Russian Perspective on Network-Centric Warfare:

The Key Aim of Serdyukov's Reform

BY ROGER N. MCDERMOTT
Senior International Fellow,
Foreign Military Studies Office

Open Source, Foreign Perspective, Underconsidered/Understudied Topics

The Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas is an open source research organization of the U.S. Army. FMSO conducts unclassified research on foreign perspectives of defense and security issues that are understudied or unconsidered.

Roger N. McDermott is a graduate of the University of Oxford specializing in defense and security issues in the Commonwealth of Independent States (CIS). He is an Honorary Senior Research Fellow, Department of Politics and International Relations, University of Kent at Canterbury (UK) and Senior Fellow in Eurasian Military Studies, Jamestown Foundation, Washington DC. McDermott is on the editorial board of Central Asia and the Caucasus and the scientific board of the Journal of Power Institutions in Post-Soviet Societies. His articles appear in scholarly journals including the Journal of Slavic Military Studies, and his weekly assessments of security developments in Central Asia, Eurasia Daily Monitor (Jamestown Foundation), are read by policy planners. He is also the co-editor of the book, Russian Military Reform 1992-2002 (Frank Cass: London/Portland, 2003). McDermott is also conducting extensive policy oriented research into Russian defense reform, and will publish a book on the 'new look' Russian armed forces, as well as a chapter in a forthcoming Routledge book based on an FOI conference in Sweden on Russian military development (October 4-5, 2010), in which he examines Russian perspectives on network-centric warfare

---

FMSO has provided some editing, format, and graphics to this paper to conform to organizational standards. Academic conventions, source referencing, and citation style are those of the author.

The views expressed are those of the author and do not represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. government.

Russian Perspectives on Network-Centric Warfare:

the Key Aim of Serdyukov's Reform

By *Roger N. McDermott*

PHOTO: Anatoliy Serdyukov. By *Cherie A. Thurlby* (defenseimagery.mil) [Public domain], http://commons.wikimedia.org/wiki/File:Anatoliy_Serdyukov.jpg via Wikimedia Commons

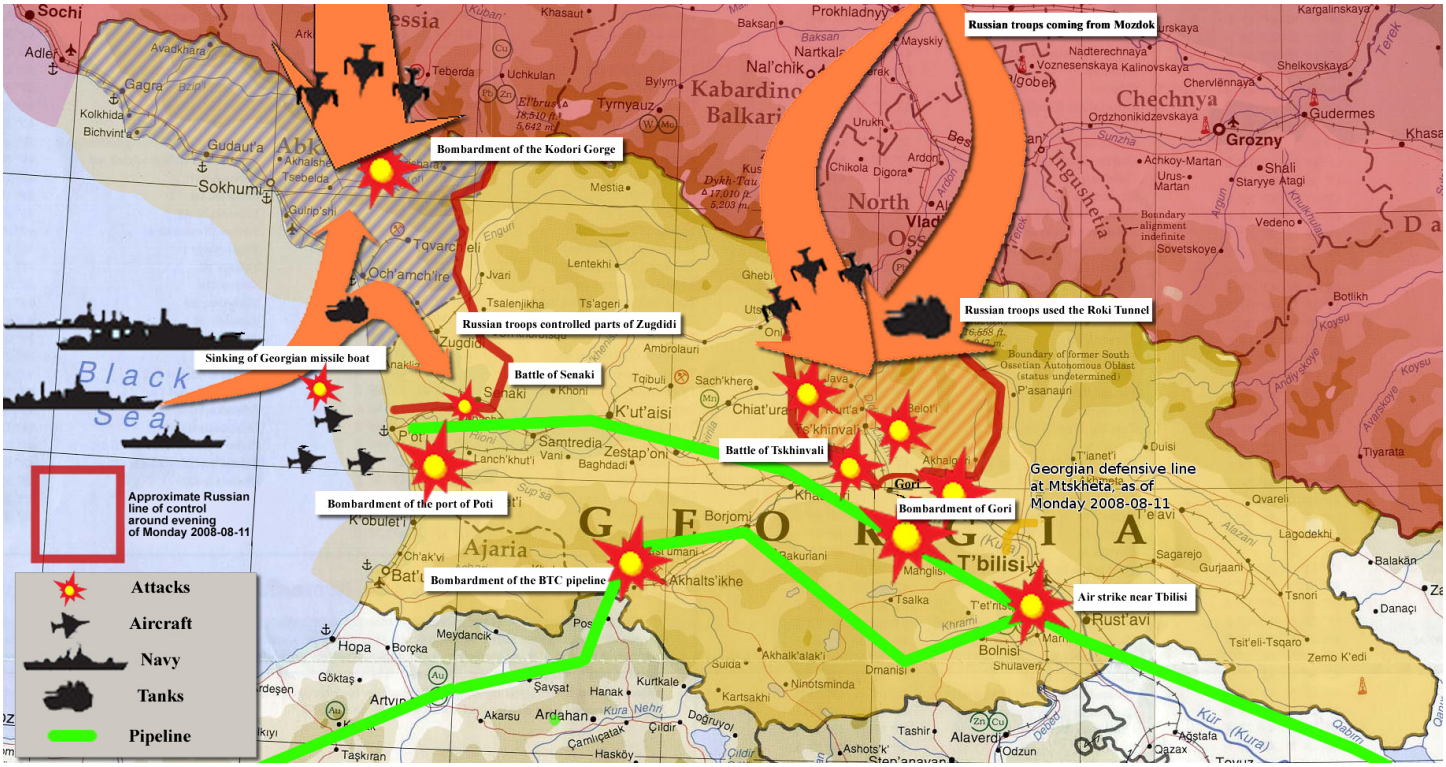
The reform of the Russian conventional armed forces, announced in the aftermath of the Russia-Georgia War in August 2008, as part of an agenda that became known as the "new look" cannot be understood, or properly assessed, unless its fundamental drivers are defined. Overall, following Defense Minister, Anatoliy Serdyukov, declaring the key features of the reform on October 14, 2008 on the day he briefed a closed session of the defense ministry collegium, the reform agenda appeared guided by an effort to enhance the combat capabilities and combat readiness of their conventional armed forces, loosely centered on the paradigm of forming mobile, smaller and modernized forces. It seemed to make sense given the operational failings of the Russian armed forces during the Five-Day War, and marked a consistent and determined campaign to drag the military out of its twentieth-century table of organization and equipment (TOE) to re-equip, restructure and train for the conflicts of the twenty-first century.[1]

In the following analysis, which draws upon Russian perspectives on foreign experience of network-centric approaches to warfare, an important caveat must first be stated. Linking the "new look" with its main driving force in this way, almost risks talking up the reform, which undoubtedly faces numerous obstacles. This chapter explores what the Russians mean when they use the term network-centric warfare (*setetsentricheskaia voina*), and examines the writings of its leading proponents and assesses the level of sophistication and understanding of such concepts among Russian military theorists and senior defense officials, arguing that the timescale involved in completing this revolutionary transition will range between ten to twenty years.

Nevertheless, Serdyukov's reform was driven by the adoption of network-centric warfare capabilities,[2] though this was not part of the declared agenda. In this chapter it is argued that the adoption of network-centric warfare capabilities is the main driving force underlying the "new look" and without first recognizing this, it is simply impossible to follow or appreciate the evolving and fluid contours of the military reform. It explains most, if not all, of the reform aims, *inter alia* abandoning cadre units, forming permanent readiness brigades, enhancing command control and communications (C^3I), reducing the number of tiers in command and control (*komandovaniye i upravleniye*), downsizing the officer corps, optimizing the military education system, developing professional non-commissioned officers (NCO's), raising officer standards, adjusting the procurement program and aiming at achieving a target (even if unrealistic) of 70 percent new weapons and equipment by 2020. Moreover, it also contextualizes how the conceptual plan-

ning of the reform, which predated the Russia-Georgia war by at least two years, was subject to adjustment during the first two years of its implementation and will continue to experience further fluctuation as Russian defense planners struggle with working out more fully the impact of adopting network-centric capabilities and its complex influence on future force structure, training and procurement. This chapter argues that the advanced development of network-centric capabilities in the US armed forces, among other NATO members, and the intensification of China pursuing asymmetric network-centric capabilities vis-à-vis the US are geostrategic factors influencing Russian defense policy, as the state seeks to harness modern approaches towards military conflict in response to its perceived lag compared with two key actors in Eurasian security. This is entirely consistent with Russian thinking on the nature of future war, encapsulated in President Dmitry Medvedev's warning that wars will erupt unexpectedly and rapidly, and represented within the 2010 military doctrine: "Military actions will be typified by the increasing significance of precision, electromagnetic, laser, and infrasound weaponry, computer-controlled systems, drones and autonomous maritime craft, and guided robotized models of arms and military equipment [Section II; 15]." Future wars may be categorized into conventional and unconventional, with the latter witnessing no physical force (which represents a current Russian understanding of future war), and by type as armed conflicts, local and regional wars, increasingly involving high-technology and seeking to establish information dominance.[3]

While Jacob W. Kipp, adjunct professor in the University of Kansas, stood out among a tiny minority of western analysts that rightly identified the link between the "new look" and the transition to network-centric capabilities, a larger group of Russia-based military analysts noted the confluence between the reform aims and developing the capability to conduct non-contact warfare.[4] Among these, Lieutenant-Colonel Aleksandr Kondratyev (candidates degree in military sciences) made an outstanding contribution, realizing at an early stage that it was no coincidence that the reform abandoned the division-based structure, and formed a new brigade-based system: since the brigade is the critical structural component in the network-centric concept.[5] Therefore, Kondratyev's recent writings will be examined closely, though the



2008 Russia-Georgia War Map By DivineDanteRay (Own work) [CC-BY-SA-3.0 (www.creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons.

main aim of this chapter is to present a clarion call to bridge the gap that has opened up between western and Russian scholars and military analysts alike and initiate informed debate about the future evolution of the Russian military and its implications for Eurasian security and conceivably the potential parameters of future NATO-Russian defense cooperation.

Despite its absence in the declaratory reform agenda, official statements in 2009-2010 indicated that the term network-centric warfare had certainly become part of the reform lexicon. It not only featured in Russian military publications, but within the mass media and increasingly in statements by the top brass. Its usage was frequently inconsistent, often betraying a simple level of understanding of the term, with scant attention paid to the implications its adoption might have on the future course of the military reform. However, that it was in reality being actively adopted, and its organic link to the "new look" was most evident not in what the reformers or senior defense officials said, but in the conduct of operational-strategic exercises, even during 2009 as the upheaval occurred that attended the transition to the brigade-based force structure; this intensified experimentally throughout 2010 and was again field tested during Vostok 2010 (June 29 to July 8, 2010).[6] Moreover, leading Russian military journals paid greater attention at a practical level to the problems involved in the application of the network-centric concept to the conduct of combat operations.[7]

"New look" and network-centric warfare

The Chief of the General Staff (CGS), Army-General Nikolai Makarov, stated in July 2010 that the defense ministry planned to switch to the "network-centric principle" of command and control (C^2) by 2015. "As regards command and control systems, the current situation is fairly thin on the ground. We are doing extensive work to ensure that all (military) districts have digital equipment," Makarov explained, adding that by introducing new communications systems this principle could be realized. Makarov boasted that a new C^2 system would integrate the means of reconnaissance, target assignment, control of troops and weapons, in order to execute operations in real time. "Of course, there are many problems, but we are firmly determined to solve this ambitious task by 2015. As regards financing, the necessary funds have been allocated for these objectives," he affirmed.[8] Indeed, the timescale set in such grand visions of the bright future promised for the conventional Russian armed forces must be regarded with caution, not least since even though President Medvedev issued a *ukaz* in October 2009, after Makarov reached retirement age (60), extending his possible service by up to three years, the latter will be in retirement as his successor explains or ignores the failure to meet such targets. Exaggeration featured in many of the claims about the "new look" and its rapid progress, almost inevitably conjuring Chatsky's words from Aleksandr Griboyedov's immortal comedy, Wit Works Woe, "Look here, lie, but have a sense of proportion!" (*Poslushay, vri, da znay zhe meru!*); behind these public statements lay real, but tentative action.

CGS Makarov described the key priorities of the operational-strategic exercises, Lagoda and Zapad 2009, as providing opportunities to field test and study the transition a new command, control and communications (C^3) system based on network-centric principles: "First of all, to study the transition to the new armed forces command and control system, which is based upon the transition to the network-centric warfare system; to see how the new air defense and air force command and control system operates; and, also to test the Republic of Belarus and Russian coalition grouping's command and control system."[9] During Lagoda 2009, Russian commanders were interested in evaluating existing communications and reconnaissance systems. The Russian-made Grusha unmanned aerial vehicle (UAV) was field tested, as the then commander-in-chief (CINC) Army-General Vladimir Boldyrev tracked an image on the screen, he asked the designer to explain how the system worked, but having identified a target he was informed that there was no possibility to carry out a strike. Referring to the standards of Israeli built UAV's Boldyrev demanded that such domestic assets should be upgraded.[10] Russian UAV design has tended to concentrate on lighter models, and during Zapad 2009 the 95 kilogram (kg) Dozor-100 was tested performing short flights over the Baltic Sea. Though such testing was apparent in the exercise, their influence on its

Dozor-100 UAV By *Allocer* (Own work) [CC-BY-SA-3.0 (www.creativecommons.org/licenses/by-sa/3.0) or GFDL (www.gnu.org/copyleft/fdl.html)], via Wikimedia Commons

conduct, especially at tactical level was unclear.[11] New experimental communications models were field tested during Kavkaz, Lagoda and Zapad 2009, but while this served to link the need to overhaul existing C^3 systems, a key aspect in the reform agenda, it also signaled an early linkage between the "new look" and developing network-centric approaches to combat operations. More than ten years ago, the use of radio sets at company level preceded their later introduction at squad level; studying these exercises convinced the General Staff of the need to equip every soldier with personal sets. Those using the automated C^2 system reported that it was overly complicated, and far from user friendly. Throughout 2010, officers received additional training in the use of the new system, as the technology compelled their retraining.[12]

Operational testing of the Unified System for C^2 at the Tactical Level (YeSU TZ) was also conducted at the base of the 5th Motorized Rifle Brigade in the Moscow Military District (MD).[13] Defense industry specialists estimated that by 2011 three or four brigades could be equipped with the system at tactical level, and that the existing capacity may yield up to five or six brigades annually. Equipping one brigade with the YeSU TZ including the purchase of 3,000 radio stations, 4,000 computers, means of encryption, and vehicles, would cost 8 billion rubles.[14]

In January 2010, Russian Prime Minister Vladimir Putin said many decisions in this area were not being implemented: "For example, a general designer has still not been appointed to supervise the development of the armed forces' automated command and control system. No integrated structure has been set up to work out and put into practice a common science and technology policy in the defense industry. No comprehensive program has been developed to accumulate funds or minimize and optimize public spending to make it more effective."[15]

Network-centric developments in foreign militaries

Russian military theorists and analysts increasingly turned their attention to closely examining the development of network-centric capabilities in foreign militaries in two stages: following the US-led intervention in Iraq in 2003 and in the period during which the "new look" reform was in preparation and since its announcement. A number of themes can be identified from work published in leading Russian military publications, revealing a divergence of views as well as a consistent trend to scrutinize foreign military experience to understand more fully the nature of these advances.

An article by K.A. Trotsenko in *Voyennaya Mysl,* in April 2008, prior to launching the reform, assessed network-centric trends and their implications for Russian security since the NATO Summit in Riga in November 2006. This was viewed as an important occasion for Russian de-

fense and security elites, as the Comprehensive Political Guidance document that emerged in Riga not only stressed traditional themes such as collective defense, but it also reaffirmed that military force could be used by the Alliance to counter terrorism and other asymmetric threats in out of area operations. Consequently, according to the article, this placed new demands on the leading members of the Alliance, to prepare their militaries to orient towards high intensity conflicts involving the use of high-technology weapons. These terms however, were noted as vague concepts. The author referred to "item technology efficiency" and for the purposes of framing his discussion, he then defined the terms more clearly as "a weapon model whose totality of properties ensures its manufacture, maintenance and technical servicing in accordance with the most effective technology by comparison with the existing ones and implies optimal inputs of labor, material and time in the process of manufacture, operation and maintenance, including the model's preparation for functioning." Accordingly, a "high-technology armed conflict can be seen as an armed clash pursuing particular military-political aims and characterized by the member-states' military organization concentrating considerable efforts in a conflict area and by one or every belligerent using weapons that exceed in efficiency the existing mass-produced models."[16]

The nature of modern warfare and the military-technical levels involved in such conflicts was examined earlier in *Voyennaya Mysl* in 2002 by V.V. Kvochkov and Y.A. Martsenyuk.[17] However, Trotsenko suggested that events since, particularly the US-led intervention in Iraq and in his view, the 2006 NATO Riga Summit, had marked a significant change: in the case of the latter, the Alliance had agreed to further develop member states military capabilities, emphasizing expeditionary operations, with the weapons systems to match. Supremacy would feature in the information sphere, utilizing space, air and sea assets, allowing military operations to be unleashed in any region regardless of the military-economic potential of those countries involved, seen embryonically in Operation Desert Storm in 1991 and refined and harnessed in the US interventions in Afghanistan in 2001 and Iraq in 2003.[18]

Trotsenko pointed to the need to optimize C^2, in order to achieve the type of flexibility demanded by network-centric operations. This would compel three major shifts in Russian approaches:

- Combat organizational standards must conform to the practical indices achieved by coalition forces in the war against Iraq (2003), meaning that C^2 would need to be reformed.
- The number of organizational measures involved in preparing military operations should be optimized and reduced to the lowest reasonable level.
- Since there was a lack of automated C^2 systems at tactical level, the number of documents drawn up by C^2 agencies during war and peacetime should be reduced.[19]

In this area, there was clearly a long way to go before progress could be made. The Russian combat regulations published in 2004 recommended greater promptness by C^2 agencies, allowing subordinates' increased independence, while on the other hand insisting that the number of combat measures should be 21 (instead of 14-16 in 1989). According to the Regulations on Organizing and Conducting Combined-Arms Tactical Exercises (Part 2, Battalion-Company, 2003), more than 40 documents were needed for one company or battalion level live fire exercise.

It is unsurprising that Serdyukov's reforms entailed overhauling the need for this vast quantity of paperwork. Trotsenko understood that such strategic evolution and change had serious implications for Russia, which he recognized could not rapidly reorganize its armed forces within a short period and re-equip them for combat operations in a high-technology environment, consequently he recommended a two stage

approach. In the first stage, prior to the emergence of the necessary economic conditions, a wide ranging debate should occur in the pages of professional Russian military journals, to examine practical issues at tactical level. The military educational establishments and staffs down to battalion level must encourage a thorough analysis of combat operations in a high-technology environment, in order to develop a single comprehensive approach to enhance combat capabilities, taking into account the changing nature of the state's economic capabilities. Rationalization should then occur within the line units, combined with partial modernization of equipment and weapons systems. Forces should be trained on the basis of the lessons drawn from the Gulf Wars in 1991 and 2003.

In the second stage, as the economic capacity appears, practical work should intensify. First, by bringing the anti-terrorist capabilities of the armed forces up to a level where they might also be used to counter enemy special forces; increase the mobility of forces: "reconnaissance capabilities, and fire engagement capabilities of missile troops and artillery, as well as close-combat forces and weapons, viewing them as systems that make it possible not only to reconnoiter, control and engage with firepower, but also to secure concealed movement and deployment in a new area and acceptable conditions for personnel during self-sustained combat operations." Next, the efficiency of C^2 would be improved, as well as air defense, information systems and troop protection. Finally, enhancing the effectiveness of logistics and technical support would prove necessary in order that combined-arms units may pursue "self-reliant highly mobile combat operations." The overall theme, therefore, was to informationize the conventional armed forces at all levels.[20]

Kondratyev: on the shoulders of giants

Lieutenant-Colonel Aleksandr Kondratyev actively engaged in the debate on intelligence, network-centric warfare and military reform, publishing more than twenty articles exploring these themes, either as co-author or single author; including several that considered the application of network-centric warfare in support of ground, air and naval operations.[21] These were published in *Nezavisimoe Voennoe Obozrenie, Voyenno Promyshlennyy Kuryer, Voennaya Mysl,* and *Zarubezhnoe Voennoe Obozrenie,* respectively *(*Independent Military Review), (Military-Industrial Courier), (Military Thought), the professional journal of the General Staff and (Foreign Military Review), the leading publication of the Main Intelligence Directorate of the General Staff (*Glavnoye Razvedyvatelnoye Upravlenie*—GRU).

In addition to his candidate degree in military science, he is a member of the Academy of Military Sciences. Moreover, Kondratyev, though still a comparatively young officer, follows in the tradition of those that paved the way for such revolutionary thinking in military affairs, stretching back to Marshal Nikolai Ogarkov, and championed in the writings of the late Major-General Vladimir Slipchenko. The latter noted just before the intervention in Iraq in 2003 that: "Any future war will be a non-contact war. It will come from the air and space. Guidance and control will come from space, and the strike will be conducted from the air and from the sea using a large quantity of precision weaponry."[22]

Slipchenko previously argued that science and technological developments determine the type of warfare being conducted at any given time. Slipchenko, classified wars into six categories: starting with ancient wars (first-generation) and ending with wars characterized by the use of advanced conventional precision weapons having the destructive potential of tactical nuclear weapons (sixth-generation).[23] Sixth-generation wars, he wrote in 1999, would witness offensive aerospace operations, led by UAV's, and proceeded by electronic warfare and a supporting role being assigned to ground forces. Victory would pivot on the destruction of the enemy's economic infrastructure; the distinction between combatants and non-combatants would become blurred. This would eventually render nuclear weapons obsolete, since operational and strategic objectives could be met by massive precision bombings.[24]

For Slipchenko, the changing nature of armed conflict was clear, dominated until 2030 by forces com-

peting for information superiority; integrating intelligence, surveillance, C^2, targeting and firing into "reconnaissance-strike complexes." Space-based assets and UAV's would dominate this conflict landscape, kinetic-energy effects will still be the primary source of damage, augmented by acoustic, electromagnetic, radiation and thermal effects. Slipchenko suggested that as the state's political leadership pursued military reform in the future, they must appreciate the likely nature of warfare, though he admitted that the ground forces would still prove necessary in local or regional conflicts.

Slipchenko had his share of critics, including Colonel (retired) V. V. Zhikharskiy and Valentin Rog, who argued that he had deduced these lessons from the 1991 Gulf War and the NATO intervention in Kosovo in 1999, which had not demonstrated the arrival of the era of non-contact warfare.[25] Army-General (retired) Makhmut Gareev, the President of the Academy of Military Sciences, also questioned Slipchenko's non-contact view of future warfare, stating that ground forces will continue to be needed, especially in local wars, "when threats [against Russia] can be expected from all sides and enormous territories must be defended." Gareev referred to Russia's experience of combat in Afghanistan and Chechnya, in which urban warfare was underestimated, and argued that precision-guided weapons might prove ineffectual "if opposed skillfully."[26] More recently, in December 2009, Gareev argued that non-contact warfare would have proved difficult and politically risky to use in Georgia in August 2008, and that traditional contact warfare had largely achieved Moscow's main strategic and operational objectives.[27]

Gareev endorsed the "new look" and its pursuit of non-contact capabilities, but cautioned that contact warfare options must be pursued simultaneously, in some cases inflicting the latter type of warfare on an enemy that wants to avoid it. Slipchenko had prominent supporters, such as Admiral I.M. Kapitanyets, who believed that sixth-generation wars would be waged primarily by space and naval assets. He said that the Russian navy could wage fourth and fifth-generation wars, but would require significant enhanced investment in the future to conduct sixth-generation naval warfare.[28]

Jacob Kipp summarized Kondratyev's refined and detailed understanding of network-centric warfare:

> Kondratyev understands the core relationship in John Boyd's OODA Loop (observe, orient, decide, and act), the struggle for the mystery of time in a combat situation. The OODA Loop takes on a new dimension in the information age. The loop could be divided into two parts –one informational (observe and orient) and the second kinetic (decide and act) relating to both maneuver of forces and firepower. If industrial war emphasized the second (kinetic part of the loop) then the information age underscored the importance of the former, understood as C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance). Computational power and networks have made possible a quantum leap in informational flow, which has changed the informational/intellectual part of the loop. It turns intelligence into knowledge to aid the decision-makers across the entire battle space. Post-industrial kinetic means would also reshape future war. Kondratyev sees major possibilities in foreign work on lasers and nanotechnologies, making them important areas for Russia to develop. Not all the issues associated with the development and employment of these systems, have been answered. Yet, Kondratyev concludes that many governments had already committed to this technological revolution reshaping military art in the twenty-first century. Russia could not afford to ignore this "qualitative new military potential."[29]

Kondratyev, therefore, was a known advocate of non-contact approaches, prior to Serdyukov's reform commencing. One year after Serdyukov first formally announced the "new look" reform, on October 14, 2008, Kondratyev co-authored an article with Aleksandr Medin in *Voyenno Promyshlennyy Kuryer,* reflecting on its progress and linking the entire reform process to the adoption of network-centric warfare capabilities. Throughout 2009, as the TOE was overhauled, abandoning the former division-based system in favor of a brigade-based structure and progressing towards a three tiered system of C^2, the authors

noted that Russia was not alone in pursuing these approaches. The brigade-based structure was being introduced in Australia, China, Portugal and Spain, among other countries, and was first initiated in the US. As the authors concentrated their analysis on the US experience, noting the origins of network-centric warfare and tracing its evolution and progress, they emphasized that the problems encountered in the US were of particular interest to Russia as its military reform advanced.[30]

The recent reorganization of the US military began in 1999, when the Army Chief of Staff, General Eric Shinseki, published his vision for an advanced model of ground troops, in which the brigade would become the main combat unit, capable of deploying its subunits anywhere globally within 96 hours. Shinseki conceived the long term strategic plan for the US Army "Objective Force," including his "Future Combat Systems." However, the basis for this shift was laid earlier in the 1990's, when Army Chief of Staff (1991 to 1995), General Gordon Sullivan, paved the way for later transformations. He proposed equipping the brigade, division, and eventually corps with armaments and military hardware employing digital technology. Later Sullivan proposed Task Force 21, involving experimental training exercises to test a new TOE capable of meeting the requirements of a present day military-political situation: this would permit the pursuit of innovative forms and methods of conducting military operations and secure a level of situational awareness of the battlefield and *speed in reaching decisions* unattainable by the enemy.[31]

The experimental 4th Infantry Division (Fort Hood) was numerically reduced while receiving high-precision long-range weapons, advanced reconnaissance and monitoring systems and a new automated logistical support system. However, the main idea was to form advanced forces by equipping them with modern C^3 systems, which prompted its unofficial name of "computerized division." The authors noted: "The characteristic trait of the 'computerized division' is the restructuring of its combat units towards the reduction of their numerical strength, but with the preservation or even enhancement of their combat effectiveness by increasing strategic and operational-tactical mobility, achieving absolute superiority in the area of information and reconnaissance support, which ultimately made it possible to forestall the enemy in making decisions and performing maneuvers." That reform process was subject to change and fluctuation, and its key driver was the experimental adoption of network-centric capabilities. In 2003, Shinseki's successor, General Peter J. Schoomaker, advanced this work and the brigade types were reduced to three (heavy, infantry and Stryker), adopting a modular structure connecting all brigade subunits in a single information space and communications network.[32] It is interesting to contrast the American experience with how Serdyukov's reform was first implemented and the General Staff's revision to the brigade concept: moving from a narrowly defined uniform "heavy brigade" structure in 2009 towards forming three basic types (light, multi-role and heavy). It is likely that the brigade re-structuring in Russia has yet to appear in its final form.

Highlighting some of the problems encountered in the US experience, the authors stated: "The program

Spc. Raymond Poltera, a Tactical Unmanned Aerial Vehicle operator with 1st Brigade Combat Team, 4th Infantry Division, launches an RQ-7B Shadow 200 TUAV on Camp Taji, Aug. 11. The Shadow provides commanders on the ground throughout the MND-B area of operations the ability to quite literally see the entire ba Photo Credit: *Sgt. Jason Dangel,* via U.S. Army (www.army.mil)

underwent serious changes. The date of beginning the arrival of new hardware in the troops was postponed by three years. The pace of rearmament was reduced many times: first to two, then to one and a half, and finally, to one brigade a year. So, instead of 65 brigades, armed with new hardware, the ground troops could count only on 15 by 2030. At the same time, the sum of the initial expenses was to increase by 60 percent and might exceed $150 billion." Moreover, they noted that the Pentagon had decided to stop at 73 brigades with additional postponements to its proposed completion date.[33]

The role of intelligence

In October 2007, Kondratyev examined the transformation of US intelligence in the aftermath of the meta-terrorist attacks on New York and Washington on September 11, 2001 (9/11) and linked this with the information age in warfare and its new demands on the intelligence community. The appointment of US Navy Vice-Admiral (retired) John McConnell as the Director of National Intelligence in February 2007 prompted Kondratyev to assess his efforts to promote intelligence reform.[34] Kondratyev's linkage of the information age to modern demands on intelligence were themes he pursued following the announcement of the "new look," tracing attempts in Europe to form closer intelligence cooperation after the failure by US and UK intelligence agencies to share intelligence with their allies during the Kosovo campaign in 1999, and suggested the French re-entry into NATO military planning and force commands might undermine such cooperative trends.[35] Nonetheless, he constantly identified any evidence of progress in the US towards enhancing intelligence cooperation between the sixteen domestic intelligence agencies, and praised McConnell for his efforts to increase the information flow, particularly his contribution in creating the online intelligence library, Intellipedia, a classified version of Wikipedia.[36] Indeed, his coverage of these issues was extensive and detailed, including consideration of the joint work between the US Department of Defense (DoD) and the intelligence community to develop multi-mission UAV's, as well as robotic platforms, or exploring how the DoD's Defense Intelligence Agency (DIA) sought to expand and recruit talented personnel.[37]

Significantly, Kondratyev traced the development of US open source intelligence (OSINT) since World War II to its increased level of importance in the information age. Referring to the legendary CIA analyst, Sherman Kent, who remarked in 1947 that in peacetime 80 percent of information needed by politicians for decision making was available from open sources, Kondratyev observed the impact of the information era and the trend towards reducing the role of covert intelligence. As Kondratyev asserted, the modern intelligence officer is no James Bond.[38]

In this context, Kondratyev highlighted the growing role of OSINT in US military operations; referring, in particular, to the experience of the US 3rd Infantry Division in Iraq in 2005. Kondratyev then delineated examples of US centers that produce OSINT, such as the Asian Studies Department tasked with serving the interests of the US Joint Command in the Pacific, reporting to the Army Intelligence and Security Command since 1947. Briefly, Kondratyev provided an overview of the evolution of the Soviet Military Studies Office from 1986 to its successor in Fort Leavenworth, the Foreign Military Studies Office (FMSO), moving from its earlier narrow focus on Soviet military operations in Afghanistan and Russian operations in Chechnya to examine the militaries of Europe, Asia and Latin America as well as diversifying its analysis to include asymmetric threats and modern information warfare. Kondratyev believes (incorrectly) that all OSINT centers, tapping into a constant flow of information in the US, are part of an integrated network accessing large databases, media, and collecting open source material and disseminating products using restricted-access networks.[39]

Kondratyev recognized that many of the trends he explored in US experience would serve as major challenges in the context of Russia harnessing its own network-centric warfare capabilities. The development and use of computer technology in OSINT during the past two decades enables intelligence officers to access vast tracts of information necessary for assessment, monitoring and filling the needs of com-

mand elements. Kondratyev observed that all developed countries, including China, were pursuing a similar route. However, within the former Soviet Union, the lack of information technology and dated views of the concept of the information society itself meant that comparatively speaking these countries were merely starting out. According to Kondratyev, this impacts negatively on military educational establishments, unable to produce "information ready" products, at a time when the demand for quality is increasing.

The one exception is Belarus, which in 2007, issued instructions for the use of the Internet in the interests of the defense ministry, which Kondratyev surmised had made progress since.[40] The implications of these shifts occurring within the intelligence services of foreign countries in the balance between open and covert sources were not sufficiently assessed in terms of the politically sensitive issue of reforming the culture and practices of the GRU, the Federal Security Service (*Federalnaya Sluzhba Bezopasnosti*—FSB) and the Foreign Intelligence Service (*Sluzhba Vneshney Razvedki* —SVR).

International trends in network-centric warfare

In June 2009, a detailed assessment of the development of network-centric warfare capabilities in foreign militaries was co-authored by Boris Cheltsov, (First Deputy General Director and Executive Director of the Moscow Research Institute of Instrument Automation (MNIIPA), meritorious military specialist, doctor of military sciences, and member of the Academy of Military Sciences), Lieutenant-Colonel Iskander Zamaltdinov (candidate of technical sciences, senior scientific worker of the NIG on problems of information security and the REhB VA VKO) and Colonel Sergey Volkov (candidate of military sciences, corresponding member of the Academy of Military Sciences). "Network-centric war," "comprehensive network capabilities," and "information-centric war," were readily identified as the key features in reforming armed forces among the leading militaries internationally, though there was also a tacit recognition that Russia had proved too slow to instigate and follow such processes. Integration, increasing the level of interaction, and achieving synergy of forces by realizing the principles of network-centric concepts and integrating systems for command and control, communications computers, intelligence, surveillance and reconnaissance (C4ISR) were thus recognized as the hallmark of such reform and modernization efforts. The concept of NATO Network Enabled Capabilities (NNEC) emerged within the Defense Requirements Review in 2005.

The Network-Centric Operations (NCOIC) consortium was formed to assist the defense industry in meeting required levels of interaction and integration of future systems and complexes and ensuring the implementation of network-centric principles for controlling armed formations. In 2004, it involved 15 companies and by June 2009, their number had increased to 96 from 32 countries; 26 of which are NATO members. The consortium worked closely with the US Department of Defense (DoD) Directorate of Information Systems (DISA), and included representatives from the DoD, the intelligence community, the Department of Homeland Security, and other US agencies. Realization of the new NATO concept aims at establishing effective information and intelligence support for a broad range of military operations, starting with peace support operations to high-intensity military action. NATO military specialists emphasize that NNEC involves more than integrating systems in C4ISR; it also increases the level of interaction between *all participants* in an operation, including the means for destroying the target and material-technical support points, etc.[41]

These Russian analysts also perused developments within individual NATO countries, such as the framework document in France for "Information-Centric War" (Guerre Infocenter), which emphasizes information streams rather than networks as in the case of the US. Similar processes were identified in the German armed forces, progressing towards the creation of a future system for equipping and arming military personnel, "Infanterist der Zuknft," permitting the implementation of new principles of C^3 between combat units and the high command. This involves developing future assets for intelligence gathering,

personal computer systems, C^3 systems, such as a "tactical internet," to facilitate interaction between analogue communication assets and digital data transmission systems. Similar patterns were assessed in the experience of Canada and the UK, as well as beyond NATO, in Australia, New Zealand and Sweden.[42]

In late 2008, Kondratyev connected the end of the Cold War with the information revolution that occurred within western countries, which paved the way to revise military strategies and blueprints and the later introduction of network-centric capabilities. The term, first coined in computer circles as the information revolution advanced, and made possible the integration of computer systems that used different operating systems. Applied in the military sphere, the term denoted the paradigm of twenty-first century warfare and was the indispensable element in the revolution in military affairs (*revolyutsiya v voyennom dele*—RVD). In the Russian context, however, many analysts of these developments tended towards over simplification, and were guilty of a type of technological determinism.

As Kondratyev highlighted, the designers of the military concept, US Navy Vice Admiral Artur Cebrowski and DoD expert John Gartska, claimed its impact would be felt widely. Therefore, Kondratyev explained that network-centric warfare not only utilizes digital networks for the purposes of ensuring vertical and horizontal integration, but this also changes the way that warfare is conducted, with altered tactics in the operations of advance formations using dispersed combat disposition, optimizing the methods reconnaissance, simplifying and coordinating firepower and a dissolution of the tiers of C^2.[43] In short, applied correctly, network-centric operations jettisoned the twentieth century need for platform-based operations, displaced by network-centric operations. This enabled the combat potential of existing formations to advance well beyond their level of technical equipment (fire power, maneuverability, controllability, survivability etc).[44]

Information technology, applied in the military realm, thus enables the attainment of new levels of combat capability and increases the degree of realizing combat potential. As Kondratyev asserted, "At present, we can really talk about the fundamental shift from the platform-centric to network-centric warfare which, as its designers say, not only sets down the new principles of command and control of troops and forces, but also facilitates implementation of the RVD at the current stage." The resulting synergistic effect (2+2=5) results from the whole becoming greater than the sum of its parts. Nonetheless, Kondratyev also criticized those who suggest that linking to such a network would resolve all existing problems. Reminding his readers of the "trash in-trash out" adage in computer programming, he said that using such capabilities depended upon accurate situational information collected by intelligence and reconnaissance. Furthermore, he stated, "If the tank which is currently in service cannot pierce the armor of the enemy tank with its standard ammunition, it will not be able to do this even if it is equipped with the latest hi-technology C^3I [command, control, communications and intelligence] systems."[45]

While Kondratyev is undoubtedly a leading Russian proponent of network-centric approaches to modern warfare, he is equally realistic in his view that it does not represent a panacea; rather it should be regarded as a vector of development. Foreign experts on network-centric warfare admit that insufficient study has been devoted to the mathematical rationale underlying the resulting increase in combat potential. Consequently, the military expert community in the US, for example, has been split into supporters of the network-centric concept and those who remain skeptical. Supporters argue that its adoption enables every participant in combat operations to access accurate data on situational awareness, improving coordination, self-synchronization, speed of managing the forces, and that it broadens the combat potential of the forces. Critics, on the other hand, argue that its promotion from above may stifle criticism of the concept by commanders at the operational and tactical command levels.[46] Additionally, if, in accordance with network-centric principles, the pace of future combat operations continues to increase, a weaker enemy will attempt to prolong the conflict and win the war using only methods of avoiding kinetic events and asymmetric tactics, aimed at weakening the political will of the US. There is also concern about the

failure of an operation if the pace of the combat exceeds the ability of the US armed forces to evaluate the situation and reach the required decisions. Furthermore, network-centrism is a thesis which "overestimates the importance of information and information technologies," and also the inability to "fully realize the available technological potential."[47]

China

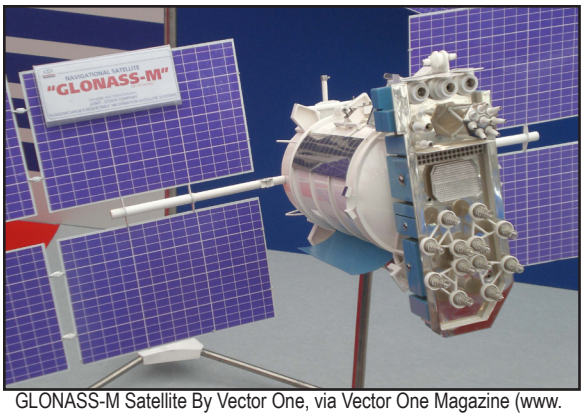
In the Russian military literature dealing with foreign developments in relation to network-centric warfare, the US military takes pole position. However, Russian analysts pay increasingly close attention to such activity in China, observing that the Chinese leadership has taken "aggressive steps" towards introducing network-centric approaches. Again, justifying this level of interest and attempting to downplay security concerns about their increasingly militarily powerful neighbor, reference is made to US studies of the People's Liberation Army (PLA). Kondratyev cited a 2006 RAND study ("Chinese Responses to US Military Transformation and Implications for the Department of Defense") which highlighted the PLA's implementation of network-centric concept as a major concern in the US: "Regardless of whether they adopt our brand of network-centric warfare, it is likely that they will enhance their investment in sensors and precision weapons."[48] Kondratyev remarked that the technological breakthrough in the PLA would provide the level of situational awareness and battlefield visibility needed by the Chinese.[49]

Other Russian assessments of such innovation within the PLA contend that it has seriously "caught up" in adopting the network-centric concept for controlling and conducting combat operations. The term "integrated network-electronic warfare" (INEW) has appeared in official PLA documents, and in the Chinese model it is envisioned that the new capability will be used both offensively and defensively. US studies, according to these Russian assessments, note an emphasis upon the former, with the development of laser weapons, Chinese space-based navigational systems to counter the space-based assets of a probable enemy, and C4ISR capabilities enabling the use of non-nuclear ballistic missiles against US Navy aircraft-carrier groups.[50]

Aleksandr Khramchikhin, Deputy Director of the Moscow-based Institute for Political and Military Analysis, described the emergence of a Chinese military mixing a mass army and modern technology, at a time when the PLA had ceased rehearsing military intervention in Taiwan.[51] In the spring of 2010, Russian advocates of the network-centric approach were actively publicizing the PLA rapidly moving towards a high-technology conventional force with its own asymmetric version of network-centric capabilities. Khramchikhin highlighted the PLA's major military exercise, Stride 2009, which involved rehearsing conducting operations at distances of up to 2,000 kilometers (km), resembling armed intervention in either Russia or Central Asia.[52]

China will not repeat the historical mistake made by the Soviet Union of entering a debilitating arms race with the US; but its network-centric emphasis appears essentially to represent a concerted asymmetric response. There was certainly long-standing grounds enabling the PLA to achieve this; ranging from the development of the People's Republic of China (PRC's) space program, the numbers of orbital satellites to advances in Chinese military theory.

FH-1 communications satellites, components of the first Chinese communications, surveillance and armed forces management system, Ku Dian, and the first navigation satellites of the BD-1 series, analogs of the US GPS system, were launched into space together with FH-1. During Stride 2009, the PLA reportedly used this system. This stands in stark contrast with the difficulties Russia has faced with its ***GLO****bal'naya* ***NA****vigatsionnaya* ***S****putnikovaya* ***S****istema*—(GLONASS) system, and introducing advanced digitized communications in the armed forces. New tactical theories in the framework of the PLA's "active defense" doctrine (which Russian observers interpret as offense based) include: "victory by using elite forces," "seizure of initiative by attacking first," "defeating the weak through superiority," "in-depth



GLONASS-M Satellite By Vector One, via Vector One Magazine (www.vector1media.com)

strikes" (operations conducted "entirely deep in the enemy's defenses," including missile and artillery strikes and use of landing forces). "Active defense," may also denote the PLA's readiness to conduct offensive operations, since Beijing would decide which state is hostile and precisely how this is manifested. Khramchikhin asserted that the PLA will "develop weapons of the surface-to-space class, which in case of war will be able to 'deafen and blind' US armed forces and deprive them of the capacity to strike targets in the Celestial Empire using high-precision weapons from the sea and from the air (it is a certainty that there will be no ground war between the US and the People's Republic of China —PRC) and make it exceedingly difficult for the US Navy to attack communications (the Chinese economy depends very much on deliveries of raw materials by sea)."[53]

In this strategic context, Moscow must not ignore this transition, even if partial, occurring within the PLA, as a shift towards information-based capabilities. While Vostok 2010, was most likely partly Moscow's response to Stride 2009, it certainly exaggerated both the progress of the "new look" and the capability to engage in network-centric operations.[54]

Cheltsov, Zamaltdinov and Volkov concluded their article by recommending further practical study of the experience of foreign countries in their adoption of network-centric warfare capabilities: "Our armed forces must thoroughly study the experience of foreign countries (China, by the way, has no qualms about doing this), in which there is both positive and negative aspects. Along with this, one must not forget about developing high-precision means of destruction, as well as about intelligence assets, which will also be augmented by the deployed information networks; otherwise, all such initiatives may be a total waste of money."[55] They also characterized the network-centric concept being pursued by the Russian armed forces as creating a system of systems:

> This "system of systems" is an aggregate of the means of intelligence gathering, the means of control and data transmission, as well as the means for destruction, all combined into a single reconnaissance-information-strike composite. The use in a combat space of a unified informational field, in which this composite is functioning, makes it possible to assign the most suitable asset to destroy an identified target. Moreover, the transmission of targeting data will be accomplished by organizing virtual channels for data transmission or via a web-portal. The successful functioning of the intelligence-information composite is, in effect, the realization of the "network-centric" war concept, meaning it makes it possible to conduct combat actions in a unified informational space.[56]

Network-centric command and control?

Testing automated C^2 systems during operational-strategic exercises in 2009-2010, and promising their full introduction by 2012-2015 within the newly formed brigades seemed, for the General Staff, to mark a shift towards realizing network-centric ambitions. Yet, the processes involved, reminiscent of earlier Soviet and Russian efforts to enhance C^2 also raised questions concerning the quality of the technology and how easy it might prove to use. These issues were raised in an article in *Izvestiya* in January 2010 by the Russian defense journalist, Dmitry Litovkin.[57]

Paradoxically some of the design issues encountered in the 1980's and 1990's during earlier efforts to develop a possible unified Soviet or Russian C^2 system inspire little confidence. In 1983, responding to a

request from the Soviet Army's Main Missile and Artillery Directorate, research and development (R&D) began on a system designated as *Manevr* (Maneuver): its purpose was to integrate C^2 over various weapons assets (artillery, missile complexes, aviation) into a single unified system capable of guaranteeing its continued link in any situation. According to Robert Nikolayev, involved in its design, the system's computer enabled C^2 via the transmissions of encoded commands, allowing headquarters to designate targets and issue orders. Nikolayev recalled how the communications directorate fiercely opposed innovation, and ignored his concerns about the unreliability of communications facilities and equipment; the directorate insisted that their systems were "perfect," and the faults lay elsewhere. However, Nikolayev criticized the weaknesses of Pentagon planning at that time in tasking different companies with designing and manufacturing individual elements of the combat management system, and suggested that by contrast Soviet systems were bulky but able to perform in a unified fashion. In 1993, Nikolayev was tasked with developing a new system, ostensibly for C^2 in airborne subunits, designated as "Polet-K," using wire, relay, space-based and computer assets. The C^2 system would be accommodated in airborne troops' existing command vehicles, with portable receivers. The Polet-K would convey C^2 to each aircraft, helicopter, gun, and individual soldier. By early 2000, the Polet-K was largely designed, with individual elements having been field tested, showing it was suitable for the airborne and ground forces; though it was not introduced.[58] However, during this period the technology gap between Russian and western combat information systems widened exponentially.

It is unclear whether Polet-K represented a move towards a single control algorithm integrating the operations of each fighting entity (brigade, battalion, company, individual soldier) in a unified system. "Today our developers are repeating the mistakes the Americans made in the early 1980's," Nikolayev suggested. "State-of-the-art components, color displays, GPS, even our own GLONASS emerges, but each element is being manufactured by separate firms. The country has no ideological substantiation of how all this is to work in aggregate. Therefore, the system is not working." Moreover, the expression of interest in procuring Mistral amphibious assault ships from France, to acquire sensitive technologies, as well as the ad hoc basis upon which the Russian defense ministry has purchased Israeli UAV's, suggests a lack of a unified and coordinated approach.[59]

The persistence of communications problems, dated assets and lack of automated systems was further highlighted in June 2010, during a high-profile visit to the Moscow MD command post, by President Medvedev, Defense Minister Serdyukov and CGS Makarov. Colonel-General Valeriy Gerasimov, Commander of the Moscow MD, reported that the Operational-Strategic Control Center, from which the district's troops are controlled, had been equipped with modern means of automation, allowing information to be exchanged in real-time. Gerasimov explained that more than 200 automated work stations were equipped with personal computers, among which 40 percent offer the means to participate in video conferencing in the directorates and services of the headquarters. The show-casing of such advances do not, however, reflect the general situation throughout the armed forces, as Medvedev said that around 80 percent of communications assets needed to be replaced, describing it as "simply not up to standard."[60] Medvedev stated that by 2012, all outdated analog means of communication must be replaced with digital systems, in order to create a unified C^2 system in the tactical echelon. Digital communication was needed in stationary and field conditions, to bring all subunits and command elements into a unified communications network, and Medvedev added: "In modernizing communications systems, the most effective technologies must be brought to bear, including foreign technologies; dual-purpose systems must be used, and when feasible, civilian technologies should be employed," referring to IR-telephone service, video-conferencing communications, and e-document exchange. In 2010, pilot projects in this regard were underway in Pskov Oblast and at 20 bases in the North Caucasus MD.[61]

Digitizing military communications, potentially an additional costly burden on defense ministry resources, was discussed and promised to be prioritized even before Serdyukov's reform. In October 2005,

the then Chief of the Directorate of Communications, Colonel-General Yevgeny Karpov, promised that a new digitized communications system, including nanotechnologies, would be appearing in the military by 2015.[62] Cost-cutting measures were pursued in order to make the project feasible, abandoning the replacement of existing cable bridging taps, and instead concentrating on using xDSL technology and flexible digital channels multiplexers to increase the traffic handling capacity of the channels.[63] More recently, it was reinvigorated by the recognition that without modernizing the C^2 system, Serdyukov's reform will simply fail.[64]

The long awaited automated C^2 system, Unified Tactical-level Command and Control System (YeSU TZ) was promised to be ready for introduction by November 2010. Its necessity was evidently underscored by the weaknesses in Russian C^2 exposed during the Five-Day War, and in March 2010 a defense ministry source said that it required up to one day for an order to reach the battlefield from Moscow (flatly contradicting CGS Makarov's claim that the new brigades are able to respond to an order to deploy "within one hour"). However, some Russian experts such as Colonel (retired) *Anatoliy Tsyganok,* head of the Military Forecasting Center at the Institute for Political and Military Analysis, believe that the YeSU TZ may already be outdated. YeSU TZ, also known as Sozvezdiye after its manufacturer in Voronezh, has had to contend with compatibility issues with the Akatsiya communications system (designed by Sistemprom). The system appears to be predicated upon developing and introducing an enhanced level of automated C^2 that will include intellectual systems of decision-making support, as part of the information and calculation subsystems as well as the decision making subsystem. In theory, orders will be issued by generals using the Akatsiya station and received at brigade level by the Akveduk station of the YeSU TZ, and in turn the latter would enable commands to reach battalion and company levels using secure high-speed digital channels. Yet, to achieve this level of integrated automated C^2, everything depends upon the reliability of the equipment and stability of the communications channels. Until the work is completed by Sozvezdiye on the automated C^2 system, Sistemprom cannot make Akatsiya compatible.[65]

There were additional concerns about how vulnerable to electronic warfare the new system might prove, which contributed to slowing its design progress. Further complicating factors related to working out operating algorithms for combat operations to allow every participant to understand them. During the field testing conducted in 2009-2010, battalion commanders complained that the system itself is extremely complex, and the large number of cursors and icons wastes time during interfacing. The defense ministry acknowledged that problems remained, but expressed confidence that these obstacles would be overcome, as the objective was to put in place a unified C^2 system for the entire armed forces. In the spring of 2010, one of the designers of the new fifth generation fighter aircraft was asked his opinion of the YeSU TZ, and his response made clear he had simply never heard of it.[66]

Synergy of man and machine and the race against time

The burden on the already overstretched Russian defense industry will certainly be accentuated over the next two decades by the adoption of network-centric capabilities. Leading Russian defense ministry researchers acknowledge this fact, and warn that it will entail a new research and development (R&D) effort to ensure the armed forces receive the necessary systems and software support. As early as May 2009, when it was still unclear to many observers that the "new look" was linked to network-centric capabilities let alone driven by it, Major-General Vasiliy Burenok, Director of the Defense Ministry's forty-sixth Research and Development Institute, co-authored with Aleksei Kravchenko and Sergei Smirnov an article in *Vozdushno Kosmicheskaia Oborona* (Aero-Space Defense) addressing this R&D requirement as a fundamental element in ensuring the transformation and modernization of the Russian armed forces. The authors argued in favor of the informationization of warfare and its connection to utilizing space-based assets to enhance C4ISR.[67]

Burenok, in the aftermath of the organizational transition to the brigade-centric force structure in the

ground forces, chose to publicly join what he characterized as the "polemic" on network-centric warfare initiated by Serdyukov's reform. In an incisive and ground-breaking article published in *Nezavisimoye Voyennoye Obozreniye* in April 2010, Burenok was in no doubt that the objective of the reform initiated in October 2008 was to enable the Russian conventional armed forces to meet the challenges that might arise in the first half of the twenty-first century: one of which will be network-centric warfare.[68] Burenok briefly defined the conceptual and theoretical features of network-centric warfare, as a system that consists of three subsystem grids: sensor, information and combat. This system is formed by the information grid, which mutually intersects and overlays the other grids and pervades the entire system of armed combat. The sensor system involves the means of reconnaissance, and components of the combat grid are the means of destruction, while these grids are combined by the technical means of C^2 bodies.[69]

Nonetheless, Burenok rounded on the existing nature of the "debate" in Russian defense and security circles, often characterized by wildly differing views on the network-centric concept, over simplification, and those who argue it is simply unnecessary. The existence of such diametrically opposed views, according to Burenok, risked negatively influencing Russian decision makers who might equally be misguided by newspaper reports or worse still, opinions voiced in the corridors of power. Burenok's contribution, however, to shaping the future debate on network-centric warfare and its implications for defense policy, lies in three areas: outlining the complexity involved in both the concept and its implementation within the Russian armed forces as an enormous challenge for the Russian state, characterizing network-centric warfare as consistent with the age-old military quest to act faster than the enemy, and highlighting the inter-relationship between force structure and the adoption of a new type of war-fighting capability.

Recognizing that network-centric warfare is essentially an attempt to achieve synergy between man and machine, an innately complex process, Burenok explained that the implications of adopting network-centric warfare on creating the necessary force structure is exceedingly difficult to predict, and he implied that logically more adjustments will be needed in the future as the transition evolves. Some, in his view, try to suggest it is possible to resolve these issues using a "big bang" approach marking a sudden leap towards its implementation, and he openly doubts whether this might prove successful. What was missing was the theoretical and practical experience within the Russian armed forces of conducting such network-centric operations. Burenok reinforced Kondratyev's earlier appeal in *Voyennaya Mysl* for greater scientific research devoted to the methodology and implications of adopting network-centric methods, suggesting that consequently the means are missing to verbalize how these wars will be fought or to calculate the algorithms.[70]

Moreover, Burenok argued that the key determinant in these operations will be achieving information superiority over the enemy, but this does not mean transmitting vast quantities of information to the combat elements (headquarters, subunits, personnel); instead it entails possessing a deeper understanding and realization of the battlefield, accurately weighing advantages over enemy disadvantages and rapidly transmitting such decisions to units and subordinates. Burenok describes this as the "game of forestalling," proving faster in intelligence collection and dissemination, decision making, employing strike and maneuver; or, in fact, what constitutes the very essence of combat. Thus, Burenok asserted:

> In general, the whole meaning of the network-centric war is precisely this: acting faster than the enemy. Forgetful of this, many Russian analysts unfortunately choose a simplified approach to the interpretation of the essence of implementing the principle of network-centric warfare, considering it as a simple automation of the process of management of the troops and armaments. True, automation does increase the speed of decision making and delivery of commands to the personnel, but what is required is not merely increasing the speed, but outpacing the enemy, not transmitting commands, but advance delivery and implementation of the rational decisions (precisely rational ones, not those that were reached in a cavalry attack-like rush!) which are best suitable

> in the particular situation and for the current positioning of the enemy troops and capabilities of the friendly troops. If this objective is not set as the main one when the path of development of the armaments and military hardware is set, it will not make sense to spend money on developing the means of reconnaissance, data transmission and automation of command and control: none of which will work and the money will be wasted. When fighting a network-centric army, we will be late all the time, hit the rearguards (*bit po "khvostam"*) and, as a boxer who misses and takes punches all the time, we will soon be exhausted. If there is no chance of winning in a straightforward "race against time," then we should look for alternative methods of achieving superiority over the enemy instead of trying to catch up with it, staying one step behind the enemy all the time. Incidentally, this is the path which the military specialists of China have chosen because they realize that they will not be able to create a network-centric system which would be on a par with the US system in the near future. This is why they chose to create forces, systems and means which ensure asymmetrical engagement of the enemy by employing firepower and electronic weapons to attack elements of the information grid (command posts, communications hubs, orbital groupings of the reconnaissance and command and control satellites, etc).[71]

It is important to note how quickly in Burenok's analysis, reference is made to the asymmetric adoption of network-centric warfare capabilities within the PLA or even the idea of future conflict between network-centric capable militaries, although he recognizes that an exclusively asymmetric approach presents its own risks. Burenok linked the adoption of network-centric warfare with longer term implications for force structure and training, since the struggle for dominance in the information space (*informatsionnoye prostranstvo*) demands developing scientifically sound theories of the use of troops in such operations, tested and refined in combat training and preparing combat training manuals and regulations. In turn, this forces change upon the system of military education, raises the need for greater levels of trained professionals and technically trained personnel with access to simulators and additional producing the necessary computer hardware and software. To adopt network-centric warfare capabilities, the force structure must be adapted to suit its needs; requiring structural identity or similarity among units, and information compatibility and transferability (the absence of nodes that might interrupt the information flow).[72]

Burenok then posited that force restructuring must therefore achieve the following:

> Stability (*ustoichivost*): the capability of forces to perform all their assigned missions. Recoverability (*vosstanavlevoaemost*): the capacity of forces to function or recover their combat capabilities after suffering defeat by the enemy. Proficiency (*operativnost*): the ability to respond to changes in the operational environment. Flexibility (*gibkost*): the capacity to generate (formulate) and execute different variants to perform a mission. Innovativeness (*innovatsionnost*): the capacity to apply new technical means and new methods of performing a mission. Adaptability (*adaptivnost*): the capacity (non-critical nature [*nekritichnost*]) to change processes for the execution of tasks and of organizational structure in response to change in the concept for the combat employment of troops.[73]

The first of these, stability (*ustoichivost*), demands forming the so-called soldier of the network-centric war, prepared "theoretically, technologically and psychologically." Burenok admitted that despite the structural progress of Serdyukov's reform the Russian armed forces in this area remain at the beginning of a very lengthy journey. However, focusing upon the last two aspects, Burenok pointed to the experience of foreign militaries in which innovativeness (*innovatsionnost*) has become a crucial principle in developing the armed forces of leading foreign countries in recent years. The US military, for instance, has outperformed all others simply in terms of the number of its innovations. This innovativeness denotes a military culture within which new types and models of arms can be quickly and efficiently absorbed into the units and formations of the US military. Correspondingly, it underscores the need to revise combat

training manuals and regulations accordingly, carefully select procurement procedures and ensure delivery of new assets to units along with the necessary resources for repair and maintenance. It is precisely this very culture of innovativeness that must be formed within the Russian armed forces, in order to ensure their successful transition into the information age. Moreover, the principle of adaptability (*adaptivnost*) implies forming military formations in ways that facilitate the information flow within the armed forces. All elements engaged in combat operations must access the network or terminate connection when the network is in operation without damaging either (the network or the combat operation). The network must "identify" structural subunits and ensure their effective operation as part of the network and "read" new data and adapt the algorithm of interaction among the elements in the network in response to new conditions.[74]

Into the future?

In this relatively sophisticated theoretical discussion within Russian military journals, it is hardly surprising to find that such views are influencing and shaping the understanding of network-centric warfare among the top brass. In March 2010, in an interview with *Rossiyskaya Gazeta*, CGS Makarov discussed several aspects of the "new look." His interviewer explored the introduction of the new C^2 systems, experimentally used during Kavkaz, Lagoda and Zapad 2009, and confirmed that the General Staff would again field test such assets during the operational-strategic exercise Vostok 2010. Makarov then corrected his interviewer, who mistakenly equated the reform and modernization of C^2 with possessing network-centric warfare capabilities; Makarov's interjection suggested that the official Russian military understanding of the network-centric concept does not limit itself to C^2, though understandably this has been designated as a key area in the reform:

> The network-centric method makes it possible to collect within the integrated information and communication space, all space, aviation, ground, and other assets, intelligence assets, and weapons: seeing in real time, the entire country, and in the future, the world. Also, to employ the requisite forces at a given moment in keeping with the situation. Modern software will make it possible to determine the most expedient options for the accomplishment of combat missions, choose the weapons, and assess the probable impact of attacks, but, *the commanding officer still has the final say*,[75] all the same. It is he that makes the final decision on the use of the troops. There is one further advantage of the network-centric method. Constant and concealed supervision of the enemy makes it possible to mount surprise attacks without direct contact with the antagonist. This sows panic and chaos, breaks his will, and ultimately results in his defeat. I shall in confirmation cite the second war in Iraq [2003]. According to our previous canons, two or threefold superiority in men and equipment was needed to break the enemy. For his assured defeat, five or sixfold. So, then, the Iraqis were five to six times superior [in numbers] to the Americans, but were smashed within three weeks.[76]

His interviewer, having grasped Makarov's reasoning, cynically asked when this "miracle" might appear in the Russian army, to which the CGS replied that "ambitious tasks" were set to "settle the issue" within two or three years; which is clearly an unrealistic timescale. Makarov stated that the future system is first being established in the North Caucasus MD, which makes sense in so far as the General Staff regard this as a probable participant in future conflict.[77] Nonetheless, Makarov offered a fairly balanced and succinct overview of network-centric warfare, and debunked the notion that Russian planners restrict themselves to a narrow understanding of the term. He also rightly identified that the human component will remain important, as the complexity of network-centric warfare is in that it seeks to produce synergy between man and machine, as well as appreciating the need to devise a systematized methodology to facilitate its introduction.[78]

It is clear, therefore, that while the fundamental driver behind Serdyukov's military reform is the adop-

tion of the network-centric concept, there is also a disconnect between the evidently unrealistic timescales advocated by the senior defense leadership and the most prominent domestic experts. Dismissing the target to implement network-centric capabilities in the Russian armed forces by 2012 or 2015, as declared by CGS Makarov at various times, domestic specialists consider that it will take a minimum of ten years, and most likely longer, to implement. Equally, the pages of the military press and media often host erroneous perceptions of the very nature of the network-centric principle, differences exist among its leading proponents, complicating the task of sifting and prioritizing at decision-making levels.

Integrating these approaches into the armed forces' structures is still more problematic. Kondratyev argues that preconditions necessary for its adoption are lacking, while there is also a need to address other problems in the Russian armed forces and in the framework of the country generally. This mostly relates to the search for new technologies, the transition of the defense industries to a path of innovative development, as well as changing the combat training manuals, overhauling military education and devising new forms and methods of using the armed forces. Military personnel will need to be taught to use modern hardware and software, revise their views of the role of information and introduce a climate of information exchange. In his view, the Russian military is only in the initial stages of the transition to network-centric principles and forming these capabilities, as it will demand developing new computer networks, support for information technology and strengthening the means of automizing C^2. During this initial phase it will prove necessary for the political leadership to grasp that the network-centric concept, as one of its founders suggested, is the same to warfare as e-business is to commerce. Digitizing the C^2 system, currently underway, is an essential element in that journey. However, there is no real parallel with western countries, where the peak of the information revolution preceded its breakthrough in the military sphere. President Medvedev's efforts to advance a culture of technical and economic innovation are also linked to military modernization: the system of e-government was scheduled to commence in 2011 and Kondratyev anticipates that the armed forces will prove able to "realize its network-centric concept, and therefore, achieve a new level of potential of the optimized armed forces, only after 2020."[79] Since the Russian military is playing catch-up, rather than assuming a leadership role in the process of the "informatization," it will only truly become revolutionary if it coincides with a comprehensive approach and a systemic effort to simultaneously develop and exploit promising technologies including laser and nanotechnologies.

Russian advocates of the network-centric concept berate those who over simplify it, suggesting that it envisages using packs of robots controlled from a single command, or tactical level combat formations do not require a unified situational awareness. Its proponents, based upon an analysis of the experience of western militaries, instead emphasize the conduct of combat operations in a unified informational space.[80] Fiber optics and space-based transmission are not possessed in sufficient quantities; acquiring other technical means that are an integral part of implementing the network-centric approach to warfare will place additional demands and burdens on the beleaguered domestic defense industry. Even its champions, such as Kondratyev, represent the adoption of network-centric capabilities as a gamble, but one in which the stakes are high and rooted in the General Staff's assessment of the type of warfare likely to be encountered in the future.[81]

Equally, the human dimension remains important, presenting significant long term challenges: the individual commander needs more than a grasp of the technology and its principles; initiative, responsibility and decision making in real time will compel changes to Russian military culture and in turn raise the expected standards among officers and NCO's. It will also present Russian intelligence with a monumental dilemma, as the recent high-profile cases of "illegals" uncovered in the US suggest that the intelligence system still places too much value on covert information. OSINT could have prevented the Russian air force bombing disused air fields during the Five Day War, and unless the culture of the GRU, FSB and SVR shifts to accommodate these new realities, the network-centric principle will encounter political barriers serving to reduce its potential effectiveness.

Adopting network-centric principles and developing such capabilities will radically alter traditional Russian military culture, displacing the rigidly vertical system of command and control: opting for a more fluid distributed model consistent with making the transition into the information age. Few Russian officials, officers and planners sufficiently appreciate the potentially revolutionary reform this process has unleashed.[82]

There will undoubtedly be problems encountered along the way, forcing rethinking and adjustment to existing and future planning. Yet, the adoption of network-centric principles is what gives real meaning to the "new look," which would otherwise fail to deliver the capability to wage information-era, 21st century military operations. Nevertheless, the implementation of network-centric principles will drive the reform process itself, dictating future force structuring, changes to personnel training, the precise and evolving procurement needs and ultimately the extent to which this proves successful will function as a litmus test for the "new look." It may be determined at a later date by the defense ministry whether to stop developing the number of network-centric brigades, to cap the process, or to prioritize particular formations on strategic axes; such recalibration would not necessarily signal failure. Alternatively, it could conceivably mutate into something unrecognizable to western military analysts.

Adopting network-centric capabilities may be characterized as a gamble, yet it will incur a high price for failure, relegating the Russian state in the future to playing a minor and decreasingly influential role as a security actor within Eurasia. On the other hand, any advance made in this long term quest will no doubt be viewed with suspicion among Russia's former Soviet neighbors. However, as the reform struggles to overcome its many hurdles, in essence this represents the underlying subtext, and its success lies predominantly in Russian hands.

---

1. The numerous challenges and policy issues raised as a result of Serdyukov's defense reform are considered in the policy-oriented book: Roger N. McDermott, The Reform of Russia's Conventional Armed Forces: Problems, Challenges and Policy Implications, (forthcoming) 2011. An independent assessment of the combat capabilities and combat readiness of the Russian armed forces on the second anniversary of the Five Day War, concluded that for the time being, many of the improvements that formed part of the "new look," such as forming operational-strategic commands, enhancing command and control and training, as well as the painstakingly slow rate of procuring new hardware and weapons systems has not delivered any tangible advance on the condition of the forces that entered Georgian territory in 2008: Aleksandr Khramchikhin, "Uroki Pyatidnevnoi Voini: Izmenilas li Rossiiskaya Armiya Posle Goryachei Dati 08.08.08?" (Lessons of the 'Five-Day War:' Did the Russian Army Change Following the 'Hot Date' of 08.08.08?), Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/wars/2010-08-13/1_5d_war.html, August 13, 2010. See: Roger N. McDermott, "Russia's Conventional Armed Forces and the Georgia War," Parameters, Vol. XXXIX, No.1, Spring 2009, pp.65-80; Carolina Vendil Pallin, Fredrik Westerlund, "Russia's War in Georgia: Lessons and Consequences," Small Wars & Insurgencies, Vol. 20, No. 2, June 2009, pp. 400–424.
2. The writings on the development of network-centric warfare capabilities are extensive. See the following examples: Vice Admiral Arthur K. Cebrowski, US Navy, and John J. Garstka, "Network-Centric Warfare: Its Origin and future," Proceedings, January 1998; Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," Proceedings, January 1999; Edward A. Smith, Jr., "Network Centric Warfare: Where's the Beef?" C4ISR Cooperative Research Program (CCRP), February 2000; John J. Garstka, "Network-Centric Warfare," Phalanx, Military Operations Research Society, December 2000; "Network-Centric Warfare," Report to Congress, Department of Defense, April 2002; Paul Murdock, "Principles of War on the Network-Centric Battlefiled: Mass and Economy of Force," Parameters, Spring 2002; Jeffrey R. Cares, Raymond J. Christian, Robert C. Manke, "Fundamentals of Distributed, Networked Military Forces and Engineering of Distributed Systems," NUWC-NPT Technical Report, May 2002; John J. Garstka, "Network-Centric Warfare Offers War Fighting Advantage: Datalinks are the New Weapon of the Information Age," Signal, May 2003; Gregory M. Maguire, "Concept of a Dynamic Organizational Schema for a Network-Centric Organization," Naval Post Graduate School, June 2003; John Arquilla, David Ronfeldt, "Swarming: The Next Face of Battle," Aviation Week & Space Technology, 29 September 2003; Michael Sirak, "Pentagon Commissions Net-Centric Studies," Jane's Defence Weekly, October 29, 2003; Henry S. Kenyon, "Tactical Operations: Tactical Web Takes Shape," Signal, November 2003; Col. Alan D. Campen, USAF (Ret.), "Look Closely At Network-Centric Warfare: Technology Can Both Aid and Dominate the War Fighter," Signal, January 2004; Daniel Gonzales, Michael Johnson, Jimmie McEver, Dennis Leedom, Gina Kingston, Michael Tseng, "Network-Centric Operations Case Study: The Stryker Brigade Combat Team," RAND, 2005; "The Implementation of Network-Centric Warfare," Department of Defense, Office of Force Transformation, January 2005; John Luddy, "The Challenge and Promise of Network-Centric Warfare," Lexington Institute, February 2005; Henry S. Kenyon, "Modular Devices Weave Tactical Networks," Signal Magazine, March 2005; Lt. Col. Steven G. Zenishek, David Usechak, "Net-centric Warfare and its Impact on System of Systems," Defense Acquisition University, April 2005; Nancy J. Wesensten, Gregory Belenky, Thomas J. Balkin, "Cognitive Readiness in Network-Centric Operations," Parameters, Spring 2005; Lt. Col. David Schmidtchen, "Network-Centric Warfare: the Problem of social Order, Working Paper No.125, Land Warfare Studies Center, June 2005; Melissa A. Schilling, Col. Christopher Paprone, "Modularity: an Application of General Systems Theory to Military Force Development," Defense Acquisition Review Journal, August-November 2005; Col. Stuart A. Whitehead "Battle Command: Toppling the Tower of Babel," Military Review, September-October 2005; Greg Grant, "Network-Centric Warfare Experts Look to Improve Communications," The Journal of Net-Centric Warfare, 11 October 2005; Brian L. Gilman, "Distributed Operations: Translating Tactical Capabilities Into Effects," Naval War College, February 2006; David S. Alberts, Richard E. Hayes, "Understanding Command and Control," Command and Control Research Project, March 2006; Network Centric Operations Case Study, Department of Defense, February 27, 2007; Clay Wilson, Network-Centric Operations: Background and Oversight Issues for Congress," Congressional Research Service, March 2007; "The Evolution of NATO Network-Enabled Capabilities," Network Centric Operations Case Study, Department of Defense, August 6, 2007.
3. V.R. Solovyev, Voyny XXI Veka (Wars of the 21st Century), Military Academy of the General Staff, Moscow, 2007; Voyennaya Doktrina Rossiyskoy Federatsii (Military Doctrine of the Russian Federation), February 5, 2010, http:// www.scrf.gov.ru/documents/33.html.
4. Jacob. W. Kipp, "Ten Years of Anti-NATO Exercises by Russian and Belarusian Armed Forces,"Eurasia Daily Monitor, Volume 6, Issue 178, September 29, 2009; Roger McDermott, "Zapad 2009 Rehearses Countering a NATO Attack on Belarus," Eurasia Daily Monitor, Volume 6, Issue 179, September 30, 2009; Jacob W. Kipp, "New Look Russian Military: 2009 Training Year and Beyond," Eurasia Daily Monitor, Volume 6, Issue 218, November 25, 2009; Roger McDermott, "Virtual Defense of the Russian Far East: Vostok 2010," Eurasia Daily Monitor, Volume 7, Issue 129, July 6, 2010; Jacob W. Kipp, "Vostok 2010 and the Very Curious Hypothetical Opponent," Eurasia Daily Monitor, Volume 7, Issue 133, July 12, 2010; Roger McDermott, "Reflections on Vostok 2010: Selling an Image," Eurasia Daily Monitor, Volume 7, Issue: 134, July 13, 2010.
5. Jacob W. Kipp, "Promoting the New Look for the Russian Armed Forces: the Contribution of Lieutenant-Colonel Aleksandr Kondratyev," Eurasia Daily Monitor, Volume 7, Issue 113, June 11, 2010.
6. See coverage of Vostok 2010 in Kipp and McDermott's work in Eurasia Daily Monitor Op. Cit.
7. V.I. Kazaryan, "Operacii, Boevie Deistviya, SetetsentrichnayaVoina," (Operations, Combat Actions and Network-Centric Warfare), Voyennaya Mysl, No. 2, 2010.
8. "Russian Armed Forces Should be Capable of Network-Centric Warfare by 2015 – CGS," RIA Novosti, July 14, 2010.
9. Vladimir Mukhin, *"Strane Skomandovali "v rug'e!" (*They Have Commanded the Country To 'Stand To'), Nezavisimaya Gazeta, September 17, 2009.

10. Olga Bozhyeva, "Festival 'Novaya Voina'" (The New War Festival), Moskovskiy Komsomolets, http://www.mk.ru/editions/daily/article/2009/10/08/364473-festival-novaya-voyna.html, October 17, 2009.
11. Viktor Litovkin, "So Strategicheskim Razmahom Rossiya Sozdaet Glubokoeshelonirovannie Oboronitelnie Strukturi na Evropeiskih Teatrah Voennih Deistvii," (Thunder of Fire, Flash of Steel. Russian Army's Operational-Strategic Exercises Have Revealed Not Only Reform Successes But Also Unresolved Problems), Nezavisimoe Voennoe Obozrenie, November 9, 2009.
12. Ibid.
13. Throughout this chapter reference is made to the former six military districts, which were subject during 2010 to the transition to four operational-strategic commands (OSK's), west, center, south and east; the original defense ministry planning envisaged these being formed by December 1, 2010, though by September 1, 2010 the West OSK had been formed and by October 1, 2010 the others followed. Critics of this initiative, intended to enhance command and control, noted the similarity of the reform with the US command model.
14. Ivan Karev, "Svyaz Dorogogo Stoit. Cena Komplekta Sredstv Upravleniya Dlya Brigadi – 8 Milliardov Rublei," (Communications Costs a Lot), Voyenno-Promyshlennyy Kuryer, No. 3, http://www.vpk-news.ru/3-319/qq/10379, January 27 – February 2, 2010.
15. "Putin Chairs Meeting in Voronezh to Discuss Re-equipping the Russian Armed Forces," Interfax, January 19, 2010.
16. K.A. Trotsenko, "O Podgotovke Voysk k Vedeniu Boevyh Deistvii v Visokotechnologichnom Voorugennom Konflikte," (How to Prepare Forces for Combat Operations in a High-Technology Armed Conflict), Voennaya Mysl, No. 4, 2008, pp. 51-57.
17. V. V. Kvochkov and Y. A.Martsenyuk, "On the Character of Wars and Armed Conflicts with the Participation of the Russian Federation," Voyennaya Mysl, No. 2, 2002, World News Connection (WNC), accessed, August 2, 2010.
18. Trotsenko, "How to Prepare Forces," Op. Cit.
19. Ibid.
20. Ibid.
21. A. Kondratyev, "Realizatsiia Kontseptsii 'Setetsentricheskaia Voina' v VVS SShA," (The Realisation of the Concept 'Network-Centric Warfare' in US Army Aviation), Zarubezhnoe Voennoe Obozrenie, http://pentagonus.ru/publ/24-1-0-1159, No. 6, May 2009; V. Baulin, A. Kondratyev, "Realizatsiia Kontseptsii 'Setetsentricheskaia Voina v VMS SShA," (The Realisation of the Concept 'Network-Centric Warfare' in US Naval Forces), Zarubezhnoe Voennoe Obozrenie, No. 6, June 2009; Aleksandr Kondratyev, Aleksandr Medin, "Doroga SShA k Novomu Obliku Sukhoputnykh Voisk," (US Path Toward the New Model of the Ground Troops: Ten Years and Almost $100 Billion Are Gone),Voyenno Promyshlennyy Kuryer, http://www.vpk-news.ru/40-306/2009-05-02-13-25-08/3329, October 14, 2009; A. Kondratyev, "Problemy Organizatsii Aviatsionnoi Podderzhki Operatsii Sukhoputnykh Voisk SShA," (The Problem of Organization of Aviation Support for Ground Troops Operations), Zarubezhnoe Voennoe Obozrenie, http://pentagonus.ru/publ/problemy_organizacii_aviacionnoj_podderzhki_operacij_sukhoputnykh_vojsk_ssha/23-1-0-1411, No. 9, November 2009.
22. "Major-General Vladimir Slipchenko Views Possible US 'Non-Contact' War on Iraq," Vremya Novostei, October 5, 2002.
23. Vladimir I. Slipchenko, Voyna Budushchego (Future War), Scientific Reports edition 88 (Moscow: Social Science Foundation, 1999).
24. Ibid.
25. Colonel (Ret.) V. V. Zhikhaskiy, "On the Issue of Wars of the Future," Voyennaya Mysl, No. 4, 2000, WNC, accessed, August 5, 2010; Valentin Rog, "Borba Zza Gospodstvo v Vozduhe," (Priority-Attainment of Air Superiority: Use of Precision Weapons Demands Adequate Means of Counteraction), Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/concepts/2001-01-26/4_struggle.html, August 31, 2001.
26. General of the Army Makhmut Gareyev, "For the Army of the 21st Century: A Local War Is First of All a War," Krasnaya Zvezda, October 31, 2000, WNC, accessed August 3, 2010..
27. Makhmut Gareev, "Opyt pobeditelei v Velikoi Voine ne Mozhet Ustaret," (The Experience of Winners of World War II Cannot Become Obsolete), Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/concepts/2010-03-12/12_experience.html, March 12, 2010.
28. I.M. Kapitanyets, "What Should We Be Prepared For?" Voyenno-Istoricheskiy Zhurnal, June 2001, WNC, accessed, September 8, 2009.
29. Jacob W. Kipp, "Promoting the New Look for the Russian Armed Forces: The Contribution of Lieutenant-Colonel Aleksandr Kondratyev,"Eurasia Daily Monitor, Volume 7, Issue 113, June 11, 2010.
30. Aleksandr Kondratyev, Aleksandr Medin, "US Path Toward the New Model of the Ground Troops: Ten Years and Almost $100 Billion Are Gone," Voyenno Promyshlennyy Kuryer, October 23, 2009.
31. Author's emphasis.
32. Kondratyev, Medin, "US Path Toward the New Model," Op. Cit.
33. Ibid.
34. Aleksandr Kondratyev, Petr Mikhailov, "Medal za . . . Reformirovanie," (An Award for … Reform), Voyenno Promyshlennyy Kuryer, http://www.archive.vpk-news.ru/article.asp?pr_sign=archive.2007.204.articles.geopolitics_02, October 3, 2007.
35. Aleksandr Kondratyev, "Edinaia Razvedka Evrosoiuza: Byt ili ne Byt?" (The European Union Intelligence Service: To be or Not to be?), Voyenno Promyshlennyy Kuryer, http://resultat61.ucoz.ru/news/2009-03-09-368, February 25, 2009.
36. Aleksandr Kondratyev, "Makkonell Sdelal Svoe Dlo, Makkonell Mozhet Ukhodit," (McConnell Has Done, McConnell Can go Away), Voyenno Promyshlennyy Kuryer, March 11, 2009.
37. Aleksandr Kondratyev, "K Voinam Bez Shertv," (To Wars Without Victims), Voyenno Promyshlennyy Kuryer, http://www.archive.vpk-news.ru/article.asp?pr_sign=archive.2009.282.articles.weapon_01, April 29, 2009; Aleksandr Kondratyev, "Detskaia Stranichka Dlia Shpiona," (A Child Page for a Spy), Voyenno Promyshlennyy Kuryer, http://www.archive.vpk-news.ru/article.asp?pr_sign=archive.2009.288.articles.conception_01, April 10, 2009.
38. Aleksandr Kondratyev, "Na Osnove Otkrytykh Istochnikov," (On the Basis of Open Sources), Voyenno Promyshlennyy Kuryer, http://www.vpk-news.ru/36-302/dss/2061, September 16, 2009.
39. Ibid.
40. Ibid.
41. Author's emphasis; Boris Cheltsov, Iskander Zamaltdinov, Sergey Volkov, "NATO and Western Countries' Work on 'Network-Centric' Warfare and Russia's Slowness in This Area," Vozdushno Kosmicheskaya Oborona, June 21, 2009, WNC, accessed, October 30, 2009.
42. Cheltsov, Zamaltdinov, Volkov, "NATO and Western Countries' Work on 'Network-Centric' Warfare," Op. Cit.
43. Kondratyev, Medin, "US Path Toward the New Model," Op. Cit.
44. M. Shchukin, A. Kondratyev, "Razvedyvatel'noe Obespechenie Boevykh Deistvii Sukhoputnyhk Voisk SShA v Gorodskikh Usloviiakh," (Intelligence Support for the Military Operations of US Ground Troops), Zarubezhnoe Voennoe Obozrenie, http://pentagonus.ru/publ/23-1-0-818, No. 9 September 2008; Aleksandr Kondratyev, "Chtoby Zamenit Riadogo Raiana,"(To Replace the Soldier Ryan), Krasnaya Zvezda, http://www.redstar.ru/2008/12/17_12/4_04.html, December 17, 2008; A. E. Kondratyev, "Obshchaia Kharakteristika Setevykh Arkhitectur, Primwniaemykh Pri Realizatsii Perspectivnykh Setetsentricheskikh Kontseptsii Vedushykh Zarubezhnykh Stran," (General Characteristics of the Web Architecture, Used in the Process of Applying the Perspective of Network-Centric Concepts of Leading Foreign Countries), Voyennaya Mysl, No. 12, December 2008.
45. Kondratyev, Medin, "US Path Toward the New Model," Op. Cit.
46. Ibid.
47. Ibid.
48. James C. Mulvenon, Murray Scot Tanner, Michael S. Chase, David R. Frelinger, David C. Gompert, Martin C. Libicki, Kevin L. Pollpeter, "Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense," RAND, 2006.
49. Kondratyev, Medin, "US Path Toward the New Model," Op. Cit.
50. Cheltsov, Zamaltdinov, Volkov, "NATO and Western Countries' Work on 'Network-Centric' Warfare," Op. Cit.
51. Aleksandr Khramchikhin, "Milliony Soldat Plius Sovremennoe Vooruzhenie," (Million Soldiers Plus Modern Equipment), Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/forces/2009-10-09/1_china.html, October 9, 2009.
52. A. Kondratyev, "Nekotorye Osobennosti Realizatsii Kontseptsii 'Setetsentricheskaia Voina' v Vooruzhennykh Silakh KNR," (Some Peculiarities of the Realisation of the concept "Network-Centric War" in Chinese army), Zarubezhnoye Voennoye Obozreniye, No. 3, 2010, pp. 11-17; "Ucheniia," Zarubezhnoye Voennoye Obozreniye, No. 8, July 31, 2009; Aleksandr Khramchikhin, "Starye Osnovy Novoi Doktriny,"(Old Basis of the New Doctrine), Voenno□Promyshlennyi Kuryer, No. 6, http://www.vpk-news.ru/6-322/2009-05-02-13-24-56/12708, February 17, 2010.
53. Aleksandr Khramchikhin, "Kitai Gotovitsya k Voine v Kosmose. V Podnebesnoi Nachinaut Razrabativat Nastupatelnie i Oboronitelnie Operacii za Predelami Zemli," (The Celestial Empires Settles in on the Orbital Theater of Operations), Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/wars/2009-11-13/1_china.html, November 17, 2009; Aleksandr Khramchikhin, "Bligaishii Sosed – Budushaya Voennaya Sverkhdergava," (Immediate Neighbor is the Future Military Superpower,) Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/forces/2009-03-27/1_china.html, March 27, 2009.
54. Aleksei Nikolsky, "To Be Assessed by the East," Vedomosti, March 9, 2010; Kipp, "Vostok 2010: and the Very Curious Hypothetical Opponent," Op. Cit.
55. Cheltsov, Zamaltdinov, Volkov, "NATO and Western Countries' Work on 'Network-Centric' Warfare," Op. Cit.
56. Ibid.
57. Dmitry Litovkin, "Prikaz Pentagona: Mobilniki – k Bou. Gotova li Rossiya k 'Setechentricheskim Voinam," (Order From the Pentagon: Cell Phones Into Battle,) Izvestiya, http://www.izvestia.ru/armia2/article3137196/, January 18, 2010.
58. Ibid.
59. Ibid; See: Roger N. McDermott, "French 'Tin Cans' or Technology Transfer? Vysotskiy on the Mistral," Eurasia Daily Monitor, Volume 7, Issue 144, July 27, 2010.
60. Andrey Garavskiy, "Svyaz Reshaet Vse," (Communications Solve Everything,) Krasnaya Zvezda, http://www.redstar.ru/2010/05/22_05/1_01.html, June 4, 2010.
61. Ibid.

62. Interview with CGS Army-General Nikolai Makarov, Voyenno Promyshlennyy Kuryer, February 25, 2010; "Russian Army To Get New Control, Communication System by 2015," Agentstvo Voyennykh Novostey, October 18, 2005.
63. Lieutenant-Colonel A.B. Akulinchev, "Problemi Chifrovizacii Voennih Setei Svyazi i Puti ih Resheniya," (Problems of Digitizing Military Communications Networks And Ways of Solving Them), Voyennaya Mysl, http://www.nateks.ru/pub/index.php?lpub=82&link=pub, No. 4, 2006.
64. Aleksandr Kondratyev, "Nuzhna li Informatsionnaia Revoliutsiia v Armii?" (Is there Any Need for Information War in the Army?), Voyenno Promyshlennyy Kuryer, http://www.archive.vpk-news.ru/article.asp?pr_sign=archive.2008.264.articles.conception_01, December 10, 2008.
65. Viktor Poltavtsev, "Batyanya-Gigabait," (Daddy-Gigabyte), Russkiy Newsweek, http://www.runewsweek.ru/country/33006, March 29, 2010.
66. Ibid.
67. Vasiliy Burenok, Aleksei Kravchenko, Sergei Smirnov, "Kurs – na Stetsentrcheskuiu Sistemu Vooruzheniia," (Direction to the Network System of Arming), Vozdushno Kosmicheskaia Oborona, http://www.vko.ru/DesktopModules/Articles/ArticlesView.aspx?tabID=320&ItemID=328&mid=2892&wversion=Staging, May 2009.
68. Vasiliy M. Burenok, "Bazis setecentricheskih voyn – operezhenie, intellect, innovacii," (Basis for Network-Centric Wars: Anticipation, Intellect, Innovations) Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/concepts/2010-04-02/1_bazis.html, April 2, 2010.
69. Ibid.
70. A. E. Kondratyev, "Problemnye Voporsy Issledovaniia Novykh Setetsentricheskikh Kontseptii Vooruzhennykh Sil Vedushikh Zarubezhnykh Stran," (Problematic Questions Over Research on New Military Concepts of Leading Foreign States), Voyennaya Mysl, No. 11, November 2009, pages 61-74.
71. Burenok, "Basis for Network-Centric Wars," Op. Cit.
72. Ibid.
73. Ibid.
74. Ibid.
75. Author's emphasis.
76. Yuriy Gavrilov, Interview with General Staff Chief Makarov, Rossiyskaya Gazeta, March 23, 2010.
77. Ibid.
78. Kondratyev, "Problemnye Voporsy," Op. Cit.
79. Kondratyev, Medin, "US Path Toward the New Model," Op. Cit.
80. Cheltsov, Zamaltdinov, Volkov, "NATO and Western Countries' Work on 'Network-Centric' Warfare," Op. Cit.
81. Aleksandr Kondratyev, "Stavka na Voiny Budushchego," (The Stake for Future War), Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/concepts/2008-06-27/1_future.html, June 27, 2008.
82. Sergey Melkov, Oleg Zabuzov, "Initiativa v Onlaine I Offlaine. Virtualnie Voini I Realnie Problem," (Initiative Online and Offline. Virtual Wars and Real Problems,) Nezavisimoye Voyennoye Obozreniye, http://nvo.ng.ru/realty/2010-07-16/1_online.html, July 16, 2010.