Military Thought

http://www.eastviewpress.com/Journals/MilitaryThought.aspx

Cyberspace in Military Operations Today

Lt. Gen. V.I. KUZNETSOV (Ret.),
Doctor of Technical Sciences
Col. Yu.Ye. DONSKOV (Ret.),
Doctor of Military Sciences
Lt. Col. O.G. NIKITIN,
Candidate of Technical Sciences

Victor I. KUZNETSOV was born in Krasnodar Territory on November 23, 1920. A World War II veteran, he completed a postgraduate course at the Marshal A.A. Govorov Air Defense Radio Engineering Academy (1951).

In 1963, he was appointed chief of the U.S.S.R. Defense Ministry's 21st Scientific Research and Testing Institute (the Defense Ministry's 5th Central Scientific Research and Testing Institute).

Since his retirement from the Armed Forces, he has been employed at the Sozvezdiye [Constellation] Concern, OJSC. A professor, he is a Merited Worker in Science and Engineering, winner of the U.S.S.R. State Prize, an honorary citizen of Voronezh, and author of over 300 academic papers.

Yuri Ye. DONSKOV was born in Shelukhovo village, Shilovo district, Ryazan Region, on August 7, 1949. He graduated from the Polytechnical Institute in Volgograd (1971) and the M.V. Frunze Military Academy (1982), and completed a retraining course at the Military Academy of the Russian Armed Forces' General Staff (1994).

He served in the North Caucasian Military District as tank platoon leader (1971 to 1975), and as reconnaissance company commander of a reconnaissance battalion of a division, and reconnaissance chief of a tank regiment with the Group of Soviet Forces in Germany (1975 to 1979). Between 1982 and 2000, he served with the Russian Defense Ministry's 21st Scientific Research and Testing Center (reformed into the Defense Ministry's 5th Central Scientific Research and Testing Institute in 1989) in successive positions from junior research associate to department chief. Upon retirement to the reserve, he was a leading research associate at the Defense Ministry's 5th

Central Scientific Research and Testing Institute (reformed to the Federal State EW and EREA Scientific Research and Testing Center in 2005).

Today, he is a leading research associate at the EW Scientific Research and Testing Center, Air Force Military Education and Research Center, N.Ye. Zhukovsky and Yu.A. Gagarin Air Force Academy. Yuri Donskov is a professor and author and coauthor of over 150 academic publications.

Oleg G. NIKITIN was born in Omsk, Siberia, on October 5, 1971. He graduated from the Higher Artillery Engineering School in Tula (1993). Assigned to the Russian Defense Ministry's 5th Central Scientific Research and Testing Institute, he rose from junior research associate to section chief. In 1996, he completed an academic retraining course for a group of EW officers at the M.V. Frunze Combined Arms Military Academy. In 2005, he finished a postgraduate course at the Defense Ministry's 5th Central Scientific Research and Testing Institute.

Today, he is section chief at the EW Scientific Research Center, Air Force Military Education and Research Center, N.Ye. Zhukovsky and Yu.A. Gagarin Air Force Academy. Oleg Nikitin is an associate professor and author of over 30 academic publications.

Abstract. The authors examine the relationship between battlespace, cyberspace, and information environment from the perspective of combat actions conducted by tactical military formations in our day.

Keywords: battlespace, cyberspace, information environment, information, action, forms, methods, decision.

Foreign and Russian academics have persisted in recent years in their efforts to develop a concept, theory, and techniques to plan and conduct ***operations in cyberspace***, an entirely new type of warfare. A great many strange-sounding terms – cyber-warfare, cyber-security, cyber-engagement, cyber-action, cyber-vulnerability, cyber-attack,[1] and lots more – have cropped up to describe, in foreign theorists' thinking, the new type of warfare that can increase the probability of occurrence of more traditional armed clashes in which explosives, firearms, and missiles are used .[2] Not infrequently, "cyber-warfare" and "information warfare," and "cyberspace" and "information environment" are used interchangeably. The polemics over which term is right which is wrong under the circumstances aside, it is far more important, in our view, to bring out the relationship between the information environment, cyberspace, and battlespace and find out where each stands in modern-day military operations.

In the narrow sense, battlespace is the traditional tangible space described by the three-dimensional Euclidean continuum defined by three mutually orthogo-

nal axes of coordinates where combat actions are conducted within a certain time frame. To give an example, the battlespace (area of responsibility) of a motorized infantry (armor) company fighting a defensive action against a motorized infantry battalion is within the field of vision on an area of up to 6 sq. km. This area can accommodate up to 30 major enemy targets.

Today and in the future, the boundaries of the traditional battlespace for military formations will be moving apart as new realms of warfare develop and, in their turn, create an entirely new combat pattern for the length and capacity of the area of responsibility, or a **battlespace in its broadest sense**. Now, *cyberspace* is its specific and most prioritized element (*see*:*Fig*,).

Many experts in this field interpret ***cyberspace*** as a combination of information and information infrastructure designed and used on the battlefield to shape, generate, transform, transmit, use, and store the information in computers and computer networks.[3]

This interpretation of "cyberspace" is accepted in our day as a consequence of the global spread of information in management practices that has become, in practical terms, an essential for effective operation of any modern control system, including the command and control system of a tactical military formation. A good example to illustrate this statement is the 1st brigade of the 4th U.S. motorized infantry division that has personal computers at almost 2,500 workstations set up in nearly 900 of its fighting vehicles to form a shared network.

Following a series of successful trial exercises, a first computerized two-brigade division (4th CMD) has been activated in the U.S. Army. Unlike all regular formations of its type, the new division was equipped with advanced electronic and computer capabilities turning it into a ***tactical high-precision weapon*** fighting system that collects information about the dispositions and actions of friendly forces, their neighbors, and the enemy and displays it on computer screens, and then uses it in real time to hit selected targets with strikes. Similar measures are also underway in the Russian Armed Forces to equip all tactical formations with computer capabilities.

We have tried to argue above that **cyberspace is a component and tangible framework of another, and more extensive, space commonly known as information environment**. Each of these components of battlespace (in its broadest sense) is unique in its own way. In particular, hardware and software capabilities of the information infrastructure on both the adversary and friendly sides are the principal targets exposed to attacks in cyberspace. More specifically, these are electronic, computer, automated electronic, and electrical engineering capabilities.[4] By extension, information in data storage, in distributed databases, and in communication and data transmission channels must also be listed among these capabilities. The "cyber-engagement," "cyber-action," "cyber-attack," "action (destruction) by specialized software," "protection against unauthorized access," and "access control" are also concepts directly applicable to these information infrastructure capabilities.

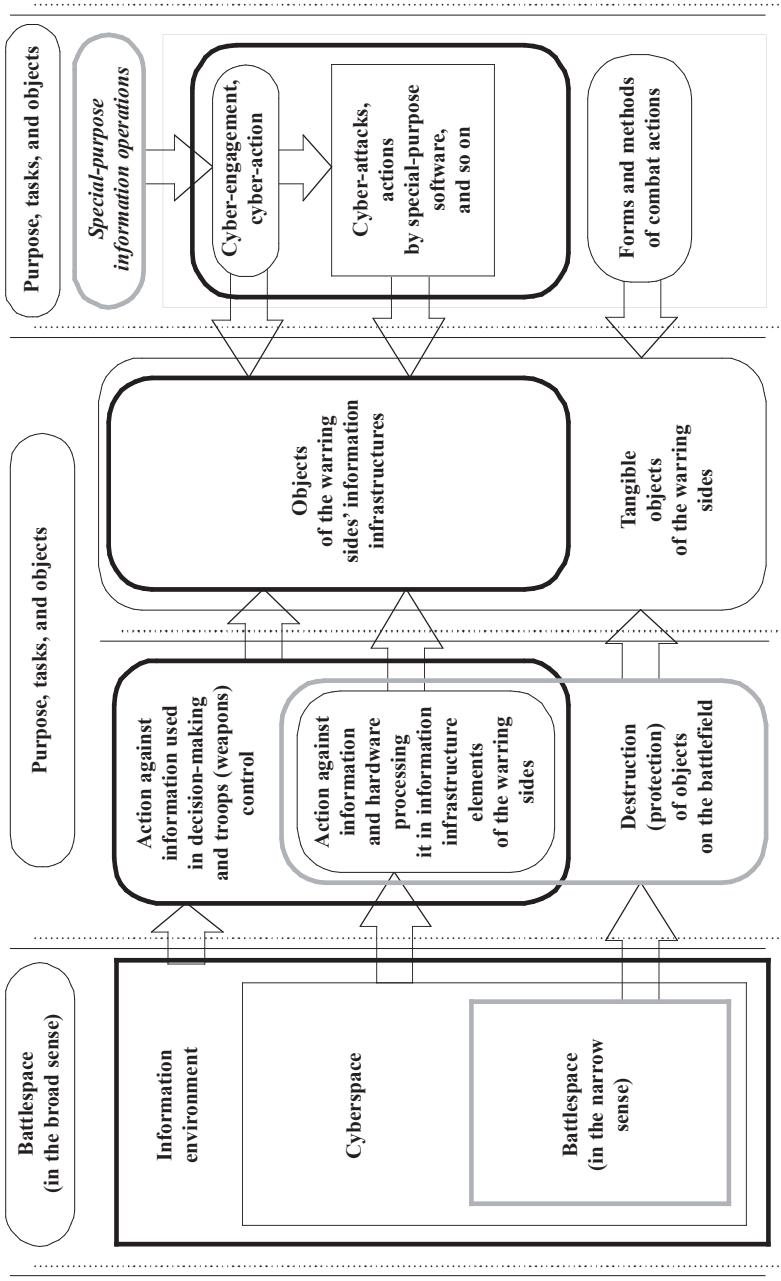

Fig. **Cyberspace and information environment in a modern-day combat situation.**

Action against information hardware and information they contain is just one of the measures decision-makers take. All-inclusive action can be taken against information of this kind in a rational combination of specialized software, functional disablement of targets, and tactical (operational) masking measures as part of a special-purpose information operation.[5]

An important point to make, **formation of cyberspace as a new realm of combat operations called for a revision of ideas held about the forms and methods of combat actions and the content of command and control over tactical military formations**. Even though the "cyber-warfare," "cyber-operation," and "cyber-engagement" categories are yet to be given an unambiguous definition to everybody's satisfaction and the groundwork is only being laid for the theory and techniques of their employment, a new type of specialized formations, ***cyber-forces***, are already being raised in the armies of several countries. Preparations are underway in the Russian Federation as well to set up similar formations. Proliferating hacker attacks against major servers and specialized computer systems are early signs of cyber-engagements and cyber-wars coming into their own.

The downside of these developments is that tactical military formations are getting much harder to command and control. The tactical C2, for example, comprises *six hierarchic tiers* – commanders and staffs of brigades and battalions, company commanders and their deputies, platoon and section (crew) leaders, and individual soldiers. Each tier will obviously require its proportional part of cyberspace of appropriate size, structure, and content to operate in. Given a time frame and staying within limitations, each hierarchic tier generates decisions to update the combat tasks assigned to its subordinate forces while combat actions are underway.

It is common knowledge derived from combat experience that every private or noncommissioned officer makes a new decision within minutes of the previous one, and acts on it alone or with several of his companions almost immediately within the field of vision. They will be acting within a very limited cyberspace, and they will require a limited number of computers and channels to access them. These limitations put restraints on selective (point) cyber-attacks, not to say massive offensive action.

For a brigade commander's C2 time frame averaging 30 to 40 minutes, his battlespace (area of his responsibility) works out, at current standards, at several hundred square kilometers. He makes his decision with support from many people who carry it out through a large number of servers, computers, and computer networks spread over an area much larger than the traditional battlespace. The content and three-dimensional scale of cyberspace at the brigade commander's tier enable the brigade to fight cyber-engagements and launch selective point cyber-attacks that will disrupt fulfillment of combat assignments (decision-making) depending fully on information traffic.

It is natural that all the six hierarchic tiers must be coordinated and mutually supportive for the brigade to achieve success in an engagement with the adver-

sary. Previously, coordination was provided by the commander's experience and skill, while with cyberspace now a reality he has to rely on systems that collect and deliver packaged information and help the commander to make decisions adequate to the evolving situation. ***Decision-making support systems*** fit into this category. They are expected to offer three or four options, for example, a rational, satisfactory, and tolerable options, and the decision-maker has to choose one and modify it, if need be, relying on his intuition or reasoning.

Battlespace, cyberspace, and information environment are each a part of the whole and each unlike any other. **Cyberspace**, for one, is a combination of information and information infrastructure that, first, gives substance to new forms and methods of combat actions (cyber-warfare, cyber-engagement, cyber-action, and cyber-attack), and second, it places more stringent requirements on command and control over subordinate forces and capabilities that can only be met by falling back on modern information technologies.

NOTES:

1. P.A. Antonovich, "Cyber-warfare: Nature and Content," *Military Thought*, # 3, 2011, pp. 35-43.
2. Richard A. Clarke, Robert K. Knake, *Tret'ya mirovaya voyna: kakaya ona budet?* [World War III: What Will It Be?], Piter, St. Petersburg, 2011 [*original title: "Cyber War: The Next Threat to National Security and What to Do About It" – Ed.*].
3. V.A. Balybin, Yu.Ye. Donskov, A.A. Boyko, "Electronic Warfare Terminology in the Context of Information Operations," *Military Thought*, # 3, 2013, pp. 108-113; P.A. Antonovich, "Cyber-warfare: Nature and Content," *Military Thought*, # 3, 2011, pp. 35-43.
4. V.A. Balybin, Yu.Ye. Donskov, A.A. Boyko, "Electronic Warfare Terminology in the Context of Information Operations," *Military Thought*, # 3, 2013, pp. 108-113.
5. Yu.Ye. Donskov, O.G. Nikitin, *Mesto i rol' spetsial'nykh informatsionnykh operatsiy pri razresheniyi vooruzhonnykh konfliktov v ugrozhayemiy period* [Place and Role of Special-Purpose Information Operations in a Period of Threat], *Voyennaya Mysl'*, # 6, 2006, pp. 30-34.