active: Detection and Destruction of Facilities
  -Strikes By Ground- and Air-Based Radiotechnical Systems
  -Jam Communications and Guidance Systems
- Passive: Troop and Equipment Protection (Fortifications, Aerosols, etc.)

COUNTERS: AGAINST C^4 ISR SYSTEMS
-"Perturbations of Environment" (Geophysical)
-System Failures (Non-Lethal Weapons)
-Nuclear Weapons and PGMs
-Computer Virus

COUNTERS: AGAINST EW SYSTEMS

- Active
  -Affect Software (e.g., Computer Virus)
  -Strike With Beam, Super-High-Frequency, and especially Electromagnetic Pulse Weapons
  -Advanced Anti-Radiation Missiles
  -Advanced Anti-Radiation Drones
- Passive: Electronic Protection and Maskirovka

THIRD-GENERATION NUCLEAR WEAPONS

Both Soviet and Russian military scientists have long discussed so-called "third-generation nuclear weapons" as countermeasures to both C^4ISR and EW systems. Their catalogue of these weapons includes the following:

- Neutron weapons
- EMP and "super-EMP" weapons
- SHF microwave weapons

- Earth-penetrating nuclear weapons
- Nuclear-pumped x-ray laser weapons
- Nuclear shrapnel
- Mini-nukes

For example, the Russian charge that in the early 1980s, U.S. military scientists began research aimed at creating one more kind of nuclear weapon -- a super-EMP with intensified electromagnetic radiation output. They plan to use it to increase the intensity of the field at the earth's surface to several hundred kilovolts per meter. In their calculations, the explosion of a 10-mt warhead at an altitude of 300-400 km above the geographic center of the United States (state of Nebraska) can disrupt the operation of electronic equipment on virtually the country's entire territory for the time necessary to disrupt retaliatory measures.

According to Russian military experts, the search for reliable destruction of highly hardened targets has led "U.S. military specialists" to the idea of using earth-penetrating nuclear devices. In delivering a penetrating warhead to the target with an accuracy characteristic of the MX and Trident II missiles, U.S. military specialists figured that the probability of destroying the enemy missile silo or command post is near 100 percent, and instead of the two warheads now planned for each target, one will be sufficient. In other words, the probability of destroying targets will be determined only by the technical reliability of delivering warheads to them. They are ear-marked above all for destroying enemy military and state command-and-control centers, ballistic missiles in silos, command posts, communications centers, and so on. Consequently, missiles with such warheads will be used in a first strike. The importance of this kind of weapon grows even more in the event of a further reduction

in strategic offensive arms, when there will be decreased combat capabilities for delivering a first strike and it will be necessary to increase the kill probability of a target by each weapon. "U.S. specialists" are examining the possibility of creating penetrating warheads equipped with a system of homing in the terminal flight phase for high accuracy in striking the target.

To eliminate warheads and decoys in the phase of their free flight on a ballistic trajectory, "U.S. specialists" also propose to use small metal particles accelerated to high velocities by the energy of a nuclear explosion and arbitrarily called nuclear shrapnel. According to the Russians, the "nuclear shrapnel" can be used only in outer space under conditions of airless space, since the particles will burn up at velocities of over 4-5 km/sec. Its use as an anti-space weapon for destroying military satellites is not precluded. Therefore, its combat use is possible for "blinding" the enemy in a first strike.

Russian military and scientific experts have also focused on the combat capabilities of low- and high-yield miniaturized nuclear devices. When based in space, such weapons are said to be capable of generating a "directed shock wave" accurate enough to strike even hardened underground targets such as military and state command-and-control centers, nuclear facilities, etc. In late 1992, General-Lieutenant Ye. A. Negin announced that Russia has already developed a mini-nuke whose yield has more than doubled and whose weight is one-hundredth of what it was.

According to V.N. Mikhaylov, Russian minister of Atomic Energy, work now is being done in the world on third-generation weapons. While atomic munitions using

the effect of fission of heavy nuclei can be included in the first generation and thermonuclear weapons operating on the principle of the fusion of light nuclei in the second, the third generation consists of weapons with a selective effect, which act using a superpowerful electromagnetic pulse, superpowerful nuclear-pumped lasers, an intense neutron flux (the so-called neutron bomb), and so on. An electromagnetic pulse is capable of damaging or disabling all kinds of electronics-based armament; thus, it acts above all on the most sophisticated armament and command-and-control and communications systems. Third-generation nuclear weapons realistically can appear in the next century. They should possess a significantly lesser damage effect on the environment, but a greater selective effect; they gradually will replace first- and second-generation nuclear weapons.

Both Soviet and Russian military scientists have long argued that "weapons based on new physical principles" constitute the essence and future of the new RMA. Their catalogue of these weapons includes the following:

- Geophysical/ecological weapons
- High-frequency radio/electromagnetic wave weapons, infrasonic weapons
- Ethnic weapons
- Directed-energy weapons
- Psychotronic weapons
- Plasma weapons
- Non-lethal weapons

As already noted, infrasonic and psychotronic weapons are viewed as "psychological weapons" and therefore components of psychological operations. Russian scientists also warn of the danger connected with the possible development of "geophysical weapons." These are weapons that generate natural catastrophes such as

earthquakes, torrential rains, tsunamis, and destruction of the ozone layer. It is possible to trigger earthquakes with underground explosions of powerful nuclear charges, particularly in areas of high seismic activity. It is also possible to trigger tsunamis with an explosion of nuclear charges in certain areas of seas and oceans. Such weapons are viewed as means of disrupting command, control, and communications systems.

Finally, Russian military scientists consider certain non-lethal weapons to be elements of IW. Their catalogue of these weapons includes the following:

- Laser weapons
- Incoherent light sources
- SHF weapons
- Infrasonic weapons
- EMP weapons
- "Information weapons" (electronic news media, EW systems, special programs, computer viruses, etc.)

NEW ORGANIZATIONAL CONCEPTS

According to Colonel-General M. Kolesnikov, then Chief of the General Staff, Russia has outlined a set of measures for Armed Forces organizational development aimed at their qualitative transformation. First is an upgrading of the Armed Forces. The Armed Forces structure is to be upgraded in order to increase efficiency of command and control and effectiveness in executing their assigned missions. The strength of troops (forces) must conform to their tasking and ensure strategic deployment of the Armed Forces.

Second is an upgrading of the Armed Forces command-and-control system, which will be built and developed according to the following principles:

- preservation and maximum use of the existing Armed Forces command-and-control system infrastructure, with subsequent integration into the country's statewide command-and-control system;

- balanced development of all component parts of the command-and-control system of the supreme echelon and of branches of the Armed Forces and combat (naval) arms, giving priority to high-tech automated systems for command and control, fire control, communications, reconnaissance, navigation, electronic warfare, precision weapons guidance, and preparation of data for their combat employment; and

- a reduced time period and expenditures for creating modern command-and-control systems and equipment through their increased degree of unification and standardization.

It is proposed to develop the command-and-control system under a unified concept and plan within the scope of an integrated program. Main efforts and resources are to be concentrated in the following basic directions:

- upgrading command-and-control entities and bringing their structure, makeup, and numerical strength into line with new missions based on the conditions and phases of Armed Forces reorganization and with consideration of troop (force) groupings being established for wartime and their operational tasking;

- ensuring stability of the system of Armed Forces command-and-control facilities under conditions of modern war, increased survivability of fixed facilities for command and control of strategic nuclear forces (at the strategic and tactical levels), and establishment of standardized mobile command-and-control facilities supporting troops (forces) under mobile defense conditions;

- modernizing and building up capabilities of automated command-and-control and fire-control systems with the goal of ensuring their

compatibility and capability for subsequent integration within the framework of the combined military and state command-and-control system; and

- establishing territorial command-and-control systems of military districts on strategic and operational axes mutually tied in with the Russian Federation statewide automated communications system.

The Russian military hierarchy has long stressed that the unification of the fragmented information-management systems of the branches of the armed forces into a unified system for the Ministry of Defense, provision for its interaction with the information systems of the bodies of state administration and, in particular, with the information systems of the apparatus of the President and the Security Council, is an urgent task for the armed forces of the Russian Federation under prevailing military-political conditions. The material, scientific, and technical basis for this task should be improved computer hardware and software support. The following basic principles should be taken into account when structuring the conceptual model for the unified information-management system (YeIUS):

- *minimization of the material and financial expenditures for the creation of the YeIUS;*
- *the maximum utilization of available command-and-control, computer, communications, and data-transmission systems and scientific-technical developments;*
- *centralization of access to information contained in the information and computer centers of the branches of the armed forces and other command-and-control points;*

- *coordination of information flows in the YeIUS being created and the systems integrated with it according to uniform requirements;*

- *the creation of support points for the gathering, study, depiction, and analysis of data; and*

- *assurance of the basic principle of the command and control of troops -- the centralization of command and control at all levels.*

The information system being created within the apparatus of the Ministry of Defense and General Staff of the armed forces could be used as the foundation for creating this YeIUS. The principal requirement for developing the YeIUS is providing information to all elements of command and control and administrative leadership of the Ministry of Defense. The accomplishment of the tasks enumerated above is impossible without the creation of scientific, technical, organizational, and financial foundations of the command-and-control system and the coordination of operations in the realm of armed forces information technology.

The General Staff's concept for modernizing the communications system of the Russian Federation Armed Forces sets forth the main directions for developing and improving qualitative characteristics of communication systems. Key points include: upgrading the communications and automated command-and-control systems for personnel and equipment in the missile and space defense troops, strategic nuclear forces, strategic reconnaissance, and electronic warfare; setting up a general-purpose territorial communications system for all services and combat units of the armed forces; upgrading field communication systems and the structure, equipment, and combat strength level of the communications troops; and increasing the level and degree of integration between communication systems and command-and-control automation to

create a combined information and technical system of the armed forces. Given the existing military-political and financial-economic realities, it is planned to have both a general-use territorial communication system and specialized communications systems for the services and combat arms in order to provide uninterrupted command and control in the armed forces.

The Russian military also plans to restructure the branches of the armed forces. Five branches exist at present: the Strategic Missile Troops, the Ground Troops, the Air Defense Troops, the Air Forces, and the Navy. The Military Space Troops and Airborne Troops are separate combat arms. According to then Defense Minister Grachev, a new structure for the armed forces will be established by the year 2000, under which they will be divided into four branches: the Strategic Deterrence Forces, the Air Force, the Navy, and the Ground Forces. Beyond 2000, the armed forces could move to a three-branch structure: it is proposed to merge the Air Force and the Strategic Forces into Air-Space Forces.

According to General-Major V.I. Slipchenko, the Russian Armed Forces will consist of two main components by the year 2000: the Strategic Strike Forces and Strategic Defense Forces. But a new and separate branch will form between them, conditionally called the EW/Information Troops. These forces will operate either with the Strategic Strike Forces when an offensive operation is under way, or with the Strategic Defense Forces when a defensive operation is under way.

The new EW/IW groupings will include existing missile-attack warning systems, space monitoring systems, SIGINT systems, and others. They will also include

information-strike assets capable of targeting analogous enemy information systems, and a comprehensive infusion of ECM and ECCM assets. Directorates for both IW and EW have already been established in the General Staff.

In search of ever-greater centralization of command and control, Russia's Defense Ministry plans to simplify the armed forces coordination system by transforming the eight operational military districts into four combined territorial commands. Each will be headed by a deputy defense minister, who will exercise control over all of the forces and assets in his region. According to then Defense Minister Pavel Grachev, the four territorial groups will be called Northern, Southern, Ural-Baykal, and Far Eastern.

All branches of the Russian Armed Forces have designed blueprints for reorganization to adapt to the new information environment:

Air Forces. According to General P. Deynekin, CINC of the Russian Air Forces, the ideal Air Force organizational structure is based on the principle of centralized command and control by the Air Force commander-in-chief for the commands (Long-Range, Frontal, and Military Transport Aviation, and the Reserve and Personnel Training Command), and by the commanders of Long-Range Aviation, Frontal Aviation, and Military Transport Aviation for large strategic formations (combined units and separate air units). At a time when the Russian Armed Forces, including the Air Force, are being cut, when there are diverse military threats, and when they are uncertain of the areas where potential military danger could escalate into a military threat, the principle of strict

centralization of the command and control of large strategic formations (combined units) is said to be one of the most important conditions for enhancing the effectiveness of the combat operations of aviation combined units (units). The Air Forces are thus being reorganized according to the territorial principle on the model of the Air Defense Troops.

Air Defense Troops. According to General V. Prudnikov, CINC of the Russian Air Defense Troops, the Order of the President of the Russian Federation and the corresponding order of the Ministry of Defense gave a new face to the Air Defense Troops. In the future they will be the basis for the creation of Russia's air-space defense. That is a natural future, because the air and space spheres are so interrelated that they have long been viewed as a seamless whole.

The present air defense system can and must become the basis of air-space defense because it is built on a territorial principle, which implies not the interworking of large strategic formations of Air Defense Troops and of air defense forces and assets of military districts, the Air Force, and the Navy, as was the case previously, but unified command and control of them in air defense zones and areas. The establishment of corresponding mobile reserves of the Air Defense Troops also is envisaged for a timely buildup of efforts in crisis situations.

National Air-Space Defense. According to Colonel-General G. Kondratyev, the Russian military plans to create an air-space reconnaissance system based on the reconnaissance information assets of all branches of the armed forces and other Russian ministries (in particular the federal reconnaissance and air-space surveillance system)

capable of detecting offensive air-space weapons and at the same time forming an integral part of the overall early-warning system. Thus, all forces within the Air-Space Defense System will receive unified information, and on a real-time basis.

Considering the great length of Russia's state border, the importance and number of installations to be covered, the swiftness of air and air defense engagements and battles (which surpass the swiftness of engagements and battles on land and sea by many times), and that essentially all branches of the armed forces have troops, forces, and assets capable of performing air-space defense missions, the conclusion can be drawn that they should be integrated to the maximum extent. This is possible only within the framework of a unified national air-space defense system based on a common responsibility and unified direction of training and operations of all air-space defense troops and forces.

A legitimate question arises: How should it differ fundamentally from the former USSR air defense system? First of all, by common programs for developing arms and training cadres for air-space defense in place of parallel resolution of these problems in other branches of the armed forces. Secondly, by unified planning and command and control of all air-space defense forces at the strategic, operational, and tactical levels instead of unified planning at the strategic level and coordination at operational and tactical levels. And thirdly, by deeper information. algorithmic, and fire ties among missile-space defense and air defense systems instead of their essentially independent existence. Realizing effective methods for combatting existing and future targets operating under a unified concept throughout their range of air-space employment

altitudes requires (especially with limited resources) a unification of efforts of all troops, above all reconnaissance and air-, missile-, and space-attack warning.

Ground Troops. According to General Semenov, CINC of the Russian Ground Troops, the Ground Troops will be developed along the following main directions:

- creating a unified automated command-and-control and fire-control system and its subsystem;
- developing multipurpose, multichannel automated combat systems, including reconnaissance-strike and reconnaissance-fire complexes;
- developing models and complexes of arms and military equipment based on new physical principles and non-traditional engineering solutions using elements of artificial intelligence;
- ensuring high mobility, survivability, noise immunity, all-weather capability, and compatibility of armament complexes; and
- reducing the nomenclature of arms and combat equipment and time periods and expenditures for their creation through standardization of completing elements, assemblies, instruments, and hardware.

Signal Troops. Colonel-General G.P. Gichkin has noted that world experience points to the expediency of creating general-purpose communication systems based on the territorial-zonal principle (territorial communication system). Plans for the development of the communication system in the Russian Federation Armed Forces provide for the creation and series production of modern communication equipment and automated command-and-control systems, which to some extent would correspond to

the world's troop communication technology level. Several directions can be singled out here:

- Development of satellite communication systems. The Russians plan to increase their carrying capacity, survivability, and jamming resistance, and also to acquire new frequency bands and use new methods of multi-station access to relay stations.

- Upgrading radio communication systems. The Russians plan to use modern methods of ensuring jamming resistance and adaptation to radio-wave dissemination, which will substantially increase radio channel capacity.

- Development of radio-relay and tropospheric communication means. The Russians plan to develop unified complexes of digital anti-jam communication stations with an expanded carrying capacity and communication range in stationary, automobile, and container options.

- Development of land-line communications systems. The Russians plan to increase the carrying capacity and operational capabilities of digital transmission systems, and ensure a wide employment of fiber-optic transmission systems.

- Development of second networks. The Russians plan to ensure integration, to reduce linking and message transmission time, to increase the number of users, to enhance the reliability and reduce the weight and dimensions of the equipment, and to create unified encryption and communication terminal complexes, ensuring the transmission of various types of information.

- Automation of the command-and-control system. The Russians plan to intensify the introduction of information technology into the command-and-control process in the armed forces (especially at the operational-tactical level), in order to upgrade the effectiveness of day-to-day activity and the operational preparation of staffs and troops at all levels, including in the course of operational training sessions and command-and-staff exercises -- without bringing the troops into the field and without target practice. The

final stage includes R&D work on disseminating information technology in various governing bodies of the Defense Ministry. They plan to use the hardware and software options developed as a result of this R&D work in equipping some military districts with secure local computing networks based on personal computers, and in the future to extend them to the entire armed forces.

Radio-Technical Troops. According to Colonel-General V.F. Migunov, commander of the Radio-Technical Troops of the Air Defense Troops, Russia is working to establish a Federal Air-space Surveillance and Control System based on the Radio-Technical Troops. This system is being established through integrated use of radar systems and equipment in the Ministry of Defense and Ministry of Transport. In accordance with Russian Federation Presidential Edict, they are intended for information support of the Armed Forces and Civil Aviation, above all for performing air defense and air traffic control missions. The basis of the federal system will be the radar system of Air Defense Troops and radar surveillance equipment of branches of the Armed Forces and Civil Aviation. In the course of 1994, a central commission and interdepartmental zonal commissions were formed which are coordinating the new system's establishment, and the formation of dual-purpose information elements is next in line. Work also is under way to certify technical equipment, and normative-legal documents are being prepared.

The concept of phased development of the federal system envisages setting up dual-purpose information elements in early 1995; i.e., radio-technical subunits and positions of the Ministry of Defense and Ministry of Transport must be capable of performing missions of the related department in addition to their own specific missions. There already is experience of such work in Karelia, the North Caucasus

region, and Siberia. For example, problems of using Ministry of Transport radar positions for building up the radar field in a given region were worked out in the course of the Sibir-95 command-and-staff exercise held in April. The Federal Surveillance and Air-space Control System now being established will bring together radar assets of all branches of the armed forces and civilian departments. A unified data bank is being established with the help of these assets. This will solve to a considerable extent the problems of closing gaps in the radar field.

POST-ELECTION PRIORITIES

In his June 1996 election program, President Yel'tsin stressed that given the real economic conditions and the military-political situation, it will be necessary over the next four-five years to focus on resolving the task of creating by the year 2000 the scientific, technical, and technological groundwork required for Army and Navy rearmament. While maintaining Russia's nuclear deterrent potential at the proper level, he continued, Russia needs to devote more attention to developing the entire range of means of information warfare, the development of precision weaponry, the individual protection of servicemen, systems for ensuring mobility, and the development of the defense infrastructure (the airfield network, roads, Navy basing systems, and so forth). The Defense Ministry and the General Staff must ensure the utmost level of technical equipment and strength levels for combined and other units in the most important areas and the main armed forces segments. Within the framework of overall defense spending, Russia must increase the share of resources allocated to research and development, to enhancing the level of technical equipment available to the Army and Navy, to modernizing armaments and military hardware, to combat and operational training, and so forth.

The new defense minister, General I.N. Rodionov, has long stressed that military reform is not quantitative changes in the armed forces, but radical qualitative transformations in the very essence of the state's military system. The military-technical policy is a most important direction in the country's activities safeguarding its security and also one of the elements of the national industrial policy. It is directly linked to the formation and execution of the state defense order for armament and military equipment. Work on the defense order today is assuming a most important significance for the country's future, since this is the only opportunity to preserve the nucleus of high technologies which are basically concentrated in the defense complex. Destroy this nucleus and the trend of turning Russia into a raw materials appendage of the world market will become irreversible. The military-technical policy must make the most effective use of achievements in the area of computer science in order to eliminate the imbalance between individual components within the weapon system itself. Thus, having outstanding models of weapons, the Russians often lag behind in means of their information support, which leads to an increase in ammunition expenditure and puts an excessive load on the support system.

Shortly after his 1996 appointment as defense minister, General Rodionov unveiled a radical military reform plan that continues to generate debate. The plan apparently includes slashing the Ground Troops from about 60 to 12 divisions, including a fifty-percent reduction in the Airborne Troops; altering defense budget priorities to focus on information and emerging technologies; and significantly delaying planned weapons procurement in order to increase R&D expenditures. He has already sacked opponents of radical reform, and appears fully capable of implementing the plan even if Lebed does not emerge as the next president of Russia. If implemented, his

reforms would create the basis for a gradual increase in Russian military capabilities over the next decade.

Most currently, General Viktor Samsonov, the new chief of the Russian General Staff, has stressed the emergence of a new element in the meaning of war: the erosion of distinctions between military and non-military means of struggle. He asserts that military confrontation has entered a new phase when the modern means, forms, and methods of this confrontation make it possible to attain the strategic objectives of war without the results which were traditional in the recent past (conquest of territory and so on). This specific approach was adopted by the United States when planning and implementing Operation Desert Storm.

The concepts of information, economic, financial, ecological, and other types of warfare, which are now becoming increasingly widespread, extend beyond the strictly theoretical bounds and acquire a perfectly specific and practical meaning. For example, the Russian-U.S. scientific conference held in Moscow at the end of 1995 noted the high effectiveness of the "information warfare" systems, which in combination with the use of highly accurate weapons and "non-military means of influence" make it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population. In other words, the effect of the use of these means is comparable with the damage resulting from the effect of weapons of mass destruction.

Scientific and technical progress and the introduction of high technologies in the defense sectors of industry make it possible to develop highly effective systems based

on new principles of physics. Intensive work is under way to develop geophysical, ozone (exotic), neutron, accelerator, plasma, laser, psychotronic, and other types of modern weapons. They are capable of significantly changing the material base of armed struggle and the appearance, nature, and content of war.

Finally, Defense Minister Rodionov has stressed that the VPK has lobbied for the army to purchase technology and arms that it really does not need. All this has been explained by the need to maintain production and jobs in the defense complex. As a result of this faulty practice, funds have been spent irrationally, and there has not been enough money for research and design work. Rodionov has already echoed Yel'tsin's proposal to the government that a significant portion of the funds previously planned for the purchase of arms be spent on R&D. "We can put off rearming for ten years," he argues, "but get twenty-first century equipment and weapons." It should be noted that the Russian government, including the Defense Council, has approved this proposal.

WHITHER THE VPK?

In a December 1992 interview, Deputy Defense Minister A. Kokoshin, head of the Military-Technical Policy Council, noted that the Russian military is trying to change the entire cycle between fundamental research and the final product (launching series production of a piece of military inventory.) One of the main objectives of Russian military-technical policy is to form a "scientific-technical reserve" in the sphere of "critical technologies," to include dual-purpose technologies. This "scientific-technical reserve" is equivalent to the Western concept of "hovering," which permits defense industries to "leap over" a generation of weaponry by focusing on the

development of prototypes and avoiding costly series production. In other words, the R&D establishment fully develops a new technology or system concept without proceeding to the next stage of acquisition until the situation warrants. This can be achieved, say the Russians, by 1) reducing procurement of arms and equipment in series production, and 2) maintaining R&D and production capacities to ensure the development and "rapid surge production" of emerging combat technologies. As already noted, Defense Minister Rodionov's reform plan embodies this concept precisely.

In June 1993, then Defense Minister Grachev announced that the Russian Defense Ministry now has "prototype development plans for all types of armaments." As Kokoshin has noted, "We are also planning... the establishment of a scientific and technical capability that would permit us to achieve a qualitative leap and to expand mass production of the most modern equipment at a time when we are a little richer."

In early 1995, the Russian government unveiled a new federal program: the "National Technological Base" program. Reflecting both the country's current lags and long-term requirements, the program focuses on the development of the following:

- Information technologies
- Technologies based on new materials
- Microelectronics, nanoelectronics
- Optical, laser, radioelectronics
- Power generation, energy savings
- Advanced engines
- Highly productive industrial equipment
- Special chemicals

- Energy-intensive materials
- Unique nuclear, environmentally safe technologies
- Biotechnologies

Like the new military reform plan, the federal program emphasizes a shift away from material-intensive and toward science-intensive systems: away from ballistic missiles, submarines, heavy bombers, tanks, and artillery and toward advanced C^{4}ISR and EW systems.

Since the 1970s-1980s, says Deputy Defense Minister Kokoshin, and then in the course of operation Desert Storm, the prime task has been to win superiority in the information sphere; then comes the struggle for air superiority; and only after that the struggle for fire and space superiority. The emergence of information warfare assets and means of impacting on the information space of another state necessitates the development of theoretical and practical foundations for conducting information warfare, and consolidating the theoretical basis of this form of warfare as part and parcel of military art. The center of gravity in modern warfare is shifting away from the large-scale effective engagement of enemy personnel, weaponry, combat hardware, and military installations toward the destruction (incapacitation) of elements that are key to the opposing side's ability to put up organized resistance. The appearance of means and systems of purposive information impacting on the information space of another state has raised squarely the question of the need for the development of the theoretical and practical fundamentals of an information confrontation and the use of information weapons in the armed struggle. The intensive development of new forms and modes of operation of the armed forces at the strategic, operational, and tactical levels under conditions of the use of information weapons is essential.

Information confrontation should be an inalienable part of military art, and the armed forces should be ensured the possibility of conducting -- in conjunction with other troops and military elements and authorities (the Federal Government Communications and Information Agency, the Foreign Intelligence Service, the Federal Border Service, the Ministry of Internal Affairs, the Federal Security Service, the Ministry of Foreign Affairs, and others) -- information-impact operations coordinated in terms of goal, targets, place, time, types of information weapons, and methods of their application. This presupposes the need for the most in-depth study of the political and social structures of various countries, their systems of state and military command and control, psychological and behavioral stereotypes, etc. This study should be conducted on the basis of the latest achievements of the social sciences -- social psychology, political science, ethnography and ethnology, and so forth.

Instead of a reliance on massive effective fire against personnel, weapons, military hardware, and military targets, the main efforts should be concentrated increasingly on the destruction (disruption of the operation) of the components on which the enemy's capacity for organized resistance depends. The main efforts in determining the directions and priorities in the development of the means and methods of armed struggle within the framework of the long-term arms program proposed by the Ministry of Defense will, accordingly, be geared to the creation of forces and facilities of information warfare (electronic warfare, intelligence, communications, operational command-and-control systems, and facilities for the protection of command-and-control systems against enemy influence).

In late 1996, Kokoshin told ITAR-TASS that the military-industrial sector's dramatic problems with defense orders had not barred its research and development programs in recent years. He cited serious developments in hydro-acoustic engineering, radars, and computer hardware for control of troops and weapons. In the nearest future, new weapon systems will appear such as anti-aircraft missile systems and means for radioelectronic warfare that will bring the Russian Army to the level of the best models in the world.