THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW.BLACKVAULT.COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

(2)

RUSSIAN VIEWS ON ELECTRONIC AND INFORMATION WARFARE:

VOLUME II

OSD/NA
Distribution B: Distribution authorized to U.S. Government agencies only due to Proprietary information, (Dec 96). Other requests for this document shall be referred to Office Secretary of the Secretary of Defense, Office of Net Assessments (OSD/NA), 1920 Defense Pentagon, Washington, DC 20301-1920.

DESTRUCTION NOTICE - For classified documents, follow the procedures in DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), Chapter 5, Section 7, or DOD 5200.1-R, Information Security Program Regulation, Chapter IX. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

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

20061227289

TABLE OF CONTENTS

I. INTRODUCTION

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^{4}ISR/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 C^{4}ISR 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.

II. NATURE OF INFORMATION WARFARE (IW)

INFORMATION WARFARE DEFINED

Russian military scientists argue that the course and outcome of modern combat actions on any scale is determined by the art of waging information warfare. Therefore a recognition of the objective law-governed patterns and principles of information warfare, as well as the intensive development of its scientific theory is an extremely urgent problem that requires broad discussion and a rapid resolution.

It is expedient to begin examining the theoretical questions by precisely defining the content of information warfare. 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).

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.[1]

"U.S." VIEWS ON IW

Russian military scientists note that the war in the Persian Gulf as a whole, in the opinion of "American specialists," showed the real results of long-term programs

[1] Colonel S.A. Komov, "The Information Struggle in Modern War: Questions of Theory," VM, No. 3, 1996, pp. 76-80.

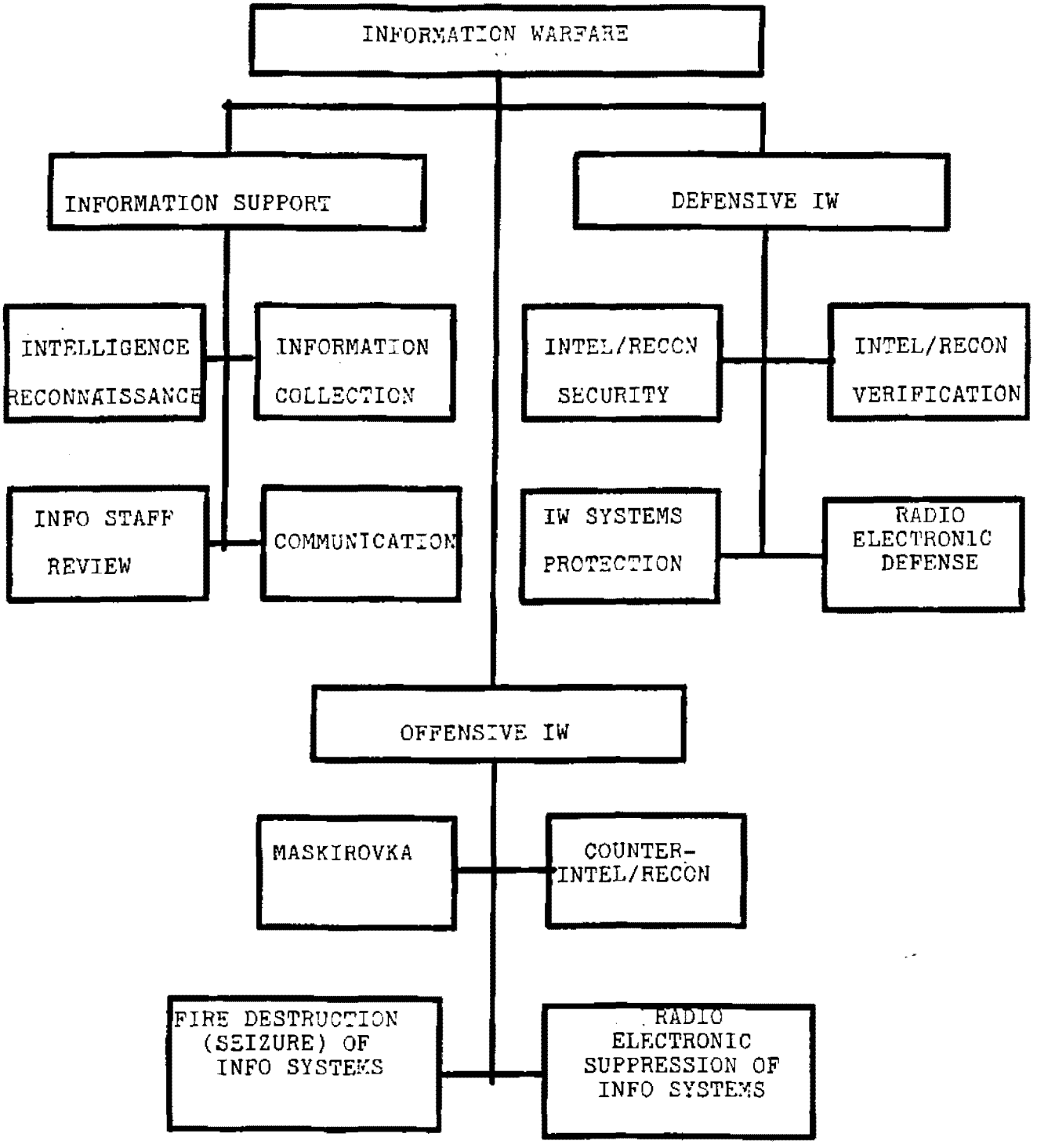

INFORMATION WARFARE
INFORMATION SUPPORT
DEFENSIVE IW
INTELLIGENCE RECONNAISSANCE
INFORMATION COLLECTION
INTEL/RECON SECURITY
INTEL/RECON VERIFICATION
INFO STAFF REVIEW
COMMUNICATION
IW SYSTEMS PROTECTION
RADIO ELECTRONIC DEFENSE
OFFENSIVE IW
MASKIROVKA
COUNTER-INTEL/RECON
FIRE DESTRUCTION (SEIZURE) OF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

FIGURE 1

whose implementation had begun many years before. The American command nonetheless feels that substantial shortcomings were revealed in the utilization of information systems:[2]

- troop subunits that were in the conflict zone in readiness for the immediate start of combat operations were often forced to wait for the arrival of communications gear, without which the organization of command and control was impossible. Even after its delivery the gear itself, extremely cumbersome and heavy, did not meet the needs of highly mobile troops;

- all of the communications nets deployed were unable to effectively handle the large masses of data typical of the video information necessary for the preparation and planning of operations;

- the time cycles for the processes of assigning strike targets and evaluating the degree of their damage after strikes were not suitable owing to imperfections of the communications systems. This frequently led to repeat strikes against targets already destroyed; and

- critically important intelligence information gathered in time, as a rule, got to the consumer with great delays, caused by the lack of a sufficient quantity of gear with message packet switching.

The results of the Desert Shield and Desert Storm operations show that the troops present in a forward theater, for the successful waging of combat operations, should also possess -- aside from the organic hardware -- a so-called "base set" of information and computer systems. The U.S. Department of Defense has given scientific and engineering specialists the task of creating a kind of "information

---

[2]Colonel V. Cherkasov, "Organization of C^3 for U.S. Forces in the War With Iraq," Zarubezhnoye voyennoye obozreniye (hereafter cited as ZVO), No. 7, 1993, pp. 11-12.

ionosphere" able to cover any conflict region on the globe in a matter of hours. A whole set of systems that currently exist separately to support the activity of headquarters and commanders, the gathering and processing of intelligence information, the command and control of troops, the selection of targets, and the planning and execution of strikes should be integrated into it. The main feature of the "ionosphere" will be the virtual absence of cumbersome station gear, and the presence of small portable devices making it possible to join the unified information network. Relays, both in the air (including on airframes and in RPVs) and in space, will be the basic element of the network. The gear of the commercial sector, which is structured on the basis of the latest achievements of technology and is considerably cheaper than military gear, will be utilized to a significant extent therein.

With a reduction in the U.S. Air Force budget and in budgets of other Western air forces, as well as a reduction in the number of aircraft, military specialists assume that the problem of sufficiency of reconnaissance assets can be solved by mass development of inexpensive drones. According to their forecasts, in the near future Western countries will produce up to 30,000 craft of various types, and the production peak will come in the year 2000. It is emphasized that despite reductions in appropriations for military purposes, the United States has sufficient financial and economic resources for creating that number of drones within the planned time periods. The press reports that two types of reconnaissance drones are being developed: the first is for reconnaissance in the tactical zone in support of divisions and brigades, with

real-time transmission of video data; the second is for reconnaissance in remote regions.[3]

The problem of increasing the reliability of information becomes especially pressing with the reconnaissance and identification of small, mobile targets and in monitoring air strike results. The experience of the Persian Gulf War serves to confirm this. Reconnaissance showed its positive side when data on stationary targets were required, and the negative side when reliable information was needed on mobile targets. Thus, it did not manage to establish the precise number and location of Iraqi missile systems that were delivering strikes against targets in Israel and Saudi Arabia. Throughout the entire war, the strike aircraft of the Multinational Forces (MNF) waged a battle against them, and not always an effective one.

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

[3]Colonel A. Krasnov, "Aerial Reconnaissance in Regional Armed Conflicts," ZVO, No. 12, 1994, pp. 28-33.

systems, which permits destroying the enemy battle management system architecture while preserving their own battle management systems.[4]

Russian experts argue that information weapons are a 21st-century weapon capable of replacing today's weapons of mass destruction. They stress that "American analysts" present one of the possible scenarios of information warfare of the beginning of the next century as follows.[5] Iran surreptitiously deploys its troops and suddenly attacks Saudi Arabia. To defend its strategic ally, the United States begins an information war against the aggressor. First of all, computer viruses and logic bombs come to life that have previously been secretly loaded into the memories of the computers used in all Iranian state, military, and economic command-and-control structures. This weapon is activated using a special command, for example, from a satellite or through international computer networks.

After the initiation of the conflict, agents of the intelligence services, who are operating on Iranian territory, use powerful portable electromagnetic pulse generators to destroy software and databases in the civilian and military command-and-control systems that are protected from computer viruses and logic bombs. At the same time, the aggressor's accounts in foreign banks are zeroed out using international

---

[4]Major M. Boytsov, "The 21st Century and the U.S. Navy," Morskoy sbornik (hereafter cited as MS), No. 7, 1995, pp. 74-78.

[5]Georgiy Smolyan, Vitaliy Tsygichko, and Dmitriy Chereshkin, "A Weapon That May Be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare," Nezavisimoye voennoye obozreniye (hereafter cited as NVO), 18 November 1995, No. 3, pp. 1-2.

telecommunications networks. These activities entail catastrophic consequences for Iran since they totally disrupt the operation of all vitally important systems (civilian and military command and control, communications, power engineering, transportation, etc.) for the country.

At the same time, the television and radio transmissions of all stations and relay stations on the territory of the country and the communications and command-and-control centers in the aggressor's troops are jammed. Materials that are directed at destabilizing the political situation, disorienting the population, and inducing panic begin to be transmitted via the electronic mass media. Chaos reigns, the collapse of the economy occurs, and the socio-political situation dramatically changes in Iran as a result of this combined attack using various types of information weapons. Under these conditions, the aggressor is compelled to abandon his plans and submits to the demands of the United States and its allies.

According to Russian experts, information warfare is not the virtual reality of computer games but a quite tangible instrument for achieving victory in a military or political conflict. The information weapon is said to be a very important part of the military and military-propaganda potential of the United States and its allies under contemporary conditions. Russia must therefore take note that the United States is consistently and aggressively preparing for the conduct of information warfare. Moreover, various types of information weapons have been tested in all of the armed conflicts in which the United States has participated (Desert Storm, the operation in Haiti, etc.).

The CIA has allegedly developed a deeply classified program able to be utilized during the development of other states' weapons and military equipment, which must contain logic bombs and viruses that are easily initiated at the required moment. This technique is called "chipping". Based upon another program, the CIA is developing techniques to influence programmers who work at firms that service military orders in order to enlist their participation in programs to introduce viruses into software.

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.

Such monitoring must encompass not only scientific-technical and technological achievements in the developments of information weapons and systems to counteract them, but also the dynamics of the prerequisites and conditions for their possible employment; i.e., changes in the foreign policy situation and predictions of global or local conflicts that carry with them the threat of information warfare. It would be natural to also track the state of domestic and international legislative and normative-legal guarantees of information security. One can imagine the ideal model of the organization of monitoring in the form of a hierarchical structure headed by a super-departmental plenipotentiary organ, for example, the Russian Federation (RF) Security Council, to which all needed and objective information on the processes that relate to the realities of information warfare flows from the ministries and departments and its own sources.

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.

The "American administration" has declared the development of a national and then an international information superhighway to be its main strategic goal. The realization of that goal not only ensures the preservation of U.S. economic and political leadership in the 21st century but will also create new conditions for the effective employment of information weapons. The prototype of this superhighway already exists -- the Internet, a world-wide association of computer networks. Operational access to the information and computer resources maintained by this network is a great benefit. But the Russians argue further that the Internet network can serve as a legal means to accomplish certain missions that would otherwise have to be resolved through the force of information weapons.

Russian military scientists stress that the latest military concept developed "in the Pentagon" is the information war concept. The primary "weapon" consists of

information devices and technologies used for wide-scale effect on enemy military and civilian information systems. The goal is to wreck his economy, weaken readiness to wage war, and ensure final victory. It is presumed that information war can be waged both independently; i.e., without using means and methods of warfare in the usual sense, as well as in combination with other kinds of combat operations.[6]

According to these experts, the U.S. military pictures realization of the concept as follows. A certain dictatorial regime (such as in Baghdad, Tehran or Tripoli) threatens a U.S. ally. Instead of sending thousands of soldiers or dozens of combatant ships to this region., the United States brings down a multitude of calamities on the dictator with the help of a computer screen and keyboard.

First, a computer virus is introduced into the country's telephone network with the help of agents, which leads to almost total disabling of telephone communications. Special microbes that cause destruction of electronic equipment also are introduced. Then computer logic bombs set for a certain detonation time destroy electronic devices controlling air traffic and rail transport. They send aircraft and trains in the incorrect direction and create preconditions for wrecks on the ground and in the air. Special Forces penetrate into the territory of the enemy capital and set off non-nuclear devices generating a powerful electromagnetic pulse (EMP). As a result of the detonation of such devices near the central bank and exchange, all computers and information systems in these establishments malfunction, and the country's financial life is paralyzed.

---

[6]Major Dmitriy Pozhidayev, " 'Computer' Aggression in Pentagon Plans," Armeyskiy sbornik (hereafter cited as AS), No. 2, 1996, pp. 90-92

Meanwhile, enemy military unit commanders are executing orders received over data systems and radio equipment, not suspecting they are false. Troops scattered over enormous expanses lose combat effectiveness. U.S. Air Force aircraft especially equipped to conduct psychological operations jam government television transmissions, substituting for them their own computer-generated transmissions in which the aggressive leader appears with unpopular statements, which leads to his loss of support by the population. And when the dictator or people from his entourage turn on "their own" computer, they discover that money placed in foreign bank accounts has disappeared without a trace.

In the opinion of the "U.S. military," information war became possible in connection with the "cybernetic revolution" and mass introduction of various information systems into all spheres of life. Western scientists even call modern society the "information" society, emphasizing the role and importance of information to man. Intelligent technology leads to changes in modern society comparable in scale and importance with those which at one time were generated by machine manufacturing. Analysts state that by 2000 people will have to work less and less with physical objects and more and more with information. According to tentative data, by this time up to 60 percent of the population of developed industrial countries will work with information, and the majority of jobs will be done by remote control.

"The Pentagon" is developing plans for accomplishing a revolution in military affairs using information technologies similar to that which occurred with tanks in the period of World War I or with nuclear weapons during World War II. Information war has been a component part of all recent U.S. troop operations. Thus, on the first day

of the Persian Gulf War, U.S. Air Force aircraft "blinded" the Iraqi Army and knocked out communications and electrical power supply systems in Baghdad. The Pentagon carried out a carefully developed psychological operation in Haiti as well to restore overthrown President Aristide to power. Based on marketing research, the Army's 4th Psychological Operations Group divided the population of Haiti into 20 groups and carried out purposeful brainwashing of each group using leaflets and radio broadcasts. Before the beginning of the invasion the CIA organized anonymous telephone calls to Haitian servicemen with the suggestion to surrender and sent corresponding messages over the computer network to members of the government.

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. Considering that the

Pentagon budget is constantly being reduced and the U.S. Army is only eighth in the world in numerical strength, the country's military leadership deems it necessary and unavoidable to use U.S. technological superiority in the data-processing and communications area.

The Pentagon leadership plans to introduce information technologies at various levels, from the large strategic formation (an information system known as "Enemy Estimate and Weapon Employment" already has been created in J. Hopkins University Applied Physics Laboratory for the U.S. Navy) to the individual soldier. By 2010 the Army command figures "to reduce combat operations to digital form by interconnecting every soldier and weapon system with electronic equipment." A Motorola study group and the U.S. Army Research Laboratory plan to demonstrate a prototype of "21st-Century Soldier" gear. His helmet will be equipped with microphones and headphones for communications, a night-vision device, infrared sensors, as well as a computer display. The microcomputer itself will be mounted in the clothing and will provide IFF, detect mines and chemical agents, indicate the precise location, and give recommendations on use of organic weapons.

And what about the "enemy"? the Russians ask. For he too may develop similar means and use them successfully. This is why last year a joint commission on U.S. security called U.S. vulnerability to information war "the principal security problem of this decade and possibly of the next century." In this connection, the country is giving special attention to developing means of protecting both military as well as civilian information systems to ensure normal functioning of the state infrastructure. The U.S.

military leadership believes that the threat of information war will grow steadily as society develops, and it intends to take all possible steps to win such a war.

According to Colonel S.A. Modestov, the war for which America is preparing will begin and will immediately follow several directions: electronic warfare, active reconnaissance, disruption of troop and weapon command-and-control systems, psychological operations, and special software programs -- hardware impact and modern computer capture: robbery carried out by hackers against foreign information systems with the knowledge of their government.[7]

In the United States, says Modestov, work has mainly ended on the compilation of a single electronic catalogue of software programs for impact on enemy information resources that have been recorded to the present day. And quite a few of them are being accumulated. If 1,450 viruses were listed in the documentation on the Dr. Web anti-virus program (version 3.08 dated December 26, 1995) that is known in Russia, then Englishmen Alan Solomon and his wife Suzanne, who owned the family firm "S. and S. International" until recently, number 8,000 viruses in their lists (including 3,000 of the most dangerous). Hundreds of new viruses are being added to this long list on a monthly basis.

A database has also been created on the personalities of all of the professional hackers who have been discovered. It should increase monitoring of this category of

[7]Colonel Sergey Aleksandrovich Modestov, "The War for Which America Is Preparing: The Evolution of Armed Combat in the Information Age," Nezavisimoye voyennoye obozreniye, 14 March 1996, No. 5, p. 2.

criminals with the goal of preventing illegal activities and rendering assistance to investigatory organs on cases that have already been committed and discovered. Data on experts of this type can be required to involve them in organized impact on the enemy if necessary.

The achievements of American computer equipment and information provide a marked advantage in preparation for the new war. Neither Russia, Ukraine, Kazakhstan, or Iran supply computers or software to the United States; it is most likely the reverse. Who can guarantee that the equipment that has been acquired is free of software and hardware rubbish?

SOVIET VIEWS ON INFORMATION TECHNOLOGIES

The Soviet vision of future war also focused primarily on the dramatic changes engendered by the incorporation of information sciences into the military sphere. According to Military Thought, for example, "NATO military specialists" pin special hopes on implementing the "Strategic Computer Initiative," whose primary objective is to make all new conventional weapons "intelligent" to ensure decision-making in real time. Indeed Soviet experts stressed that the enhanced effectiveness of weaponry resulting from its "intellectualization" underlies many of the current, revolutionary changes in military affairs.

The "intellectualizing methods" permit control of the weapon not merely up to the moment of fire, but throughout the entire cycle of its use. This produces an almost 100-percent probability of kill, and frequently makes excessive projectile speed and weight unnecessary. The control factor becomes determining, whereas increasing

speed and weight leads to reduced control and effectiveness. As a result, said the Soviets, the emphasis in the competition between offensive and defensive weapons is shifting in favor of the control factor: the more controllable and maneuverable weapons system will win. A tank, for example, is inferior to a missile in all respects. The ideal design is a flying disc on an air cushion that can move easily in all directions and is armed with a variety of missiles.

According to Soviet experts, 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.

Soviet experts noted further that 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.

Soviet military scientists also noted that the Gulf War allowed the MNF to test the application of some of the latest military technologies -- particularly advances in information science -- for the first time under actual battlefield conditions.[8] Elements of artificial intelligence were present in virtually all weapon systems that the MNF employed during the war -- the highly accurate Tomahawk cruise missiles, the Patriot antiaircraft missile system, the new F-117A Stealth aircraft, the M1A1 Abrams tank, the JSTARS ground surveillance and fire-control radar, and many others.

According to Soviet experts, airborne guidance and fire-control systems incorporating elements of artificial intelligence enabled the MNF to economize substantially in their operational employment of combat assets and to employ these assets with greater effectiveness. Thanks to microprocessors not only on board the carrier, but also integrated in the weapons themselves, they were able to increase the accuracy of delivery to the target by factors of 3-4 and achieve hit probabilities of 90 percent (although they were doing all this in an environment where Iraqi electronic countermeasures [ECM] systems remained virtually "silent"). They were achieving accuracies so high that crews were being tasked with the destruction not of entire targets, but only of critical components of a target.

[8]For example, see V. Frolov, "Artificial Intelligence Goes to War," Krasnaya zvezda (hereafter cited as KZ), 24 October 1991.

Soviet experts also noted that the extensive employment of computers in support of MNF military operations played a no less important -- and perhaps even a more important -- role in the war. The MNF accumulated detailed data on the enemy both during the period over which they were preparing for an operation and during the conduct of the operation itself. This enabled them to pinpoint troop dispositions and the location of command posts, communication centers, and air defense systems. The coordinates of primary fixed targets (militarily significant industrial installations, electric power plants, scientific research centers working on the development of nuclear and chemical weapons, storage facilities etc.) were fed into an integrated guidance system for various types of high-precision guided weapons. Using supercomputers, the MNF was able to compile an "electronic dossier" on 100 top-priority targets, a number which was soon increased to 300. This "electronic dossier," located at MNF headquarters, was updated continuously. Fragmentary and occasionally contradictory information was filtered out; then, with the establishment of a list of priority targets, it became possible to determine with mathematical accuracy the optimum routes of approach to these targets, and the forces and number and mix of weapons that would be required to neutralize air defenses and damage specific targets to the level required by the MNF command.

According to Soviet experts, the computers and other electronic equipment that the MNF employed in support of its command, control, and communications systems proved fairly effective and reliable. This concrete example has now inspired the addition of a new axiom to the body of military art: For combatants contending in military conflict today, "superiority in computers" is of precisely the same significance as superiority in tube artillery and tanks was to belligerents in earlier wars.

RUSSIAN VIEWS ON INFORMATION TECHNOLOGIES

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. For example, Rear-Admiral V.S. Pirumov explains that combat potential is an objective integral (generalized) index of the aggregate capabilities of a grouping of troops (forces), on the basis of a comparison of which the degree and nature of the superiority of one side over the other can be determined. Needless to say, in calculating a given index it is necessary, out of all the diverse characteristics of weapons and military equipment, to count only those that influence definitively the nature of armed conflict. Here one should keep in mind that some of them can have a direct effect on the enemy (for example, means of fire destruction), and others an indirect effect, by building up the combat potential of the means of direct effect. These include, especially, information systems and resources, as well as electronic warfare (EW) resources.[9]

There has clearly appeared a specific field -- information -- the gaining and holding of superiority in which can play a 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

[9]"Rear-Admiral Pirumov Defining Defensive Sufficiency," in JPRS-UMA-91-008-L, 22 August 1991.

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 he means 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.

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).

Admiral Pirumov also argues that the experience of exercises and local wars 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.[10] He notes especially the MNF's broad

[10]Rear-Admiral V.S. Pirumov, "Two Aspects of Parity and Defense Sufficiency," VM, No. 2, 1992, pp. 26-34.

use of precision weapons of various modifications and principles of action. For example, sea-launched Tomahawk cruise missiles were employed massively for the first time, and comprised the forward echelon of first and subsequent MNF missile and bombing strikes against installations of Iraq's state and military leadership. These missiles' inertial guidance system and active radar homing head provided a CEP of no more than 10 m and a target kill probability of at least 0.9.

Precision weapons also were widely employed in air force combat operations. These basically were air-to-surface anti-radiation missiles with devices homing on a source of electronic emission. Their mass employment with simultaneous creation of a powerful, effective jamming field essentially paralyzed Iraqi air defense. Guided aerial bombs with laser illumination of the target as well as air-to-surface guided missiles also gave a good account of themselves.

On the whole, writes Pirumov, wide use of precision weapons permitted the MNF to have a smaller arsenal of weapons by the beginning of combat operations than if the entire unit of fire had been only traditional. In addition, these weapons made possible the destruction of military installations in areas of mass residence of citizens without inflicting great losses on the population or installations of the Iraqi economy. "American military specialists" regard precision weapons as more advantageous than traditional weapons according to the cost-effectiveness criterion. According to their calculations, destroying six different targets requires 100 sorties with conventional 500-pound bombs (costing $15 million), or 20 sorties with guided bombs (costing $0.6 million). In addition, the massive use of missiles with different or combination guidance systems sharply improves effectiveness of a strike under conditions of heavy

air defense, in the presence of jamming, and in adverse weather conditions. Thus it can be stated that without electronic equipment and computers to implement information support to the employment of weapons, it is impossible not only to offer effective opposition (even with a considerable number of attack weapons available), but also to create precision weapons themselves.

RUSSIAN VIEWS ON INFORMATION WARFARE

According to Russian experts, the principal shortcomings in information technology in the armed forces of the Russian Federation are:

- *a sharp lag in information technology of lower levels of command and control and, as a consequence, the absence of a real information base;*
- *the adoption of various hardware and software that are not compatible;*
- *the insufficient level of the capabilities and characteristics of the computer technology being used, and the low degree of saturation of subunits and services with modern computer hardware;*
- *the insufficient utilization in the armed forces of contemporary achievements in the field of new information technologies, methods of mathematical modeling, and artificial intelligence.*[11]

These experts state further that the principal directions and aims of the dissemination of information technology in the armed forces are:

---

[11] V.N. Medvedev and S. K. Lopukhov, "Information Technology in the Armed Forces of the Russian Federation," Vooruzheniye, politika, konversiya (hereafter cited as VPK), No. 1, 1993, pp. 57-60.

- **in the field of military construction:** the fuller utilization of information resources for the scientific substantiation of armed forces structures, their necessary size, sophistication, development prospects and support, through the broad-scale incorporation of modern means of information technology for the accelerated use of the achievements of science and technology in the interests of the armed forces, predicting the military-political situation, and performing measures for the preparation of the armed forces and the country as a whole to repel aggression, based on the development of multifunctional information-management systems;

- **in the field of armed combat:** increasing the effectiveness of the development of plans for the employment of the armed forces, reducing the times and raising the quality of decision-making in preparing for operations, and providing a flexible response to changes in the military-political situation;

- **in the field of command-and-control of the armed forces:** increasing the operatibility, reliability, and concealment of the command and control of troops (forces) through the adoption of improved means of automation;

- **in the field of supporting the troops:** raising the qualities, completeness, and operatibility of all types of support for the troops, under any conditions, through the widespread and comprehensive incorporation of means of information technology and new information technologies, and the creation of favorable conditions with the aim of supporting the everyday activity of units and subunits in peacetime for the organized and timely conduct of operations under conditions of a combat environment;

- **in military-scientific activity:** raising the effectiveness of the fulfillment of scientific-research work on the basis of equipping the subunits (units) for military-scientific information with the latest means of information technology, uniting them into information networks, priority research of problems in the preparation and waging of modern operations and combat activity connected with the increasing influence of information technologies, intensification of the creation of new means of armed combat and command and control of troop support, substantiation of efficient forms and methods of combat preparation of the troops, and optimization of the ways of achieving the required characteristics of arms and military hardware;

- **in the field of military education, military training, and indoctrination:** enhancing the quality of training of military specialists on the basis of efficient information support for the tasks of training personnel, creating an information-technological base for the restructuring of military education through a deepening of scientific research, the intensification and individualization of training, and adaptation to the abilities of the trainees and the activation of their creative potential;

- **in the field of routine activities:** raising the quality of decision-making in the process of everyday activity of the subunits, units, and institutions of the armed forces, the performance of garrison and guard duty, the escort of military freight, the observance of regulation order, and the reinforcement of military discipline;

- **in the military-legal and social realm:** the information technology of the armed forces pursues the aim of a substantial rise in the quality of information-legal support for the everyday activity of the troops, improvements in law-making activity, and assurance of a greater level of awareness on questions of social protections for servicemen and their families.

The dissemination of information technology, along with the development and improvement of traditional information technologies, presupposes the adoption of new information technologies that support the automated resolution of poorly formalized tasks in various fields of activity of the armed forces, including by a user who does not have special training in the field of computers. The new information technologies are the foundation for resolving applied tasks in the command and control of troops; the creation of robotized weapons systems; and the support of the everyday activity of the troops, services, and the training of personnel.

The directions for the dissemination of information technology in the armed forces also encompass priority problems, within the framework of which the following tasks should be resolved in the near future.

- *the gradual creation of a telecommunications environment for the armed forces and its link-up with nationwide communications and data-transmission systems, and the further development of communications equipment;*

- *the development and incorporation of base problem-oriented systems, software, and hardware for the structuring of local and global information and computer networks;*

- *the fastest possible equipping of armed forces staffs and organizations with base means of information technology and personal computers, advanced communications and telecommunications gear, and improved organizational techniques as the foundation for the adoption of "paperless" information technologies;*

- *the improvement of methods and tools for the development of software and the use of CASE technologies, without which progress in the creation and adoption of subsequent generations of automated systems and ASUVs is impossible;*

- *assurance of the technical, information, linguistic, and program compatibility of the means of information technology;*

- *improvement of the system of training, retraining, and skills enhancement of military specialists in the realm of information technology;*

- *the creation of standardized, advanced means of information technology with a regard for the requirements of ensuring the security of the information.*

The strategy of information technology for the armed forces and plans for the performance of the priority operations should be defined in the Conceptual Framework

for the Dissemination of Information Technology in the armed forces and the Program of Information Technology for the armed forces.

According to General-Major N.A. Kostin, the results obtained through simulation attest to the fact that a specific field is emerging as a phenomenon in modern warfare -- that of information where, once superiority is won and held, it can play the decisive role in achieving success by one of the warring sides. Proceeding from the experience of the war in the Persian Gulf the formula of success in modern war can be as follows: first win supremacy in command and control, then in the air, and only then commit your ground troops to action. Although this statement is imprecise, it essentially reflects the probable nature of modern combat operations. Hence the conclusion -- that already at this stage combat operations of the initial period of hostilities will be a struggle for information dominance between the opposing groupings of forces -- is well-founded.[12]

From the point of view of information confrontation, armed hostilities today can be viewed as a conventional set of two components: that of electronic and fire, and that of information, each of which has specific targets, facilities, and methods. The electronic and fire component implies a field where the capabilities of weapons and electronic warfare facilities combine in making a direct impact on the enemy's hardware and personnel.

---

[12]General-Major N.A. Kostin, "Appraising the Effectiveness of Troops (Forces) and Weapons Control Disorganization," Voennaya mysl' (hereafter cited as VM), No. 11, 1993, pp. 39-44.

The information component implies a sphere defined by the capabilities of facilities that procure information (reconnaissance) and its utilization (command and control) in the interests of realizing the combat potential of what directly impacts on the enemy (weapons and electronic warfare facilities). This sphere accounts for nearly half of the combat potential of a grouping being realized. The mentioned data essentially determine the role and importance of the information component; i.e., the system of reconnaissance and command and control in the realization of combat capabilities of troops.

According to Major M. Boytsov, the goals of information warfare can be characterized briefly: to blind, deafen, demoralize, and decapitate enemy entities for command and control of the armed forces.[13] To blind means to disrupt the flow of intelligence from collecting entities to the enemy command element and also to disrupt the output of target designations and warnings from reconnaissance to command-and-control entities. To deafen means to use EW assets to neutralize enemy information networks. To demoralize means to saturate enemy information networks with false commands and reports, misleading him and corrupting his command-and-control system. To decapitate means to destroy enemy command-and-control entities and their communications equipment. Successful operations of cruise missiles and aircraft which disrupted the Iraqi command-and-control and communications system in the first hours and days of the Persian Gulf War contributed to the realization of the importance of performing these missions.

---

[13]Major M. Boytsov, "The 21st Century and the U.S. Navy," MS, No. 7, 1995, pp. 74-78.

The military-technical direction of Russian military reform oriented toward the highest world level, where high technologies hold the leading place, therefore becomes one of the determining factors. In other words, it is a matter not only of precision weapons for priority development of strategic systems, qualitative changes in conventional weapon systems, elimination of distinctions between nuclear and conventional weapons, and military use of space, but also of military-information technologies. They are what will become the most formidable weapon of the 21st century.[14]

The assessment of information as a strategic resource by the military-political leadership of a number of countries, above all the United States, becomes understandable. Herein lie the causes of a constant increase in appropriations for development of information technologies. The greater the information capacities a state possesses, the more likely it can achieve strategic advantages with other conditions being equal. The growth in the need for information actually has led to where it is not legitimate to estimate a state's military might and security without considering the information component.

A new power deterrence factor -- the threat of inflicting irreparable damage on a particular country's information resources -- is 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

---

[14]"New Trends in Power Deterrence" (Roundtable Discussion on Power Deterrence), AS, No. 9, 1995, pp. 12-19.

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.

According to Naval Digest, the development of science and technology in recent decades engendered discussions about the use of robots; psychotronic means; antimatter; and also plasma, laser, beam, electronic, and other varieties of lethal and nonlethal weapons in future wars. Some of these ideas are materializing already, and

with them a new quality of information opposition.[15] The circumstance that over half of the world's population will be living in cities in the first third of the 21st century and can especially suffer in the event of wars began to play a role of no small importance here. Therefore it is believed that to win victory with minimum victims among the civilian population and minimum property damage, it will be necessary to employ very precise lethal and nonlethal kinds of weapons in order to exert sufficient pressure on the opposing country's leadership directly or through the population masses of cities. Electronic weapons in particular can prove to be specifically such a means.

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:

---

[15]Information War," MS, No. 10, 1995, pp. 69-73.

- 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.

The essence of IW/C^2W is to take advantage of vulnerable places in the enemy system of command and control, communications, computer support, and intelligence in order to diminish the effectiveness of their work, to create a false picture or a distorted impression of the situation in the enemy, and under conditions of a scarcity of time to force him to take incorrect and disadvantageous actions. This will permit friendly command-and-control entities, using the advantage of time and reliability of information, to preempt the enemy in estimating the situation, making a decision, planning, communicating orders to those responsible for execution, checking plans of

action by running them on automated systems for modeling combat operations and, finally, to preempt him in the final organization of combat employment of troops and forces. Superiority in IW/C^2W ensures surprise and the possibility of delivering a knock-out blow even before a formal announcement of the beginning of combat operations (and such blows already have been legitimized), and it will permit seizing and holding the initiative and concluding the military conflict as fast as possible on terms most favorable to yourself.

As of today the organization of IW/C^2W in the United States includes the following aspects:

1. Deception
2. Operations security
3. Psychological operations
4. Electronic warfare (EW)
5. Destruction

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/C^2W. 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. For example, in preparation for and during the 1944 Normandy Operation, the Allies used simulated assets to create a situation that forced the Germans to hold 19 divisions on a diversionary axis at the Strait of Dover; feints with a similar concept by U.S. amphibious groups with only one Marine brigade, as well as disinformation and a false electronic situation created in the Persian Gulf in 1991 forced the Iraqis to divert 7 divisions for an anti-landing defense.

Electronic means of deception now are used, first of all, by introducing to enemy systems one's own emissions that simulate his; secondly, by changing friendly emissions or simulating them. In the first instance enemy disinformation is achieved

by penetrating his unclassified and classified information networks and channels to transmit false information in them. In the second instance disinformation is achieved, for example, by the creation of dummy ship groups that divert enemy forces and assets to themselves and allow the main body to act covertly and suddenly.

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. For example, such an effect was accomplished during the war against Iraq by disseminating appropriate video materials inside the country and by radio and television broadcasts from outside. The Iraqi command even went so far as to confiscate radio receivers from its servicemen. As it turned out, around 60 percent of Iraqis who surrendered had listened to foreign broadcasts and largely gave them credence. The U.S. Voice of the Gulf radio, which broadcast to the Iraqis 18 hours a day, achieved such authority among them that transmitting a message about the approach of coalition forces to Kuwait contributed to the beginning of mass flight of Iraqi troops from the city.

Electronic warfare envisages accomplishing EW suppression by jamming enemy communications equipment; detection and position-finding equipment; navigation equipment; and space-based, airborne, ground-based, and sea-based computer support equipment in order to make him blind, deaf, and dumb. The success of operations by U.S. forces for EW suppression of Iraqi radar and communications equipment in the 70 MHZ-18 Ghz band is generally known. It seemed that new electronic warfare tactics also were tried out in combat operations against Iraq. For example, one cannot exclude the use of software inserts in imported gear used in the Iraqi air defense system for blocking it at the beginning of the war. In general, EW suppression methods are becoming more and more refined and effective.

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.

Based on the experience of the war against Iraq, the blinding of its command-and-control system began at H minus 22 minutes by the destruction of air defense radars, which by the end of the first 24 hours of the war disrupted the operation of 95 percent of radars by massive employment of anti-radiation missiles and by missile and bombing strikes. Decapitation of the Iraqi military command-and-control system began

at H minus 9 minutes to H plus 5 minutes by the delivery of air strikes and Tomahawk sea-launched cruise missile strikes against armed forces and National Air Defense command-and-control entities. As a result, in the first two weeks of the war 60-75 percent of command-and-control facilities of the highest and middle echelons had been destroyed or damaged.

The delivery of air and missile strikes against civilian radio broadcasting and television stations, against radio-relay station masts, against bridges over which fiber-optic communications lines ran, and against telephone and telegraph stations and switching substations also contributed to the disruption of command and control. Destruction of the electrical power supply, achieved by analogous strikes against electric power stations or by using carbon fiber from air-launched cruise missiles against power transmission lines, disrupted the operations of military computers and created an acute time shortage for command-and-control entities.

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.

According to Russian general officers, achieving superiority in information opposition, with the tendency of its importance to grow as levels of nuclear opposition decrease, is becoming the most important factor in the nature of modern warfare. Therefore a traditional analysis of the state of strategic balance with consideration only of quantitative-qualitative characteristics of strategic forces can provide worse results than with a more realistic account of the influence of the sum total of parameters of strategic forces.[16]

New criteria are thus needed for estimating the effectiveness of strategic forces and arms under conditions of information warfare. Development of weapon systems also is an incentive for this. The criteria are oriented both toward strategic offensive as well as defensive systems -- and above all reconnaissance-information systems, toward development of weapons based on new physical principles, and toward a shift of the center of gravity of warfare from continental and ocean theaters of military operations (TVDs) into the sphere of space.

Among others, Major D. Pozhidayev argues 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

[16]General-Lieutenant Aleksandr Skvortsov and General-Major Nikolay Turko, "Strategic Stability: Key to National Security," AS, No. 1, 1996, pp. 4-8.

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.[17]

All branches of the Russian Armed Forces have designed blueprints for reorganization in the new information environment. Russian naval theorists, for example, understand the information revolution to mean the process of ever-greater use of information and knowledge as a third type of asset (in addition to material and energy) that involves the introduction of systems to automate the processing and employment of information in all areas of life and social activity. It is not specialists in cybernetics and computers who give the forms and means of acquiring and processing information but the information revolution that is determining the paths of development of research, production improvement, productive forces, etc.[18] On the basis of systematizing and generalizing domestic and foreign trends of development in information science, they think it expedient for the Russian Navy to take the following strategic lines on information development (see Figure 2):

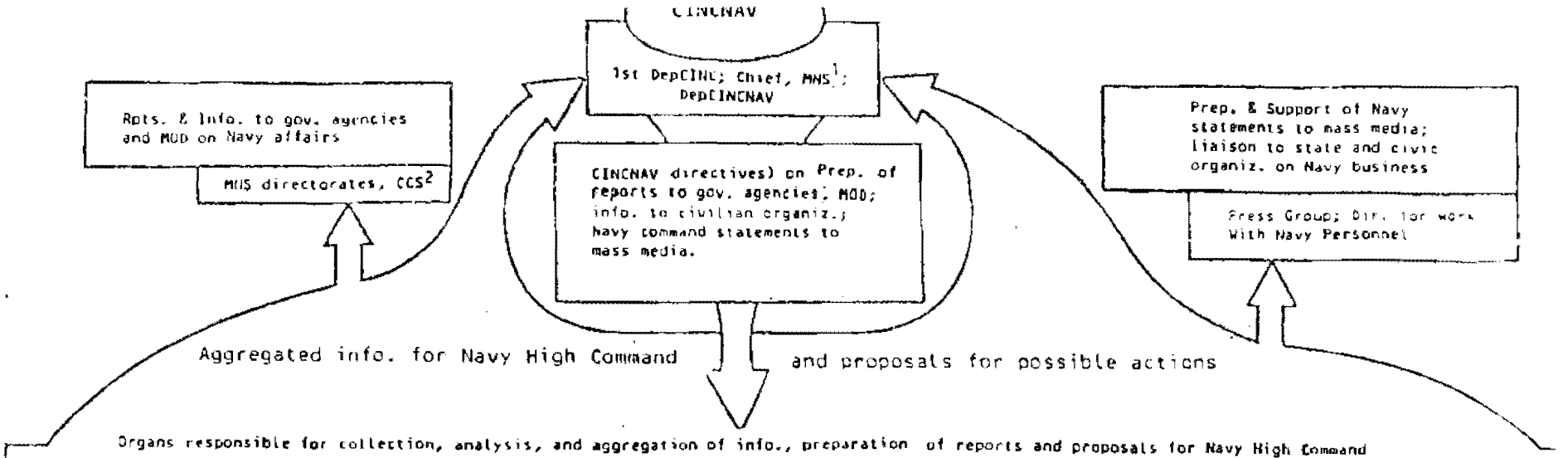
1. Developing a single Navy information environment, organically a part of the armed forces information environment;

2. Making the structures of information facilities and information-processing equipment general-purpose;

---

[17]Major D. Pozhidayev, "General Problems," ZVO, No 2, 1996, pp. 2-4.

[18] Captain 2nd Rank A. Tutushi and Captain 2nd Rank O. Turovtsev, "The Objective Logic of Bringing About the Information Revolution in the Navy," MS, No. 6, 1993, pp. 24-28.



Organs responsible for collection, analysis, and aggregation of info., preparation of reports and proposals for Navy High Command

Main directorates, directs., services and depts. of Navy	MNS directorates; Navy Internat. Press Service; MNS Foreign Technica. Relations Dept.; MNS Intell. Direct. (within the scope of competence)	MNS directorates, CCS; Dir. for Work with Navy Personnel; Navy main directorates, directorates, services & depts.; Navy Press Center.	MNS Intell. Directorate	Navy Press-Center; MNS directorates; CCS; Navy main directorates, directorates, services & depts.; Direct. for work with Navy Personnel	Navy Internat. Comm.; MNS Intell. Direct. (on foreign scientific info. matters); Navy scientific organiz.	Direct. for work with Navy Personnel; Navy Logistics, Navy Financial Service, MNS Legal Group; Navy Medical Service; Navy Main Engineer. Direct
Content of the main areas of information for the Navy High Command						
Normative acts (laws, decrees statutes of RF; MOD orders and directives) on Armed Forces & Navy building, and their implementation.	Treaties & agreements; MFA papers; military technical cooperation; press conferences and statements of officials, publications and broadcasts in foreign mass media about CIS and Navy problems.	Info. called for by Navy prompt reports schedule; crises involving Navy forces.	Intell. info. (operational, scientific, naval policy & doctrines of the major naval powers & alliances; ITAR-TASS info.; COMPAS S&T Center, etc.	Media statements by officials & private individuals; public coverage of the work of civic & govt. organizations on problems of basing and building the RF/CIS Navy; crises.	Scientific info. (directive decs., participation in conferences, symposia, seminars & exhibitions; major problems of mil. science; technology policy; weapons & equip. development; improvement of Lab R&D network, upper-level schools, training grounds; scientific personnel training; basic & investigative research; expenditures in comparison with major world navies); publication of Navy Information Digest	Social-living cond. problems of Navy personnel (supplies mess, R&R, housing, pay, etc.

[1]Main Navy Staff [2]Central Cartographic Service (Navy)

FIGURE 2

3. Developing architecture concepts, global standardization of functional design, interfaces, and inter-system protocols;

4. "Intellectualizing" information systems, development of semantic structures and inclusion of rules of data interpretation, and expert derivation logic as part of data- and knowledge-bank systems;

5. Introducing technological processes of hardware-software components, local and global information-computing nets, graphic data processing equipment, optical disks, etc.; and

6. Introducing information systems for mass users on a wide scale.

RUSSIAN VIEWS ON INFORMATION SECURITY

According to Russian military scientists such as Colonel A.I. Pozdnyakov, a new, post-nuclear development stage is beginning. The effectiveness of modern weapons is increasingly determined not so much by their firepower as by the informational logistics level. Information provision for the army has become a priority task of military-technical policy. Within the content of warfare the importance of informational and technical struggle has grown. Superiority in the information provision level is an indispensable condition for victory in an air, sea, and even ground battle (engagement or operation), and a guarantee of success in air defense. This is borne out by the experience of contemporary armed conflicts and local wars. The growing role of informational and technical struggle obliterates the boundary between war and peace. The armed forces of a number of countries are in a state of constant informational confrontation, while military information science in peacetime addresses the tasks characteristic of war. "The Pentagon," for example, takes guidance from the slogan: electronic warfare is never declared by anyone; it never stops; it is conducted covertly and knows no boundaries in space or time. Struggle has begun for control over

computer networks. Exchange of informational strikes is becoming increasingly dangerous because their effectiveness is growing very fast.[19]

The informational security of the individual is characterized by the extent of the protection of his psyche and consciousness against dangerous informational impacts: manipulation, disinformation, driving towards suicide, humiliation, and so forth. It should be noted that informational impacts are dangerous (or useful) not so much in themselves as in that they set off powerful substance and energy processes and direct them. The essence of informational influence lies precisely in its ability to set off and control the substance and energy processes whose parameters are higher by several orders of magnitude than the information itself.

The first is related to the loss of valuable information which either lowers the effectiveness of one's own activity or enhances the effectiveness of the activity by an adversary or a competitor. If the target of such an impact is people's consciousness, then what is involved is the revelation of state secrets; the recruitment of agents; special monitoring measures and means; the use of lie detectors; and also medical, chemical, and other impacts on man's psychology with the aim of forcing him to loosen his tongue or, on the contrary, forget something. Security against this type of informational impact is ensured by censorship and counterintelligence bodies and by other informational security subjects. If the source of information consists of technical systems, then we are dealing with technical intelligence or espionage (interception of telephone conversations, radiograms, and other communication systems signals), and penetration

[19] Colonel A. I. Pozdnyakov, "Information Security of the Individual, Society, and the State," VM, No. 10, 1993, pp. 13-18.

of computer networks and data banks. This sort of activity is undertaken, for example, by the U.S. National Security Agency, which spends $15 billion a year on such programs. Technical intelligence is counteracted by counterintelligence bodies and also by structures dealing with the theory and practice of protecting computing means and communication systems.

The second type of informational impact is related to the dissemination of the negative information which may not only lead to dangerous mistaken decisions but also force the individual to act to his own detriment and even commit suicide, or lead society to a catastrophe. Informational security of this type should be ensured by special information and technical counteraction structures. They neutralize the acts of disinformation, cut short manipulation of public opinion, counteract electronic warfare, and remove the effects of computer-assisted attacks.

Among others, Colonel Pozdnyakov notes that 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.[20]

According to Military Thought, the active dissemination of computerized systems in the various spheres of society's life inevitably makes it increasingly dependent on the stable circulation of information flows. As a state evolves further, the share of information product in the overall production volume will be growing, substantially defining its economic and military potential.[21] The effectiveness of using information resources depends primarily on the availability of data; their configuration; and means and methods of obtaining, processing, distributing, and storing them. Therefore computerized data and the sum total of various means of managing and controlling them will constitute a specific sphere of production. Specialists call it a computer information sphere or simply infosphere, understanding it as a body of general and specialized programs for creating, processing, and storing computerized data.

Because the viability of many elements of the state depends directly on the state of its infosphere, it would be logical to consider the latter as a new object of military or subversive impacts. With the current pace of computer technology dissemination in the so-called vital systems -- complex organizational-technical and technical systems whose malfunctioning or breakdown results in the disruption of state and military control as well as financial and money circulation systems, a sharp decline in the country's defense capability, and global ecological and man-caused catastrophes -- the

---

[20]"Press Review," ITAR-TASS, 1 August 1995.

[21]Lieutenant Colonel A.N. Lukashkin and Captain 2nd Rank A.I. Yefimov, "The Security of the Infosphere of Strategic Defense Systems," VM, No. 5, 1995, pp. 48-52.

infosphere is bound to become one of the most likely objects of military confrontation in the near future. Clearly, in possible military conflicts that side will have an advantage which will be able to produce a covert impact on elements of the enemy's infosphere, hampering or precluding the use of its vital systems.

Therefore the processes of computerization and intellectualization of vital systems lead to the fundamental problem of infosphere security, elevating it to the rank of a major national security problem. Special attention needs to be given to the security of the infosphere of strategic defense systems which are understood as critical military application systems used by the state for addressing global tasks in ensuring strategic deterrence and repulsing possible aggression (combat command-and-control and communication systems of the Strategic Nuclear Forces, the early-missile-attack warning system, the air defense system, and so forth).

Research shows that the problem of the security of the infosphere of strategic defense systems (ISDS) has several aspects. Among these, two aspects occupy a dominant position: the operational and technological security of infosphere components. Operational security is related to the possibility of direct or indirect unauthorized impacts on ISDS elements in the process of their operation (combat employment). Subject to impacting can be both the information capabilities and means of their control. This aspect is not new, and there is sufficient scientific basis and practical experience to address problems related to protecting information in computer systems and ensuring their security in operating military systems.

The problem of technological security stems from the possibility of producing an early covert impact on elements of the infosphere of emerging strategic defense systems. It is little investigated and so far it is too early to talk about its practical solution. Studies show that the most likely target of such impacts will be the software constituting the basis of the complex ensuring the reception, semantic processing, distribution, and storage of data used in employing strategic defense systems in combat. The Russians believe that the main means of hostile impacts will be algorithm and software bombs.

The algorithm bomb manifests itself in a deliberate, covert distortion of a particular element in a task-resolving algorithm or such an organization of this algorithm whereby the realization of the software package in the making will be accompanied by unauthorized limitations on the implementation of the required functions, their rejection, or the appearance of unforeseen functions (actions) under certain conditions in the computing (data-processing) process.

The software bomb is a set of operators deliberately inserted in covert form into software components at any stage of its development, realizing a certain condition in the computing (data-processing) process. The bomb as such constitutes an information-logical construction that includes both an activation mechanism and an implementation mechanism. Depending on the method of building the activation mechanism, bombs are subdivided into automated and controllable. In the former case the mechanism is prepared to be activated when a weapon or a command-and-control system is employed in combat. In the latter case the activation mechanism is controlled from the outside. The implementation mechanism can be realized by one or several commands from a

software component or generated dynamically during the computing process. In the latter case there can be an option for its self-destruction after the task has been executed. The orientation of the implementing mechanism's action is determined by the creative abilities of the bomb's developers.

It appears that one-use algorithm and software bombs are the most dangerous, because the principle of using them envisions their covert presence within a software component. Such bombs will probably be realizing the algorithms of full or selective blocking of software component functions. Multiple-use bombs will eventually manifest themselves, directly or indirectly. Therefore in peacetime they will be detected sooner or later.

Opinions of Russian specialists in military systems about the feasibility of using algorithm and software bombs as a means of impacting on the infosphere are divided. There are two -- basically opposite -- views on the problem. Some skeptics consider the possibility of impacting on weapon and command-and-control systems by using algorithm and software bombs as a kind of semi-scientific fiction. Some of them reject the mere question, regarding it as an element of spy-mania. Apparently their position partly stems from their unpreparedness to believe in the software-informational vulnerability of leading-edge systems. Some skeptics think that bombs as information objects may be studied scientifically but only from the theoretical point of view, because covert realization of bombs within the body of a software component is unlikely and also unsafe for their developers from the legal point of view.

Others, optimists, are sure that the use of algorithm and software bombs as elements of information weapons is feasible and quite effective. Their opinion is backed up by a number of publications in domestic and foreign literature, which data to a certain extent can be seen as precedents of the practical application of algorithm and software bombs.

The discussion of the issue of algorithm and software bombs raises many questions. Four of them are of key importance: Who potentially can create and plant bombs into the software components of military systems? What can be the motives for producing an algorithm or software bomb? How to detect the presence of a bomb within the body of a software component before a given weapon system or command-and-control system is manufactured or adopted for service? What are the most likely operational-tactical and strategic consequences of activating bombs in the process of combat action with the participation of corresponding systems?

Answers to these questions to a large extent define the makeup of the model of threats and the concept for ensuring the technological security of the ISDS. As far as the first question is concerned, the answer is clear-cut and unequivocal -- personnel directly involved in working out algorithms and software for military systems, who are well acquainted with software development technology and the combat employment of a new system.

Russian experts stress that a programmer has a highly "plastic" material at his disposal, which conveniently lends itself to creativity. Wide use can be made of the specifics of the internal-machine representation of constants or groups of constants and

the latent specifics of command or micro-command implementation which are normally not described in documentation but are known to the programmer. For instance, one can organize a "second-level" computing process or form a deliberate "dynamic defect" which is absent in the original software code. Therefore it is logical to suggest that, unlike the widely used "electronic bombs," algorithm and software "bombs" are a more sophisticated means of counteraction. As for the possibility of detecting algorithm and software "bombs" in the body of a software component, special research is needed here. The consequences of using "bombs" are defined by the designation and design characteristics of specific systems.

Therefore the problem of ISDS security exists, and its resolution is primarily related to the scientific and practical analysis of the technological aspect. The adoption for combat service of advanced computerized (intellectualized) strategic defense systems must be accompanied by special independent control procedures to ensure the security of all their software components; until the security of the infosphere of strategic defense systems is reliably ensured, it is expedient to have reserve (duplicating) elements (subsystems), built on the principle of the minimum use of software.

In 1995, Colonel A. Pozdnyakov reiterated that the effectiveness of modern weaponry is determined not only by firepower, but also by information parameters -- precision, controllability, and high-speed operation. The importance of information-technology countermeasures in the content of military operations is growing. Superiority in the airwaves is now an indispensable condition for victory in combat, battles, and operations. This is evidenced by the experience of modern-day armed

conflicts and local wars, and especially by the results of the first strike against Iraq in the Gulf War.[22]

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

[22]Colonel Aleksandr Pozdnyakov, "Information Security," Granitsa Rossii, September 1995, No. 33, pp. 6-7.

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.[23]

Insufficient attention is being given to ensuring the reliable functioning of the command-and-control system in work being done in the armed forces to create automated command-and-control systems. Certain work has been done, but questions of ensuring reliability of software and hardware are almost not considered. The crux of the problem in the manufacture of components of automated command-and-control systems is not to allow the use of insufficiently reliable software and hardware that has not been checked on a guaranteed basis for being "clean" of "logic bombs," "traps," "viruses," and "inserts."

Leading Western firms have continued to hold key positions in the field of information support of the most diverse spheres over the last 5-7 years. It is natural that manufacturing firms and sellers are guided by their own political and economic interests in presenting any kind of S&T and technological assistance. Suffice it to recall the discussion that unfolded in the United States over introduction of the Clipper integrated microcircuit to communications systems and the formation and legal formalization of a new standard for automated data-transfer systems. The device itself and the algorithm for working with it have been developed by order of the National Security Agency. The presence of a special "hatch" permits federal agents not only to track the direction of information flows in a data-exchange network, but also to decode encoded secret messages, gaining access to subscribers' classified information.

---

[23]Captain Vladimir Plotnikov, "The Information Phenomenon," AS, No. 5, 1996, pp. 89-91.

There is a high likelihood that this or similar developments in the software and hardware field will be offered to potential consumers in Russia or in other countries where the situation affects U.S. national interests. Certain episodes of the Persian Gulf military conflict are confirmation of this -- for example, the use of foreign information technologies in the Iraqi air defense command-and-control systems. One possible reason is the use by military equipment manufacturers of special hardware and software "inserts" prohibiting normal operation of the command-and-control system at critical moments. One need not doubt that these "inserts" were installed and activated with the sanction of the manufacturing country's national security entities.

There are two groups of electronic computer equipment manufacturers in Russia and countries of the near abroad which can be used in automated command-and-control systems being designed. The first consists of institutes and enterprises of the national economy that have great experience in joint work with the Ministry of Defense and that produce equipment using domestic technologies and materials (although modern, and above all American, high technologies also penetrate this field, as occurred, for example, in the development and production of the Baget family of computers). As a rule, their product undergoes military review and a special check, and although it satisfies requirements for use in automated command-and-control systems, it does not always have a sufficiently high technical level. Computer equipment being manufactured at these enterprises often is considerably inferior to foreign analogues in specifications and performance characteristics.

The second group consists of young manufacturing firms and computer equipment sellers developing dynamically under conditions of the evolving market

economy. As a rule, they began by trading in imported office equipment and then shifted to assembling articles from imported completing parts and to their own production. They offer modern models of personal computers, network equipment, modems, and peripherals in which foremost foreign technologies were used to create them. The endeavor to increase turnover and the struggle for new markets within the country are forcing these firms to contact the Ministry of Defense, and are making special checks of the manufactured product and its use in automated command-and-control systems possible.

The picture is less pleasing with software. Domestic general software (local and network operating systems, programs for operating with modems, and so on) is considerably inferior to foreign analogues. Special software is being developed primarily using Western program products such as C++, Clarion, Paradox, and so on. The problem is that they are not acceptable for creating tactical software. No one can guarantee the stable, faultless operation of these programs in a critical situation.

This situation emerged only recently, when automated workstations based on personal computers began to be introduced to officials' work practice. Back in the 1970s and 1980s, when YeS and SM series of domestic computers were the principal automated data-processing equipment in staffs and in other command-and-control entities, a large amount of software for automated command-and-control systems was being developed using Soviet software.

Unfortunately, the policy on procurement and use of software being followed in the Russian Federation Armed Forces is insufficiently coordinated. The situation is

exacerbated by the fact that instances of operating unlicensed copies of software of different manufacturing firms are noted in various Ministry of Defense command-and-control entities and establishments. This contradicts legislation in force and creates difficulties in "interfacing" the applied systems being developed. Various protection mechanisms are being used to prevent the illegal use of software products. Their start-up leads to operating malfunctions and irretrievable loss of information stored in computer memory.

Selection of the software to be used in creating the automated command-and-control system is one of the key points back in the system design stage, since no complex, even the most high-tech one, will be able to function stably without reliable programs. This principle is important in developing automated control systems in the logistic and technical support area, since these two spheres interwork with entities not only of military, but also civilian administration.

Thus it is advisable to carry out official procurement of programs for use in automated command-and-control systems only after preliminary marketing research and thorough testing, taking into account that S&T developments in the field of new information technologies become obsolete extremely swiftly. Software for Army and Navy needs should be developed under the strict supervision of national security entities. In addition, scientific research must be accelerated in the field of developing models and methods of monitoring the quality of software being used in military automated control systems.

INFORMATION WARFARE LESSONS FROM DESERT STORM

In the view of Russian military experts, the Persian Gulf War attracts attention not so much by the size and number of forces engaged in the combat operations, but by wide-scale employment of various types of information complexes and systems by the Multinational Forces (MNF). These were employed in the means of reconnaissance and control, in high-precision weapons, and in the forces and means of electronic warfare (EW). Thus it is no mere chance that some experts have nicknamed the Persian Gulf War a "war of technologies," which may be conditionally divided into three stages. During the first one the main efforts of the MNF were directed at disorganizing the control systems of Iraqi state and military leadership with the aim of gaining and subsequently maintaining superiority over the enemy in control of troops and weapons and, above all, in the actions of its air defense systems. The essence of the second stage of combat operations was destroying the most important defense industry installations of Iraq -- above all the nuclear and chemical weapons enterprises, as well as delivering blows against the enemy main force, defended on the possible directions of MNF combat operations. The third stage of operations was to inflict defeat on groupings of the Iraqi forces by fast-moving maneuver on flanks and from the rear, which forced the enemy to withdraw the troops from the territory of Kuwait.[24]

Among others, Admiral V.S. Pirumov has noted that the share of ground operations in the six-week war was about 100 hours. The main burden of this war fell to the air forces with the support of naval forces (during the initial period of war in

---

[24] Admiral V.S. Pirumov, et al., Problems of Regional and Global Security at the End of the 20th - Beginning of the 21st Centuries: The Armed Forces and Higher Military Education (Moscow: RF Academy of Natural Sciences, 1993), pp. 114-116

particular). He stresses that not only the superiority in control, reconnaissance, and electronic warfare systems contributed to the success of MNF operations, but primarily the punctual realization of the modern "electronic-fire" concept of fighting. This concept involved the wide-scale use of electronic means and systems of destruction, reconnaissance, and electronic warfare, closely coordinated in a general scenario of operations on the basis of a large-scale application of automated control systems.

Artificial earth satellites, strategic and tactical reconnaissance aircraft, and carrier aviation aircraft as well as ground communications and electronic reconnaissance units were widely used to conduct reconnaissance, with accuracy from 3 meters to 5 kilometers and production of data in a time close to real. The Russians also stress the use of civilian artificial satellites to increase space reconnaissance, as well as the employment of the pilotless aerial vehicle "Pioneer-1" with a complex of television and infrared reconnaissance equipment to adjust the fire.

They also note that a special feature of control was the usage of air command posts with EC-130E and EC-135 aircraft and such aircraft as E-3A AWACS, E-3C, "Orion" remote radar surveillance (RRS) and control aircraft. The large number of control and RRS aircraft has also drawn their attention. For example, the total number of E-3A aircraft was more than twenty, a feature conditioned by combat operations in which the main role was played by air forces and the U.S. military leadership's desire to ensure maximum crew practice of troop control.

The control and exchange of information among all elements of MNF control were ensured by modern automated control systems, which had made it possible to carry out the following main tasks:

-ensuring control of transporting large contingents of troops and conducting the air operation, as well as the ground and naval operations; and

-ensuring control of the material and technical supply of troops (forces).

But 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/mc 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.

UKRAINIAN VIEWS ON IW

According to Ukrainian military experts, informatization is adding new qualities to all areas of life, but at the same time the potential vulnerability of societal processes to the effects of information is increasing. Information has become a factor capable of leading to large-scale emergencies; military conflicts and defeat; and disorganization of government control, the financial system, and the operation of scientific centers. The essence of the effect of information also includes its ability to "trigger" and control matter-energy processes, the parameters of which are many orders of magnitude greater than the information itself.[25] It is correct to use the term "information weapon" because in the context of the use of information as a weapon it must be characterized by such factors as targeting; selectivity; dispersion; scale of effect; range; rate of delivery; comprehensiveness of the effect on equipment, systems, and personnel; possibility of regulating the "strength" of the effect, etc.

One can formulate the basic principle of war on an information level: the targeted complex effect on the information resources of the opponent. The latter determines the urgency of developing a methodology for automating the solution of problems regarding control of troops and weapons based on a comprehensive use of the properties of information both in the interests of increasing the validity of an evaluation of the situation and with the goal of affecting the behavior of the opponent. This methodology should be based on current advances in cybernetics, which considers information to be communication in any goal-oriented system that determines its integrity, stability, and level of function.

---

[25] A.A. Ros and V.L. Petrov, "The Information War: Its Essence and Basic Concepts," Nauka i oborona, No. 2, 1994, pp. 15-20.

The object of the information war is the information resources of one's own side and the opposing side. Intrinsic to the information war are the following basic common laws: the use of common, objectively existing physical fields for informational assurance of the operation of weapons systems, weapons, and equipment; common frequency, spatial, and temporal resources; common laws and rules at the basis of the construction of weapons systems, military equipment, and means of processing information; and the decisive role of the human factor based on the military use of weapons systems, weapons, and military equipment. The operation of the control systems of opposing groups has the following tendencies: expansion of the inventory and volume of individual physical fields used to ensure the functioning of weapons systems, weapons, and military equipment; increasing the depth of information contact of control systems and reducing the time to conduct all basic operations for the acquisition, analysis, and distribution of information; a decrease in free regions of the frequency range and an increase in its energy load; simultaneous use of a large number of functionally united systems using various physical principles; and a complex of various systems and tools according to one plan in a single control system.

The goal of an information war is to achieve an advantage in solving the problems facing one side by achieving a superiority over the opposing side on an information level. In this context the information war is manifested in two basic ways: the battle for reliable information, and the fight to affect the information representation of the opposing side. The goal of the information war may be achieved by complex solutions by each of the opposing sides to the following interconnected problems: targeted acquisition of reliable information about the state and activity of its own objects and the objects of the opponent with strict requirements for quality, volume,

completeness, and rate of updating; targeted and comprehensive effect on the information resources of the opponent at all phases of its production, dissemination, and use; and protection of one's own information resources from the effects of the opponent at all phases of its reproduction.

Thus, the interaction of the control systems of opposing sides has the distinct character of conflict on the information level, which is expressed in the combat for reliable information and in thrusting the desired information representation on the opponent -- the essence of the information war. An advantage in the information war is the decisive factor in the positive outcome of operations and military actions. It may be provided by a more complete automation of all devices of the information war based on increasing the level of "intellectualization" of analysis of the situation and reducing the time required to make information decisions.

Ukrainian experts also note that many nations are continuing to improve their armed forces by conducting an energetic search for new means of armed struggle, including in the information sphere, which could become the main feature of wars in the 21st century.[26] One could describe an approximate scenario for such a war even today. A modern-day "Babylon" (possibly Baghdad, Teheran, or Tripoli) secretly deploys its troops and suddenly attacks a U.S. ally (Saudi Arabia, Egypt, or Israel). The United States, not having an opportunity to shift its troops and ships to that region, launches an information war against the aggressor to protect its strategic ally.

---

[26] Oleksandr Manachynskyy, "Information Warfare: Myth and Reality," Narodna armiya, 1 February 1996, pp. 3-4.

First of all, they activate the computer viruses and logic bombs that were secretly placed ahead of time in the memory of the computers that are used in all structures of state, military, and economic administration of the aggressor country. This weapon is launched by the use of a special command, for example, from a satellite or through international computer networks.

After the start of the conflict, intelligence agents operating on the territory of the aggressor country, with the assistance of powerful, portable generators of electromagnetic pulses, ruin software and destroy databases in the systems of civil and military administration that are protected against computer viruses and logic bombs. The accounts of the aggressor in foreign banks are simultaneously "zeroed out" on international telecommunications networks. These actions have catastrophic consequences for the aggressor, since they completely disorganize the operations of all of the systems vitally important for the country (civil and military administration), communications, power engineering, transport, etc.

Television and radio transmitters, relay stations, and command, control, and communications centers on the country's territory are simultaneously suppressed. Materials aimed at destabilizing the political climate, disorienting the population, and instilling panic begin to be broadcast on the electronic mass media. A collapse of the economy begins and occurs in the aggressor country as a result of this combined attack using various types of information warfare, and the socio-political situation is radically altered. The aggressor is forced to reject his plans and submit to the demands of the United States and its allies under these conditions.

The considerable achievements of the last decade in the field of computer, information, and telecommunications technologies have made the world vulnerable to a new weapon that is possibly more dangerous than nuclear weapons. It is becoming obvious that information warfare is not the virtual reality of computer games, but rather an entirely tangible instrument for achieving an advantage in a military or political conflict. There is no doubt that information weaponry is becoming a highly important part of the military and military-propaganda potential of the United States and its allies under contemporary conditions. Testifying to this is the fact that whereas in 1980 approximately one billion dollars were spent on the acquisition of information technologies, more than 21 billion dollars were spent in 1994. The acquisition of information technologies has moreover moved into first place among U.S. weapons programs in financing, considerably outstripping even the space and nuclear-missile programs.

Information warfare is a means of destroying, distorting, or stealing bodies of information, extracting essential information from them after overcoming defensive systems, limiting or barring access to it for legitimate users, and disorganizing the operations of technical networks, computer systems, and all of the highly technological support for the life of society and the functioning of the state.

"American experts" cite the following means of exerting information influence:

- computer viruses, able to multiply themselves, attach themselves to programs, jam communications lines and networks with the transmission of data, and penetrate electronic telephone exchanges and command-and-control systems to disable them.

- logic bombs are introduced ahead of time into information-control centers of the military and civilian infrastructure and are activated on a signal or at an appointed time, destroying the operation of software and hardware. One variety of these bombs -- a "Trojan horse" -- is a program that makes it possible to gain concealed, unsanctioned access to the information resources of an enemy to extract intelligence information;

- means of suppressing the exchange of information in telecommunications networks, falsifying it, and transmitting required information (from the standpoint of the opposing side) on the channels of state and military command and control, as well as on the mass media; and

- means or methods that make it possible to introduce computer viruses and logic bombs into state and corporate information networks and systems and controlling them from a distance (from the introduction of microprocessors and other components into electronic equipment to the creation of international information networks and systems such as are operated by NATO and the United States).

Targets that should be assured of uninterrupted operability or functionality in real time are the most vulnerable to these means. The likelihood of the restoration of automated early-warning complexes of ABM systems and other systems of strategic significance is quite low, in the estimation of "foreign specialists," and the results of deliberate interference in their operation could be of a catastrophic nature and comparable to the possible damages caused by the use of nuclear weapons.

The United States is consistently and energetically preparing to wage information warfare. Various types of information weapons have moreover been tried out in all of the armed conflicts in which the United States has taken part (Desert Storm, the operation in Haiti, etc.) The CIA has already developed two classified programs: the first has received the name "chipping" technology, and envisages that all chips that

could be used in the creation of weapons and military hardware of other nations should contain logic bombs and viruses that could easily be initiated at a required moment. The second is testing methods of influencing programmers who are working at firms that support military orders to enlist their participation in programs to introduce viruses into support programs.

The "military leadership of the United States" thus considers it expedient that future military operations reject the use of weaponry that causes large human losses, ruins industrial enterprises and the infrastructure, and destroys the ecology. The qualitatively new weapons should, in the opinion of the Americans, be used not so much for waging traditional military operations as for depriving an enemy of the opportunity of active support, which should be achieved through "surgical strikes" by PGMs and the mass application of information weapons, which are able to paralyze the actions of state and military structures. The conduct of ground operations should be minimal therein, or not take place at all. Some "American specialists" regard information warfare as the "new Armageddon." Others feel that information weapons may be interpreted as an "electronic Pearl Harbor."

The use of the latest means of influencing the information sphere and of the high-precision destructive properties of PGMs are becoming a very important strategic factor of the military-political leadership of the United States, which assigns paramount importance to it today. The continuous work in the realm of creating information weaponry testifies to this. The appearance of new high-precision weaponry defines the necessity of creating suitable means of counteraction. The discussion should concern more than technologies for detecting the influence of information weapons alone. The

continuous improvement and development of software and technical methods for preventing the loss, destruction, distortion, or capture of information, including ruling out nonsanctioned access to it, and cryptographic means of protecting information when it is being transferred on communications channels also must be envisaged.

The mathematical product and program support of systems that are being imported must be analyzed. This sometimes requires the work of several specialists. That is why the solution to this problem requires a combination of the efforts of the Ministry of Defense, Security Service of Ukraine, and the Ministry of Communications. That combination is also needed because people with all of their weaknesses are working with the communications systems, and the security technology itself cannot secure it. The intelligence services should be mandatory participants in agreements in the supply of imported communications systems for the bodies of state power and administration. Program and technical methods could thus possibly counter the influence of information warfare directly. These methods should be supplemented with methods of counter-control of information weaponry, as well as various legal and organizational economic measures aimed at protecting state information resources.

An intensification of the development of Ukrainian information weapons as an inalienable part of weaponry and military hardware is essential right now. The security of the state requires the equivalent correlation of the forces of information warfare. It should be taken into account at the same time that the likelihood of disinformation regarding the quality and options for the employment of information weaponry is considerable. Owing to the fact that information on a war today comes from the mass media, a large portion of the material on it is generally classified. That is why the

multifaceted assessment of information that we have regarding information warfare is essential, since one could assert that information warfare is not declared and never stops, and knows no limits in space and time.

III. NEW C⁴ISR SYSTEMS AND CONCEPTS

SOVIET VIEWS ON ADVANCED C³I SYSTEMS

According to the Soviets, the new RMA dictated a re-examination of Soviet C³I 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.[27]

The Soviet military repeatedly stressed that information technologies have become one of the main criteria for the modernity of armed forces.[28] 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.

---

[27] For example, see Kochetkov and Sergeyev, "Artificial Intelligence."

[28] For example, see Lieutenant Colonel Yu. Ryabov, "The Development of Troop Command-and-Control Systems," Voyennyi vestnik (hereafter cited as VV), No. 10, 1991, pp. 47-49

The struggle is bloodless at first glance, primarily in the spheres of equipping troops with technical C³I 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 Soviet experts, the first results of the utilization of field automated command-and-control systems (PASUV) in the Soviet Army permitted them to discover a large number of their advantages. Experience was accumulated and the directions of future improvements of field automated command-and-control systems were studied during the course of several years in division-sized and smaller units and during the training of academy students. But this experience also revealed the shortcomings that prevented PASUV from successfully operating as a genuinely automated command-and-control system.

First of all, experience indicated that the types of combat documents developed for use in PASUV turned out to be divorced from the practice of the troops. Second, the capabilities of PASUV's computer system and its information and mathematical software clearly lagged behind personal computers, all the more so when connected in a network. For example, the computer system solved only one calculation task and was based on obsolete data (technical specifications of vehicles, weapons, etc.) and had not been adapted to the new arbitrary tactical symbols or to changes in the approved organizational structure, etc. Third, the algorithms of combat operations and the duties of officials at automated work stations needed finishing touches and refinement. They were primarily intended for professional military men who, of course, are computer-

literate but who are not narrow electronic computer specialists. Fourth, the problem of combining the advantages of the conversational (direct interaction with the computer and a satisfactory reaction time) and batch modes (lock-out utilization of computer resources and relatively cheap mathematical software) had not been resolved in PASUV. Personal computers have these qualities. Experts thus concluded that the Soviets needed to immediately begin to develop new programs that provide increased efficiency and quality of information processing.

Soviet commentary also stressed the role of automated C^{2}I systems in facilitating the MNF's immediate seizure of air superiority in Desert Storm. As combat multipliers, these systems were said to have negated the Iraqi quantitative superiority in tanks, and radically shifted the correlation of forces in favor of the coalition.[29] Soviet military scientists noted that air-ground coordination and deconfliction reflected an advanced C^2 system on the part of the coalition.[30]

Writing in Military Thought, General-Major Lebedev and General-Lieutenant Lyutov noted that the MNF command successfully put into practice modern principles of organizing command and control according to which mobility and survivability of command-and-control systems must be no lower than for combat units. This was achieved by comprehensive use of command-and-control facilities with different forms of basing: fixed and mobile ground, airborne, and shipboard; and by using all kinds of

---

[29] For example, see Gorbachev, "Tanks "

[30] For example, see Interview with Colonel-General Ye. Shaposhnikov, "In the Sky Over Iraq," KZ, 26 January 1991.

communications, primarily satellite (as being most stable and essentially global and prompt) in combination with electronic warfare. The allies also took advantage of capabilities of national command- and-control systems, in particular using not only military communications systems, but also commercial ones for directing the troops. For example, commercial communications channels were put to use via Intelsat-5 to support operation of the automated telephone communications system at the JCS-U.S. Armed Forces Saudi Arabia level.[31]

The Soviets concluded that the war showed the changing ratio in accomplishment of combat missions between attack systems and weapons (such as tanks, artillery, combat aircraft, helicopters, and missiles) on the one hand and tactical command-and-control and information support systems on the other. The MNF victory was won not only because of a quantitative and qualitative advantage in weapons, but also because of the overwhelming superiority in combat and information support systems as well as in logistics.

Conversely, military analysts noted that disruption of Iraqi C^2 negated its advantage in armor -- the decisive element in deep operations of the past.[32] According to General-Major A.N. Bazhenov, the new concept of "information warfare" thus means that C^3 and information are becoming one of the most important elements of

---

[31] Lebedev, et al., "Gulf War."

[32] For example, see D. Bel'skiy, "Is Everything According to Plan?" Sovetskaya Rossiya, 22 January 1991.

combat strength.[33] Indeed the Gulf War is said to have demonstrated that automated C^3I systems are equally as important as "the entire correlation of forces and means."[34] As a result, the Soviet military began to call for a total centralization of fire destruction not only at the front and army levels, but also at the level of TVDs.

RUSSIAN VIEWS ON ADVANCED C^3I SYSTEMS

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.[35] 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

---

[33] Bazhenov, Presentation, May 1991.

[34] Colonel-General A V. Kovtunov, "Improving Troop C^2 Systems in a TVD," VM, No. 4, 1991, pp. 25-33.

[35] For example, see Colonel-General A.P. Yelkin and Colonel A I. Starikov, "On the Question of Intelligent Command-and-Control Systems," VM, No. 1, 1992, pp. 35-39

enormous volume of various data in extremely limited time periods exceeding the capabilities of existing command-and-control systems.

Realizing full well that information warfare assumes "decisive importance" under present conditions, the U.S. and NATO leadership is said to be conducting detailed studies and taking practical steps to create intelligent command-and-control systems at various levels capable of real-time problem-solving. The attempt to improve the effectiveness of combat employment of forces and weapons is connected with studies conducted along the line of automating the command-and-control process, shifting human functions to technical equipment, and replacing heuristic methods of decision-making with formalized ones. Some success has been achieved here -- automated command-and-control systems have received recognition and have become a necessary element of the command-and-control process. But the main burden of making responsible decisions under conditions of a time deficit and information shortage and often with the contradictory nature of information continues to be placed on man. His capabilities are not always realistically taken into account here.

According to Russian experts, this dictates the need to develop technical equipment which is capable of intensifying intellectual abilities and realizing scientifically substantiated methods of organization; in other words, intelligent command-and-control systems. This is not a question of intelligent information retrieval systems or expert systems, which have become widespread of late, but of systems simulating the activity of command personnel. An intelligent command-and-control system duplicates man, as it were, but at the highest level of all his abilities -- methods, information, operational. Of course, such an interpretation does not signify

replacement of a human commander by a robot, since only his place and role in the command-and-control loop changes. On the one hand, the machine realizes his will and aspirations and, on the other hand, at any moment he can "overpower" it and take control.

In contrast to automated command-and-control systems, which fulfill only the simplest command-and-control operations (collecting, processing and displaying data, performing auxiliary operational calculations), intelligent command-and-control systems also perform man's basic creative function for him -- they make a decision for conditions at hand. The assignment of such a task is fully realistic, but its practical realization depends above all on capabilities of the computer. To evaluate productivity of hardware systems for processing symbolic data which carry out logical operations, a unit of measurement has been introduced known as the LIPS (logical inferences per second), which corresponds to the execution of 100-1,000 commands of modern (von Neumann) computers. According to data of "American researchers," creating an automated command-and-control system for U.S. Army transportation assets requires a 7,000 LIPS processing rate, and a battle management system requires 12,000 LIPS. Modern computers are incapable of solving such problems in a real-time mode because of capacity.

The next factor hampering creation of highly efficient systems for command and control of forces and weapons is an adequate description of real combat operations. In addition to automated command-and-control system functions, the intelligent command-and-control system must possess the ability to solve non-formalized problems of conducting combat operations with consideration of all rules of

operational-tactical art and of conditions and dynamics of combat operations. A high level of software development is a characteristic feature of automated systems oriented toward supporting decision-making on complex problems that are non-formalized to one degree or another. There are also effective methods for representing informal procedures in intelligent systems, such as based on the production method. In the Russian view, a more important factor should be noted: in developing intelligent systems, specialized hardware is being used more and more often which realizes their basic functions to one degree or another. A transition to hardware implementation of processes permits the following: substantially increasing the data-processing rate and effectiveness of displaying in memory the data being processed, which allows moving to a qualitatively new level of problem-solving such as development of systems for making decisions in real time: it permits simplifying system software.

Interest in studies in the area of hardware implementation of intelligent systems is said to have emerged after 1982, when Japan came out with a ten-year research program on fifth-generation computers. A similar project in the United States was basically oriented toward developing new weapon systems and was called the "Strategic Computer Initiative." The principal indicator of quality of developments in the sphere of hardware functions of intelligent systems is an increase in machine productivity by 3-5 orders of magnitude and taking it to a hundred billion commands per second.

According to Russian experts, choosing an appropriate element base and the standard devices and modules used is one of the basic problems of building the hardware of high-capacity control systems. The next one is hardware implementation

of processes in the intelligent command-and-control system by creating real physical mockups. As the basis for building universal bread-boarding media simulating processes in the intelligent command-and-control system and possessing necessary properties, a base module (element) has been given the name "transputer." It represents very large-scale integration which realizes the functions of a von Neumann microprocessor with developed communications equipment. Several types of transputers have been developed. Diverse bread-boarding media can be built on their basis by connecting the communications equipment included in them. For example, homogeneous control structures simulating behavioral acts by using results of neurophysiological and neurocybernetic command-and-control systems and their hardware permit creating a system of adaptive control of moving objects functioning in a real environment with various local obstacles. The solution to such a problem takes ten-thousandths of a second.

As already noted, artificial intelligence systems must reproduce natural intelligence functions. By using equipment reproducing the solution to problems of a behavioral nature, it is possible to have successively increasing complexity of control structures leading to an expansion in their functional capabilities. By taking into account principles of the structure (organization) of natural intelligence and a reflex approach to describing the process of functioning, it is possible to create intelligent, multilevel, hierarchic command-and-control systems based on homogenous structures. The problem area is simulated in them by hardware located at their lower levels, and structures situated higher are used for obtaining (or rather, representing) optimal command-and-control decisions. Such an intelligent system essentially is a digital computer, whose neuro-like network performs functions not only of a displaying

structure, but also of afferent synthesis and the making and implementation of decisions. It can be used for solving a very wide range of problems (including aboard aircraft). The most obvious ones are preventing mid-air collisions of aircraft; guiding to a target (single or group); landing in IFR weather; determining the moment personnel and equipment are moved up to an initial zone for an enemy's head-on attack; supporting the landing of groups of aircraft after their combat employment; evaluating capabilities of friendly forces as well as of joint employment of different combat arms in major operations; ensuring defense of individual regions; and creating systems to control drones and simulators for forecasting the effectiveness of measures to conduct combat operations under various conditions and for rehearsing operational command-and-control skills.

An analysis of the Gulf War is said to demonstrate that some of the aforementioned problems have been successfully solved by American specialists within the scope of the Strategic Computer Initiative. Thanks 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 efficiency and 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, multivariant 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.

Admiral Pirumov has noted that in regard to command and control, too few writings are devoted to questions connected with the mass employment of weapons, in which there is an integration of both command-and-control systems and fire-control systems (based on wide use of computer technology) into a unified automated system for command and control of mixed forces and different types of weapons systems. Mutually coordinated (horizontally and vertically) use of automated command-and-control systems supporting mass missile and bomb strikes by air-, sea-, and ground-based platforms against Iraqi state and military installations, as well as the movement and logistic support of forces, serves as an example of this. The automated command-and-control system was deployed on the basis of a unified, automated digital communications system, a great portion of which (60 percent) was made up of space equipment. The number of communications stations deployed in the theater (over 500,

of which only four were fixed) indicates the scope of their use. Not only staffs, but also every line or artillery battalion, strategic bomber, reconnaissance aircraft, and combatant ship were end subscribers of space communications.[36]

According to Pirumov, a significant place was set aside for airborne command posts in the system of MNF command-and-control entities. For example, there were over 20 E-3A AWACS early-warning and control aircraft alone, which was dictated not only by specifics of the armed conflict -- the principal role in which was played by aircraft -- but also by the U.S. military leadership's desire to give combat practice to the maximum number of airborne command post teams and their aircraft crews. An appreciable contribution to the effectiveness of artillery fire was made by the NAVSTAR space radio-navigation system, which provided data with an accuracy of from 1 to 3 m.

In short, command-and-control systems have an enormous impact on the effectiveness of operations by force groupings. Underestimating this impact can lead to an incorrect assessment of the combat capabilities of the opposing sides. For example, without having examined these questions in detail, it is difficult to determine which force grouping is stronger: that with lesser capabilities of attack (conventional) weapons and a good (automated) command-and-control system or vice versa. But there is no doubt that introducing new information technologies to MNF battle management practice permitted considerably increasing their combat potential (by at least two-fold).

---

[36] Pirumov, "Parity."

Russian experts have also noted that in recent decades the integration of reconnaissance assets, weapons, ECM assets, and command-and-control equipment at the formation and large strategic formation levels became a fundamentally new direction in developing command-and-control systems at the tactical level. Its essence consists in the direct interface of reconnaissance, target designation, and decision-making systems with automated fire control systems. Operator involvement in decision-making for immediate use of weapons thereby is limited.

But the experience of establishing and using the WWMCCS is said to indicate that at the present stage of military art, as a result of the large spatial scope of military operations, it is necessary to develop a world-wide military command-and-control system for their successful conduct. Data sensors and communications systems supporting the real-time arrival of data from any point in the world are of special importance for effective functioning of a modern operational command-and-control system. Indeed it was the work of these components of WWMCCS that successfully repelled Iraqi operational-tactical missile strikes during the Gulf War.[37]

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

[37] For example, see Colonel B.G. Putilin, "The U.S. World-Wide Military Command-and-Control System," VM, No. 11, 1992, pp. 65-70.

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.

Modern enemy means of reconnaissance "remove" information not only by getting a fix, by intercept, and by connection to information channels, but also by penetration into electronic data-processing systems of the automated command-and-control system and other command-and-control equipment. At the present time approximately 60-70 percent of intelligence is collected by the enemy by means of SIGINT.[38]

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

---

[38] Lieutenant Colonel B.V. Fefelov, "Information Support of the Command-and-Control System," VM, No. 1, 1993, pp. 36-39.

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.

Russian general officers note that in connection with cuts in the Russian Federation Armed Forces, requirements for qualitative indicators characterizing troop combat readiness have been rising. In these conditions the role of command and control increases considerably. The desire to have first-class armaments, military hardware, and well-trained personnel may be weakened owing to the low level of command and control, which will make it impossible to use combat capabilities to advantage. This is why the improvement of the command-and-control system of troops is one of the priority areas in the organization of the Armed Forces. The theory of command and control of troops and, particularly, the methodology of assessing its effectiveness, which require continuous development, have an important role to play in the efforts to resolve this problem.[39]

[39] General-Major O.V. Sosyura and General-Major V.P. Pyatkov, "Theoretical Fundamentals of Assessing the Effectiveness of Command and Control of Troops," VM, No. 11, 1993, pp. 31-39.

These experts note the need to expand the term "theory of the command and control of troops." In their view, the current definition reflects three substantive elements. First, the theory of the command and control of troops is an independent part of military science with its own scientific objectives, not an appendix to operational art (unfortunately, they say, this misconception is still held by some specialists). Second, it is essential to reflect the role of methods of measuring the effectiveness of the command and control of troops (MOEs), without which the command-and-control theory is reduced to a groundless discipline unable to give any substantial assistance to the armed forces. Third, the command-and-control theory exists in order to improve the command and control of troops. This is why it should be understood as an independent part of military science, the main objective of which is to study and to measure the effectiveness of systems, forms, and methods of the command and control of troops.

It is therefore necessary to resolve the following questions: What is meant by the command and control of troops; what are its purposes, essence, and content? What is meant by the command-and-control system, what is it made of? What are the laws and principles of command and control? What are the main requirements established for the command and control of troops and what is their essence? What is meant by the term "effectiveness of troop command and control," and what are its MOEs?

At present, a certain degree of unanimity of views can be seen only with regard to the content of the command and control of troops, which includes the degree of troop combat effectiveness and their continuous combat readiness to gain a clear understanding of an operational mission; to gather and to analyze data on the current

situation; to make a decision regarding an operation; to assign missions to the troops; to organize coordination, comprehensive support, and command and control; to plan combat operations; to organize control over carrying out orders given and providing assistance to troops, etc. As for other terms, they differ substantially from each other (see Figure 3).

Among others, Generals Sosyura and Pyatkov believe that matters pertaining to the content of command and control should be separated from the term "command and control of troops," namely: the gathering and processing of information; the maintenance of troop combat readiness; and the acquisition and analysis of data on the situation, making decisions on it, and conveying decisions made to executing entities. Aside from this, in determining the objective of command and control it should be noted that it is by no means irrelevant at what cost the troops perform combat missions assigned to them (here it would be apt to recall the term "Pyrrhic victory").

Experience has shown that for the purpose of analyzing the effectiveness of command-and-control systems, they can be conveniently represented as a set of echelons, levels, axes, and lines of command and control. In addition, within them various subsystems can be singled out. For instance, a front's command-and-control system of troops may include: the front command-and-control echelon, including the front's command post, alternate command post, and rear services command-and-control facilities; similar army and division command-and-control echelons; and the army command-and-control level, including all army command-and-control echelons and those equated with them. A set of agencies that exercise the command and control of a specific strategic or operational formation or unit from top to bottom makes up a

Terms of the Theory of Command and Control of Troops

Sources	Command and Control of Troops	Objective of Command and Control	Essence of Command and Control	Command and Control System
Military thought, 1992, No 10, pp. 48-50	Purposeful, uninterrupted influence by officers and command and control elements on command objects by gathering, processing, and transmitting information inherent in the process	Main and definitive objective of command and control is to organize and to ensure the effective performance by troops of missions assigned to them in established periods of time and with the minimum losses	–	–
Military thought, 1992, No 12, p. 28.	Purposeful activity by commanders and command and control elements subordinated to them in order to maintain combat readiness of troops, to prepare operations (combat activities) and to organize the performance by troops of missions assigned to them	–	–	A set of functionally interconnected command and control elements, posts, and technical means
Voyennaya mysl, 1971, No 1, p. 90	–	–	Boils down to the utilization of the available combat potential of men and equipment in the specific conditions of a given situation for the purpose of achieving combat or operational objectives	–
Ivanov, Savelyev, Shemanskiy, Osnovy upravleniya voyskami v boyu, Moscow, Voyenizdat, 1977, p 23	Reasonable activity by a commander, a staff, and other command and control elements in order to prepare combat operations and to channel the troops' efforts into the successful performance of a combat mission during combat by obtaining and studying data on the situation, decisionmaking on it, and conveying missions to those who will perform them	–	–	–
Osnovy teorii upravleniya voyskami, Moscow, Voyenizdat, 1984, pp. 55, 68.	–	The main purpose of command and control is to achieve the maximum effectiveness of the use of subordinate troops in order to perform missions assigned for an operation (combat)	The essence of command and control is the activity of commanders (chiefs), political and other command and control elements aimed at achieving combat readiness and combat effectiveness of troops, preparing operations and combat activities, and exercising command and control over them while performing combat missions	A set of functionally interconnected command and control elements, command posts, command and control systems and automated equipment, and also special systems ensuring the collection, processing, and transmission of data
Textbook by the Higher General Staff Academy, 1992, pp 9-31.	–	Objectives of command and control that pertain to its essence are to ensure the effective utilization of the troops' combat capabilities and the successful performance of missions assigned to them in any conditions	The essence of command and control is the purposeful activity by commanders-in-chief (commanders, chiefs) and other command and control agencies aimed at maintaining the troops' combat readiness, preparing operations (combat activities) and organizing the performance of missions assigned to them in operations	A set of functionally interconnected command and control elements, command posts and command and control equipment

FIGURE 3

command-and-control axis, including various lines (command or combat; alternate command, combat, or rear services command-and-control lines; and so forth). A number of contiguous command-and-control levels may make up compound echelons, such as front-army or front-army-division. Finally, a communications subsystem, a command-and-control subsystem for the Missile Forces and Artillery, the Air Force, the Air Defense Troops, etc.

For the purpose of making a detailed measurement of the effectiveness 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.

According to General-Major N.A. Kostin, the introduction over the recent 15-20 years of new information systems and facilities in combat activities of troops has improved the quality of weapons, control, and reconnaissance, and has made it possible to considerably upgrade the combat potential of troops without increasing their numerical strength. Importantly, one of the crucial factors in achieving success in present-day operations consists in ensuring superiority in controlling troops and weapons. The struggle to seize and hold this superiority is going to assume the

toughest and most resolute forms and become an inalienable part of military operations. Hence the confrontation in the sphere of command and control at the present time is the most important component of an operation of any scale.[40]

The most promising and economic way to solve this problem is to raise the efficiency of disrupting enemy control of troops and weapons in operations. This is linked directly with the development of forces and means of fire destruction and electronic countermeasures (ECM), and with the improvement of methods of their employment in combat. A more complex nature and a wider spatial scope of modern operations, the increased mobility of troops, and the pervasive introduction of information systems in their practical activities sharply enhance the importance of disrupting command and control of enemy troops and weapons in operations.

One more regularity should be pointed out -- a great dependence of the effectiveness of disrupting enemy command and control on which side has gained air supremacy. The supremacy cuts back considerably on efforts involved in the disruption objectives. The disruption of command and control of the enemy's air force results in increased advantages for the friendly air force. It is therefore a good idea to deliver strikes, as fast as possible, directly at the aviation grouping. The mission consists in that one should capitalize on the sharp decline in the combat capability of the enemy's aviation owing to the disruption of its command and control, and to at least not waste the achieved equilibrium if not to gain supremacy in the air. Unless this has been done,

---

[40]General-Major N.A. Kostin, "Appraising the Effectiveness of Troops (Forces) and Weapons Control Disorganization," VM, No. 11, 1993, pp. 39-44.

the correlation of forces will return to the initial state some time after the command-and-control systems have been restored, and the supremacy would be on the side of the enemy. Thus it pays to try to disorganize the enemy's air force command and control even if the enemy holds supremacy in the air. Capitalizing on the results achieved, one should consolidate the gained balance of forces. A purposeful and active disruption of the enemy's air force is a shortcut to success in trying to achieve supremacy in the air even if the initial correlation of forces is unfavorable.

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.[41]

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.

---

[41] General-Major V.A. Denisenko, Colonel Ye.I. Suborin, and Major P.S. Romanov, "Intellectual Command-and-Control Systems of Integrated Reconnaissance-Strike Systems of the Ground Forces," VM, No. 1, 1995, pp. 54-59.

In the Russian view, a higher combat efficiency of IRSS can be achieved if the following problems are resolved.

First, the identification of targets according to information transmitted by various reconnaissance means with the requisite trustworthiness, accuracy, and promptness (target identification is defined as an automated process of searching for, discriminating, and describing targets on the basis of real data). The main reconnaissance means of the IRSS is an aircraft radar, so target identification completely depends on its resolution, which in combination with available radar systems of high-precision missile guidance clearly does not contribute to a rational -- to say nothing of effective -- solution to the problem under consideration. In order to receive integrated high-quality information on targets it is necessary to use various types of reconnaissance functionally united into an integrated reconnaissance system of an IRSS. In real time, this can only be done by using an intellectual command-and-control system. A definitive solution to the problem, however (along with the creation of an ICCS), hinges on equipping the high-precision missile with a target identification system. At the same time, the missile must operate on the basis of information coming from on-board reconnaissance means operating in various ranges of electromagnetic radiation (infrared, visible, and radio) and integrated in information and navigation channels. This system should be an integral part of an intellectual guidance system (IGS) of a high-precision missile.

Second, a drastic reduction in the time of preparation and launch of high-precision missiles, particularly right from the march in an unprepared area. This problem has been caused by an increasing percentage of highly maneuverable targets.

Research has shown that this trend will continue in the future, but the time they spend in positions will be decreasing. Therefore the priority objectives are the optimization of the process of a missile's technical preparation and an "analytical" display of on-board equipment (topographic and geodetic linkage of the starting position and the spatial orientation of missiles before launch). This problem can be resolved in an effective fashion only by using an IGS.

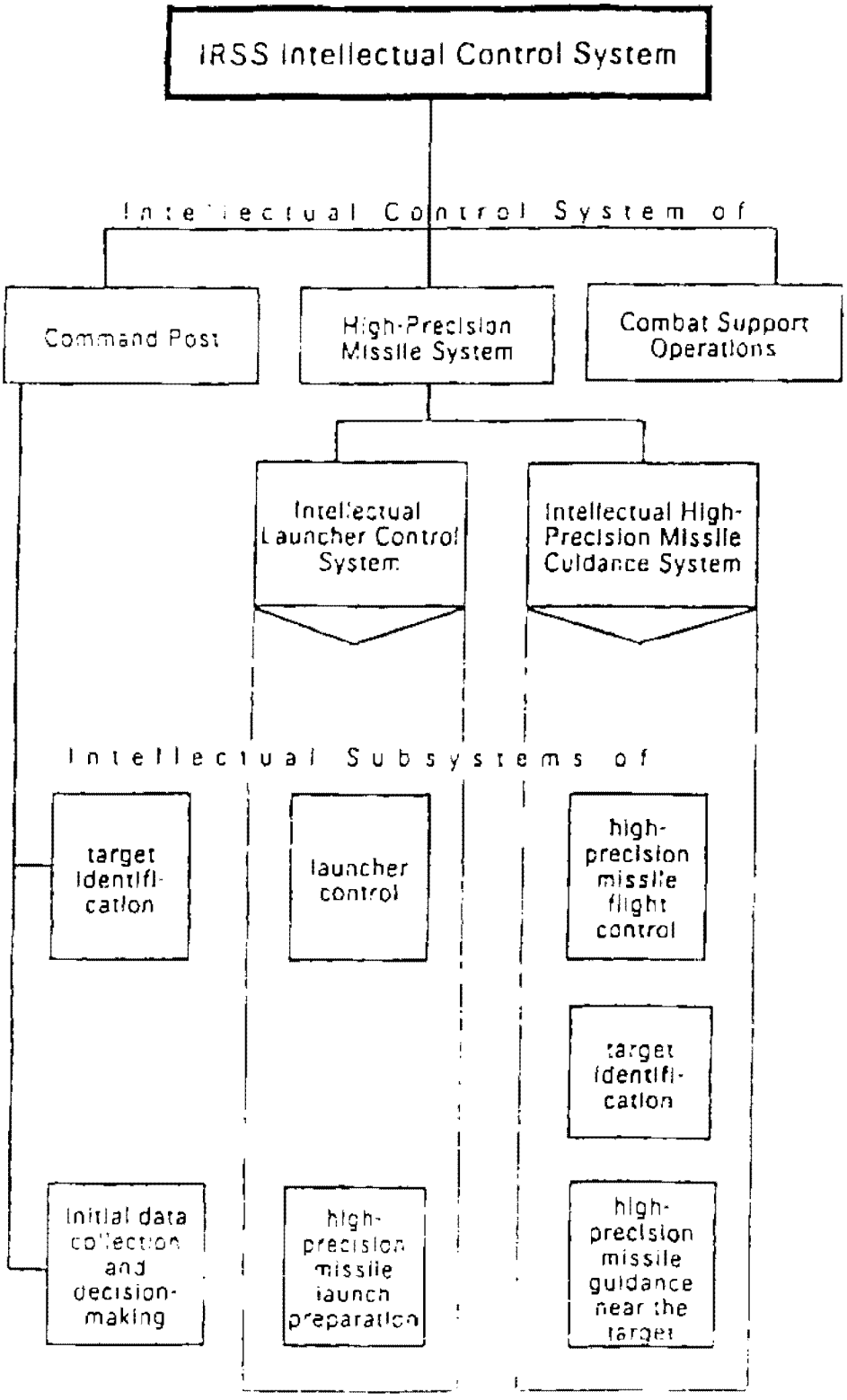
Third, ensuring that the high-precision missile's intellectual control system makes decisions on selecting the optimum conditions for destroying a target. This problem entails the selection of the optimum trajectory depending on changing flight conditions; the penetration of the enemy's air defense system by using energetic anti-missile maneuvers based on information about actions of enemy anti-missile systems received by on-board radars; target identification; the retargeting of the missile (if necessary) with external and/or self-correction; and control over the height at which the multiple warhead opens and its elements are scattered according to a distribution law and depending on the type and configuration of the target. The above list of specific missions can be appended or amended if more specific research is conducted, but the IGS will continue to play the key role.

Solutions to this set of problems can be provided by the development and creation of an IRS intellectual control system. Intellectual systems (IS) are defined as systems simulating human activity at the highest peak of human abilities (methodical, information, operational) and designed to fulfill practical missions that are called intellectual if performed by humans. One such mission is decision-making in current conditions. It follows from this definition that an ICS is an intellectual system designed

to fulfill the missions of commanding and controlling troops and weapons in real time, some systems of which may function without human intervention (autonomously); while an IGS is an intellectual system functioning autonomously and designed to select operational aims, to shape the process, and to program the desirable -- from the point of view of these aims -- behavior of guided systems.

An intellectual control system of an IRSS can be, first, a unit of the relevant commander's ICS integrating ICSs of combat branches, formations, and force elements participating in combat operations; second, it should ensure an effective fulfillment of missions assigned to an IRSS by optimizing the process of its functioning (see Figure 4). It should be noted that an ICS of a high-precision missile (HPMS) consists of two interrelated parts: an intellectual launcher control system (ILCS) and an intellectual guidance system of the high-precision missile; while the former is the land-based part of the HPMS ICS, the latter is located on board the missile. At the same time, the high-precision missile's IGS is a more important part of the HPMS ICS and the IRSS ICS as a whole. This is attributable to the characteristic features of its functioning: an autonomous mode and the complex environment of its operation (dynamic changes, resistance on the part of the enemy, existence of obstacles, etc.).

Command Post Intellectual Control System. The main mission of the subsystem of target identification is the classification of targets in accordance with information received from various reconnaissance means. The main missions of the subsystem of initial data definition and decision-making on the preparation and delivery of a missile strike are as follows: the identification of targets, forces, and weapons subject to destruction; types and numbers of combat units armed with high-precision missiles;



Structure of IRSS Intellectual Control System (option)

FIGURE 4

target allocation; the receipt from the HPMS ICS, processing, and transfer of information on the target and the state of the launcher and missile; and control of all IRSS and IRSS ICS subsystems.

Intellectual High-Precision Missile Control System. Functionally, it consists of a number of subsystems which, depending on the state of the HPMS and the missile, fulfill a range of complex missions. Missions to be fulfilled by the missile system before launch are assigned to the launcher control subsystem. They include technical diagnostics of the launcher; calculations of the optimum mode of operation; and the adoption of the optimum plan of action with regard to movement, topographic survey, camouflage, and protection from the enemy's high-precision weapons and aviation depending on the conditions of the situation.

Missions to be fulfilled during launch preparation are performed by the high-precision missile's launch preparation subsystem. These are technical diagnostics of the missile, the "analytical" display of on-board equipment, and the formation of the optimum flight trajectory. Missions to be fulfilled in flight are performed by the high-precision missile's flight control subsystem. These include control over the missile IGS's intellectual subsystems, all on-board equipment, and the multifunctional engine unit capable of operating in various modes; and the adoption of a decision to overcome the enemy air defense system in case on-board equipment is out of order.

Missions to be fulfilled in the vicinity of a target are performed by the high-precision missile's near-target control and target identification subsystems. These include the neutralization of natural and man-made obstacles near the target; the

retargeting of high-precision missiles; control over the multiple warhead and its cluster submunitions (the height of opening the warhead and the scattering of submunitions according to a distribution law depending on the type and configuration of the target) and the orientation of the missile; and target identification taking into account external dynamics. Analysis of the above missions makes it possible to formulate verbal requirements for intellectual control systems that are set forth in Figure 5.

Therefore, 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.

According to General-Lieutenant V. Bazhenov, the organizational development of the Russian Armed Forces is based primarily on qualitative parameters. This calls for a quest for new ways to maintain the country's defense capability, one of which is

Requirements set for IRSS intellectual control systems (subsystems)

System (subsystem) name	Requirements
IRSS Intellectual Control System	General requirements for the system as a whole Inherent stability in operation, high level of protection from reconnaissance, electronic reconnaissance interference, and electronic countermeasures of the enemy. Reliability and survivability. Ability to be transported by air. Simplicity in operation, possibility quickly to assimilate techniques of operating the device, principles of personnel command and control, and to replace faulty units. Hardware implementation using highly productive control systems based on an up to date component base
Command post, HPMS, and combat support operation intellectual control systems	Requirements common for low-level ICSs Capability to operate 24 hours a day for a long period of time. High mobility. Accumulation of information received to be used in new situations. Ergonomic hardware implementation. Capacity to be used in combat operations while in motion. Operation in a regime close to real time, and also in a dialogue regime
Command post intellectual control system	Individual (specific) for systems Possibility to process information received from various reconnaissance means. Control over all IRSS and IRSS ICS subsystems. Compatibility with ICSs of other IRSSs and with ICS of senior and junior command and control echelons. Ensuring high probability of identifying targets and allocation of targets between missiles
HPMS intellectual control system Launcher ICS	Possibility to receive and process information required for launching high-precision missiles directly from the reconnaissance subsystem of the senior echelon IRSS and ICS. Compatibility with navigational and time support equipment
High-precision missile ICS	Possibility to receive data and missions directly from the CP ICS. Autonomy, compact size, operation in a real time regime. Hardware implementation as microprocessors containing requisite software. Ability reliably to maintain the nature of its relations with the external environment, to simulate collective decisionmaking on complex problems.

FIGURE 5

the use of information technology in the armed forces.[42] This implies the process of large-scale introduction and application in various spheres of the Russian military's peacetime and wartime activities of methods, means, and systems for the acquisition, transmission, collection, processing, storage, and utilization of data for decision-making. The topicality of this process was confirmed by then Defense Minister P. Grachev, who in 1994 assigned to the General Staff, the branches of the armed forces, and the Ministry of Defense main and central directorates the task of introducing automation (information technology) down to the level of large strategic formations.

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

[42] General-Lieutenant Viktor Bazhenov, "Computer Technology Being Called Up," Krasnaya zvezda, 22 April 1995, p. 4.

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.

The technical basis of the Ministry of Defense telecommunications network is provided by technical system units being developed on the basis of modern computer technology; network access units; automatic packet switch centers; internet work interface gateways that ensure the Ministry of Defense telecommunications network's joint functioning with diverse networks and sub-networks and function on the basis of other information exchange protocols; and subscriber terminals connectable to the Ministry of Defense telecommunications network that could be various items of information technology, automation, and document exchange operating as sources and recipients of information.

The development of the network's package of hardware is based on Russian-made and partly import elements. This process is making use of new technologies ensuring the development of zero-level and low-level manning hardware, which

substantially reduces costs and does not require any special preparation of premises. During the first stage (1995) it is planned to offer the telecommunications network's resources to the General Staff, individual branches of the Armed Forces, and the main military districts that resolve priority tasks in the organizational development of the Russian Federation Armed Forces.

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 general officers stress that the issue of command and control during wartime occupies an important place among the measures to develop and reform the armed forces. Neither the "Basic Provisions of the Military Doctrine of the RF" nor the new "Law on Defense" that was adopted by the State Duma in October 1995, however, has any instructions for the creation of a system of military-political and strategic leadership of the country and the armed forces in wartime. The experience of past wars confirms the urgent necessity of the advance creation and preparation of the entire system of that leadership. The Supreme High Command could become the

supreme body of strategic leadership, carrying out the overall supervision of all of the activity of the armed forces during wartime.[43]

The Russian military could also return to the experience of the creation and functioning of the Defense Council, which directed all of the country's forces and capabilities toward the attainment of victory. The composition of the Defense Council and Supreme High Command, their functional purposes and duties, and the nature of their joint actions in converting the armed forces to wartime status all need to be defined now. The main thing is to teach them in peacetime to perform those tasks, as is done in the United States and the other NATO countries today.

According to Russian experts, the Russian military has a tendency to destroy an already existing system for the command and control of the armed forces in peacetime, which could lead to the complete loss of control of the troops and risks extremely negative consequences. The functions of the Ministry of Defense and the General Staff, for instance, are divided up without any scientifically substantiated study whatsoever, with the former given administrative supervision and the latter operational control. This provides nothing but more expenses and confusion, and most importantly, the disorganization of centralized command and control. Experts stress the need to strengthen as much as possible the ties between the Ministry of Defense and the General Staff, giving them greater authority in the area of coordinating issues of

[43] General-Major Vladimir Kalennikovich Lozovoy and General-Lieutenant Viktor Vasilyevich Solovyev, "An Arch-Important State Problem -- What Kind of Armed Forces Does Contemporary Russia Need?" NVO, 27 January 1996, No. 2, p. 4.

organizational development, planning, and the preparation and employment of all other troops under wartime conditions.

Some reformers are proposing that the unified system of administrative and operational control in the branches of the Armed Forces also be split up, copying the American system of command and control. That system envisages the presence of elements on U.S. territory that are performing chiefly administrative-support functions. Their departments of the Army, Air Force, and Navy work on the development of their own branch of the armed forces, the acquisition of weaponry and military hardware, manpower acquisition, the performance of mobilization measures, etc. If one takes into account that the U.S. forces intended for waging combat operations are largely far removed from the mother country, the placement of operational functions on unified and special commands created in advance in the theaters of war can be considered entirely expedient.

The concentration of both administrative and operational functions in the hands of the high commands of branches of the Russian Armed Forces conforms to the specific features of Russia, the disposition of the armed forces therein, and the forms of strategic operations adopted, as well as to the extant traditions and experience of the prior war. This system is more economical and requires a smaller administrative apparatus than the creation of separate administrative and operational elements. All of this testifies to the necessity of preserving (at least during the transitional period) both administrative and operational command-and-control functions in the General Staff and the main staffs of the branches of the armed forces.

BRANCH-SPECIFIC C^2 SYSTEMS

Air Defense Troops. Russian miliary experts note that to combat enemy operational-tactical ballistic missiles successfully, groupings of SAM Troops in an air defense zone must have functionally interconnected command-and-control entities, a communications system, and sets of automation equipment at the division/brigade (regiment)/battalion levels as a minimum. They must have automated command-and-control systems supporting the collection, processing, and display of data on the air enemy, target distribution, target designation, and monitoring of fire mission execution.[44]

It would appear that command-and-control system capabilities can and must be expanded to the strategic or operational level, such as in the collection, processing, and transmission of missile-attack data (warning) to air defense zone CPs for placing active means of intercepting operational-tactical ballistic missiles in combat readiness. When the warning time is greater than or equal to the time the SAM Troops grouping needs for intercepting ballistic missiles, then the latter's destruction is possible. But if this condition is not observed, then intercept and destruction of the missiles are not supported.

In the absence of data on a missile attack it is necessary, first of all, for all groupings of SAM Troops capable of repelling operational-tactical ballistic missile strikes to be in a combat-ready condition in air defense areas; secondly, data on the direction of these strikes and on the installations against which they are being delivered

[44] Colonel Vladimir Sayenko, "A Counterbalance to Intimidators," AS, No. 10, 1995, pp. 23-24.

must be present in command-and-control systems. Consequently, there is a requirement for serious transformations in the structure, organization, and combat algorithms of command-and-control systems of the Missile-Space Defense Troops, SAM Troops, and Radio-Technical Troops -- or the establishment of a fundamentally new local ABM defense system in the region (in air defense areas) that combines within itself mobile missile-attack warning equipment and means of intercepting operational-tactical ballistic missiles based on existing SAM complexes.

The following are said to be necessary in air defense areas for command and control of groupings of SAM Troops used to intercept ballistic missiles:

- additional missile-attack data (warning) from higher systems for placing groupings of SAM Troops in a combat-ready condition;
- the coordinate data for selecting installations in air defense areas against which a ballistic missile strike is possible;
- trajectory data on the flight of ballistic missiles for developing target designation coordinates in command-and-control systems for combat-ready groupings of SAM Troops; and
- data on the expected direction of flight of ballistic missiles for posting sectors for final target search by radar equipment of SAM battalions (groups of battalions).

It also must be taken into account that demands on accuracy characteristics are increased because of the short ballistic-missile approach time. In essence, the air defense area command-and-control system must have functional missile-attack warning system elements (modules); i.e., it must be a prototype of a small (local) system for command and control of missile-space defense. This is especially urgent today, when

the possibility of missile strikes being delivered against ecologically dangerous point targets (atomic electric power stations, hydroelectric stations, chemical plants, and so on) is not precluded.

The conclusion is clear: as a counterbalance, it is necessary to have a minimum of forces and assets based on groupings of SAM Troops to deter a potential aggressor. Therefore a probable threat of a ballistic-missile strike against Russian Federation targets requires the peacetime establishment of a command-and-control system in air defense areas for combatting operational-tactical ballistic missiles, and in the future a system for command and control of ABM defense in the TVD. This is especially important as multiple-warhead operational-tactical missiles are coming to replace single-warhead ballistic missiles. Experts note that to create such a system the Russian military should interface command-and-control echelons at various levels, from the operational-strategic level (the central command post, where all data on ballistic-missile launches for the region is concentrated) to the tactical level (CP of a group of battalions).

After the Persian Gulf events, tests of the S-300 SAM system for intercepting ballistic missiles were held at Russian ranges. Results were reassuring: two out of four missiles fell 7-8 km from the point of aim; i.e., they were dislodged from the flight path. Thus, it is possible not only to bring fire on ballistic missiles on the descending flight path, but also dislodge them from their course to preserve the covered installation. The Russian military claims that its S-300 SAM systems can perform this mission. It is only a matter of information/command-and-control support and of the interface of command-

and-control systems of different levels or the establishment of an intermediate CP in a region (in air defense areas) for receiving data from the missile-attack warning system.

In the future attention must be given to the development of a mobile, effective ABM defense system that is capable of reliably intercepting single-warhead ballistic missiles and the reentry vehicles from them, including stopping attempts to deliver operational-tactical missile strikes against area targets ("hostage" cities and ecologically dangerous point targets). Conditions for command and control of groupings of SAM Troops become more complicated with the transition from single-warhead ballistic missiles to multiple-warhead ballistic missiles and with their increased flight speed (over 1,100-1,200 m/sec). This is connected with a reduced flight time of targets and their reduced detection range. Until an ABM defense system is established in the region (in air defense areas), the missions of intercepting warheads also can be performed by groupings of SAM Troops with a certain reduction in defense areas, an increase in the number of battalions used, and development of high-speed SAMs with a more powerful warhead.

Naval Forces. According to Vice-Admiral Yu. Kaysin, the growing importance of naval forces in the politics of the leading world powers as well as the growing importance of the Russian Navy for maintaining peace and stability, carrying out peace-making functions in various regions of the world, performing and supporting foreign policy actions, and offering help to the public when extraordinary situations arise entails some changes in the functioning of the entire system of command and control. Though such elements of command-and-control systems for naval forces as command posts, communications facilities, and automated command-and-control systems were

created on a fundamental basis and were universal, the training of staffs and advance planning were concretely oriented toward a specific scope of missions and therefore require deep analysis and rethinking at the present time.[45]

In connection with this it becomes necessary to redistribute the efforts of staffs and concentrate attention on matters of indirect training and conducting operations not only within the framework of a large-scale war, but even under conditions of an outbreak of regional conflicts or local wars as well as the implementation of certain foreign policy actions. In doing so, it is necessary to consider fundamentally new approaches to creating groups of forces in ocean and sea zones and controlling them in the course of an operational deployment. This will require additional knowledge and skills of admirals and staff officers and the consideration of not only purely military matters, but also political, economic, and social questions. It is necessary to learn how to control forces operating as part of a multinational force, including forces under the aegis of the U.N., and provide for coordination of these forces.

One of the main trends in maintaining the established level of operational readiness of the fleets is a comprehensive approach toward the training of command-and-control organs and forces, which calls for combining the necessary intensiveness of operational, combat, and mobilization training with the efficient use of forces and funds in the course of combat training. Today's conditions raise even higher the personal responsibility of leaders at all echelons for the operational readiness of the command-and-control system to carry out its intended missions, and toughen the

[45] Vice-Admiral Yu. Kaysin, "Special Features of Building the Command-and-Control System for the Fleets in the Current Stage," MS, No. 4, 1993, pp. 33-36.

requirements for a clear demarcation of the functional responsibilities of command-and-control organs at various echelons and for the professional knowledge and skills of admirals and officers in ensuring the efficient use of available forces and resources of the fleet. All of these have been and remain the main factors which determine success in carrying out assigned missions by the command-and-control organs of the fleets.

Today it can be said that the "arms race" is a thing of the past. However, the "race of command-and-control systems and logistical support systems" continues and is even picking up the tempo on the basis of new scientific and technological achievements. The improvement of such systems greatly enhances the potential strike capabilities of naval forces, which is especially important under conditions of the quantitative reduction of forces. Therefore it is very important when elaborating plans for developing the Navy to determine the priority of various projects, estimate their share in executing the entire complex of missions facing the Navy, and ensure their priority financing. In doing so, it is advisable to perform the fundamental research and development of new combat means on the basis of integration both at the level of the Russian Defense Ministry (branches of the armed forces) as well as at the level of state institutes. The financing of the command-and-control system should correspond to its contribution to the execution of defense missions.

Of vast importance in determining the numerical strength and organizational and manning structure of the staff of combined-arms formations and large formations of fleets is an expert evaluation of the quantity and content of their command-and-control activity. It is advisable not only to specify the list of missions being executed, but also to analyze information flows and data on the status of technical facilities possessed by

each subunit. One should strive for maximum unification of the structures of command-and-control organs: from the Main Staff of the Navy to the staffs of formations and units of the fleets. This will permit both reacting more flexibly to possible changes in the makeup and character of operations and ensuring better coordination.

According to Russian naval officers, electronic situation coverage occupies a special place in the series of measures for supporting the command and control of combat and other activities of naval ships. The sphere of its operation extends in space from the surface of the sea to its bottom on the one hand, and to near space on the other hand.[46]

At the present time, various guiding documents and official publications contain a certain inconsistency in the interpretation of the concept "electronic support," including the electronic situation coverage process as the initial component of this type of support. As a result, achieving uniformity of existing views is becoming an urgent task. Naval experts present the entire process of electronic situation coverage in the form of the structural diagrams that are depicted in Figures 6, 7, and 8. Based on the theoretical bases that assume the gradual nature of the resolution of each electronic situation coverage mission that is depicted in Figure 6, the algorithm reveals existing communications and dependence between the stages examined and displays a definite symmetry in the dynamics of its implementation.

[46] Captain 1st Rank V. Luzgin and Captain 1st Rank S. Smirnov, "Electronic Support to Combat Command and Control," MS, No. 11, 1993, pp. 33-35.

A Graphic Algorithm of the Electronic Situation Coverage Mission Accomplishment Process

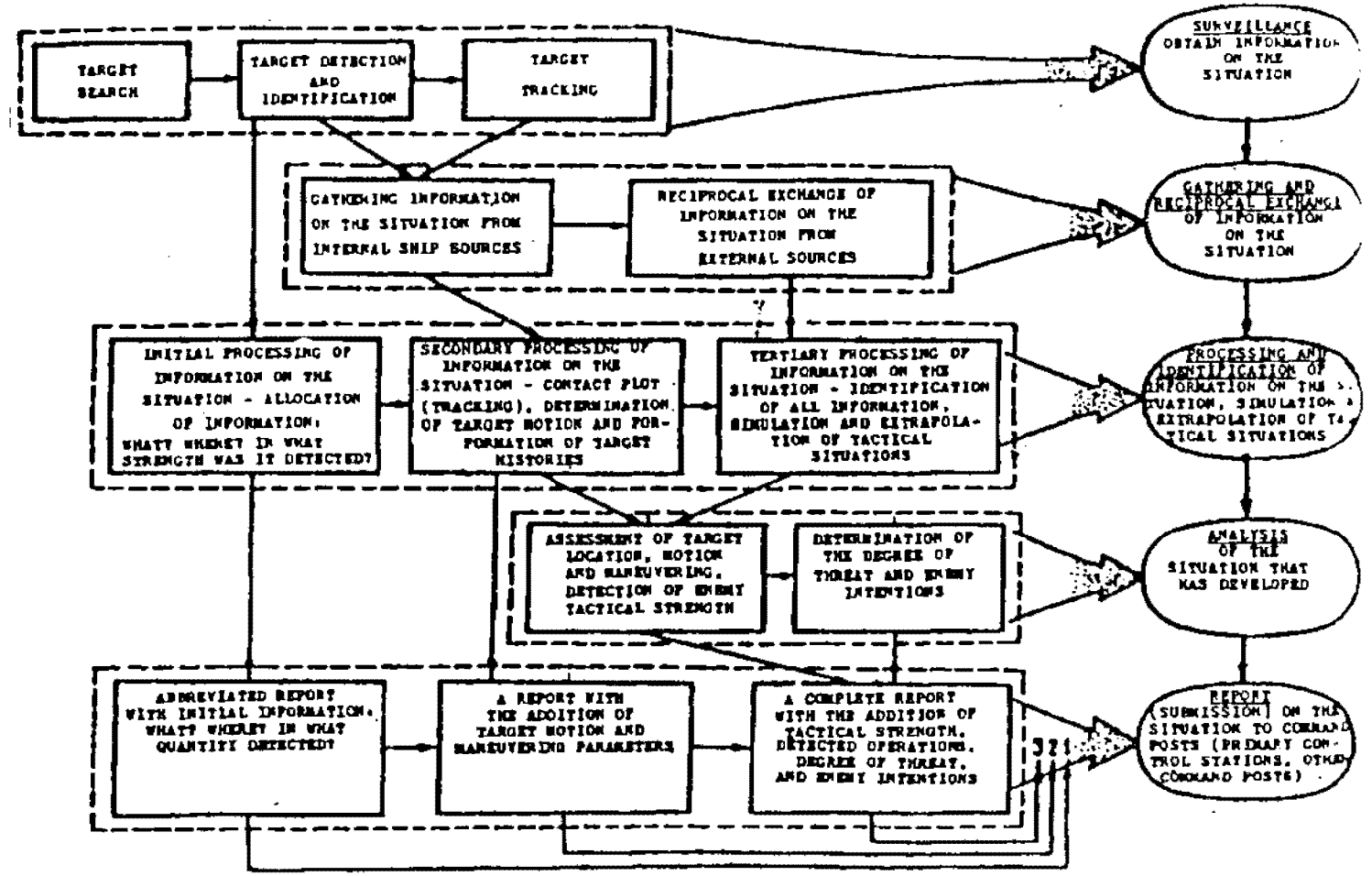


FIGURE 6

Based upon the results of the electronic situation coverage, information processing support must be attained using the MRO systems, combat information command-and-control system loops, BITs equipment or PU-N recommendations. Taking these into account, the Primary Control Station and other command posts of ships, task groups, and task force command posts make decisions on the command and control of the electronic situation coverage systems themselves, electronic jamming systems, weapons systems, ships, task forces, and coordinating forces. The process of implementing each of the possible decisions also entails a number of consecutive conditional stages. The majority of these stages, in turn, require electronic support through the utilization of target identification and target designation systems and schemes; weapons fire control systems; electronic warfare systems; shipborne aircraft take-off, flight, vectoring, and landing control systems; diagrams and shipborne combat information command-and-control system loops; navigational radars; etc. The composition of the command-and-control missions based upon which the recommendations indicated above can be developed is shown in Figure 7.

Consequently, based upon electronic situation coverage, we can totally achieve the required level of electronic support of command and control during combat and other activities of ships and task forces only as a result of all of the examined processes (see Figure 8). What has been set forth above should ameliorate to a certain extent the existing inconsistencies in understanding and interpreting the issues of "electronic support" and "electronic situation coverage".

The examined provisions can be accepted as a sort of methodological basis of the scientific and academic discipline being formed -- "Electronic Support of the

Recommendations for Combat Command and Control That Have Been Developed Based Upon the Results of Electronic Situation Coverage and the Stages of Their Implementation and Electronic Support

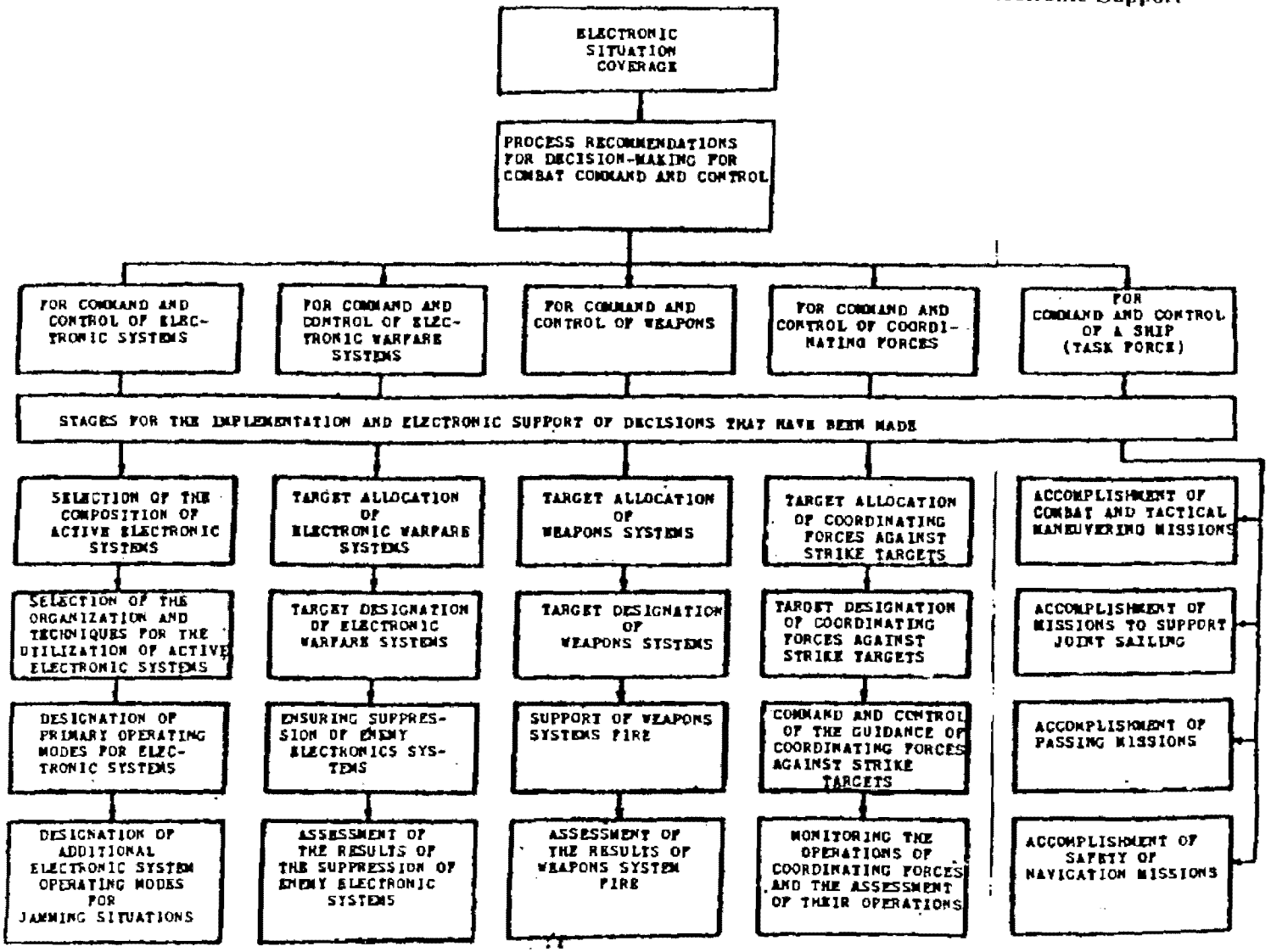


FIGURE 7

The Content of Electronic Support of Combat Command and Control

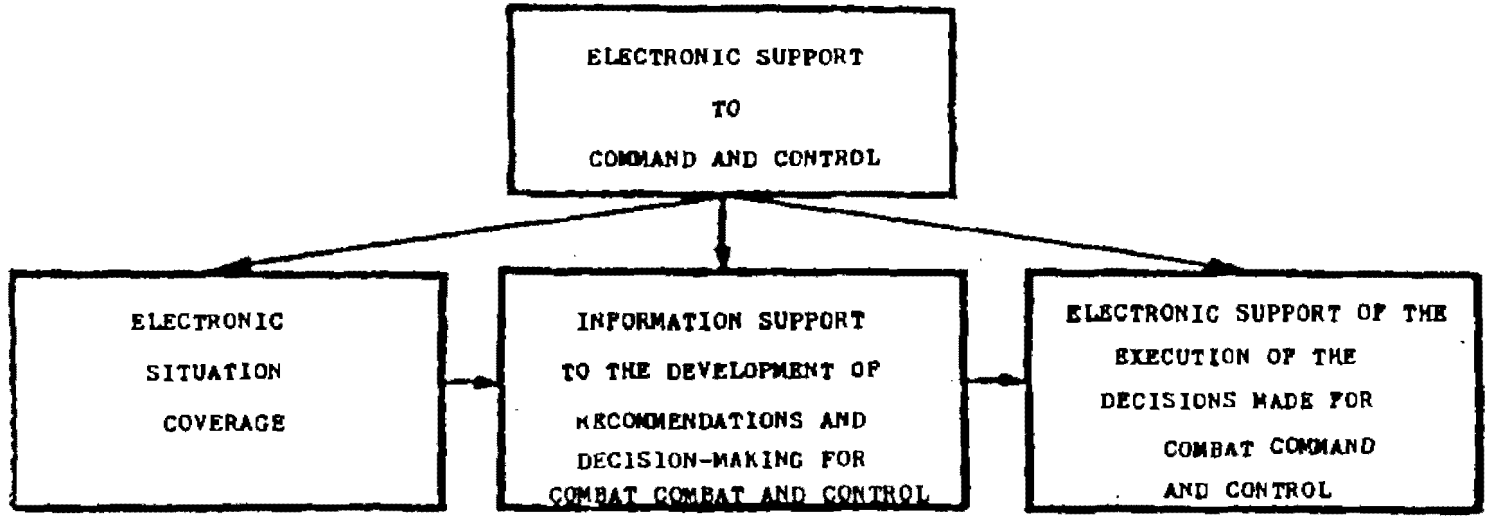


FIGURE 8

Command and Control of Ships, Their Weapons, and Coordinating Forces." This discipline must follow the content and patterns of the resolution of various electronic situation coverage missions and electronic support of combat command and control on the whole and, through its stages, the patterns of interrelationships and the dependencies of these stages. The development of a technical and organizational context for the effective electronic support of combat command and control of naval ships and task forces must be its practical result.

Ground Troops. According to officers of the Russian Ground Troops, command and control means the purposeful activities of commanders and staffs to maintain combat readiness of aviation units of the Ground Troops, prepare them for a battle (operation), and lead them when performing assigned missions. Its organizational and technical basis is a command-and-control system which today is viewed as a command-and-control subsystem of the Ground Troops. A close analysis indicates the existence of serious problems in the structural and functional configuration of command-and-control bodies and facilities if Ground Troops aviation does not conform their capabilities to modern conditions.[47]

It is therefore necessary to reorganize the system of command-and-control bodies and aviation control posts of the Ground Troops. In particular, it makes sense to make wider use of the modular principle of building the control posts. The primary module in a motorized rifle (tank) regiment may be an aviation control team [ACT] made up of 4-5 people (ACT chief; coordination officer; officer for collection, processing, and

[47] Lt. Col. V. Shamauskas, "Aviation Command and Control in Combined-Arms (Operations)," Voyennyy vestnik, No. 8, August 1993, pp. 24-27.

analysis of information on the air and ground situation; and 1-2 guidance and target designation officers).

In a division (brigade) it is desirable to create an aviation control group [ACG] of 18-20 people. Several independent groups can be assigned from it, each of which would include a position for a tactical control officer [TCO] of the front air army operations group. The ACG must be equipped with a radar with an operating range of up to 40 km. In a combined-arms formation (army corps, army) it is advisable to have an aviation control center [ACC] with 30-36 people, in which a front air army operations group [OG] also works.

For increasing the quality of aviation command and control, closer coordination with Ground Troops units, and centralized command and control of weapons of the combat arms, it is necessary to locate all of the above aviation command-and-control bodies together with the control posts of the missile troops and artillery, air defense, and electronic combat. It is also necessary to form a main Combat Operations Control Center [MCOCC] at a front, a Combat Operations Control Center [COCC] at a combined-arms (tank) army, a Combat Operations Control Group [COCG] at a division (brigade), and a Combat Operations Control Team [COCT] at a regiment. A structural model of the proposed system of aviation control posts is shown in Figure 9.

Aviation tactical control complexes [ATCC] can make a significant contribution to increasing the effectiveness of command and control of aviation in a battle and operation. Equipping them with advanced communications and data transmission equipment will ensure complete technical compatibility of the ATCC with aviation

ground control posts of the Ground Troops deployed on the base of the "Maneuver" automated command-and-control system and its effective use in the interests of both organic and supporting aviation.

In addition, for vectoring helicopters to ground and airborne targets, it makes sense to install a special radar on the ATCCs, which would provide an information field for command and control of combat formations of Ground Troops aviation in the zone of operations of the combined-arms formation. Use of the ATCC could ensure not only detection of enemy offensive air weapons but also reconnaissance of moving ground targets. Among others, officers of the Russian Ground Troops conclude that command and control, including of forces and assets of Ground Troops aviation, is becoming just as important a factor of success as the number of troops and weapons, and the correlation of command-and-control capabilities of the opposing sides often decides the outcome of a battle.

NEW VIEWS ON AERIAL RECONNAISSANCE

Russian military experts stress that in the opinion of the military leadership of leading Western countries, in order to identify destabilizing factors and possible threats "to vital interests" of the United States and NATO, aerial reconnaissance must have the following indicators: readiness for emergency movement of its assets to operational tasking areas over great distances in short time periods, the capability of conducting observation under different physical-geographic and climatic conditions, and the capability of collecting data from places where tension is growing in the absence of a

state of war but in the presence of actual preconditions thereof.[48] Changes in aerial reconnaissance requirements are reflected in the content of reconnaissance missions. Methods and tactics will remain essentially unchanged, since their arsenal is rich and diverse. What is required, however, is an improvement of tactics as new aircraft are created, as the enemy air defense system is strengthened, etc. But without rejecting the experience accumulated in numerous local conflicts, military theorists note the need for a further expansion in the range of reconnaissance missions. The latter are formulated in a period when there is not yet an immediate threat and when there is no specific enemy or preconditions for the movement of armed forces to threatened areas and for subsequent initiation of military operations.

Reconnaissance missions which must be accomplished in a period preceding regional wars include the following: identifying signs of preparation for them; collecting data on the products manufactured by major enterprises of the military-industrial complex, on power supply systems, and on other infrastructure installations; uncovering air defense system installations; and collecting data on the physical-geographic and climatic conditions of various regions.

Areas of possible regional wars are forecast based on a possible destabilization of the international situation at a regional level. "U.S. political scientists and analysts" include among them so-called traditional "zones of instability": the Near East, Persian Gulf area, South and Northeast Asia, the Balkans, and certain regions of the former

[48] Colonel A. Krasnov, "Aerial Reconnaissance in Regional Armed Conflicts," ZVO, No. 12, 1994, pp. 28-33.

Soviet Union. They must be under constant observation by all kinds of reconnaissance, and the period of its conduct may be very lengthy or even have no time frames at all.

From the moment troop contingents are moved to a conflict area until the beginning of military operations, aerial reconnaissance missions may be to update specific strike targets and classify them by degree of importance. Priority targets include command-and-control centers, mobile operational-tactical missile launchers, and SAM system positions. In addition, final reconnaissance of targets already identified earlier and monitoring enemy activity at airfields, on lines of communication, and in troop concentration areas ensures that the first massive strike is sufficiently powerful and would immediately deprive the opposing side of the possibility of resistance.

In subsequent stages of the development of regional wars (holding back enemy invasion forces and building up one's own combat might, defeating the opposing side, ensuring postwar stability), aerial reconnaissance missions continue to be the search for and final reconnaissance of targets, participation in reconnaissance-strike operations, and monitoring strike results.

The diversity of new aerial reconnaissance missions, which substantially supplement previously known ones, and the specifics of their fulfillment in regional wars and armed conflicts are fraught with a number of problems which previously did not arise or were of secondary importance. For example, great significance is attached to supporting the rapid movement of aerial reconnaissance assets to a given region. "Western experts" admit that the structure of reconnaissance which took shape during

the Cold War does not conform to the existing geopolitical situation and the intensifying instability of the situation in various regions. This is why, in their opinion, it is necessary to develop a new structure which will permit conducting aerial reconnaissance of previously unknown territory and will be integrated with other kinds of reconnaissance and function in support of multinational force elements when questions of the compatibility of command-and-control systems have not been resolved. NATO countries do not yet possess such a reconnaissance system. It is also necessary to create more flexible organizational forms of employing reconnaissance units capable of operating autonomously in isolation from their bases while performing a wide range of missions.

The "U.S. military leadership's efforts" are therefore aimed at seeking ways to overcome the separateness of reconnaissance assets. One way is to develop a highly integrated system for automated distribution of reconnaissance forces and assets by regions and axes in accordance with the degree of military threat and with the number and priority of targets, including preliminary preparation and assignment of missions to reconnaissance aircraft crews.

Another way of solving this problem is to further integrate airborne and space-based reconnaissance systems, and in support not just of the strategic echelon, but also the operational and even the tactical echelons. The first experience in successful use of such a combined air-space system based on joint use of U.S. reconnaissance satellites and strategic reconnaissance aircraft was gained during the Persian Gulf War. This system is irreplaceable in situations when it is impossible to forecast the place

where a military threat will appear or when the area of expected operations is rather vast.

Within the framework of a highly integrated reconnaissance system, its combination with the most diverse information sources appears possible. For example, before the beginning of the war in Iraq the Multinational Forces [MNF] command element was comparing air-space reconnaissance data with results of interviews with both scientists and specialists who had visited Iraq recently and representatives of firms which had built various installations there.

Increasing the flexibility of employment and universalizing reconnaissance assets, from which it is possible to quickly form nonstandard table of organization structures adapted to conditions of a specific situation in a particular region, is considered to be one other way of solving this problem. Composite air wings with a high level of manning and professional training of all specialists are most suitable for this. Their makeup includes military transport aircraft and aerial tankers for independent, swift rebasing to remote areas, including those with poorly developed infrastructures. The presence of groupings of U.S. reconnaissance aircraft permanently deployed in Western Europe and the Pacific will facilitate such a maneuver.

The problem of sufficiency is considered to be one of the most serious for the immediate decade. It is being solved today against the background of a reduction in military expenditures, which gives it special acuteness. Foreign military analysts note that there has not yet been a single war or armed conflict where reconnaissance assets turned out to be sufficient. In planning aerial reconnaissance in the Persian Gulf area,

preliminary calculations of the U.S. Air Force staff indicated that it was necessary to deploy six squadrons of RF-4C tactical reconnaissance aircraft, but only 1.5 squadrons managed to be formed. As a result, the daily number of sorties by crews exceeded the standards, and in one sortie they had to photograph up to 30 targets instead of 6-8, which led to a great physical overload of the pilots and a resulting deterioration in the quality of performance of reconnaissance missions.

The insufficient number of reconnaissance aircraft was compensated for by drones. They supplied information chiefly on stationary targets, determined the degree of their destruction after air strikes, and were used to search for Iraqi mobile operational-tactical missile launchers. In the latter case the results naturally were considerably lower than with the use of manned reconnaissance aircraft.

In the assessment of "Western specialists," the integration of reconnaissance systems and thorough reconnaissance planning will permit performing missions with fewer personnel. The U.S. Air Force command proposes a more rational way of reducing reconnaissance forces to a reasonable minimum; i.e., reducing the number of reconnaissance aircraft types and selecting the most effective ones. True, these specialists take a very cautious approach to this, since a system of aerial reconnaissance assets was used in the war against Iraq: TR-1 strategic reconnaissance aircraft, RF-4C tactical reconnaissance aircraft, and drones. In addition, combat aircraft crews were used to perform reconnaissance missions.

Just what kind of reconnaissance aircraft is the most rational? "Foreign experts" respond that it is the one which can be used in any region with a takeoff from air bases

located in the continental United States. Such a strategic reconnaissance aircraft is being created in the United States (codenamed "Aurora"). It is expected to be capable of operating at hypersonic airspeeds (Mach 5-6) at altitudes of around 36 km, which means it will be capable of obtaining necessary data quickly and will be relatively invulnerable to enemy air defense weapons.

But in the assessment of "Western experts," such aircraft, which are intended for large-scale wars, will not be able to perform all reconnaissance missions and will be too costly for local conflicts. It was the high operating costs that explained the removal of Aurora's predecessor, the SR-71, from the inventory. Therefore it must be supplemented by operational-tactical aircraft, above all aircraft having a low radar signature.

With a reduction in the U.S. Air Force budget and in budgets of other Western air forces, as well as a reduction in the number of aircraft, "military specialists" assume that the problem of sufficiency of reconnaissance assets can be solved by mass development of inexpensive drones. According to their forecasts, in the near future Western countries will produce up to 30,000 craft of various types, and the production peak will come in the year 2000. It is emphasized that despite reductions in appropriations for military purposes, the United States has sufficient financial and economic resources for creating that number of drones within the planned time periods. The press reports that two types of reconnaissance drones are being developed: the first is reconnaissance in the tactical zone in support of divisions and brigades, with real-time transmission of video data; the second is for reconnaissance in remote regions.

The problem of increasing the reliability of information becomes especially pressing with the reconnaissance and identification of small, mobile targets and with monitoring air strike results. The experience of the Persian Gulf War serves to confirm this. Reconnaissance showed its positive side when data on stationary targets were required, and the negative side when reliable information was needed on mobile targets. Thus, it did not manage to establish the precise number and location of Iraqi missile systems which were delivering strikes against targets in Israel and Saudi Arabia throughout the entire war. MNF strike aircraft waged a battle against them, and not always an effective one.

According to General-Major A.M. Bykov, the role of air reconnaissance at sea in the past, present, and future is difficult to overestimate and dangerous to underestimate. An acute question of reconnaissance support to Soviet naval forces and issuance of target designation data to their long-range weapons arose in the postwar period, when confrontation at sea was exacerbated. With unique capabilities of conducting reconnaissance in vast and distant ocean areas, collecting reliable intelligence and transmitting it to the command element and to strike forces essentially in real time, reconnaissance aviation rightly received priority among other kinds of reconnaissance. It was in this period that air reconnaissance systems based on the Tu-95RTs aircraft, equipped with an effective reconnaissance and target designation system for operations in the far zone, as well as Tu-16R and Tu-16RM aircraft for reconnaissance in the middle and near zones became operational in the Soviet Navy.[49]

[49] General-Major Anatoliy Mikhaylovich Bykov, "Reconnaissance as It Is," MS, No. 3, 1995, pp. 45-47.

Their ability to detect foreign naval groupings (above all carrier groupings, missile and amphibious landing task groups and convoys) and transmit target designation data in real time to submarines, missile-armed naval aircraft, and surface missile ships had a fundamental effect on the concept of naval warfare. In this period the Soviets came close to solving the problem of conducting a naval battle using precision weapon reconnaissance-strike complexes.

Demands on air reconnaissance also rose accordingly. The main ones presently are still purposefulness (concentration of main reconnaissance forces on the most important axes), aggressiveness (striving for unconditional performance of the assigned mission), timeliness (obtaining information in a time period ensuring its effective use by fleet forces), continuity (day, night, under any situation conditions), as well as covertness of reconnaissance and the accuracy and clarity of information.

Two main missions should be singled out among the numerous ones facing fleet reconnaissance under the new conditions. The first, which reconnaissance forces and assets are obligated to perform in peacetime, is a guaranteed warning to the fleet command about the possibility, probable place, and tentative time of an armed clash in any form. The second, accomplishment of which is connected with the immediate conduct of military operations, is to provide fleet forces with vectoring and target designation data.

Both of these missions require reconnaissance forces and assets to keep approximately 1,000 naval targets of foreign states under surveillance in fleet zones of responsibility. They include aircraft carriers, submarines, and missile ships armed with

precision weapons located in areas from where a surprise strike can be delivered against Russian Federation territory and military installations. For reliable, timely performance of those missions it is necessary to conduct reconnaissance to the full depth of ocean and sea zones, and to determine target locations with an accuracy ensuring their guaranteed engagement in case combat operations begin.

The Pacific Fleet Air Force holds a key place in performing general reconnaissance missions, since in peacetime aviation is assigned the following:

- determining the surface and undersea situation to maintain the theater operational regime;
- detecting and pinpointing ship groups and lone ships of target countries and determining the nature of their activity, operating tactics, and features of weapon employment;
- promptly detecting ASW forces on deployment routes and in areas of activity of Russian strategic missile submarine cruisers;
- collecting information on ship and continental air defense forces and assets;
- pinpointing areas, makeup of participants, and operating tactics of forces during national and joint exercises of target country navies; and
- determining routes and intensity of civilian shipping within the operating radius of air reconnaissance forces.

General Bykov also stresses the capabilities of the new Su-24M and MR reconnaissance aircraft. He states that by forming a flying unit equipped with these specialized aircraft, which are outfitted with modern reconnaissance equipment, the Russian Navy will be able to compensate to a considerable extent for the loss of

obsolete Tu-16R and Tu-95RTs reconnaissance aircraft. But the Su-24, created as a front reconnaissance aircraft, proved ill-suited for an ocean theater in view of its short flying radius. In addition, its onboard reconnaissance complex is intended for hunting small, well-camouflaged ground targets, which generally is unnecessary in operations over the sea. At the same time, the aircraft lacks sufficiently powerful and vital panoramic radar. But its most important shortcoming is that air reconnaissance results cannot be processed on the ground without a special complex, and the plant which produces it ended up outside of Russia. Therefore there are no deliveries of this equipment for now, and it is unknown whether or not it will be produced. But without this complex the value of this aircraft as a reconnaissance aircraft is almost nil.

A rather large range of air reconnaissance problems which arose for fleet aviation in recent years stands out. That is why air reconnaissance is the focus of attention of the Pacific Fleet Air Force command element and of leadership personnel. Indeed the most recent experience of the Persian Gulf War showed persuasively that success of modern operations by Navy, Air Force, and Army groupings depends largely on how they are used within the framework of a united supersystem in which air reconnaissance has priority importance.

During Operation Desert Storm the Americans created a radar surveillance field in the space from the Gulf of Hormuz to the Red and Mediterranean seas with five E-3 AWACS radar early-warning and control aircraft as well as three E-2 Hawkeyes simultaneously on airborne alert. They covered the air and surface situation essentially continuously and in real time in supporting an average of 2,240 strike and fighter aircraft missions a day. Pioneer drones operating from aboard the battleships

"Missouri" and "Wisconsin" proved to be an indispensable means of detection, target designation, and gunfire spotting. All this permitted coalition troops to conduct combat operations with minimal losses and high effectiveness.

Russian military officers stress that aerial reconnaissance played a key role in supporting the preparation and conduct of the offensive air campaign and air-land operation of the Multinational Forces [MNF] against Iraq (17 January - 29 February 1991). In the phase of strategic deployment and preparation of the armed forces grouping of the United States and its allies for combat operations, main efforts were concentrated on following the progress of operational deployment by the Iraqi Armed Forces and on collecting and processing data on military installations on the territories of Iraq and Kuwait for planning missile-bombing strikes and electronic suppression and for supporting measures for monitoring the naval blockade in the Persian Gulf. With the beginning of combat operations, reconnaissance missions were retargeted to assess missile-bombing strike results, detect new targets for engagement (above all Scud mobile operational-tactical missiles), follow Iraqi troop and aircraft movements, and monitor airspace, above all in order to detect Iraqi missile launches.[50]

Reconnaissance missions of detecting operational-tactical missiles proved to be the most difficult for allied aircraft. During the first two weeks up to 30 percent of all combat sorties by allied aircraft were spent on those missions, but they did not manage to destroy all mobile systems despite the fact that they were on open terrain in a stationary position for almost an hour before launch. A small number of systems were

[50] Colonel V. Palagin and Captain A. Kayshauri, "Air Force," ZVO, No. 12, 1995, pp. 26-29.

detected in the initial stage of preparation for launch, owing to which there was an opportunity to vector strike aircraft to them. Some sorties were flown against decoy targets, which diverted considerable reconnaissance and strike aviation forces.

In estimating results of the MNF air and air-land operations in the Persian Gulf, "foreign specialists" note that comprehensive reconnaissance support considerably facilitated successful performance of assigned missions. Because of this, a rather high level of knowledge managed to be achieved on Iraqi troop groupings; command-and-control systems; and weapons and military equipment, their specifications and performance characteristics, vulnerable aspects, tactical capabilities, and features of employment in the given TVD. Thorough, lengthy reconnaissance (more than 5 months) of the territories of Iraq and Kuwait permitted the MNF command to plan and conduct military operations precisely.

Aerial reconnaissance promptly provided the U.S. and MNF command with detailed topogeodetic and topographic data with a precise tie-in of important military-political, economic, and military installations; and the disposition of armed forces groupings, command-and-control and communications facilities, lines of communication, and engineer fortifications. Based on the information received, optimum routes of approach to targets were selected and calculated, and force details and the necessary quantity and mix of weapons were determined. In some cases intelligence on key components of targets had to be updated to increase the effectiveness of precision weapons.

At the same time, the Persian Gulf War revealed a number of shortcomings in the organization and conduct of MNF reconnaissance. "Specialists" believe that despite the use of all available air and space assets, U.S. intelligence services were unable to uncover the locations of all Iraqi operational-tactical missiles and determine their precise number, although it was known that they were based only in a relatively small territory in two areas. Delays were repeatedly noted in the processing and presentation of operational information to appropriate battle management entities. Thus the tempo of air combat operations often outstripped the rate of flow of data coming from air and space electro-optical reconnaissance assets.

SOVIET VIEWS ON SPACE-BASED RECONNAISSANCE

Space is a new medium for military actions offering a truly intercontinental reach, but the Soviet approach had long emphasized the integration of military space systems into support of earth-bound war-fighting capabilities. In a lecture delivered to the General Staff Academy, for example, General-Major I.B. Shaposhnikov noted that the main missions of military space systems are reconnaissance and command and control (C^2). In regard to these missions, he stressed that space-based assets have very special capabilities that greatly exceed those of ground-based systems in terms of range and response time. While these capabilities offer substantial advantages, however, space-based assets should be viewed as part of an integrated system employing both space- and ground-based assets, and not as a replacement for the latter.[51] Soviet military writings focused repeatedly on the role of space-based systems in

[51] Jacob W. Kipp, "The Problem of Space in Soviet Operational Art," Soviet Army Studies Office Paper No. 88-3744, pp. 10-11.

Shaposhnikov's support and command-and-control missions. Soviet doctrine had long recognized the vital importance of accurate, real-time intelligence and redundant C^3I, as well as a blinding of the opponent's C^3I as a priority task for the initial period of the war.[52] Colonel-General K. Kobets, for example, argued in 1990 that satellite communications will soon dominate in wartime because they provide fast communications with command objects at practically unlimited distances, have a large number of high-quality channels, and are less vulnerable to various interdicting and disabling actions.[53]

Interdiction or preemption of enemy forces was said to be impossible without accurate, real-time reconnaissance -- and this can only be accomplished from space. Hence Soviet discussions of air superiority at the tactical, operational, and strategic levels insisted that it is unattainable without pre-existing or concurrent superiority in low space. Soviet military writings thus stressed the growing importance of space as providing a platform for global monitoring of ships and terrestrial targets, and for coordinating fire strikes against missile platforms.[54] Experts noted that space-based systems in the current U.S. inventory are oriented toward accomplishing strategic tasks,

---

[52] I.I. Anureyev, "Determining the Correlation of Forces in Terms of Nuclear Weapons," VM, No. 6, 1967, pp. 164-168.

[53] Interview with General of the Army M. Moiseyev and Colonel-General K. Kobets, "Crucial Links in Command and Communications," VV, No. 10, 1990, pp. 3-7.

[54] Philip A. Petersen and John G. Hines, "The Soviet Air and Anti-Air Operation," Air University Review, March-April 1985, pp. 36-54.

and can increase the potential of the U.S. Armed Forces by a factor of 3-4 or more.[55]

Soviet experts often examined the role of small satellites in combat support missions.[56] "American military specialists" were said to believe that with a reduction of conventional arms and general-purpose armed forces, priority should be given to programs supporting their high combat effectiveness, and to space programs above all. The following were said to be the basic elements of the small satellite concept: creation of small inexpensive vehicles oriented toward supporting combat missions within the limits of a specific TVD, with the possibility of their prompt mass launch; transition to use of expendable, primarily air-based launch vehicles to achieve covertness of inserting satellites into orbits; and development of mobile ground equipment for receiving, processing, and providing commanders with satellite data needed for organizing and conducting combat operations.

In examining the directions of development and creation of small satellites, the Soviets noted that they supplement space systems and remedy a number of deficiencies inherent to the latter. Small intelligence satellites conduct operational (electro-optical and photographic) reconnaissance for detecting force groupings, uncovering the enemy defense, and obtaining images of military installations in a TVD; perform COMINT and ELINT collection by intercepting data being transmitted over radio channels and the emissions of radio-technical equipment for purposes of detecting them and

---

[55] V. Savichev, "A New Pentagon Concept," KZ, 14 November 1990.

[56] For example, see Colonel V.V. Savichev, "On the Question of the Role of Small Satellites in Accomplishing Operational (Tactical) Support Missions," VM, No. 7, 1991, pp. 23-28.

determining characteristics; monitor effectiveness of troop camouflage measures; and evaluate the effectiveness of diversionary, demonstration, and simulation measures for deceiving the enemy. The task of producing and issuing target designations directly to entities and systems for command and control of attack weapons and EW equipment with accuracies ensuring their effective use against all types of targets, including moving point targets, is among the most important ones.

According to Soviet experts, increased demands on reconnaissance for promptness, depth and number of objects uncovered, and accuracy in determining their coordinates can be realized by introducing small satellites into the structure of operational (tactical) support. Their use substantially expands the information field and permits employing the most powerful weapons to maximum range. For example, reconnaissance depth can be increased to 2,500 km (for an orbital height of 500 km) with real-time transmission of data to the division or corps CP. In addition, by transmitting intelligence on the enemy directly or via relays to an E-2C Hawkeye airborne early-warning aircraft, for example, these satellites provide an opportunity for increasing their loitering range and altitude from areas of combat operations. This increases survivability of airborne command posts and the range to which weapons are vectored to targets to be engaged.

The Soviets believed that in the future small satellites will open up ways for transforming intelligence and EW from support forms to a component part of combat operations in a TVD, and proposed to outfit them with telescopes with optics having a diameter of around 600 mm and a focal distance on the order of 2 m. Data will be transmitted from them to mobile receiving facilities equipped with small-aperture

antennas. In short, high promptness of preparing and covertness of inserting small intelligence satellites into orbits and the possibility of their high-reliability group launch increase the effectiveness of surveillance of the enemy in a local conflict area.

Soviet experts also noted that developers of the small satellite concept allocated an important role for them in the system of early-warning and ballistic-missile defense in a TVD. In analyzing available systems for detecting and tracking missiles based on the use of large satellites, "U.S. specialists" concluded that they do not provide requisite promptness in processing data on the launch of tactical missiles. Therefore to solve this problem a decision was made to develop and create a new theater missile defense system for detecting launches of tactical missiles, which in their opinion should function independently. Small satellites are its basis. After intersecting the exhaust plumes of missiles being launched, they will track them for the time needed to select targets and determine target designations. Data are transmitted from aboard these satellites to a ground data-receiving facility and go to the command post, the interceptor missile launch position, and the interceptor control radar. The Soviets claimed that U.S. planners proposed to use as a satellite a vehicle weighing 450 kg inserted into a geosynchronous orbit, which permits monitoring a territory of around 4 million km^2 with a three-second zone surveillance periodicity. U.S. allies were also said to be interested in development of the theater missile-defense system. For example, Israel will be able to obtain data from it in real time about the launch of missiles by Arab states and provide target designations to radar equipment and to Patriot, and in the future also to other interceptors.

The Soviets therefore concluded that small satellites can be viewed as a new class of armament. Their use in space support systems will improve the effectiveness of combat employment of forces at operational and tactical levels by improving operational-tactical characteristics of reconnaissance systems and upgrading capabilities for massive employment of ground-, air-, and sea-launched offensive weapons.

Soviet military scientists also evaluated the effectiveness of such systems as the Pegasus air-launched launch vehicle.[57] They noted that in the middle of the 1980s two trends became clear as the United States attempted to realize the integration of outer space: considerable growth in spending and an increase in the number of failures of the more and more complicated space hardware. At the beginning of 1987, the United States took the initiative and began the detailed study of new concepts to support the launch of payloads into outer space with the aid of launch vehicles (LV) launched from an aircraft. It was assumed that such a missile would make it possible to launch small satellites, including most importantly reconnaissance and communications satellites, into space in a very operative fashion and at comparatively low cost. The "American press," in emphasizing the merits of the small LV, noted that it can be launched under conditions of enhanced secrecy, since virtually any airfield is adequate for the takeoff of the launching aircraft. These satellites will be able to issue important information literally from the first minutes of their arrival in near-earth orbit, while an enemy would need at least several hours to detect the satellite and take steps to counteract it. The

---

[57] For example, see Colonel V. Kistanov, "The Pegasus Air-Launched Launch Vehicle," ZVO, No. 9, 1991, pp. 34-38

tracking of small satellites will be made more difficult by the use of elements of Stealth technology.

According to Soviet analyses, hypersonic speed trials in the interests of creating an aerospace plane could be yet another realm of possible application of the Pegasus LV. The rocket could be used within the framework of corresponding research for flights in cruising mode at high altitudes and at high Mach values without going into space. Flights in such modes would make it possible to gather valuable information for subsequent calculations of the dynamics of airflows, essential for design engineering on an aerospace plane. The payload mass of the Pegasus rocket in that case could reach 680 kg. The U.S. Defense Department, despite the incomplete testing process for the Pegasus launch vehicle, was said to have verified its operability under the real conditions of military conflict in the Persian Gulf. The Soviets concluded that even if the United States does not proceed in the future with the conversion of the Pegasus LV into an important element of anti-satellite weaponry, its use with small satellites will make it possible for the Pentagon to develop a new broad-scale system of aerospace surveillance possessing sufficient technical capabilities to conduct military and economic reconnaissance on a global scale.

Finally, the Soviet military repeatedly stressed the role of space-based systems in the allied victory over Iraq. According to General-Major Kutsenko, allied forces of battalion size and higher utilized space-based communications systems, while allied staffs used satellite reconnaissance to monitor developments along the front.[58] In fact,

[58] For example, see Barbara Starr, "Satellites Paved the Way to Victory," Jane's Defense Weekly, 9 March 1991, p. 330.

the first Military Thought article to examine Gulf operations focused on the performance of space-based systems. According to the authors, these systems constituted "the basis of all technical reconnaissance" in the war.[59] With a resolution of about .5 m, electro-optical means provided the capability to swiftly and reliably detect changes in the operational configuration of Iraqi armed forces. In addition, the United States is said to have experimented with ways of expanding the application of space-based reconnaissance means. For example, space-based systems proved effective in detecting SCUD ballistic-missile launches, and increased warning time from 1 to 5 minutes. They also proved effective in correcting the trajectories of airborne and cruise missiles. These systems functioned effectively at all levels of coalition forces, including the tactical. Because the Iraqis lacked radioelectronic means of suppression, space-based systems ensured uninterrupted and undetected command and control of troops and weapons.[60]

But the Soviets also noted that the conflict in the Persian Gulf revealed a number of shortcomings in space equipment. Existing reconnaissance systems are not fully adapted for discriminating dummy targets. The Iraqi side's skillful conduct of operational maskirovka and disinformation measures and timely dispersal and sheltering of the main kinds of equipment and supplies in reliable structures created in advance significantly reduced the effectiveness of tactical employment of MNF aircraft and cruise missiles. Space-imaging reconnaissance equipment did not always produce

---

[59] Colonels V.V. Romanov and V.P. Chigak, "On the Use of Space-Based Means in the Persian Gulf," VM, No. 3, 1991, p. 76.

[60] Ibid., p. 78.

the expected effect, basically because of a deterioration of weather conditions and smoke cover of terrain. This led to a situation where effectiveness in acquiring and tracking Iraqi mobile operational-tactical missile launchers was clearly insufficient. "British experts" mention that the absence of all-weather reconnaissance and acquisition equipment and the high effectiveness of maskirovka of the Iraqi missile launch positions were among the main reasons hampering warfare against them. Due to poor resolution, space radar surveillance data were used chiefly as target designations for other kinds of weapons. Statements made earlier by U.S. specialists about the capability of this equipment to detect underground targets were not confirmed. On the whole, however, the Soviets concluded that a stable trend was manifested in the Gulf War toward expanded use of the data of space equipment right down to the tactical level in the system of support to troop combat operations.

RUSSIAN VIEWS ON SPACE-BASED RECONNAISSANCE

According to Russian military scientists, the U.S. military space forces that support operations at the strategic, operational, and tactical levels have actively participated in local wars and conflicts of recent years. These space forces are substantially expanding the capabilities of troops to accurately determine their coordinates, ensure reliable communications, and detect targets in a timely manner. This provides additional advantages to subunits in the use of modern types of weapons and military equipment that have been deployed in unequipped theaters and without development of their infrastructure.

"Foreign experts" conclude that the dependence of U.S. military might on military space has significantly increased owing to modern American weapons systems

and U.S. military tactics. At the same time, they note the serious shortcomings of traditional military space systems that substantially limit the sphere of their application. Specifically, high-capacity spacecraft are extremely vulnerable due to their substantial dimensions. This situation has resulted in the accelerated development of anti-satellite systems. In the United States, say the Russians, the MALS aircraft-missile anti-satellite system has successfully undergone testing, they are designing satellite destruction weapons based on mobile ground-based missile complexes, and they are developing the capability to install anti-satellite weapons on surface ships and submarines.[61]

Missile launch vehicles that are based at unprotected stationary launch complexes and have a long active trajectory sector are used to launch traditional large spacecraft. In the event of a military conflict, such facilities may be destroyed by non-nuclear weapons, and the missile launch vehicles themselves are an ideal target for the space echelon of an anti-ballistic missile system under any variation of its deployment. Difficulties with maintaining a large ready inventory of spacecraft on the ground (due to their technical complexity and high cost) and the long periods required to prepare spacecraft and missile launch vehicles for launch (tens of days) make it practically impossible to effectively build up orbital formations of space systems in wartime.

"American experts" think that the anti-satellite battle can be conducted not only during a world war but also during local conflicts. Traditional military space reconnaissance and communications systems have been oriented primarily toward providing information to strategic and operational-tactical command-and-control

---

[61] For example, see Lieutenant Colonels A. Kuznetsov and A. Yakushin, "Small-Scale Military Satellites," Tekhnika i vooruzheniye (hereafter cited as TV), No. 7-8, 1992, pp. 34-37.

elements, and planning for the employment of these systems is carried out at the strategic level. According to expert assessments, space information is not disseminated to tactical element commanders in a timely manner or in sufficient volume because of the need to ensure the secrecy of the space information being disseminated, which is transmitted through the elements of a complicated hierarchical structure.

These problems were resolved to a certain degree during the war with Iraq. Division-sized and smaller units that were involved in the conduct of combat operations were equipped with a significant number of satellite communications systems. This required retargeting more than 3/4 of the spacecraft from the U.S. Space Command's orbital formation to the combat operations area. According to "foreign experts," planning the employment of reconnaissance and communications spacecraft at the strategic level and their priority operation to carry out strategic tasks could result in denying access to space communications and reconnaissance data to the majority of tactical element commanders in conflicts of greater scale and intensity. And finally, long periods of time (5-7 years) are required to develop spacecraft and they function in orbit for an adequately long period of time (3-10 years). As a result, obsolete equipment is being operated.

"U.S. experts" see the most radical path to solving the afore-mentioned problems in the development of cheap, small-scale spacecraft designed for a short period of active functioning along with the development of traditional spacecraft. They must have simplified on-board equipment and weigh up to 1,000 kilograms. Due to their small size and thanks to the use of low-signature systems, the probability of their destruction by anti-satellite weapons will be reduced in contrast to traditional

spacecraft. Furthermore, the cost of a single small-scale spacecraft will be less than the cost of firing a round from an anti-satellite weapons system. Due to simplicity of design, these devices may be developed in 1-2 years. Mobile launchers that are capable of conducting space launches during all periods of the military-political situation are being developed to place them into orbit. Low cost, simplicity of the small-scale spacecraft, and a high launch rate capability will permit these spacecraft to be used for operational follow-up reconnaissance and to augment space system orbital formations to increase their combat capabilities and to replace spacecraft that have been destroyed by anti-satellite weapons systems. The possibility for decentralized employment of small-scale spacecraft by tactical element commanders is an important specific feature of small-scale spacecraft. Any consumer who has the appropriate equipment can turn on and tune in to a satellite's on-board systems in such a way that he can obtain the information he needs.

Russian experts assert that U.S. planners intend to use low-orbit small-scale spacecraft to carry out the following missions: provision of tactical communications in TVDs; collection of reconnaissance information and target designation data from automated sensor systems (including under-water situation broadcast and automated meteorological site systems); and remote control of weapons. "Microsat" small-scale spacecraft are said to have been developed to provide tactical communications to U.S. Army division-sized and smaller units and subunits. They have been equipped with intersatellite communications systems that also permit them to be used to obtain information from combat engineer-reconnaissance teams and automated reconnaissance systems that are located in the enemy's deep rear areas. Optical, radar, and electronic reconnaissance small-scale spacecraft are designed to warn tactical element

commanders about missile attack, to conduct reconnaissance of the TVD, and to transmit target designations to weapons systems.

Russian experts have also noted that the involvement in Gulf combat operations of space equipment for detecting ballistic-missile launches considerably expanded the combat capabilities of conventional weapons. Thus, two U.S. IMEWS spacecraft separated in a geostationary orbit, intended basically for determining launch coordinates of Soviet and Chinese ICBMs, detected Iraqi SCUD operational-tactical missile launches from two directions and gave preliminary warning to Patriot SAM system command-and-control facilities used to destroy the warheads when fired against the territory of Israel and Saudi Arabia.[62]

The wide use of a space system for detecting ballistic-missile launches, along with use of other space equipment for COMINT and electro-optical reconnaissance in the period of preparation for and conduct of combat operations in the Persian Gulf, are said to reflect the overall thrust of U.S. military-technical policy toward using outer space as a component part of the TVD.

Russian experts conclude that on the whole, space reconnaissance assets permitted effective use of their data in planning massive fire strikes with precision weapons. In particular, based on satellite intelligence it was possible to make a prompt estimate of the degree of target damage for planning subsequent strikes. But the war also revealed a number of shortcomings of these assets. Intelligence was not

[62] For example, see Colonel B.S. Skrebushevskiy, et al., "On the Principles of Creating Missile-Attack Warning System Space Equipment," VM, No. 6-7, 1992, pp. 20-23.

communicated promptly enough due to incomplete deployment of the orbital grouping of imaging reconnaissance spacecraft and troop facilities of the Constant Source system. The rate at which combat operations were conducted by MNF aviation often exceeded the rate at which intelligence was updated. With the Iraqi's skillful use of maskirovka and creation of decoys, space reconnaissance assets did not always reliably support the identification of targets. As a result, a number of air strikes were delivered against dummy targets.[63]

Use of the IMEWS system in the Persian Gulf is said to have confirmed the possibility of establishing effective TVD missile-attack warning systems. The possibility was demonstrated for the first time of using ballistic-missile launch detection spacecraft for performing a qualitatively new mission -- issuing target designations on mobile missile systems. In this connection the United States made the decision to begin work on operational-tactical missile launch detection spacecraft and mobile equipment for the Army and Navy.

At the same time, the shortage of communications channels was felt during military operations, above all at the tactical level. To solve this problem the U.S. Defense Department is said to have activated work to create the new MILSTAR jam-resistant communications system, which consists of spacecraft inserted into geostationary and highly elliptical orbits, and tactical satellite communications systems

---

[63] Lieutenant Colonel A.N. Kuznetsov, "The Technical Capabilities of U.S. Space Assets," VM, No. 8-9, 1992, pp. 70-76.

based on the small low-orbiting TACSAT spacecraft intended for supporting battlefield communications.

The high effectiveness of NAVSTAR under combat conditions led to a revision in the amount of navigation gear procured for the U.S. Armed Forces. In addition to 27,000 autonomous navigation receivers of different types ordered by the Defense Department, it is planned to procure at least another 25,000. The decision also was made to install the BLOCK-3 receiver of the NAVSTAR system in advanced Tomahawk cruise missiles, which will accelerate and simplify their strike planning and increase the flexibility of their employment, since in a number of cases it will be possible to reject missile guidance based on digital terrain maps. In local wars, when the enemy does not use ECM, advanced cruise missiles will be able to be guided to targets based only on this system's information.

In assessing the results of Desert Storm, Russian experts speak confidently about the capability for significantly increasing combat effectiveness of TVD forces through use of military space forces. This is confirmed by the fact that they provided the MNF with prompt information about the redeployment of Iraqi troops, thereby supporting effective fire engagement of Iraqi personnel, equipment, and military-industrial targets with precision weapons, and also prompt command and control of forces and weapons.

"American military specialists" consider the Persian Gulf War to be the "first space-age war" because military space assets were used to support all branches of the MNF. The integration of military space assets into a unified reconnaissance system permitted advance discovery of the concept of Iraqi troop operations and timely

operations planning. Thus, a week before the beginning of the conflict a sudden transition of radars to an intensive operating mode was registered in southern Iraq with the help of space reconnaissance equipment. Then forward movement of military units and equipment toward the Kuwaiti border was detected using space-imaging reconnaissance equipment. These and a number of other reconnaissance signs permitted the CIA to discover Iraq's aggressive intentions. Subsequently space reconnaissance equipment performed monitoring in that region, and with the beginning of and during military operations effectively performed follow-up reconnaissance missions after delivery of air-missile strikes in air and ground operations. In the absence of any kind of opposition, the Americans tested upgraded electro-optical reconnaissance satellites as well as mobile stations and special terminals supporting reception of video images directly from the satellites. Space reconnaissance equipment was used for the first time as a means of combat support to Patriot SAM systems in combatting Scud missiles.[64]

Russian experts also note that despite activation of reconnaissance equipment systems (Lacrosse, KH-11M and DSP satellites, Tornado aircraft, and so on), missions of detecting and identifying routes of forward movement of mobile weapons (particularly operational-tactical missile launchers) in hours of darkness were not accomplished so successfully.[65] To remedy this and certain other shortcomings, "American specialists" deem it necessary to further integrate military space assets with personnel and equipment of Air Force, Navy, and Army groupings. But an analysis

---

[64] Major L.N. Doda, "On Revealing Signs of Space Reconnaissance Equipment," VM, No. 10, 1992, pp. 42-47.

[65] Ibid., p. 42.

shows that this tendency leads to reinforcement of the overall radar signature background when military space assets perform a unified, specific mission, as well as to the initiation of radar signatures for each asset in performing local missions. Therefore detection of these signatures using national means of monitoring outer space and an analysis of presumed operations of naval, air, and ground groupings can be used a priori for uncovering the enemy's concept of operations.

According to Russian experts, space-based monitoring equipment can detect changes in frequency, intensity, and density of space reconnaissance equipment overflights of specific application areas and in the makeup and orbital alignment of their groupings. An analysis of these and other reconnaissance signs even before combat operations begin determines the space-time parameters of the onset of important events under conflict conditions; i.e., predicting the beginning and possible course of combat operations with a certain validity. It should be noted that this is a very complicated task, but modern methods permit formalizing, modeling, and assessing it with the help of a generalized indicator of the status of the air-space and ground situations. The methodology's essence consists in advance establishment of a data base of radar signatures and a knowledge base for their use in assessing and analyzing (with the help of special algorithms) the ground-space situation in a specific region.

Russian experts note further that one feature of using space reconnaissance equipment in the Persian Gulf was its effective use in a limited TVD. This became possible because of coordinated receipt of information from assets of both echelons in a single command-and-control circuit and its highly automated processing, identification, and prompt communication to consumers. According to these experts,

the use of space reconnaissance equipment in the Persian Gulf demonstrates the following:

First. A combination of radar signatures of ground and orbital groupings of space reconnaissance equipment and of personnel and equipment of the air force, navy, and army identified in functional, structural, coordinating, and opposing situation elements can be used in forecasting important events under conditions of a conflict similar to the Iraqi-Kuwaiti conflict.

Second. Expert systems intended for analysis, assessment, and forecasting of the ground-space situation must include programmed components for detecting and coordinating the radar signatures of orbital and ground equipment. Operations groups must include operators for assessing the ballistic situation with equipped, automated workstations and appropriate dialogue-oriented and expert support.

Third. Use of Stealth technology (especially for small satellites), active maneuvering, and orbital servicing are factors reducing the revealing capabilities of space reconnaissance equipment. In connection with this, one can expect accelerated development of orbital equipment for outer space coverage in various wavebands and creation of a system for detecting aerodynamic targets in flight (based on the AFP-888 satellite and space-based radars).

Fourth. A tendency toward further integration of space reconnaissance equipment with other reconnaissance equipment, weapons, and command-and-control and communications equipment leads to the need for developing effective mathematical

and other methods for detecting, analyzing, and coordinating the revealing signs within the framework of a model for assessing and forecasting the ground-space situation.

According to Colonel V. Cherkasov, "foreign specialists" analyzing the information support for the Desert Shield and Desert Storm operations are drawing conclusions and generalizations with great circumspection. It cannot be unilaterally asserted that the future of "information warfare" belongs only to satellite communications systems. Natural factors should be taken into account, aside from the risk of the suppression of transmissions and destruction of the space-based elements of the systems. The peak of solar activity on 1 February 1991, for example, led to the virtual cessation of all satellite communications for six hours every day for six days. The following must also be taken into account.[66]

1. Enemy electronic countermeasures systems were either destroyed or turned off by the operators themselves during the battles. The threat of the use of missiles that guide themselves to radio emissions played a large role in that. This is an important element of "information warfare," making it possible to influence the enemy and force him to refrain from the use of ECM resources.

2. One of the fundamental principles of "information warfare" that has arisen lately is the necessity of evaluating a communications system not only by the technical characteristics inherent in it, but also the opportunities for adapting it to changing conditions.

3. The requirements of the concept of Air-Land Battle for the support of combat operations by highly mobile troops makes it necessary to incorporate strategic

[66] Colonel V. Cherkasov: "The Role of Satellite Communications Systems in Information Support for Combat Operations in the Persian Gulf," ZVO, No. 8, 1993, pp. 40-44.

satellite communications systems into command-and-control elements at the tactical level.

4. The control of the space elements of satellite communications systems should be accomplished by one central body able to embrace the entire global system. An element of adaptivity to the changing conditions of a situation should be present here.

5. The requirement for transmission in real time of intelligence data from the processing centers to the lower levels of command and control at the tactical level cannot be ignored. Means of access to broad-band satellite communications channels must be included in tactical systems when they are created in the future.

6. Virtually all of the satellites of the DSCS strategic satellite system were out of order, to this or that extent, after the conclusion of the Desert Storm operation. At least another ten years will be required, according to the estimates of American specialists, to achieve the desired operability of the system. One of the lessons of the conflict is the fact that the necessary flexibility of satellite communications systems can exist only in a case where there is a sufficiently operable and effective ground element. The apparatus of the ground element of the DSCS system had already been in service for no less than 15 years, and was in need of replacement.

7. The combat operations in the Persian Gulf region showed that the development of new technology effectively erased the clear-cut demarcation between military and civilian systems. The military potential of commercial communications systems -- which in some cases proved to be even more operable --was visibly demonstrated.

8. Finally, the actions of the mass media, which actually had an effect on the preparation for and waging of combat operations as well as on public opinion, moved to a leading place in "information warfare" during the conflict.

NEW SPACE MISSIONS

According to Russian military scientists, the scientific-technical potential accumulated by the United States will allow it to deploy orbital groupings by the beginning of the year 2000 capable of the following: effectively combatting strategic missiles in flight and if necessary sealing off outer space; "seizing" the most important spheres of near-earth space; and delivering strikes from space with precision weapons or new-generation mass-destruction weapons against ground, sea, and airborne targets in order to "deter enemy attacks" and also "reinforce operations of U.S. and allied forces."[67]

Conditions will also be created for conducting real-time (at any time of day), all-weather scanning and highly detailed reconnaissance from space and navigational, meteorological, and other kinds of support to Army and Navy forces and to ground-, sea-, air-, and space-based weapons systems. Command-and-control entities are being supported by space communications and relay channels even at the present time.

Under certain conditions the basic forms of military operations in near-earth space can be the following: operations to destroy strategic nuclear (or conventional) weapons in flight and to seal off outer space; strikes from space against ground, sea, and airborne targets; operations to defeat orbital and ground space groupings and to seize and hold strategically (operationally) important spheres of near-earth space; and operations to suppress radio-technical equipment of orbital and ground groupings of

[67] For example, see General-Major M.A. Borchev, "On the CIS Military Organization," VM, No. 3, 1993, pp. 2-10.

space units. Military space operations can acquire operational or strategic significance depending on the scope of warfare and forces and assets used in operations.

In the Russian view, an increased dependence of success in military operations on land, at sea, and in the air-space on the degree of effectiveness and stability of orbital groupings will be typical of conventional warfare. Precision weapon strikes against ecologically dangerous targets located in any region of the globe can produce the effect of using nuclear weapons or toxic chemical agents. In addition, strikes can be delivered from outer space by "supernew weapons of mass destruction capable of paralyzing command and control of a state or coalition of states and groupings of its (their) armed forces for a certain period of time, or attaining a mass effect on the country's population without destroying installations and the environment."

The increased power, accuracy, and swiftness of strikes against enemy forces as well as the struggle for superiority in the air-space above ocean and sea areas will be typical of military operations at sea. All-weather space reconnaissance and other kinds of space support will detect the heading and speed of weapons, surface ships, and submarines at any time of day with high probability and providing precision weapons systems with data for essentially real-time engagement. The importance of maneuver and concealment increases under these conditions, and submarines are forced to operate at a great depth. In the future, missions of delivering strikes against naval targets also can be accomplished from space.

SPACE-BASED SYSTEMS

Despite dramatic cutbacks in Russia's arms procurement budget, a top priority in R&D and procurement is still given to strategic weapons, as well as ABM and ASAT weapons.[68] Russia also inherits from the former Soviet Union those military space programs designed for the creation of space forces, which consist of space-based missiles and directed-energy weapons. These programs were originally justified as Soviet responses to SDI, whether "symmetric" (space-based ABM weapons) or "asymmetric" (space-based missiles designed for striking earth targets or "neutralizing" a missile defense system in space, as well as other ASAT weapons).

In August 1990, General-Major V. Ivanov proposed a radical plan for restructuring the Soviet Armed Forces. Under this plan, a new space-based "Space Troops" armed with means for "destroying enemy targets from space" would be formed.[69] A possible precursor organization for this new branch of the Armed Forces may have been the "Space Units" or, formally, the Chief Directorate of Space Systems. The role of this directorate has evolved from that of "supporting strategic forces"[70] to being a direct component of strategic forces designed for "accomplishing strategic

[68] Interview with Andrei Kokoshin, Izvestiya, July 20, 1992, p. 2.

[69] General-Major V. Ivanov, "A Radical Renewal, and Not Cosmetic Repair," Kommunist vooruzhennykh sil, No. 15, August 1990, p. 17.

[70] Interview with Colonel V. Savchenko in Krasnaya zvezda, 15 January 1992, p. 2.

missions," together with the strategic nuclear triad and the ABM forces.[71] In July 1992, perhaps as a reflection of the shift in mission described above, Marshal Shaposhnikov gave the directorate a new name: the Chief Directorate of Space Forces.[72] Its intended role is probably offensive in character, since it is a separate organization from the Space-Missile Defense Forces or ABM forces.

President Yel'tsin subsequently announced that "No matter how difficult, Russia will revive. It is and will continue to be a space power. Remember that we began it all in even more difficult times."[73] In December 1992, the then commander of the Military Space Forces, Colonel-General V. Ivanov, stressed that "Priority development of space systems ensuring effective support to operations by troops and naval forces, attack warning, and deterrence against aggression in space and from space is consistent with Russia's national security interests and maintaining strategic stability in the world."[74]

---

[71] General-Colonel V. Samsonov, "The System of Collective Security: an Objective Necessity," Krasnaya zvezda, July 3, 1992, p. 2

[72] Press conference by Shaposhnikov, report in Izvestiya, July 9, 1992, p. 2.

[73] Interview with Colonel-General V. Ivanov, KZ, 2 October 1992

[74] Interview with Colonel-General V. Ivanov, "Military Space: Meeting with the Press," KZ, 12 December 1992.

According to General Ivanov, the mission of the Russian Space Forces is to "deter aggression in space and from space." A Russian Air Force general has asserted that the Space Forces will be used in joint operations with the Air Force as well as forces tasked with air and missile defense in "combat to gain air superiority."[75] General Ivanov has also noted that in terms of expenditures, the Space Forces occupy third place in the Russian Ministry of Defense -- after the Navy and the Air Force, and before the Strategic Missile Troops and Air Defense Troops.[76] In April 1993, the Russian Supreme Soviet published a decree entitled "On Measures to Stabilize the Situation in Space Science and Industry." The decree confirms that space science and industry continue to be controlled by the military, and operated primarily for the military.[77] General Ivanov thus announced that "the lion's share, the main share of our work is for the Defense Ministry. If you look at this year's launch program for maintaining the orbiting group of satellites, two-thirds were in the interests of the Defense Ministry, while the remaining one-third were for the manned program, for science, and for the national economy."[78]

---

[75] General-Lieutenant N.N. Ostroumov, "The Air Force in Defensive Engagements," VM, No. 11, 1992, p. 57.

[76] Interview with Colonel-General V. Ivanov, "Space and the UFO," Argumenty i fakty (hereafter cited as AF), No. 16, April 1993, p. 5.

[77] FBIS-SOV-93-093, 17 May 1993, p. 51.

[78] "Program Describes Military Space Forces," in JPRS-UMA-93-004, 3 February 1993.

Russian experts have stressed that the achievements of Russian space science are of enormous interest to any industrially powerful country.[79] "American experts" estimate that Russia occupies a leading position in roughly 50 percent of space technologies. Of particular note are Russian advances in propulsion systems based on various fuel components, in electric power systems, in orbital stations, in assimilating new materials (above all composite materials), in launch systems, in hydrogen technology, and in nitrogen injectors.

ASW AND INFORMATION TECHNOLOGY

According to Russian naval officers, the last decades demonstrate the rather swift development (although also with an evolutionary character) both of means of detecting submarines and antisubmarine weapons, which is connected with progress in the electronics area and with upgrading of data-processing equipment and information technologies as a whole. The following can be included among the main features in the development of modern means of detecting submarines:[80]

- gradual displacement of passive by active detection equipment -- bistatic and multistatic -- in a complex with data-processing equipment, which is connected with the continuing noise level reduction of modern submarines and is especially pertinent for shallow-water areas;

---

[79] "Implications of Joint SDI Idea Discussed," in FBIS-SOV-92-074, 16 April 1992.

[80] Captain-Lieutenant N Rezyapov: "ASW and Information Technologies," MS, No. 2, 1995, pp. 82-85.

- a shift toward use of the low-frequency band of audio signals in sonar equipment (infrasound), which permits achieving long submarine detection ranges; and

- development of non-acoustic detection equipment along with sonar, and wide introduction of fiber-optic engineering.

All this becomes possible basically because of the sufficient level of development of information technologies, use of digital data-processing hardware based on specialized processors, wide use of computer programs and mathematical models which optimize search efforts of ASW forces, and large data bases on hydrologic conditions of the area of operations and of characteristics of different targets.

The most promising among non-acoustic means today are space assets. In particular, good results are provided by a search for submarines located at a depth of 100 m or less using a synthetic-aperture radar installed on a spacecraft, which permits detecting surface waves arising during a submarine's movement. True, this search method largely depends on the submarine's speed and submergence depth. Further, based on the property of a laser in the green-blue spectrum to penetrate water to a depth of several hundred meters, lidars are being developed which also can be used successfully in shallow-water areas, including for hunting mines. There also are infrared submarine detection systems. But operation of the latter equipment depends heavily on weather conditions.

A modern magnetometer permits detecting a submarine at a depth to 600 m, but it is used primarily to refine (localize) a submarine's location after she has been detected by acoustic equipment. It is believed that introduction of the high-temperature

superconductivity method (the Squid magnetometer is being developed) will give the device a sensitivity even exceeding the requisite level, although this will complicate the problem of discriminating a valid signal against the background of interference (or the target signature from the geomagnetic background).

Nevertheless, "foreign specialists" believe that for the near term sonar systems will remain the principal means of long-range detection and tracking of submarines, since of all physical fields created by submarines, the hydroacoustic field will remain the most informative and the one which makes a submarine stand out most among background fields of the marine environment. In addition, non-acoustic equipment cannot for now fully provide target designation for onboard weapons and will be used in areas with poor hydrology and also with the enemy's mass use of sonar countermeasures.

High capacity fiber-optic equipment (a fiber-optic communications line already has been created with a capacity of 1.7 Gbit/sec) is used in data exchange and communications nets and as a means of data transmission from hydrophones of fixed detection systems, including in an advanced system such as the FDS (Fixed Distributed System). Research is being performed on their use as acoustic sensors, sonar arrays, temperature and pressure sensors, sensors for determining the orientation of a long towed array for more precise localization of target position and determination of its motion, in the "non-penetrating" type of electro-optical periscopes, and in a number of other instruments and devices. New data-processing equipment is being used in sonar to compensate for the platform's internal noise, discriminate a valid signal at the

interference level, form a sonar array radiation pattern, identify a target (including also in ASW weapon homing systems), and for other purposes.

The development of detection assets and ASW weapons is closely linked at the present stage with further upgrading of automated battle management systems, which connect submarine detection equipment and systems; ASW weapons; and communications, data-processing, navigational systems, and so on in a common complex.

The stages of development of submarine detection equipment singled out by "foreign naval specialists" can be cited as a small summary of this survey of data-processing equipment and use of information technologies in the sphere of ASW:

- first -- development of low-frequency technology in postwar years, which concluded with the creation of a towed sonar array in the 1960s;
- second, which concerns to a greater extent the process of signal processing -- the beginning of electronic forming of the radiation pattern of towed arrays and the appearance of the first automated battle management systems in the early 1980s;
- third -- adaptive forming of the radiation pattern of sonar arrays and the appearance of fixed arrays, and also the appearance of BSY-1 and BSY-2 systems and specialized processors such as the EMSP; and
- the current phase involves introducing artificial intelligence principles and the appearance of a new element base and software based on expert systems, neural networks, and transputers using "acquired" knowledge.

As we see, the most advanced directions of development of science and engineering, especially information technologies, are involved here. Progress in the area of information technologies will permit introducing self-contained submersibles to the inventory of submarines; as a result, this will revolutionize the entire ASW system and change the very concept of ASW, not to mention operating tactics of ASW forces, and above all submarines. A self-contained vehicle will be created that is used from submarines, is capable of operating both independently as well as in coordination with her, and has "intelligence."

One of the first models of a miniature robot submarine, "Sova," declassified by the firm of International Robotic Systems, is 3 m long and is capable of developing a speed up to 65 km/hr. This submarine can use the data of satellite navigation systems. Another model of such a vehicle is the submersible MUST (Mobile Undersea System Testbed) created in 1988 by Martin Marietta for testing new technologies in the area of command-and-control systems and detection equipment. It is equipped with a sonar with a data-processing system and is controlled on the basis of an expert system; control system software consists of 30,000 lines of code in C language. Thus, say the Russians, the breakthrough by Western countries in using the most advanced information technologies in the area of naval arms demands fully comparable efforts by the Russian Navy, since otherwise their very best ships will soon look like medieval caravels.

SOVIET VIEWS ON MILITARY ROBOTS

Soviet military scientists also examined the development and combat employment of military robots.[81] They argued that through robotization, military specialists strive to achieve not only qualitatively new properties of military equipment, create conditions for improving the effectiveness of human activity, and prevent personnel losses from precision, chemical, biological, nuclear, and other mass-destruction weapons, but also to raise the effectiveness of employing forces under conditions of an ever-growing intensity of enemy opposition.

In recent years, said the Soviets, the West has been expanding a study of capabilities for creating systems and weapons possessing higher survivability and stability and permitting specific combat missions to be accomplished independently or at an operator's command. For example, the United States is said to be developing over 40 different robotized pieces of equipment for the Army, for which it plans to spend around $840 million by 1995. This approach will ensure that the simplest modifications of military robots become operational with the troops in sufficient numbers by the mid-1990s.

Meanwhile, there is no single, precise definition of "military robot" for now, and its existing variants most often are tied to the concept of "industrial robot," which hardly is accurate. Based on this, questions of their classification are not being decided quite correctly. According to Soviet experts, the military robot represents a set

[81] For example, see Colonel A.A. Korabelnikov, "Military Robots," VM, No. 6, 1991, pp. 43-47.

(system) of military equipment outfitted with information-measurement and actuation systems and an automatic control device and is intended for performing combat missions or comprehensive support missions both with man's direct involvement as well as with a wired-in instruction. This definition points to a greater extent than others the possibility of categorizing military robots as military equipment. Thus their division by type also can be subordinated to general principles of classification of equipment: combat, combat support, special- technical support, and logistic support robots.

Soviet experts noted that robotized equipment which takes a direct part in combat operations and serves to damage enemy personnel, equipment, and other targets should be included among combat robots. It is presumed that these will be robotized tank, antitank, missile, air defense, and low-power and medium-power laser weapon systems as well as direct and indirect fire artillery systems, attack drones, and remotely controlled helicopters. Combat support robots are intended for creating favorable conditions for conducting combat, for effective use of weapons, and for warning of surprise enemy attacks against troops. They will be used as automation equipment in all kinds of reconnaissance, engineer and chemical support, EW, and security units and subunits. This class can include remotely controlled reconnaissance-weapon complexes; small robotized vehicles for simulating column movement; water obstacle reconnaissance robots; radiation and chemical reconnaissance robots; robotized EW; mine-clearing, obstacle clearance, and smoke-screening equipment; patrol robots; and so on.

According to Soviet experts, robots performing functions of keeping military equipment in a combat-effective condition and of rapidly restoring or repairing it in

case of malfunction or damage are intended for special technical support. Armored recovery vehicles, diagnostics equipment, and robotized prime movers should be included among such equipment. Measures aimed at satisfying the material, transportation, and other needs of the troops can be performed by logistic support robots. The use of robot-loaders and fuelers in these areas as well as devices for loading units of fire and feeding artillery rounds significantly increases the effectiveness of this work and helps free up a considerable number of personnel for accomplishing other no less important tasks that demand a person's intellectual abilities to a greater extent.

Soviet experts noted that despite certain differences, and not just in name, all military robots are united by a degree of automation; i.e., by a certain method of their control. An analysis of work done in this area permits the conclusion that military robots can be divided arbitrarily into two groups: remotely controlled and automatic. If the main portion of military-technical actions is programmed and done automatically and the human operator only specifies a particular program or intervenes in control in critical cases, then we are dealing with remotely controlled robots. They are divided into two kinds: with supervisory and with interactive control. In supervisory control the operator breaks the initial task into parts which can be performed autonomously and controls the robot in the pointing mode. Here the automated actions in each intermediate task can be done by wired-in instruction or with adaptation.

According to Soviet experts, the interactive method is the highest form of remote control. The robot not only executes commands, but also evaluates and predicts the consequences of each of them and "advises" the operator. The person makes final

decisions and further control is exercised in a supervisory mode. In performing combat missions, robotized equipment has remote communication with the human operator first of all for displaying the situation and its actions on his panel and secondly for independent execution of all prescribed actions through supervisory or interactive control equipment. In cases where it is impossible or inadvisable to program and automatically execute certain jobs, combination systems with machine and manual remote control are used; i.e., everything that is possible to realize in software for machine actions is programmed, and either a copying or semiautomatic remote control system is additionally connected for performing the other jobs.

In the opinion of Soviet specialists, the existing technological base facilitates the development of remotely controlled vehicles for the needs of the Ground Troops. Their wide-scale introduction for accomplishing combat and specialized missions will not crowd out, but merely supplement other kinds of military equipment; will increase the firepower, striking power, and maneuverability of subunits and units; will influence methods of employing means of warfare; and will require qualitatively different troop actions on the battlefield. As for robots functioning under a program, their difference from remotely controlled robots lies in control and monitoring methods.

While the active work of the latter can be disrupted through loss of contact between operator and machine, the former are devoid of this shortcoming. They are independent and can perform prescribed actions independently and quickly. In addition, they are distinguished by effective coordination of actions in performing a combat mission. But automatic robotized equipment can be used on a limited basis for

now, particularly as strike and reconnaissance-strike drones and equipment for accomplishing logistic support missions.

Soviet experts also noted that the work of creating military robots presently is aimed at developing those elements which would supplement existing equipment with rather limited capabilities and would be capable of performing certain human functions under emergency conditions of a combat situation. Further explorations are oriented toward increasing this equipment's autonomy by "intellectualization;" i.e., realization of ideas of artificial intelligence. The results of incorporating achievements in this area will determine future prospects for creating and using autonomous robotized military equipment.

RUSSIAN VIEWS ON MILITARY ROBOTS

According to Russian military scientists, the robotization of military systems is a major trend affecting the development of combat operations.[82] In practice this direction is being realized by creating unmanned military equipment capable of intensifying the battle and reducing the scale of personnel participation and losses. In the first stage, employment of combat robots will merely supplement existing weapons; subsequently it may lead to two-sided, independent clashes on individual axes. An uncompromising nature, ferocity, and active operations "to the end" will be inherent to them. Appreciable successes already have been achieved in creating both air robots--drones--as well as automated ground weapons. Their advantages are obvious. For example, drones have higher maneuver capabilities and survivability compared with

[82] For example, see Colonel V.V. Krysanov, "On Features of Development of the Forms of Military Action," VM, No. 2, 1992, pp. 42-45.

manned flying craft. They can be employed in areas densely covered by air defense weapons, in centers of radioactive contamination, and under various visibility conditions. In time they may become the primary offensive air weapon (see Figure 10).

According to Russian military scientists, the transition from human-operator systems to military robots cannot be accomplished in one leap. Hybrid military systems (human-operator systems + robotic devices) will be created first.[83] One specific feature of military robotics is that it includes automatic (non-programmable) equipment, machinery without crews (BEMSs), military robotized systems, and military robots. The machinery without crews is military hardware on which a crew is lacking entirely on the mobile vehicle, with the crew located at a specially equipped control point. A robotized system is understood to mean any previously known military hardware, one or several of the operations of which has become robotized by virtue of its modernization and improvement.

The machine systems without crews could be synthesized from the standpoint of contemporary systems theory using various methodologies. Individual technical solutions at the contemporary stage of robotics development are teleBEMSs, autoBEMSs, and robotoBEMSs, which are specialized technical hardware that is synthesized according to the methodology of remote control, automatic control, or robotic control respectively.

---

[83] Colonel A. Averchenko, V. Kuleshov, and B. Kononykhin, "Robotization of Armaments," TV, No. 3, 1993, pp. 34-37.

Principal Spheres of Application of Military Robots and Robotized Systems

General purpose	Combat	Combat support	Engineer support	Rear and technical support
Identification and monitoring of state of environment	Defeat of targets	Performance of reconnaissance (radiation, chemical, biological and tactical)	Engineer reconnaissance of terrain and water obstacles	Tactical and technical support
Performance of transport operations	Patrolling in areas of special objects			
Performance of manipulation operations	Performance of protective and guard functions	Surveillance, detection and target designation	Emplacement of minefields and clearing of lanes in minefields	Evacuation and repair
Improvement of systems for servicing various assemblies and units		Reconnaissance of means of electronic warfare		Transporting of freight and ammunition
		Detection of wireline communications and command and control	Clearing of routes, digging of trenches and excavations	
		Laying of smoke screens	Support of crossings	

FIGURE 10

The functions of observation, work, and movement are dimensional degrees. The concept of a "robotized system" may be interpreted with a regard for the foregoing. A robotized military system is a hybrid technical device (teleBEMSs, autoBEMSs, robotoBEMSs), one or several dimensional degrees of which can be partially or entirely robotized.

The predictions of the American Robotics Institute state that only robotized military systems, and not military robots, will be incorporated into the armies of all countries before the year 2000, with the most preferred areas of robotization being means of reconnaissance, mining and mine-clearing, transport, and various self-training systems.

Russian experts also claim that a number of programs are being implemented in the West for creating ground combat robots. The United States already has created the Prowler reconnaissance robot; Robotic Ranger and Demon robotized antitank mounts; and remotely controlled tanks which will be effective for operations under special conditions (on contaminated terrain, on likely avenues of tank approach) or in the first line of attacking combat formations, for reconnaissance in force, and for conducting dummy attacks, as well as in ambushes, on a line of fire positions, in negotiating minefields, and so on. Consequently, a conclusion can be drawn about the possibility of establishing a new form of combat operations--"robotized battle."

According to Russian military scientists, the Gulf War served as a powerful stimulus to the development and creation of weapons using new technologies. It is therefore planned in future units, formations, and large formations of NATO ground

troops to have a significant number of combat robots, which can be formed into subunits and even units. Even now different options are being elaborated for the employment of a group of combat robots of an army corps, which will drastically enhance its combat capabilities by robotizing the ground and air weapons systems -- specifically, by using automated systems of directed-energy weapons. But for the immediate and short-term future, the army corps will continue to be the main operational formation of many NATO nations.[84]

The concept of a crewless combat vehicle specifically intended for the protection of important targets and for patrol was incarnated most clearly in the American Prowler combat robot. It has combined control, is executed on the chassis of a six-wheeled off-road vehicle, and is equipped with a laser range-finder, Doppler radar, night-vision instruments, and three television cameras (one of which can be raised on a telescoping mast to a height of 8.5 meters), as well as other sensors that make it possible to detect and identify anyone breaching a secured zone. The information is processed using an on-board computer, and programs for the autonomous movement of the robot along a closed routing are stored in its memory. The decision to destroy an intruder is made either with the help of a computer (in autonomous mode) or by an operator (in remote-controlled mode). The information in that case comes to the operator on a television channel from the three television cameras, while the control commands are transmitted by radio. It must be noted that the elements of interactive (dialogue) control of the remote-control system of the robot are used only to perform diagnostics on its systems,

[84] For example, see Moscow Conversations, May 1993.

for which a special monitor is installed for the operator. The Prowler is also fitted with a grenade launcher and two machineguns.[85]

Reconnaissance functions are entrusted to all models of crewless combat vehicles. The "Temporary Regulations for the Use of Radio Tanks," which define the procedure for the use of the B-4 minitanks, indicated two reconnaissance functions in particular: reconnaissance of enemy defenses in the offensive zone of a tank formation by means of drawing fire and revealing mines, and reconnaissance of terrain in order to establish its traversability (swamps, steep slopes, depressions, antitank ditches etc.).

Special crewless combat vehicles employed only for reconnaissance purposes appeared in the 1980s. They included the TMAP (United States), Commando Scout (United States), ARVTB (United States), ALV (United States), and ROVA (Great Britain) combat reconnaissance robots, among others. The four-wheeled, small (mass of 270 kg) TMAP crewless remote-controlled vehicle performs reconnaissance at any time of day using television cameras, night-vision instruments, and acoustic sensors. It is also fitted with a laser target-designator.

The Commando Scout is a wheeled vehicle with combined control using thermal-television cameras, various sensors, and manipulators for controlling movement. Commands come from a command-and-control vehicle accommodated on a prime mover and trailer when in remote-control mode, and from three on-board computers using digital maps of the terrain when in autonomous mode.

---

[85] Colonel V. Litvinenko: "Crewless Combat Vehicles: From the Past to the Future," ZVO, No. 1, 1994, pp. 24-28.

The ARVTB crewless combat reconnaissance vehicle was created on the basis of the M113A2 armored-personnel carrier, and has a navigational system and technical surveillance equipment in order to perform its functions. Like the Commando Scout, it may operate in two modes -- remote-controlled (with transmission of commands by radio), and autonomous.

One specific feature of the ROVA combat robot is the use of a television channel for remote control. Two types of control are used in all of the reconnaissance operations indicated above: supervisory remote control is used in the remote-controlled mode (according to generalized commands of the operator, including speech), and adaptive control -- with a limited ability by the robots to adapt to changes in the external environment -- is used in the autonomous mode.

The ALV reconnaissance vehicle is more advanced. In its initial stages it had a system of program control with elements of artificial intelligence which have subsequently been incorporated into the control system; this has provided greater autonomy in the performance of combat tasks. The "intellectualization" was first applied to the navigational system. The navigational system allowed the ALV vehicle to cover independently a distance of one km as early as 1985. That movement, it is true, was accomplished according to the principle of automatically holding it in the middle of the road, using information from a terrain-scanning television camera.

A color television camera and acoustic sensors of objects located nearby, as well as a laser scanning device with precise measurements of the range to obstacles and the depiction of their three-dimensional positions, are used as sensors of navigational

information in the ALV vehicle. American specialists hope that the ALV will be able to select independently an intelligent route of movement across rugged terrain, skirt obstacles and, where necessary, alter the direction and speed of movement. It will become the basis for the creation of an entirely autonomous crewless combat vehicle able to perform other tasks as well as reconnaissance, including the defeat of enemy weaponry using various weapons.

It should be noted that the term "fully autonomous operation" is, strictly speaking, a hypothetical one, since even the most advanced autonomous combat robots should have remote control, so that it is at least possible to turn them on or off (or destroy them) in emergency situations when their behavior does not correspond to the assigned task or poses a danger to interacting subunits.

The concept of the integrated utilization of crewless combat vehicles was further developed under the RCV ("Robotized Combat Vehicle") program. It envisages the creation of a system consisting of a command-and-control vehicle and four robotized combat vehicles that perform various tasks, including the destruction of targets using antitank missiles.

More powerful weapons, and in particular a robot tank, are being created abroad in conjunction with the light, mobile weapons-platform robots. This work has been underway in the United States since 1984, with the gear for the receipt and processing of the information moreover manufactured in modular form, which allows any conventional tank to be converted quickly into a robot tank.

Many crewless combat vehicle projects in recent decades have led "Western specialists" to the conclusion that the standardization of their assemblies and systems is essential. This pertains to the chassis and to the movement control systems. The versions of crewless combat vehicles being tested now do not have a clearly defined, dedicated purpose, but are rather used as multipurpose platforms on which both reconnaissance gear and various types of weaponry and equipment may be installed. These include the aforementioned Robotic Ranger, ALV and RCV vehicles, as well as the RRV-1A vehicle and the Odex robot. The latter is a walking platform that has six legs, with the movement of each supported by three electric motors, controlled using a central processor and six microprocessors (one for each leg). The width of the robot varies from 540 to 690 mm and the height from 910 to 1,980 mm when in movement. The remote control is accomplished by radio channel. Reports have appeared that a version of a robot has been created on the basis of this platform that can operate both on the ground and in the air. The robot moves in the first instance using the legs, and in the second has special blades that provide for movement similar to a helicopter.

All of the contemporary crewless multipurpose platforms, regardless of the type of movement, are designed as semi-autonomous robots. A trend toward reducing remote control (primarily of the digital type) to a minimum is distinctly noticeable. The platforms are thus equipped with information and measuring systems that contain a large number of sensors of various types (acoustic, infrared, television, laser), an on-board computer, and actuators. All of the equipment is being improved constantly through the incorporation of the latest achievements in the field of artificial intelligence, as well as fast-acting fifth-generation computers. Although the contemporary level of development of the means of artificial intelligence does not permit the creation of an

entirely autonomous robot by the end of this century, specialists are optimistic regarding the prospects for the future robotization of the battlefield.

"NANO-TECHNOLOGIES"

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.[86] 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.[87] Speaking at the 2nd Russian conference

[86] "Military Reform is in Earnest and for a Long Time," (Roundtable on Military Reform), AS, No. 1, 1995, pp. 34-50.

[87] "Neurocomputers May Cause 'Revolution' in Military," Interfax, 14 February 1996.

"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.

IV. PSYCHOLOGICAL OPERATIONS AND WEAPONS

RUSSIAN VIEWS ON PSYOPS

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.[88]

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

---

[88] For example, see Mary C. FitzGerald, Transcript of Conference with Russian General Officers October 1994 (Hudson Institute Report, January 1995).

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."[89]

Psychological operations represent propaganda activity and psychological actions. In this case propaganda is systematic, purposeful dissemination by varied means of communications and information of specific ideas, with the goal of

[89] Lieutenant Colonel K. Polyakov, "The War for Minds (Psychological Operations and Countermeasures)," MS, No. 4, 1993, pp. 58-63.

influencing the opinions, conditions, feelings, and conduct of the targets of influence in order to achieve direct or indirect benefits. Here, if an objective source of received information is indicated, they talk of "white" propaganda, if the source is not disclosed -- "gray," and when it is a spurious source -- "black" propaganda.

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.

Psychological operations on any level are carefully coordinated in regard to place, time, and mission and are coordinated with the combat plans of the command element of the troops and forces being supported, while providing mutual support and flexible reaction to a changing situation. They are carried out by special forces--psychological operations units and subunits, which form specialized formations to carry out specific missions. PSYOP organs are manned by qualified psychologists, technical specialists, artists, journalists, linguists, etc. All of them undergo special training and retraining at centers where they also organize courses in the principles of PSYOPs for commanders and staff officers.

Depending on the vulnerability (soft spots) and receptivity of the targets of influence and the missions being executed in psychological operations, a selection is made of the appropriate theme, which includes the content and orientation of the measures being carried out to achieve the goals of psychological influence. The theme is the connecting link between the vulnerable aspects uncovered by intelligence and the

nature of the conduct of the targets of interaction on whom it is necessary to exert the appropriate influence. As a rule, the theme of psychological operations is realized in two ways -- causing a schism between certain categories and groups of people, and instilling the inevitability and naturalness of the predicted development of events.

For example, in the course of the psychological operations conducted by the Multinational Forces against Iraqi forces, especially in the concluding phase of the war, broad use was made of leaflets urging surrender. The leaflets were not of a threatening nature and showed an amicable attitude toward those who surrendered. The goal of the leaflets was to convince enemy servicemen that such a step was fully natural in the situation that had developed and was not shameful. In this case the necessity of a choice -- "either surrender or die" -- was not emphasized. This permits avoiding a challenge which touches on a man's honor, when the responsive reaction often is: "death is better than the open display of fear and submissiveness."

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.

At the same time the methods of psychological influence also include assisting friendly local authorities and inhabitants and staging insurgent operations, strikes, sabotage, civil disobedience, mass rallies, demonstrations, marches, etc. For example, in the course of operations Desert Shield and Desert Storm the PSYOP units of the multinational forces disseminated more than 20 million leaflets, transmitted broadcasts of six radio stations around the clock in the frontal zone, and made intensive use of loudspeaking systems. To disseminate printed matter, the U.S. Marine Corps made broad use of American and British airpower in addition to artillery. And the complexities of relations between the authorities and Kurds and other ethnic and religious groups were not ignored. Thus, psychological operations represent a complex of measures conducted with the goal of exerting psychological influence on the consciousness, feelings, will, convictions, and conduct of the opposing side.

Achievement of the specific goals of psychological influence is accomplished by a number of methods of suggestion and persuasion. And the effect of suggestive influence is determined first of all not by the content of the information, but by its external form, expressiveness, emotional tinge, and also by the authority of the source. Because suggestion is based on low critical perception, its effect is reckoned on weak activism of understanding and the absence of logical analysis. The basic methods of suggestion include:

- Statements presented as indisputable facts;
- Using comparative materials;
- Selecting arguments to strengthen or weaken statements;
- Fragmentation and speed in presenting a large number of reports;
- Giving out doses of negative and positive elements;
- Repetition of slogans, catchwords, and stereotyped phrases; and
- Creating dissatisfaction.

A special place among PSYOP methods is occupied by rumors. They become an effective means of psychological influence, especially in crisis situations, the extreme manifestation of which is armed conflict. The goal of rumors is to sow distrust, compel one to doubt, lead astray, confuse, etc. And though the effect of using false information, as a rule, is of a short-term nature--mainly in the period when propagandistic influence is accomplished under conditions of a shortage of information, and the receipt of more complete and authentic information has not yet led to the fact that a lie "has come to the surface" -- even the temporary creation among the targets of influence of some wavering, uncertainty, doubts, etc., can have an effect that is sufficient to achieve the goals of specific psychological operations.

From the above it follows that an invariable condition of the successful execution of combat missions by a unit, large formation, combined-arms formation, or a large force is maintaining a stable morale-psychological condition among personnel. A most important orientation in this work should be counteraction against the enemy's psychological measures with the goal of not allowing disinformation or reduction of the morale-psychological condition of troops (or forces).

The success of counteraction against enemy psychological operations is achieved:

- by the activism and clarity of one's own interests (standing up for the interests of one's own country and one's own people), by the promptness of work pertaining to problems which arise in the course of executing combat actions and operations and their support, and also by disseminating preemptive information;

- by the regularity of the collection and analysis of information on the morale-psychological condition of personnel and by dynamic and efficient reaction to a change in the situation, conditions, and nature of events;

- by the resourcefulness and simplicity of the arguments, proofs, and evaluations used; and

- by the emotional saturation of the measures which are carried out, with a combination of the rational and the emotional.

At the same time, the effectiveness of countermeasures will be greater of they are carried out with due consideration of certain psychological recommendations:

- explain to the troops the goals, methods, and techniques of the enemy's use of propaganda and the psychological actions and operations undertaken by him, in order to form foundations for the critical perception of these activities;

- acquaint servicemen with facts that illustrate the mendacity and refinements of the procedures and methods used by the enemy with the goal of psychological suppression of the individual and group consciousness of the opposing troops (or forces);

- execute one's own psychological operations aimed at enemy troops, the local population, interned civilians, and prisoners of war;

- reconnoiter and destroy enemy psychological operations units and the technical facilities for executing the operations;

- predict the trends and themes of enemy psychological actions with the goal of deterring them and thereby neutralizing or reducing their effectiveness;

- monitor collective and public opinion of the servicemen of one's own units and formations with the goal of exposing the degree of the enemy's psychological influence on them, evaluate the degree of vulnerability (or susceptibility) of one's own troops to enemy propaganda and psychological operations, forecast the danger of the consequences, and plan the amount of work to counteract these measures; and

- form a negative attitude toward everything that comes from the foe. But a gross error is committed by anyone who categorically and without reasoning talks about the negative peculiarities of the enemy. This is perceived as a sign of exasperation and an unwillingness to look truth in the eye, and a sign of a clear lack of knowledge of the real traits of a specific enemy. An objective evaluation of one's own successes and failures and a refusal to embellish the actual state of affairs are most important conditions for achieving the goal of counteracting enemy PSYOPs.

According to Russian military theorists, an analysis of the military-police actions of recent years shows that information-and-propaganda support for troop operations is gaining more and more significance. One direction of information warfare -- direct influence on the enemy -- has been known from time immemorial, and is widely employed in all contemporary conflicts. The appearance of another is connected with the formation of a worldwide information expanse in the 20th century, and the increased influence of public opinion on the extent of freedom of governments.[90] The aim of the actions conducted in this area is a dual one: to prove that the opposing side

[90] Sergey Grigoryev, "The Chechen Operation in Light of Others Like It -- A Comparative Analysis of One Type of Military Conflict," Nezavisimaya gazeta, 21 June 1995, pp. 1, 3

is a mob of scoundrels and inveterate criminals, and simultaneously to present the actions of one's own side as forced measures to protect liberty, the constitution, law and order, etc.

Such campaigns have been waged with varying degrees of success by all initiators of military-police actions in recent years. This is associated to a considerable extent with the fact that as opposed to a large war, such actions are not always unequivocally supported by one's own population and the world community. Considerable efforts were required, for example, for the number of Americans who approved of the Gulf War to grow from 10 percent of the population in September 1990 to 80 percent in January 1991.

The operation against Iraq is in general an exceedingly interesting example of a battle for public opinion. The work with journalists was done according to specially developed programs. Only correspondents accredited with the MNF command who had signed obligations to observe specified norms regarding the nature and content of their reports were permitted into the field. Only specially selected servicemen gave interviews. All of the material was censored. The need to reduce information about dead and wounded to a minimum was emphasized. The air time granted to opponents of the war was limited. There were slip-ups, of course. Information on the large quantity of hospital ships or the shipment there of several tens of thousands of plastic body bags (the expected MNF losses were 30,000 people) had a negative impact. There is an example of negative information of another sort as well -- journalists dug up information that children of only two of the 535 congressmen, and none of those of the president's cabinet, took park in the Desert Shield operation, while the children of

74 congressmen fought in Vietnam (that statistic is unfortunately lacking for other, similar conflicts). The system operated without a hitch as a whole, however, since there was an enormous flow of information favorable to the MNF command and the leaders of the United States in the area of the conflict. The negative aspects of the conflict were drowned in cheerful reports on the successes of American weapons. And it did not matter that some of the most effective frames (contemporary weaponry is very telegenic) were shot on test ranges and not in the Persian Gulf.

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.[91]

What are the special formations responsible for the direct organization of information-and-propaganda support? Above all, they are public relations (press

[91] Colonel N.D. Plotnikov, "Information-and-Propaganda Support of Operations and Combat Action in Armed Conflicts," VM, No. 1, 1996, pp. 64-70.

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.

What should be the principles of organizing information-and-propaganda support? Analysis of the work by foreign and domestic press services of the power (military) structures points to the main principles of their operation: persuasion, taking the lead in breaking news over the opposing side, using reliable facts, and supplying the requisite information in a prompt and efficient way.

As regards the actual coverage of armed conflicts by the media, it is essential to work out in advance rules for the journalists, laying down norms of conduct in various situations. In particular, the rules should envision non-disclosure of sensitive information; oversight by the power ministries' information agencies of the reports filed to media organizations; and banning the arbitrary interpretation of facts, one-sided commentary, playing up instances of violence and atrocities, and discrimination on ethnic or religious grounds.

This can lead to a legitimate question: Why should the journalists' activity related to the coverage of armed conflicts be regulated by any additional rules? After all, there are corresponding state-level normative enactments, while society has the right to know everything that affects its interests, moreover its security. The sad statistics of armed conflicts show that their coverage, especially operations to localize inter-ethnic or inter-command clashes, calls for the utmost circumspection, balance, and objectivity. False, unverified information, and attempts at sensationalism can engender events with unpredictable consequences, and result in the death of military servicemen, law enforcement officers, and civilians.

In this context it appears that a normative document (presidential edict of governmental resolution) on the conduct of an operation based on the use of force, if it does not envision the imposition of a state of emergency, should necessarily contain a provision whereby all materials transmitted from the conflict area should be monitored by state agencies. Furthermore, before the operation begins, it is advisable to hold a joint meeting between the troop command and the chief editors of the main media organizations, newspapers, radio and television networks, and leading anchors and commentators to explain the possible negative socio-political consequences of the violation of the established order for covering events in the media. It is desirable that such a meeting be conducted by the Security Council secretary on authority from the country's president or by the chief of the Russian Federation government press service on authority from the prime minister.

In the operational zone it is essential to create, in advance, a press center under the troop command. Experience shows that it is advisable to assign it the following

tasks: regular briefing of media representatives on the progress of the operation, and on events and facts that can attract public attention; preparation of regular media surveys for the force commander, covering the activity by the relevant armed units; assistance to journalists in an objective and timely coverage of the course of combat operations (which will help to rule out the spread of biased information, capable of producing a negative impact on the servicemen's morale); briefing the servicemen about the situation at home; and coordination of activity by teams of media workers arriving in the area to cover the operation. Journalists wishing to comment on the operation will first have to receive accreditation at the ministry's press service whose chief is appointed by the federal force commander (after a corresponding check by counterintelligence agencies).

It is advisable to send media representatives to the zone of action as part of already formed teams with the transport facilities provided by the ministry responsible for the operation. The teams should not be very large: from four to six people. The teams should be accompanied by a representative of the press center (public relations center) from a corresponding power department. His functions should be as follows: selection, in coordination with the command, of material that should be covered in the interests of ensuring an early termination of the conflict; screening the earlier shot video footage or photo material; and organization of interviews with conscripts and officers. In the latter case it is key to observe the following conditions: only facts must be discussed, and there must be no speculation or discussion on moot political issues. These requirements are binding on everybody -- from soldier to general. In order to avert misunderstanding in the future, it is expedient to copy audio and video material and to keep it until after it has been used in the media.

The main methods of information-and-propaganda support can be as follows: press conferences and briefings by the command for media representatives; radio and TV addresses by commanders for the civilian population; censorship of media material coming from the conflict zone; identification of individuals spreading rumors, literature, and audio and video material deliberately compromising military servicemen, fomenting ethnic and religious discord, calling on soldiers to disobey their commanders' orders, and so forth; discrediting the leaders of extremist, nationalist, and criminal groups, debunking their political programs and slogans; and encouraging the members of illegal and armed formations to stop their illegal activities.

"REFLEXIVE CONTROL"

Among others, General-Major M.D. Ionov has stressed 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.[92]

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,

[92] General-Major M.D. Ionov, "On Reflexive Enemy Control in a Military Conflict," VM, No. 1, 1995, pp. 46-50.

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.

It is very important to make sure that the enemy has a shortage of time for making and executing decisions. An element of surprise produces a strong psychological impact; it not only disturbs the chosen algorithm of decision-making and reduces the effectiveness of the control system, but also forces untimely, insufficiently prepared actions and upsets its plans.

Enemy control is based on the transfer of information to the enemy which would stimulate it to make decisions objectively beneficial (desirable) to the "controlling" side. The following methods can be used to this end: power pressure; presentation of information about the situation for decision-making; presentation of information for the enemy to define a new target of action whose accomplishment requires additional preparation, assets, and time; transfer of information with the aim to upset the algorithms of addressing control tasks accepted by the enemy; and impacting on the moment of its decision-making.

The power pressure methods can be as follows: the employment of superior force; the demonstration of force (force blackmail); "psychological attack;" the demonstration of an actual grouping, installation, or weapons; the ultimatum; the threat of use of force (sanctions); the threat of risk (focusing attention on irrational conduct, on delegating powers to an irresponsible person); reconnaissance in combat;

provocative maneuvers and weapon tests; denying the enemy access to a certain area or isolating it; putting troops on a higher alert status; forming military unions; the official declaration of war; support of internal forces destabilizing the situation in the enemy rear area; a limited strike in order to put part of its forces out of action; exploiting the victory; demonstration of express ruthlessness in action; a show of mercy toward an enemy ally which has stopped fighting; and so forth.

The methods of presenting information about the situation include concealment of installations and groupings (a show of weakness in a strong place), positional victims (abandoning one position in order to reinforce defenses on another, luring the enemy under a prepared strike: the "fire pocket"), the show of one installation under the guise of another (camouflage, disguise), the "Trojan horse" technique (leaving dangerous objects on positions), a demonstration of nonexistent relationships between installations or the concealment of a true relationship, keeping new weapons in secrecy or "armament bluffing" (a demonstration of mockup models of nonexistent combat hardware, with corresponding reports in the press), changing the operating mode, deliberate loss of critical documents or transfer of information in a code known to the enemy, and so forth.

There are several measures for forcing the enemy to assume a new target of action. These are conflict escalation or de-escalation (gradual control of its intensity); deliberate demonstration of a particular chain of actions, based on surprise; strike on the enemy base when the enemy is outside it; acts of subversion and provocations; leaving a route for the enemy to withdraw from encirclement; and measures forcing the

enemy to take retaliatory actions involving a substantial expenditure of forces, assets, and time.

The enemy decision-making algorithm can be influenced, for instance, by a systematic conduct of games that are perceived to be standard plans; by publishing a deliberately distorted doctrine; by delivering strikes against control system elements, including the "hunting" for key figures; by transferring false background data; by operating in a standby mode; and by taking actions to neutralize the enemy's operational thinking (working out such plans of action whose aim and concept cannot be uncovered, at least until the final stage of the operation; and creating a situation wherein a large number of equally possible options can be expected in actions by the "controlling" side, with each of them being critical in terms of expected damage, and calling for effective efforts to counteract it). The enemy can be forced to change the moment of decision-making in the following manner: by unexpectedly starting combat actions; by transferring to it information about the background to an analogous conflict so that the enemy, having worked out what it regards as a feasible forecast of the situation, must make a hasty decision, sharply changing the mode and character of its operation; and so forth.

Actions to control the enemy are aimed at a concrete personality or group of persons with a particular psychology, way of thinking, and professional preparation level. Two approaches can be used in this process: universal and role-based. With the universal approach, impact on the enemy consciousness is produced via a number of universal human psychological motives, in correspondence with the hierarchy of their force. These motives can be as follows: the need to avoid danger, the unwillingness

to "enter a fight" or to "do the dirty work for somebody else," orientation toward confrontation no matter what ("this may be bad for me but then you will not get away easily either," "after me, a deluge"), and so forth. With the role-based approach, it is not the possible motives of action that are analyzed but the role which is played by a particular person or a group of persons (claims to an exceptional role in history, leadership or, quite the contrary, the position of a subordinate coalition partner, and so forth).

The variety of approaches affects the choice of means and methods of impact as well as the style and order of information transfer. Measures can also include those which evoke a chain reaction of dissemination (false rumors, panicky appeals, and so forth). This makes it important to analyze not only the veracity and the reliability of the information source but also the possible motives for its disclosure, especially in using unconventional channels (indirect or neutral) and forms of information transfer. Noteworthy in this respect is "silent bargaining," when the conflicting sides express their consent through their conduct.

The regularities of reflexive enemy control arise from the basic laws of control, psychology, human thinking, and societal development. Russian military theorists single out a number of propositions among them. First, the content of methods used, and their combinations, is conditioned by the regularities and internal interrelations of the process of thinking and psychology, while the form of their implementation depends on the arsenal of technical means used in the conflict. Second, the more persistently the "controlling" side seeks to convince the enemy about the reality of its aims and

intentions, the more realistic the means employed should be; the more forces, assets, and time will be needed to undertake corresponding activities.

Third, powerful technical systems, after reaching a critical threshold of force, cease to be a means which can be used for controlling the enemy. Fourth, the technical revolution in the military sphere brings forth new methods and techniques for weakening the enemy, for instance, by forcing it to allocate substantial expenditures of assets and time to analyzing, controlling, and effectively neutralizing the activity by the "controlling" side. Even the mere analysis of such programs as the "Strategic Defense Initiative" calls for considerable expenses on scientific, research and development work, experiments, and tests on the part of the "controlled" side.

Fifth, in choosing options for controlling the enemy, it needs to be taken into account that owing to differences in aims as well as political and ethical approaches toward choosing methods and ways of achieving them, the internal appraisal by the sides of the possible results of action is done according to various complex criteria, reflecting the relative character of their confrontation. Sixth, because the interests of particular states and their internal situation assessments do not fully coincide, a coalition enemy constitutes a complex system whose stability changes depending on the character of the situation, the state, condition of the parties, and their interrelations (internal assessment systems in particular countries can vary).

In a conflict between coalitions, the "controlling" side directs its main efforts toward destroying the enemy coalition. This can be accomplished by: power pressure, with real threats to particular participants in the coalition, in order to urge them to

withdraw from it; powerful strikes on the coalition leader, with no action being taken against other coalition members at the time; strikes on a weak ally to force it to withdraw from the fighting and prevent those vacillating from acting; granting exemptions and privileges to some of its participants; pursuing a flexible policy; and showing greater clemency toward a defeated coalition member which has pulled out of it at an earlier stage of the conflict.

According to Russian military scientists, all measures to mislead the enemy always pursued one goal -- to evoke a fully specific reaction and force some kind of reflex action. If the enemy "obeys" the concept of the [friendly] commander in an operation, then it is possible to speak about controlling and controlled entities, or reflexive control. According to the definition of military systems analysis, the latter consists of transmitting motives and grounds from the controlling entity to the controlled system that stimulate the desired decision. Consequently, the goal of reflexive control is to prompt the enemy to make a decision unfavorable to himself. Naturally, one must have an idea about how he thinks.[93]

Ideally, the enemy comes up with a decision based on the idea of the situation which he has formed, including about the disposition of troops and installations and about the command element's intentions. Such an idea is shaped above all by intelligence and by other factors, which rest on a stable set of concepts, knowledge, ideas and, finally, experience. This set usually is called the "filter," which helps a commander separate necessary from useless information, true data from false, and so

[93] Colonel Sergey Leonenko, "Reflexive Control of the Enemy," AS, No. 8, 1995, pp. 27-31.

on. Based on this, the chief task of reflexive control is to locate the weak link in the "filter" and find an opportunity to act on it.

In all wars and battles, military leaders attempted to outdo each other by putting the enemy in the position of the controlled system, or in other words, they tried to create for him the model of a situation favorable to themselves. But as a result one side won! That means that the level of the victor's reflexive control turned out to be prevailing. This provides grounds to compare the depth of penetration of one model into the other, determined by the so-called rank of reflexive action. Reflexive action is used to form the model of battle, but for this one must have a complete impression about the enemy.

Moral, social, ideological, emotional, personality, and other factors also have an effect on commanders' capabilities for reflexive control. But the enormous information flow which comes down on commanders requires the involvement of rather cumbersome command-and-control staffs. And the larger the troop body or scale of battle, the stronger the factor of collective decision-making both by attackers and defenders manifests itself. It is obvious that reflexive control by one collective will be directed against a similar enemy collective, its antipode.

Computers do not necessarily hamper reflexive control though they make it easier to process data and calculate options. First of all, because one commander completely believes computers and another does not. Secondly, the algorithms with which information flows are processed are written based on general theory and probably are accessible to the enemy.

There is no difference, say the Russians, in the fact that reflexive control was realized through stratagem in the past and through maskirovka in the present. The essence lies not in terminology, but in enemies' striving to interfere with each other, convince each other of the "correctness" of one's actions and prompt an erroneous decision. Formulating the goal of reflexive control begins with the question: "What enemy decision is favorable to us?" After this a reflexive control model is developed in which factors are determined which "prompt" the opposing side's command element to make the decision we need.

For example, based on a knowledge of enemy views on conducting offensive operations, it is determined that, first of all, the possibility of delivering an attack from the left against a weak spot "tempts" him. Consequently, everything necessary must be done for the concealed concentration of a grouping on the left flank and for establishing a strict maskirovka regime there. Secondly, the nature of terrain and elements of the infrastructure must give him an opportunity to employ large mechanized groupings and freedom of maneuver. With the goal of forming the opinion in the enemy of the impossibility of further use of elements of the infrastructure on other axes, that means it is necessary to simulate the destruction of roads, bridges, and airfields there and demonstrate the preparation of dams for detonation and the creation of vast sectors of obstacles. Thirdly, the "absence" or "small numbers" of second echelons (reserves) on a given axis may serve as an attractive prospect for the enemy to develop the offensive. The disposition of troops, advantages for establishing an attack grouping, as well as other factors must be taken into account here.

Sometimes, especially in the case where the enemy plan has been divined, the commander will be forced to "play up" to him by weakening or strengthening the factors cited above. This means that the decision for the operation will have to be made (or updated) with consideration of the reflexive control model. It is also not precluded that this model sometimes may become the basis of the operational concept.

Reconnaissance acquires special importance in reflexive control. It provides it with flexibility and also promptly informs the commanding general and staff about the enemy's reaction and about conformity of the chosen model to the situation at hand. Reconnaissance can play the role of the enemy by putting itself in his place for the purpose of checking and giving this model greater credibility. In addition, reconnaissance is assigned what is the most important mission -- exposing the enemy's reflexive effect.

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).[94]

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

[94] For example, see FitzGerald, Transcript.

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.[95]

[95]Lt. Col. V. Pavlychev, "Psychotronic Weapons: Myth or Reality?" ZVO, No. 2, 1994, pp. 17-19.

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.

In the opinion of "foreign scientists," the current level of development of physics, chemistry, and biology makes it possible to place the study of the bio-field on a scientific basis, which will help accomplish a number of important tasks of applied importance, including in the military field. Various sensors are used in experiments on bio-energy. They are able to register certain manifestations of the bio-field and transform them into electrical signals that are easily recorded by appropriate instruments, a large number of which have been developed recently. High-capacity computers are used to process the data. "American experts" have stated that they are close to solving the problem of controlling a person's ability to emit and receive bio-energy. Creation of technical devices for detecting bio-emissions will continue in the

United States in the 1990s, and studies of mathematical modeling of bio-energy interaction between people will develop further.

Today, there is evidence that parapsychological phenomena are real and can be controlled under certain circumstances. An attempt has been made to assess the military potential of such controllable parapsychological phenomena. Claims that psychotronic weapons already exist, although their capabilities have not yet been fully determined, are appearing more and more often in the Western press.

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.

"For the past twenty years our enterprise has specialized in manufacturing psychotronic devices for arms systems and control systems for intercontinental missiles and space vehicles," the deputy director of a Russian defense enterprise told the Moscow News weekly. Deputy director Martynov also said that his enterprise and another company, whose name he did not disclose, have begun to produce a physical amplifier (metathrone), Miranda, developed on the basis of fundamental achievements

in the field of psychotronics.[96] The weekly then conducted independent research, which revealed that work indeed had been done at the plant to produce metathrones, which are regarded as a side branch of psychotronic weapons. Such devices have long been used in the American industry to locate and establish the causes of any systemic failures. The weekly cites specialists as saying that "on September 24, 1990 an agreement was signed between the Central Intelligence Agency (CIA) of the United States and the KGB of the USSR on joint research in the field of psychotronics." The weekly said, however, that cooperation in this field has not developed.

Russian scientists note that experiments are being done in Russia in the sphere of directed non-contact electromagnetic fields in the SHF hydrogen bomb or chemical and bacteriological weapons. Psychotronic generators are capable of suppressing human willpower and imposing a criminal will. These weapons are continuing to be developed, tested on people, and improved.[97]

"Radio waves," the journal ZVO says, "can disrupt the brain and people's central nervous system. An infrasonic weapon, even at low power, is capable of generating an involuntary sense of fear and creating panic in a crowd..." The psychotronic effect is said to be the directed irradiation of people with electromagnetic fields from electronic equipment. This generates changes in their behavioral functions and their reactions to various kinds of events and situations, disrupts their functional systems, and brings about morphological changes in their cell tissue. Brick walls, concrete

[96] " 'Psychotronic Devices' Developed For Military, Space," ITAR-TASS, 24 March 1994.

[97] Andrey Ivanov, "Intelligence Official Denies 'Psychotronic Weapon' Report," Rabochaya tribuna, 5 August 1994, p. 4.

ceilings, wood, and other materials and structures can be "transparent" to electromagnetic radiation of a certain wavelength and strength.

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."

It is particularly easy to identify people with diseased organs, and even easier if they have a number of diseased organs which together provide certain pain reactions in the shape of frequency characteristics. Identification can even be done over incredibly long distances by using a telephone, TV, or radio communications system in conjunction with a satellite system for transmitting the data with the help of

extrasensory influence. This, for instance, is how an electronic fingerprint differs from the physical variety, which requires the person in question to be arrested. It is this BED capability that makes it possible to develop systems to carry out a search for people with certain radio-wave frequencies.

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.

There was once a great deal of talk about the "radioson" hypnoradiation source. This device is capable of putting people to sleep from a long distance away. But this is far from its entire range. It can also be lethal -- causing cell degeneration, cancer, radiculitis, and paralysis. It is just a question of the exposure time and the density of the waves directed at the target.

Here the Russians include infrasonic acoustic devices. The principle of their operation lies in the fact that, for example, special acoustic emitters near a group of hostages and terrorists are used to create a powerful field of infrasonic frequencies that are inaudible to the human ear, but are sensed well by its body and cerebrum. If the terrorists lose self-control as a result, individual means of pressure can be used. But infrasonic acoustic devices are very complex and cumbersome systems, though working to improve them can be of benefit in fighting terrorism.[98] For the present there are preconditions for creating quite effective physiological weapons. Their use should lead to a temporary, but completely restorable disturbance of certain physiological functions of the human organism which can also sharply reduce the activities of terrorists.

[98]Interview with Vladimir Alekseyevich Vasilyev, "If Budennovsk Were Abroad... (Foreign Trends and Experience in Combatting Terrorism)," Granitsa Rossii (hereafter cited as GR), July 1995, No. 25, pp. 12-13.

V. NATURE OF ELECTRONIC WARFARE (EW)

SOVIET VIEWS ON EW

The Soviet vision of future war included a focus on the growing role of electronic warfare (EW) in modern combat operations. In a 1990 Military Thought article, for example, General-Major I.N. Vorob'yev noted that the dialectic of offensive and defensive means is assuming new forms. Now it encompasses not only ground space, but also air-space on a wider scale by invading the spheres of weapons control and command and control in the form of a "struggle over the airwaves."[99] Other theorists stressed that the electronic suppression of reconnaissance and fire-control electronics now assumes one of the central roles in the system of struggle for fire superiority.[100] Intelligence and EW were thus viewed as "an independent component of the operation or battle: an independent form of combat operations."[101]

Soviet military assessments of the Gulf War likewise focused on the significant role of electronic warfare in the coalition's victory. For example, General-Major G. Zhivista of the General Staff's Center for Operational-Strategic Studies gave major credit for allied successes to the comprehensive use of ground- and air-based electronic

[99] General-Major I.N. Vorob'yev, "Questions of the Theory and Practice of a Mobile Defense," VM, No. 9, 1990, pp. 34-40.

[100] Shishkin, "Fire Superiority."

[101] Krysanov, "Ground Forces."

countermeasures in the air operation.[102] General-Lieutenant V. Gorbachev noted that the decisive factor in the success of allied air operations was American EW systems, which overwhelmed Iraqi C^2 in the first few minutes of the air operation.[103] According to General Slipchenko, the United States used EW as an integral element of air-land battle -- not as a support to it.[104] In praising the skill of the U.S. EW capability against Iraq, General-Major N. Kostin of the General Staff Academy called EW "the technical basis of modern combat."[105]

According to Soviet Air Defense officials, the Gulf War differed from any other because EW played a very special role in it. "If we do not work in advance to counter EW systems," they noted, "they can nullify some air defense systems entirely."[106] General-Major Bazhenov argued that combat operations are "virtually impossible" today without EW systems -- even at the division level.[107] Indeed the achievement of "command of the airwaves" was said to have permitted the achievement of "command of the air."

---

[102] General-Major G. Zhivista, "How Professionals Wage War," Izvestiya (hereafter cited as IZ), 19 January 1991.

[103] "Gorbachev, "Tanks."

[104] Slipchenko, "Impending Changes."

[105] N. Burbyga, "Ground War Inevitable," KZ, 8 February 1991.

[106] Falichev, "Shilka vs. B-52."

[107] Bazhenov, Presentation.

Soviet experts also argued that owing to the massive use of EW equipment under a unified plan, the MNF succeeded in achieving total tactical surprise in the initial stage of the conflict. The first electronic effect on selected operational axes was manifested in the "blinding" of electronic equipment of Iraqi reconnaissance and of the air defense system in order to deprive it of necessary information on intentions of coalition forces. Following this came unexpected, powerful air and missile strikes. In the assessment of military specialists, EW equipment was used on a wide scale for the first time in the history of wars, which ensured the United States and its allies of attaining surprise as well as reliably suppressing Iraq's air defense C^3I systems. According to "official U.S. military press reports," air losses of the international forces in the first month of the war were only around 30 aircraft in 70,000 combat missions.

The MNF command gave great attention to organizing EW against Iraqi air defense. Over 100 special EW aircraft were concentrated in the TVD for this purpose. In addition, essentially all attack aircraft were outfitted with individual EW equipment. Combat employment of EW personnel and equipment was thoroughly planned and conducted in strict conformity with the offensive air operation plan. Several hours before the beginning of combat operations, communications equipment was jammed, followed by early-warning and acquisition systems, fighter-control radars, and command-and-control nets. Intensive jamming was performed both from combat air patrol zones as well as from strike aircraft combat formations essentially against all Iraqi electronic equipment. In addition, special aircraft delivered strikes against key air defense targets with anti-radiation missiles. In their view, the continuous, comprehensive use of EW equipment was a deciding factor that reduced Iraqi air

defense combat effectiveness. Winning superiority over the airwaves determined the success of winning superiority in the air.[108]

According to Soviet experts, the effectiveness of EW can be evaluated by the relative losses of MNF aircraft to Iraqi air defense weapons, which were less than 0.5 percent of the sorties flown. This was achieved first by massive use of airborne EW forces, the basis of which were EF-3A, EA-6B, EC-130, and other jammer aircraft. Secondly, by wide use of air-to-radar homing missiles, which destroyed electronic equipment of Iraq's command-and-control and weapons control systems without entering the air defense kill zone. Thirdly, by stable, continuous, efficient command and control of EW personnel and equipment in all stages of their employment. Measures to disorganize command and control of the MNF on Iraq's part were conducted on a limited basis; i.e., EW was conducted essentially one-sidedly, which ensured the MNF of superiority in command and control. A preliminary analysis of the conduct of EW by the MNF confirms the stable trend which has been seen toward its development from a kind of support into a component part of warfare.

Writing in Military Thought, General-Major Lebedev and General-Lieutenant Lyutov noted that the growth in effectiveness of fire destruction in modern operations is dictated by its combination with mass suppression of enemy systems for reconnaissance and command and control of forces and weapons. Electronic warfare long ago developed from a form of operational support into an inalienable content of combat operations, and in this war it played the role of a type of attack. They argued

---

[108] For example, see Roundtable Discussion, "First Lessons of the War," VM, No. 5, 1991, pp. 60-71.

that in the future the execution of combat missions by EW equipment must be planned at operational levels of command-and-control entities. Immediate organization for combat should be conducted at the tactical level with consideration of this. In other words, organization of EW and protection against it are becoming functions of formation and unit commanders and staffs.[109]

All of this attests to a qualitatively new stage in the development of military affairs in general. Just as "motorization" changed the appearance of armies and nature of warfare in the 1920s and 1930s, 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.

Soviet naval officials have long examined the role of EW in combat operations at sea. Writing in the Naval Digest in early 1991, for example, Rear-Admiral V. Kalinin and Captain 1st Rank A. Lobanchuk noted that two directions should be singled out in examining development trends of EW in combat operations at sea: the improved organization of EW in operations and the development of EW equipment itself. Despite an overall trend toward a quantitative reduction in offensive weapons on platforms, they continued, one sees an attempt to preserve and even increase their

[109] Lebedev, et al., "Gulf War."

combat capabilities by upgrading reconnaissance, target designation, and EW systems. Three factors presently influence the organization and conduct of EW.

The first is the existing structure of the system of command and control of forces and weapons. In recent years there has been a transition in the assessment of future methods of conducting combat operations at sea from the concept of "forces against forces" to the concept of "combat systems against combat systems," in which the command-and-control system is one of the principal elements. This in turn influenced the content of EW, one of the most important missions of which is to disrupt the functioning of that system by the effect of EW equipment on electronic equipment included in the system's makeup and by a change in properties of the environment hampering the propagation of electromagnetic or other waves. This is done in combination with the use of weapons against all elements of this system.

The second factor is the sharp quantitative leap in outfitting sea and ocean TVDs with electronic equipment and electronic systems and the saturation of ships, submarines, and aircraft with them. This in turn influences the quality of that equipment's operation, which is determined not only by its technical reliability, but also by the capability to function stably under the effect of different kinds of jamming. The more electronic equipment in the system, the more possibilities there are of affecting it by EW equipment, which means the more possibilities there are of reducing the functioning reliability of the system as a whole.

The third factor is the increasing consolidation of various kinds of electronic equipment in special systems (for situation coverage, for command and control, for

issuing target designation for weapon employment and so on). Confirmation of this is the creation of a U.S. antisubmarine surveillance system (SOSUS), a space system for reconnoitering naval targets (NOSS), the global system for operational command and control of U.S. Armed Forces with the system for operational command and control of naval forces included in it, and so on. This in turn also requires a comprehensive approach to accomplishing the mission of disrupting their functioning in case combat operations begin.

The fourth factor is the increased effect of the results EW on the end result of an operation or naval battle. In connection with this, EW equipment has begun to be taken into account in assessing combat potentials of opposing groupings.

Unquestionably, the final missions of an operation, engagement, or battle are achieved by delivering effective fire on the enemy (by destroying or inflicting maximum damage on his forces), but EW is capable of considerably facilitating accomplishment of this mission by disorganizing command and control of enemy forces and weapons, reducing the capabilities of his technical means of reconnaissance, and ensuring stable operation of friendly electronic equipment. Integrated use of electronic warfare equipment is dictated by the fact that effectiveness of its action against any system as a whole is achieved as the sum of results of action against the system's individual elements (detection, command-and-control, target designation, homing, and other equipment).

RUSSIAN VIEWS ON EW

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.[110] 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.)

The "foreign press" emphasizes that along with air defense suppression, a fight against enemy battle management systems is presumed in the course of winning air superiority. In this case EW directly helps to accomplish this mission and holds a subordinate position while retaining independence. The above indicates that there is a tendency for crossover and integral confluence of EW missions with missions of winning air superiority, interdiction of a combat operations area, and close air support.

[110] For example, see Lieutenant Colonel A Vasilyev, "Electronic Warfare in U.S. Air Force Air Operations," ZVO, No. 1, 1992, pp 41-44.

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 jamming and the enemy's use of weapons; and ensuring security and decisive operations of friendly forces.

According to Russian experts, the following can be among the most important principles in organizing and conducting EW in an air operation: continuity and timeliness in providing reliable information to EW entities, units, and subunits; centralized distribution of data among EW systems and equipment; conformity of its goals, missions, and measures to the operational concept and plan; optimum distribution and rational use of limited Air Force EW resources in an operation; coordinated employment of means of electronic jamming and fire damage in combination with the maneuver of air and ground forces; and centralized direction of EW and decentralized performance of missions by corresponding personnel and equipment.

EW generally presumes several methods of operations: measures to remove friendly personnel and equipment out from under the threat of enemy action;

employment of EW personnel and equipment; reducing the effectiveness of enemy reconnaissance, command and control, EW, and air defense equipment; and its destruction by limited strikes. The U.S. Air Force command is said to believe that to achieve maximum EW effectiveness, it is advisable to use all the enumerated methods, but this does not preclude sufficient flexibility of their selective use depending on combat mission, degree of enemy threat, and available personnel and equipment.

In analyzing the employment of EW personnel and equipment in local wars and the experience of Air Force exercises, "Western specialists" have singled out four basic methods of conducting EW in suppressing an air defense system: "from a combat air patrol zone," "from combat formations," "mutual cover" ("mutual support"), and self-maskirovka. The second method is considered the most versatile.

Russian experts note that further development of S&T progress has led to overestimating the capabilities and effectiveness of passive jamming assets in support of tactical air operations. The primary methods of their employment in suppressing air defense are considered to be the "corridor," "zone," "active cloud," and "small cloud," which are intended for group, collective, and individual protection of aircraft in combination with active jammers and weapons.

In assessing the effectiveness of individual EW measures in tactical air operations, U.S. Air Force specialists are said to have calculated that the probability of an aircraft surviving without use of these means is very low, 0.02-0.35. It rises to 0.44-0.85 when individual onboard equipment is used, and increases to 0.95 with use of group and collective means. It is legitimate to assume that introduction of Stealth

technology also will substantially increase the capabilities of tactical aircraft to penetrate an enemy air defense system. This is indicated by the first experience of combat employment of F-117A fighters in offensive air operations by the MNF during the Gulf War.

Russian experts thus argue that EW has acquired the nature of an independent combat mission of tactical aviation. As a special form of combat operations and a special combat mission in an air operation, it will have two areas of basic application: combat against battle management systems and suppression of the enemy air defense system.

Admiral Pirumov has also praised the performance of the MNF's EW personnel and equipment.[111] He noted first of all their unusually high concentration in such a small theater (more than 100 land-based and deck-based aircraft and around 15 ground units and subunits); secondly, the precise organization of their coordination with striking forces in a unified combat operations scenario. Ground EW grouping subunits began jamming channels of the Iraqi state and military leadership 24-36 hours before aircraft took off. After 18-28 hours their efforts were augmented by jammers of numerous groups of EW aircraft operating from loitering zones against radar early-warning, guidance, fighter aviation, and command-and-control system installations. With the beginning of the ground operation, the established EW grouping (up to 20 aircraft) effectively neutralized acquisition and target designation radars as well as radio communications of the Iraqi air defense system (by using jamming systems of the

[111] Pirumov, "Parity."

attack aircraft) in coordination with ground units and subunits. F-4C EW aircraft with anti-radiation missiles and F-117A Stealth aircraft operated in the penetration element.

According to Pirumov, all this confirms once again that the presence specifically of a powerful grouping of EW personnel and equipment as well as their effective employment against electronic equipment reliably ensured MNF superiority both in the air as well as on the ground. They essentially conducted combat operations against an enemy whose command-and-control systems were disorganized and whose personnel were demoralized. (In some cases spectrum density of spot jamming output reached 4,000 watts/MHZ, which essentially precluded Iraq's use of radar surveillance and VHF/UHF communications equipment.) All this makes possible the conclusion that the priority and weight of the contribution of information support to troop combat effectiveness in developed countries has determined the dominant role of the "electronic-fire" concept of conducting warfare.

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.[112]

---

[112] Colonel L. Vasylevych, " 'Desert Storm': Electronic Warfare," Narodna armiya, 20 July 1993, p. 2.

The air-defense (AD) suppression echelon in the first mass air strike included approximately a third of the aircraft assigned to the strike, with 20 percent of the EW aircraft and 30 percent of the fighter cover for the strike groups. The jamming aircraft, which went out in the battle formations and loitered in the zones, performed electronic suppression of the Iraqi radars and covered the strike aircraft and Tomahawk ship-launched cruise missiles. Powerful and active mass jamming was set up in the frequency ranges from 700 MHZ to 18 Ghz. Special diversionary groups of aircraft with remotely piloted decoy targets were employed in some cases in order to force the Iraqi air defenses to turn on their radars. HARM anti-radiation missiles with an improved system for homing in on emissions, as well as the latest British AAM anti-radiation missiles, used for the first time, were employed in order to defeat the radars.

The activity of Iraqi air-defense radar was reduced as a result of electronic suppression and delivery of fire. More than 50 percent of the ground radars and command posts were completely disabled. The combat aircraft of the allied forces, having suppressed the SAMs, were able to fly at medium rather than low altitudes, where they could be hit by the fire of anti-aircraft artillery and portable SAM systems.

All of the aircraft, with exception of the 117A, were fitted with active jamming sets, which create imitative jamming for the radars controlling the weaponry, including the radar homing heads of missiles. The new-generation active homing set that is installed on some aircraft, for instance, can create combinations of various types of jamming.

Layered tactical formations of mixed groups of aircraft were employed in the execution of strikes against airfields. The fighter pilots received clear instructions on the procedure for the re-assignment of targets in a case where the strike group encountered Iraqi aircraft on its flight route. Particular attention was devoted to reducing the time for intercept and the fastest possible return of fighter cover to the strike group after the destruction of the target.

The passive actions of the Iraqi Air Forces aroused astonishment among foreign military experts. The American pilots, who had scrupulously studied the tactical methods of the enemy aircraft, were amazed at the virtually complete absence of any resistance in the air. All of the aircraft lost by MNF aviation under combat conditions were shot down by the fire of ground AD. The greatest losses were suffered in the first days of battle by the pilots of the British Tornado aircraft, which operated at low altitudes during the performance of their missions to shut down Iraqi airfields. The electronic reconnaissance that was performed from the reconnaissance aircraft, as well as the E-3A early-warning radar aircraft of the AWACS system, played a large role in the operation.

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.

The figures cited by "U.S. Air Force specialists" also confirm the exceptional importance of EW. The likelihood of aircraft survival without the use of means of EW is very low, equal to 0.02 -- 0.35. When on-board jamming systems are used for individual protection, it increases to 0.44 -- 0.85; for group protection it is 0.95. All of the experience of combat operations in Desert Storm proves convincingly the importance of EW.

According to Russian naval scientists, the ever-growing role of electronic warfare in naval combat operations has led to its acquiring the status of a specific form of combat -- electronic warfare [radioelektronnaya voyna]. This term is understood to mean the sum total of measures (or special operations by forces) mutually tied in by goal, place, and time aimed at reducing the effectiveness of enemy use of electronic equipment for command and control of forces and weapons and protecting friendly equipment against similar measures on the enemy's part.[113]

Electronic warfare (EW) includes three basic components:

- electronic support measures (ESM);
- electronic countermeasures (ECM); and
- electronic counter-countermeasures (ECCM).

ESM implies conduct of measures of signal intelligence (SIGINT), acoustic intelligence (ACINT), and partially opto-electronic intelligence by search intercept, position-determination, and identification of emission sources for an immediate reaction to the combat situation taking shape (basically for countering enemy missile attacks

[113] Senior Lieutenant A. Longinov, "Modern Concepts of Electronic Warfare," MS, No. 1, 1993, pp. 66-69.

using fire-delivery weapons and EW). ECCM includes measures for operational-tactical electronic maskirovka, countermeasures to enemy technical intelligence, technical monitoring of emissions of friendly electronics and installations, and also protecting electronics against jamming.

An analysis of the course of combat operations in local wars and armed conflicts in the Near East, Falkland Islands, Libya, and the Persian Gulf, where basic methods of modern EW by full-scale naval force groupings and small tactical ship elements were demonstrated and evaluated, shows that combat stability of forces at sea and the effectiveness of their weapons employment depends largely on the level of development of EW equipment and forms and methods of its use. Conduct of EW by ship elements consists in accomplishing three interrelated sets of measures, which include the following: determining the electromagnetic environment and giving over-the-horizon (OTH) target designations to attack weapons, operational-tactical maskirovka, and defense against antiship weapons.

Processes of determining and tracking the electromagnetic environment, which is part of the overall situation, and accomplishment of OTH target designation are inseparable from each other in performing primary missions assigned to ship forces at sea. "Foreign naval experts" believe that the commander of a tactical element must constantly have exhaustive decision-making information on enemy forces and enemy operations in a given area, as a rule within a radius of at least 250 nm (the effective range of ship offensive weapons), and he also must determine the enemy concept based on this information. The task of determining and covering the situation must be done in such a way as to ensure maximum concealment of friendly forces.

The electromagnetic environment is determined by searching for, intercepting, and direction-finding the emissions of enemy electronics and sonar equipment, as well as making a recording and technical analysis of them. The final stage of its determination is an identification based on COMINT, ELINT, ACINT, and IRST data of the target electronic and sonar equipment platforms and their classification as friendly, neutral (unidentified) or enemy, and also a display of data on maps and terminals of tactical element CPs and ship combat information centers. Identification of target electronic and sonar equipment platforms and their operational-tactical tie-in are the primary mission in the process of determining the electromagnetic environment.

Another important mission of ELINT, and to a lesser extent of COMINT, is OTH target designation for long-range antiship and operational-tactical missiles. The main role is played here by the process of direction-finding the target's active electronic equipment emissions. OTH target designation data are transmitted over NTDS channels of the tactical element to missile-fire direction devices of ship attack systems.

A large role is set aside for EW measures in supporting operational-tactical maskirovka of ship elements. This concept is based on three interrelated and interdependent components: reconnaissance, concealment of friendly forces, and disinformation of enemy forces. It must be noted that the basic part of practical EW measures within the scope of the concept is aimed at performing missions of C^3CM or "combatting the battle management system" of the enemy by affecting its various elements. Measures aimed at disorganizing communications and combat information exchange systems have been given the name "offensive" EW abroad, and other measures are "defensive" EW.

Data of all kinds of reconnaissance for determining the air, surface, and underwater situation serve as the basis for accomplishing measures for maskirovka of forces at sea during an operation. EW measures to conceal friendly forces are based above all on protecting friendly electronics against enemy reconnaissance and surveillance equipment. Concealment of friendly forces includes measures of the "friendly electronic emission control" plan, which regulates the conditions and sequence of using friendly electronics, above all active equipment, and measures of the "communications security" plan, providing for modes of communications equipment use, volumes and priorities of information transmitted over the radio, as well as protection of friendly communications channels against enemy communications intelligence.

A third component of this concept is disinformation of enemy forces, achieved by creating a vague situation for them, particularly a false electronic and sonar situation where the main role is played by ECM and ECCM. Disinformation measures are aimed at making it as difficult as possible for the enemy to obtain adequate, timely information about friendly forces and protecting friendly forces against his ECM.

Depending on the technical features of implementation, EW measures supporting operational-tactical maskirovka are divided into communications, electronic, radio-navigational, sonar, and anti-space measures. Communications maskirovka measures consist in performing communications deception by imitating the operation of friendly and enemy communications equipment and also by changing radio traffic volumes on friendly radio nets and deliberately violating measures for concealment and security of functioning of the friendly communications system.

Electronic maskirovka includes simulating friendly forces on dummy axes (dummy orders and the formation of a dummy electromagnetic environment), active and passive jamming of enemy electronic equipment, and also distorting the thermal fields of ships and aircraft and reducing the radar signature of the order as a whole. The goal of radio-navigational maskirovka is to preclude enemy use of friendly and international radio-navigation (including space) systems and ensure stable functioning of one's own navigation systems in operations, especially under conditions of the enemy's purposeful disorganizing effect on them.

Acoustic maskirovka is a key element in providing stability and reliable antisubmarine defense of ship tactical elements. Acoustic maskirovka measures are aimed at creating maximum difficulties for enemy submarines in detecting, tracking, and using their offensive weapons against ships and submarines of the tactical element, and also at facilitating performance of ASW missions. Acoustic maskirovka includes conducting ACINT, implementing acoustic maskirovka measures against the detection of friendly forces by enemy sonar, and also creating a dummy acoustic environment by conducting sonar countermeasures and simulating sonar fields by changing modes of operation of ship and submarine power plants as well as their motion.

Anti-space maskirovka is a component part of warfare against the space echelon of the enemy navy command and control, communications, and intelligence system. It envisages conducting disinformation measures on satellite communications channels and satellite telemetry data exchange channels, use of smoke and aerosol screens by tactical elements both at sea and in bases, and certainly the use of dispersed combat formations and dummy orders.

The third set of EW measures of ship elements -- protection against antiship missile and torpedo ordnance -- is a key element in supporting antimissile defense and torpedo countermeasures of task group ships. In the opinion of "foreign specialists," these measures are divided into two kinds depending on their practical implementation. The first includes measures for protecting ships against antiship missiles and torpedoes using weapons; i.e., surface-to-air missiles, antiaircraft, and general-purpose high-rate-of-fire guns (against antiship missiles); and rocket-propelled depth charges and anti-torpedo torpedoes (against torpedo weapons). Measures aimed at destroying an attacking antiship weapon by fire have been given the name "Hard Kill". The other kind of measure includes nonfire-delivery methods of protection, "Soft Kill," which are not inferior to the first measures in effectiveness, but are considerably cheaper in means of implementation. The principal place in "Soft Kill" is given to EW, since the target of its effect here consists of electronic equipment and homing systems of the weapons attacking the ships.

"Soft Kill" measures are based on a combination of two basic components of EW -- ESM and ECM. In protection against antiship missiles and torpedoes ESM consists in conducting ELINT, ACINT, and IRST for early detection of a launch and identification of the attacking missile or torpedo, determination of its location at each point in time, and clarification of its target as well as its type of homing system. It is very important to know from where the missile or torpedo was launched (position and type of launch platform). That information is transmitted from reconnaissance equipment to the active and passive jammers and to ship SAM systems and air defense guns. Introduction of ELINT, ACINT, and IRST in a certain tactical situation is

combined with the use of active means of detection (radar, sonar, and so on) and visual lookout.

Electronic and sonar countermeasures systems working in tandem with intelligence-collection equipment disorient missile and torpedo homing systems, divert them to decoys, or lead them away from the chosen target of attack by active and passive jamming. According to provisions of modern Western tactical manuals and guides, it is of great importance here to combine EW measures with maneuver in heading and speed by the ship being attacked to reduce her radar, sonar, thermal, and visual signature, which helps to break the lock-on of homing systems.

"American specialists" believe that the principal direction in EW development is a unification of COMINT, ELINT, and IRST as well as active and passive jammers into automated systems supporting the principal requirement placed on them: maximum reduction in time of response to electronic emissions (or the time for jamming). To this end they will make wide use of digital computers, with which it is possible to perform missions of automatic detection, determination of coordinates, classification, and assessment of the degree of risk of emitting electronics and their platforms, as well as development and execution of a decision for using active and passive jammers.

According to General-Major N.A. Kostin, 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.[114]

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 both defensive

[114] General-Major N.A. Kostin, "Appraising the Effectiveness of Troops (Forces) and Weapons Control Disorganization," VM, No. 11, 1993, pp.39-44.

and counteroffensive 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.

The importance of electronic warfare is becoming increasingly apparent with the growing impact of the quality of command and control on the progress and the outcome of operations, and with the growing skills of commanding officers and their staffs in the organization and conduct of electronic warfare. It has already become vital for electronic warfare to graduate from a type of combat support to a component part of combat operations and in the future, to an independent type of combat operations. It is therefore quite legitimate to speak about the creation of a new combat arm -- the electronic warfare troops.

Russian military theorists assert that the experience of local wars in the 1970s-1990s has shown that EW, the essence of which is the struggle against combat command-and-control electronic systems and high-precision weapons of the enemy, together with its main components -- electronic countermeasures, countermeasures against technical intelligence systems, and electronic protection of one's own command-and-control systems -- has evolved from an operational (combat) support service into a special kind of combat operations conducted by diverse forces and fires, but one that is aimed at achieving a common objective and requires at the same time a high degree of integration of intelligence and weapons systems, as well as

coordinated actions of the EW reserves of all combat arms and special troops according to one single concept and plan.[115]

The content and effectiveness of the entire set of EW measures in operations are characterized by the nature of operational missions assigned and the reasons for using particular methods of operational employment of EW reserves. This requires a quantitative assessment of EW influence on operational indicators as early as at the decision-making stage, and at the same time enables us to do so. The main drawback of the existing methodologies of operational-tactical calculations is that they cannot assess the effectiveness of EW as a whole, that is, taking into account all its integral parts: electronic countermeasures, electronic protection, and countermeasures against technical intelligence systems. Current methodologies suggest that the effectiveness of EW measures be assessed by their contribution to the combat potential (CP) of a group of troops. However, given the existing differences in the calculation of quantitative assessments of EW effectiveness in the practical operation of staffs it is qualitative indicators, such as the degree of command-and-control disruption -- interrupted, broken, restricted -- that are used most commonly.

According to Russian naval officers, the intensive development and comprehensive use of electronic equipment in the interests of ensuring accomplishment of the missions facing naval forces have accelerated the creation of new, effective EW

[115] Colonel Ye.V. Malyshev, "On Assessing the Effectiveness of Electronic Warfare in Operations," VM, No. 11, 1993, pp. 49-52

equipment. Preserving the combat stability of one's electronic equipment has become an essential condition of modern combat largely determining its success.[116]

As "foreign experts" believe, all categories of personnel operating electronic equipment in peacetime must acquire the necessary experience of conducting combat operations in EW conditions. At the level of operators of electronic equipment, individual combat posts, and command posts, this is achieved by means of training on specialized electronic simulators; at a higher level, this is achieved during the course of exercises with practical use of equipment and weapon systems. However, creating a tactical background that ensures realistic conditions for organizing two-sided EW is quite a complicated military-technical task. To accomplish it, it is not enough to use one's own forces with organic electronic and EW assets to designate the enemy.

First of all, one's own EW assets are optimized by the frequency and type of jamming for the parameters and characteristics of the electronic assets of the probable enemy and in many cases are unable to create the necessary jamming environment for friendly electronic assets. In turn, the organic electronic assets of the forces used to designate the enemy, as a rule, differ in parameters from the "enemy," which makes it difficult to reproduce a near-real electronic environment. Second, using EW combat subunits to organize a jamming background at exercises leads to premature consumption of their technical service life and a decrease in the combat readiness of forces as a whole.

---

[116] Captain 2d Rank M. Partala and Captain 2d Rank V. Osipov, "Support of Naval Combat Training in Conditions of Electronic Warfare," ZVO, No. 3, 1995, pp. 51-54.

Taking the above into account, it is considered advisable to form special EW support subunits for combat training methods with development of special equipment for them. For example, the United States and other armed forces have special aviation and ground subunits for support of combat training of naval forces in EW conditions. Indeed, in the navies of the United States, Great Britain, and other countries, much attention is being devoted to practicing combat operations in EW conditions. To create an electronic environment that is close to real during the course of combat training, special support subunits are formed in the structure of naval forces which have the necessary equipment at their disposal. Private firms and companies specializing in the area of simulating enemy EW equipment are also used. In the opinion of "Western experts," such an approach makes it possible to increase substantially the effectiveness of combat training and ensure a qualitatively new level of readiness of naval forces to wage modern warfare at sea. Thanks to this, it will be possible to avoid repeating mistakes associated with the practical and psychological unreadiness of personnel to conduct electronic warfare.

According to Colonel-General V. Semenov, CINC of the Russian Ground Troops, the effectiveness of employing EW forces and assets is acquiring special urgency. Such forms of operations as the electronic-fire engagement, electronic-fire strike, and electronic strike, in which means of electronic engagement will be widely used, will fill operations and combat operations of combined-arms units with new content. In the aggregate they can comprise a special operation to disorganize enemy

command-and-control and fire-control systems on the axis of concentration of main efforts.[117]

"ELECTRONIC-FIRE OPERATION"

According to Russian military scientists, 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

[117] Colonel-General Vladimir Semenov, "Main Directions of Ground Troops Development," AS, No. 3, 1995, pp. 9-15.

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.

Admiral Pirumov argues that the effectiveness of information systems has led "developed countries" to acknowledge the dominant role of the "electronic-fire" concept of waging war.[118] In force structure and equipment, this concept manifests itself not in competing for numerical superiority in motorized rifle (tank) formations for

[118] Rear-Admiral V.S. Pirumov, "Two Aspects of Parity and Defense Sufficiency," Ibid., pp 26-34.

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."

Pirumov argues further that 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. Pirumov concludes by arguing that 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.

VI. NEW EW SYSTEMS AND CONCEPTS

SOVIET VIEWS ON RADAR SYSTEMS

For over a decade, the Soviet military argued that radar systems play a critical role in the ongoing RMA. As a result, military scientists focused on the cutting-edge technologies in this sphere. For example, they repeatedly examined the developmental trends and capabilities of various phased-array radars.[119] The process of developing radars is determined to a considerable extent by the level of parameters and the state of the technology base of antenna systems, which in recent years have been realized in the form of phased arrays. Such antennas not only characterize the prospects of development of modern radars, but also have a significant influence on the design and layout philosophy of their construction. Therefore, recently they have been devoting increasing attention "abroad" to the development and use of phased arrays as antennas with a wide variety of purposes. Modern phased-array antennas used in foreign radars are, as a rule, an aggregate of a large number of elements. For these elements, they use various dipoles, open-ended wave-guides, and other devices which can be excited by changing the amplitude and phase of radar signals or their frequency. The class of phased-array radars encompasses virtually the entire contemporary and future list of radars which comprise the basis of outer space monitoring, air defense, air traffic control, nuclear-missile strike warning, and also special-purpose measurement systems.

In the opinion of "foreign experts," one of the main reasons for the shift from conventional antennas to phased-array antennas is the desire to create, using inertia-free

---

[119] For example, see Colonel V. Pavlov and S. Grishulin, "Foreign Phased-Array Radars," ZVO, No. 7, 1991, pp. 36-46.

electronic control of the directional pattern, multifunctional radars which would ensure on a real-time basis the detection, tracking, and identification of a large number of targets in the air-space, and also the performance of a number of other functions (e.g., radio control of anti-aircraft missiles and spacecraft). Inertia-free control of the directional pattern makes it possible to scan space according to a preset program, ensure optimization of processes of detecting signals against the background of a variety of interference, reduce time and energy costs, and also increase the capacity of radars by the simultaneous formation of multibeam directional patterns. As "Western experts" believe, phased-array radars can successfully combine different methods of measuring target coordinates. In particular, in one the coordinates may be measured without stopping the beam, and in another the beams are directed to a designated sector, taking into account previous measurements, at times determined by the scanning program.

To increase the accuracy of determining coordinates in the vicinity of extrapolated points, a monopulse mode based on addition-subtraction signal processing is realized, making it possible to decrease measurement errors to an amount not exceeding 0.002 of the width of the antenna's directional pattern in the corresponding plane. From "foreign press reports" it follows that realization of the advantages of phased-array antennas proved possible mainly after development and assimilation of new technologies by leading Western firms in the field of electronic devices and instruments, including creating such elements as phase shifters, power dividers, amplifiers, and oscillators operating in various frequency bands, and also high-speed control devices based on mini- and microcomputers, including optical-electronic computers.

All types of phased-array antennas differ basically by principles of powering the radiating elements. In particular, in the classic antenna arrays, the radiated energy is generated by several power sources and distributed among the phased-array antenna elements by using power dividers, for which phase shifters are used to control the position of the directional pattern. As is noted in the "foreign press," the need to use a system of distributing energy among a large number of radiating elements (up to tens of thousands) leads to large losses of high-frequency energy, and it is necessary to generate additional power to compensate for these losses. In this connection, when building modern radars, preference is given to phased-array antennas with a modular design, in which the energy is generated by a large number of small low-power sources (as a rule, solid-state), each of which directly powers its own radiating element or group of elements. Due to the fact that the output amplifiers of the transmitting portion of these modules and also the preamplifiers of their receiving portion are located in the immediate proximity of the radiators, it can be operated at considerably lower power levels and, as a result, can minimize energy losses in the radiated and received signals.

The modular principle of building phased-array antennas, as is emphasized in the "foreign press," significantly depends on the technology for building solid-state microwave integrated circuits (Monolithic Microwave Integrated Circuit), which can ensure operation with a high pulse ratio (20-30 percent of the repetition period) and a sufficiently long range. In doing so, however, the radiation of long-duration pulses limits the minimum range of the radar, which results in the need for sounding of space with pulses of a shorter duration and varying their repetition period, taking into account the radar cross-section of the targets and their distance from the radar. In addition, this entails a complication of algorithms for processing radar information and software.

The frequency method of controlling the directional pattern is used in a number of antenna arrays. It is characterized by economy, comparative simplicity, and reliability. An antenna array with the frequency scanning method, as a rule, includes a wave-guide or coaxial delay line linked in series to the linearly positioned elements. The frequency scanning method is most common in radars designed primarily for scanning the airspace and air traffic control. The design of the antennas is based on optical, linear, or combined power supply systems and dipole, slotted, or horn-type elements. Formation of the directional pattern and control of its position are accomplished by changing the carrier frequency. Frequency scanning makes it possible to implement the multibeam radar variant.

Unlike large radars whose antenna arrays occupy a fixed position during combat operations and can accomplish azimuth scanning in a wide sector (over 100 degrees), some special-purpose radars are required to accomplish electronic scanning of the directional pattern in comparatively small sectors -- usually in the range of 15-30 degrees. This group includes gun-laying radars, radars for various weapons, air traffic control system aircraft landing radars, and antenna systems of certain stations. As a rule, such radars use phased-array antennas as the radiation sources of the primary reflector.

The development of phased-array radars and electronic methods of directional pattern control has made it possible to begin developing qualitatively new acquisition and tracking algorithms and to free part of the potential of radars for weapon guidance. The AN/MPQ-53 radar of the Patriot missile system is an example of such a radar.

Lately, ground radar antenna systems in the form of phased-array antennas have begun to find application not only in stationary long-range radars but also in mobile ones designed to detect low-flying targets. Among phased-array radars, a special place is occupied by radars with rotating antennas, including those with electronic elevation and azimuth control of the directional pattern. Their speed of updating target data to ensure the required tracking accuracy turns out to be dependent on the azimuthal rotating speed of the antenna, since it is possible to increase the target detection and ranging time by beam scanning and turning the radar in the opposite directions. Therefore, if necessary, the radars can irradiate several targets within a longer period of time, which makes it possible to use special methods of identifying or forming signals with greater energy to distinguish targets against a background of various interference.

Since phased-array radars can form special beams for each target, the pulse repetition frequency and signal energy can be selected so as to eliminate blind ranges and speeds and also to maximize the signal-to-noise ratio for more accurate tracking of the targets. In addition, the possibility of their taking a bearing can be reduced by optimizing the radiating time. Tuning the carrier frequency and changing the pulse repetition frequency and the type of signals as a whole increases the radar's resistance to jamming even more in a complex noise and target environment. In addition, the antenna system operation can be implemented in the functioning algorithms of such radars not only in the entire hemisphere but also in a certain portion of it, that is, in the most important sector where attacking targets are expected to appear.

RUSSIAN VIEWS ON RADAR SYSTEMS

In their analyses of radar systems, Russian military scientists have focused repeatedly on the combat employment of over-the-horizon (OTH) radars. They note that work to create OTH radars has been going on in the former Soviet Union since the mid-1980s. Assessments made of the effectiveness of a unified air defense system show that creating an OTH radar system on Commonwealth territory will permit substantially increasing the depth of warning of an attack by offensive air weapons. This will enable promptly placing not only Air Defense Forces equipment, but also that of other branches of the Armed Forces in higher degrees of readiness and moving the bulk of fighter and attack aviation forces out from under the strike. By using OTH radars to vector fighter aviation it is possible to realize potential combat capabilities for interception of offensive air weapons by modern fighters at maximum ranges. On the whole, Russian experts believe that creating an OTH radar system within the scope of allocated defense appropriations will increase the effectiveness of a unified air defense system by 1.6-1.8 times.[120]

According to Russian military experts, the armed forces of the United States and other NATO countries are working actively to upgrade military radar systems. Creation of EHF-band electronic devices is considered to be one promising direction in this area. Successes in recent years in the technology of manufacturing the element

[120]For example, see General-Major A.S. Sumin, "On Establishing an International Air-Space Control System Based on OTH Radars," VM, No. 6-7, 1992, pp. 24-27.

base in this band made possible the development of electronic equipment for operating at frequencies above 30 GHz.[121]

Compared with SHF-band systems, use of EHF-band engineering in radar permits higher resolution with the very same antenna aperture and thereby improved accuracy in tracking and identifying targets as well as improved terrain mapping quality. EHF-band radars are less susceptible to deliberate enemy jamming since the capability of operating in a broad band of frequencies permits increasing anti-jam capability and the data processing rate by using broadband FM and signal coding. Identification and classification of moving and maneuvering targets is facilitated because of increased doppler frequency shifts of signals reflected from them.

Considering the broad capabilities of EHF-band radar systems, "foreign specialists" are continuing intensive research in this area to increase the combat effectiveness of various kinds of weapons. It is being done basically along the following lines:

- development of advanced technologies for manufacturing an element base, including monolithic phased arrays and specialized integrated circuits with high packaging density on gallium arsenide substrates, which should lower the cost of gear elements in mass production;

- upgrading of micro-processor equipment with elements of artificial intelligence permitting fuller use of the capabilities of electronic systems;

[121] Major A. Skorodumov "The Prospects for Using EHF-Band Electronics," ZVO, No. 9, 1992, pp. 30-34.

- increased speed of radar image-forming equipment to achieve real time; and
- theoretical and experimental research of multi-channel effects arising with the propagation of EHF-band radio waves to reduce their influence on the functioning quality of radars.

Mobile radar units form the backbone of all air defense systems in the Russian Army, just as in the past they formed the backbone of all air defense systems in the USSR. Traditionally they use the meterband in the production of these radars. This band offers certain advantages. A whole range of these advantages has become particularly important in recent years. The prime advantage is the ability of these radars to detect aircraft using Stealth technology. These radars are also relatively more efficient compared with other waveband radars in detecting small-dimension targets -- high-precision weapons, cruise missiles, and other small-dimension targets.[122]

These radars are the least affected by electronic countermeasures of the opponent. In order to organize effective electronic countermeasures against such radars, the opponent has to have relatively big antennas. This is fraught with specific engineering problems from the viewpoint of the installation of these systems on aircraft and missiles and even on the ground.

According to the Russians, these radars are also the least vulnerable to anti-radiation missiles. The reason is the same. In order to build a precisely aligned

[122] From the "Nauka i Tekhnika" program: Video report by Sergey Tibilov, chief designer of the Nizhniy Novgorod NITEL Joint-Stock Company, Russian Television Network, 14 April 1995.

antenna in a relatively long waveband a fairly big antenna is needed. To install this on a missile is a relatively difficult engineering task. Therefore, the potential enemy at the moment has no high-precision missiles self-homing on radiation in this wave-band. Various generations of meter-band radars account for more than 70 percent of total army radar equipment.

In the opinion of "foreign military specialists," say Russian military scientists, guided missiles with passive radar heads homing on radio-frequency emitters (chiefly on radars of air defense weapons) are the most effective means of electronic warfare. Their principal advantages are autonomy of guidance, which after launch of a missile permits the platform aircraft to execute a maneuver to evade anti-aircraft fire or to deliver strikes against other targets; absence of emission of electromagnetic energy, which precludes detection by SIGINT assets; small radar cross-section and high flight speed, which considerably hamper detection and intercept of missiles; the possibility of employment in essentially any weather conditions day or night; the capability of intercepting a target considerably earlier than enemy detection of the missiles; and the platform aircraft does not have to enter the impact and fire zone of surface-to-air missile systems and artillery in delivering strikes with certain types of missiles. In addition, when the missile approaches the target, the latter's signal constantly increases, thereby improving conditions for discriminating it against the noise background and increasing guidance accuracy.[123]

[123] Colonel Aleksandr Manachinskiy, "Airborne EW Equipment," AS, No. 4, 1994, pp. 86-88.

Modular design is said to be used widely in the development of anti-radiation missiles abroad. Families of multipurpose missiles equipped with various guidance systems are being created. "NATO military specialists" believe that use of anti-radiation missiles must be massive to ensure effective fire suppression of air defense. Thus, foreign sources assert that one sortie will require the expenditure of 1.5 anti-radiation missiles. As applied to a massive air raid made up of hundreds of strike aircraft, this means that 500 and even 1,000 anti-radiation missiles will be required daily to neutralize the air defense system in the first stages of a conflict.

NEW VIEWS ON ELECTROMAGNETIC WAVE WEAPONS

Russian military experts note that the combat operations in the Persian Gulf are still the subject of analysis by their own specialists. Quite a few high-precision weapons systems were tested in battle there. The outlines of that conflict could be typical of a number of other contemporary wars as well. Those wars will evidently be typified by the precise proportioning of a combat impact that is formulated in advance by the military-political leadership.[124]

The quality of support of one's own troops in a conflict with the use of high-precision weaponry has a decisive effect on the outcome of the battle. The AD resources should cover the troops against small, high-speed, and maneuverable weapons platforms in a rapidly changing situation and in the face of enemy EW. The complexity of support under those conditions and the strike accuracy necessary for the

[124] Aleksandr Borisovich Prishchepenko and Colonel Vladimir Petrovich Zhitnikov, "EMO [Electromagnetic Weapons] in PVO -- Some Questions of the Use of Electromagnetic Emissions in the Radio-Frequency Band as a Weapon," VPVO, No. 7, 1993, pp. 51-55.

efficient destruction of a target using firepower lead to a substantial rise in the cost of production and maintenance of AD systems.

Powerful radio-frequency electromagnetic emissions (RCHEMI), emitted at a target that includes electronic gear made of semiconductors, creates powerful current pulses in the electrical circuitry of the target, disabling the semiconductors. The outlook for the use of these radio-frequency electromagnetic emissions (RChEMI) as a destructive factor, expending less energy to disable semiconductor elements than any mechanical influences on the target, is thus important.

Experiments have shown that very little energy is required to disable semiconductors. Before reaching them, however, the RChEMI pass through the SHF path of the target, where they are weakened substantially. Neglect of this fact leads to markedly reduced destructive criteria. Field practices have shown that the value of the safe distance between the same types of radars with emitter power in the tens of kilowatts is on the order of a hundred meters. The radar will thus remain guaranteed to be operable at distances of hundreds of times more (tens of kilometers) even if the corresponding power is increased exponentially (hundreds of megawatts). The euphoria that was initially observed on the score of the combat capabilities of electromagnetic weapons (EMO) may be premature.

The training of considerable EMF (electromotive forces) -- which are the cause of the functional disruption -- onto the housing of the electronic gear (RES), as a rule metallic, is typical of waves a meter or more in length. Various elements of the

electronic circuitry, as well as actuators, fail in that case. Random actuation could also occur.

Shorter waves -- decimeter and centimeter -- are comparable in length to the operating waves of most RES. The input devices (SHF-diode mixers, for example) are damaged under exposure from them. The impact, however, depends strongly on the orientation of the directivity pattern (DN) of the RES relative to the source. Even small deviations from the major lobe lead to a sharp increase in the destructive values of power flux density of RChEMI. When the differences in the wavelengths are increased, the DN of RES reception of out-of-band emissions "is smoothed out" and the effects of directivity become minimal. Millimeter waves penetrate through slots in protective screens, servicing hatches, etc. The input circuitry and even the screening circuitry of internal digital signals processing machinery are damaged therein.

Analysis of the results shows that the threshold values for the power flux density of RChEMI inflicting functional damage on various types of RES is from thousands to millions of watts per square meter in a case of exposure to out-of-band emissions. The effects on the same types of objects by RChEMI of identical spectral composition had to be observed. Different values for the power flux density led to random actuation, retargeting, temporary functional failure, and disabling; i.e., the defeat was of a comprehensive nature. Modern items are especially vulnerable. This can be explained by the fact that the extent of integration of semiconductors in them is higher and thus, the dimensions of the active elements and their resistance to shock current overloads are less. If EMO are to have a place in the arsenal of means of warfare, the

development of a parametric series of protective devices and their installation will be required not only on input circuitry, but in other circuit assemblies as well.

The creation of EMO is possible on the basis of powerful emitters of traditional vacuum high-current electronics (gyrotrons, magnetotrons, Cerenkov generators, etc.). A concentration of emitted energy with a small, solid angle and low (10%) scattering of frequencies in the spectrum of the RChEMI formed are typical of them. A very narrow beam of RChEMI, in which the power flux density considerably surpasses the penetrating, could "pass" through a plasmoid created by it. The beam "sharpens" even more therein, but at the price of substantial losses of energy in the formation and heating of the plasma. This phenomenon is moreover observed only for comparatively long (microsecond), and thus ineffective RChEMI pulses.

The electronic emissions require considerable (up to units of megavolts) operating voltages. But the electrical strength of the design must also be ensured, and that leads to an increase in the dimensions and a reduction in the unit characteristics. The RChEMI power draw is 5×10^{-5} J/cm^3. Traditional emitters permit repeated actuation.

Sources in which the formation of RChEMI occurs through the compression of a magnetic field have greater unit power. These include a shock-wave emitter, an explosive-magnetic frequency generator, and a superconducting magnetic-field shock-wave shaper, which make it possible to obtain a RChEMI power draw of 10^2 J/cm^3. The isotropic distribution of the RChEMI formed are typical of them. Power supply

is accomplished through high-current (hundreds of kA) pulses at low (tens of kV) voltages.

The emitting, dimensional, and operational characteristics of the sources in various classes differ markedly. This means that the conceptual foundations of the weapons systems created on the basis of them will differ as well. The large dimensions and directed nature of the emissions of traditional generators condition the creation of directional sources based of them, which should be supplied with a guidance system. The isotropic nature of the emissions and small dimensions of sources based on the compression of a magnetic field makes it possible to fit them to existing types of platforms and use the flux of the RCHEMI created to compensate for the inaccuracy of the platform. That use makes it possible to consider these sources as the foundations for the creation of electromagnetic ordnance.

The use of EMO in an actual combat situation will sometimes be ineffective. An antiship missile that continues to fly with a disabled homing head at a distance from the target of about one kilometer with an undamaged airframe, engine, warhead, and impact detonator will defeat a ship all the same. If the homing head is disabled at a distance of three to five kilometers, errors in homing accumulate and the likelihood of hitting the ship becomes acceptably low. The RChEMI strike only the RES, and the combat impact from the application of EMO is thus manifested the more fully, the more important the role of RES in a given situation. RES plays the most important role in long-range battles as well as in the most maneuverable types of close-range battle with a target at top speeds.

An analysis of the properties of electromagnetic emissions in the radio-frequency band makes it possible to consider them an effective destructive factor when operating against targets that include RES. The maximum effectiveness is achieved for tasks that require the isotropic distribution of the RChEMI. The use of electromagnetic ordnance will make it possible to reduce the cost of weapons systems through reductions in the requirements for accuracy of the delivery of that ordnance.

Russian naval scientists note that along with other precision-guided weapons systems, new modifications of the Tomahawk cruise missile were used in the numerous strikes with which the anti-Iraq coalition opened combat operations in the Persian Gulf. These missiles were equipped with powerful radio-frequency emitters (instead of high-explosive warheads) that were developed within the framework of "black programs," and were used in the enemy air defense penetration echelon to disable its electronic systems (RES).[125]

For the first time, pulse radio-frequency electromagnetic radiation (RChEMI) that had previously been employed as an information carrier was utilized as a damage-producing element which, while affecting a target, induces currents and voltages in its electrical circuits in such a manner that semiconductors malfunction from the overloads. In the process, incomparably less energy is required for this destruction than for any mechanical damage. Furthermore, the frequency agility is not capable of parrying the strike of an electromagnetic weapon (EMO), and therefore this strike turns out to be significantly more effective than the impact of jamming on a target. The appearance

---

[125] Doctor of Technical Sciences A. Prishchepenko, "Ship Electronic Warfare -- the Warfare of the Future?" MS, No. 7, 1993, pp. 35-38.

of electromagnetic weapons completes EW's evolution from a supporting to a primary type of combat operation, which requires the development of a number of new naval tactics wherein the study of the combat capabilities of electromagnetic weapons appears to be extremely important.

Traditional emitters (gyrotrons, magnetrons, Cerenkov generators, and others) can serve as the basis for the development of electromagnetic weapons for which the following are characteristic: the concentration of radiated energy in a small solid angle, and a small (10%) dispersal of the frequencies in the spectrum of the radio-frequency electromagnetic radiation being formed. The very narrow beam of radio-frequency electromagnetic radiation, in which the power flux density significantly exceeds breakdown density, can "pass" through the plasmoid created by it. In the process, the small beam is "excited" even more (although at the cost of substantial losses of energy in the formation and heating of the plasma), but this phenomenon is observed for comparatively prolonged (microsecond) and therefore ineffective pulses of radio-frequency electromagnetic radiation.

Significant (up to a megavolt) operating voltages are needed in traditional sources of electromagnetic energy for effective electronic emission. The need to ensure electrical durability leads to an increase of the dimensions and, therefore, to the reduction of the corresponding characteristics: specific energy output of the radio-frequency electromagnetic radiation totals several tens of millijoules per liter. Indeed, traditional emitters permit reuse.

Sources in which the formation of radio-frequency electromagnetic radiation occurs when the magnetic field is compressed have significantly higher average specifications. An impact-wave emitter, a magnetic-bust frequency generator, and a super-conductor magnetic field impact wave oscillator that were recently developed permitted the Russians to obtain average energy output of radio-frequency electromagnetic radiation up to 10 joules per liter. The following are characteristic for these sources: practically isotropic distribution of the radio-frequency electromagnetic radiation stream formed in space, and a wide (several decades) radio-frequency electromagnetic radiation frequency range. Energy supply is carried out with a high-current pulse (hundreds of kiloamperes) with low voltage (tens of kilovolts).

The two indicated classes of sources are substantially differentiated by emitter, size, and operating specifications. Therefore, the conceptual bases of the weapons systems that could be developed based upon them will be differentiated. Obviously, traditional generators can be employed as fixed directed sources equipped with guidance systems. The isotropic nature of the radiation and the small dimensions of the sources based on a compressed magnetic field make possible their delivery by existing types of platforms and the utilization of a radio-frequency electromagnetic radiation current that is formed to compensate for a failure that permits them to be viewed as the basis for developing electromagnetic munitions.

The combat effect from employing electromagnetic weapons is caused by the specific impact of radio-frequency electromagnetic radiation as a damage-producing element exclusively on an electronic system: it is manifested more completely when the electronic system has a more substantial role in the given combat situation. Electronic

systems play a most important role in combat at long distances and also in maneuvering types of combat. Situations in which the employment of electromagnetic weapons is possible without coordinating with weapons assets are more characteristic for a defensive engagement: in order to avoid being hit, it is sufficient to "blind" the antiship missile for a few seconds. If the ship has been damaged by electromagnetic weapons, but enemy weapons systems do not immediately "reach" it, its crew can replace even irreparably disabled units of electronic systems and continue to fight. An electromagnetic weapon will not be able to completely replace weapons systems and the choice of weapons systems on ships of the future is a choice between competing technical solutions.

Therefore, at this stage, electromagnetic munitions have significantly greater capabilities for compensating for a miss than a munition that destroys a target with a shock wave and shrapnel. Furthermore, the introduction of electromagnetic munitions can make a number of types of electronic warfare systems unnecessary. And finally, electromagnetic munitions still have a number of advantages. Based upon their dimensions electromagnetic munitions are suitable for employment in many shipborne weapons systems. They can be utilized in a salvo at a range that is determined only by the capabilities of the platforms and compensation for a miss, and the increase of the impact on a target is attained by increasing the number of munitions in the salvo. Moreover, the presence in electromagnetic munitions of a significant (up to 1.2 by volume) quantity of explosives permits it to be utilized for the effective engagement of a target in extreme circumstances.

Thus, the application of pulse radio-frequency electromagnetic radiation to combat targets which functionally consist of electronic systems is quite promising and, at the present time, the maximum effectiveness of this new damage-producing element can be realized with the isotropic dissemination of its energy in space.

Russian naval scientists continue to focus on electromagnetic wave weapons (EWW), or those means which can damage the semiconducting elements of targets through electromagnetic radio-frequency band radiation impacts. Their energy impact is well known: the induction of radio-frequency electromagnetic radiation (RFER) in electronic current and voltage circuits damages some semi-conducting elements as a result of overload. Because the main target of EWW is electronic equipment, they call the damage effects inflicted electronic suppression.[126]

Studies show that the character of RFER impacts depends on the wave length. If its magnitude considerably exceeds the size of the target, large currents and voltages are induced in the conduction frame, which can lead to a disturbance in the normal distribution of currents and voltages in the equipment operating within the frame, and put it out of action. Long-wave RFER does not penetrate the conduction frame. If the wave length is on the order of centimeters or millimeters, then the indirect impact, conditioned by current and voltage induction on the frame, is supplemented by direct impacts: millimeter waves penetrate through radio-transparent fairing, slots, and inspection and maintenance holes, and induce currents and voltages directly within the target's electronic circuits.

---

[126] A.B. Prishchepenko and Colonel M G. Akhmetov, "Electronic Suppression in an Army Operation (Combat)," VM, No. 2, 1995, pp. 42-48.

The former impact is also characteristic of the electromagnetic impulse of the nuclear explosion, whose nearly entire energy is realized in electromagnetic waves of EWW. Thus, depending on the wave-length band of impacting radiation, the effect can manifest itself in various electronic chains, and the resistance of a weapon system to the electromagnetic impulse of the nuclear explosion does not guarantee its resistance to the impact of millimeter or centimeter wave radiation.

The more the impact radiation frequency band differs from the operating frequency band of the electronic equipment, the less the directionality effect. The densities of the energy flux of such out-of-band radiation whose impact irretrievably disables the majority of targets lie within the 10^2 -- 10^7 W/m^2 interval. With respect to RFER, there is a specific target vulnerability scale. Thus, the densities of the radiation power flux necessary for damaging two missiles of the same type, but outfitted with different classes of electronic equipment (radar or infrared homing head), can differ by more than a factor of 10.

The effectiveness of RFER greatly depends on its capability to cause the breakdown of the atmospheric air. The plasma resulting from the breakdown screens the source, and the radiation energy is spent only on heating the plasma layer. As pressure lowers (altitude increases), the breakdown effect declines. The limitations related to the breakdown of the atmospheric air rigidly determine the correlations between the size of a RFER source and the radius of damage effects, because power density weakens in proportion to squared distance. Therefore the maximum distance at which electronic equipment is irretrievably put out of action does not exceed the

typical size of a radiation source (for a directional source, this is the length; and for an isotropic source, the radius) by more than 1,000 times.

At the same time the phenomenon of temporary (from fractions of a second to several hours) blinding of electronic equipment with the subsequent restoration of its functions. Such a damage effect can be realized by substantially less powerful RFER. An analogous effect is observed also in the event of consistent impacts on a target: a considerably lesser aggregate energy of several impulses is required for putting it out of action than in order to achieve the same effect by a one-time impact. These phenomena certainly contain possibilities for substantially enhancing the effectiveness of electromagnetic weapons.

RFER as a damage effect has a number of distinguishing features which set it apart from conventional ones, whose comparative characteristics are shown in Figure 11. Analysis of the data shown primarily points to the selectivity of RFER: it affects exclusively EW equipment, notably micron-dimension semi-conducting elements, which are the most vulnerable to overload. Because basic priority lines in the functional upgrading of modern electronic equipment are the miniaturization of semi-conducting elements and enhancing the extent of their integration, the energy effectiveness of RFER can exceed that of conventional damage effects, which inflict mechanical damage on the target. It should be noted that a far smaller portion of the explosive substance energy can be converted into RFER energy than into shock wave. This circumstance somewhat neutralizes the difference between the effectiveness of the damage impacts shown in Figure 11.

Comparative Characteristics of RFER and Conventional Damage Effects

Characteristics of damage effects	Damage effects		
	RFER	Shock wave	Fragments
Limitations on list of impacted targets	Targets not including electronic components are not damaged	Targets heavily protected against mechanical impacts are not damaged	
Effectiveness of damage	Damage of electronic equipment is only possible	Damage of various extent of seriousness is possible.	
Factors limiting correlation between size of weapon system and size of damage zone	Breakdown of atmosphere	Energy content of explosive substance	
Impact of atmospheric pressure on effectiveness	Present in approximately same measure as in shock wave	Present; impact radius lessens as explosion altitude grows	Absent
Negative ecological fall-out from employment	Absent	Present	Present
Energy densities required for disabling standard target, J/m	10-3 -- 10	105	5x104

Figure 11

In order to further analyze EWW properties, it is essential to consider the sources of RFER formation. They can be subdivided into two classes. The first will include directed radiation sources: conventional vacuum electronic devices (magnetones, vircators). The radiation they induce is directional and narrow-band (the frequency spread does not exceed 10 percent). Analogues of these sources find a broad application in electronic suppression systems, and therefore the functional features distinguishing EWW from such systems are reduced merely to quantitative indicators: the impulsive character of radiation and a substantially greater power, facilitating damage to electronic equipment. The main problem in creating conventional superpowerful RFER sources is to ensure the electrical strength of the structure because it is necessary to realize a considerable electron emission. The high operating voltages precondition the substantial size of sources (on the order of cubic meters) and rather low specific energy characteristics, which creates a number of intractable technical problems that prevent their military application.

The large size and therefore low mobility, the directional character of radiation, the need to aim and guide the RFER beam on a target, and radioelectronic incompatibility create a rather unfavorable combination, which lessens the possibility of using conventional sources in EWW. If such EWW are created after all, the maximum damage effect range of a one-meter long directional source will be a mere one km. Consequently, the effective impact range of directional radiation sources is comparable with or slightly below the range of a direct fire shot by main anti-tank systems or small caliber anti-aircraft artillery.

Another class of emitters created recently are direct transformers of conventional explosive substance energy into electromagnetic energy. Their magnetic field changes as a result of its quick compression by the conduction environment, propelled by the explosion energy. These transformers are characterized by sizes of 1-31, and by an isotropic distribution of energy of the formative RFER in space, which makes their application as electromagnetic wave ammunition (EWA) the most expedient. The enhanced energy effectiveness of RFER as a damage effect compensates for the possible failures of EWA, and therefore facilitates effective fire to a long range and successful engagement of dispersed targets. The creation of combined ammunition is also possible -- for example, high explosive-electromagnetic ammunition, using the same explosive substance charge.

EWW used against electronic equipment have an advantage over regular fire delivery systems. Thus, a 120-mm EWA can damage a target within a radius of 60 meters, which is approximately one order of magnitude higher than the damage radius of radar-type targets with the same caliber HE-ammunition. Furthermore, estimates show that in order to clear a passage in a 20x100-m influence minefield with a 95-percent probability, using the Nona artillery system, at a range of 4km, with 21-meter error in fire preparation data, and the spread of 8 meters, 550 HE charges or five EWA are needed.

Because EWA have relatively small weight and size characteristics, they can predictably be used to equip missiles, anti-aircraft and tube artillery shells, aviation rockets, air bombs and containers, and means for clearing influence minefields. Therefore EWA can be carried by weapon systems of front aviation and ground force

aviation, missile forces and artillery, and air defense forces. The technical standards of these munitions now are such that they can be integrated into already existing systems without substantially changing the methods of their combat application in an operation.

Target damage caused by EWW is relatively easy to mend. Thus, a trained crew, given the requisite spare parts, can easily cope with this task within several minutes. At the same time experience shows that if complex electronic equipment is disabled, army or factory specialists have to be called in, which shows that it can be put out of action for longer periods. In addition, RFER resulting from the explosion of EWA at the same time damages the target with its fragments. Although the effectiveness of such damage is not substantial, considerable damage can be inflicted on unprotected personnel and unarmored equipment.

The above EWW characteristics and specifics call for their purposeful employment in certain periods of an operation, in interaction with fire-delivery and radioelectronic suppression systems, and if need be, should be employed on their own. It is expedient to organize and effect electronic suppression primarily in performing such operational and tactical tasks in which the role of electronic equipment is particularly important, for example: disorganizing the enemy troop command-and-control system; disrupting the planned operation of enemy technical reconnaissance and EW systems; ensuring overflight by aviation through the enemy air defense system and the passage of missiles through the enemy anti-missile systems; ensuring the overflight passage and the return of air assault forces; repulsing the landing of enemy naval forces and assisting the landing of friendly forces; conducting counterbattery activities;

blocking enemy penetrating groups and air assault forces; repulsing massed missile and air strikes; and fighting armored groupings, combat robots, and other remotely controlled systems.

EWW targets can be semiconductor-based electronic equipment. The following groups can be singled out, in the order of their priority and importance on the battlefield:

Group 1: radars (in the air-defense system, field artillery, and tactical and army aviation aiming and guidance systems);

Group 2: all types of radio stations, other electronic equipment of troop and weapon command-and-control systems, and reconnaissance and EW systems;

Group 3: radioelectronic, optico-electronic, and TV means and devices mounted on combat equipment and weapon systems, especially on combat robots and automated command receivers/transmitters;

Group 4: electronic equipment (onboard navigation means, radio-detonators communications, and remote command-and-control systems) of aircraft, warheads of missiles of all types, guided and homing ammunition and submunition; and

Group 5: influence mines.

While damage to the first three groups of targets is related to the task of weakening the enemy combat potential, damage to the last two groups of targets is aimed at protecting friendly troops against enemy impacts, and ensuring survivability. Damage to Group 1 targets can sharply impact on the enemy's combat capabilities, and jeopardize the fulfillment of its combat tasks; damage to Group 2 targets can

substantially complicate its actions; and damage to Group 3 targets can lower the effectiveness of combat equipment and weapon systems on the battlefield. Thus, for instance, the disabling of the radars of field artillery or the air defense system or the tactical aviation aiming and guidance system can not only impair the operational effectiveness of these weapon systems but also frustrate the execution of their combat missions.

From the point of view of main damage effects, electronic suppression differs from the known types of damage. At the same time the commonality of targets (electronic equipment) and the functional character of their damage (suppression) link EWW to electronic warfare (EW). This means that electronic suppression is a type of damage and at the same time a component part of EW. Electronic suppression is the employment -- according to a single concept and plan -- of special munitions and devices whose damage effect consists in electromagnetic radiation, with the aim of temporary or long-term disruption of the operation of enemy electronic equipment. It is a component part of EW, is organized and conducted in the area of responsibility of a combined-arms unit by the EW commander in interaction with EWW carrier command-and-control bodies, and is based on the given situational data, the tasks assigned by higher command, and the commander's concept.

EWW can be subdivided by mission: EWW aimed at engaging ground (surface) and air targets and at ensuring protection against precision weapons; by the effective range: short- and long-range; and by basing methods: ground- and air-based. Close-range electronic suppression should include directional radiation EWW mounted on mobile systems and used within a direct visibility range to neutralize ground or air

targets and also to ensure protection against enemy precision weapons. Long-range systems include weapons capable of impacting on the effective range of delivery means: aviation, rocket, and missile complexes, and artillery.

In the overall effective engagement system, electronic suppression will be ensured in interaction with other types of effective engagement and electronic suppression. Therefore in an operation it may not have an independent structure, like engagement by conventional or nuclear weapon systems, but be used as an additional method of impact in the process of inflicting other types of damage and electronic suppression. Proceeding from this, it should be organized and effected based on the chosen order for using basic damage infliction means both in the entire area of responsibility of a given unit, in the interests of the operation as a whole, and in sectors assigned to its particular elements.

For missions requiring isotropic distribution of the damage-producing element, with consideration of limitations on breakdown of the atmosphere, radii of damage caused by electromagnetic munitions to targets having electronic equipment in their makeup is approximately an order of magnitude higher than for fragmentation-HE munitions of the same caliber. It is also important that in terms of their size, electromagnetic munitions can be integrated into practically all existing weapon systems (even into projectiles less than 120 mm caliber and right down to 20 mm). On the one hand, this promises a great saving of assets, but at the same time requires

special research to determine specifically in which weapon systems the combat capabilities of electromagnetic munitions can be realized most fully.[127]

Although it promises economy, outfitting systems already in the inventory with electromagnetic munitions involves placing increased and extremely rigid demands on these munitions. Nevertheless, resolution of this contradiction is possible in realizing the following directions of priority introduction of electromagnetic munitions:

- use electromagnetic munitions to rationally equip systems whose nature of tactical employment is such that even the minimal effect of the radio-frequency electromagnetic radiation they form is much higher than the effect of fragmentation-HE munitions of similar size (an example can be aircraft systems of close-in defense against SAM attacks, where it is enough not even to disable the homing head or proximity fuze, but to "blind" them for a few milliseconds);

- use electromagnetic munitions to equip narrowly specialized systems with a limited list of targets to be engaged (for example, systems for suppressing an enemy's active defense), whose stability to radio-frequency electromagnetic radiation already is known or can be determined after the very first combat use; and

- use electromagnetic munitions to equip systems which can conduct volley fire or can fire cluster munitions, inasmuch as the supercumulative effect of the pulse sequence of radio-frequency electromagnetic radiation on electronic equipment is known.

As a result, equipping operational weapon systems with electromagnetic munitions will lead to the appearance of weapons occupying an intermediate position in the nature of combat effect between fire-delivery weapons and ECM equipment.

---

[127] A. Prishchepenko, "Electromagnetic Weapons in Future Battle," MS, No. 3, 1995, pp. 71-72.

And their differences from the latter will be that even after the effect of radio-frequency electromagnetic radiation has ceased, electronic equipment will lose its combat effectiveness temporarily or persistently. And this in turn will require considerably less expenditure of weapons with conventional munitions to destroy these targets should it be required.

VII. COUNTERING C^4 ISR/EW SYSTEMS

RUSSIAN VIEWS ON FUTURE TRENDS

In analyzing the destructive properties of various types of weapons, General-Lieutenant A. Paliy notes that despite their diversity, the effect on targets is determined primarily by three basic forms of energy -- physical, chemical, and biological. Depending on the forms of destructive energy, it is possible to define the kinds of weapons being used at the present time (or which may appear in the future), the means of protection, and the kinds of warfare equivalent to them.[128]

General Paliy gives principal attention to analyzing means of physical destruction, which can be represented as the result of casualty and damage effects of physical energy capable of disrupting the functioning of or destroying personnel, means of warfare, military installations and structures, and also affecting people's minds, behavior, and their delayed hereditary, carcinogenic, fetal, and other effects. In a number of cases the effect of powerful physical energy can alter the state of the natural environment, stimulate natural disasters, and disturb the ecological balance in nature.

Based on the forms of energy used, it is possible to describe physical destruction in mechanical (kinetic), acoustic, electromagnetic, radiation, and thermal terms. Inasmuch as there are common properties inherent to acoustic, electromagnetic, and partially radiation kinds of destruction which are of a radiated (wave) nature, in classifying them this permits consolidation into one kind which can be conditionally

---

[128] General-Lieutenant A.I. Paliy, "A Methodology for Classifying the Means and Forces of Warfare," VM, No. 2, 1993, pp. 53-60.

called "radiated destruction." The energy not of substances but of physical fields is issued here in contrast to means of mechanical (kinetic) destruction. In connection with this the effect of the radiated energy on electronics, weapons, military equipment, targets, and people as well as protection against radiated destruction can be called "radiated warfare."

Contemporary armed forces chiefly employ weapons which act by kinetic, nuclear, and thermal energy. But even now means of radiated destruction -- laser, radio-frequency, accelerator and infrasonic -- are beginning to enter the inventory which possess significant destructive capabilities and essentially instantaneous action (see Figure 12).

Kinds of Casualty and Damage Effect (Destruction)	Kinds of Means of Destruction (Weapons)	Nature of Casualty and Damage Effect on Targets
Acoustic	Infrasonic weapons; acoustic generators; explosions generating (forming) acoustic energy; means of acoustic (sonar) suppression	Functional and structural disturbances in living organisms and demoralization or death of people; suppression of operation or disabling of acoustic equipment, diversion from targets of weapons guided by acoustic (sonar) means; destruction of earth's ozonosphere
Electromagnetic	Laser and radio-frequency weapons; nuclear weapons (electromagnetic pulse); means of electromagnetic suppression	Destruction of cells of living organisms; charring, partial fusion, or vaporization of surface of objects; structural changes of equipment materials; suppression of operation or disabling of electronics and of electrical and optical devices; effect on minds, behavior, and reproductive function of humans
Radiation	Particle-beam weapons; nuclear weapons (ionizing); elementary particle accelerators; nuclear power plants; radiological weapons; radioactive substances	Ionization, structural changes (destruction), other disturbances of physical and chemical processes in organisms, military equipment materials, structures, and environment; radiation sickness; genetic changes in populations

Figure 12

Radiating weapons and equipment for electronic countermeasures (ECM) use one and the same kinds of energy, but depending on the magnitude they can either suppress the operation of electronics or destroy their sensitive elements, cause personnel casualties, and also damage certain kinds of weapons and military equipment. Therefore ECM should be considered one of the degrees (a level) of radiated destruction, and electronic warfare (EW) should be considered the content or a component part of radiated warfare and consequently also of warfare as a whole.

It is believed that success in EW is equivalent to achieving superiority over the enemy in combat power and can become the key to victory in the operation (battle). Thus, with electronic suppression of reconnaissance and command-and-control systems, precision munitions, surface-to-air missile (SAM) systems, aircraft, ships, and spacecraft, their combat employment becomes altogether impossible.

Reconnaissance also should be viewed as an inalienable element of any battle, engagement, or operation and not as a kind of support, since effective destruction and protection in warfare are possible only with timely identification of the composition and operations of forces and the coordinates of enemy targets. The unity of reconnaissance and destruction as bases of combat operations is clearly visible in the introduction of "reconnaissance-strike" and "reconnaissance-fire complexes" to armed forces. According to Soviet and Russian military scientists, reconnaissance-strike (strategic) and reconnaissance-fire (operational and tactical) complexes consist in a triad of 1) highly effective ground-, air-, and space-based reconnaissance, surveillance, and target acquisition (RSTA) systems; 2) deep-strike systems; and 3) intelligent command-and-control systems that ensure the delivery of strikes in real time.

Similar reasoning also is applicable when determining the place in warfare of maskirovka (cover, concealment, and deception). Its means and techniques contribute to protection against destruction and ECM, to increased survivability, and to preservation of the combat effectiveness of forces. For this reason it is also legitimate to include maskirovka among measures for protection against destruction and to consider it a component part of combat operations. Maskirovka is outgrowing the framework of a kind of combat support and is becoming a form of day-to-day activity of troops in peace and wartime. In connection with this, a number of authors are proposing more aggressive operations to combat enemy reconnaissance instead of using reconnaissance countermeasures.

Russia is forging ahead with large-scale research into the development of high-tech weapons despite the nation's economic crisis. Many of the country's top scientists are employed on a wide range of major arms projects, not just to boost domestic defense but to capture lucrative overseas sales. British and Western experts would be anxious to get their hands on top-secret scientific data. "Weapons research is continuing in all areas -- the range is extensive," says Robert Hall, editor of Jane's Intelligence Review.[129]

The Russians have already demonstrated that they can generate 10 times the electromagnetic energy the United States has achieved and with much smaller equipment. This could be used in a variety of weapons, such as tank guns and an air "bomb" that could disable all electronics over a wide area. There is also speculation

[129] Charles Miller, "Major Efforts to Develop Advanced Weaponry," London Press Association, 1 March 1994.

that the Russians have developed an ultra-quiet submarine propulsion system that uses electromagnetic forces to draw in water through a duct and squirt it out the stern. Some of their electronic systems have confused Western experts, including the Zasion radar fitted to MiG-31 aircraft. Leading electronics expert Mike Witt has noted that: "This system puzzled Western experts when it was unveiled in 1991 because it appeared to be able to see backwards." Russian scientists are also working on a system known as Infrared Search-and-Track that detects aircraft by their heat and, therefore, overcomes so-called "Stealth" technology. Britain is developing a similar system for the four-nation Eurofighter project and scientists would be very keen to establish how the Russian system works.

COUNTERING THE RMA

According to General Staff analyses, a classification of possible measures for protecting the 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

Like its Soviet predecessor, the Russian military views third-generation nuclear weapons as a critical component of the RMA. Defense Minister Rodionov has mentioned "the possible appearance of third-generation nuclear weapons in the next

few years."[130] V.N. Mikhaylov, Russian minister for Atomic Energy, has argued that third-generation nuclear weapons will be "capable of destroying enemy strategic targets both in space and on earth," and may be usable "in any conflict."[131]

Unlike today's warheads, third-generation weapons will have a small fraction of the global contamination effects, but with the same destructive capability. They will be weapons of directional, selective emission of energy on a target. Such a weapon works like a scalpel. A laser-beam, electromagnetic, X-ray, or microwave radiation; a shock wave: the force of any of these factors is concentrated in the direction of the target. Their development is now under way, and they may well appear within ten years or so. The only barrier to this would be the total prohibition of nuclear tests.

General-Major V.S. Belous has repeatedly warned of the continuing U.S. development of third-generation nuclear weapons.[132] He notes that special charges (munitions) in which the energy of the explosion is redistributed in favor of one of the casualty-producing factors because of a special design served as the origin of third-generation nuclear weapons. For example, the neutron weapon is said to have met the requirement of the Pentagon to develop tactical nuclear weapons capable of destroying enemy personnel with "minimum collateral effect."

---

[130] Colonel-General I. Rodionov, "On Several Problems in the Development of Military Science," VM, No. 11-12, 1991, p. 47.

[131] V.N. Mikhaylov, "The Keys from the Nuclear Arsenal," Pravitel'stvennyi vestnik, No. 12, 1991, p. 12.

[132] For example, see FitzGerald, Transcript.

Belous claims that when the United States resumed nuclear testing after World War II, a new physical phenomenon was discovered – the creation of a powerful pulse of electromagnetic radiation (EMP) -- that proved especially effective in high-altitude bursts. The frequency spectrum of the EMP, corresponding to the radio waveband, is capable of disabling electronic gear, communications and power lines, radios, and radars at great distances.

He charges 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.

The casualty effect of the SHF microwave weapon, which has been under development at Sandia National Laboratory beginning in 1983, is based on the use of powerful pulses of electromagnetic energy with a wavelength from a millimeter to a meter. The goal is to create a weapon distinguished by aim and narrow directivity of effect. The diameter of the casualty field on the earth's surface should be around 10 km. One design of this weapon consists of three successively arranged explosive electromagnetic generators in which high-speed compression of the magnetic field occurs with the help of the explosion of a small nuclear device. In using this weapon

special significance is attached to combatting "targets which may change their positions."

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. With their detonation there is a considerable increase in energy going to form the crater, areas of physical destruction, and seismic waves. The first model of a penetrating warhead was developed for the Pershing II missile in the early 1980s. The casualty effect of such a warhead depends on the TNT equivalent of the charge and degree of its burial. Theoretical calculations relying on results of underground nuclear bursts showed that for reliable destruction of hardened targets it is necessary to ensure a considerable burial of the nuclear charge in the soil. For example, the destructive effect of a 200-kt nuclear charge detonated at a depth of 15-20 m is equivalent to the surface burst of the 600-kt warhead of an MX missile.

Russian experts also assert that 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. A small, dense particle possessing great kinetic energy because of high velocity is the basis of the new weapon. In striking the target such a particle is capable of damaging or even piercing the casing of a warhead or decoy, which will be demolished on entering dense layers of the atmosphere as a result of intensive aerodynamic heating.

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. V. Mikhaylov, Russia's minister for Atomic Energy, has noted that "You can drop a couple of hundred little bombs on foreign territory, the enemy is devastated, but for the aggressor there

are no consequences."[133] 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. In the words of Yu. Khariton, it has "many subtleties and much elegance."[134]

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.[135]

---

[133] V. Mikhaylov, Komsomol'skaya pravda, 19 July 1990.

[134] Cited in M. Rebrov, "Three Generations of Bombs...," KZ, 27 October 1992.

[135] Interview with Viktor Nikitovich Mikhaylov, minister of Atomic Energy of Russian Federation, "Russia Is a Great Nuclear Power," VPK, No. 4(7), 1994, pp 4-10.

According to Colonel-General Ye. P. Maslin, neutron munitions belong to a fundamentally new variety of nuclear weapons, which can be called selective-effect weapons. There can be several types of such weapons. A distinguishing feature of neutron munitions is the substantial increase in neutron yield per unit of power. In addition, neutrons which form during the explosion are distinguished by increased energy, which reinforces their casualty and damage effect. The casualty radii of neutron munitions for personnel are the very same as in the explosion of a conventional atomic munition of ten times greater yield. At the same time, casualty radii for shock-wave and thermal radiation even turn out to be somewhat less than from an atomic munition of equal yield, since a significant portion of explosion energy is carried off by neutrons. As a rule, the size of the area of physical destruction and consequently of possible obstacles in the path of advancing troops from the explosion of a neutron munition turns out to be several times less than from the explosion of a conventional atomic munition.[136]

Like any other explosion, a nuclear explosion is a powerful source of energy which in principle can be converted and used most effectively in a specific, special situation. Conversion of the nuclear explosion's energy into any given form naturally is a very complex S&T task because of the extremely high energy density and extremely limited time of its release. But there are no fundamental limitations on solving this problem; therefore it is theoretically possible to create devices converting the energy released in a nuclear burst into specific casualty-and-damage factors such

[136] Colonel-General Yevgeniy Petrovich Maslin, "Nuclear Weapons: Results and Prospects," VPK, No. 4(7), 1994, pp. 31-35.

as electromagnetic emission of the radio frequency or x-ray bands of wavelengths or the flux of high-speed plasma or metal particles.

The formation of a narrowly directional beam of such casualty- and damage-producing elements is a further development of these kinds of weapons. This permits the creation of directed-effect weapons having a large casualty radius with minimum effect on oneself. But its realization requires solving a large number of technical tasks dictated by the difficulties of preserving the converting devices under the strong effect of a nuclear explosion during release of the energy of this explosion.

One of the most familiar versions of directed-effect weapons is the x-ray laser. The press has reported that the principle of its operation was checked for the first time in a U.S. underground nuclear test on 14 October 1980, and there is information about a large number of other similar experiments being conducted, but a combat version of an x-ray laser was not created. In the assessments of "U.S. specialists," its creation will require several tens or hundreds more underground nuclear tests.

The principal trend in work to create the majority of versions of third-generation directed-effect nuclear weapons is the attempt to ensure high effectiveness in damaging enemy technical equipment with minimum collateral effect on one's own nearby systems. Versions of selective-effect weapons also are being examined which provide for disrupting the working capacity of electronic equipment at distances of tens and hundreds of kilometers with relatively little effect on the environment and on one's own technical equipment, which must have necessary resistance for this. Versions of

directed-effect weapons form a localized damage radius at great distances, but in a narrow beam, and they facilitate obtaining a guaranteed damage-producing effect.

Versions of selective-effect weapons such as so-called electromagnetic pulse munitions, used to create an electromagnetic pulse with an intensity of up to 400-500 kw/m or more, lead either to a temporary loss of working capacity of the target's sensitive components and interruptions in operation or to malfunctioning of sophisticated technical systems over a large expanse.

WEAPONS BASED ON NEW PHYSICAL PRINCIPLES

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.)

COUNTERING COMMAND-AND-CONTROL SYSTEMS

Soviet and Russian military scientists have noted that the essence of warfare in the sphere of command and control consists of opposing the purposeful intellectual-organizing activity of enemy command personnel, achieving advantages in the technical sphere, and disrupting the stable functioning of his command-and-control systems.[137] Active pressure on systems for command and control of forces and weapons is said to be an effective method of achieving the goals of warfare in the sphere of command and control. The attempt by opposing sides to partially or fully disrupt their functioning is a characteristic feature of modern military art which is the result of a number of factors, above all a sharp increase in combat effectiveness of equipment capable of

[137] For example, see Colonel R.M. Portugalskiy, "On the Struggle in the Sphere of Command and Control," VM, No. 3, 1991, pp. 25-30.

accomplishing this mission. Precision weapons have appeared. Troop attack, fire, maneuver, and airmobile capabilities have risen. Electronic countermeasures equipment is developing rapidly, a new generation of electronic systems is being introduced, and so on.

According to Soviet and Russian experts, a qualitative leap also occurred in reconnaissance equipment in the last decade. On the whole, an evaluation of existing equipment only according to range of effect (65 percent of command-and-control facilities of operational-tactical echelons are positioned at a depth of up to 10 km and 15 percent up to 40 km), indicates that the goal of active pressure on systems for command and control of enemy forces and weapons can be achieved by destroying their most important elements, and by capturing, disabling, or neutralizing radio nets (links) as well as radar and radio-navigation equipment (see Figure 13).

Range of Forces and Equipment Influencing Stability of Command-and-Control System Functioning

	Forces and Equipment						
						For Neutralizing:	
Characteristic	**Aircraft**	**Airborne Launchers**	**Airborne Forces**	**Artillery**	**COMINT Equipment**	**Radio Communications**	**Radar**
Range, km	2,000	300-500	100	35	Up to 70	20-80	15

Figure 13

Aircraft are said to have great capabilities for destroying command-and-control facilities, communications centers and lines, and other installations of command-and-control systems. In Vietnam, U.S. aircraft used guided bombs with television and laser homing systems. Air strikes in the Gulf War were characterized by high effectiveness. Artillery also is capable of accomplishing the mission of disrupting the functioning of

enemy command-and-control systems. Missions of disorganizing command and control can be accomplished by operations of forward and enveloping detachments and raiding parties, which possess such capabilities to the greatest extent.

Jamming radio communications and radar and radio-navigation equipment is said to be one of the most effective forms of disrupting command and control of enemy forces and weapons. It began to be used during World War II. Subsequently the rapid development of radar equipment as well as ECM equipment dictated the origin of new concepts such as "radio warfare," "war on the air-waves" and "electronic warfare." The last local wars were characterized by a great diversity of techniques and methods of accomplishing missions, which spawned the following conclusions. First of all, EW equipment capabilities are constantly growing, and their proportion in accomplishing missions is increasing. Second, it is possible to accomplish a large set of missions by employing ECM personnel, and equipment emitting electromagnetic energy is the priority. Another legitimate conclusion is that in combination with the destruction and capture of electronic targets, ECM can allow changing the operational-tactical situation in a certain manner and influencing the success of the operation or battle.

According to Soviet and Russian experts, it is advisable to be guided by the following principles in accomplishing missions of disrupting command and control: maximum pressure on all detected targets of the opposing side's systems for command and control of forces and weapons with mandatory concentration of efforts on the most important of them (command posts, aircraft vectoring centers, and so on); comprehensive use of reconnaissance equipment as well as of forces intended for disrupting command and control (which showed up to the greatest extent in wars in the

Near East); and comprehensive support of personnel and equipment, including those employed to pressure component elements of enemy systems for command and control of forces and weapons. Centralization of the personnel and equipment involved, especially in the planning stage, and strict responsibility of officials for their preparation and employment is the main principle of achieving the goals of disrupting enemy command and control. Finally, warfare in the sphere of command and control is multi-faceted and holds an important place in achieving the final objectives of the war, the operation, and the battle.

Experts such as General-Major R.M. Yusupov have examined the basic methods of disrupting the stability of an opponent's C^2 systems.[138] The problem of command-and-control stability is said to have acquired special urgency in connection with the high dynamism and transient nature of combat operations, the complexities of their preparation and the leadership of forces, and increased enemy capabilities for detecting and engaging command-and-control system targets. The experience of local wars of recent years -- including the Gulf War -- confirms that the course and outcome of military operations are directly dependent on the opposing side's capabilities for disrupting command and control. The presence of perturbing effects disturbs normal system operation and reduces its capabilities.

According to Soviet and Russian experts, there are three basic sources of perturbations: the environment, the system itself, and the enemy. Perturbation of the

[138] For example, see General-Major R.M. Yusupov, et al., "Ways of Comprehensive Research of Command-and-Control Stability," VM, No. 11-12, 1991, pp. 16-21.

environment involves various natural phenomena, and geophysical factors (floods, earthquakes, storms, atmospheric phenomena, and electromagnetic interference). The system itself acts as a source of perturbations in case of equipment failures and personnel errors. Equipment failure involves damages to mechanical and electronic parts, incorrectness of programs, and distortions of data in the process of their collection, processing, storage, and communication to the troops. Personnel errors are subdivided into miscalculations by teams (operators) and by persons making decisions.

An analysis of perturbing effects is said to reveal the following basic kinds of possible consequences: impossibility of command and control at a given command-and-control facility as a result of its total disabling; temporary preclusion of command and control at a command-and-control facility with destruction of information bases or heavy distortion of data, including programs; and reduced quality of command and control at a command-and-control facility with its individual elements disabled or data partially distorted. These consequences also can occur in the event of total or partial jamming of communications equipment.

The enemy can also exert a wide range of purposeful effects on the command-and-control system. For example, he can employ conventional, nuclear, and precision weapons against command-and-control facilities, communications centers, and other installations; use electronic countermeasures; exert a psychological and psychotropic effect on personnel; and so on. Manifestations of these effects involve total or partial damage to command-and-control entities, destruction of command-and-control facilities, disabling of command-and-control equipment, introduction or leak of false

information, distortion of information, electronic suppression of the most important equipment, failures in software, and so on.

According to Soviet and Russian military scientists, "information weapons" are regarded as one means of conducting warfare. These are systems of specific data-base devices designed to destroy the enemy's information assets. The "logic bomb" is a program which is activated at a certain signal or at a preset time for destroying or distorting information. A "program virus" is even more destructive, since it can produce "logic bombs" and insert them into interacting information nets. The "Trojan Horse" is a program whose introduction provides secret access to enemy information -- "a neutralizer of test programs" for revealing random or deliberately installed bugs in software. In addition, there are various kinds of deviations and bugs deliberately incorporated in software by the individuals preparing it. Certain of these have undergone practical testing.

"Information weapons" pose the greatest danger because their use is impersonalized and is easily disguised as steps to protect the copyrights and patents of companies. When a large volume of programs is prepared, it is not difficult to create sections with several commands in each, which, when the system is operated, can be turned into any type of bug.

At the present time it is possible to tentatively single out several types of special effect on enemy computers:

1. Include appropriate elements in the software of weapon, command-and-control, and communications systems in advance which disable the computers being served (the elements are activated at the expiration of a certain time

interval, by special signal or by another method). The failure may be perceived as a natural equipment malfunction.

2. Introduce computer viruses by agents, over communications channels, or by other methods to destroy data in data banks and combat system software.

3. Enter communications channels between computers and introduce false data in them.

4. Disable computers and erase data by a powerful SHF emission, by electromagnetic pulse, or in another way.

COUNTERING EW SYSTEMS

Soviet and Russian military scientists have also examined possible counters to the opponent's application of advanced EW systems.[139] They describe recent searches for new methods of disrupting the operation of electronic equipment as well as for new means of combatting it -- particularly by affecting its software (database organization and support). Of interest in this respect is the possible threat to computer system networks of automated systems for command and control of troops and weapons resulting from the deliberate introduction of a so-called "computer virus" into the channel of an information-calculation system or directly into a computer. The latter is rather difficult to detect and difficult to counter, since it can not only perform destructive work, but also upgrade itself.

Russian experts predict that a qualitatively new stage in solving the problem of interference immunity of electronic equipment may come with the development and

[139] For example, see Colonel V.V. Krysanov, "On Incorporating Electronics into Forces and Equipment," VM, No. 5, 1991, pp. 17-20.

introduction of weapons based on new physical principles. "Western military specialists" believe that achieving "total superiority on the airwaves" necessitates not only functional damage to enemy electronic equipment, but also the total disabling (disruption of operation) of various electronic objects simultaneously over large expanses. Employment of accelerating (beam), SHF, and especially EMP weapons in the initial period of war can considerably influence the course of military operations as a whole by paralyzing the operation of electronic equipment.

The development of means for disorganizing command and control of forces and weapons is said to dictate a need to search for and adopt appropriate countermeasures for "electronic cover" or "cover on the airwaves." They can be viewed as a new component of operational cover representing a set of measures carried out in an overall system with consideration of the predicted electronic environment in certain regions and TVDs. Such measures include the following: SIGINT collection in a contiguous territory (water area, air space); planning and conducting measures for countering enemy electronic detection equipment; conducting measures to uncover enemy military preparations; ensuring effective use of friendly electronic equipment; preparing personnel and equipment for disorganizing enemy command and control and for disrupting his first massive electronic attack; and so on. Advance fulfillment of specific measures for the electronic preparation of TVDs and operational axes is therefore advisable. Command-and-control facilities, communications centers, reconnaissance and EW equipment, and other targets are considered mandatory components of operational preparations of a TVD.

The growing scale of the use of electronics in reconnaissance and weapons systems poses in a new way the task of ensuring survivability of troops and military equipment during combat operations. Here the trend toward incorporation of electronics is actively manifested above all in electronic protection and electronic maskirovka of troops (the latter is considered an advanced element of operational maskirovka). Based on the experience of local wars, the first mission was successfully accomplished by creating counter-interference and deceptive emissions, by using diversionary transmitters, by an optimum distribution of operating and alternate frequencies, and so on.

The development of various mockups of military equipment which reproduce emissions characteristic of a specific model is said to be a fundamentally new direction in the development of electronic maskirovka (electronic protection). For example, the United States already has created some 1,500 M-1 tank mockups. Other dummy targets -- "decoys"-- also are being fabricated which should help reduce the effectiveness of SIGINT equipment and guided munitions and ensure the preservation of combat effectiveness. Thousands of weapons mockups made of synthetic materials coated with metallized paint and supplied with thermal emitters served as dummy targets on Iraqi territory against which the MNF aircraft delivered strikes.

Research efforts are said to be creating new aerosol-forming substances for collective and individual protection of military installations and troops. For example, the United States has created a smoke grenade permitting concealment of tanks not only in visible light, but also in the infrared band. Wide use is made of thickening and metallized aerosols capable of protecting objects against detection by laser equipment

and EHF radars. "Foreign military specialists" believe that disrupting the normal functioning conditions of electronic devices for unassisted flight of guided cruise missiles and drones is an important measure for protecting troops and installations against them. It is therefore recommended that the radar (television, thermal) terrain map be distorted by "leveling" important objects to resemble the natural background, concealing reference points, and changing the configuration (of reservoirs, river beds, and so on) using various reflectors.

Onboard systems for self-protection of combat vehicles have been incorporated actively in recent years. Priority here belongs above all to upgrading systems warning tank or aircraft crews about detection of radar emissions and automatically laying down a smoke screen or ejecting chaff. Even now many armies are using releasable thermal decoys. The development of "active protection" using "anti-projectiles" also is under way. Stealth technology is another new direction in combat vehicle self-protection. To this end special dyes are being used which reduce the signature of objects, and "low-reflective" constructions and radio-reflecting or absorbing materials are being developed -- which has been graphically manifested in the B-2 and F-117A combat aircraft. The latter aircraft operated more or less successfully during Persian Gulf combat operations.

COUNTERING AIR DEFENSE RADARS

Soviet and Russian military experts have described the equipping of aircraft with advanced anti-radiation missiles (ARMs) as "one of the most important trends" in

further elevating the combat potential of aviation vis-a-vis air defense.[140] These systems are able to defeat radar stations under conditions of tactical and technical countermeasures, which was demonstrated especially clearly during the Gulf War. "Foreign specialists" note that the appearance of anti-radiation missiles in air forces was brought about by the increasing complexity of the confrontation of attacking aviation with the air defenses of the defending side.

The use of new and advanced ARMs is said to presuppose more complicated tactics. The "sweeping of a corridor" -- the suppression or destruction of air-defense radars along the flight paths of groups of strike aircraft -- is becoming the chief mission therein. Launches of ARMs by aircraft when they are located outside the zones of engagement of air defenses are also becoming typical.

According to Russian naval experts, the effectiveness of airpower against enemy surface ships depends to a large extent on the degree of suppression of their systems for detecting air targets and directing shipboard anti-aircraft weapons. Among existing means for carrying out this mission, the more effective are anti-radiation guided missiles (ARGMs) mounted on aircraft which are part of special groups for suppressing air defense weapons, air strike groups, and groups for carrying out demonstrative actions. The special feature of ARGMs is that they destroy or disable enemy radar sets

[140] For example, see Colonel Yu. Omelchenko, "Anti-Radiation Missiles: Development and Methods of Use," Vestnik protivovozdushnoi oborony (hereafter cited as VPVO), No. 12, 1991, pp. 34-37.

rather than causing only a temporary cessation of their operation -- as, for example, in the use of jamming.[141]

At present, "foreign specialists" are considering two basic concepts for creating and developing airborne ARGMs. According to the first concept, the missiles will destroy the radars and fire-control systems of surface ships from outside the close-in air defense zone (50-150 km). According to the second, the missiles will destroy shipboard radars, surface-to-air guided missiles, and air-to-air guided missiles at short distances.

In the course of Desert Storm, massed strikes of the MNF air forces were delivered along with anti-radiation missiles and prior electronic suppression of the communications systems and electronic facilities of Iraqi air defense. From the beginning of combat operations, active use was made of "Alarm" anti-radiation missiles, which had been incorporated by MNF countries even before completion of their testing and played an important role in suppressing Iraq's air defense system.

According to Soviet and Russian experts, a fundamentally new stage in solving the problem of suppressing air defense facilities is the emergence of anti-radiation drones. The "Tacit Rainbow" anti-radiation drone was developed for the U.S. Air Force and Navy and represents a cruise missile capable of loitering aloft for up to 40 minutes. In the long-term it is planned to increase flight time to 80 minutes.

---

[141] For example, see Captain 3rd Rank A. Mazmanov, "Anti-Radiation Guided Missiles of Foreign Countries," MS, No. 2, 1992, pp. 66-70.

Russian military experts note that pilots of the U.S. Navy and Marine Corps made extensive use of decoy gliders to mislead Iraqi air defenses, reveal deployments of units and subunits, and divert anti-aircraft guided missiles away from attacking aircraft. A raid against an airfield south of Baghdad in that city's air defense zone was a typical example of the use of decoys in the early stage of combat operations in the Persian Gulf. Several A-6 medium bombers operated just as carriers. Each aircraft carried eight decoys, which reliably covered a large zone in an area of concentration of air defense assets. This enabled the American pilots to carry out the combat mission successfully.[142]

Decoys have a flight range of 48-113 kilometers, depending upon the altitude at which they are released and their air speed. They conceal the real air strike force, saturating zones of radar coverage with a quantity of targets which exceeds the capabilities of the radar stations. They simulate active and passive radar features typical of aircraft.

HARM anti-radiation missiles carried by multipurpose F/A-18 aircraft were launched immediately after the decoys were released. These missiles were intended to destroy tracking radar locked onto the approaching decoys. For example, more than 200 HARM anti-radiation missiles were launched in the air strike against Baghdad on the first day of the war. It was calculated that the probability of target destruction by

---

[142] Colonel Andrey Smirnov, "Dummy Targets Against Hussein," VPVO, No. 7, 1993, p. 58.

anti-radiation missiles would be increased 2-to 3-fold by using them together with decoys, which would keep the enemy's radar in the operating mode.

Another tactical procedure consisted in sending the aircraft carrying the decoys away from the main strike force and releasing the decoys on one side of the target, while the bombers would approach from another direction. After launching the HARM missiles carried on board, the F/A-18 aircraft would switch to operating as escort fighters to cover the withdrawal of the bombers to their bases.

The Persian Gulf War demonstrated that it was more expedient to use F/A-18 aircraft as decoy carriers, even though they carry 2-4 decoys fewer than the A-6. This is due to the fact that the F/A-18s can release the decoys at higher altitudes and greater speeds. This makes the multipurpose aircraft less vulnerable to the enemy's guided missiles and fighters.

In the later stages of combat operations, after the Iraqi air defense system had been destroyed, it was deemed expedient to use aerial bombs. In addition, HARM anti-radiation missiles were already being installed on the EA-6 electronic warfare aircraft. These aircraft were then used in support of assault operations.

Pilots of F/A-18 aircraft of the U.S. Marine Corps also used TALD decoys. The use of decoys was included in plans for every flight to suppress air defenses in both Iraq and Kuwait (SA-2 SAM systems were deployed around the Kuwaiti International Airport, and SA-6 SAMs were active in the north of the country, where formations of

Iraqi Republican Guards were concentrated). Each aircraft would usually have extra fuel tanks mounted on two armament suspensions and four TALD decoys.

"High-level representatives" of U.S. military planning services note that the decoys are effective only when they take the enemy by surprise. A well-trained operator of an air defense radar system drilled in combat conditions can distinguish a decoy from a real aircraft by differences in the characteristic radar indications, in speed, flight path, and the thrust modulation of the jet engine.

VIII. NEW ORGANIZATIONAL CONCEPTS

KEY TRENDS

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.[143]

With respect to numerical strength of the Armed Forces, it is directly dependent on a given level of readiness and the amount of main arms determining Army and Navy combat effectiveness. This concerns the Strategic Missile Troops, Navy, Air Defense Troops, and Military Space Forces to a greater extent, since it is connected with the complexity of command and control of different types of arms, with the difficulty and duration of training command and technical personnel, with their teamwork, and so on.

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;

[143] Colonel-General Mikhail Kolesnikov, "Colonel-General Kolesnikov on Russian Military Reform," AS, No. 1, 1995, pp. 4-9.

- 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.

Third is the development of armament and military equipment. One of the main tasks in this direction is to increase the effectiveness of weapon systems and military equipment and the level of Armed Forces technical outfitting with modern models. The newest scientific-technical achievements and advanced technologies and materials must be used in conducting RDT&E to prevent a critical military-technical and technological lag behind developed world states. Kolesnikov notes the following as priorities:

- developing and producing highly effective, multifunctional weapon systems supporting real-time operation; systems for command and control, fire control, communications, reconnaissance, navigation, strategic warning, and electronic warfare; mobile non-nuclear precision weapons; and their information support;

- expanding the scale of use of information from space systems by troops (forces);

- keeping the entire strategic arms complex at a level ensuring Russian Federation security, strategic stability, deterrence of nuclear and conventional war, and nuclear safety; and

- enhancing the soldier's outfitting with more effective weapons, individual protective armor, and communications and reconnaissance equipment.

Fourth is a reorganization of the system of orders for armament and military equipment. The present system of orders does not permit fully excluding parallelism and duplication in the development and production of armament and military

equipment. As a result, there is a rather large amount of weapons of the same type in the troops (forces), and the expenditure of state resources is not always justified.

Fifth is mobilization preparation of the economy and the Armed Forces. Sixth is an upgrading of the system of all kinds of support. Three parallel and not always coordinated logistic support systems presently function in the country (Armed Forces, MVD Internal Troops, and Border Troops), which leads to dissipation of personnel and assets. Seventh is an upgrading of the military education and cadres training system. Eighth concerns military science. An orderly system of military science has taken shape in the Armed Forces in recent years as a result of structural and functional transformations, but now the need has matured to concentrate efforts of scientific subunits of the Armed Forces and other Russian Federation troops to solve problems of scientific support to their activity.

NEW C^4 ISR/EW TRENDS: GENERAL

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):[144]

- *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

[144] "Information Technology in the Armed Forces of the Russian Federation," VPK, No. 1, 1993, pp. 57-60.

foundations of the command-and-control system and the coordination of operations in the realm of armed forces information technology. The following measures would be expedient to pursue in these areas:

1. A staff coordinating element -- a Committee on Information Technology for the armed forces -- should be created under the General Staff, answering directly for the resolution of issues in the dissemination of information technology in the armed forces.

Two independent elements could be formed under the Committee for Information Technology of the armed forces: an Expert Council and a Council of Chief Designers. The Expert Council should be composed of leading specialists in the field of information technology from the scientific-research organizations of the Ministry of Defense, while the Council of Chief Designers should include representatives of the General Staff of the Ministry of Defense, organizations in the defense sectors of industry, and the scientific-research organizations of the Russian Academy of Sciences associated with the development of information technologies and systems for military purposes.

2. It is essential to determine the General Customer and the sources, principles, and procedures for financing the work under the program of Information Technology for the armed forces.

3. The creation of centers for the certification and funding of software are also best created in order to provide expert analysis of plans for assessing the quality of information technologies being developed, and for the purpose of ensuring the compatibility of the means of information technology being employed in the armed forces.

The problem of the dissemination of information technology in the armed forces is thus becoming a priority one today, determining both the nature of the armed forces and the principles for its combat application. The economic expenditures for the realization of the Program of Information Sciences will be recouped over a short time through the marked increase in efficiency of the performance of tasks by the armed forces.

According to Colonel-General G.P. Gichkin, the status of the command-and-control system predetermines the effectiveness of using the Russian Armed Forces during combat operations. This was confirmed by the experience of the Great Patriotic War, subsequent armed conflicts, and especially the Gulf War. Thus the set of measures for the reorganization of the armed forces includes the creation and improvement of the command-and-control system, and also the search for new approaches to the organization of communications.[145]

A modern communications system is a complex, multifunctional organism involving numerous various-purpose communications centers and thousands of kilometers of radio, space, radio-relay, tropospheric, and wire communications lines. Its primary mission is to ensure the transmission of all the requisite information in the interests of the command and control of forces and weapons. At present, the armed forces have a large arsenal of means of transmitting information which is steadily increasing. Each of these means has a certain advantage, but at the same time it also

---

[145] Colonel-General G.P. Gichkin, "New Approaches to the Organization of Communication Designed to Guarantee Reliable Command and Control of Troops (Forces)," VM, No. 8, 1993, pp. 35-40.

has operational and tactical peculiarities and drawbacks which are characteristic only of a particular system. A carefully designed and smoothly organized command-and-control system, combined with the skillful utilization of all types of communications and automation systems on a comprehensive basis, can guarantee reliable command and control of forces in present-day operations. In various types of combat operations, one single piece of communications equipment, however perfect it might be, cannot guarantee uninterrupted command and control. Just as success in a modern combat action can only be achieved through joint actions of all the services and combat arms, so uninterrupted command and control can only be secured by a coordinated utilization of all means and types of communications.

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 territorial system will be used in the interests of all forces deployed or executing missions in a given area. Specialized systems are designed to provide assistance in carrying out the missions of reconnaissance, warning, authorization of the use of nuclear weapons, and combat command and control of combined units and formations of forces. All of these systems are to be developed and organized according to a single plan. Uninterrupted command and control will be ensured by using them as a single complex and merging them into a joint communications system of the armed forces. This will be established on the basis of existing communications centers and lines, to be subsequently expanded and augmented taking into account new force structure and deployments as well as the future command-and-control system. It is expected that the communications systems will be expanded gradually: initially, the current communications system will be modernized and its qualitative characteristics improved; subsequently, insofar as the requisite conditions are created, profound structural transformations will take place.

Whereas in the past, while making preparations for offensive operations, primary importance was attached to upgrading communications systems in the military groups and border areas of the former USSR and to creating and modernizing the field systems and equipment of the communications troops within strategic formations, in current defense conditions the foundation of communications is the fixed-site territorial communications system of Russia. It is being established according to a single plan by all the services, all of which will have access to it. At the same time, the existing communications facilities will be used in the interests of all the forces as efficiently as possible. The territorial communications systems will cover all regions of the country,

areas of deployment, mobilization, concentration, advancement, and deployment of forces. They will ensure the exchange of information in the interests of command-and-control posts via a number of echelons of command regardless of their subordination and manner of coordination; be capable of providing any grouping, including mobile forces, with communication; and accomplish this without changing the configuration of the region's communications system. In the future it is essential to establish a communications system for the armed forces with a structure whereby command-and-control posts, wherever they may be located, could be linked to a general communications network at the minimum cost of forces, means, and time so as to provide forces and equipment with command and control. The scale and importance of objectives set for the territorial communications system give sufficient grounds to consider it one of the most important priorities in the development of armaments and military technology. This approach is logical because it is the territorial system combined with specialized communications systems of the services that is designed to guarantee the uninterrupted and prompt command and control of strategic and general-purpose forces.

The Russian military plans to establish the territorial systems in a phased fashion by combining the existing and upcoming communications systems and automated control systems. Currently, efforts have been concentrated primarily on the development of primary networks of wire, radio-relay, tropospheric, radio, and space communications. Subsequently, they will lay the foundation for the creation of automated secondary networks of telephone, telegraph, and facsimile communications as well as data transmission. Automating territorial networks will make it possible to increase the system's capacity and efficiency of utilizing communications equipment

and maintenance personnel, to reduce the time required for the establishment of communications and the transmission of information, and to provide as broad a range of users as possible with communications. Whereas the military's requirements for electronic communications trunk channels were formerly satisfied, as a rule, through the state network, now it is essential that they establish their own service channels. Leased channels will continue to be widely used, but meeting the requirements of continuity and reliability of communications without having their own primary network (at least reserve and redundant channels) would be difficult at this stage.

In view of the introduction of mobile defense in wars and armed conflicts, fixed-site elements of territorial systems should be augmented by field communications networks. Field systems ensure command and control during mobile operations of troops, as well as in emergency situations. Depending on assigned missions and the conditions of utilization, they should be capable of rapid deployment, reinforcement, and restoration, and of high resilience when affected by means of mass destruction and electronic jamming. Their development will be based on the following principles: increased mobility; comprehensive automation; and compatibility with military territorial communications systems and the state communications network -- the system of government communications with technology being as much standardized as possible.

The exhibition of computer technology intended for use by the RF Defense Ministry, which was held at the end of 1994, was highly rated in specialized "computer" publications. The Directorate of Informatization and Automation of the RF Armed Forces, a subunit of the General Staff (Chief of Signal Communications of the

RF Armed Forces), was the organizer of the exhibition.[146] The reform of the command-and-control system of the Russian Armed Forces depends largely on the successful work of this subunit. It is solely responsible for organizing development of the scientific basis of computer technology in industry, for experimental design developments of automated command-and-control systems and computer hardware, and for implementation of the whole program of Informatization of the military department.

At present, associates of the directorate are "curing" the development of command-and-control systems for the RF Armed Forces in several directions. They are engaged in the creation of automated command-and-control systems both for daily activity and for extreme situations, and of general-use computer equipment from large computer systems to personal computers. Under their jurisdiction is the developed automated command-and-control system for mobilization resources, which is intended to combine the structure of military commissariats, troop command-and-control elements, and state industrial enterprises in a data net with the General Staff, the central command-and-control element of mobilization resources of the RF Armed Forces. In addition, they are developing a telecommunications system for the Defense Ministry and future command-and-control systems for the mobile forces being formed, for military lines of communications, and even a system for data support of the war against crime in the RF Armed Forces, which was created by presidential order.

In the opinion of General-Major Viktor Bazhenov, in addition to the obvious "plus" of effective supply of the armed forces with up-to-date computer equipment, this

---

[146] Aleksandr Yegorov: "The Defense Ministry Builds Data Command-and-Control Nets Based on Domestic Computer Companies," KZ, 28 January 1995, p. 5.

brings closer the moment when the domestic industry, after assimilating analogues of the main components and accumulating scientific-technical and production reserves, will switch to its own developments, corresponding to the world level. These are not just good intentions, but an objective need, springing from a number of causes that make it impossible to use imported components in systems which will be on combat duty, in the command and control of mobile forces, and also in automated command-and-control systems in a "special period." One of them, a delicate question, lies in their probable "loads" (various types of viruses, for example).

By streamlining military-technical policy (including in the orders and procurement system), in the context of transition to the market economy and higher technical equipment standards, it is planned to create such a communication system which can effectively address the missions entrusted to it. In so doing, those military communications options should be chosen which best realize the principle of integration by the missions addressed, the spheres of combat action, and the unity of command and control in peacetime and in wartime, which means : first, a more effective utilization of the command-and-control system's potential, eliminating its redundancy (any system is the more economical, the more of its service assets are generally available); second, a single technical development policy and, as a result, a reduction in the range of types of technical equipment and information systems, expanding the scope of their unification and standardization; and third, upgrading the quality of service and maintenance, based on the implementation of uniform organizational-technical principles in building a command-and-control system and eliminating inter-departmental (inter-agency) isolation.

NEW C⁴ISR/EW TRENDS: SPECIFIC

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.[147]

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.

---

[147] Vadim Byrkin, "Grachev Says Military Budget Cuts 'Criminal'," ITAR-TASS, 8 July 1994.

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.[148] 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.

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.

---

[148] Aleksandr Pelts: "Defense Minister Clarifies Army Reform Plans," KZ, 28 October 1994, p. 1.

On this basis the Russian Air Forces are qualitatively upgrading aviation groupings by re-equipping them with multi-role aviation complexes using all-weather precision ordnance. In bomber aviation all versions of the Tu-22M and the Su-24 will be replaced with a multi-role bomber with an expanded combat performance. Fighter-bomber aviation will be equipped with the new Su-27 fifth-generation combat aircraft, which is currently undergoing flight testing. Intelligence-gathering aviation will receive intelligence-gathering aircraft developed on the basis of this model. A promising all-weather ground-attack aircraft is also required to replace their ground-attack aircraft. Military Transport Aviation will receive a modern military transport with an enhanced transport and airborne-assault performance.[149]

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.[150]

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

[149] Colonel-General of Aviation Petr Deynekin, "Russia Has Been, Is, and Will Remain a Great Aviation Power," KZ, 19 August 1995, pp. 1-2.

[150] Interview of Colonel-General of Aviation Viktor Prudinov by Aleksandr Ivanov, "Air Defense Troops Will Be the Basis for Creation of an Air-Space Defense," KZ, 9 April 1994, p. 3.

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.[151]

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.[152]

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

---

[151] Colonel Sergey Volkov, and Colonel Yuriy Kovtunenko, "So as Not To Leave the Sky 'Untended'," AS, No. 5, 1994, pp. 8-10.

[152] Interview with Colonel-General Georgiy Kondratyev, "Second Stage of Reform: What Lies in Store for the Army. Colonel-General Georgiy Kondratyev, Russian Deputy Defense Minister, Answers Krasnaya zvezda's Questions," KZ, 22 March 1994, p. 2.

common responsibility and unified direction of training and operations of all air-space defense troops and forces.[153]

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:[154]

- creating a unified automated command-and-control and fire-control system and its subsystem;

---

[153]Colonel-General of Aviation Viktor Prudnikov, "Air-Space Defense," AS, No. 4, 1995, pp. 6-10.

[154] "Colonel-General Semenov on Main Directions of Ground Troops Development," AS, No. 3, 1995, pp. 9-15.

- 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.

Organizational development of the Russian Federation air defense system on a territorial principle has been going on since 1993 in accordance with the Russian Federation Presidential Edict and orders of the Russian Federation Minister of Defense. In accordance with orders, the organizational development of the Russian Federation Air-Space Defense System includes the Ground Troops Air Defense Troops as one component of the system for covering installations of the country and armed forces against enemy air strikes and precision weapon strikes, and the primary means of preserving the combat effectiveness of groupings of the Ground Troops and mobile forces in the course of combat operations.

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). A general-purpose communication system, based on automated primary and secondary communication networks, features a high level of independence with respect to the structural changes

occurring in the armed forces command-and-control system. It should be built according to a single concept and by the joint efforts of the General Staff, combat arms and services, special troops, and other ministries and departments concerned, in close interrelation with the general program for the development of the communications sector in the Russian Federation.[155]

The general-purpose communication system should be based predominantly on the resources of the state network plus the stationary primary network of the Russian Federation Defense Ministry, and have a mobile component (field signal troops element). It needs to be stressed that field communication networks of the services are deployed as a field element according to the emerging operational situation to ensure command and control in the course of an operation.

The Russians plan to ensure the development of the military communication system in gradual stages, based on a coordinated plan for the buildup and unification of the existing communication systems. Additional measures to create communication networks in basic strategic sectors and a space communication system in the interests of all the services will also be taken. The content, stages, and time frame for upgrading the existing command, control, and communication systems should correspond to the analogous stages and time frame of upgrading the Russian Armed Forces structure. At the same time it is necessary to give priority to the development of control and communication systems over the other structures. To this end, it is expedient to adopt a program ensuring: the elaboration and adoption of a state-targeted comprehensive

[155] Colonel-General G.P. Gichkin, "The Signal Troops of the Russian Federation Armed Forces: Problems and Solutions," VM, No. 3, 1995 pp. 21-27.

program for the development of the command-and-control system which in its turn should have a sub-program for the development of communication systems, communication technology, and automated control systems; a priority of projects related to command, control, and communication systems; upgrading command, control and communication systems of the armed forces as a whole, not their separate elements; and a reasonable combination of military command, control, and communication systems with state systems. The implementation of this program will address the majority of questions bearing on the creation of a command, control, and communication system in the Russian Armed Forces that responds to modern requirements.

In the process of the organizational development of the Signal Troops, says Gichkin, it is important to ensure the correspondence of their new organizational structure to the combat composition and missions of the forces and the armed forces command-and-control structure. The main lines of the possible reorganization of the Russian Armed Forces are the following: changes in the system of armed forces command-and-control posts, upgrading the existing centralized combat control communication systems, streamlining the structure of the Signal Troops and their composition, adapting them to operational missions in peacetime and wartime, reducing the general number of communication channels on the main information lines, priority development of satellite communication facilities, and the creation and use of dual-purpose facilities in the military communication system.

In order to implement the proposed lines of upgrading the Signal Troops, the following measures are envisioned:

First. Based on the existing field signal troops contingent, separate, gradual changes should be made in the organizational structure of the Signal Troops, which should include highly mobile communication nodes (centers, groups) and line units. They should not be used as a base for training specialists in peacetime and for deploying troop units in wartime.

Second. In the process of upgrading the Signal Troops, an increase in the share of space communication means should be envisioned. Main efforts should be concentrated on modernizing the technical equipment level of stationary communication nodes.

Third. To ensure in-operation coverage of general-purpose communication systems, brigade-level territorial troops should be introduced, which would be under central and regional command and ensure the coverage of corresponding communication zones (territorial troops organization in a particular region is defined by its specifics).

Fourth. In the process of upgrading the Signal Troops, it is essential to have: at the front level, forward and rear area communication system brigades; and at the army command-and-control level, a communication brigade, created by uniting army signal troops units and elements.

Fifth. Modern communication means and complexes should be introduced. Signal units and elements, equipped with such means, should be able to deploy, in the unit area of responsibility, a communication network, ensuring access to it to virtually

all consumers, and providing guaranteed encryption channels in transmitting any types of messages. If the communication networks have automatic channel- and message-switching capability, signal units and elements should be able to deploy nodal and linear communication modules. Based on preliminary estimates and analysis of trends in signal troops reorganization in the developed countries, it can be supposed that the modular organization of communication systems will reduce the number of personnel in the main signal units and elements by 30-40 percent, at the same time upgrading the quality of communication.

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.

Research is under way into the possibilities of using civilian communication systems in the interests of the armed forces insofar as they meet the military requirements. Production of obsolete equipment or equipment not subject to modernization is to be stopped. The main emphasis will be placed on creating such communication means and automated control systems which have a long service life and are fit for further modernization.

Gichkin stresses that the Russian military is constantly upgrading radio communications, and in a most serious manner. The main efforts of research and production collectives are concentrated on the following directions: increasing the level of equipment automation and the anti-jam protection of channels, including under conditions of enemy EW; integrating with a unified digital communications system (with secondary data-transmission systems); improving qualitative characteristics of equipment and channels; and developing new technology and principles of organizing radio communications (communications systems with automatic relay centers, cellular radio communications, and others).[156]

Successful realization of tasks in each of the directions enumerated can lead not to one, but several qualitative leaps in the area of creating radio communications equipment and systems and to a substantial increase in the role of radio communications in command and control. But here they must solve a rather large number of problems of varying complexity. For example, it is becoming more and more difficult to protect channels against interference, so scientists created adaptation equipment which improved communications reliability under the effect of random interference from 0.5 to 0.9.

The creation of automated adaptive radio networks will permit selecting the optimum data-transmission routes using both direct paths as well as indirect paths via relays. This will help combat not only natural effects negatively influencing channel quality, but also deliberate disturbances of layers of the ionosphere, such as by its

[156] Interview with Colonel-General Gennadiy Pavlovich Gichkin, "The Toiler' Airwaves: Radio Is One of the Primary Means of Command and Control," AS, No. 4, 1995, pp. 16-20.

artificial ionization. In addition, there is a possibility of using a higher frequency band less loaded with random interference but with a large frequency capacity.

The introduction of a cellular organization of communications will provide high-quality information exchange among mobile users and will present them with an expanded spectrum of services: telephone, data transmission, and fax. The development of packet-type radio networks envisages transmitting messages in small portions over several free routes with a high degree of validity. Here it will be possible to organize the so-called "avalanche" transmission of data; i.e., one station of the network transmits a packet and subscribers who have received it relay the message.

It also should be noted that the development and creation of new equipment will permit forecasting conditions of radio-wave propagation and of the interference environment using automated frequency-control stations. Using programmed returning of operating frequencies in receivers and transmitters will preclude spot jamming by the enemy and thereby will protect radio links against deliberate distortions. Using antennas with a controlled radiation pattern and with interference compensators will improve the protection of channels against intelligence collection and jamming.

Implementing organizational-technical and hardware concepts will elevate radio communications to the level of modern requirements for command and control of troops and naval forces. The goal of Russian military-technical policy in radio communications is to create an integrated, automated, jam-resistant territorial-zonal network supporting all branches of the armed forces. This will permit using both direct as well as indirect routes for transmitting messages in accordance with conditions of

radio-wave propagation and deliberate enemy jamming. Automated mobile and fixed radio centers are to become its basis.

The basic radio communications complex which has become operational supports the organization of fixed and primary radio centers of communications systems at all command-and-control levels. Its operation will increase the use factor of technical equipment from 0.1-0.2 to 0.4-0.6, it will substantially reduce channel preparation time, and it will increase channel traffic capacity by 25-30 percent. As a result, the proportion of information being transmitted over radio channels will be up to 15-30 percent.

In accordance with the new planning, the Russians have begun to redistribute fixed radio receiving and transmitting equipment and remote-control channels and links. Regional adaptive radio links are being organized and tied into zonal territorial primary communications centers. Work is being done to create standardized equipment and to establish communications using long-range scatter and meteor trail UKV (VHF/UHF). Adaptive radio communications equipment is being developed for the tactical command-and-control echelon. The radio center control system is being improved. Other problems also are being resolved in accordance with the "Concept for Development of Communications Systems up to 2000."

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.[157] 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.

---

[157] Interview with Colonel-General Vasiliy Fedorovich Migunov, "It Is Time To Close the Gaps," AS, No. 10, 1995, pp 2-4

IX. POST-ELECTION PRIORITIES

GOVERNMENT VIEWS

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.[158] 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.

Major tasks set by the president thus include ensuring the maximum technical provision and manning of units and formations engaged in the main activities of the armed forces, maintaining the nuclear deterrence force at the proper level, and

[158] Text of Yeltsin Election Program, Rossiyskiye vesti, 1 June 1996, pp. 1-16.

developing the whole complex of information warfare means, high-precision weapons, and mobile defense infrastructure.[159] He also called for an increase in R&D appropriations within the framework of general military expenses: "The strengthening of the scientific and military-industrial potential should allow Russia to independently produce all the necessary types of armaments and military hardware." Military education should be improved and certain provisions of military theory and art should be reviewed.

The Russian Military-Industrial Complex (VPK) will concentrate on designing new state-of-the-art equipment for the Air Force, the Navy, the Ground Troops, and the Air Defense Troops, Yeltsin's adviser told Interfax in an exclusive interview. The VPK will focus on these "elite" areas because the present economic and financial situation in Russia prevents the country from attending to all areas of the complex's development at the same time, he said. However, a selective approach has allowed Russia to create a number of vehicles, ships, and systems in high demand on the world arms market. In particular, Russia has developed the MIG-29 aircraft; an air defense system which is now being created by the Antey concern; and the Grad, Smerch, and Uragan multiple-rocket launchers.[160]

The elite group of the VPK will be formed during 1996 and 1997. These elite companies may become a basis for future "powerful transnational companies" due to their current success in foreign markets. A number of companies in Belarus, Ukraine, Kazakhstan, and other CIS member-states have contemplated joining the "prosperous

[159] Andrey Shtorkh, Moscow ITAR-TASS, 18 July 1996.
[160] Moscow Interfax, 12 October 1996.

concerns in the Russian VPK." Some well-known companies in Eastern and Western Europe have also shown an interest in such cooperation.

In late 1996 Defense Council Secretary Yuriy Baturin gathered together the luminaries of Russian defense science and technology for the first working conference. The defense order does not ensure full loading of enterprises, the participants in the conference said before it started. The creation, testing, operation, and recycling of arms take far more funds than the government can provide. The effectiveness of defense research is falling. Although Russia, along with the United States, Japan, France, and the FRG still possesses 17 critical technologies which enable it to preserve its defense potential, a real threat that this will be lost has emerged.[161]

In the opinion of academician Yevgeniy Velikhov, member of the Defense Council, there are at least two ways to preserve Russia's defense potential. First, to support at the state level those areas where it is possible to produce both defense and commercial output on the basis of dual-purpose technologies. Second, to carry out the full conversion of those production processes where dual-purpose technologies are impossible, leaving only micro-production facilities to create experimental models for the preservation and development of modern knowledge in the sphere of military hardware.

---

[161] Viktor Litovkin: "The Defense Council Gathered Leading Lights Together to Tell Them There are Insufficient Funds for Them," Izvestiya, 24 October 1996, p. 2.

MILITARY VIEWS

According to the new defense minister, retired General I.N. Rodionov, it is impossible to ignore that major states (the United States and other NATO countries) have enormous military might and that they not only are preserving it, but also are reinforcing it, so that a certain quantitative reduction in armed forces is quickly compensated for by adopting new, more effective kinds of weapons. NATO countries presently have around 20,000 different offensive air weapons and a developed system of their basing near Russia's borders, so that they have enormous offensive might which is being developed rapidly. Maintaining superiority in the air-space and at sea is one of the U.S. strategic principles. Under these conditions it is not at all precluded that these countries may employ military force to achieve their military-political goals. Many military conflicts which have broken out since World War II, including the Persian Gulf War, attest to this.[162]

A military threat to Russia's national interests exists and hardly will disappear in the near term. This is confirmed by conclusions from an analysis of actions by probable enemies and allies, which are very important in forming the state's military doctrine. That assessment is not at all simple and lately has been distinguished by extremes. Previously it was considered that almost the entire world was the probable enemies and now -- that all former enemies are friends. That approach is profoundly erroneous. Russia in fact does not now have direct enemies which would immediately

[162] Presentation by Colonel-General I N. Rodionov, chief of General Staff Military Academy, at the General Staff Military Academy's Military-Science Conference from 27-30 May 1992, July 1992, Special Edition, VM, pp 6-14.

threaten it with attack. At the same time, military conflicts are occurring on ethnic, territorial, and religious grounds.

What is the nature of wars which Russia may be forced to wage? First of all, a global nuclear threat will be preserved as long as other states have nuclear weapons and the capability of using them. Secondly, major aggression against Russia with conventional weapons also is possible in the future. The initial period of such a war can differ, but an enemy invasion most likely will begin in air and sea space with delivery of strikes by aviation and naval forces and in the future also from space. It is not precluded that this option of an aggressor's initiation of war will become the most realistic as a result of the existing military-political, military-strategic, and military-technical situation (for Russia and the former Soviet republics). This is also confirmed by the fact that developed countries have powerful, effective means of precision air attack and have an advantage in their development.

A large-scale conventional war also can arise as a result of the development of local wars and military conflicts into a major military clash, as well as because of military assistance being given to one or more countries which have been subjected to aggression. Such a war using precision weapons and enhanced-yield munitions can have serious consequences, and if opposing sides set for themselves the achievement of decisive goals, it is fraught with the constant threat of developing into a nuclear war. Because of the reality of these options, Russia must openly declare that it has the right to use the entire arsenal of weapons at its disposal, including nuclear weapons, to repel aggression.

Thirdly, local wars and military conflicts affecting Russia's national interests may arise. They can be waged with limited involvement of armed forces and the extension of military operations to relatively small territories. But local wars and military conflicts are fraught with developing into major military clashes both from escalation as well as from ruling circles of individual countries using them as a pretext to carry out large-scale aggression.

Fourthly, the country's internal situation can be destabilized by ethnic and religious conflicts, by civil war, and by the intervention of armed forces in these processes. It is curious to note that the concept of employing armed forces for accomplishing internal missions is rejected by opposition forces fighting for power until they obtain it, after which they begin to look differently on the role of the armed forces. Thus the Russian Armed Forces must be capable of conducting military operations of any nature and on any scale.

The methods of military operations of the Russian Armed Forces at the beginning of a war can vary. Previously the state's military doctrine envisaged only defensive operations in the initial period. Later it was presumed that the enemy would be expelled from captured territory with the help of a counteroffensive, and military operations would cease without invading the aggressor's territory. It is impossible to be reconciled any longer with such doctrinal provisions on the methods of conducting military operations. They clearly reflected specific political sentiments and did not consider the laws of warfare. These provisions, predetermining defeat in a future war in advance, essentially are very dangerous for a state.

The new Russian military doctrine must precisely, clearly, and unequivocally reflect the proposition that if an enemy has begun aggression and armed conflict, its evaluation must proceed from the laws of warfare. In this case the armed forces must choose and carry out those forms and methods of military operations most effective in a given situation: the offensive, the defense, and the delivery of strikes against the enemy no matter where he is located. This includes strikes that must be delivered above all against the aggressor country's territory and against his most important military and economic installations. It is also time to reject such concerns as "defensive doctrine," "defensive strategy," "defensive armed forces," and so on. In establishing the Russian Armed Forces it is necessary to set a course not toward their quantitative, but toward their qualitative development. The priority should be given to the new, most effective means of warfare (air-space weapons, precision-guided weapons, and modern command-and-control and reconnaissance equipment).

In the future, says Rodionov, nuclear weapons will be the primary means for deterring possible aggression, which also means preventing war. It is therefore advisable to entirely exclude wordings about the use of nuclear weapons from the content of military doctrine. Everyone must know firmly that in case of aggression against Russia it will employ all means it has to protect its interests.

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.[163] The military-technical policy is a most important direction in the

[163] Colonel-General Igor Rodionov, "In Russia and for Russia: Basic Directions of Military Reform," NVO, 22 April 1995, No. 2., pp. 1, 3.

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. Modern models of armament and military equipment are regarded as high-tech products, and they are the ones that determine the demand for high technologies. Russia's security today, tomorrow, and especially in the future requires precisely high-tech weapon systems.

In addition, the defense order must preclude the possibility that many types of weapon systems for performing the same combat missions will appear in production. It is abnormal when there are 62 basic models and modifications of missile and artillery armament (37 in the United States), 62 models and modifications of armored equipment (16 in the United States), and 26 models and modifications of surface-to-air missile systems (4 in the United States) in service in the Ground Troops. From an economic standpoint, this raises the price of production quite a bit, and from the operational and tactical standpoint, it makes it more difficult to provide technical and logistical support to the troops when conducting combat operations.

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.[164]

---

[164] Army General Viktor Samsonov, "A Different Interpretation of the Concept of War. Time Demands That Karl Von Clausewitz's Classic Formula Be Amended," NVO, No. 23,

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.

On 1 October 1996 Defense Minister Rodionov addressed a press conference and made the sensational statement that nuclear weapons were obsolete and were being replaced by more powerful weapons based on other physical principles. General V.I. Slipchenko has expanded on this theme. In none of mankind's wars have weapons performed an independent role in attaining the war's objectives. They were merely a

---

December 1996, pp 1-2.

means of destroying the enemy or defending against him. Victories depended on the size of the assembled mass of cavalrymen and foot soldiers and the talents of the Tamerlanes or Napoleons sending the masses into battle. That was before the advent of the nuclear era. It makes no difference to the atom bomb whom it destroys: an armed peasant or Alexander the Great. Fortunately, nuclear wars have not taken place, and they are unlikely in the future. But nuclear weapons are being replaced by something else no less dangerous -- the "perfect" weapons of the 21st century.[165]

In the wars of the future , the decisive role will be performed not by manpower and not by nuclear weapons but by precision conventional weapons and weapons based on new physical principles. These new weapons will form the basis of many states' armed forces in 10-15 years. New conventional weapons have appeared, with entire combat systems capable of doing the job of personnel and sometimes of nuclear weapons. The dynamics of the adoption of new types of weapons and means of employing them are as follows: in the 1950-1953 Korean War, nine previously unknown types of weapons were used. In Vietnam in 1964--1975 it was 25. In the Arab-Israeli wars of 1967, 1973, 1982, and 1986 it was around 30. In the 1991 war in the Persian Gulf it was 100. You can be sure that if there is another war, there will be an even greater surge in the growth of the use of new types of weapons.

Kinetic Weapons: "Fire and Forget". The main type of weapon in the 21st century will be a precision weapon. The accuracy of target destruction could be decided not only

[165] Report by Aleksandr Khokhlov on conversation with military analyst General-Major Vladimir Slipchenko, "Secret Weapons of the Future: One Military Generator Can Turn a Division into a Herd of Idiots," Komsomol'skaya pravda, 15 October 1996, p. 5.

by the strategic aims of the war, but by the political aims as well. If you double the explosive force of a missile warhead the weapon's destructive capability increases by 40 percent. If you double the target strike accuracy, the missile's destructive capability increases by 400 percent. Explosives are currently being developed which will be 30-50 times more destructive than familiar, traditional ones, but this is nonetheless a blind alley in military evolution. The future lies with increased weapon precision.

The formula describing a human being's actions in the wars of the future will be a simple one: "Fire and Forget." Everything will be done by the "smart" weapons themselves. At the moment the advanced countries of the world are busy developing tactical, operational, and strategic reconnaissance-strike systems. The reconnaissance elements will be located on artificial satellites.

The main attack element will be high-speed (five to eight times faster than sound) air- and sea-launched cruise missiles. These missiles will be able to destroy targets at a range of 500-8,000 km. They will be "taught" to fly to their targets at altitudes of between 30 meters and 60 km in conditions of radio silence. Using observation, correction, and target designation systems installed on artificial satellites, the cruise missile will travel along a complex path, changing speed and altitude. It will be able to approach an object from the rear, giving the enemy no chance, and dive toward the target at high speed virtually from space.

A number of countries will evidently be arming themselves with massive quantities of these reconnaissance and attack systems in the next 10-15 years. The

radiation-source-seeking systems installed on the combat elements of these weapons will make their accuracy of delivery absolute.

Laser Weapons. It is fruitless to pursue every enemy soldier on the battlefield with a laser. So work is geared to developing laser devices that "blind" weapon-sight optics and combat system electronics. In the future it is most likely that military lasers will be used to disable military space systems. The strategy of nuclear wars provided for nuclear explosions at an altitude of 50-100 km not to destroy personnel, but to destroy electronic instruments with an electromagnetic pulse. Military lasers in future wars could be based on the same "lightning striking the antenna" principle.

Acoustic Weapons. The emission of energy at a certain frequency makes it possible to destroy enemy personnel and radioelectronic facilities. Military generators can be installed on delivery systems at sea, in the air, and in space. They have potential for use on balloons. By directing an energy emission at a target or creating a background energy emission it is possible to turn an enemy division into a herd of frightened idiots. People will experience inexplicable fear and a severe headache and their actions will become unpredictable. They may become totally and irreversibly deranged. Acoustic weapons are under active development, and laboratory versions already exist. Armed forces in a number of countries could have them in 10-15 years.

Electromagnetic Weapons. In theory these weapons can be combined with acoustic weapons, making something called beam weapons. They are based on the principle of emission of energy at different wavelengths. The probable delivery systems are

artificial satellites. Little is known about their destructive effect, although active work is being done to develop them, so these weapons do have a future.

Radiation Weapons. They are based on the use of ionizing radiation for military purposes. Very simply, in Dubna you have electrons and positrons running around the closed circuit of an accelerator. Would there be anything left alive in the area if the circuit were to be opened? It is hard to imagine at the moment the technology involved in using radiation weapons. But work is under way on developing them and the estimated timescale for the development of these systems is 25-30 years.

The new weapons will not just increase the combat potential of armed forces but will change their composition and structure. Operations by ground forces groupings will become a thing of the past, and nuclear weapons, although they will remain, will be supplanted by precision weapons and weapons based on new physical principles. Armies will be small and will have two categories of forces: strategic defensive and strategic offensive. The funds made available as a result of the inevitable reduction in numbers absolutely must be invested in science. To create "perfect" weapons the Russians need a scientific breakthrough in the spheres of microelectronics, fiber optics, and computers not only with a mathematical but also with a geographical memory.

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."[166] It should be noted that the Russian government, including the Defense Council, has approved this proposal.

WHITHER THE VPK?

Russian experts such as Colonel-General V. Miruk have stressed that the course and outcome of combat operations largely are determined by the capabilities of arms and military equipment with which forces are equipped. Air-space defense arms must ensure effective combat against low-altitude cruise missiles, operational-tactical and tactical ballistic missiles, and targets manufactured with small-reflecting-surface technology. Along with upgrading the weaponry of SAM troops and fighter aviation, automated command-and-control systems, and air defense information assets, the problem of creating effective reconnaissance equipment and new EW assets has advanced to the category of priority problems which must be solved. Considering the limitations on defense appropriations for the next few years, this means creating new models of arms and military equipment and conducting preparatory measures that support a high degree of readiness to launch their series production. But series production itself and deliveries to troops should begin only with the appearance of a direct military threat.[167]

---

[166] Interview with Defense Minister I. Rodionov, "Igor Rodionov: Unpopular Measures Can No Longer Be Avoided," Moskovskiye novosti, 11-18 August 1996, No. 32, p. 7.

[167] For example, see Miruk, "Air-Space Defense."

In a December 1992 interview, Deputy Defense Minister A. Kokoshin, head of the Military-Technical Policy Council, thus 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.[168] 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."[169] As Kokoshin has noted, "We are also planning... the establishment of a scientific and

[168] Kokoshin, "Contradictions."

[169] "Defense Minister Grachev Interviewed," in FBIS-SOV-93-109, 9 June 1993.

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."[170]

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^4ISR and EW systems.

In the last six months Defense Ministry analysts, jointly with corresponding government subdivisions, have accomplished much work to correlate the parameters of the development of the Russian Federation's economic capability with force

[170] Moscow Conversations, May 1993.

development plans. This work comprises an in-depth appraisal of complex and interdependent military-economic, demographic, and financial factors. Another area of analysis was the character of future wars and armed conflicts, with due consideration for the growing role of aggregate information, including electronic warfare assets, precision weapons, and illegal means of warfare.[171]

Since the1970s-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. Priority needs to be given to building up the capabilities of friendly forces to defend against current and prospective weapon systems.

In considering the requisite technical supply level for the armed forces, it is essential to bear in mind that owing to the ongoing economic crisis, Russia's

[171] Interview with First Deputy Defense Minister Andrey Kokoshin, by Nikolay Ivanov: "Military Reform Plan Has Been Outlined. By the 21st Century Russia Should Be Ready to Meet All Military Challenges," NG, 24 July 1996, p 2.

capabilities for building up the number of weapons to their optimal strength level and for modernizing and upgrading them are thus far limited. Therefore the main attention will be given to developing cutting-edge weapon systems and defense R&D projects. At the same, time everything needs to be done to maintain the existing equipment and to ensure its gradual modernization. Kokoshin points out that any armed conflicts today are rather politicized, and the use of force even on a very limited scale in most parts of the world immediately -- primarily via television -- produces a reaction from public opinion and the political establishment. Therefore all questions pertaining to the use of military force even on the tactical level should be carefully considered with due account for their impact on politics and the various direct and indirect connections.

Kokoshin notes that aspects of military reform were elaborated in a 1995 study by the General Staff Academy entitled "The Military Security of the Country and the Armed Forces: Problems and Ways of Addressing Them," as well as in a research project completed by the same academy on information warfare, which was supervised by Rodionov and included proposals by well-known Russian military leaders and military civilian specialists from the Academy of Military Sciences and the Russian Academy of Missile and Artillery Sciences.

Options for the combat composition of the armed forces were elaborated until the period 2000-2005. In particular, blueprints were considered for a multi-mission combined-arms division of the 21st century with various weapon systems designed for different theaters of military operations. Such units are designed to be used for a wide range of missions -- from full-scale combat action to peacekeeping operations. The number of such divisions will be relatively small, and they will be used as the basis for

the deployment of large formations in wartime. On the whole it is vital to have a basis for mobilizational deployment, including by employing a new reserve (conscript and officer) training system, and accumulating mobilization resources -- both human and material. Much work is in hand to develop a new type of mixed ground and naval force formation.

According to Kokoshin, 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.[172]

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

[172] Andrey Kokoshin, "What Sort of Army Do We Need: Some Military-Political Propositions of the Reform of the Armed Forces in Russia," Segodnya, 7 August 1996, p. 5.

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); the development of precision weapons of varying range and purpose; the development and adoption of non-lethal means of armed struggle; the improvement of facilities supporting the mobility of combined units and units of the armed forces; the development of the entire complex of forces and systems of nuclear deterrence; and the creation of a fundamentally new system of personal gear and equipment.

The difficulties of the first and subsequent stages of the organizational development of the Russian Armed Forces have been intensified by a whole number of problems which were inherited from the Soviet Armed Forces and which to a large extent have not been tackled for decades. These problems include the imbalance in the development of weapons on the one hand and a number of the systems supporting their

use (facilities of intelligence, command, control, communications, electronic warfare, and concealment); and precision weapons on the other. This stems largely from the growing lag of Russian industry and science in the fields of microelectronics, computer technology, and communications facilities and from the fact that a civilian market for these products has not developed inside the country.

As already noted, the Russian government and Ministry of Defense plan to increase the share of funds allocated for research and experimental design, the modernization of arms and military equipment, combat and operational training, and so forth. This objective was clearly set once more by President Yeltsin at the meeting with the collegium of the Ministry of Defense in July 1996. The military-technical foundation for the rearmament of the Army and the Navy is to be created thanks to this in the period 1996-2002. Considering that until the completion of this period the military's receipt of new equipment will be of an extremely limited nature owing to obvious budgetary and financial factors, it is essential to preserve in a state of combat readiness what is in the arsenals today. This will make it possible to embark on the relatively broad-based rearmament of the Army and Navy as of the period 2002-2007, when the country will have both the resources and a new military-technical base for this.

The army reform must not be reduced to the simple reduction of armed forces, Kokoshin told Interfax in an exclusive interview in late 1996. He said that the Ministry of Defense has worked out a program of reforming the army that would meet long-term conditions and needs. This document provides for setting up new types of units and formations -- it will be a new military organization with a new organizational structure,

equipped with new types of arms and hardware. The reform also implies new approaches to military theory. This question is being intensively discussed at the Defense Ministry and General Staff.[173]

Also 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.[174]

[173] Moscow Interfax, 14 October 1996.
[174] Anatoliy Yurkin, Moscow ITAR-TASS, 23 October 1996.