

# CHAPTER 23

## THE RUSSIAN UNDERSTANDING OF INFORMATION OPERATIONS AND INFORMATION WARFARE

By  
Timothy L. Thomas

**F**inding similarities in the Russian and U.S. approaches to information operations (IO) is not a difficult task. Both countries' specialists closely study electronic warfare and command and control systems of other countries, and both stress the importance of the use of computers and information management in the preparation and conduct of modern combat operations. This includes the use of information to conduct psychological operations (PSYOP).

Upon closer examination, however, the Russian approach to the information warfare (IW) aspect of IO has several elements that makes it unique and different. There are three principal reasons for the distinct Russian method.

First, there is the issue of overall context. The Russian state, economy, and society are in a transition period resulting in institutional and philosophical instability. Russian mass consciousness, according to many prominent scientists and government officials, is vulnerable to manipulation by slick marketing

campaigns and to exploitation by promises of economic and social prosperity during this transition period. As a consequence, the Russian specialists' approach to information threats places strong emphasis on what it terms information-psychological processes as well as state laws to guarantee the information security of individuals and society.

A second reason for a dissimilarity in emphasis is that traditional Russian military thinking developed differently than in the West due to geographical considerations, varied military threats, the economic realities imposed by a different ideological background, and the emphasis placed on the study of military affairs as a science. The Russian study of the impact of the use of information weapons on military art will differ in emphasis from the Western assessment due to this prism through which these operations are viewed and measured, a reflection of the military's traditional thought process.

Finally, the Russian approach is unique due to the budgetary, technological, and infrastructure restraints under which information capabilities are developing. Regarding the infrastructure, it is simply insufficient to handle the onslaught of new technological improvements associated with the information age. The phone system in Russia, for example, is antiquated, with a limited number of trunk lines to handle the volume of calls in most cities. It will be difficult to adapt this system to a greater load caused by computers. Technologically, it will be years before fiber optic cables arrive in some locations, and only recently have computer companies begun the production of all Russian component computers. The inability to produce miniaturized components in a

modern production facility has been the major drawback. Severe budgetary restraints curtail other efforts to bring change quickly to the country.

As a result, Russian scientists have initially spent more time on IO theory than in the West, with the latter focusing on practice over theory. It will take several years for Russia to catch up with the West in the technological area. But backwardness can be turned to an advantage when others pay for the trial and error of first generation technology, provided that there is some plateau at which you reach reasonable parity.

Russian specialists acknowledge this backwardness as a fact and try to work with it. Even though the introduction of information technologies has been ongoing since the late 1970s, it is only during the 1990s that up-to-date systems have been produced. In a discussion of the "information IQ" of the armed forces, that is the ratio of the quantity of equipment required to that in existence, 450,000 computers were noted as still needed, compared to only 25,000 presently in existence. This yields an IQ of 18 out of 100. At that rate, it will take 50-60 years to get to an IQ of 90. Russia probably will get to that figure much faster now that it is starting to mass-produce its own computers. The goal should be attainable in no more than 5 to 8 years, if the budget allows for it. It will be hard to divorce the military IQ from the societal IQ in this area.

In addition to these three reasons, it is also important to remember that only a handful of experts write openly about information operations in Russian military journals in contrast to the hundreds of authors who publish on the subject in the West. Since there is not an official Ministry of Defense [MOD] regulation or

publication that defines and outlines the Russian concept of IW, the West must depend on the viewpoints offered by a few serving and retired officers, narrowing the scope of the dialogue. Fortunately, many of these officers are not only experts in the area but are responsible for teaching information operations subjects at academies and institutions in Russia. Their opinions are worthy of close consideration.

These factors should be considered in the discussion of ten key elements of the Russian approach to information warfare that follows. First, however, a short description is offered of the Russian view of the terms information security and information warfare that serve as a base for the remainder of the discussion. These terms are themselves unique in that they reflect both the Russian experience and dialectical thought process.

## **Defining Information Security**

Russia's national security concept as well as several state laws refer to information security as a national interest of Russia. One of Russia's first attempts to develop a draft law on information security was in 1995. An equivalent document does not exist in America. In defense, this unique and comprehensive assessment discussed critical areas, the status of information security in Russia, perceived threats to information security, methods of providing information security to the state, and the organizational structure and principles of a system of information security. It listed critical areas as:

- information resources of the Ministry of Defense, General Staff, main staffs of the components of the armed forces, and scientific-research

establishments; information, facts, and figures about the preparation and conduct of operational and strategic plans, deployments and mobilizations; and the tactical-technical character of equipment;

- information resources of the military-industrial complex as well as the industrial potential and quantity of raw materials available to the force; information on the basic direction of the development of the equipment of the armed forces;
- the country's command and control system of personnel and weaponry, and their information support;
- the political-moral condition of the force; and
- the information infrastructure (control points and connections, relay points, tropospheric and satellite communications), to include communications with other ministries.

External threat sources included:

- all types of intelligence activities;
- information-technical activities, such as electronic warfare and computer intrusion methods;
- psychological operations of probable enemies, either through special activities or through means of mass communication; and
- activities of foreign political or economic structures that work against Russia's interests in the defense sphere.

Internal threat sources included:

- disrupting established communication and information means in staffs and establishments of the Ministry of Defense;
- premeditated or unpremeditated mistakes of personnel in the information system of special significance; and
- information-propaganda activities of organizations and individuals directed against the interests of the government that result in the lowering of the prestige and combat preparedness of the armed forces.

The draft noted that these threats are particularly dangerous when the military-political situation is aggravated. The information security draft also divided the main methods for improving information security in the defense sphere into three areas:

- conceptual: structure goals to provide security in the defense sphere, i.e., goals which flow from practical tasks or missions, and a correct evaluation of information threats and their sources;
- technical: improve the means of protecting information resources from methods of unsanctioned access by developing protected, secure systems of command and control and raising the reliability of computer resources; and
- organizational: form the optimal structure and composition of functional organs of a system of information security in the defense sphere and coordinate their effective cooperation, improve the methods of strategic and operational disinformation, intelligence gathering, and electronic warfare, and improve the methods and

means of actively counteracting information-propaganda and psychological operations of a probable enemy.

According to the best available information, this draft has not become law. However, a host of other laws (draft or otherwise), edicts, and statutes on information operations already exist.

## **Defining Information Warfare**

While no official (that is, MOD, Security Council, or Defense Council approved) military definition of information warfare has been endorsed to date, several unofficial ones are available from speeches or articles. What makes them distinct is that they are careful not to copy the U.S. understanding of the term. Russian analyst V. I. Tsymbal has noted that “it makes no sense to copy just any IW concept. Into the IW concept of the MOD must be incorporated the constitutional requirements of the Russian Federation (RF), its basic laws, specifics of the present economic situation in the RF, and the missions of our Armed Forces.” In addition, Tsymbal points out, in the RF the organs of state security are responsible for the accomplishment of IW in the broad definition of the term.

Partial confirmation of this fact was recently affirmed by the attempt of the Federal Agency for Government Communications and Information (FAPSI) to have the State Duma allow FAPSI to control the Internet in Russia. FAPSI, the former KGB Eighth Chief Directorate and Sixteenth Directorate, alleged that the CIA was creating information weapons and combat computer viruses, and FAPSI control over these attempts was needed.

Russian definitions of IW encountered thus far do seem to adhere to a common theme that differs from the U.S. view, namely that information warfare is conducted in both peacetime and wartime. In its peacetime use, the term refers to the information security of society and the government in the psychological, scientific, cultural, and production aspects, among others. In its wartime use, it refers to the attainment of superiority in the use of information protection and suppression systems, to include command and control, EW, and reconnaissance.

Retired Admiral Vladimir Pirumov is perhaps the most authoritative person to define the term so far. He is a former instructor of electronic warfare and now is the Scientific Advisor to the President of Russia. He defines information warfare as follows:

*“Information warfare” is a new form of battle of two or more sides which consists of the goal-oriented use of special means and methods of influencing the enemy’s information resource, and also of protecting one’s own information resource, in order to achieve assigned goals. An information resource is understood to be information which is gathered and stored during the development of science, practical human activity and the operation of special organizations or devices for the collection, processing, and presentation of information saved magnetically or in any other form which assures its delivery in time and space to its consumers in order to solve scientific, manufacturing, or management tasks.*

His definition implies that information warfare is an activity that can be carried on in peacetime as well as wartime. For strict wartime scenarios, Pirumov offered a definition of information warfare in operations that aimed at gaining an information advantage:

*“Information warfare in operations (combat actions)” is the aggregate of all the coordinated measures and actions of troops conducted according to a single plan in order to gain or maintain an information advantage over the enemy during the preparation or conduct of operations (combat actions). An information advantage assumes that one’s own troop and weapon command and control components are informed to a greater degree than are those of the enemy, that they possess more complete, detailed, accurate, and timely information than does the enemy, and that the condition and capabilities of one’s own command and control system make it possible to actualize this advantage in combat actions of troops (forces).*

Other Russian definitions of the term information warfare are also available. V.I. Tsymbal, a Ministry of Defense civilian analyst mentioned earlier, offered both a broad and narrow definition of information war, noting that:

*In the broad sense, information warfare is one of the varieties of the “Cold War”—countermeasures between two states implemented mainly in peacetime with respect not only and not so much to the armed forces as much as to the civilian population and the people’s public/social awareness, to state administrative systems, production control systems, scientific control,*

*cultural control, etc. It is namely in this sense that the information security of the individual, society, and state is usually understood.*

*In the narrow sense, information warfare is one of the varieties of military activity/operations/actions (or the immediate preparation for them) and has as its goal the achievement of overwhelming superiority over the enemy in the form of efficiency, completeness, and reliability of information upon its receipt, treatment, and use, and the working out of effective administrative decisions and their purposeful implementation so as to achieve combat superiority (victory) on the basis of this. The waging of information warfare in the narrow sense is the field of responsibility of mainly the ministers of defense of modern states.*

A final definition is offered by Colonel S. A. Komov, a Candidate of Technical Sciences and Professor. He defines information warfare within the confines of an article that looked only at its wartime use, defining it as:

*...a complex of information support, information counter-measures, and information defense measures, taken according to a single design and plan, and aimed at gaining and holding information superiority over an enemy while launching and conducting a military action/battle. Interconnections between information warfare and other types of operational/combat support and activities that make up its contents should be noted as well (intelligence, information gathering, communications, etc.).*

Komov believes four issues are at stake in his definition: first, identifying a set of measures to gain information on the opponent and on the condition of an engagement (electronic, weather, engineer, etc.), to gather information on friendly forces, and to process and exchange information between command and control echelons or sites; second, identifying measures to block the information gathering processes of others, and to feed deceptive information at all stages; third, identify friendly countermeasures; and finally, gain information superiority over the enemy.

Do these definitions compare favorably with the U.S. definition of information warfare? According to Department of Defense Directive S-3600.1, approved on 9 December 1996, IW is defined as “an information operation conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.” An information operation is defined as “actions taken to affect adversary information and information systems while defending one’s own information and information systems.”

Comparing the U.S. and Russian definitions, there are similarities and differences. One similarity is that both countries include the concept of defending one’s own information (in Pirumov’s definition, information resources) while affecting the information of an adversary. In addition to pure information, the U.S. definition includes information systems as items to be affected or defended. The Russian definitions are broader and encompass considerations of the information security of society in both peacetime and wartime, while the U.S. definition confines itself to time of crisis or conflict.

This short discourse demonstrates a concern as we talk about information operations: we are using two different languages and conceptual approaches in our attempts to define terms. The U.S., for example, does not define information resource or information advantage or a term used later, information potential. Russians, on the other hand, have trouble finding a precise Russian term for the concept of information warfare, using several names to describe it. These include information voyna (war), borba (struggle), and protivoborstvo (confrontation), with all taken to mean information warfare as well.

## **Ten Key Elements of the Russian Approach**

In the past, some of the key elements that defined Russia's approach to the study of military operations included officers' interpretations of the principles of war (Russia's 13 versus the U.S.'s 9); the nature of armed conflict; the coefficient of effectiveness of nuclear weapons; an evaluation of the military potential of a possible enemy; the correlation of forces of two opposing sides; and arms control concepts such as deterrence and parity, among other subjects.

The current study of military operations reflects many of these elements, but with an information operations twist. This was apparent in the concepts of information security and information warfare outlined above. While not direct parallels, one is able to discern that military thinking has adjusted and metamorphosed, resulting in terms such as "the development of information-psychological operations," the "study of the computer-operator interface, the "effect of information operations on arms control issues such as parity," the "scrutiny of the information

potential of a country,” the “effect of information operations on military art, especially the understanding of the initial period of war,” the “use of computer viruses as weapons,” the “development of neuron computers and the infosphere,” and the “ability to use space and information based assets to detect and kill an enemy force with speed, precision, and stealth.”

The first key element to the unique Russian approach to information warfare is what theorists refer to as “the natural laws and principles associated with information warfare.” Komov ascertains that the identification of the objective laws and principles of IW are urgent problems for the development of the scientific theory of IW. Pirumov states that he has already done this, and notes that the general, universal laws and principles of armed battle remain fair and useable in the information battle. However, the information battle also has its own specific inherent aspects as well. Pirumov lists the law-governed patterns (trends and predictive in a mathematical sense) of the information battle as follows:

1. The constantly growing role of information warfare in carrying out assigned missions in the combat operations of troops (forces). This is determined primarily by the increased informatization of the armed forces and, consequently, by the increased means and forces which are enlisted for this informatization. It should be noted that the advent of new means and methods of information warfare does not carry with it a rejection of the traditional means, methods, and forms of armed battle, but it does have an impact on the methods of resolving combat missions with the help of traditional

means, and it also changes the capabilities of traditional means and the effectiveness of the combat use of troops (forces).

2. Information warfare today is carried out both in war time and in peacetime. In the latter instance, the means of information warfare are employed in order to diminish the enemy's information resource prior to the commencement of combat actions. It should be noted that the conduct and consequences of information warfare are not always known to the side against whom it is being conducted.
3. The ever growing impact of informatization on all levels and spheres of governmental and military control systems provide some basis for identifying information warfare as an independent form of armed battle. The reason for this is that most developed nations today possess powerful information potential which under certain conditions can be concentrated and utilized to achieve their own political goals. Two factors lend added appeal to such an approach in resolving external political conflicts, i.e., the current trend of avoiding the use of armed force in international conflicts, and the lack of international legal norms which would regulate the methods of conducting information warfare.

The basic principles involved in organizing and conducting information warfare operations (combat actions) include, according to Pirumov:

1. subordinating the goals, missions and measures of information warfare to the missions of the troops in combat actions, as well as assuring that the information operations are so organized as to fit the plan and intent of the operation (combat actions);
2. preemptory resolution of the tasks of information warfare vis-à-vis the combat missions of the troops in combat actions;
3. a multi-purpose use of the forces and means of information warfare in the preparation and conduct of combat actions, as well as a rational combination of the measures of information warfare with the actions of troops to destroy the enemy;
4. the constant and covert conduct of information warfare throughout the entire operation (combat action); and
5. the principle of a counter system, according to which the forces and means enlisted for the conduct of information warfare must be unified into a functional system which is in no way inferior to the enemy's command and control systems.

Of course, the laws and principles examined here are not immutable. Rather, they are clarified as the content, forms and methods of conducting information warfare evolve or develop.

A second difference is the main objectives and methods of implementing information warfare

concepts. This is a major difference due to the differentiation in peacetime and wartime missions.

In peacetime, IW is conducted secretly through means of intelligence, politics, and psychological actions, according to Pirumov. Actions are conducted against armed forces, the civilian population, and the systems for administering production, research, and culture. Each side seeks to undermine the information security of the individual, society, and the state of the opposing side, while safeguarding one's own information security. The main role here is played by government propaganda institutions, foreign intelligence, and counterintelligence, as well as institutions protecting information. Most important is the fact that an ever increasing role is played by specially programmed hardware and software techniques against the information assets of the engineering systems of the enemy, that is, virus warfare.

In wartime, Pirumov says, IW operations are more overt. They act as a system supporting the traditional forms and methods of warfare. They also support information and intelligence activities, and the secrecy of primary activities of friendly troops in the preparation and conduct of operations. They assist with measures for obtaining surprise (especially in a period of threat such as the initial period of a war) and can drastically reduce the information assets of the forces and diminish their combat possibilities, while protecting one's own forces if jam-proof equipment can be developed. The primary way to do this is to disrupt enemy command and control systems and weapons, while protecting these systems on the Russian side.

The main methods or means by which one can engage military information systems, Pirumov continues are:

1. physical destruction or taking actions to prevent an operation, such as capture of operating personnel or other actions by assault groups or special detachments, fire strikes on the systems, actions of reconnaissance groups, or incapacitating the systems;
2. electronic countermeasures against designated command posts and electronic facilities;
3. the use of specially programmed hardware and software techniques against information assets of automated control systems, or for the surprise destruction or blockage of information assets of potentially dangerous states at the start of combat actions;
4. distortion of information used by the enemy to evaluate a developing operational-strategic situation or for decision-making (PSYOP or manipulation effect); and
5. psychological impact of IW operations on leaders and servicemen of the facilities of systems of command and control.

The main forms of IW and electronic warfare, IW's main component, Pirumov posits, are:

1. a special operation to disrupt enemy command and control;
2. EW attacks;

3. an information blockade (for example, through the use of an electronic blockade); and
4. the systematic actions of forces and assets utilized in IW functions.

There are three levels at which IW is conducted, according to Pirumov:

1. state;
2. scientific and technological; and
3. weapons systems and technology.

At the state level, the aim of IW is to lower the information potential of probable enemies while supporting the information security of the state. At the scientific and technological level, the aim is technological superiority to ensure parity or superiority in military power due to advanced information and technological assets. These assets must be able to withstand the electronic impact or counteractions of the enemy while protecting one's own assets. At the level of weapons systems and technology the goal is to conduct actions against sources of information threats to eliminate, suppress, or reduce their effectiveness. Measures must also be taken to protect ones own command and control elements.

A third and perhaps primary difference in the Russian and Western approach is the Russian focus on the impact of information on members of its society. This "information-psychological" aspect of information warfare is not as predominant in the U.S., where electronic warfare, defensive and offensive mechanisms, and digitalization of the force/information dominance are the centers of interest. American

society is relatively stable and, at least for the present, the impact of foreign influence on the U.S. mind and psyche is viewed as minimized. By contrast, the Russian emphasis is understandable since society lost its cementing mechanism, the ideology of communism, when the USSR disintegrated. Only control over the “information-psychological” aspect can produce the mental stability the country desperately needs to allow it to proceed with future reforms and to rebut rumors and disinformation, in the view of many sociologists and scientists.

Russian candidate for President and Communist Party Chief Gennadiy Zuganov, who believed he was a victim of an information-psychological strike by the Yeltsin campaign during the Presidential elections of June and July 1996, underscored the importance of information for Russian society in a recent interview:

*It is necessary to remove the quotation marks from the concept of “the fourth estate” and to legally recognize state electronic mass media as an autonomous—information—branch of power besides the legislative, executive, and judicial branches.*

Zuganov’s emphasis corresponds to the traditional importance placed on the moral-psychological factor by the Russian military, since the moral-psychological factor is regarded as one of the 13 principles of war.

Fourth, and closely associated to the information-psychological element, is a serious attempt by the Russians to harness the energy generated by human beings. The so-called “Computer Operator’s Security Problem” is a multi-disciplinary one, these scientists believe, connected to the integrative efforts of different

areas of knowledge—physics, biology, psychology, cybernetics, philosophy, and religion. From this perspective, if man is viewed as an open system capable of communicating with the environment using material, energy, and information flows, then it is possible to influence him by means of radiation (electromagnetic, acoustic, etc.) and to cause changes in the psycho-physiological condition of his organism. In addition to energy sources, information alone can also influence the vital processes of a person if it is properly packaged. This theory appears to have strong appeal for such Russian scientists as Victor Solntsev and Vladimir Pirumov, who often write on information operations.

Solntsev, for example, believes that to all people the world appears as diverse forms of information flows, which everyone processes differently. Certain forms of radiation-information fields, according to these scientists, can cause disease, disorder of the gums and systems of an organism, modification of behavior, suppression of thinking, manipulation of one's consciousness, and the destruction of one's personality, among other problems. Deaths have resulted in Russia from the computer-operator interface as well, they report:

*August 13, 1994. There was an accident in Voronezh City. One user of a personal computer lost consciousness in less than 20 minutes. His friend—a programmer—said that he had a strange feeling, as though... he had a headache and some noise in his ears. It was almost impossible to stop it, as though it was some type of hypnosis. Luckily he managed to shut off the computer. His friend was dead some time later,*

*never regaining consciousness. The diagnosis was bleeding inside the brain.*

*The cause of his death was a computer virus named "666." Experts determined that it produces on the computer monitor a so-called 25th frame with a special color combination, that can immerse the person in a sort of hypnotic trance. Each 25th frame the picture changes. And the subconscious perception of the new pattern results in arrhythmia of the heart. Blood pressure sharply increases, and then falls sharply. And blood-vessels of a brain cannot withstand these pulses. Later, nearly 50 similar cases of sudden death were registered.*

To date, the Russians have not talked openly about their use of computer-generated morphed images, but they have referred on more than one occasion to the U.S. use of holographs in the operations in Somalia and during Desert Storm. In addition, the priorities of the Committee on Science and Technology indicate that research is underway in this area. Most significant in the Committee's list was the reference to speech, text, and image recognition and synthesis systems under study, as well as artificial intelligence and virtual reality systems. Some Russian scientists believe that technical objects, the consciousness of a person, and the group consciousness of a community can be affected through the computer-operator interface. Others are studying the perception-machine operator interface.

Fifth, Russia views information operations developments as phenomena that have not only tactical and operational but geo-strategic significance. Superiority in information technologies, as an example,

could debilitate a nuclear coding or launch command procedure. This would make the more traditional “numbers and megatonage” norms of parity disappear as information technologies become capable of disabling these systems and causing them to be either unreliable or unusable. Information warfare systems (including intelligence and information collection) do this by upsetting existing nuclear and conventional norms of parity based primarily on numbers and quality, the Russians believe. Intelligence, command and control, early warning, communications, electronic warfare, “special software engineering effects,” and disinformation are issues that contribute to superiority on the battlefield in ways different than before and upset the traditional correlation of forces. They can also be used as a hidden form of military-political pressure. In this sense, Russia considers information operations to be a key geo-strategic element capable of upsetting the status quo. Information operations, for example, can bring catastrophic results in a number of areas—an information strike on a strategic command and control site can relinquish control over assets, an information strike at a national power grid can lead to a destruction of hardware, or an information strike at the control systems of a nuclear power plant can lead to a melt down. None are excluded from warfighting or even peace-time covert information strikes.

Sixth, Russia calculates the information potential of a country as a measure of that country’s military power that is information based. Components of information potential lie in essentially two areas. The first is information resources, defined by Pirumov as information which is gathered and stored during the development of science, practical human activity, and

the operation of special organizations or devices for the collection, processing, and presentation of information saved magnetically or in any other form which assures its delivery in time and space to its consumers in order to solve scientific, manufacturing, or management tasks. The second is information means, those assets that carry out tasks in the launching and conduct of an operation.

Another category is the information potential of a weapon, which is the degree to which a weapon is "informationalized," that is, the degree to which a weapon's internal components rely on information or computer functions to attain maximum effectiveness. There is an additional linkage between economic-societal potential and state and then military information potential.

Seventh, information operations greatly affect the study of military art, in the view of some Russian military specialists. They view these operations as a separate and self-sufficient type of conflict; as operations that make the initial period of war extremely uncertain (one doesn't know what preparations were or are being prepared by a potential opponent during peacetime to alter the effectiveness of weapons or the strategic perception of the situation at hand, implying that the initial period of war may already have started); and as operations that increase the tempo of battle, focusing on continuous attacks designed to blind an opponent by destroying his information operations capabilities and achieving information dominance.

If the form of warfare is changing under the influence of informatization or computerization, then there will be changes in military art as well. Pirumov, for one,

believes that there are three ways that military art is being effected. First, the rapid development of communications facilities along with the appearance of various automated control systems and increased numbers of combat assets now enable unity and coordination of combat actions on heterogeneous forces and their fire interaction without spatial concentration (allowing for new operational ideas such as the air-land nature of combat actions). Second, computerization allowed us to see deep through reconnaissance-in-depth equipment and facilities, increasing the accuracy of destroying enemy facilities. Thus, the concept "second-echelon combat" offers opportunities to deliver precision selective strikes against enemy reserves moving up, on his rear facilities, and so on. Finally, operations will no longer be conducted cyclically, with intensive operations followed by lulls. Rather they will be conducted continuously, making it important to kill an enemy immediately after he is detected. This means warfare will evolve to "detect-kill" and a "reconnaissance-strike-jam" concept will be inevitable. Decisive superiority will be gained by the side having command and control in real time, demanding a new level of computerization in the armed forces.<sup>25</sup> Winning the battle of the ether is winning the battle.

In Tsymbal's view, the conduct of IW is felt at all three levels of military art: strategic, operational, and tactical. He noted that in peacetime, the goal will be to accumulate information on an enemy while developing and testing one's own IW weapons. Immediately prior to military action and during military action, IW systems will work to destroy first of all command and control systems of the enemy and any other information

systems which receive, store, or process information of military significance. Or, an IW operation will be run independently prior to the onset of combat actions of the traditional type.<sup>26</sup>

Perhaps the most important targets identified through a study of military art are those battlefield systems that work in tandem to first uncover and then destroy an object, the reconnaissance-strike and reconnaissance-weapon complexes. There is a need to have real time and accurate battle-damage assessment for this to really work and counter any “maskirovka” or deception attempts. Asked to demonstrate the relation of processes that lead detection to kill mathematically, one Russian scientist offered the following:

*destruction capability equals exposure of an object (via satellite or reconnaissance asset) times asset's precision and speed of its components*

All of these assets (reconnaissance, acquisition, control, precision, etc.) are interconnected and controlled by the infosphere (see key element 10) if the latter is understood to be programs for processing, storing, and creating data. The satellite locates, the precision guided weapon uses data sent by the satellite, and the information component of the weapon determines Ks speed and accuracy.

Acquiring and fixing the force in a manner compatible with this line of reasoning is a priority and one of several areas of agreement between Russian and Western thinking. Even a cursory look at Russian military writings underscores the importance placed on the acquisition of the location of the enemy by a

military force, followed by fixing the enemy force through fire. As one analyst noted:

*The increase in fire capabilities of the troops, the appearance of high-precision weapons, and the development of various types of guided missiles are objectively increasing the role of reconnaissance and command and control systems. In conditions when the likelihood of hitting targets with the first shot or salvo is approaching 1, reaction speed is becoming a paramount factor. The main targets of battlefield reconnaissance are enemy artillery and armored equipment.<sup>27</sup>*

Target detection as a result is now of primary importance to the Russian military. The pages of the Russian military journal *Military Thought* carried a serious discussion of no fewer than seven articles from 1994 to 1996 that discussed effective target engagement (ETE), that is, how to acquire and destroy enemy targets. The discussion was thorough, covering such aspects as should ETE be zonal or target (area or point) oriented, how can it be integrated into combined arms criteria of successful combat action, and so on. One article noted that productive ETE “mainly depends on how quickly information flows from reconnaissance agencies are transformed into command and control impacts on ETE assets,” among other items. This is a random process, however, and only a certain degree of probability can be expected.<sup>28</sup> This emphasis on acquisition also coincides with changes predicted by Pirumov on changes in military art.

General Colonel N. M. Dimidyuk, Commander in Chief of the Missile Forces and Artillery of the Ground Forces,

concluded the ETE discussion in *Military Thought*. He called for closer integration of assets, noting that “under present conditions ETE cannot be separated from the EW [electronic warfare] suppression of enemy command and control, information, and reconnaissance systems and networks.<sup>29</sup> This led to the emergence of ETE as “one decisive factor determining the course and outcome of a combat operation and often times of a war as a whole...<sup>30</sup> and to the use of ETE assets to “disrupt enemy troops and weapon command and control systems at the very start of an operation, to inflict a decisive defeat on the main enemy forces and logistical installations, and to seize and maintain fire superiority”<sup>31</sup> through coordinated and massed use while attaining surprise. Such coordination will require that:

*the main task...is coordination of the ETE plan with the operation’s objective, concept, and design, which can be achieved only in the event that ETE planning is carried out by an operational (combined-arms) staff command and control agency: the ETE planning and coordination group (ETE PCG)...This will shift the center of gravity in ETE planning to the operational level...<sup>32</sup>*

Dimidyuk concluded by noting that:

*the results of the discussion show that in assessing ETE, it is appropriate to use a single indicator that has a graphic physical interpretation and is easily integrated into the operational criterion used in operation planning: the force incapacitation rate expectation. It should objectively reflect strike, reconnaissance, maneuvering, and other capabilities of the forces*

*in question that characterize their striking power in an offensive and their operational stability in defense. It needs to be finally recognized that not enough has been done yet in substantiating the requisite correlation of the sides' forces in operations of various types and scale, when the combat capabilities of the forces are expressed through their combat potentials.*

*...with respect to same-type (homogeneous) multiple targets, the ETE rate affecting the target's combat capability is defined by the number (proportion) of individual targets to be engaged, whereas with respect to different-type (heterogenous) targets, it is defined by their composition (combination). While there can be several such combinations, it is believed that if at least one target out of this combination is not effectively engaged, then it retains its combat capability and is therefore in a condition to perform its functions.<sup>33</sup>*

Eighth, the computer research and development process has produced some unexpected results unique to the Russian experience. One is the neuron computer, expected to replace the pentium chip for speed and effectiveness. Other areas identified and approved by the government's Science and Technology Committee as priority directions for federal-level technologies in information related fields included multiprocessor parallel-structure computers; computer systems based on neuronet computers, transputers, and optical computers; speech, text, and image recognition and synthesis systems; artificial intelligence and virtual reality systems; information and telecommunication

systems; mathematical modeling systems; microsystem technology and microsensors; superlarge integrated circuits and nanoelectronics; optical and acoustic electronics; cryoelectronics production technologies; laser technologies; precision and mechatronic technologies; robotic systems and micromachines; electronic-ion-plasma technologies; intellectual systems for automated design and control.<sup>34</sup>

Of particular interest in this list are the neurocomputers. According to one report, these computers are now being developed in Russia. They are reportedly 1,000 times faster than traditional computers, according to Yuriy Glybin, deputy head of the State Committee for Defense Industry. Military uses include the development of state-of-the-art high-precision weapons, military equipment, optic devices to detect missiles, as well as use in ABM programs and dual technologies. In financial markets, the computers are used to make highly accurate forecasts (supposed 90 percent accuracy) of currency and futures rates, stocks, and other securities.<sup>35</sup>

Ninth, Russian scientists, recognizing the increased importance of systems, have focused more attention on the interaction of combat systems instead of on simple force on force (the old correlation of forces) ratios. This approach differs from the U.S. systems approach by its dialectical nature, measuring combat systems against one another instead of in isolation. According to this logic, warfare is viewed as the interaction among the military systems of the sides in confrontation. This idea has extended to modeling at the General Staff Academy, where Red versus Blue force-on-force reportedly is no longer played as it once

was. Instead, high tech systems are modeled against other high tech systems.<sup>36</sup> Integrating these systems is also important, as other analysts have noted:

*...the reconnaissance-information-command and control component ensures system integrity. Therefore, as a rule it also acts as an object of information confrontation; its disorganization, neutralization, or destruction leads to the disruption of system integrity and to a loss of its potential capabilities.*<sup>37</sup>

Within the discipline of military systemology, information is viewed as the “nourishment” that gives life to all elements of the system from top to bottom, according to one expert. This applies in particular to reconnaissance, command and control, support, and strike systems. Information warfare as a system, according to this view, includes three components: information support of the functioning of one’s own combat systems; information counteraction against the functioning of the enemy’s combat systems; and information protection or defense of one’s own combat systems against the informational counteraction of a possible enemy.<sup>38</sup>

In short, the side that cannot conduct real-time fire control on an enemy force is doomed to defeat in large scale conflict, and in some conflicts of lesser intensity as well. Emphasis is on the ability to acquire and process information through systems utilizing space or the airways, and resulting in target acquisition:

*The number of information sources for tactical command and control systems is growing. Use of remotely piloted reconnaissance vehicles*

*[RPVs] is becoming more and more widespread. Radar detection and command and control aircraft...are being improved. All this leads to a growing interconnection and interdependence of air and ground weapons. The airways are becoming a distinctive "fourth dimension" of the space in which combat is waged. Fighting is also waged in them: radars and communications equipment are jammed, radiation sources are discovered and destroyed, and electro-optical surveillance systems are blinded.*<sup>39</sup>

Finally, one of the most important factors considered from a technical standpoint is that "the infosphere, understood as a body of general and specialized programs for creating, processing, and storing computerized data, is bound to become one of the most likely objects of military confrontation."<sup>40</sup> Specifically, Russian scientists are worried about the impact of hostile actions to influence the infosphere through such items as "algorithm bombs" capable of distorting a section of an algorithm that limits the ability of software to function as required and "software bombs," those bombs that insert an uncalled for algorithm that limits the execution of software functions or that steers it to commit computations unauthorized by the software program as originally intended. This final key factor is also a major element of the U.S. approach to IW.

This idea first was described in an article from 1991 by Russian Captain Vladimirov, who noted that:

*In the French air defense systems sold to Iraq, so-called "logic bombs" were installed, which*

*made it impossible to use these systems against the multinational force during combat operations in the Persian Gulf. An American missile went off course and was blown up on command from the ground, because a "1" instead of a "7" was indicated in its computer program...[Thus] the effectiveness of electronic computers depends upon the quality of the software. Defects in the form of incorrectly written sections of programs frequently result in a complete breakdown of the systems...Sabotage bugs substantially exacerbate the problem of quality and reliability of software.<sup>42</sup>*

Since software programs run many systems, it is no surprise that Russia has developed viruses to affect these systems. Four types of computer viruses were listed by one Russian analyst, although it was unclear if he was referring to Russian or U.S. variants of these viruses.<sup>43</sup> The Russians also claim to have developed a "stealth virus."<sup>44</sup> This virus does not allow for its detection by the usual method, comparing file space with total free space, and so is termed stealth. By the year 2000, Russian scientists also expect to confront "distance virus weapons," computer viruses introduced through radio channels or laser lines of communications directly into computers that pose an instant threat to command and control means of units such as the strategic missile force.<sup>45</sup> A final threat is the use of "microwave weapons," electromagnetic impulses designed for use against the electrical components of Russia's space, aviation, ground, and sea-based means of combating information warfare.<sup>46</sup> Russia is also studying how to develop and implement these means, according to some sources.

The infosphere can become a target of hostile intentions in peacetime or wartime, according to Russian analysts. Attacks are most dangerous if aimed against the target acquisition systems and command and control setups of a nation.

## **Conclusions**

The 10 elements outlined above highlight some of the terminology and conceptual landmarks that outline Russian thinking on the problem. Are these elements really different from the Western approach?

Clearly, identifying the targets of information operations for any country is easy: EW systems, command and control nodes, satellites, and AWAC planes stand out as clearly today as targets as did massive armored formations 50 years ago. What is really different is the conceptual understanding of an information operation from a cultural, ideological, historical, scientific, and philosophical viewpoint. Different prisms of logic may offer totally different conclusions about an information operation's intent, purpose, lethality, or encroachment on sovereignty; and this logic may result in new methods to attack targets in entirely non-traditional and creative ways.

Russia's approach is a reflection of its dialectical logic, the historical processes that have shaped it, and its efforts to adjust to a new environment. In the past, control over information was dominant. Even Xerox machines were off limits to many people. Today, Russia is battling a creeping "information anarchy" that, in the opinion of its citizens, is saturating society. Citizens are confused over just what to believe when

they are reading the papers or watching television. The problem is just as difficult for the military. Threat perceptions were developed over the course of many years. While there is a reason and cause for cooperation with the West, the military must engage in these discussions with a wary eye. They still tend to blame the end of the Cold War on a successful information operation run by the West that destroyed not only the Soviet Union but communism, the country's unifying ideology. Why would the West not engage in another ambitious undertaking to further its control over Russia, the military asks.

The primary concern is that in its attempt to catch up with the West in information operations, Russia does not appear to have a clear idea where it will end up when the process is finished. This is reflected in the military definition of terms such as information warfare which are much more vague, open to interpretation, and a cause for misunderstanding than in the past. What do Russians mean when they refer to an action as an "information-psychological" strike? What are the ramifications of such an action? Will it be an accusation of a violation of international law or will it result in a nuclear exchange? Where are the areas of misunderstanding on the U.S. side that can cause a similar response?

Much remains to be done to overcome the terminological and conceptual problems associated with unique parochial views of information operations if we are to avoid information confrontation or warfare in the future. The 10 elements listed in this paper are important considerations that, in a general fashion, represent a unique and different way of looking at the problem. As the U.S. and other nations continue to cooperate with

Russia, everyone should pay close attention to one another's thinking in this sensitive area. Conflict prevention or crisis management techniques are needed here every bit as much as they were over nuclear weapon concerns in the past. Further, a comparative analysis of Chinese, U.S., Russian, Canadian, German, and British views, among others, is required to understand the extent of this problem, not to mention to help avoid both current and future problems in the area of information operations.

---

<sup>1</sup>For example, Russian specialists put a physiological-psychological spin on Pavlov's reflexive control, while Westerners saw it as a biological process.

<sup>2</sup>Alexander Yegorov (interview with Victor Bazhenov), "Kaz izmenit' 'voyennyi intellekt'" ("How to change the 'Military Intellect'"), *Krasnaya zvezda*, August 3, 1996, p. 5.

<sup>3</sup>Dmitriy Semenovich Chereshkin and V.A. Virkovskiy, "Kontseptsiya informatsionnoye bezopasnosti Rossiyskoye Federatsii" (proekt) ("The Concept of Information Security of the Russian Federation") (draft), Moscow, 1994.

<sup>4</sup>*Ibid.*, p. 19, 20.

<sup>5</sup>*Ibid.*, p. 20.

<sup>6</sup>*Ibid.*, pp. 20-21.

<sup>7</sup>*Ibid.*, p. 21.

<sup>8</sup>*Ibid.*, p. 21.

<sup>9</sup>These Laws, edicts and statutes include the following: Draft: "Concept of information Security of the Russian Federation," 1994; Law: "Federal Law on Communications," passed by the State Duma on January 20, 1995; Edict No. 65: "On the Ratification of the Statute on the Russian Federation Presidential Staff's Information Administration," Law: "Russian Federation 'Federal Law on Information, Informatization, and the Protection of Information,'" enacted by the State Duma on January 25, 1995; Directive: "On the Confirmation of Lists of Informations, Relation to State Security," November 30, 1995; Edict: "Edict of the President of the Russian Federation, 'Measures to Regulate the Development, Production, Sale and Purchase for Purposes of Selling, Importing into, or Exporting out of the Russian Federation, as well as the use of Special Technical Equipment Intended for Secretly Obtaining Information,'" January 1996; Statute: "Statute

on the Council of Heads of State Information Agencies of the Commonwealth of Independent States," February 1996; Directive: "On the Development of a Situation Centre within the Federal Government Communications and Information Agency (FAPSI)," April 1996; Decree: "On a Special Comprehensive Program for Creating Communications, Television, and Radio Broadcasting Technologies," May 1996; Law: "On Participation in International Information Exchanges," July 1996.

<sup>10</sup>Professor V.I. Tsymbal, "Kontseptsiya 'informatsionnoy voyny' ("Concept of Information War"), paper received at conference with the Russian Academy of Civil Service in Moscow, September 14, 1995, p. 2.

<sup>11</sup>Russia Reform Monitor, No. 215, January 10, 1997, American Foreign Policy Council, "Former KGB Reportedly Tries to Control Internet in Russia."

<sup>12</sup>From a speech delivered in Brussels in May 1996 by Admiral Pirumov, "Certain Aspects of Information Warfare," p. 2.

<sup>13</sup>*Ibid.*

<sup>14</sup>Tsymbal, pp. 3-6.

<sup>15</sup>S.A. Komov, "Information Warfare in Modern War: Theoretical Problems," *Military Thought*, May-June 1996, pp. 76-70.

<sup>16</sup>Pirumov, pp. 3, 4. The laws and principles in the text are taken from these pages of Pirumov's report.

<sup>17</sup>*Ibid.*, p.9.

<sup>18</sup>*Ibid.*, pp. 9, 12, 13. The writeup on the wartime use of IW as well as the methods and forms of IW is a summary of the main points of these three pages of Pirumov's text.

<sup>19</sup>Pirumov, p. 5.

<sup>20</sup>Gennadiy Zyuganov, "On the Threshold of a 'Government of Seven Boyars'," *Sovetskaya Rossiya*, October 26, 1996, pp. 1, 2.

<sup>21</sup>Victor I. Solntsev, "Information War and Some Aspects of Computer Operator's Defense," paper presented at the InfoWarCon 5, Washington D.C., September 4-6, 1996, pp. 2-7.

<sup>22</sup>*Ibid.*, p. 7.

<sup>23</sup>"New Trends in Power Deterrence," *Armeyski Sbornik*, No. 9 (September 1995), pp 12-19, as reported in FBIS-UMA-96-011-S, January 17, 1996, p. 12.

<sup>24</sup>I. Panarin, Georgi Smolyan, Vitaly Tsgichko, and Dmitriy Chreshkin, "A Weapon that may be more Dangerous than a Nuclear Weapon: The Realities of Information Warfare," *Nezavisimoye Voyennoye Obozreniye* (supplement to *Nezavisimaya Gazeta*), November 17, 1995, No. 3, pp. 1-2, as reported in FBIS-UMA-95-234-s, December 6, 1995.

<sup>25</sup>Pirumov, pp. 14, 15.

<sup>26</sup>Tsymbal, p. 11, 12.

<sup>27</sup>Sergey Grigoryev, "Who Will Fire First? The Eyes, Ears, and Nervous System of the Ground Troops," *Nezavisimiya Gazeta*, August 22, 1996, No. 16 (20), p. 6.

<sup>28</sup>V. Ye. Shulgin and Yu. N. Fesenko, "Effective Target Engagement Planning in Combined-Arms Operations," *Military Thought*, (January-February 1996), pp. 33, 34.

<sup>29</sup>N. M. Dimidyuk, "Principles of Effective Target Engagement: Summing Up the Discussion," *Military Thought*, (May-June 1996), p. 16.

<sup>30</sup>*Ibid.*, p. 15.

<sup>31</sup>*Ibid.*

<sup>32</sup>*Ibid.*, p. 16. Dimidyuk added three pages later that "the importance of the group's coordinating role grows especially in implementing the zonal-target principle of ETE planning. It is called upon to ensure, above all, an efficient coordination of fire delivery with ETE assets under the control of the superior commander in the area of responsibility of subordinate levels: and coordination of actions by ETE and EW assets of the air force, missile forces, artillery, air defense forces, and special troops, and in maritime sectors those of battle front forces, in delivering massed and concentrated strikes. The need for coordinating the ETE plan with the operation's overall objective and concept highlights the necessity to relate the indicators characterizing the expected ETE results with the results of the operation as a whole. Furthermore, it is key to provide for the possibility of ensuring the integration of the ETE indicator (measure) into the operational criterion used in elaborating the concept and objectives of an operation, and in decision-making. Considering that this indicator is the correlation of the sides' forces, calculated through the combat capabilities of their contingents, one indicator of the effectiveness of the engagement of enemy forces, as a number of authors pointed out during the discussion, can be the extent to which their (the forces') combat potentials are reduced—a measure that in the present situation is assumed as their combat incapacitation rate expectation."

<sup>33</sup>*Ibid.*, pp. 20, 21.

<sup>34</sup>Andrey Fonotov, "Science and Technology Policy," *Rossiyskaya Gazeta*, August 8, 1996, p. 6, from FBIS-UST-96-037, August 8, 1996.

<sup>35</sup>INTERFAX, February 14, 1996. as reported in FBIS-UMA-96-040-S, February 27, 1996, p. 64.

<sup>36</sup>Based on a discussion with modelers at the General Staff Academy in December 1991, during a visit by a Fort Leavenworth Command and General Staff delegation.

<sup>37</sup>Nikolay Turko, Sergy Modestov, and Nikolay Shvets, "...And Data Confrontation," *Armeyskiy Sbornik*, October 1996, No. 10, pp. 92, 93.

<sup>38</sup>Author's discussion with General-Major (retired) V. D. Riabchuk, Fort Leavenworth, September 1996.

<sup>39</sup>Grigoryev.

<sup>40</sup>A.N. Kukashkin and A.I. Yefimov, "The Security of the Infosphere of Strategic Defense Systems," *Military Thought*, No. 5, 1995, pp. 45-48.

<sup>41</sup>*Ibid.*, p. 46.

<sup>42</sup>A. Vladimirov, "Informatsionnoe Oruzhie: Mif ili Rea'lnost'?" ("Information Weapons: Myth or Reality?"), *Krasnaya Zvezda*, October 5, 1991, p. 3.

<sup>43</sup>Aleksandr Pozdnyakov, "Informatsionnaya Bezopasnost'" ("Information Security"), *Granitsa Rossii* (September 1995), No. 33, pp. 6-7; as reported in FBIS-UMA-95-239-S, December 13, 1995, pp. 41-44. These viruses are: 1) trojan horse virus, which is introduced into the victim system, remains idle for a certain period of time, and then causes catastrophic destruction of the system; 2) forced quarantine virus, which is introduced into a network and knocks out the program of the unit into which it was planted. If components are not separated, then the entire system network is destroyed; 3) overload virus, which quickly spreads throughout the entire system and gradually slows its operation; and 4) sensor virus, which penetrates a preplanned sector of a computer's data storage area and, at a critical moment, destroys the data bank and its information.

<sup>44</sup>Pal'chun, B.P., and R.M. Yusupov, "Obespecheniye Bezopasnosti Komp'yuternoy Infosfery" ("Providing Security in the Computer Infosphere"), *Vooruzheniye, Politika, Konversiya*, No. 3, 1993, p. 23.

<sup>45</sup>M. Boytsov, "Informatsionnaya Voyna" ("Information Warfare"), *Morskoy Sbornik*, No. 10, 1995, pp. 69-73.

<sup>46</sup>*Ibid.*