MP190451V1
MITRE PRODUCT

MITRE

Russian Military Thought: Concepts and Elements

Sponsor: US European Command ECJ39
Dept. No.: P663
Contract No.: W56KGU-18-D-0004-S120
Project No.: 0719S120-J3

The views expressed in this document are those of the author and do not reflect the official policy or position of MITRE, the Department of Defense, or the US government.

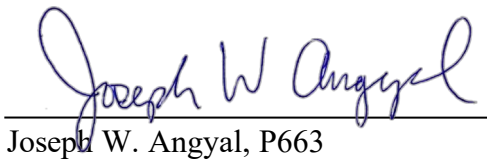
This document is approved for public release, distribution unlimited. Case numbers 19-1004 Russia's military thought; 19-0592 military art; 19-1069 reflexive control; 19-0047 asymmetric operations; 19-18-4231 A2AD; 18-1941 cyber concepts; 19-0314 information environment; 19-1451 definition of war; 18-4369 future war; 19-0807 Gerasimov; and 19-1546 Conclusions (and Foreword and Introduction) were used to compose this document.

Timothy L. Thomas

August 2019

McLean, VA

Approved By



8/8/2019

Joseph W. Angyal, P663
US European Command Project Leader

Date

Foreword

Technology has dramatically increased the speed at which decisions must be made, expanded the spectrum of military thought (from the strategic to the planetary), and focused more attention on innovative thinking and risk-taking. This report, *Russian Military Thought: Concepts and Elements*, considers technology's impact on military thought while also considering the latter's historical legacy passed from the Soviet to the Russian period. Two issues are thus at play in the report, traditional ones and those associated with information-age advances. Initially, the report examines several concepts from the Soviet era still in vogue today, such as the forms and methods of warfare, forecasting, and the initial period of war, among others. The past remains important for the present and continues to affect the way Russia analyzes its situational context. Next, how these basic concepts are applied to information-age advances are examined. For example, there are Russian-authored articles on the forms and methods (traditional thought) of network-centric conditions, aerospace defense, and cyber issues (information-age thought), among others. Forecasting must assess the impact on the nature of war from weapons based on new physical principles. The speed of cyber operations indicates that forces must be prepared now for the initial period of war (IPW). Planning tomorrow for a surprise attack is more than a day late, as the cyber IPW may result in the conflict's end before it starts.

The report is divided into twelve chapters. Chapter One provides an overall introduction to the topic of military thought. Chapter Two offers some historical and current contextual information regarding Russian military thought, to include what is expected from military officers today. Chapter Three looks at the importance of military art's influence on thought processes. Chapter Four updates Russian use of its reflexive control concept, which is a way of manipulating or deceiving adversary thought processes. Chapter Five updates Russian use of asymmetrical and indirect operations. Chapter Six discusses Russia's concept of disorganization and its impact on command and control issues. Chapter Seven offers nine Russian cyber and information issues for consideration. Chapter Eight explores the invisible aspect of the information environment (underwater cables, satellites, electrons, etc.). Chapter Nine examines a 2017 discussion on the concept of "war" in Russia. Chapter Ten looks at Russian forecasts of future war. Chapter Eleven offers a summary of the thoughts of General Staff Chief Valery Gerasimov. Chapter Twelve offers several conclusions about Russian military thought.

The report is of interest for its focus on purely Russian military thought. It attempts to avoid mirror-imaging Western concepts (hybrid, grey zone, etc.) onto Russian military thinking. It represents the first focused study on the topic of military thought since the edited 1981 book *Soviet Military Thinking*. The report in no way replaces that volume but rather supplements it.

Timothy Thomas
EUCOM Information Operations Domain Specialist
MITRE Corporation, 2019

Acknowledgments

The author is solely responsible for the selection and analysis of the material in this work.

While there are many people who assisted in the preparation of this work, the author would like to acknowledge the support of several individuals. First, Dr. Harold Orenstein of Leavenworth, Kansas, deserves special recognition. He translated numerous key documents from Russian into English, as the footnotes continuously note. Without his support, this report would lack many key details. Second, the author would like to express his thanks to Colonel Michael Jackson, the European Command's former J39, who supported and encouraged this work along with two important staff members, Chris Kirschman and Alan Bal. Finally, the MITRE staff, who helped with the editing and clearing of the chapters, were instrumental in pushing the product along. Joe Angyal, Matt Eager, and Marion Michaud were key players who spent numerous hours working through the report's chapters. David Cleary helped with formatting the final product. My sincere thanks to all of you for your help.

Table of Contents

This page intentionally left blank.

1 Introduction

There are many issues that have motivated the development of this report. However, two primary ones are a need to inform Western analysts of Russia's military thought process, which differs from that in the West; and the need to demonstrate that Western mirror-imaging of its concepts onto Russian thinking doesn't always work, whether it be hybrid warfare concepts, anti-access area denial (A2AD) thinking, or grey zone concepts. Russia doesn't utilize many of the concepts that the West does, and those that it does use may be interpreted in different ways or have other issues attached to them. There are also many assumptions about Russian military thought that are based on false premises.

Initially, the report examines several specific thought processes of the Russian military, to include some that are seldom if ever discussed in the West. These concepts include disorganizing an opposing force, reflexively controlling them, examining numerous forms and methods of applying force by branch of service, and finding innovative ways to employ military art, among other issues.

There are other concepts, such as indirect and asymmetric operations, that numerous countries examine but implement them in various ways according to national values and traditions. Russia is no exception to this process, as several authors have written on indirect and asymmetric operations. Even the definition and concept of "war" is being reconsidered by Russia. In 2017, there was a long discussion among military specialists in Russia about the topic of war. These articles examined whether nonmilitary issues, to include the civilian use of cyber capabilities, had changed war's character. Once it became apparent that cyber weaponry potentially could take out a nation's power or state control mechanisms with special operations to destroy critical infrastructure targets (SODCIT), the definition of war apparently warranted reconsideration.

Over the course of the past two decades, Russian military thought also has benefited from the conduct of serious "lessons learned" analyses from their forces' combat operations in Chechnya, Ukraine, and now Syria. Russia's Chief of the General Staff, Valery Gerasimov, underscored the need to learn not only from the conflicts that involved Russian operations but also those that the West undertook, such as in Afghanistan and Iraq, and they have done so.

Recent developments initiate new forms and methods of warfare and require new forecasts of the evolving nature of future war. For example, Russia's military-industrial complex has developed new electronic warfare capabilities that offer additional protections for domestic command and control functions, while finding ways to debilitate foreign ones. In turn these developments have enabled new applications of military art, which is defined as the use of knowledge in innovative ways. Gerasimov noted that advanced weaponry imparts a new impetus to ways of thinking about military art and stressed that warfare cannot be stereotyped, since each conflict has a logic all its own.

Cyber and digital issues have been introduced into underwater cables and satellites, creating an invisible digital environment with which to contend. These science and technology issues affect warfare, military art, and other issues such that it is fair to say that technology now determines strategy, since with such assets it is now possible to reach the other side of the globe in milliseconds. On a geopolitical scale, Russia concentrates attention on trends in warfare that are developing and that affect how future war might unfold. It remains equally important for the ntion to ensure its "equal security" when nuclear weaponry and other non-nuclear but strategic operations are involved.

Meanwhile, in the West, the focus has centered on several specific topics: hybrid or grey zone operations, multi-domain operations, A2AD, and C4ISR issues. Each of these concepts is valuable, but they sometimes are mistakenly transferred onto Russian thought. Such stereotyping of Western concepts onto Russian actions causes analysts to miss some of the key directions in which Russian thought is taking the Defense Ministry.

This report attempts to offer some of these concepts and elements of contemporary Russian military thought for the consideration of Western analysts. It is composed of this chapter and eleven others. Chapters Two through Five discuss the basic building blocks of military thought and apply them to some contemporary examples. Chapters Six through Eleven discuss how these elements are either applied or updated to fit some specific information-age advances in more detail. Some new concepts have emerged as well.

Chapter Two, "Russian Military Thought: Building on the Past to Win Future Hi-Tech Conflicts," discusses the need to not only uncover the nature of future struggles but how to contend with them. Similarities between Soviet and Russian thought are examined as well as the need to avoid stereotyping and to develop creative thought in Russian officers. It is the latter who must demonstrate initiative, boldness, decisiveness, and risk in their decision-making in a hi-tech environment, according to Gerasimov.

Chapter Three, "Russian Military Art and the Creative Employment of Knowledge," focuses on Gerasimov's desire to improve the application of military art, which he noted is due to new developments in weaponry. Technological advances are providing the impetus for such thinking. The use of electronic warfare or cyber capabilities, for example, can debilitate adversary systems and thus alter the correlation of forces of the sides. The future promises to provide opportunities in artificial intelligence and quantum computing, so creativity has few boundaries at the moment.

Chapter Four, "Russia's Reflexive Control Theory: Manipulating an Opponent to One's Advantage," discusses numerous uses of the concept over the years, from manipulating an adversary's view of Russian military doctrine to altering an opponent's understanding of information space. Reflexive control theory is used in cyber and information capabilities as well as on the battlefield, according to Russian documents. It is a method of deception.

Chapter Five, "Russia's Asymmetric Concept: Based on Military Art, Geopolitics, and Risk," is based on a force's intellectual-technical superiority over an opponent and focuses on uncovering a weak spot in an adversary's systems that might have tactical or even strategic consequences. It is an important theory, such that Gerasimov requested that the Academy of Military Science develop a holistic approach to the theory of asymmetric operations. He has not requested that in regard to any other issue.

Chapter Six, "Connecting GPS Interference with Russia's A2AD Concept," discusses Russia's focus on disorganizing an opponent's command and control capabilities. It appears that even at the brigade level, Russia has called for the development of a disorganization plan to be implemented against an opponent in time of conflict. From a Russian perspective it appears that the disorganization of command and control (C2D) is as important as A2AD.

Chapter Seven, "Russia's Context for Cyber and Information Issues: Nine Thoughts for Consideration," discusses the importance of the initial period of war, the worries of Russian cyber planners, and Russia's view of the information-technical and information-psychological confrontation between or among adversaries. A short discussion of a cyber "dead-hand" and cyber's use to conduct reflexive control operations is included.

Chapter Eight, "Electrons, Underwater Cables, Satellites, and Creative Thought: The Russian Military's Invisible Information Environment," examines specific elements of the information domain that are often invisible and thus extremely hard to predict with confidence. No one really knows the intent of an electron except the executor of the action which may be an adversary or a surrogate; it is hard to know if satellites and underwater cables are being monitored and in what ways; and it is of course impossible to know what military thought is driving decision-makers in Russia in peacetime and wartime in an age of hypersonic speeds.

Chapter Nine, "Russia's Military Discusses the Definition of War," looks at several discussions that took place in 2017 and two follow-on discussions, one in 2018 and one in 2019. The focus was on the impact of nonmilitary capabilities and whether they might be considered as an act of war; or whether only military actions can result in war. The 2017 discussion lasted from January through the summer. In August, there was to have been a summation of the results of the discussion, but this summary has never been published. The Defense Ministry is thus playing this one close to the chest.

Chapter Ten, "Russian Forecasts of Future War," demonstrates how Russia will continue to periodically (one recommendation was every three to five months) update its forecasts of the potential for a war to occur. The changing nature of war, due to technological achievements in weaponry, new trends in warfare (artificial intelligence, quantum computing, etc.), and new ways that the initial period of war might unfold, is the motivator for these periodic updates.

Chapter Eleven, "Russian General Staff Chief Valery Gerasimov: Shaping Russia's Armed Forces and Military Thought," begins with a brief description of Gerasimov's military career and qualifications to be the Chief of the General Staff. It then focuses on two separate areas: interviews with him that appeared in the Russian press; and a focus on the seven detailed presentations he has made at the Academy of Military Science from 2013-2019.

Chapter Twelve, "Conclusions," wraps up the discussion with a list of thought priorities and vectors used in Russia's military establishment. The analysis ends with a short comparison of Russian military thought juxtaposed against that used by the Kremlin leadership. The results are surprising and imply several cultural biases that exist in Russia that negotiators will need to take into consideration when dealing with either the President of Russia or the members of the Defense Ministry.

To summarize, the analysis that follows will demonstrate that the Russian thought process is a complex mixture of vision, deception, deterrence, outright power, innovative thought, preparation, and the development of alternate realities. Vision and foresight heavily influence Russia's focus on ensuring superiority in the initial period of war. Deception includes reflexive control operations and deterrence measures accomplished through legal, information, demonstration, or other means to contain or scare opponents. Power is found in Russia's military-industrial complex, which produces nuclear and nonstrategic nuclear forces, weapons based on new physical principles, and the capabilities to strike deep into the heart of another nation with cyber capabilities. Innovation is most apparent in new applications of military art and the use of disorganization of an opponent's information and C2 capabilities. Preparation is influenced by the Soviet past and Russian presence, from methods passed down through the years such as the importance of the initial period of war to today's lessons learned from observing foreign armies in action or from their own experiences. Alternate realities and the rewriting of history provide certain rationales for specific situations.

This page intentionally left blank.

2 Russian Military Thought: Building on the Past to Win Future Hi-Tech Conflicts

> Knowing the adversary to perfection, assessing his action plan correctly, estimating precisely his forces, assets, and potential are among the major conditions that influence the success of an engagement, operation, or battle.[1]

Introduction

Military thought in Russia and elsewhere is changing and advancing rapidly due to numerous technological achievements. This has resulted in older concepts being reorganized, updated, or even discarded. Cyber issues have increased strategy's reach to attain a global scale. Unmanned aerial vehicles (UAVs) and a satellite's reconnaissance capabilities have affected the speed and influence of operational decisions. Disorganizing an opponent's command and control facilities is now possible with advancements in electronic warfare. Tactical actions now can have strategic impact in the age of instant media relations. Technology no longer just influences tactics, as Engels proposed. It now influences strategy.

One of the ways to know an adversary better is to study both how he thinks and how he includes technological changes into his military art and decision-making processes. Several aspects of Russia's military thought process are discussed below, resulting in the sharpening of one's view on the topic. Soviet and Russian military theoreticians have a reputation for creative thought, having developed numerous innovative concepts over the years. Several commanders' concepts that come immediately to mind are the deliberations of Aleksandr Svechin on strategy, Georgii Isserson on operational art, and Makhmut Gareyev on the operational maneuver group, among many others. New concepts are under study today.

As the character of conflict and potential for war has changed, educational and professional instruction in Russia has followed suit. Commanders and professors teach subordinates how to operate independently, take the initiative in combat, and develop new and creative applications of military art. Due to high-tech developments in artificial intelligence, quantum computing, and other areas, Russian leaders are continually updating their views on emerging trends in warfare. Now they make new forecasts of future war every four to six months due to the introduction of new technologies. Trends and forecasting, along with contemporary requests for the development of new forms and methods of conflict for many branches of service, indicate that the basic concepts of past thought remain relevant today, since they are repeatedly revisited.

It is important to tap into Russia's rich historical and contemporary thought processes to better understand Russia's military developments—and improve our own. First, Soviet and Russian military thought are compared in this chapter, and the similarities are intriguing. Second, two Soviet books are examined. One is on Soviet military thought from 1914-1941, written in 1980 and the other is on the culture of Soviet military thought, written in 1991. Several of these concepts still affect thought today. Third, a synopsis of military thought from 2007 to the present is offered, with a key warning from several prominent commanders to avoid stereotyping. These perspectives include lessons learned from Chechnya, Ukraine, and Syria as well as the lessons commanders have learned from watching foreign armies.

---

[1] A. M. Goncharov, V. N. Dybov, and Yu. D. Podgornykh, "Actual Aspects of Situational Assessment," *Voennaya Mysl' (Military Thought)*, No. 2 2017, p. 34.

Basic elements of historical military thought are now mixed with and updated by technology's new developments. Past concepts such as annihilation, attrition, and maneuver are all dramatically affected today by the power and speed that technology has brought to the table. Innovation, creativity, risk-taking, and other parameters of thought are vastly different in scope and scale due to their immediate consequences when affected by technology. These traits were present in Soviet times but were not a focal point for Western analysts. For example, one Soviet-era author noted regarding risk-taking that it "could be said that this is the highest manifestation of a commander's military skill, experience, endurance, and ability to anticipate."[2] Western analysts at the time did not appear to center attention on this Soviet concept. Today, how Russia is accommodating such traits with technological changes is where the important forecasts of military actions lie.

The Soviet Past Influences the Present

Before examining two books on Soviet military thought, it is worth noting that there are trends that have carried over from the Soviet to the Russian way of configuring and handling threats and thought:

- In Soviet times, the leadership expressed concern over capitalist encirclement. Today its leaders fear North Atlantic Treaty Organization (NATO) encirclement.
- In Soviet times there was a tremendous study underway that considered how to take advantage of the initial period of war (IPW), where mobilization priorities were examined along with deployment schedules. Today the IPW is focused on the potential insertion of viruses into an adversary's infrastructure in peacetime which can serve as an "on-call" capability if war erupts. The goal will be to destroy the state control facilities of an adversary.
- In Soviet times mobilization issues were a key takeaway from World War II's lessons learned, since the Union of Soviet Socialist Republics (USSR) was unprepared for war's beginning. In a 2016 article devoted to the Kavkaz-2016 exercise, General Staff Chief Valery Gerasimov noted that optimizing mobilization issues remains crucially important. The Kavkaz exercise included the mobilization of the military-industrial complex and numerous administrative offices in the region.[3] In 2018 Defense Minister Shoygu opened an operational-mobilization leadership conference.[4] A mobilization focus further increases Russia's preparations for the IPW.
- In Soviet times, there were studies of deep strikes that included ways to use aviation and special forces to strike deep into an opponent's territory and strike at command posts. Today such cyber deep strikes can potentially disrupt or destroy stock markets while hypersonic weaponry is designed to strike capitals on the other side of the globe. Technology is causing thought to move forward at hyper speed.
- In Soviet times there were political officers. In 2018 the Defense Ministry developed a Main Military-Political Directorate to handle the moral and psychological stability of servicemen.

---

[2] F. F. Gaivoronsky and M. I. Galkin, *The Culture of Military Thought*, Moscow: Voennoye Izdatelstvo, 1991, p. 19.
[3] Aleksandr Tikhonov, "In the Southwest Sector," *Krasnaya Zvezda (Red Star)* Online, 16 September 2016.
[4] See, for example, "Russian Federation Defense Minister Sergey Shoygu Opened Russian Federation Armed Forces Operational-Mobilization Leadership Conference," *Ministry of Defense of the Russian Federation*, 12 February 2019.

- In Soviet times there were exhibitions of World War II trophy weapons, designed to foster patriotism, that crossed the country. This tradition has been reinstituted with a Syrian trophy train that has been touring Russia since 23 February with plans to visit 60 cities. Military bands, song and dance ensembles, and a field kitchen accompany the train, as well as mobile recruitment posts for contract service.[5]
- In Soviet times, the economy was an appendage of ideology. In a 2018 report it was stated that patriotism is the main reason for adopting decisions in the sphere of economic development. Economic projects "show off a bridge or missile, or pipeline, and in passing employ people to create them, provide work for manufacturing plants, and so forth" which ultimately "serve the purposes of patriotic propaganda."[6]

In addition, several prominent Russian journalists have noted that the Soviet experience is being repeated. Russian journalist Pavel Felgengauer offered the following statement about the Soviet and now Russian experience in the Middle East:

> The present return to the Middle East is increasingly akin to a repetition of the Soviet experience of 30-40 years ago: the confrontation with America, which has already entirely officially been renamed from 'partner' to 'probable adversary'; the growing costs and uncompensated supplies of arms, equipment and apparatus to Syria, Egypt, Libya, and Lebanon. The capital investments in the development of useless overseas bases. The loss of life and losses of equipment; and the most displeasing—local allies, who, as in the past, are dragging our country increasingly deeply into endless, pointless, and bloody quarrels.[7]

Well-known journalist Aleksandr Golts offered a similarity with the Soviet period from a different perspective. He wrote in 2019 that the Defense Ministry is drawing a closer link between the military and civilian enterprises, since new developments (drones, cyber, artificial intelligence, social networks, etc.) influence both. There is also a constant requirement to foster patriotism, as in Soviet days, and an emphasis on mobilization potential.

Golts claims that the military-civilian relationship has been a constant in the minds of Russian citizens for a few centuries based on the nation's history. He wrote that the "militarization of Russian minds" is a process that strongly influences modern leaders and it is based on old Russian and Soviet era thinking. Golts wrote that Nicholas I purportedly wrote in the margins of a geography textbook that Russia is a military state and its purpose is to menace the rest of the world; that Alexander III believed Russia's only friends are the army and navy; and that Russian political philosopher Petr Struve wrote that the army is the living embodiment of Russian statehood. Golts's point is that the military component of statehood has always influenced Russia's national consciousness in many ways. Militarism has been a way of state building that Putin has adopted, as it helps legitimize his regime and his system for governing Russia and elevates his global influence.[8]

---

[5] Vladimir Ruvinskiy, "Trophies of a New War. Exhibition of Trophy Arms from Syria Looks Not Like a Continuation of Soviet Tradition but Like a Simulacrum," *Vedomosti (Bulletin)*, 28 February 2019.
[6] Vitaliy Shklyarov, "Business Soviet-Style. How Patriotism is Taking control of the Economy," *Novaya Gazeta (New Newspaper) Online*, 17 June 2018.
[7] Pavel Felgengauer, "'Above the Arabian Peaceful Hut.' Israel Could Once Again Become the Adversary," *Novaya Gazeta (New Newspaper) Online*, 24 January 2019.
[8] Alexandr Golts blog post, "Why Militarization of Russian Minds Happens and Why It Is Dangerous," *Ekho Moskvy (Echo Moscow) Online*, 19 February 2019.

Another 2019 article noted that President Putin's preoccupation is not with domestic or economic affairs but rather with foreign policy and defense building. He has shaped a Russian corporate identity with the security services at the helm, resulting in their production of conspiracy theories and a desire for control, like the Soviet period. Finally, it was noted that Russian strategic culture is shaped by the recognition of post-Soviet territory as a sphere of Russian influence, with Ukraine and Belarus as important territorial buffers against Western influence. Soviet and now Russian strategic patience indicates the Kremlin is waiting for a window of opportunity to take advantage of these issues.[9]

Two Important Books on Military Thought

This section discusses two books of interest about Soviet military thought. They are I. A. Korotkov's 1980 *History of Soviet Military Thought*, which covered Soviet thought from 1914-1941 and the 1991 work of editors F. F. Gaivoronsky and M. I. Galkin titled *The Culture of Military Thought*. The latter covers much of the period in the few decades before the fall of the Soviet Union. Both offer interesting insights into the thought patterns of two major periods in Soviet history. Some of their main points of emphasis still influence Russian military thought today.

Korotkov

Korotkov's work consisted of six chapters. They covered Marxist-Leninist theory; the preparation of a Soviet military-scientific cadre; the struggle for the confirmation of Marxist-Leninist theory as a military branch; lessons from war's experiences; basic problems of military art; and the theory of military economics.[10]

Korotkov stated that he had limited his book to researching both the origin of problems associated with military theory and a determination of the nature of a possible war and its initial phase. New weapons and the impact of shifting to a war economy for future operations were also discussed. He stated that **the goal of military thought is to uncover the nature of future struggle and its direction at every period of development.**[11] He listed as important sources for understanding military thought the speeches of political and military figures on war and military affairs. Korotkov noted that Lenin had cautioned against using arbitrarily chosen facts to create "subjective" concoctions. He added that Lenin had underscored the importance of studying context as well, stating that theory must take into account "the relationship of an epoch to a given war."[12]

Strategic plans must correspond to objective conditions of a struggle, and they must be flexible, since even defeats must be endured and studied. A retreat can win time[13] and offer another opportunity for success. Soviet military thought in the 1920s began to develop the theory for organizing and conducting deep operations.[14] This continues today with Russia's focus on using cyber operations to attack deep into an opponent's territory.

Korotkov notes that M. V. Frunze wrote during the 1920s that military doctrine's goal is to reveal the nature of military confrontation and determine whether passive defense or active offensive

---

[9] Valeriy Solovey, "'What Are They Doing?!' How the Thinking of Russia's Ruling Elite Is Organized," *Republic*, 25 February 2019.
[10] I. A. Korotkov, *The History of Soviet Military Thought*, 1980, pp. 3-4. The translation of Chapters 1-3 of this work are the product of Francis J. Sullivan's 1983 Student Research Report at the US Army Russian Institute, Garmisch Germany. However, actual pages in Korotkov's book are cited for reference purposes.
[11] Ibid., pp. 9, 11.
[12] Ibid., p. 15, 21.
[13] Ibid., p. 26.
[14] Ibid., p. 28.

operations are required. Doctrine indicated the system of training required and the system for preparing the country's security.[15] Frunze listed the tasks for developing the theoretical foundations of military doctrine in the following way:

> To study the nature of the social environment that surrounds us, to define the nature and essence of military tasks that stem from the essence of the state itself; the study of those conditions which guarantee their fulfillment not only in relation to material prerequisites but spiritual ones as well; the study of the peculiarities of building up the Red Army and the methods of struggle that are applied in it; agreement between the demands of military science and art of those peculiarities that are objectively and inseparably connected with the nature of our proletarian state and the revolutionary epoch which we have experienced.[16]

Military theory's conclusions are used to build up the military via military doctrine, that is, the officially accepted views of military and Kremlin officials.[17] It was noted that:

> Politics, without a doubt, plays the deciding role in determining the means and methods of conducting war, but we must also direct our attention to the internal logic of the development of military technology in order to correctly define in the future the general tendencies of military affairs. Taking into account the changes in the means and methods of struggle, politics then defines their direction and possible use in war.[18]

Korotkov's chapter on military art was of interest. It covered the social-political character of future war, war's strategic concept and the content of the initial period of war, questions on the theory of operational art and tactics, and the character of the future use of the various branches of the armed forces. Many of the thoughts he uncovered are in use today in the political-military speeches of President Putin.

In Korotkov's section on strategy, he stated that an incorrect determination of war's future scale will adversely affect how a nation conducts it. Everything an armed force requires must be provided when war appears imminent. A reliable estimate of the war's scale and duration are needed.[19]

In the early 1920s, the reliable estimate in use appeared to predict a war of attrition and not one of lightning strikes and annihilation. However, the point was debated, even at the Frunze Military Academy in 1926. K. D. Golubev believed in a strategy of annihilation and B. B. Kasani believed in a strategy of attrition. Other analysts contributed to the discussion. Svechin's *Strategy* focused mainly on annihilation, and he believed annihilation would lead to faster political goals and the use of fewer resources. His theory was predicated on the existence of four things: that military preparations for conflict were available; that there were good lines of communication; that there was a superiority in forces; and that the enemy state appeared politically weak.[20]

Other theorists supported the thought of annihilation as well. It was noted that "the best strategic defense was a swift offense into the depth of an enemy country, turning foreign territory into a theater of military operations."[21] Attacks ensured that the initiative and surprise were in friendly hands, which a defensive posture could not produce. Frunze, while in favor of annihilation, did not

---

[15] Ibid., p. 60.
[16] Ibid., p. 66.
[17] Ibid., p. 67.
[18] Ibid., p. 90-91.
[19] Ibid., pp. 120-123. The translation of the rest of this section on Korotkov's book was provided by Dr. Harry Orenstein.
[20] Ibid.
[21] Ibid., p. 123.

discard attrition, noting that idealizing conclusions was the wrong approach to take. He believed there are times when withdrawal may be necessary to prepare for a new offensive. Thus, the idea was to remain flexible[22] and, perhaps more like the thoughts of Svechin, take into consideration that each situation may have a logic all its own.

Lenin wrote that all forms of struggle should be used, especially swift and unexpected changes in an operation's form. He also stated that he preferred the offensive and that pauses in such operations had to be expected. Frunze emphasized that maneuver was preferable over positional forms of military operations. He considered the latter as an exception and not a main form of operations.[23]

Writing on the initial period of war, Korotkov noted that the mobilization period and the massing and strategic deployment of the main forces were indicators of war's preparation. The political and economic situation in a country along with geographic and other factors help determine the tempo of the deployment. He added that whichever force could accomplish these goals in the shortest time period would achieve strategic superiority.[24]

Gaivoronsky and Galkin

Gaivoronsky and Galkin's book covered numerous topics. The work's 16 chapter titles are listed below. They offer their own insight into the elements that made up Soviet military thought in 1991. Many of these topics probably influence Russian military thought today. They are:

PART ONE: The Essence and Distinctive Features of Military Thought

1. Military Thought: The Specific Nature of Cognition
2. The Interrelation of Thinking and Language
3. The Creative Nature of Thought
4. Military-Theoretical Thought
5. Military-Practical Thought

PART TWO: The Methodology, Logic, and Methods of Military Thought

1. World View and the Methodology of Military Thought
2. The Dialectic of Military Thought
3. The Formal and Logical Bases of Thought
4. Methods of Cognition of Military Phenomenon
5. The Systemology of Military Thought
6. Mathematical Modeling and Scientific Thought

PART THREE: The Perfection of the Culture of Thought

1. The Stimuli of Creative Thought
2. The Teaching Process in Institutes
3. The Rational Organization of Combat Preparations, Learning
4. War's Experiences, the Patterns (Rules) of the Development of Military Affairs
5. The Culture of Military Thought and Style of Work
6. Conclusions

[22] Ibid., pp. 123-125.
[23] Ibid., pp. 126-127.
[24] Ibid., pp. 129-130.

Only chapters one, three, seven, and eight are discussed below. What is interesting is the focus on creative thought and risk-taking, which are also stressed today.

In Chapter One the authors write that thought is the product of the interaction of objective (surrounding reality) and subjective (knowledge and a thinking person's attitude to it) processes. The latter is affected by technology, since battle is perceived as a complex, organized process where speed in recognizing a situation is more important than it was before. This is due to combat systems that rely on precision and rapid response.[25]

It is necessary to know not only one's forces, the authors write, but also those of an adversary, otherwise there is no way to understand how to efficiently use one's weapons or offer operational goals that ensure success. Operations require daring creative thought as one side tries to disorganize the other and impose its will while preserving friendly forces and command and control capabilities.[26]

Risk-taking is an important element of military thought and it "**could be said that this is the highest manifestation of a commander's military skill, experience, endurance, and ability to anticipate**."[27] It must be based on reasonable caution and a "profound knowledge of the nature of the battle" and the conditions of the adversary. The greatest risk can be inactivity. A commander must examine objective facts and consider them as constantly changing and developing. Contradictions must be unearthed, and commanders must have the ability to creatively apply their knowledge of theory to real situations.[28]

In Chapter Three, "The Creative Nature of Thought," it was noted that military art is where creative thinking fuses with practical activities. Creativity offers something qualitatively or quantitatively new and previously nonexistent. It is novel and original, procuring new knowledge outside the framework of existing ideas (these actions also contain some risk, the authors note). The creative process is a synthesis of cognition, emotions, and knowledge that can produce an epiphany.[29] Knowledge is the prerequisite of creativity while inspiration and enthusiasm motivate its discovery.[30] Other attributes of an officer who possesses creativity are: receptivity to new ideas; overcoming conservatism and inertia with independent judgement; a critical and daring nature; tenacity and persistence; and intuition.[31] The latter usually is described as the immediacy of result with no real logical reasoning or rationale, just discovery.[32] Finally, there is premonition, the advanced reflection of reality or the potential for foresight. Premonition can be based on a cause-effect link among the past, present, and future.[33]

In Chapter Seven, "The Dialectic of Military Thinking," it was noted that there is a difference between objective and subjective factors because the former does not depend on the will and desire of humans. The latter is determined by them. The cognition process is affected by both factors, as the following example demonstrates:

> When developing a plan for a forthcoming battle, the commander and his staff highlight the objective circumstances affecting its outcome, including the correlation of forces, both

---

[25] F. F. Gaivoronsky and M. I. Galkin, *The Culture of Military Thought*, Moscow: Voennoye Izdatelstvo, 1991, pp. 9, 12-13.
[26] Ibid., p. 15.
[27] Ibid., p. 19.
[28] Ibid., pp. 19-20.
[29] Ibid., pp. 34, 36-37.
[30] Ibid., pp. 43-44.
[31] Ibid., p. 45.
[32] Ibid., p. 47.
[33] Ibid., p. 81.

> qualitative and quantitative, terrain conditions, weather, and so on. Nevertheless, occasions are not uncommon where even the most favorable circumstances are not taken advantage of and the mission is not accomplished because of actions with subjective causes: an inadequately thought-out decision, erroneous instructions during combat operations, and so on.[34]

The authors state that it is important to continually follow the thoughts of an adversary and to highlight any changes in their tendencies or other aspects of organizing their forces. An opponent's military art, like that of friendly forces, depends on his level of knowledge, intellect, and other qualities, to include his battle experience and lessons learned. The authors add that "what is true in military knowledge is what has been confirmed by the totality of practical military experience."[35] The task for officers lies not in using stereotypes or ossified ways of thinking or "minted coins," the latter being something ready-made. The task is to extract something different or create something new.[36]

In Chapter Eight, "The Formal and Logical Bases of Thought," a definition of formal logic was offered. It was said to be a science about the laws of correct thought and the demands made of consistent and evidentiary discourse. Numerous laws of logic were then offered. They were:

- The law of unity was said to reflect the relative stability and distinctiveness of objects and the phenomena of reality.
- The law of contradiction's essence is to prevent logical contradictions during discourse.
- The law of the excluded middle aims to exclude contradictions in thought about the same object taken at the same time and in the same relation.
- The law of sufficient grounds is that any correct (and objectively true) idea must be reasoned and based on sufficient grounds.

The authors added that the main form of an indirect thought is an inference, and there are three types: induction (particular to general), deduction (general to particular), and analogy (particular to particular).[37]

A final discussion in the chapter was on the balance of forces in combat. It was noted that to ensure victory, calculating possible changes in a balance of forces during military operations is important as well as determining ways to create or maintain them. Victory may, however, not go to the stronger side if superiority is achieved by an adversary on the main direction or through surprise or the use of a combat method that was unexpected. Further, foresight can help attain victory if it is able to objectively analyze the present and use important lessons from the past, thereby providing a quantitative and qualitative prognosis of the probability of an event.[38]

Modern Times

Much of the content of Soviet and Russian thought has carried over to today. Subordinates are taught to be creative, innovative, and risk-taking. Examples are provided later below from major

[34] Ibid., p. 105.
[35] Ibid., p. 119.
[36] Ibid., p. 120.
[37] Ibid., pp. 123-127, 134-137.
[38] Ibid., pp. 253-254.

contemporary leaders of Russia's military that highlight these consistencies. However, other specific elements of thought have appeared as well.

For this author, a methodology of Russian thought has developed that might be considered the "five factors" for attaining at least a partial understanding of how to piece together Russian thought. These factors are the trends, forecasts, strategy, forms and methods, and operational design of Russian thought. Initially, trends in military developments and warfare are discussed, which help forecasters predict what a future war might look like. Once this picture is developed, a strategy is orchestrated to achieve successful results in a future conflict based in a particular region of the world. When revolutionary changes occur in situational analysis or due to technological enhancements that might affect warfare everywhere, new military doctrine (the equivalent to US military policy) may be developed (the last doctrinal change in open source writing occurred in 2014). Next, leaders require that theorists develop the proper forms and methods to conduct the conflict. Various branches of service require different forms and methods. An operational design is then constructed to carry out the plan on specific strategic or operational axes. New ways of employing military art are encouraged, that is, new ways to employ weaponry or forces (to view a detailed discussion of this methodology.[39]

Other more recent discussions of military thought are often associated with military art. General of the Army Makhmut Gareyev, President of the Academy of Military Science in Moscow, offered an example of new thinking in military art in 2017 in the journal *Military Thought*. His analysis was noteworthy for its focus on the creative use of knowledge and its combination with many of the items (trends, forecasting, etc.) listed above.

Gareyev began by recounting two important lessons he learned in fighting in WWII—the need for reconnaissance and fire destruction. Russia's current focus on the development of UAVs and reconnaissance-fire and -strike complexes fit this requirement. Ground troops and other branches of service are important but not as important as the two lessons from WWII in Gareyev's opinion.[40]

To train for future wars, Gareyev recommends focusing on operational-tactical tasks, teaching or developing creativity, and directing methods of organizational (form) work. While military art contains several long-lasting principles and tenets (surprise, mass, etc.), new ones are required due to new technological achievements. He adds that it is not just experience from the past that informs military art but also "those underlying sometimes hidden sustainable processes and phenomena that have a tendency for further development."[41] He defined military art in the following manner:

> Military art begins where, on the one hand, profound theoretical knowledge and its creative employment help a commander to better see the overall relationship of phenomena that have occurred and to more confidently orient himself to the situation; and, on the other hand, the commander, without fettering himself by a general theoretical plan, attempts to penetrate more deeply into the essence of the situation that has actually developed, grasp its advantageous and disadvantageous features, and, proceeding from their analysis, find original solutions and methods of action that are, to the greatest degree, appropriate with respect to the specific conditions and assigned combat mission.[42]

---

[39] For an extended discussion of trends, forecasting, strategy, and forms and methods, see Timothy Thomas, "Thinking Like a Russian Officer," Foreign Military Studies Office, Fort Leavenworth, Kansas, website.
[40] M. A. Gareyev, "On the Development of Qualities and Skills in Officers Necessary for Demonstrating a High Level of Military Art," *Voennaya Mysl'* (*Military Thought)*, No. 12 2017, pp. 72-73.
[41] Ibid., p. 73.
[42] Ibid., pp. 73-74.

Gareyev noted that military art's essence is determined by the relationship between objective and subjective factors observed and developed by the commander. The fundamental law of military art is that "the greatest enemy of military art is templating and schematism."[43] Peacetime is when educational institutes must train officers to take the initiative and learn to work independently. This is also when it is necessary to examine and foresee whether changes in the nature of armed conflict had occurred and if new requirements have been made on command and control systems.[44] He ended his article noting that it is improper to copy the standards of other armies, but it is acceptable to learn what worked and what did not work for them. He stated that the closer integration of nonmilitary means and forms of confrontation with military ones must be considered more thoroughly.[45] The following section indicates that Gareyev's opinion matches that of most Russian officers at this time.

Military Leaders and Educational Institutes on Officer Training

This section follows, in temporal order, some of the articles in Russian journals on military thought. Many adhere to the same principles established years earlier in the Soviet period.

In 2007, in the journal *Military Thought*, an article was published under the title "The Way Military Leaders Think: Looking into the Past." It recounted some of the thoughts of famous leaders from Napoleon to Clausewitz to Moltke, among many others. At the end of the article author A. V. Lebedev listed criteria and intellectual qualities that form, from his perspective, the bedrock of intellectual thought. Thus, while not purely Russian thinking, the list is indicative of the types of issues Russian theorists are considering. They are:

- The use of spatial and temporal considerations
- The use of caution and sustained thought (when under threat, limited time, etc.)
- The ability to analyze and synthesize and carry out systemic analysis
- The ability to generate creative thought and to forecast
- The use of logical thought and independent thinking
- The selective power of observation
- Critical and flexible thought
- And a rational specification or ability to plan actions[46]

This, Lebedev noted, was not an exhaustive list but one for constructive discussion.[47]

There have been several important discussions of creative thought over the years, most likely because it is a main contributing factor to the further development of military art. In 2009, for example, N. M. Ilyichev wrote on "Certain Specificities of the Formation of Creative Thinking in the Process of Military Training" in *Military Thought*. Creative thinking in military matters, he noted, is aimed at the development and introduction of new methods and forms of armed struggle and the effective use of military hardware and equipment, among other issues. Ilyichev stated that the creative process involves the emergence of a problem; a search for an idea to resolve it; the elaboration and proof of the idea; its concretization; and its practical implementation. The main

[43] Ibid., p. 74.
[44] Ibid., p. 75.
[45] Ibid., p. 76.
[46] A. V. Lebedev, "The Way Military Leaders Think: Looking into the Past," *Voennaya Mysl'* (*Military Thought)*, Volume 3 2007, in English, downloaded from https://www.opensource.gov on 27 March 2014.
[47] Ibid.

idea involves various forms and methods of cognition, to include intuition, which is an original leap in grasping the essence of the subject so long as it does not have an algorithmic method of investigation. Intuition is distinguished not only by spontaneity and free thinking but also using previous knowledge and, in some cases, analogies. Finally, it was noted that teachers must adhere to the demands of dialectical and formal logic.[48] Thus, many of the points covered in the two Soviet era books are included in this article, some 20 or more years later.

A 2012 article on creative thought appeared in the military newspaper *Red Star*. It stressed the need for learning how to become more creative in order to overcome the dominance of "reproductive" methods of thought, where learning took place according to patterns. It was noted that he who memorizes and simply reproduces is not acquiring creative development. Creative thought does not come from simply repeating arguments made by someone else. The article concludes that problem-based methods are the basis for learning creativity, a way for military school graduates to develop creative thought.[49]

In another 2012 report, this time on the military-controlled *Star TV* in honor of the 180th birthday of the Russian General Staff Academy, it was stated that military economics, strategy, and global political change are taught at the academy. The Integratisya geo-informational system is used to play out combat scenarios on a vast geographic scale in support of learning how to make decisions in real-time. General Staff Chief Valery Gerasimov noted that the academy teaches inter-service and interdepartmental training as well.[50]

A 2018 report stated that the General Staff Academy researches the following: tasks involving threat prediction for the coming 30-50 years; lessons learned in Syria; the feasibility of strategic deterrence; the prediction of the nature of conflicts of various scales; and effective means of using weapons systems based on new physical principles. Command and control issues, the use of forces in new theaters of military operations, and the development of future forms and methods of operational training were also covered.[51] Thus, officers attending the academy are taught a great deal about major issues affecting military thought.

General Staff Chief Valery Gerasimov has focused on officer training in several of his interviews with the press. In 2016 he stated, "We cannot operate in stereotyped fashion. We need to seek atypical solution options which result in the achievement of the set goal."[52] In a 2017 presentation he stated the following:

> Special attention in training military command and control entities is given to introducing foremost methodologies and experience of employing troops (forces) in modern armed conflicts and to developing the ability of commanding generals and commanders to quickly estimate the situation; anticipate its development; make unconventional decisions, employ methods of operations and stratagem

[48] N. M. Ilyichev, "Certain Specificities of the Formation of Creative Thinking in the Process of Military Training," *Military Thought* in English, Volume 3 2009, downloaded from https://www.opensource.gov, accessed on 4 August 2017.
[49] V. Volodin, "Learning Creativity," *Krasnaya Zvezda* (*Red Star)*, 26 September 2012, p. 3.
[50] No author provided, "News of the Day," *Zvezda TV*, 8 December 2012.
[51] Dmitriy Semenov interview with Aleksey Kim, "Priority Given to Syrian Experience. At the General Staff Military Academy Emphasis in the Teaching Process Is Placed on Experience Gained while Performing Assignments in Syria," *Krasnaya Zvezda (Red Star)* Online, 6 July 2018.
[52] Aleksandr Tikhonov, "In the Southwest Sector," *Krasnaya Zvezda (Red Star)* Online, 16 September 2016.

> unexpected by the enemy, function actively and purposefully, achieve surprise, take a substantiated risk, and seize and hold the initiative.[53]

Later in the same article he stated that combat operations in Syria had educated personnel under difficult conditions. This helps instill in them "such qualities as an aggressive spirit, initiative, boldness, decisiveness, readiness to take a risk, staunchness, endurance, and the ability to overcome any difficulties"[54] when faced with new situations.

During his 2018 presentation at the Academy of Military Science, Gerasimov noted that contemporary military operations are demanding new training techniques. He stated that "special attention is being focused on the development of skills for a commander to make rapid and completely justified actions. Skills for making nonstandard decisions are being developed."[55] These skills include forecasting the situation, acting decisively, and being prepared to take a justified risk. Most of the requirements were conditioned by Russian experiences in Syria.[56]

In another interview related to Syria, General-Lieutenant Mikhail Matveyevskiy, Chief of Russia's Ground Force Missile Troops and Artillery, stated that the Syrian experience had changed training for artillerymen. Now, "on all tactical drills and exercises we create a situation that requires initiative, military cunning, perseverance, and persistence to be displayed."[57]

Another report stated that the General Staff had developed a code of conduct for commanders. It describes what an officer's appearance should be and how he or she should speak to subordinates about their tasks. A "special section is devoted to information technology and security discipline," with cell phones receiving special monitoring and social networks declared "taboo." The code has Gerasimov's ratification, but it is only of a "recommended" nature. However, the code's observance will be part of an officer's evaluation report.[58] Jackets and t-shirts with slogans in foreign languages and flags of other nations are deemed as inappropriate.[59] The code and regulations may affect military thought in other ways.

Service to the nation and other leadership attributes are part of 21st century military thought. A few days before 9 September 2018, which is Tank Day in Russia's Armed Forces, the military paper *Red Star* interviewed the deputy head of the Kazan Red Banner Higher Tank Command School, Colonel Aleksandr Sukhikh. He stated that the qualities of a tank officer include professionalism, independence, determination, initiative in battle, courage and bravery, dedication, and willingness to sacrifice oneself for the sake of victory. Sukhikh added that the most important issue is a deep sense of camaraderie, fairness, and respect for subordinates. [60]

---

[53] V. V. Gerasimov, "On Implementing the Executive Orders of the President of the Russian Federation of 7 May 2012, No. 603 and 604, and the Development of the Armed Forces of the Russian Federation," *Voennaya Mysl'* (*Military Thought)*, No. 12 2017, p. 15.
[54] Ibid., p. 19.
[55] Valery Gerasimov, "The Influence of the Contemporary Nature of Armed Struggle on the Focus of the Construction and Development of the Armed Forces of the Russian Federation. Priority Tasks of Military Science in Safeguarding the Country's Defense," *Vestnik Akademii Voennyh Nauk (Journal of the Academy of Military Sciences)*, No. 2 2018, p. 20.
[56] Ibid.
[57] Aleksey Ramm and Aleksey Kozachenko, interview with Mikhail Matveyevskiy, "Fire Barrage: How Russian Artillery is Being Reequipped," *Izvestiya (News) Online*, 19 November 2018.
[58] Aleksandr Kruglov, Nikolay Surkov, and Aleksey Ramm, "Army. Taboo on Social Networks Has Been Included in the Code. Detailed Collection of Rules of Conduct Drawn Up for Commanders," *Izvestiya (News) Online*, 28 February 2018.
[59] Ibid.
[60] Aleksandr Tikhonov, "A Fusion of Knowledge, Will, and Armor; It is Formed at Renowned Military School; 9 September is Tank Troops Day," *Krasnaya Zvezda (Red Star) Online*, 7 September 2018.

The Chief of the Mikhaylovskaya Military Artillery Academy, General Lieutenant Sergey Bakaneyev, stated that a statistical-probability style of thinking is needed among artillery officers. This type of thought is "most effective for decision-making under conditions of a fast-changing situation: it is a question of predicting a situation's development when it appears unpredictable."[61] This requires knowledge of mathematics, Makaneyev added.[62] Thus, military thought has special characteristics depending on the branch of service.

In 2018 the journal *Military Thought* celebrated its 100th anniversary in Russia. The journal continues to publish articles attempting to solve problems of military science and military art. These include articles dealing with geopolitics and security, Russia's vital interests, the nature of warfare and conflicts, strategic stability, information-technologies and automated systems of command and control, various branches of service, nuclear deterrence, and numerous other topics. While an unclassified edition is available for purchase, it is suspected that a classified version also exists.

The journal's tasks in the coming months of 2018 were deemed to be as follows:

- Participate in generalizing the practice of contemporary warfare (especially local wars and armed conflicts of varying intensity) regarding major issues of strategy and operational art, and defining the nature of future warfare;
- Highlight the methodology of military science, military art, military development, specialized branches of social, natural, and technical sciences that underly the military affairs of the state;
- Render science-and-information support for the main development trends in weapons and military hardware, military technological cooperation, and state programs of arms and military hardware;
- Generalize the experience of operational training of troops/forces, particularly operational-strategic exercises, in the interest of furthering military art and the development of new manuals;
- Cover the more important incidents in military history, especially the history of domestic and foreign military thought, and propagandize the heritage of domestic military theorists and outstanding army commanders and military leaders;
- Participate in generalizing the practice of moral and psychological training of the Armed Force's personnel, in solving the problems of military training and education, and of normative legal support of the activity of state military organizations;
- Cover issues of foreign army buildups, combat, and training experiences;
- Review domestic and foreign military theory literature.[63]

In addition, the editorial board plans to discuss new problems and encourages the participation of younger scholars.

Finally, in February 2019 a mock battle was reviewed in a district journal that focused on the use of a commander's intuition. Innovations and nonstandard decisions were employed instead of

[61] Anatoliy Stasovskiy and Aleksandr Drobyshevskiy, "It is Impossible to Imagine a System of Modern Education without a Reliance on the Principle of Surpassing Instruction," *Yezhenedelnik Zvezda (Weekly Star)*, 24 September 2018.
[62] Ibid.
[63] S. V. Rodikov, "The Journal *Military Thought* Is 100 Years Old," *Voennaya Mysl'* (*Military Thought)*, No. 5 2018, p. 16.

predictable routines. Intuition was in demand as much as military skills. It was noted by one participant that "We operate within an integrated reconnaissance and fire system" which allows for independently using forces and fires. The time between detecting a target and destroying has been reduced severalfold. A key factor in modern warfare is thus the speed of data-gathering and decision-making.[64]

Conclusions

There appears to be much in common with the way thought was developed and expressed in the Soviet period when compared to its Russian counterpart. This includes both general trends and specific processes. However, these general concepts are all affected by the technological achievements of the modern era, and herein lie major differences.

Of primary interest is the emphasis in Russia on its leaders developing creative and innovative thought; on learning when and how to take risks; and on the further development of military art. The academies, journals, and leaders have the nation oriented in the direction of advanced and independent thought. Several theorists, to include the Chief of the General Staff, have advocated for the elimination of stereotypical and "minted coin" thought, stressing the need to learn how to use intuition and knowledge together when confronting new situations. It is apparent that lessons learned in Syria are having a great impact on training methods, as they are stressed in most contemporary exercises.

Past concepts such as annihilation, attrition, and maneuver are all dramatically affected today by the power and speed that technology has brought to the table. All three appear to have some contemporary relevance. Annihilation could be linked to Gerasimov's 2018 statement that "the comprehensive destruction of the enemy has advanced to the foreground."[65] Attrition could be the nonmilitary propaganda and cyber-attacks designed to slowly erode a nation's national will. Maneuver could be Gerasimov's belief that operations now are continuous, dispersed, and simultaneous. He also stated that theaters of military operations are expanding their borders, which can imply a global or planetary scope; and that military and economic targets can be a significant distance from where operations are being conducted.[66]

Technology has offered a new impetus and immediacy to military thought. Today the IPW might last seconds if the correct cyber destruction of an opponent's infrastructure and command and control is possible. The immediate consequences of the use of technology are its impact on the speed of decision-making and the vast scale of territory to which such thinking can be applied, since it can now affect a spectrum from the strategic to the planetary. The potential speed of maneuver and destruction is where military thought today differs from its Soviet predecessors and where the most important lessons for Western analysts lie for consideration. Attrition, on the other hand, from a Russian perspective appears to be more associated with color revolutions or nonmilitary matters due to their slower impact.

Russian military thought and advancements in military art should be studied closely in the West. Without doing so, it will be even less capable of attaining the initial quote of this article:

---

[64] Natalya Borodina, "An Integrated Reconnaissance and Fire System Is a Lesson for All Participants," *Voyennyy Vestnik Yuga Rossii (Military Bulletin of the South of Russia)*, 11 February 2019.
[65] Gerasimov, "The Influence…," p. 22.
[66] Ibid., p. 18.

> Knowing the adversary to perfection, assessing his action plan correctly, estimating precisely his forces, assets, and potential are among the major conditions that influence the success of an engagement, operation, or battle.[67]

As General of the Army Makhmut Gareyev stated, Russia should not copy what other armies do, but should learn from their mistakes and successes.[68] Learning about Russian military thought can improve our own combat thought and capabilities and help us avoid stereotyping Russia with US concepts such as hybrid operations, C4ISR, and A2AD, among others. Analysts need to dive into real Russian thought templates.

[67] A. M. Goncharov, V. N. Dybov, and Yu. D. Podgornykh.
[68] Gareyev, p. 45.

This page intentionally left blank.

3 Russian Military Art and the Creative Employment of Knowledge

> The development of new types of weapons, practical experience gained in Syria and in various exercises, as well as an analysis of modern military conflicts have given impetus to the development of the theory of military art.[69]—General Staff Chief Valery Gerasimov, 2018

Introduction

Military art's traditional components, according to Russian military thought, are strategy, operational art, and tactics. Contemporary military technology is erasing some of these distinctions and creating new forms and methods of warfare in others. In 2015, during the fighting in Syria, there were reports of the potential use of the thermobaric Solntsepek flamethrower. It is capable of clearing a four-hectare area, which the author noted is like the detonation of a super-low yield nuclear munition.[70] That is, a flamethrower with strategic impact.

Russian Colonel (retired) Vladimir Denisov noted in December 2018 that there have only been two significant changes in military art over the years, those being the German blitzkrieg and Soviet deep strike concepts.[71] It is interesting that a cyber-attack contains both a blitzkrieg at the speed of electrons and a capability to conduct a deep strike into the infrastructure of an adversary anywhere on the globe. Technology thus has transformed Denisov's two most important changes in military art's history into one contemporary planetary operation. Distinctions are being erased.

Often less studied are Russian technological innovations that are having an impact on the forms and methods of warfare from a tactical point of view. This especially includes developments in the use of reconnaissance and electronic warfare assets that have made the battlefield more visible and controllable. Russian military art prizes the creative employment of knowledge and battlefield experiences from commanders and scientists that enable such developments. Conversation between them helps focus research priorities and encourages developments that provide the capabilities required to compete in contemporary conflict. Results of these conversations can sometimes be found in the media. For example, a 2014 claim indicated that robotic fish were under development, which act as a noiseless drone and are used in military reconnaissance and mine clearing missions.[72] In 2016 it was stated that Russia is developing a large-caliber sniper rifle that uses 23-mm bullets. It can purportedly disable enemy tanks and destroy armored vehicles. One platoon of 'mini-canons' will be planned in each motorized rile company of snipers. An Army infantry brigade has such a company.[73]

Further, new breakthroughs in the application of technologies can also theoretically change the correlation of forces (COF) on the battlefield. This may be the first time in history, for example, that an electronic warfare contingent, outfitted with the newest high-tech gear, can actually

---

[69] Valery Gerasimov, "Gerasimov Briefs Foreign Military Attaches," *Ministry of Defense of the Russian Federation*, 5 December 2018.
[70] Vladimir Mukhin, "Rebels in Syria Are Fleeing Thermobaric Weapons. Several Tactically Important Areas Have Been Liberated from the Islamic State," *Nezavisimaya Gazeta Online*, 19 October 2015.
[71] Vladimir Denisov, "We Have Given Our Adversary a 15-Year Advantage and We Cannot Win It Back," *Novaya Gazeta Online*, 2 December 2018.
[72] *Interfax* (in English), 19 January 2014.
[73] Aleksey Ramm, "Defense Ministry Orders Sniper 'Mini-Cannon': It Can Be Used to Smash a Tank Gun, Destroy a Caterpillar, and Shoot Off a Track," *Izvestiya Online*, 14 October 2016.

debilitate the frequency capabilities of an opponent and totally disorganize his command and control capability (C2). This would alter the COF as a result.

This chapter will first define military art from a Russian perspective and then offer technological developments from 2016-2019 that have introduced new innovations to the tactical battlefield. One is reminded of two Russian ideas that correspond to the importance of military art: that "thought is the first to enter battle"[74] and that Russia has learned "to fight with skill, not numbers."[75]

Definitions of Military Art

The Defense Ministry's *Military Encyclopedic Dictionary* defines military art as "the theory and practice of preparing for and conducting military operations…it consists of strategy, operational art, and tactics, which are closely interconnected."[76] It was noted that "historical and ethnic features, geographical conditions, and other factors"[77] also impact a nation's understanding and development of military art.

The idea of "preparing for and conducting military operations" is where technology is having its greatest impact. Russian officers understand military art as not just strategy, operational art, and tactics but how a commander skillfully employs his knowledge to achieve surprise over an opponent or to unleash an unconventional/unique operation. This is confirmed by another Russian definition of military art:

> Military art is a sphere of theoretical and practical activity that involves the ability to create knowledge, taking into consideration the specific conditions of a situation when preparing for and conducting military operations (combat), where, in addition to knowledge, developed creative thinking and high organizational and strong character qualities are necessary for the commander.[78]

The idea of creative thought has long been a criterion in Russian military thought. Russian strategist Aleksandr Svechin, for example, was summarized as follows years ago:

> The main content of *A History of Military Art*, according to Svechin, was changes in the forms and methods of warfare that occurred depending on the economic, political, and military-technological prerequisites. He saw the purpose of military art in providing a foundation of higher education, and military disciplines, as well as in assisting the development of independent thinking in commanders, their ability to create, and master the rapid evolution in military affairs.[79]

The creative use of technology is manifested not only in the realm of the commander but also in the thoughts of scientists at the military-industrial complex, where innovative solutions to problems drive the need to help servicemen. Russia's Advanced Research Foundation is home to many of these developments.

---

[74] V. D. Ryabchuk, "Problems of Military Science and Military Forecasting under Conditions of an Intellectual-Informational Confrontation," *Voennaya Mysl'* (*Military Thought)*, No. 5 2008, pp. 67-76.
[75] Interview with Franz Klintsevich, "Lessons Learned from Afghan War Contributed to Success of Russia's Campaign in Syria," *Interfax* (in English), 15 February 2019.
[76] *Voennyy Entsiklopedicheskiy Slovar' (Military Encyclopedic Dictionary*), Moscow Military Publishing House, 1986, p. 139.
[77] Ibid.
[78] Nikolaiy Nikolaevich Tyutyunnikov, *Military Thought in Terms and Definitions*, *Voennaya Mysl'* (*Military Thought)*, Volume 1 2018, p. 156.
[79] Kh. I. Saifetdinov, "Alexander Andreevich Svechin—Outstanding Military Thinker of the 20th Century," *Voennaya Mysl'* (*Military Thought)*, No. 8 2018, pp. 101-109.

The following discussion and listing of technological accomplishments/research highlights how the scientist and officer/soldier have interacted to produce creative applications of military art. Some of these exchanges are observable from Russian actions in Syria while others are more representative of the unique (indirect or asymmetrical, for example) applications of technology fitting the requirements of a situation at hand.

Weapons and Military Art: 2016-2019

For the past several years, new applications of technology have led to new developments in military art. Many of these advances are related to how various types of weaponry are employed in accordance with contemporary trends. This has particularly applied to the use of drones/UAVs (or their counters) and to new developments in laser technologies. Here scientists are either responding to their discussions with soldiers for new and better equipment; or the scientists dream up new uses for weaponry as they consider their various properties and relate their suggestions to military authorities. Military theorists note that new tactical methods and the requirements of contemporary tactical art must be "based on the capabilities of the latest military equipment against the old methods of conducting battle, which have ceased to be appropriate for conditions that have developed."[80]

Trends have changed over the years and they are expressed in the lists that follow below. First, however, one is reminded of how trends change. In 2016 President Putin focused on reconnaissance systems, thermobaric munitions, and lasers as important areas that must not face reductions in spending. He also singled out information support, communication systems, electromagnetic weapons, weapons based on new physical principles, and precision-guided weaponry as other areas of extreme importance.[81] By 2018 the perspective of General Staff Chief Valeriy Gerasimov had become more general in describing trends in the changing character of armed conflict, perhaps because many of Putin's desires had already been achieved or work had begun on them. Gerasimov noted that robotic complexes, the information realm, and precision weaponry were some of the main features of future conflicts. However, he added that priority destruction targets were a state's C2 and economic objectives; and that there was a possibility of conflict along various strategic sectors, predetermining the need to create integrated groupings of troops and forces.[82] Thus, while Putin focused on specific weaponry, Gerasimov was more apt to place as much emphasis on how such weaponry might be employed. He was calling for creativity in the use of such weaponry and their application among soldiers and scientists, that is, new ways to consider the implementation of military art.

This section highlights some of the technological achievements outlined in the Russian media that have more tactical than strategic significance. The purpose is to show that skill and creativity, and not necessarily numbers, are driving Russian military efforts to achieve battlefield dominance. Each development enables tactical missions in the army, navy, and aerospace components of the armed forces.

---

[80] V. N. Verem'ev, "The Development of Tactics at the Contemporary Stage of Development of the Armed Forces of the Russian Federation," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science*), No. 3 2017, pp. 22-25.
[81] Vladimir Mukhin, "Putin Doesn't Intend to Reduce the Army: The Supreme Commander-in-Chief Is Betting on Reconnaissance, Lasers, and Thermobaric Munitions," *Nezavisimaya Gazeta Online*, 14 November 2018.
[82] Valeriy Gerasimov, "Ministry of Defense Describes 'Wars of the Future,'" *RIA Novosti*, 24 March 2018.

2016:

1. Scientific research codenamed Alabuga involves the experimental development of microwave pulse weaponry that can shut down electronics in a 3.5-kilometer radius. Its effect can blind or cause physical damage to electronic circuit boards and systems. Further research plans to create electromagnetic weaponry that includes projectiles, bombs, and missiles carrying special magnetic explosion generators.[83]
2. The Armata series of vehicles are to be equipped with a reconnaissance drone known as the Pterodakti. It is a light UAV connected to the combat vehicle with a flexible cable that allows the vehicle to monitor situations over hills or in areas where visibility is limited. It can circle in a radius of 50-100 meters around the vehicle, has a radar and thermal imaging device, and can reach an altitude of several dozen meters.[84]
3. The Arsenal design bureau is arming a group of space vehicles with electronic warfare weapons and nuclear power plants. The latter enables the installation of wide-ranging radio interference transmitters aboard the vehicle and increases a satellite's electronic power capacity.[85]
4. The Defense Ministry is working with industry to develop bridges that are invisible to modern sensing systems. This will enable their survival for longer periods of time.[86]
5. The Navy has deployed an underwater Internet that can deliver voice or digital information up to 35 kilometers and to depths of 6 kilometers. It allows for communication with deep-sea submersible, submarines, robots, and divers.[87]
6. The Navy has multiple rocket launch systems, the Udav and Zapad complexes, that can strike and divert attacking torpedoes. They can also deliver strikes on submarines and against underwater sabotage forces and means.[88]
7. The Shipovnik electronic warfare (EW) system is known as the "drone whisperer" in that it can intercept C2 from robot aviation (UAVs) in less than a second, along with an accuracy of up to one meter for computing the location of former owners. With a range of ten kilometers, it can suppress adversary command center and cellular and satellite communications.[89]
8. Radio-photonic radars are planned in Russia. They will be able to detect small UAV, including those with an anti-radar coating, that is stealth equipment. The system is resistant to jamming and electromagnetic pulses.[90]

2017:

1. C2 from the tactical to the strategic realm has become a priority target.[91] Electronic warfare forces intend to accomplish the following: disablement of adversary electronic assets; technical control over electronic countermeasures; countering adversary reconnaissance

---

[83] Aleksey Ivanov, "Electromagnetic Bombs Created in Russia," *Rossiyskaya Gazeta Online*, 28 September 2017.
[84] Aleksey Moiseyev, "They Will Equip the Armata with a Reconnaissance Drone: An Unmanned Aerial Vehicle Named 'Pterodaktil' Will Follow the Combat Vehicle Like a Tethered Aerostat," *Izvestiya Online*, 18 November 2016.
[85] Ivan Cheberko, "Roscosmos Has Found an Application for Nuclear Engines," *Izvestiya Online*, 31 August 2016.
[86] No author provided, "Russian Defense Ministry Develops Invisible Bridges," *Interfax* (in English), 14 March 2016.
[87] No author provided, "Russian Sailors Deploy Underwater Internet Network," *RIA Novosti*, 22 December 2016.
[88] No author provided, "Russian Navy to Receive Multiple Rocket Launch Systems to Divert Torpedoes," *Interfax* (in English), 29 December 2016.
[89] Anton Valagin, "Best New Russian Weapons Named," *Rossiyskaya Gazeta Online*, 25 December 2016.
[90] No author provided, "Advanced Research Foundation to Create Radio-Photonic Radars that Can Detect UAVs," *TASS* 20 December 2016.
[91] V. F. Lazukin, I. I. Korolyov, and V. N. Pavlov, "Basic Elements of the Tactics of Radio Electronic Warfare Troops," *Voennaya Mysl'* (*Military Thought)*, No. 11 2017, pp. 15-20.

technical assets; camouflaging one's own troops; disorganizing adversary troops and weapon C2 systems; reducing the application of the efficiency of adversary weaponry and electronic assets; and ensuring friendly force stability in control over one's own troops and weapons.[92] The main planning documents will be the "Adversary C2 Disorganization Plan" and the "Electronic Warfare Forces and Assets Employment Plan in Operations."[93]

2. The Vist-2 is an acoustic jammer that defeats sensors of self-homing torpedoes and submarine sonars. It can become a decoy target as well. It can operate for more than five minutes.[94] Another development, the Paket-E/NK, is an anti-torpedo complex that can destroy hostile ships and submarines as well as protect a ship from a torpedo attack.[95]
3. Work on an "invisibility cloak" has developed in Russia. The cloak is an assembly of ferrite fabric that protects armaments and hardware from electronic warfare systems. The cloak hinders an objects identification. The subject is identified only as a reflecting object.[96]
4. Russia has developed several types of reconnaissance capabilities, which utilize radars, sensors, detectors, rangefinders, UAVs, and thermal imaging sights. There are three levels (strategic operational, and front), but there is also tactical-echelon/combat (division or brigade) and special reconnaissance (Spetsnaz, at depths of 400 km to disable strategic deterrence assets; there is also tactical depth Spetsnaz missions). Each classification was provided by General Major Vladimir Marusin, ground force deputy chief.[97]
5. Russia has developed tactical groups to counter adversary UAVs. They include air defense specialists, electronic warfare assets, and sniper fire.[98] Russian UAVs are also being taught to independently identify targets in any conditions, thus becoming an important part of automated reconnaissance and strike systems. The UAVs will identify a target's coordinates and parameters and the nature of their operation, and then transmit them to the command and control system of the reconnaissance-strike system. Purportedly the system "provides a calculation and a graphic image: the probability of detection of the target to be destroyed; and the probability of the correct identification as a consequence of the adversary's counteraction."[99]
6. Russia is developing a mobile laser to blind the optics of aircraft, helicopters, missile and bomb homing heads, tanks, and antitank missile systems' aiming devices. It includes several laser emitters and thus can blind many targets or concentrate on one target.[100]
7. Russia has developed inflatable copies of its S-300PM air defense missile systems to deceive adversaries as to their actual location.[101]

---

[92] Ibid., p. 16.
[93] Ibid., p. 20.
[94] Aleksey Ramm, "Submarines and Ships Concealed by Sound Barrier: Miniature Vist-2 Acoustic Jammer Defeats Sensors of Self-Homing Torpedoes and Submarine Sonars," *Izvestiya Online*, 31 March 2017.
[95] No author provided, "Russia Developing Unique-in-World Anti-Torpedo," *Interfax* (in English), 24 January 2017.
[96] No author provided, "Russian Army to be Supplied with 'Invisibility Cloaks' Soon," *Interfax* (in English), 26 January 2017.
[97] Aleksandr Stepanov interview with Vladimir Marusin, "Find and Destroy in Seconds: How Reconnaissance Works," *MK*, 2 November 2017.
[98] No author provided, "Groups to Counter UAVs Created in Eastern Military District Combined-Arms Army in Amur Region," *Ministry of Defense of the Russian Federation Website*, 6 June 2017.
[99] Aleksandr Ramm and Vasilisa Belokopytova, "Defense Ministry to Teach Drones to Accurately Identify Targets," *Izvestiya Online*, 22 March 2017.
[100] Aleksey Ramm and Dmitriy Litovkin, "Defense Ministry to Get Light Saber; 'Szhatiye' Laser System Which Blinds Enemy Optics Has Been Revived," *Izvestiya Online*, 7 February 2017.
[101] No author provided, "Mock Enemy Aviation Misled by Inflatable S-300 Missile Systems," *Interfax* (in English), 17 April 2017.

8. The Russian Advanced Research Foundation has opened a laboratory to study liquid breathing. This is a method to advance man's study of sea and ocean depths. It may also have medical applications.[102]

2018:

1. A pilotless vehicle will be built into a round for the "Smerch" multi launch rocket system (MLRS). The round is launched into an area where a target's precise coordinates are unknown. The separated-UAV loiters over the zone until the object is recognized, and a signal is passed to the MLRS command center, which then destroys the targets with precision.[103]
2. In October 2018 it was reported that electromagnetic weapons "can be regarded as a further development of electronic warfare devices. So far, they can operate at a distance of several tens of kilometers…"[104] These ultra-high-frequency weapons disable radio-electronic and optical elements of equipment and weapons, but also disorganize control.[105] Another report noted that there are plans to "install electromagnetic guns on 6th-generation Russian unmanned aerial vehicles."[106]
3. Two lasers of distinction mentioned in 2018 were the Peresvet, which can not only counter air attacks but fight satellites in orbit according to one source; and the Svetozar, which received no further explanation.[107] The Peresvet system is excepted to be able to intercept UAVs at distances of 100 kilometers over the next few years.[108]
4. Over the course of the next three years the Kh-25MP tactical anti-radiation missile will be converted to a Kh-25ML model. The latter will be an upgraded precision munition with a laser homing sensor and a modified control unit. It will be able to strike surface-to-air missile complexes and other ground targets such as radars and bridges. Launched from fighters, bombers, or ground attack bombers, the missile has a launch range of about 20 kilometers and a speed of 850 meters a second. The missile was purportedly tested in Syria.[109]
5. Russia is developing a Cephalopod unmanned submarine, designed to be a submarine hunter. It has a small radius of operation and carries a small warhead. It may escort strategic missile submarines during a combat alert or guard ports and other facilities such as derricks.[110]
6. The Defense Industry intends to equip the Balkan automatic grenade launcher with grenades capable of conducting electronic warfare and video surveillance missions. The grenade's range is 2500 meters and the 40-mm grenades will have double the amount of explosive potential. The grenades will be belt fed from a box of 20. The defense industry

---

[102] Unattributed interview with Andrey Grigoryev, "We Have Created an 'Invisibility Cloak' and We Are Studying Liquid Breathing," *RIA Novosti,* 8 February 2017.
[103] Artem Kolchin, "Murakhovskiy: The 'Smerch' MLRS UAV Will Destroy Any Target," *PolitEkspert*, 27 November 2018.
[104] Oleg Bozhov, "We Have It! The Invisible Sword; Russia is Testing Electromagnetic Weapons That Burn the Insides of Enemy Missiles," *Armeyskiy Standart*, 12 October 2018.
[105] Ibid.
[106] No author provided, "Microwave Guns: Tests of New Weapon Have Started in the Russian Federation, Russia Has Begun Field Tests of an Electromagnetic Weapon," *Gazeta.Ru*, 1 October 2018.
[107] No author provided, "Peresvet Combat Laser Can Fight Satellites—Russian Defense Ministry," *Interfax* (in English) 5 December 2018; and no author provided, "New Combat Laser System Svetozar Sent to Troops Since Last Year—Expert," *Interfax* (in English) 10 May 2018.
[108] Dmitriy Yurov, "Burning Through Steel: Why Army of the Future Will Go Over to Lasers," *Zvezda TV Online*, 11 July 2018.
[109] Aleksandr Kruglov and Bogdan Stepovoy, "Killer of Air Defense Systems Given a Second Life: Aerospace Forces to Obtain Modernized Laser-Radar Munition," *Izvestiya Online*, 24 July 2018.
[110] Anton Valagin, "Russian 'Cephalopod' Will Become a Submarine Killer," *Rossiyskaya Gazeta Online*, 31 July 2018.

is also creating shrapnel munitions that spray destructive elements to destroy UAVs. In Syria a "shock-resistant ball robot" was tested. It can withstand being thrown or dropped from a height of 5 meters, after which it adjusts itself to vertical. With four video cameras and light-emitting diode (LED) lighting, a microphone, and transmitter, it can transmit images from a 360-degree view.[111] The ball is known as the Sfera intelligence-gathering suite (referred to as the roly-poly in the army) and is used to reconnoiter tunnels.[112]

7. Work is underway in foreign nations to create a swarm of UAVs, some designed to uncover frequencies. To confront them, Russia is developing false beacons that transmit dummy frequencies to fool the UAV reconnaissance swarm.[113] A shortwave infrared camera has been tested on a drone. It can see through dense fog and in a forest fire it can identify the center of the burn, which is what firefighters must go after.[114]
8. New Syrian-based tactics included the "Syrian berm." It is a barrier of sand or earth behind which an assault subunit takes cover. A tank group delivers fire through gaps in the obstacles, where the primary target is enemy artillery positions. Another report stated that the berm would be pushed forward by armor-plated bull dozers, allowing the attackers to slowly approach a target. If the berm was of sand, it would deflect lasers and infrared targeting systems.[115]
9. A Russian urban warfare tactic was to encircle and blockade a town, preventing supplies or reinforcements. Then a series of offensives were launched against the city from several directions at once. With the defense then spread thin, pockets of resistance were hammered by artillery and air strikes, sapping further any ability to resist. Swift strikes then cut the contested area into isolated pieces to break the will to resist.[116]

2019:

1. The Glaz [eye] individual reconnaissance system has been tested in Syria. It included a high-resolution camera that can view areas where an enemy is concealed in uneven terrain or behind buildings. The system is fired 300 meters into the air with a hand-held rocket launcher. A parachute is deployed, and the camera transmits images to a soldier's tablet. The maximum field of view is about one-half of a square kilometer.[117]
2. The Karnivora UAV is equipped with a net thrower to intercept other UAVs. It is envisioned to be able to drop high explosive fragmentation grenades and small anti-tank bombs. It can loiter for 15 hours in the air.[118]
3. Russia continues to test its reconnaissance-fire methodology, which it believes has caused a threefold improvement in carrying out fire missions. Coordinates for targets are transmitted in real time from Orlan UAVs and Strelets reconnaissance, control, and communication systems to the artillery control center.[119]

---

[111] Nikolay Grishchenko, "Russia to Develop Spy Grenades with Video Surveillance," *Rossiyskaya Gazeta Online*, 6 February 2018.
[112] Aleksandr Khoklov, "Tactical Innovations: Why the 'Tank Carousel' Behind the 'Syrian Parapet' is So Scary for the Enemy," *Yezhenedelnik Zvezda*, 14 December 2018.
[113] Mikhail Goldreyer, "The UAV Swarm: Concerns and Reality," *Arsenal Otechestva Online*, 1 February 2018, No. 1, pp. 86-87.
[114] No author provided, "In Rostekh, They Developed and Successfully Tested an 'All-Seeing' Drone," *Mir TV Online*, 28 December 2018.
[115] Aleksandr Khoklov, "Tactical Innovations: Why the 'Tank Carousel' Behind the 'Syrian Parapet' is So Scary for the Enemy," *Yezhenedelnik Zvezda*, 14 December 2018.
[116] Anton Lavrov, "Outcomes of the Russian Military Campaign in Syria," *Moscow Defense Brief*, No. 3 2018, p. 14.
[117] Aleksey Ivanov, "Russian Soldiers to be Equipped with Rocket 'Eye'," *Rossiyskaya Gazeta Online,* 28 January 2019.
[118] Aleksandr Belozerov, "Karnivora UAV Fires Nets and Drops Bombs," *Interfax*, 1 February 2019.
[119] No author provided, "Southern Military District Artillery and Armored Subunits Conduct Fire Exercises Using Reconnaissance-Fire Loops," *Ministry of Defense of the Russian Federation* (in English), 7 February 2019.

4. Russia's Okhotnik heavy combat UAV is designed to break through air defenses, allowing manned aircraft such as the Sukhoi Su-57 to enter the perimeter afterwards.[120] One report listed its speed at 1400 kilometers an hour and a flight range of 5000 kilometers. The strike UAV will have 2800 kilograms of weight allowed for weaponry.[121]
5. The Samum (Arabic for torrid desert wind) is an ultramobile upgraded multirole artillery piece designed to protect against tactical fighters, helicopters, and certain types of UAVs operating at low and ultralow altitudes. It has a remote-control module as well.[122] The latter is based on the ZU-23 air defense mount and helps fight snipers and drones in urban conditions. Samum has three types of 23-millimeter ammunition: fragmentation-high explosive-incendiary, fragmentation-high explosive-incendiary-tracer, and armor-piercing-incendiary-tracer.[123]
6. Russia has developed a radio electronic gun, the Pishchal, to counter adversary UAVs navigation and communication systems. It operates over the 600 to 6,000 MHz frequency range with an effective range of use over 2 kilometers. More than 200 sets have been ordered.[124]
7. An interesting development that the military has discussed for two years is known as the tank carousel method. It employs tanks moving in a circle, which take turns engaging the enemy from the same firing position. As one source noted, servicemen practice "continuous fire with tanks taking turns to change firing position until the pop-up and moving targets at ranges of between 500 meters and 2500 meters are completely destroyed."[125] A 2018 article noted that tanks can "conduct fire from behind a so-called 'Syrian berm' and execute fire according to the 'tank carousel' method" from subunit to full tank company strength.[126] In a 2017 description of the method, it was stated that while the first tank crew delivered fire in place, "the crew of the second loaded the ammunition. When the first tank rolled out for flanking fire, the second took up a position for fire from the halt."[127]

Many of the descriptions above are of weaponry or tactics in the experimental stage, but they offer focal points of interest for the Russian military. The discussion indicates that several developments are assisting commanders on the battlefield in their attempts to command and control forces, to conduct realistic reconnaissance missions, and to counter or disorganize adversary capabilities.

Conclusions

Technology is influencing the development of tactics, especially ways to create new and artistic employments of weaponry. While less studied, Russian tactical capabilities to conduct detailed reconnaissance of the battlefield and offset the electronic parameters of equipment are designed to result in the disorganization of an opposing force and neuter their ability to integrate and relay commands. While not as conceptually intriguing as the use of cyber forces, these capabilities can

---

[120] No author or title provided, *Interfax* (in English), 28 January 2019.
[121] Anton Valagin, "Okhotnik Heavy Strike UAV Proves to be Supersonic," *Rossiyskaya Gazeta Online*, 13 February 2019.
[122] Irina Dronina, "Russia Develops Drone Killer," *Nezavisimoye Voyennoye Obozreniye Online*, 7 January 2019.
[123] Ivan Surayev interview with Umakhan Magomedgadzhiyevich Umakhanov, "Tests of Anti-UAV Complex Will Begin at the End of the Year," *RIA Novosti*, 5 February 2019.
[124] Nikolay Grishchenko, "Russian Federation Security Agencies Receive Electronic Pishchal to Hunt Drones," *Rossiyskaya Gazeta Online*, 21 January 2019.
[125] *Website of the Ministry of Defense of the Russian Federation* (in English), 30 January 2019.
[126] Andrey Sergeyevich Ivanayev, interviewed by Viktor Siryk, "Whoever Is Given More Has More Responsibility," *Zvezda TV Online*, 24 July 2018.
[127] *Website of the Ministry of Defense of the Russian Federation*, 15 September 2017.

totally disrupt the plans of an opponent to command and control forces and potentially change the COF on the battlefield.

The creative thought of Russian commanders and scientists is the motivating factor behind the implementation of new concepts in military art. As they study foreign lessons learned in warfare and discuss their own battlefield experiences and needs, new ideas germinate and take root. Skill and knowledge are replacing the former requirement for more numbers of troops, turning dreams turn into reality and affecting the implementation of tactics. Further, scientists continue to study and collect the operating parameters of foreign equipment closely, because it is these parameters that they strive to offset.

Of the 32 examples provided from the years 2016-2019, there were near equal results posted for the use of UAVs, EW, electromagnetic, and tactical applications of research. Offensive weaponry, laser applications, and communication issues were also areas of importance. The overall capability appears to be centered on observing or reconnoitering an adversary (UAVs) and then choosing the way to proceed: with precision weaponry, blinding (lasers) equipment, or cutting off access (EW) to specific frequencies. There is also a push to make equipment appear invisible to either radars or satellites. Thus, there are offensive and defensive uses of the technologies discussed above. Goals appear to be the disorganization of any command and control options available to an adversary or his destruction with reconnaissance-strike assets.

The age of artificial intelligence and quantum computing is now upon us, and they will bring new advances in how strategy, operational art, and tactics are conceived and applied. What once was science fiction or on a wish-list for military leaders is now being developed in the research labs of scientists, especially ways to attack or protect the electronic frequencies found in so much equipment today, whether it be UAVs or satellites or missiles. Military art must be studied and anticipated in the West as Russia develops new offensive and defensive concepts. It will be the creative innovations and uses of technology on the battlefields of the future that will enable many successful gambits.

This page intentionally left blank.

4 Russia's Reflexive Control Theory: Manipulating an Opponent to One's Advantage

> The method (technique) of reflexive control of an enemy is the devices and techniques for implementing measures and actions that incite the enemy to act in a corresponding way that is advantageous for our side…Reflexive control can make it possible to change the enemy's goals and his methods of operation in favor of one's own forces, i.e., to contribute to the creation of favorable conditions to accomplish the assigned mission.[128]

Introduction

For the past few decades, Russian military authors have discussed a concept known as "reflexive control" (hereafter RC). The concept is used in negotiations, in battlefield deception activities, in space activities and deterrence operations, and in a host of other venues. It is discussed in Army, Navy, and Aerospace publications.[129]

The term is defined in general as providing a stimulus (information, an action, etc.) to make an opponent to do something for himself (organize in a specific way, develop certain weaponry, maneuver, etc.) that he is doing for the initiator of the action. To utilize the concept, the proponent must know how an opponent thinks and processes information, and what his prejudices, likes, and dislikes are. Targeting can be as detailed as a psychological profile of specific officers in command positions.

This article explains several aspects of this Russian concept. It looks at how various Russian experts define RC; how RC is used in deterrence, systems analysis, deception, negotiations, doctrine, and other venues; and how it has been used in Ukraine and elsewhere. It is a concept that needs to be considered by tacticians and strategists when contemplating Russian military moves and the potential rationale behind their actions.[130] Ignoring RC invites being controlled by the Russians.

Definitions and Use of RC: 2002-2013

When retired (now deceased) Russian General-Major V. D. Ryabchuk discussed the intellectual confrontation on the battlefield in 2008, he noted that, regretfully, calculations still need to be made on the intellectual potentials of opposing sides, just as are done with both sides' information or other capability measurements.[131] For Russian military officers, intellectual confrontations and calculations of a potential adversary's capabilities can involve RC. Officers examine objective situations and subjectively think through how to manipulate the environment to their advantage. Their analysis considers the thought patterns and tendencies of potential opponents and, when

---

[128] F. Chausov, "Command and Control of Battle on the Basis of a Reflexive Analysis of the Situation," *Morskoi Sbornik* (*Navy Journal*), No. 6 2017, p. 52. The author would like to thank Dr. Harold Orenstein for his translation of this article from Russian to English.

[129] A semiannual journal titled *Reflexive Processes and Control* was also published in Russia. It is not known for certain if the journal is still in existence.

[130] For more information on this concept, see Timothy Thomas, *Recasting the Red Star*, 2011, pp. 118-131; Timothy Thomas, *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*, 2015, pp. 117-123; and Timothy Thomas, *Kremlin Kontrol*, 2017, pp. 175-198.

[131] V. D. Ryabchuk, "Problems of Military Science and Military Forecasting under Conditions of an Intellectual-Informational Confrontation," *Voennaya Mysl'* (*Military Thought*), No. 5 2008, pp. 67-76.

combined with their own forecasting of potential future actions, results in the forms and methods needed to fulfill the forecast. One of the thoughts involved with the successful use of "thought being the first to enter battle" is formulating a method that sets an enemy up for defeat via the use of RC.

Russian military analysts have defined RC in a standard manner over the years. In earlier articles on RC, this author defined RC according to analysts who wrote mainly in the 1990s (the footnote on the preceding page is where many of these definitions can be found). This section takes up where those definitions left off, examining RC definitions from 2002 to the end of 2013, followed with a section addressing how RC was used in that time period. That is followed by a section that examines RC definitions and use from 2014 to the present time.

1. RC is essentially information and psychological effects against persons on the opposing side who are making decisions. It is "a set of measures, interconnected with respect to goal, place, and time, aimed at…forcing the enemy to reject his initial plan and accept knowingly a decision that is disadvantageous for him…"[132]
2. "The objective of reflexive control is to create favorable conditions for the performance of one's own combat mission by adversely affecting the opposing side's decision-making."[133]
3. In WWII, reflexive control was achieved "by implementing an array of measures and activities, interconnected by the goal, place, and time and designed to foil the adversary's plans by imposing one's will on the enemy through concealment, masking, deception, feints, decoy actions, and diversionary actions."[134]
4. "…the question must be not so much about countervailing and deceiving enemy reconnaissance as about the reflexive control of the person, who takes decisions about the actions of adversarial troops (forces), by way of communicating to him relevant false information (and under certain conditions, partly true information)."[135]
5. "Fighting today is primarily intellectual, information-reconnaissance-navigational. Troop control is assuming the form of battle control, which means reflexive control of enemy actions."[136]
6. "Deterrence does not imply overpowering the adversary on the battlefield, but rather it is intended to impress a vision of defeat on his mind. In fact, deterrence is a reflexive game in visions of victory, defeat, and unacceptable (restraining) damage, among others."[137]
7. "An important feature of such a war [information] is the extensive use of enemy resources. Influencing his information systems based on the principle of

---

[132] Stanislav Ermak and Aleksandr Raskin, "Are All Methods Good in Battle? On Some Aspects of Reflexive Control of the Enemy," *Armeyskiy Sbornik* (*Army Journal*), No. 7 2002, p. 44. The author would like to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[133] A. V. Raskin and V. S. Pelyak, "On Network-Centric Warfare," *Voennaya Mysl'* (*Military Thought*), No. 3 2005, p. 46.
[134] I. N. Vorobyov and V. A. Kiselev, "The New Strategy of the Indirect Approach," *Voennaya Mysl'* (*Military Thought*), No. 9 2006, pp. 2-5.
[135] V. N. Karankevich, "How to Learn to Deceive the Enemy," *Voennaya Mysl'* (*Military Thought*), No. 9 2006, pp. 44-46.
[136] I. N. Vorobyov and V. A. Kiselyov, "From Present-Day Tactics to Network-Centric Action," *Voennaya Mysl'* (*Military Thought*), No. 8 2011, pp. 19-27.
[137] S. G. Chekinov and S. A. Bogdanov, "Strategic Deterrence and Russia's National Security Today," *Voennaya Mysl'* (*Military Thought*), No. 3 2012, pp. 11-20.

> reflexive control, one can achieve desirable actions from opposite sides, that in real practice are often referred to as a provocation."[138]

A somewhat hidden military reference and definition of RC (one had to know what one was looking for) was offered in 2011. It is listed here out of chronological order, since it appeared in an official Ministry of Defence (MOD) document titled "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space." The term "information war" was defined as follows:

> Conflict between two or more States in information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents.[139]

The last line, "forcing a State to make decisions in the interests of their opponents," is key. There is no difference between this statement and those from the definitions offered by many theorists over time. In 1974, for example, K. V. Tarakonov stated that "RC is understood as the process of one of the sides giving reasons to the enemy from which he can logically infer his own decision, predetermined by the first side."[140]

These definitions indicate that Russian military planners consider the use of RC when they develop an operation. To avoid being deceived, the militaries of other nations should at least take RC into consideration as they contemplate the battlefield information they are receiving about Russian operations and the picture that is developing before them. As the definitions above demonstrate, the use of RC even extends beyond the battlefield.

When examined over time, it is possible to view the wide use and application of RC in Russian planning and strategic actions. It enriches military art, is used against decision-makers, enables wide-spread misunderstanding and deception among Western experts, corrupts computer networks, and manipulates social media, among other uses. Some twenty different ways that Russia uses RC are looked at here. Several examples will be discussed that cover the time period 1995-2012. More contemporary uses are then described in the next section.

Enriching the arsenal of military art. In 1995, when discussing information weapons, scientists at the Russian Academy of Sciences' Systems Analysis Institute noted that transmitting false or distorted information influences decision-making and thus how combat operations are conducted. Such techniques reflexively control the enemy and enrich the arsenal of military art,[141] that is, they offer deceptive ways that tactics, operational art, and strategy might be considered and implemented.

Negotiations. The following year, 1996, the same publication noted that "simulated negotiations incorporate both conventional marketing techniques and specialized methods of

---

[138] Nikolay Khorunzhyy, "Does Russia Need a Cyber Command?" *Kovrov VPK.name*, 23 August 2013.
[139] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministerstvo Oborony Rossiyskoy Federatsii* (*Ministry of Defense of the Russian Federation*), 2011, at ens.mil.ru.
[140] Clifford Reid, "Chapter Fourteen: Reflexive Control in Soviet Military Planning," in Brian D. Daily and Patrick J. Parker, editors, *Soviet Strategic Deception*, Lexington Books, 1987, p. 294.
[141] Vitaliy Tsygichko and Dmitriy Chereshkin, "Perspective: A Weapon that May Be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare," *Nezavisimoye Voyennoye Obozreniye* (*Independent Military Review*), 18 November 1995.

psychological support during negotiations, including techniques based on reflexive control."[142] Thus, negotiators should be aware of RC.

Military doctrine and deception. A very important use of RC was noted in 1997 in the journal *Military Thought*. Major-General A. F. Klimenko stated that Russia's military doctrine contains recommendations on how military force might be applied in specific situations. He noted that "the property of reflexive control of the other, competing, side is set forth in it."[143] Reflexive and normative functions are "programmed" into military doctrine and can accomplish their RC role in such open publications.[144] Very few U.S. analysts have ever considered the publication of Russian military doctrine to be a RC operation.

Space and RC. In 2002, authors Stanislav Ermak and Aleksandr Raskin discussed RC methods in general and as they apply to space. Coercive pressure, transmitting false information, influencing an opponent's decision-making algorithm, and information and psychological effects were discussed in the general section. They then noted that a special role for RC was provided in space information resources for enemy control. To be effective, a holistic idea of the armed struggle process in front of a commander must be viewed as an integrated system, where the creativity of a commander to adjust to this view of reality is essential to the successful use of RC.[145] Today, Russia's space troops have developed an "inspection satellite" than can inspect other orbiting satellites for their function. They can also be turned into space interceptor satellites.[146] As a result, they can be used for RC measures such as deterrence by indicating that their value or use has been discovered and therefore neutered to a degree—when in fact they might not have been.

Deterrence theory and RC. RC is used extensively in deterrence theory. In 2003 three academicians at the Russian Academy of Military Science noted that "Reflexive control of the adversary as he makes decisions in the course of a conflict" becomes a significant component of nuclear concepts. The purpose of control is to convince the adversary of the uselessness of nuclear blackmail and military pressure on the country, where the "victim" strives to make an "aggressor" understand that the attacking side will also suffer the consequences of an attack.[147] Two years later, in 2005, one of the authors of this article (V. Kovalev) stated that even U.S.-Russian joint nuclear deterrence modeling "provides excellent opportunities for reflexive control over the Russian side."[148] Of interest, of course, is that Kovalev ascribed RC to U.S. thought, even though it is strictly a Russian concept.

---

[142] Petr Shlayev, "The Human Aspect of the Problem: Arms Exports and Ergonomics," *Nezavisimoye Voyennoye Obozreniye* (*Independent Military Review)*, 24 February 1996.
[143] A. F. Klimenko, "Theoretical-Methodological Problems of the Formation of Russia's Military Doctrine. The Techniques for their Resolution," *Voennaya Mysl'* (*Military Thought*), No. 3 1997, pp. 6-14.
[144] Ibid.
[145] Ermak and Raskin, pp. 44-46.
[146] S. Valchenko, N. Surov, and A. Ramm, "Russia Sends Inspector into Orbit: Military Test Operations of Maneuvering Identification and Intercept Satellite," *Izvestiya Online* (*News Online*)*,* 26 October 2017.
[147] S. Yu. Malkov, V. I. Kovalev, and B. Konyakhin, "On the Question of a Methodology for Selection of Rational Strategies to Safeguard Strategic Stability and Nuclear Deterrence in the Modern Era," *Strategiskaya Stabilnost* (*Strategic Stability*), No. 3 December 2003.
[148] V. Kovalev, "Temptation for a Preventive Strike: What's 'New' in the Liberal Theory of Deterrence from the Standpoint of a Representative of 'Caveman' Thinking," *Voyenno-Promyshlennyy Kuryer* (*Military-Industrial Courier*), 9 November 2005.

RC, decision-makers, and stratagems. In 2005 A. V. Raskin and V. S. Pelyak stated that RC's objective "is to create favorable conditions for the performance of one's own combat mission by adversely affecting the opposing side's decision-making."[149] Influencing decision-makers is clearly the main purpose of RC. In 2006 it was noted that RC uses military stratagems to control an enemy force. It is implemented with an array of measures interconnected by goal, place, and time to foil an adversary's plans through concealment, masking, deception and so on.[150]
Computer networks and systems. The wide use of information technologies in military troop and weapon control system promotes the use of RC in computer networks and enemy control systems. It is possible to distort true information and substitute it with false data or perform other actions. This can be used to "compromise the military political leadership of an enemy-country in the eyes of its people, to persuade some into betrayal."[151] RC is also used in systems analysis, where a "decision-maker in the first system demonstrates to a decision-maker in the second system false intentions and thus encourages it to make decisions favorable for itself,"[152] which are actually beneficial to the first system.

Information-psychological aspect of information war. In 2008 well-respected authors I. N. Vorobyov and V. A. Kiselev wrote that modern strategic operations are stressing the increased role of information-psychological support, which is an integral part of information war. Information-psychological support has for some time included the use of reflexive control of the behavior of an enemy force, employing complex military-political and diplomatic measures to deceive the enemy.[153]

Make abstract knowledge a strength. In 2009 A. V. Pervov discussed the reflexive approach as a way of safeguarding Russian national security, since in the 21st century there are more nontraditional ways of waging war.[154] Now it is possible to influence leaders, the population, and even decision-makers in ways not possible in the past. The reflexive approach intends to control cognitive subjects, the importance of which is expressed in the thought "the first into battle is thought."[155] The idea is to turn abstract knowledge into strength, if one can think in a nonstandard way through the construction of cause and effect relationships that may have to be adjusted as a situation develops. The reflexive approach forms structures of behavior for participants, and the goal is to get the enemy to act in accordance with an externally imposed scenario.[156]

Reflexive approach, reflexive analysis, reflexive control, and air defense. In 2011 S. A. Nesterov and V. V. Stepanov noted the following: the reflexive approach suggests an unorthodox way of thought, a sign of one's intellectual frame of mind (for example, air defense preparation). Reflexive analysis is the tool to implement the reflexive approach, a way to

---

[149] Raskin and Pelyak.
[150] Vorobyov and Kiselev, "The New Strategy…"
[151] Karankevich.
[152] F. G. Kolomoyets, "Systems Analysis: Recommendations for Problem Identification, Formulation, and Study," *Voennaya Mysl'* (*Military Thought*), in English, Volume 3, 2007, Eastview Publications.
[153] I. N. Vorobyov and V. A. Kiselev, "The Evolution of the Principles of Military Art," *Voennaya Mysl'* (*Military Thought*), in English, Volume 3 2008, Eastview Publications.
[154] A. V. Pervov, "The Reflexive Approach as An Important Tool of a Mechanism for Safeguarding Russia's National Security," *Vestnik Akademii Voennykh Nauk* (*Journal of the Academy of Military Science*), No. 3 2009, p. 20. The author would like to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[155] Ibid., p. 21.
[156] Ibid., p. 22.

construct the enemy's probable objectives and how to achieve them, by analyzing his train of thought (weapons to be used). Reflexive control is control that exercises one's intellectual superiority over the enemy. Control is efficient if it includes the moves the enemy is forced to make by the friendly commander (tactical masking, false maneuvers, ways to gain time, etc.).[157]

Deterrence as a reflexive game. In 2012, in an article on air and space defense, it was noted that the development of mechanisms to penetrate the enemy's process for arriving at operational solutions presupposes misinforming people via a reflexive command and control operation. The reflexed person thinks he is acting in an advantageous way, but is actually doing something that rather is advantageous for the disinformation administrator.[158] The same year other authors argued that since information rivalry is now a key component of modern geopolitics, a dangerous trend is reflexive control, since deterrence is a reflexive game of visions of victory, defeat, or unacceptable damage. Deterrence offers a demonstration of resolve, which can be accomplished with reflexive control.[159]

RC and Internet phishing. Authors Andrei Soldatov and Irina Borogan described a 2012 RC episode in their book *The Red Web*. Supporters of opposition candidate Alexi Navalny began receiving a surge of messages promoting a rally against Putin. The e-mails' only sentence was "Instructions for your actions in the rally against Putin." When accessed, the document contained malicious macros and loaded a hidden piece of software, called Trojan.Gen. It overwrote files with common extensions and eventually caused the computer to crash.[160] Thus, the goal was to get Navalny's supporters to do something for themselves (access instructions for a rally against Putin) that they were actually doing for the Russian authorities who had planted the virus, getting them to download it and ruin their computers. In effect, this implies that government-directed phishing attempts are a type of RC activity in Russia.

Definitions and Use Since 2013 and Ukraine…Some Recent Examples to Consider

In 2018 the journal *Military Thought* published three volumes of definitions of military terms. One of the volumes defined reflexive terms. The use of these definitions stretches from 2011-2014, and the year in which each appeared is listed after the definition. They were not listed above because they were not published as a comprehensive unit until 2018. Those relating to RC are:

Reflexive control: 1. The process of transmitting to an enemy "justification" for making a decision. 2. Special effects against an enemy for the purpose of "persuading" him to make a decision that has been predetermined by the controlling side. (2013)

Reflexive control: Control with the help of stimulation for the desired decisions. Under contemporary conditions and, moreover, in the foreseeable future, the role of control based on intellectual superiority over an enemy is becoming a decisive factor. One of the sides

---

[157] S. A Nesterov and V. V. Stepanov, "A Reflective Approach: How Surface Warships Prepare for and Fight Off an Air Attack," *Voennaya Mysl'* (*Military Thought*), No. 8 2011, pp. 28-36.
[158] Oleg N. Shevchenko, Petr N. Marushchenko, and Varvara Petrovna Obrazovtsa, "Winning…with the Help of Deception: Today Within the Content of Maskirovka Development of a Mechanism for Penetration into the Process of the Enemy's Arriving at a Solution for an Operation Is Moving to the Fore," *Vozdushno-Kosmicheskaya Oborona Online* (*Air-Space Defense Online*), 14 May 2012.
[159] S. G. Chekinov and S. A. Bogdanov, "Strategic Deterrence and Russia's National Security Today," *Voennaya Mysl'* (*Military Thought*), No. 3 2012, pp. 11-20.
[160] Andrei Soldatov and Irina Borogan, *The Red Web*, Public Affairs: New York, 2015, pp. 162-163.

effectively controls battle if the situation develops in accordance with its own plans. However, this is possible when control encompasses the entire battle process, including enemy operations imposed upon him by the other side. (2011)

Reflexive control of an enemy: Control in all spheres of confrontation, aimed at achieving the operational goal, forcing an enemy to reduce the degree of realization of his operational and combat capabilities, reflect his initial plan, and make irrational decisions. In addition, it is also necessary to conduct measures against the subject of protection against similar effects on the part of the enemy. The following are the result of reflexive effects against an enemy: predetermined conclusions about the enemy from an assessment of the conditions of combat, one's own forces, and enemy forces; the result of understanding the method for achieving the operational goal, necessary for the reflexive combat system; determination of enemy operations; and others. (2013)

Information packet: A specific technique of reflexive control of an enemy, which can be the transmission of risks, motivation, transmission of certainty, transmission of a reflexive depiction of the situation, formation of stereotypes, delay, dispersion, etc. Within the framework of a method of reflexive control, an information packet is implemented through the totality of simulacra, embodied both in a nonrepresentational form (simulation) and in a representation form (disguise). (2014)

Method of reflexive control of an enemy: The systematic totality of information packets sent to the enemy for the purpose of creating favorable conditions for accomplishing a combat task. (2014)

Reflex: The ability to take the position of an "observer," "researcher," or "controller" with respect to one's body, thoughts, actions. (2013)

Reflexive approach: …This is a parameter of a person's intellectual state. The principal instrument of the reflexive approach is reflexive analysis, the content of which in time of war is a reproduction of probable enemy goals, methods of achieving them, logic of reasoning, and assumed methods of obtaining necessary situational information. When employing the method of reflexive analysis, the process of justifying decision by taking into account one's own situational conditions assumes modeling enemy activities during the decision-making process, i.e., it is a complex reflexive process that requires, in turn, modeling the enemy's impression about the activities of the decision-maker himself. Reflexive functions include obtaining additional information about the process, organization, identifying the enemy's goals and plans, and formulating one's own preemptive goals and plans. (2011)

Reflexive technologies: The totality of methods, means, and techniques for information-psychological effects against an enemy, integrated by priority tasks and ensuring the most effective achievement of the goal of the operation (combat). Reflexive technologies in the organization and conduct of the confrontation of combat systems are the most important instrument in developing a plan for and making a decision about an operation and combat. Reflexion of an enemy in the process of preparing for and conducting contemporary operations (combat) includes a system of special organizational measures in various spheres of

confrontation of combat systems: informational, cognitive, socio-cultural, and physical. (2013)[161]

In addition to these definitions, there were several reports of RC's use since 2013, most in relation to the situation that developed in Ukraine or in relation to social media. Three important 2013, 2015, and late 2017 articles on RC by Russian analysts include those by V. L. Makhnin, who writes often in military journals about a host of topics; V. G. Kazakov and A. N. Kirishin, who have written on RC in Russia's *Journal of the Academy of Military Science*; and F. Chausov, a prominent RC analyst who writes on the topic for the *Navy Journal*.

V. L. Makhnin

The friendly embrace and RC. In 2013, writing in the Russian journal *Military Thought* about the conflict in Ukraine, V. L. Makhnin noted that going from the reflection of cooperation to that of conflict can break the will of the adversary's military and political leaders. This is known as strangling the enemy in a "friendly" embrace.[162] One is reminded of the Putin-Poroshenko meeting for a truce after Russia's occupation of Crimea, which was immediately followed by a Russian military invasion of Ukraine. Was Poroshenko strangled in the "friendly" embrace? One should closely observe recent cease-fires to see if the same "friendly" embrace repeats itself.

Supply of interests and reasons for RC. Makhnin stated that the organization of the reflexive process between opposing combat systems is related to the development and implementation of a series of measures to supply the reflexed combat system with interests, motivations, and reasons. These measures combine to create a desired operational-tactical situation and provide an incentive for making desired inferences and conclusions that benefit the friendly decision-maker.[163] The use of the reflexive process leads to the use of false-real, information, and psychological images of objects, processes, and phenomena.[164] Reflexive influence using simulacra paralyzes the adversary's (decision-maker's) intelligent (creative) activity.

Use of analogies and RC. Yet another way to induce reflection may be the most interesting and it involves the use of analogies. One is reminded of the use of the fascist and Nazi analogy in reference to people fighting in Maidan Square against Ukrainian President Viktor Yanukovych, an analogy drawn to acquire support from the Russian population. Older Russians well-remember the devastation of the Nazi onslaught against Stalingrad and Leningrad in World War II, and so this parallel/analogy touches a raw nerve. Thus, in this case RC was inflicted on the Russian population and succeeded through analogy.

The pace of conflict and RC. RC can cause an opponent to slow down his operations, abandon plans, and make irrational decisions, which could be exactly what is happening in Ukraine. Makhnin describes what he terms as creative and destructive reflexive functions (a commander's concept that is based on a tested way of action or an old idea). The former develops "in a situation when the struggle goes on at a slow pace and, accordingly, the

---

[161] N. N. Tyutyunnikov, *Military Thought in Terms and Definitions*, *Voennaya Mysl'* (*Military Thought)*, *Volume 1*, Armed Forces of the Russian Federation, 2018, pp. 218-221.
[162] V. L. Makhnin, "Reflexive Processes in Military Art: The Historico-Gnoseological Aspect," *Voennaya Mysl'* (*Military Thought*), No. 1 2013, p. 40.
[163] Ibid., p. 34.
[164] Ibid., p. 37.

operational-tactical situation changes slowly as well, when the opponents' objectives are clear, and the way to reach them has been figured out."[165] Clearly the slow pace of the conflict in Ukraine has offered Russia the opportunity to thwart opinions that have developed against Russian support for the separatists and to keep Ukrainian forces from taking control of pro-Russian-controlled territory.[166]

V. G. Kazakov and A. N. Kirishin

Controlling friendly forces and RC. In 2015 V. G. Kazakov and A. N. Kirishin wrote an article on RC for the *Journal of the Academy of Military Science*. It appeared to be an expanded version of an article they wrote in 2013. They stated that control of one's own troops is as important as control of the enemy. Such combat operations need the creation of "favorable conditions to execute combat tasks with the help of deception and covert control of the enemy."[167]

Controlling an enemy force and RC. Military art has long used deception, defined as a "premeditated action aimed so as to create in another an impression of facts that do not correspond to reality."[168] It appears that the theory of RC is another method, which the authors understand in the following way:

> Generally understood as the process of transmitting to the enemy the 'bases/foundations' for making a decision. At the same time, Lefebvre [Russian RC expert, believed by many to be its founder] believes that RC is a special action against the enemy, with the aim of 'persuading' him to make a decision that has been predetermined by the controlling side.[169]

To impact an enemy at the tactical level, leaders must be preempted in the sphere of thinking and planning to examine a situation in a specific way. If an enemy force is to be placed in the position of a controlled system, it must become a victim of what is known as "reflexive superiority." This requires knowing how an opponent makes decisions so that the proper "information packets" [targeted at an opponent's decision-making] can be developed and distributed to an opponent, which can result in a reflexive controlling action.[170] Simulation and concealment are two aspects of deception that help form the foundation of reflexive interaction.[171]

Developing an RC force. The most probable areas where command and control and RC can be combined are in the process of decision-making in general and in the planning of combat operations. To reflexively control the enemy, a specially designated force and means should be developed to study opponents, that is, a specific Table of Organization and Equipment (TO&E)[172] with information-psychological confrontation qualifications. These forces would develop and transmit recommendations to the commander on how to use RC measures together

---

[165] Ibid., p. 44.
[166] Ibid.
[167] V. G. Kazakov and A. N. Kiriushin, "All-Inclusive Command and Control of Combat Operations," *Vestnik Akademii Voennykh Nauk* (*Journal of the Academy of Military Science*), No. 4 2015, p. 36. The author would like to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[168] Ibid., p. 37.
[169] Ibid.
[170] Ibid.
[171] Ibid., p. 38.
[172] Ibid., p. 39.

with command and control actions against an opponent.[173] These forces would be expected to accomplish the following:

> Here the implementation of the RC method at stages of immediate preparation for and execution of the combat mission is carried out by means of sending the appropriate information packets to the enemy. It should be recalled that an information packet within the framework of a RC method is implemented through the totality of simulacra, which are embodied in both a nonrepresentational form (simulation) and a representational form (concealment). Information packets are sent to the enemy with the goal of creating favorable conditions for executing a combat mission .[174]

Information packets and RC. Information packets are designed to conceal existing combat situations or describe a nonexistent situation.[175] Such situations are subject to two sets of reflection, information and actual operations. Information reflection is how the enemy views friendly forces and their condition based on their system of intelligence and the enemy's assessment of an opponent's potential. Operational reflection is the principles and features of an enemy's decision-making within the information he has about the condition of his opponent's force and combat operations plans. Combat experience also counts when such decision-making is conducted.[176]

F. Chausov

Defining RC. Chausov has written a few articles for the publication *Naval Journal* on RC. His definition of RC is, as of the writing of this article, the most recent that has been observed in military publications:

> The method (technique) of reflexive control of an enemy is the devices and techniques for implementing measures and actions that incite the enemy to act in a corresponding way that is advantageous for our side…Reflexive control can make it possible to change the enemy's goals and his methods of operation in favor of one's own forces, i.e., to contribute to the creation of favorable conditions to accomplish the assigned mission.[177]

Reflexive analysis. In the 2011 article cited above, Nesterov and Stepanov discussed reflexive analysis, and Chausov, a reflexive control expert, returned to the topic in 2017. It will be important, he noted, to foresee future situations for the use of forces and means based on calculations and modeling; and to forestall an enemy's command and control processes. He stated that information technologies now make it possible to exclude the formation of a situation that would be disadvantageous for the Russian side using reflexive analysis of the situation. Battle control is possible if command and control effects can be applied to both one's own forces and the enemy's. Reflexive control of the enemy is the highest form of a commander's manifestation of his intelligence and talent. A combination of direct and indirect actions is needed.[178]

---

[173] Ibid., p. 41.
[174] Ibid., p. 40.
[175] Ibid.
[176] Ibid.
[177] F. Chausov, "Command and Control of Battle on the Basis of a Reflexive Analysis of the Situation," *Morskoi Sbornik* (*Navy Journal*), No. 6 2017, p. 52. The author would like to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[178] Ibid., pp. 50-51.

Chausov stated that a reflexive analysis of the situation involves both one's perception of a situation and "living through the situation" from the vantage point of one's opponent. Such situational analysis helps explain why a situation will develop in one way or another and allows Russian commanders to utilize reflexive activity over reactive activity. RC is a technology of disorganizing the enemy's network command and control cycle of "find-assess-make a decision-strike."[179] Chausov notes the following about the decision-making between two sides in confrontation and ways to influence the situation towards one's own interests:

> This instrument is reflexive analysis, the content of which is the reproduction of the enemy's probable goals, methods of achieving them, the logic of his thinking, and assumed methods of obtaining the necessary information about the situation. Reflexive analysis is a mirror of complex military thinking, which determines the degree of practically implementing a systemic approach and the basis of a creative approach to accomplishing the tasks assigned to commanders in combat.[180]

He adds that it is the information component that includes the transmission of information (a justification) to the enemy so that he makes a decision that satisfies the friendly commander's plan.[181]

Reflexive control techniques. These techniques are information-psychological effects; the formation and transmission of false information to make an enemy develop new goals and methods of operation; virus attacks on integrated information network domains; special software effects; and radio-electronic suppression of elements of the network infrastructure.[182] Knowledge of the enemy's concepts and doctrine are vital to success.[183] In this regard, military institutions should prepare military specialists for the use of reflexive analysis.[184]

Conclusions

The twenty or so areas listed above indicate the extensive reach of RC's use in Russian military thought. Two issues are important to remember when considering RC. First, there are various venues (computers, systems, space, deterrence, doctrine, etc.) that Russia employs to deceive an adversary. RC is not employed constantly everywhere, but its use should always be postulated and considered when Russian operations are examined. Second, it is important to stress that Russia understands how to think and process information like an opponent (or is learning to do so) and to focus on concepts of interest to him. Without the logic and vocabulary of enemy thought, Russian RC specialists would not know where, when, or how to insert specially developed information for the enemy consumer to digest, process, and act on according to a Russian plan.

The latter point is important for Western analysts to consider carefully. Trying to describe Russian actions by looking at its use of the grey zone or hybrid operations misses the point. Some good could come from looking at how Russia might utilize U.S. concepts, but the most important and useful way to look at Russian military or geopolitical operations is through the lens of their concepts and vocabulary, that is, look at their use of terms like equal security, forms and methods, reflexive control, trends, new-type warfare, strategy (it is different than the U.S. definition of strategy), information-technical and information-psychological aspects of information war, and so

---

[179] Ibid., pp. 51-52.
[180] Ibid., p. 53.
[181] Ibid., p. 54.
[182] Ibid., p. 52.
[183] Ibid., p. 53.
[184] Ibid., p. 54.

on. It is important to define these terms and address how they might be used. As President Putin said, “Listen to us now.” We need to do this better if we are to understand their intentions and goals. And if we do, Putin may be surprised by what we find out and by how we intend to put such knowledge to use.

5 Russia's Asymmetric Concept: Based on Military Art, Geopolitics, and Risk

> I must say that our defense spending is a tiny one-twenty fifth of that in the United States. But we have given thought, of course, as to how to maintain our national security. Our responses will be highly effective and asymmetric—President Vladimir Putin, 2007[185]

Introduction

For the past few years, US analysts have been writing extensively about Russian hybrid warfare tactics. Finland even has developed a hybrid warfare institute. Russia's military, on the other hand, has only tangentially admitted to using hybrid techniques, equating the concept most often with Russia's "new-type" warfare method. The term hybrid, in fact, is placed in parenthesis behind the term new-type in articles, implying its secondary role in importance. Even General Staff Chief Valery Gerasimov, as late as 2017, stated that it was too early to call Russian techniques "hybrid."[186] Instead, Russia states that it is the West who uses this US-developed concept against Russia.

Western fascination with hybrid topics has diverted attention away from other Russian military concepts that remain in use. One that has appeared often since the 1990s is asymmetric operations. Since the demise of the Soviet Union, Russia has considered itself as the weak opponent to US military superiority. Asymmetric operations have become their counteraction as a result. In 2004, for example, retired Major General Vladimir Belous noted that studies show how asymmetric measures are preferable in terms of cost-effectiveness. He offered three missile defense countermeasures: improving strategic offensive arms (such as the capability to maneuver in the boost phase); developing new methods of employing these arms (use of shallow trajectories or decoys); or finding new means and methods of delivering strikes against enemy missile defense system facilities (such as blinding reconnaissance systems).[187]

More contemporary asymmetric counters include technical developments, the suggestion of the preemptive use of strategic missiles,[188] the employment of military art (surprise, mass, deception, etc.), the placement of specific weapons in geolocations outside of Russia (Cuba, Venezuela), the exploitation of target density factors (power plant locations in Europe),[189] and the use of prohibited weapons,[190] among other measures. All such actions were specifically stated to be "asymmetric."

This chapter focuses on Russia's use of asymmetric thought. It will first define the topic along with the terms military art and risk. It will then offer how the concept would be understood as an

---

[185] No author or title provided, *ITAR-TASS* (in English), 1 February 2007.
[186] See, for example, Dr. Harold Orenstein, "Contemporary Warfare and Current Issues for the Defense of the Country," *Military Review*, November-December 2017, pp. 22-27.
[187] Vladimir Belous, "This Is What I Think: The Answering Move: How Can the American 'Star Wars' Be Nullified?" *Labor*, 22 December 2004.
[188] See, for example, Viktor Yesin, "If the Americans Nevertheless Begin Deploying Their Missiles in Europe, Nothing Will be Left for Us to Do Than Reject Launch on Warning Doctrine and Go to a Preemptive Strike Doctrine," *Weekly Star*, 8 November 2018.
[189] E. N. Akhmerov, N. F. Kravchenko, and I. I. Sobchenko, "On the Direction of Regional Nuclear Deterrence," *Voennaya Mysl'* (*Military Thought)*, No. 4 2000.
[190] N. N. Tyutyunnikov, *Military Thought in Terms and Definitions, Voennaya Mysl'* (*Military Thought)*, Volume Three, page 29. The author wishes to thank Dr. Harold Orenstein for his translation of this section from Russian to English.

operation and a form and method of Russian military thought and logic.[191] That discussion will be followed by several examples of asymmetry's contemporary use over the past decade, to include its use as a geopolitical tool. Many of these assessments are made not only by the Defense Ministry but also by people in the Kremlin, to include President Putin and even accountants (who look for cheap, asymmetric counters).[192]

Definitions of Asymmetry, Military Art, and Risk

In general, asymmetric actions are those that are unexpected and dependent on the exploitation of vulnerabilities in an opponent's situation. Military art's principles (surprise, mass, deception, etc.) are often used as key elements in the development of an asymmetrical operation. Risk relies on a leader's assessment of a situation. Each time an asymmetric operation is planned, it contains elements of risk (will surprise work? Will an opponent take "the bait" of a deception operation, and so on).

In 2018 the popular Russian military journal *Military Thought* issued a three-volume set of terms. It offers the most recent examples of how terms are defined and understood by Russian military leaders. The three-volume set of terms stated the following regarding asymmetric operations, military art, and risk. Only short, cryptic summaries of these definitions from the terminology set are offered, as some definitions covered two or three pages (the longer explanation of asymmetry is offered at Appendix A):

- Asymmetric operations: strategy of the struggle of a weak side against a strong one. It is a strategy employed most often for conflicts between enemies' unequal with respect to economic development or the level of military force. [193]
- Military Art: a sphere of theoretical-practical action that applies creative knowledge to concrete situations using creative thought, organization, principles, and will. [194]
- Risk: the existence of a situation or the possibility of a situation arising where prerequisites are formed (potential accrues) to counter the realization of national values, interests and goals, and safeguarding of national security.[195]

The latter definition offers that a country (system, ideology, etc.) is at risk when conditions arise, either internally or externally (implied but not stated outright in the definition) that are contrary (possibility of loss) to national values, interests, goals, and/or national security. Putin's risky decision to acquire Crimea fits these criteria.

---

[191] For a discussion of Russian forms and methods of military thought, see Timothy Thomas, "Russia's Forms and Methods of Military Operations," *Military Review*, May-June 2018, pp. 30-36.

[192] For reference purposes only, a very short history of the term "asymmetric" from various sources from 1998-2007 is attached after the conclusion section in Appendix A as A.1, along with a more extensive definition of the term asymmetric from a 2018 source at A.2, and a more extensive definition of disorganization at A.3.

[193] N. N. Tyutyunnikov, *Military Thought in Terms and Definitions, Voennaya Mysl'* (*Military Thought)*, Volume One, Armed Forces of the Russian Federation, 2018, p. 29. This definition and the next two (FTN's four and five) were translated by Dr. Harold Orenstein.

[194] N. N. Tyutyunnikov, *Military Thought in Terms and Definitions, Voennaya Mysl'* (*Military Thought)*, Volume One, 2018, pp. 156-157.

[195] N. N. Tyutyunnikov, *Military Thought in Terms and Definitions, Voennaya Mysl'* (*Military Thought)*, Volume One, 2018, p. 88.

Where Do Asymmetric Operations Fit in Russian Military Thought?

An operation is defined as an aggregate of battles, engagements, strikes, and maneuvers linked in objective, task, place, and time.[196] Thus an asymmetric operation would probably represent only one element of an overall operational plan. A predominant Russian military analytical format is to then further examine the forms and methods of developing and implementing an asymmetric operation. This methodology is used to analyze not only asymmetric operations but also artillery, cyber, aerospace, and other military operations. O. V. Korol and N. L. Romas noted that a form describes the organization of a combat action. It is how operations, engagements, combat, and strikes are organized to conduct a mission, whether it be offensive, defensive, or asymmetric.[197] M. G. Valeyev and N. L. Romas defined a method of warfare as a specific way that troops accomplish their mission by employing actions characteristic of a method's essence or combining processes, techniques, and rules of their use. They noted that troop armaments (i.e., weapons) and the principles of military art are the greatest components of methods.[198] Asymmetric operations would thus be a concept that is expressed via a form (organization) and method (specific weapons or use of the principles of military art) to conduct such an operation. An asymmetric organization (form) could be a nonmilitary one. An asymmetric weapon could be a prohibited one. An asymmetric use of military art could be its use as a reflexive control tool (to get an adversary to do something for themselves that they are actually doing for their opponent through the use of deception or some other means).

Sources of Asymmetry

In general, for all nations, the development of asymmetric thought relies on an adequate understanding of the vulnerabilities inherent in how an opponent thinks and formulates decisions as well as its national interests. It also relies on a nation's understanding of the evolving nature of military and nonmilitary operations in the information age and the vulnerabilities therein. These vulnerabilities can be exploited through the creative use of geopolitics, science, military art, and other sources.

Only four examples of potential sources of Russian asymmetric thought are offered here, surprise, system warfare, disorganization, and indirect operations. Many more clearly could be offered. Surprise is an element of military art. System warfare is an acknowledgment in Russian thought that warfare, having evolved, is no longer force on force but system on system. Disorganization is a current topic under discussion in Russian periodicals that involves the ability to cause chaos in an opponent's command and control capability. Indirect operations are often linked with asymmetric operation. If an operation is not direct, its asymmetric offset would be an indirect operation.

- *Surprise*: In 2018 V. V. Andreev wrote on the use of surprise to achieve military goals. A principle of military art, surprise can cause changes in opposing force potentials through unexpected attacks. It can cause panic in an opposing force and take the initiative from him. Surprise is an asymmetric option that can allow a weaker force to defeat a stronger one. It requires the proper use of decisiveness, timeliness, continuity, and initiative. Spatial and geographic factors also play

[196] N. V. Ogarkov, Main Editor, *Military Encyclopedic Dictionary*, Moscow: Military Publishing House, 1983, pp. 514-515.
[197] O. V. Korol and N. L. Romas, "Form of Military Actions: On the Meaning of the Category," *Voennaya Mysl'* (*Military Thought)*, No. 3 2008, pp. 149-153.
[198] M. G. Valeyev and N. L Romas, "Choosing Methods of Warfare," *Voennaya Mysl'* (*Military Thought)*, No. 6 2010, pp. 4-8.

important roles in how surprise is administered. Six basic methods for administering surprise were listed:

- The unexpected method for delivering the strike
- The covertness of strike preparations
- The unexpectedness of the time of the strike
- Disinformation
- The unexpectedness of the place at which the strike is delivered
- And the uniqueness of the weapons employed.[199]

Using the concept of reflexive control (without naming it), Andreev noted "it is necessary to impose on the enemy one's own state-of-the-art methods for creating conditions for surprise operations."[200] Surprise can manifest itself not only in fire destruction capabilities but also in a state's functioning systems, such as the diplomatic, economic, information, and cyber spheres. It is conditioned by the "development of the concept of 'new forms of warfare.'"[201]

- *System Warfare*: In the early days of the new millennium, Russian officers wrote often on the thought that warfare would no longer be fought just force on force. Their observation of US actions in Iraq and Afghanistan justified this concern and caused a revolution in military thought in Russia, where the focus shifted to system on system battles in space. Former General Major Viktor Ryabchuk, discussing combat systems, stated that even though there may be significant differences between combat systems of opposing sides, the less developed systems can contest successfully with a superior opponent if it possessed either greater organizational characteristics or greater functionality.[202] These functions, Russian authors believed, could now be accomplished via asymmetric or indirect means using signals or electronic warfare means or even diplomatic or information means (cyber) to contaminate or disorganize such systems.

- *Disorganization*:[203] Disorganization is a very important means of employing an asymmetric operation. For example, in June 2018, an article noted that the Russian Navy may damage unprotected US underwater communication cables, which could lead to wide-scale disorganization.[204] Such an act of sabotage would be an asymmetric method of attack instead of just using a strike operation on a communication site. Two Russian authors who have written extensively and professionally about military thought are S. G. Chekinov and S. A. Bogdanov. In their work, which has been quoted extensively by Western analysts over the past decade, they reference the disorganization concept often:

---

[199] V. V. Andreev, "Surprise as an Aspect of Achieving Goals in an Armed Confrontation," *Journal of the Academy of Military Science*, No. 2 2018, pp. 58-59. The author wishes to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[200] Ibid., p. 60.
[201] Ibid.
[202] Victor Ryabchuk, *The Theory of Managing Conflict*, Moscow: Science Press, 2002, pp. 48-49. The author would like to thank Dr. Jacob Kipp for this citation.
[203] For an entire article on Russia's disorganization concept, see Chapter Six.
[204] Aleksey Ivanov, "Russian Navy May Deprive the United States of Communications," *Russian Newspaper Online*, 22 June 2018.

- Experience gained in local wars and armed conflicts in the past few decades shows that strategic information confrontation has a major role in disorganizing military control and state administration…[205]
- The aggressor will take every possible measure to prevent retaliation by the defender and avail himself of the early hours of aggression to disorganize the defender's air force and air defense system.[206]
- A strategic information standoff is important for disorganizing military and state governance and systems of military aerospace defense, fooling an adversary, creating the desired public opinion…[207]
- …the new Military Doctrine also lists the chief internal military dangers for the Russian Federation. These include activities aimed at violent change of the constitutional system in the Russian Federation, destabilization of the internal political and social situation in the country, and the disorganization of the work of state government infrastructure of the Russian Federation.[208]
- The essence and content of information warfare thus consist of the Armed Forces using information, computer, and telecommunications technologies as a means of suppressing the adversary in war by disorganizing its command and control, bringing chaos into the work of its computer centers…misinforming and morally and psychologically crushing the adversary army personnel and population.[209]

The definition of disorganization, from a 2018 *Military Thought* source, is listed at the end of this document as Attachment Three.

- *Indirect operations*: This concept is often associated with asymmetric operations. For example, in Chekinov and Bogdanov's article on military strategy, they used the term indirect ten times, with seven of the ten paired as "indirect and asymmetric operations."[210] The pairing was used once in Russia's 2014 Military Doctrine and in three of the six presentations that General Staff Chief Valery Gerasimov made at the Academy of Military Science (2013, 2014, 2016). Chekinov and Bogdanov wrote an entire article on indirect operations, stating that it displays a great variety of forms and methods of indirect military and nonmilitary actions and means, such as information and remote/noncontact confrontations. In fact, the emphasis on nonmilitary operations implied that indirect operations were closely associated with them. Strategic information confrontations, they noted, can disorganize military

[205] S. G. Chekinov and S. A. Bogdanov, "Asymmetric Actions to Ensure Russia's Military Security," *Voennaya Mysl'* (*Military Thought),* No. 3 2010, p. 20.
[206] S. G. Chekinov and S. A. Bogdanov, "The Character and Content of a New Generation War," *Voennaya Mysl'* (*Military Thought)*, No. 10 2013, p. 22.
[207] S. G. Chekinov and S. A. Bogdanov, "The Art of War at the Beginning of the 21st Century: Problems and Opinions," *Voennaya Mysl'* (*Military Thought)*, No. 1 2015, p. 42.
[208] S. A. Chekinov and S. A. Bogdanov, "Particular Features of the Military Security of Russia in the 21st Century in Conditions of Globalization," *Voennaya Mysl'* (*Military Thought)*, No. 6 2016, p. 47.
[209] S. G. Chekinov and S. A. Bogdanov, "The Evolution of the Essence and Content of Understanding War in the 21st Century," *Voennaya Mysl'* (*Military Thought)*, No. 1 2017, pp. 37-38.
[210] S. G. Chekinov and S. A. Bogdanov, "Military Strategy: a Look into the Future," *Voennaya Mysl'* (*Military Thought)*, No. 11 2016, pp. 12-13.

and state control, deceive the enemy, and create the desired public opinion.[211] Also discussed were psychological, climate, and biological weapons.[212]

Russian Military Asymmetric Thought in Action: The Past Decade

In 2008 there were several references to asymmetric operations in the military press. A Strategic Missile Troop representative noted that a defense system must be asymmetric—in particular, it must be able to achieve a reduction in a friendly missile's signature and cloud the predictability of a warhead's trajectory.[213] General of the Army Makhmut Gareyev, at age 95 (in 2018) still the President of the Academy of Military Science, wrote on strategic deterrence in 2008, noting that answering threats requires not direct but rather asymmetric measures united by a common goal and concept of actions.[214] In addition to such military examples of asymmetric thought, there were several geopolitical references to asymmetry in 2008, some of which have relevance to Russian actions today. One reference was about an asymmetric response to the deployment of US missile defense components in Poland and the Czech Republic. Russia's asymmetric counter was to place S-300 air defense missile systems in Venezuela,[215] which has reappeared as a potential location for Russian bombers in 2018. A second geopolitical reference listed sixteen areas where Russia could conduct patrols and exercises or deploy equipment, such as bombers or air defense equipment.[216] There were recommendations to place Iskander missiles in Kaliningrad and Belarus, which would serve as another type of asymmetric response to the Czech and Polish based Western systems.[217] Some Russian authors stated that the nation's innovation and intellectual technology superiority were asymmetric counters to developments in other nations. Such asymmetrical developments are usually short-term and somewhat demonstrative in nature, the authors noted, since they can often be offset by one of the warring sides with an analogous system. This requires the efficient use of resources and the acceptance of a certain degree of risk.[218] Finally, Duma member Andrey Kokoshin noted that an asymmetric response must be an integration of a political-military, political-psychological, and military-technical nature. Kokoshin stated that A. A. Svechin's work on asymmetric strategies in different historical periods (which means the concept was discussed in the 1920s in Russia) and the work of Chinese strategist Sun Tzu played important roles for him in forming his "ideology of asymmetry," which was not defined further.[219]

In 2010 an *Interfax* Online article quoted a Military Academy deputy head, who said Russia would be building a global information and communication space for its Armed Forces. The system would be considered as an asymmetric counter to the US's network-centric warfare concept.[220]

---

[211] S. G. Chekinov and S. A. Bogdanov, "The Influence of Indirect Actions on the Character of Modern Warfare," *Voennaya Mysl'* (*Military Thought)*, No. 6 2011, p. 6.
[212] Ibid., pp. 11-12.
[213] Pavel Sergeyev, "Asymmetric Launch," *Lenta.ru*, 29 August 2008.
[214] M. A. Gareyev, "Strategic Deterrence: Problems and Solutions," *Red Star*, 8 October 2008.
[215] Yelena Pavlova, "Now that the Swans Have Returned, Peter is Sailing to Venezuela," *Moscow Komsomol (literally Young Communist League)*, 23 September 2008.
[216] Vladimir Kozhemyakin, "Caribbean, Iran, and the Caucasus—Three of the Most Painful Calluses for the US," *Arguments and Facts*, 17 September 2008.
[217] No author or title provided, *RIA-News*, 7 November 2008; and Vadim Mamlyga, "A Military Analyst's Notes: You Have the Floor, Mr. Iskander. 'Asymmetric Response' to the American BMD System," *Flag of the Motherland*, 16 December 2008.
[218] Vladimir Yuryevich Korchak, Aleksandr Vasilyevich Leonov, Igor Leonidovich Borisenkov, and Aleksandr Dmitriyevich Yurin, "There Is a Need for a Qualitative Quantum Leap in the Field of Weapons Development. Rearmament Becomes Vital for the Russian Federation Armed Forces Today," *Air-Space Defense*, 10 November 2008.
[219] Vladimir Sharonov, "Behind the Scenes of Politics: How Anti-SDI Was Born," *Red Star*, 29 October 2008.
[220] No author or title provided, *Interfax-AVN Online*, 22 December 2010.

However, the most important 2010 discussion of asymmetric operations was conducted on the pages of the journal *Military Thought*. Authors S. G. Chekinov and S. A. Bogdanov wrote what, in this author's opinion, is the most extensive description of Russian thinking about asymmetric operations. Their outline of asymmetric warfare templates closely resembles the military actions that Russia and President Putin have developed for the modern era to protect the military security of the Motherland. They defined the asymmetric approach in the following manner:

> It is the total of the forms and methods of employing forces and assets based on the sides' non-identical capabilities, which makes it possible to avoid (diminish the consequences of) a confrontation or a direct armed clash with a potential adversary…asymmetric operations in the military sphere may include:
>
> - the implementation of measures that induce apprehension in the opposing side concerning the intentions and retaliatory steps of the Russian Federation;
> - demonstration of the readiness and capabilities of a Russian Federation troop (force) grouping in a strategic sector to repel an invasion with consequences that are unacceptable for the aggressor;
> - and operations by troops (forces) to deter a potential adversary that envisage the guaranteed engagement of his most vulnerable military and other strategically important and potentially dangerous facilities with the aim of convincing him of the futility of an attack.[221]

Of interest is that the topic of "forms and methods" (outlined above) was used at least six times in the article.

Today the concept of globalization reflects the growing interdependence of nations and people, indicates that other security types, especially nonmilitary ones (political, economic, information, etc.), are now more actively used.[222] The strategy of the indirect approach, which is closely aligned with asymmetric operations, is characterized by the multiplicity of forms and methods of military operations that are employed, such as information, remote or noncontact confrontations, or electronic-fire or antisatellite operations. Some operations mislead or surprise opponents while others intimidate or undermine their authority. Information influence operations can now perform strategic missions, to include disorganizing military and state command and control systems. To ensure the security of the Russian Federation the country must undertake "asymmetric measures that must be of a systemic, comprehensive nature, combining political, diplomatic, informational, economic, military, and other efforts.[223]

Asymmetric relationships are paradoxical in nature in that the weak can impart damage to the strong via the use of nonmilitary actions or through the exploitation of vulnerabilities in a stronger opponent. Asymmetric operations can be unpredictable, since they can rely on the use of prohibited means. They can also project the inability of a stronger side to defend a position against a weaker yet innovative opponent.[224]

Another important aspect of asymmetric operations is that the success of a military campaign can depend on the interaction of military and nonmilitary factors and not just the coercive potential of two opposing sides.[225] The authors note that:

---

[221] S. G. Chekinov and S. A. Bogdanov, "Asymmetric Actions to Ensure Russia's Military Security," *Voennaya Mysl'* (*Military Thought),* No. 3 2010, p. 21.
[222] Ibid., pp. 14-15.
[223] Ibid., p. 20.
[224] Ibid., p. 16.
[225] Ibid., p. 17.

> In contemporary conditions, asymmetric operations are characterized by the qualitative difference in the employment of new (nontraditional) means of armed struggle and the forms and methods of waging that struggle on the part of both (weak and strong) contending sides, and also by their identification of military campaign end goals entirely opposite to those declared.[226]

The authors ended their article on an ominous note, describing the application of asymmetric operations based on precision-guided munitions along with the use of sabotage and reconnaissance teams to a European environment. This would create the prerequisites to compel an adversary to cease operations on terms favorable to Russia. Targets could include European economic facilities and other types of infrastructure important for the population's survival. This could include state or military command and control installations, industrial enterprises, the fuel and energy sectors, critically important communications facilities, and installations posing a significant hazard (dams, nuclear power stations, chemical plants, etc.).[227] The combination of direct and asymmetric means was explained as follows:

> Hence, outright military measures to protect Russia's national interests and avert and repel possible aggression have to combine both direct (symmetric) operations envisaging the preparation and staging of operations with the categorical goals of defeating an adversary's invading troop (force) groupings, and the realization of asymmetric measures whose essential content may consist of inflicting unacceptable damage on him in other (nonmilitary) spheres of security.[228]

In 2012 President Putin stated that to counter the US's missile defense project, Russia will "either need to create missile defense for ourselves or give some kind of asymmetrical response."[229] Setting up a missile defense response would be expensive and whether it would actually work would require real-world testing (risk!). Therefore, Putin added, Russia will reinforce its air defense forces and the air defense systems around Moscow and the strategic forces bases. It will also build new tracking stations and create "such systems for which US missile defense systems will be no hindrance."[230] Priorities he listed were "strategic nuclear forces, Aerospace Defense Troops, aviation, space systems and complexes, and reconnaissance, electronic warfare, communications, and automatic control systems."[231] A more distressing 2012 article, composed by a Russian Major General, stated that one of the types of asymmetric actions that the Russian Armed Forces might employ would be preemptive strikes using highly effective and accurate weaponry against critically important objects whose destruction would lead to a loss of stability in an enemy state.[232]

In 2013, writing about the nature of a new-generation war, Chekinov and Bogdanov stated that asymmetric actions will help eradicate an enemy's superiority through the use of indirect actions and nonmilitary measures. This approach will rely on attaining information superiority to help enable these actions and measures.[233] In a speech at the Public Council of the Military-Industrial Commission, General Gareyev underscored the following:

---

[226] Ibid., p. 19.
[227] Ibid., pp. 21-22.
[228] Ibid., p. 22
[229] No author or title provided, *Interfax*, 22 February 2012.
[230] Ibid.
[231] Ibid.
[232] Aleksandr Tsymbalov, "Mission to Attain Strategic Mobility," *Air-Space Defense Online*, 14 May 2012.
[233] S. G. Chekinov and S. A. Bogdanov, "On the Character and Content of a New-Generation War," *Voennaya Mysl'* (*Military Thought)*, No. 10 2013, p. 17.

> With the comparative weakness of our economic potential, it is desirable to place the main emphasis on asymmetric means and methods of actions. We know, for example, that the present-day leading states accomplish communications, navigation, reconnaissance, and all command and control of strategic nuclear, missile defense, and precision-guided munitions through space. A breakdown of this entire systems by electronic and other asymmetric assets can largely reduce this advantage of the opposing defense.[234]

Russian Chief of the General Staff, Valery Gerasimov, noted in 2013 that the significance of asymmetric and indirect operations is increasing. He stated that military science's role includes "creating a holistic theory of asymmetric operations"[235] and that new forms and methods of fighting must include asymmetric and indirect actions.[236] Nonmilitary methods, Gerasimov stated, are new forms and methods of conflict. They may be expressed as political pressure, the use of economic sanctions, blockades of maritime, air, and land lines of communication, and in introducing international peacekeeping contingents under the pretext of the defense of human rights and humanitarian operations.[237]

In 2014 Gareyev stated in a speech at the Academy of Military Science that "due attention must be paid to the development of general-purpose forces," where the main emphasis must be placed on "asymmetric systems and methods of neutralizing the enemy's technological superiority."[238] Gerasimov noted at the same location that "Special attention must be devoted to the development of a comprehensive theory of indirect and asymmetric actions, carried out by various federal executive agencies based on a unified plan, in support of the preventive neutralization of threats to Russia's military security"[239] and, once again, that the changing nature of war includes the use of asymmetric and indirect operations.[240] Thus, in both 2013 and 2014, Gerasimov called for a comprehensive theory of asymmetric operations to be developed by researchers at the Academy.

In an extensive 2015 article outlining "new-type" warfare, then General Lieutenant Andrey Kartapolov, at the time the Chief of the Operations Directorate of the Russian General Staff, discusses asymmetric operations. He stated that nonstandard forms and methods are being developed for Armed Forces deployments. They will exploit the uncovering of vulnerable areas that offer the best effect with minimal expenditure of one's own forces and resources. These effects may include special forces operations, foreign agents, various forms of information effects, and political, economic, and other nonmilitary forms of activity. Each conflict requires a different set

---

[234] D. Rogozin, A. Zabrodsky, A. F. Ioffe, and M. Gareyev, "Defense Establishment: Strategic Goals of National Security: Military Science Must Forecast and Plan the Development of Arms and Military Equipment in the Spirit of the Times," *Military-Industrial Courier Online*, 2 August 2013.

[235] V. V. Gerasimov, "Principal Trends in the Development of Forms and Methods of Employing Armed Forces and Current Tasks of Military Science Regarding their Improvement," *Journal of the Academy of Military Science*, No. 1 2013, p. 26. The author wishes to thank Dr. Harold Orenstein for his translation of this article from Russian to English.

[236] Ibid., p. 25.

[237] Ibid.

[238] M. Gareyev, "Consistently Defending National Interests. In Forecasting the Nature of Future Armed Struggle, It Is Necessary to Look Boldly Forward but Not to Fantasize Too Much but Proceed on the Basis of Real Trends in the Development of Arms and Military Equipment," *Military-Industrial Courier Online*, 22 January 2014.

[239] V. V. Gerasimov, "The Role of the General Staff in the Organization of the Country's Defense in Accordance with the New Statue on the General Staff, Approved by the President of the Russian Federation," *Journal of the Academy of Military Science*, No. 1. 2014, p. 19. The author wishes to thank Dr. Harold Orenstein for his translation of this article from Russian to English. The author wishes to thank Dr. Harold Orenstein for his translation of this article from Russian to English.

[240] Ibid., p. 15.

of asymmetric operations that fit the logic at hand. They must be timely and coordinated, often utilizing various departments of a government's organization.[241]

Asymmetric operations are conducted with the aim of eliminating (neutralizing) enemy advantages while subjecting him to damage using minimal expenditures. He listed the principles of asymmetric operations as the following:

- Covertness of preparation for and conduct of operations;
- Persuasion of the weak side to use prohibited means to conduct military operations;
- Concentration of efforts against the enemy's most vulnerable locations (targets)
- Search for and exposure of the enemy's weak points;
- Imposition on the enemy of one's own variant (one's own will) for the course of the conflict;
- Low resources expenditure of asymmetric operations with respect to enemy actions.[242]

The end goal is the achievement of superiority or parity in the results of armed opposition.

In 2017, Gareyev noted that asymmetrical plans are designed to take advantage of ways to influence the opposing side. He stated that the main emphasis should "be placed on creating asymmetric means and methods of response. Attacking an opponent through space, for example, greatly lowers his advantages, since that is where many of them lie."[243]

In 2018 there were several references to asymmetric operations. In March Kremlin spokesman Dmitry Peskov noted that Putin, back in 2003-2005, stated that Russia would not count on symmetrical responses to US plans. Rather Russia would count on asymmetric responses, such as the development of attack systems that could overpower any missile defenses.[244] Russia's recent successful testing of its Avangard hypersonic system, capable of traveling at 20 times the speed of sound, attest to the type of attack weapons to which Putin was referring. Aerospace aircraft and systems, in another article, were listed as another asymmetric response. These orbital aircraft can freely change their orbit parameters and maneuver outside the visual range of an enemy's electronic systems. Such aircraft are reusable and economical, many times cheaper than launching a rocket booster.[245] Two other asymmetric responses were noted in 2018. First, a Ministry of Defense statement declared that domestic electronic warfare systems, which were highly effective in Syria, are now viewed as an asymmetric weapon for new-generation wars.[246] Second, one analyst noted that Russia had an asymmetric response to the US's network-centric warfare concept. That

---

[241] A. V. Kartapalov, "Lessons of Military Conflicts and Prospects for the Development of Resources and Methods of Conducting Them. Direct and Indirect Actions in Contemporary International Conflicts," *Journal of the Academy of Military Science*, No. 2 2015, pp. 35-36. The author wishes to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[242] Ibid, p. 35.
[243] M. Gareyev, "Mobilization of Minds: Our Leaders Must Have a Fundamental Change in Attitude Toward Science," *Military-Industrial Courier Online*, 29 March-4 April 2017.
[244] No author or title provided, *Interfax* (in English), 2 March 2018.
[245] Aleksey Leonkov, "Arms Room: Space Reconnaissance Is Seldom Bored or Left Idle. By What Means Can the Development of the 'Instrument' Proceed, Which Permits Us to Obtain Strategically Important Information Because of the Line of Sight Horizon at Distances, Which Exceed a Thousand Kilometers," *Weekly Star*, 5 December 2018.
[246] Aleksey Ramm and Bogdan Stepovoy, "The Army: To Pick Up the Trail: Sukhoi Aircraft Will Be Transformed into All-Seeing Reconnaissance Aircraft. Improved Electronic Warfare Complexes Will Increase the Effectiveness of Aerospace Forces' Operations in Combat Operations Areas," *Izvestiya Online*, 3 August 2018.

turned out to be simply Russia's National Defense Management Center or NDMC, which directed combat operations in Syria. Thus, the asymmetric issue is both conceptual and organizational, in this case. The NDMC was touted as the world's first unified system for managing all military subunits in the Russian Armed Forces. It is composed of three command and control centers, a Center for the Management of Day-to-Day Activities, a Center for Managing Special Issues (such as the Strategic Nuclear Force), and the Battle Management Center (which monitors the world military-political situation and analyzes and forecasts threats to Russia). A computerized "automated expert system for monitoring and analyzing the military-political, socioeconomic, and sociopolitical situation in Russia and the world became the nucleus of the NDMC."[247]

Conclusion

There are several items to which special attention should be paid in this discussion of asymmetric operations. First is Gerasimov's 2013 statement that a holistic theory of asymmetric operations is required along with new forms and methods for the use of indirect and asymmetric operations. He repeated this requirement in 2014. This clearly indicates that there was a concerted effort to develop this theory and how to use it. Analysts should be on the lookout for the theory's further development. Second is the apparent similarity among the terms asymmetric, indirect, and nonmilitary, terms that the major military figures in Russia all use. All three terms have been used interchangeably and appear to be one and the same at certain times. Third is the continued reference to the term by not only military figures but also its attribution to Kremlin figures. Putin's official spokesman, Dmitry Peskov, noted in 2018 that Putin had said he would respond asymmetrically to US actions. Putin mentioned the use of asymmetric approaches in 2001, 2007, 2012, and 2018, so this is a topic that remains consistent with Kremlin as well as military thought. Fourth, it is important to keep in mind that the topics of military art and geopolitics often utilize asymmetric or indirect concepts. For example, military art can involve the use of deception, surprise, deployments, and other actions to offset adversary advantages or simply to create new advantages of their own. Geopolitics can be used to influence those leaders in opposition to US and NATO policies to place weapons and forces in their lands, especially those that border on or are near to Western borders.

The topic of risk was mentioned but not analyzed further. That is because risk is inherent in each of the operations mentioned above. Will an operation intended to surprise an opponent actually take the opponent by surprise or will the opponent discover the operation beforehand? Will disorganization actions work or could "friendly" (i.e., Russian) operations backfire when an opponent merely feigns disorganization? In most cases only adequate intelligence about an opponent's current understanding of a situation and their internal thought process will help minimize, but never eliminate, risk. The best recent example of geopolitical risk-taking was Vladimir Putin's 2014 operation to acquire Crimea. Putin noted that there was total chaos in Kiev with the expulsion of President Victor Yanukovych. Putin guessed correctly that the US would be leery of offering military assistance at that moment to a country that bordered Russia. Putin had warned against NATO expansion in both Georgia and Ukraine. Further, the US military was monetarily stressed and tired from its decade of conflict in the Middle East. With Russian forces already present in Crimea (Black Sea Fleet), he decided that there would be limited opposition to the movement of more Russian forces into Crimea.[248] His risky operation proved to be successful

[247] Aleksey Leonov, "Russian Armed Forces: Our Asymmetric Response to America's Netcentric Warfare," *Weekly Star*, 18 October 2018.
[248] Daniel Treisman, "Why Putin Took Crimea," *Foreign Affairs*, May/June 2016, p. 47.

and supported by the Motherland's population. The lesson to be learned is to better understand the Kremlin's risk calculus and thought processes, especially after Russia establishes or sees a strategic advantage that it can exploit.

It will be important for Western analysts to devote attention to Russia's use of asymmetric operations on the geostrategic chessboard. As this article has noted, it is one of several (new-type, hybrid, indirect, nonmilitary, etc.) concepts ascribed to Russia, but it is one that is long-standing and deserves some of the attention currently spent on hybrid issues. As Putin's spokesman noted in December 2018:

> Putin is a pragmatic man. He is pragmatic in global affairs and, importantly, in domestic issues. So symmetric answers can be given sometimes, they may cost a lot in some cases or cost less in others, but asymmetric answers are no less effective. I think the elaboration and fulfillment of Russia's asymmetric answers will not be long in coming.[249]

The West needs to open its aperture of creative thought and be prepared for some interesting and probably threatening Russian responses.

Finally, it is important to note that Russia attempted to put many resources together during the last US presidential election. It was able to influence voters, some believe, with a deluge of negative information about one of the candidates. Democracies worldwide must be on the lookout for such techniques as they move nearer to their next electoral process.

The warning is quite clear. Democratic constituencies must remain very skeptical about news reports from Russian sources in particular. They bank on persuading with perspective and not the truth. Mental barriers to such input must be developed for both citizens and governments to recognize the methodology of the construction of an objective reality that is based on fake news or facts taken out of context.

[249] No author or title provided, *Interfax* (in English), 21 December 2018.

6 Connecting GPS Interference with Russia's A2AD Concept

> …the resolution of problems of creating and maintaining superiority in forces and means on operational (strategic) axes at the required level is the main thing for achieving the goal of an operation. In connection with this, disorganizing a spatially distributed system of command and control of the enemy's operational reserve—reducing the tempo of his advance to the required level—becomes one of the key tasks…[250]

Introduction

From a Russian perspective, the title of this article is misleading. According to Russia's *Military Encyclopedia*, there is no Russian equivalent to the West's A2AD concept. This is a Western construct that suggests how Russia may deny access to its territory using its weapons and missiles in offensive or defensive operations against the West.

However, there is a Russian term/concept that describes a method for denying access to its territory. That term is "disorganization" and it is the topic of this article, especially as the term is applied to the disruption of C2 using radio-electronic warfare (REB) capabilities under circumstances such as GPS jamming. Disorganization is designed to disrupt elements of the information environment. The term C2D, which stands for command and control disorganization, will need to be better understood by Western analysts as a way for Russian forces to gain superiority in an A2AD standoff.

Recent Russian GPS jamming activities of aircraft in Norway and Finland are indicative of this effort to disorganize an opponent. Finnish Prime Minister Juha Sipila stated that "This is not a joke. The air safety of ordinary people is under threat," regarding GPS interference in Lapland during a recent NATO exercise. Norwegian authorities stated that the interference was carried out by the Russians.[251] Finnish Foreign Minister Timo Soini promised to provide a report to Parliament regarding Russia's alleged jamming.[252] At this time the disorganization is limited to aircraft, but Russian plans clearly focus on numerous command and control issues.

This article initially notes how the disorganization concept has risen in importance. It then divides the discussion into two parts. Part One discusses Russian use of the disorganization concept in Syria as well as Russian thoughts for its potential use against nation-states. Part Two examines several recent and important references to disorganization that have appeared in the work of Russian REB authors. The discussion also demonstrates how REB and kinetics are working together to win future confrontations.

Background

Very seldom have Western assessments of Russian capabilities focused on the disorganization concept, most likely because the concept has lurked quietly in the background. That appears to be changing. In mid-2017 the C2 discussion stated that a special disorganization subgroup needed to be created. By the end of 2017 REB authors stated that a "C2 Disorganization Plan" was now a part of REB planning. Whether the plan was the work of the subgroup is unknown, but the timing

---

[250] V. I. Stuchinskii, "Methodological Approach to Assessing the Effect of Disorganizing Command and Control by Operational Reserves at the Tempo of the Enemy Advance," *Voennaya Mysl'* (*Military Thought)*, No. 11 2016, pp. 43-49. The author wishes to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[251] No author or title provided, *Interfax* (in English), 12 November 2018.
[252] No author or title provided, *The Independent Barents Observer* (in English), 9 November 2018.

implies it is plausible. Further, the authoritative journal *Military Thought* published four articles with the disorganization concept in the title in 2017.

Russia's disorganization effort aims to disrupt/jam adversary C2 links, whether by soft (REB, cyber, etc.) or hard (physical destruction) means. The concept has been under discussion since at least the early 1990s.[253] Disorganizing an opponent's C2 can collapse his ability to coordinate and integrate nearly every aspect of his plans, whether it be logistic support, the use of fire support means, or his command over troops in the field. Disorganization successes lead to Russian decision-making superiority and chances of winning a conflict.

Western planners have mainly focused, for good reason, on what they see as Russian attempts to attain A2AD superiority with various types of weaponry. Missiles are usually portrayed with schematic arcs that denote their reach and thus ability to hit Western territory. The US Defense Intelligence Agency's (DIA) 2017 document *Russia: Military Power*[254] stated that Russian A2AD plans are accomplished using information operations (which appears closest in content to disorganization, since it focuses on information control), strategic air operations, integrated air defense systems, and modern precision strike capabilities. *The Economist*, in a January 2018 special report on "The Future of War," published a schematic of Europe overlaid with Russian missile arcs and the legend "Russia's anti-access/area denial capabilities."[255]

Russian theorists consider the West to be the aggressor (while denying that their actions in Crimea and Ukraine precipitated Western reactions) and, along with the use of missiles, have developed a disorganization plan to disrupt or attack C2 nodes to slow adversary logistic support, tempo of advance, and other activities. Since Russia can be expected to employ its missiles and disorganization concept in an integrated fashion, there remains much for analysts to consider about the shape of Russia's future war capabilities. Disorganization is a priority focus here.

Part One: Disorganizing Control: From Syria to Future War

A serious discussion is underway in Russia to define the disorganization concept, determine its goals, and establish likely targets of the C2 disorganization effort. Several articles published in 2017 offer a good description of the concept, to include a road map for its future development. However, the seeds of disorganization had been planted as far back as 1990 and interest in the concept continued in a variety of discussion forums. For example, two important military authors, S. G. Chekinov and S. A. Bogdanov, used the term "disorganize" in several of their articles since 2010.

In 2015 Russia entered combat with ISIS in Syria. A year later, *Military Thought* published an article on "Disorganizing the Command and Control of Illegal Armed Groups (IAG) during Counterterrorist Operations."[256] Russian combat experience and lessons learned in its recent wars in Chechnya indicated that blocking and annihilating illegal armed groups largely depended on the efficiency of disorganizing adversarial C2.[257] When the IAG commander was located with the control group, zonal electronic blocking was used. When the commander was located some

---

[253] See, for example, A. A. Anokhin, "New Forms and Methods of Adversary Troop and Weapons Command and Control Disorganization," *Scientific Collection*, No. 1, 1993. Further, a Russian information specialist told this author in 1996 that the key element behind information warfare was the ability to disorganize an opponent.
[254] *Russia: Military Power*, Defense Intelligence Agency, 2017, pp. 32-34.
[255] No author provided, "The Future of War," *The Economist Special Report*, 27 January 2018, pp. 5-6.
[256] S. A. Gritsenko, L. B. Ryazantsev, O. N. Sklyarova, and I. Yu. Cherednikov, "Disorganizing the Command and Control of Illegal Armed Groups during Counterterrorist Operations," *Voennaya Mysl'* (*Military Thought)*, No. 5 2016, pp. 22-27.
[257] Ibid., p. 22.

distance from the combat zone, both zonal and point electronic blocking were used or the annihilation of the commander was recommended using drones. The conclusion reached was that the disorganization of the function of IAG C2 bodies permitted the ability to disorient militants, demoralize them, and rapidly annihilate them.[258] Many of the same concepts will likely be used to confront larger opponents.

In another example, this time from 2016, a Russian officer noted the following when discussing command and control disorganization, tempo of advance, and correlation of forces issues:

> …the resolution of problems of creating and maintaining superiority in forces and means on operational (strategic) axes at the required level is the main thing for achieving the goal of an operation. In connection with this, disorganizing a spatially distributed system of command and control of the enemy's operational reserve—reducing the tempo of his advance to the required level—becomes one of the key tasks…[259]

Disorganizing enemy command and control at the initial stage of combat operations, it was noted, makes it possible to accelerate the accomplishment of tasks and goals. Radio-electronic destruction and aviation assets occupy lead positions in the resolution of tasks associated with disorganizing the command and control of operational reserves. When the volume of timely information is reduced, so is command and control efficiency and decision-making. Blocking information transmission channels by 40-60 percent can decrease the correlation of forces of the advancing side twofold, for example from a 6:1 to a 3:1 advantage.[260]

The disorganization topic was highlighted in Russian discussions in 2017. Four articles in the journal *Military Thought* are summarized here (with titles) in the order in which they appeared.

Military Thought (6/17): "About the Complex Defeat of an Enemy and the Methods of its Implementation during the Disorganization of Command and Control"

General Major S. I. Pasichnik wrote that to defeat an adversary, a major operational task is the disorganization of adversary control over its troops and weapons. The electronic and information boom of this century has offered new methods, apart from force, such as the use of electromagnetic radiation weapons to disable electronic assets. These weapons will be used in concert with traditional firepower and electronic damage, such as electronic suppression.[261]

Pasichnik believes the construction of a subgroup for "disorganizing adversary C2 bodies that should include officers who are experts in electronic and fire damage of the aggressor's information-driven systems in operations (combat actions)" is required.[262] To efficiently disorganize an opponent's C2, it is necessary to: compose the REB forces and assets required to defeat information-driven systems; define the tasks for electronic versus fire damage coordination; devise temporal models for comprehensive damage to specific adversary systems; and elaborate approaches to assess the comprehensive damage to these systems.[263]

---

[258] Ibid., pp. 24-27.
[259] V. I. Stuchinskii, "Methodological Approach to Assessing the Effect of Disorganizing Command and Control by Operational Reserves at the Tempo of the Enemy Advance," *Voennaya Mysl'* (*Military Thought)*, No. 11 2016, pp. 43-49. The author wishes to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[260] Ibid.
[261] S. I. Pasichnik, "About the Complex Defeat of an Enemy and the Methods of its Implementation during the Disorganization of Command and Control," *Voennaya Mysl'* (*Military Thought)*, No. 6 2017, pp. 38-42.
[262] Ibid., p. 42.
[263] Ibid.

Military Thought (8/17): "On the Issue of Disorganizing the Command and Control of Troops (Forces) and Weapons"

The authors of this article believe that the *Strategic Rocket Forces Military Encyclopedic Dictionary* defined the command and control of troops best:

> Command and control of troops is the purposeful activities of commanders (chiefs), staffs, and other command and control organs regarding the guidance of subordinate troops by means of working out and organizing the execution of control actions (decisions) and specifying tasks to subordinates and the sequence and methods of accomplishing them, ensuring the most effective realization of the potential capabilities of troops for accomplishing assigned tasks of preparing for and conducting combat operations.[264]

Command and control tasks must consider assessments of information about the situation and forecasts of potential changes to troop actions, as well as controlling and analyzing the accomplishment of assigned tasks. Information, computers, means of storing information, automated C2 systems, and telecommunication systems comprise the technical basis of C2 systems.[265]

The authors wrote that a C2 system is the object of disorganization, leading to the following definition:

> The disorganization of command and control is a process aimed at the disruption of the functioning of a command and control system or its elements, leading, in fact, to a state of disorganization of command and control that does not allow for the effective accomplishment of assigned tasks by troops.[266]

Disorganization requires an appreciable C2 breakdown. Three types were listed: collapse (enemy loses C2 of troops, and friendly effectiveness is above 0.7); disruption (disorganization only periodically lost, effectiveness is less than 0.7 but more than 0.4); and impediment (information exchanges are reduced but loss of C2 does not occur, effectiveness is more than 0.2 but less than 0.4). If the effectiveness of the disorganization is less than 0.2, then the adversary's system is still considered stable. Using these criteria, another way to measure the disorganization of enemy command and control of troops and weapons is "the totality of coordinated measures and actions aimed at the substantive reduction of the capabilities or full cessation of the functioning of his organs and technical resources for command and control of troops and weapons."[267]

Disorganization aims to impede C2 organs from obtaining information, or distorting said information; reducing the timeliness and quality of decisions; and impeding C2 action transmissions. The authors added that killing an opposing side's commander and his staff is the best way to assure disorganization. Disorganization targets include: decision-makers, command posts, information resources about the situation, automated C2 systems and their software, information transmission resources, and telecommunications channels. Fire destruction, REB interventions, software and hardware effects, and disinformation can cause disorganization.[268]

---

[264] Iu. E. Donskov, A. L. Morarescu, and V. V. Panasiuk "On the Issue of Disorganizing the Command and Control of Troops and Weapons," *Voennaya Mysl'* (*Military Thought)*, No. 8 2017, pp. 19-20. This quote from the *Rocket Forces Encyclopedia* was on page 548 of the encyclopedia. The author wishes to thank Dr. Harold Orenstein for his translation of this article.
[265] Ibid., p. 20.
[266] Ibid., p. 21.
[267] Ibid.
[268] Ibid., pp. 22-23.

The adversary's hierarchy C2 structure also can be disorganized by "fragmentation," such as eliminating elements of the information management system. Fragmentation can be selective, paired, or group oriented using any of the methods described above. The goals of fragmentation include the physical elimination of decision-makers from the C2 process, isolating them from information, or blocking REB or information that serve decision-makers. The authors noted that there is no planning document to disorganize enemy C2, and that a disorganization plan needs to be developed for subsequent versions of regulation documents.[269]

Military Thought (9/17): "On the Provisions of Troop (Forces) Command and Control Disorganization Theory"

This article discussed C2 disorganization theory. A C2 systems efficiency under various forms of influence (such as electronic, fire, or electromagnetic) was examined for weaknesses and places to introduce disorganization methods. C2 disorganization can result in C2 superiority for Russian forces and the ability to influence operations. It was noted that "in the coming years gaining superiority in C2 will become the principal task of troop groups in operations."[270] The theory is not mature yet, the authors state, since it still requires the development of basic concepts, disorganization assets, forms and methods, a place in the military science structure, and a methodology for C2 disorganization efficiency assessment. The theory should eventually become an independent part of operational art and tactics, since the C2 disorganization effort is "defined as a principal task for troops, whose performance is an indispensable prerequisite for obtaining success in carrying out other operational (tactical) tasks."[271] Disorganization's goal is to reduce "or totally exclude its [C2's] functioning according to its inherent purpose," thereby reducing adversary C2 capabilities "of implementing controlled combat potential of troops or a military formation."[272] Disorganization efficiency can be classified as sustainable, hindered, disturbed, or undermined.[273]

C2 disorganization targets are automated control systems or information-driven systems. Three disorganization methods are isolation, division, and severance.[274] Isolation distorts the operational (tactical) group's interaction among elements of its operational order of battle. Division reduces strike and fire potential by distorting interactions among service arms and task forces. Severance reduces firepower or striking force by distorting the interaction inside a functionally homogeneous group of forces.[275]

Military Thought (11/17): "Determining the Methods for Disorganizing Enemy Command and Control of Troops and Weapons"

This article discussed methods to disorganize command and control. Initially enemy actions must be clarified. A descriptive model of an enemy's C2 is then made, examining execution elements and processes, tactical tasks, critical C2 organs in an adversary's process, and elements of information support. The model supports a disorganization plan against specific directions that the enemy might take in executing tasks and helps in the administration of fire control guidance against

---

[269] Ibid., pp. 23-25.
[270] A. N. Klyushin, D. V. Kholuyenko, and V. A. Anokhin, "On the Provisions of Troop (Forces) Command and Control Disorganization Theory," *Voennaya Mysl'* (*Military Thought)*, No. 9 2017, pp. 65-69.
[271] Ibid., p. 66.
[272] Ibid.
[273] Ibid., p. 67.
[274] Ibid., p. 68.
[275] Ibid., pp. 68-69.

enemy C2. Temporal changes in the tactical situation influence which effects are chosen.[276] A determination is made of the minimum number of objects to be affected by fire destruction and the use of REB. Three methods are used to "fragment" enemy C2: single (one C2 organ is selected); paired (two C2 organs selected); and group (three or more organs selected). The type of effects selected help designate the forces and means to be used. Principle disorganization methods include radio-electronic blockades of C2 organs and radio-electronic blocking of information support elements. Proper resources are then allocated to accomplish disorganization's goals.[277]

Part Two: REB and Disorganization

REB has become a major method to deny communications and information to opponents and to disorganize them. REB Chief General-Lieutenant Yuriy Lastochkin, for example, mentioned REB's ability to disorganize adversary troops and weapons eight times in a 2017 article.[278] Lastochkin and two other authors described how operational art is developing in conjunction with improvements in weaponry and ways to conduct combat. Capabilities, it was noted, have always determined methods. Weapon improvements have resulted in new operational tasks for REB and allowed the force to both disorganize adversary troops and weapons and repulse aerospace attacks.[279] Destroying circuitry, distorting or destroying information, or simple electronic suppression all contribute to the C2 disorganization effort.[280]

Several other REB articles in 2017 and 2018 in *Military Thought* referred to the disorganization concept but not always directly to the issue of C2. For example, REB specialists were instructed on how to confront adversary UAVs and robots with new tasks and disorganization methods. Tasks involved organizing ground and airborne REB forces and assets along with special software to disorganize UAVs and robotic control. This requires that REB specialists understand a potential adversary's UAVs and robots, their characteristics and employment methodologies, purpose of equipment functions, control systems, REB assets, and guidance systems. Equally important is understanding Russian methods to employ such assets to disorganize adversary systems.[281] One discussion noted that what merited scrutiny was the specific content of the "Plan of Disorganizing Adversary Troop Control."[282]

REB assets are now designed to carry out the operational task of "adversary control disorganization."[283] In the past the use of fire operations and force characterized disorganization control, but now intelligent disorganization methods, such as "software impact complex weapons," have started to appear more often.[284] It appears that with REB's new status as an arm of the service,

---

[276] P. V. Kaminsky, "Determining the Methods for Disorganizing Enemy Command and Control of Troops and Weapons," *Voennaya Mysl'* (*Military Thought)*, No. 11 2017, pp. 33-34. The author wishes to thank Dr. Harold Orenstein for his translation of this article.
[277] Ibid., pp. 34-35.
[278] Yu. Lastochkin, Yu. Koziratsky, Yu Donskov, and A. Mororescu, "Combat Employment of EW Forces as an Element of Ground Forces Operations," *Voennaya Mysl'* (*Military Thought)*, No. 9 2017, pp. 18-25.
[279] Ibid.
[280] Ibid., p. 24.
[281] S. V. Golubev, S. V. Plotnikov, and V. K. Kiryanov, "Training EW Specialists to Counter Foreign Armies' Unmanned Aerial Vehicles and Robotics," *Voennaya Mysl'* (*Military Thought)*, No. 4 2017, pp. 74-80.
[282] Yu. L. Koziratsky, A. L. Morarescu, and P. N. Besedin, "Assessing the Efficiency of an EW Force's Command and Control in a Combined-Arms Operation," *Voennaya Mysl'* (*Military Thought)*, No. 2. 2017, pp. 67-71.
[283] V. V. Andreyev, O. G. Nikitin, and A. V. Marasanov, "Substantiating Ground Forces EW Control Bodies Composition," *Voennaya Mysl'* (*Military Thought)*, No. 6, 2017, pp. 51-54.
[284] Ibid., pp. 52, 54.

control disorganization can be assigned to REB forces. The rational strength and methodological support plan for a Ground Force formation's REB control bodies must be ascertained.[285]

Another 2017 *Military Thought* article described REB use not in operational art, as Lastochkin advised, but in tactical situations. Since the information domain is now considered a key element of the military environment, C2 from the tactical to the strategic realm has become a priority target.[286] REB forces and assets as a Task Force "carry out operational support of the main tactical tasks performance in combat by a Ground Force formation" and these forces are intended to accomplish the following: disablement of adversary electronic assets; technical control over electronic countermeasures; countering adversary reconnaissance technical assets; camouflaging one's own troops; disorganizing adversary troops and weapon C2 systems; reducing the application of the efficiency of adversary weaponry and electronic assets; and ensuring friendly force stability in control over one's own troops and weapons.[287] The main planning documents will be the "Adversary C2 Disorganization Plan" and the "REB Forces and Assets Employment Plan in Operations."[288]

In 2018, C2 and disorganization of an adversarial force were discussed in an article that used the C2 term over 20 times and the disorganization term some 13 times. The authors stated that "superiority in C2 constitutes a component of superiority over the adversary."[289] Two important C2 components are the abilities to disorganize an adversary's C2 and to stabilize Russian C2.[290] C2 disorganization of an adversary is a main operational task for ground force formations in operations. Isolating an adversary from C2 information prevents him from receiving timely information support. On today's battlefield, special software and REB can disorganize decision-making, offsetting military and technological advantages by reducing the timeliness of adversarial plans and precision weaponry efficiency.[291] Perhaps GPS signals are a focus of REB.

In October 2018 it was reported that electromagnetic weapons "can be regarded as a further development of electronic warfare devices. So far, they can operate at a distance of several tens of kilometers…"[292] These ultra-high-frequency weapons disable radio-electronic and optical elements of equipment and weapons, but also disorganize control.[293] Another report noted that there are plans to "install electromagnetic guns on 6th-generation Russian unmanned aerial vehicles."[294]

Conclusions

While Russia does not appear to have a specific A2AD concept, it has various capabilities that can accomplish that mission. The disorganization concept is perhaps a key one. It has been a part of Russian military thought for at least three decades, if not earlier, and requires immediate consideration. The disruption of an adversary's intentions and plans is the intended goal of the

---

[285] Ibid., p. 54.
[286] V. F. Lazukin, I. I. Korolyov, and V. N. Pavlov, "Basic Elements of the Tactics of Radio Electronic Warfare Troops," *Voennaya Mysl'* (*Military Thought)*, No. 11 2017, pp. 15-20.
[287] Ibid., p. 16.
[288] Ibid., p. 20.
[289] Yu. Ye Donskov, A. L. Morarescu, and P. N. Besedin, "Achieving Superiority in Command and Control as the Goal of the Use of Radio-Electronic Warfare in Army Operations," *Voennaya Mysl'* (*Military Thought)*, No. 1 2018, pp. 28-32.
[290] Ibid., p. 30.
[291] Ibid., p. 31.
[292] Oleg Bozhov, "We Have It! The Invisible Sword; Russia is Testing Electromagnetic Weapons That Burn the Insides of Enemy Missiles," *Armeyskiy Standart*, 12 October 2018.
[293] Ibid.
[294] No author provided, "Microwave Guns: Tests of New Weapon Have Started in the Russian Federation, Russia Has Begun Field Tests of an Electromagnetic Weapon," *Gazeta.Ru*, 1 October 2018.

concept and is behind the use of many types of Russian weapons, from information operations to underwater cables[295] to (the focus of this work) command and control issues.

Recent GPS interruptions near Russia's borders indicate that work on jamming GPS signals is clearly being tested. Such interruptions are similar to how the disruption of C2 capabilities would appear. Leaders in Norway and Finland were not amused at techniques that disorganize location-finding equipment. Finnish Prime Minister Juha Sipila stated that "This is not a joke. The air safety of ordinary people is under threat," regarding GPS interference in Lapland during a recent NATO exercise. Norwegian authorities stated that the interference was carried out by the Russians.[296] Finnish Foreign Minister Timo Soini promised to provide a report to Parliament regarding Russia's alleged jamming.[297] Thus Russia's disorganization concept can be applied to numerous capabilities (C2, airliners, drones, etc.).

The disorganization of command and control was stated to be a process that prevents an opponent's effective accomplishment of assigned tasks. Three types of disorganization were specified: collapse, disruption, and impediment. These "types" sometimes appear in descriptions of Russian exercises. For example, on 20 September, the Eastern Military District Press Service wrote that the Borisoglebsk-2 electronic warfare system was used to disrupt a notional enemy's system of command and control of troops.[298]

In addition to types of disorganization, two articles discussed various methods and ways to disorganize an opponent by the fragmentation of one or several C2 organs: single, paired, and grouped. Together, the disorganization types and fragmentation methods compose measures aimed at the substantive reduction of the capabilities or full cessation of the functioning of an opponent's technical resources for control.

The disorganization of command and control issues is Russia's method for attaining one part of what the West would label as A2AD superiority. REB's development of a disorganization plan should be followed closely. REB superiority is not easy to achieve, since it can involve knowledge of an adversary's UAVs and robots, command and control processes, employment methodologies, equipment functions, and control systems, not to mention how to employ Russian disorganization assets.

Developing Russia's C2 capabilities remains a center of attention for Russia. Defense Minister Sergey Shoygu recently noted that new tasks for the Armed Forces' C2 systems related to informatization have increased. Automation has increased sevenfold regarding the recording, analyzing, and generalizing of data at all levels of C2. The time to exchange information between military C2 organs has been reduced 30 times, he added.[299] Meanwhile President Putin and other military officials have trumpeted many significant advances in Russian weaponry and missiles. Perhaps the disorganization concept is still maturing or perhaps it is the confidential asymmetric counter of Western weaponry to which Putin and others often allude.

---

[295] Unattributed report, "Secret 'Rus' Surfaces Successfully," *Argumenty Nedeli Online*, 17 December 2015.
[296] No author or title provided, *Interfax* (in English), 12 November 2018.
[297] No author or title provided, *The Independent Barents Observer* (in English), 9 November 2018.
[298] No author provided, "Electronic Warfare Subunits of a Tank Formation and a Motorized Rifle Formation in the Eastern Military District Conduct Exercise in Which They Disrupt a Notional Enemy's System for Command and Control of Troops," *Ministry of Defense of the Russian Federation*, 20 September 2018.
[299] No author provided, "Session of the Russian Defense Ministry Collegium Held in Moscow," *Ministry of Defense of the Russian Federation*, 18 September 2018.

The concept is worthy of immediate Western consideration as a means Russia's military may use (or is using) in various situations. Developing serious security measures and counters to Russian disorganization plans, especially as concerns command and control issues, are vitally important areas for future attention.

This page intentionally left blank.

7 Russia's Context for Cyber and Information Issues: Nine Thoughts for Consideration

Putin Press Secretary Dmitri Peskov on Kim Kardashian's popularity and reach to her admirers:

> She's got no intelligence [service], no interior ministry, no defense ministry, no K.G.B…The new reality creates a perfect opportunity for mass disturbances.[300]

Introduction

Since the 1980s, Kremlin attitudes about the information age have changed and evolved. During the days of the Soviet Union, media outlets and TV, to include Xerox and fax machines, were tightly controlled, since information access or its spread was associated with power elements. With the 1991 demise of the Soviet Union, information control gradually evaporated. However, Russian agencies soon came to understand that new developments, such as the Internet, offered information access to anyone with a link. Peskov's more recent statement about Kardashian's popularity and ability to reach millions of followers without any government agencies demonstrates that recognition. Seemingly unlimited data had become available for free and individuals or groups could link up with those of similar interests (pro- or anti-government, etc.) and become influential segments of society with at least the power to correspond among themselves without government control. Eventually Russia's leadership decided to corral this new power, especially as the Kremlin witnessed the overthrow of governments due to "color revolutions." The latter are revolutions energized and integrated through the widespread use of cell phones and other information technologies and devices.

By 2013, as problems in Ukraine captured Russian and world attention, the Russian leadership decided to take internal information control a step further, as it saw compelling reasons to conduct information offensives abroad themselves and try to influence populations to their way of thinking or to just manipulate the media. Internal control had been reestablished (via legislation and state takeovers of communication assets) and external influence abroad was needed. The latter case was accomplished through a host of tactics (fake photos, use of Internet trolls, one-sided reporting, etc.) that manipulated public opinion in tune with Russia's interpretation of objective reality. Through media outlets such as Russia Today (RT) and Sputnik, Russia has accessed both compatriots located in other countries (in former Warsaw Pact nations or republics) and numerous external media markets, which happily accept Russian rubles and offer Russian TV packages.

The following discussion covers nine contemporary cyber/influence issues associated with Russia's military or civilian agencies and their attempts to control information agendas. It offers views from some surprising perspectives of Russia's approach to its control methods over its own population and to its methods to gain a strategic propaganda advantage abroad.

Consideration One: Have Media Tactics Changed over Time?

Vladimir Ryzhkov, a Russian State Duma Deputy from 1993 to 2007 and now a political analyst, described in detail a conversation he had with a former KBG officer's propaganda experience in Afghanistan from the 1980s, in which the officer outlined the Soviet principles of an information

[300] J. Rutenberg, "The Disruption," *The New York Times Magazine,* 17 September 2017, p. 50.

campaign. The methods recalled by Ryzhkov from his KGB conversation are listed below,[301] followed in parentheses by an example of a similar method used by Russia in Ukraine:

- It is necessary to convince the general population that the government is acting correctly and that the enemy is guilty of fomenting the crisis (Maidan protesters are to blame, the new government is linked to fascists, extremists, the US, and the West, which are the "real aggressors").
- The Kremlin creates myths about the terrible persecutions of the Russian-speaking population (the spin doctors created a virtual reality that appeared to find the right balance between truth and fiction, even though a human rights investigation by an independent European human rights agency found no violations or persecutions of the Russian-speaking public in Crimea).
- The enemy must be demonized (Ukrainian Right Sector leader Dmitry Yarosh was used for this. Moreover, the moderate forces were presented as neo-Nazis, and negative background information on Ukraine's new leaders was brought to light).
- The authorities disguise their aggressive actions as humanitarian (Russia had a humanitarian need to protect "defenseless" Russians in Crimea from the events that transpired in Kiev).
- The Kremlin justifies its methods by citing alleged enemy actions (the US is trying to take over Ukraine, so we must defend our ancestral territories).
- Authorities must be presented as legal and legitimate (Crimeans have a right to self-determination).
- War propaganda depends on a totalitarian approach (domestically, Russia cracked down on TV Rain and Lenta.ru for airing opposition points of view and earlier had silenced the media in Crimea once their forces intervened, pulling Black Sea TV, a local station that supported the new government in Kiev, off the air).[302]

Numerous other uses of cyber and information activities also took place in Ukraine. There was an attempt to interfere in the Ukrainian elections[303] and there has been an extensive information-psychological campaign on the battlefield via the manipulation of or warnings over the cell phone use of Ukrainian soldiers.[304]

Consideration Two: Russian Templates for Influence

Consideration one, above, offered one such template from the perspective of a KGB officer. Another was discussed in the book *The Red Web*, where authors Andrei Soldatov and Irina Borogan developed a template through which to understand the Kremlin's domestic approach to media control. They noted that Parliament produces a flow of repressive legislation that exploits cracks in previously published rules and regulations; hacktivists and trolls attack and harass liberals online, posing as someone other than a Kremlin supporter; Roskomnadzor [Russia's Federal Service for the Supervision of Communications, Information Technology, and Mass

[301] V. Ryzhkov, "The Kremlin's War Propaganda," 25 March 2014, at http://www.the *moscowtimes.com/opinion/article/the-kremlins-war-propaganda/496779.html*
[302] Ibid.
[303] No author or title provided, *Interfax-Ukraine News Agency,* 9 May 2014.
[304] K. Peshko interview with A. Hrytsenko, "Singular Impression—New Authorities Made Deal with 'Predecessors'," *Glavkom,* 14 July 2014, no page listed.

Media] is granted the power to censor and filter the Internet; Kremlin-affiliated oligarchs bankroll and take over media companies; specific manufacturers are selected to provide surveillance equipment; and Putin's paranoia of enemies ties these actions together, resulting in threats and intimidation. Putin's system is effective if people are certain the Kremlin is in control. This dynamic is transformed when a crisis occurs, and a message must be shared in real time.[305]

In a 2014 article in the Russian *Journal of the Academy of Military Science*, three authors from Belarus described a different type of template, offering an opinion on what they termed the ongoing information-psychological confrontation. They believe the West was victorious in the information-psychological war (an economic and information war) in the early 1990s. They termed this to be a "new-generation" war since the confrontation rejected actual weapons. They state that information-psychological warfare has now become an acknowledged form of military art.[306] This is an extremely important statement and one which Western analysts should seriously consider as to its meaning and expression.

The authors then discussed the goals, trends, and information measures of such confrontations. First, they listed 13 ways to achieve the goals of information-psychological confrontation. Second, they listed five trends that will determine the nature of information-psychological confrontations in the near future. Finally, when planning and implementing measures for information-psychological confrontations, they listed five principles that should guide actions.[307] The goals will be discussed further, along with trends.

The authors note that the principal goals of an information-psychological confrontation are regime change, an increase in the time to make decisions, and the means to control people. These goals are achieved via the following methods:

- Changing the citizens moral values
- Creating a lack of spirituality
- Destroying traditions and cultivating a negative attitude toward cultural legacy
- Manipulating the social consciousness
- Disorganizing systems and creating obstacles
- Destabilizing political relations
- Exacerbating political struggles and provoking repression
- Reducing information support
- Misinforming, undermining, and discrediting administrative organs
- Provoking social, political, national, and religious conflicts
- Mobilizing protests and strikes
- Undermining authority
- Damaging interests of a state[308]

Trends that determine the nature of information-psychological confrontations are: shifting aggression from the military-geographic domain to the information-psychological field; the role of television in initiating conflict; the influence of Western ideology on society's values; the

---

[305] A. Soldatov and I. Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries* (New York, Public Affairs), 2015, pp. 313-314.
[306] Iu. E. Kuleshov, B. B. Zhutdiev, and D. A. Fedorov, "Information-Psychological Confrontation under Contemporary Conditions: Theory and Practice," *Vestnik Akademii Voennykh Nauk (The Journal of the Academy of Military Science)*, No. 1 2014, pp. 104-106. Dr. Harold Orenstein translated this article from Russian to English.
[307] Ibid., pp. 106-109.
[308] Ibid., p. 106.

absence of direct invasion and destruction; and the irreversibility of the confrontations consequences.[309] The mass media's methods of manipulating TV were: blatant lies; concealing important information; immersion of information in a morass of garbage; replacement of terminology and use of unclear concepts and terms; introduction of taboos into certain sections of news; acknowledgement of the importance of images (use of well-known personalities with impact); and transmitting negative information that is perceived as better than positive news by the listener.[310] While the source of this information is from a Belarus perspective and not a Russian one, it still offers insights into considerations of value and publishable in an important journal.

One final template, used in both the MH-17 shootdown and the poisoning of Sergey Skripal,[311] is the methodology for confronting accusations of a true but damaging nature. When an event happens, the initial response is to (1) deny guilt and involvement (2) immediately begin editing reality and creating "evidence" or "the rationale" of another side's involvement, to include enemy forces in the area of the attack (3) make pleas to involve Russia in the investigation (4) make it appear that Russia is merely responding to attacks and (5) make conciliatory statements such as Russia is "detached from unnecessary emotion." Meanwhile, Russian citizens are denied access to much of the countervailing information.

Consideration Three: Military Directorates for Cyber

In *Moscow Defense Brief* Number One of 2017, author Aleksey Ramm offered definitions, force information, and defense mechanisms of Russia's cyber and information concepts. An information operation was defined as using specially prepared information against the adversary's armed forces, military or political leadership, or population to attain military, social, and political goals. A cyber operation was defined as attacking an adversary's information technical systems to disrupt their operation or to steal or delete sensitive information. Goals have changed from disrupting social networks to affecting the target audience of each. Ramm notes that the Main Intelligence Directorate of the General Staff oversees information operations. There are reasons to believe, he notes, that the 12th Directorate is in charge here. The General Staff Academy has a training course for senior officer in defensive measures against an adversary's information and cyber operations, as well as training on offensive operations by Russia's own forces. Naturally the Federal Security Service or FSB handles cyber operations for the government and its citizens. Finally, Ramm states that defensive measures for the military include a "Military Internet," a protected network with few interconnections. Thus, the concept, mentioned above in 2012, reappeared here in 2017. The Defense Ministry also has a Main Directorate for the Protection of State Secrets (also known as the 8th Directorate) and a Main Directorate for the Development of Information and Telecommunication Technologies.[312]

In February 2017 Defense Minister Sergey Shoygu stated that information operation forces had been established in Russia. His comments led one to believe that these were psychological operation forces, since he said they were more effective than the old counterpropaganda directorate. He then added that propaganda "must be smart, literate, and effective."[313] A former

---

[309] Ibid., pp. 107-108.
[310] Ibid., p. 107.
[311] The MH-17 shootdown refers to the destruction of Malaysian airline flight 17, destroyed by a missile launched by Russian troops in Eastern Ukraine; and the Sergey Skripal incident refers to the poisoning of a Russian defector to Great Britain, who was poisoned along with his daughter.
[312] Aleksey Ramm, "Russian Information and Cyber Operations," *Moscow Defense Brief,* No. 1 2017, pp. 16-17.
[313] M. Latsinskaya, A. Braterskiy, and I. Kalinin, "Russia Sent Troops onto the Internet: Shamanov Explained Why Information Operations Troops Are Necessary," *Gazeta.ru,* 22 February 2017, no page provided.

Chief of the USSR's KGB Analysis Directorate, Vladimir Rubanov, stated that Russia's cyber troops amount to 1,000 soldiers, and that information space is now as important as land, sea, and aerospace theaters of military operations.[314] Alexander Perendzhiyev, an expert at the Association of Military-Political Scientists, stated that today victory is achieved in virtual space and not on the real-world battlefield. Further the report noted that:

> According to information on the Defense Ministry official website, there are several subunits in the department's structure for now whose zone of responsibility can include information operations. Above all this is the Main (Intelligence) Directorate, the Main Directorate for the Development of Information and Telecommunications Technologies under the direction of Colonel Maksim Bets, as well as the Press Service and Information Directorate headed by Major General Igor Konashenkov. The General Staff Eighth Directorate's 6th Scientific Company located in Krasnodar probably also plays a certain part.[315]

The article added that the Russian General Staff Academy is teaching a course on information conflict.

Consideration Four: Cyber and the Initial Period of War

From their own experiences, Russian leaders believe that the readiness of the Armed Forces to fight has had the greatest impact on the course and outcome of armed struggles. The ability to plant cyber and information means before such struggles occur has significantly increased the importance of the concept of "the initial period of war (IPW)." Such means can serve key information links or corrupt entire systems, enabling victory before the first battle. The IPW was first defined in the 1920s. In 2012, it was defined as when warring states conduct military operations involving groups of their armed forces that are "deployed before the start of war to achieve short-range strategic objectives or to create favorable conditions for committing their main forces and continuing with more operations."[316]

Cyber implants are one of the most invasive tools that can be "deployed" forward through their insertion into foreign systems in peacetime and remain capable long after insertion to achieve short- or long-term objectives (either conducting reconnaissance or destroying systems when activated). Due to such scientific advances, it appears that protecting critical infrastructure and cyber resources from cyber-attacks may even take precedence over other factors early in a conflict. Information technologies, precision weaponry, reconnaissance and electronic warfare technologies, and automated control procedures provoke new challenges and threats in the IPW for other nations. Many believe that the IPW will be decisive for the outcome of a war. A state that is planning aggression will use peacetime or a period of threat to plant viruses, disorganize systems of the country it wants to attack, and launch wide-scale targeted information operations and intense reconnaissance activity.

Perhaps due to concern for the US's cyber security in the IPW, the US Federal Bureau of Investigation (and earlier, the government of Ukraine) decided to no longer tolerate the use of Kaspersky anti-virus solutions, a product sold in stores and advertised on prominent radio stations. Is it possible that the FBI feared Kaspersky's ability to insert a virus or logic bomb into their critical

---

[314] Ibid.
[315] Ibid.
[316] S. G. Chekinov and S. A. Bogdanov, "Initial Periods of War and their Influence on a Country's Preparation for Future War," *Voennaya Mysl' (Military Thought),* No. 11 2012, pp. 14-27.

information domain that would ensure Russia would have information superiority if an IPW between Russia and the US ever developed? A *Wall Street Journal* article noted that the Kaspersky anti-virus has been on a Defense Department watch list of potential problems since 2004. In 2013 the Defense Intelligence Agency issued a Pentagon-wide threat assessment about the company. US officials note that the firm's products were used as a tool for spying on systems in the US.[317] What wasn't discussed was whether the products could also have planted malware that can sit, wait, and be ordered on command to cause banking, infrastructure, or other types of damage in times of stress.

Consideration Five: Warning of Presidential Election Meddling

For the past two years, nearly every country in Europe has put their cyber forces at some time on alert for possible interference from Russian hackers or cyber warriors. This is particularly true near election time in these nations. Their warnings are based on finding active indicators of reconnaissance activities emanating from Russia. Meanwhile, Russia continues to reject any complicity in the face of overwhelming evidence.

While it is extremely hard to know just how widespread such discussions are in Russia and the locus and extent of their cyber planning, there is at least one historical example worthy of mention. Writing in *Armeyskiy Sbornik (Army Journal*) in October 2004 author Boris Rodionov discussed weapons of influence. In an eerie reference to problems associated with the 2016 US Presidential election and the elections in Europe, the article twice referenced influencing elections. One of those references read as follows:

> Today one can already predict the evolution of a weapon's purpose; from weapons of destruction to weapons of deterrence and then to weapons of influence. Using such weapons, it will be possible to exert long-range controlling effects on persons, and consequently on the course and results of election campaigns, on the decision-making of presidents, prime ministers, and other high-ranking persons, and in this way to control the entire world.[318]

Again, this article appeared in 2004! The article further stated that it was the use of information influence operations in the early 1990s that caused the USSR to cease to exist as a superpower. This is a reference to the belief that the US had conducted some sort of information-psychological attack on the USSR that aided in the dissolution of the nation.

Consideration Six: The Worries of Russian Cyber Planners

During a 2010 Russian-sponsored conference in Garmisch Germany, a member of the Russian delegation was asked to rank order threats as he perceived them to Russia. Interestingly, escalation models were listed first. His concern clearly was that a cyber exchange could mistakenly get out of control, especially due to the use by some nations of surrogates or anonymous actors taking actions that responsible government officials would never consider. The risk associated with such gambles was simply too high. Second on the list of threats was the protection of civil infrastructures from attacks, which could result in the collapse of key banking or service-oriented (gas, electric, etc.) organizations, resulting in chaos or confusion. Protection of critical infrastructure was listed as a priority concern. Definitions were next, as it was felt the ability to define concepts such as cyber-attacks, cyber law, or other issues were key to keeping control over

---

[317] P. Sonne, "Russian Firm Was Long Seen as Threat," *The Wall Street Journal,* November 18-19, 2017, p. A2.
[318] B. Rodionov, "On the Waves of Energo-Information," *Armeyskiy Sbornik (Army Journal),* October 2004, no page provided.

cyber-related issues and offering a venue for not only discussion but a common understanding of threat issues. Of lesser concern to the individual was the threat of industrial espionage, most likely because Russian software developers had become so adept and invasive in this area. For both Russia and the US, there are issues here that need to be discussed and settled. Peacetime is the place for a discussion of escalation models and ways to prevent cyber issues from escalating out of hand, not after escalation occurs.

Consideration Seven: Reflexive Control and Cyber

For at least the past 30 years, Russia's military has employed a concept known as reflexive control (RC). In its simplest form, it means making someone do something for themselves that they are actually doing for you. A simple e-mail phishing attempt fits the definition perfectly, as the initiator of the attack gets a person to do something for themselves (open a file to see what is there based on misleading information in the e-mail), which allows a virus into the system. The e-mail's initiator thus accomplishes his or her goal, as the e-mail recipient's action does your work. An example of such an operation occurred during the 2012 Presidential elections in Russia. Spam e-mails promoting a rally against Vladimir Putin's 2012 Presidential run contained a document titled "Instructions for our actions in the rally against Putin." The attachment carried malware, and the software overrode files and ran code that caused computers to crash.[319]

The use of analogies works the same way, as a person is led to believe based on an analogy (the Russians, in 2014, made the claim that many Ukrainians involved in the anti-government demonstrations in Kiev were Nazis) that he or she (a Russian) must fight them, as the analogy draws on a Russians reflexive response to World War II recollections.

In 2011, Russia's military published a document known as the "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space."[320] The definition of information war discussed damage done to information systems, potential damage to the stability of society via brainwashing, and, at the end of the definition, stated that information war's confrontation was for "forcing the state to make decisions in the interests of the confronting party."[321] Thus, when defining information war, the Russians included the RC concept, although most Western readers of the definition would not spot it.

In 2015, V. G. Kazakov and A. N. Kirishin wrote an article on RC for the Journal of the Academy of Military Science.[322] They noted that the commander needs a special group (outside the Table of Organization and Equipment) with information-psychological qualifications to develop and transmit the use of RC measures together with command control ("readiness to execute assigned tasks") actions. This is done through the spreading of "information packets" on the battlefield. An information packet could be a fake electronic warfare transmission that influences conditions. There was a diagram that accompanied this explanation, showing how command control and RC fit together to manipulate an enemy's decision-making process.

---

[319] Soldatov and Borogan, pp. 162-163.
[320] "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministerstvo Oborny Rossiyskoy Federatsii (Defense Ministry of the Russian Federation)*, 2011, p. 5.
[321] Ibid.
[322] V. G. Kazakov and A. N. Kiriushin, "All-Inclusive Command and Control of Combat Operations," *Vestnik Akademii Voennykh Nauk (The Journal of the Academy of Military Science)*, No. 4(2015, p. 39. To view an English version of the diagram from this journal, see Timothy Thomas, *Kremlin Kontrol* (Fort Leavenworth, KS: Foreign Military Studies Office, TRADOC, 2017), pp. 195-196. Dr. Harold Orenstein translated the article from Russian to English.

Consideration Eight: Is There a "Cyber Dead Hand?"

In 1985, the Soviet Union tested and put on alert status a system known as Perimeter.[323] It was designed to deliver a nuclear strike against the US if the latter's nuclear weaponry destroyed the USSR's leaders and command systems before they could retaliate [or if an electronic warfare strike took out the USSR's rocket force command and control capability]. The system consisted of missile launches from a secret bunker that could in reality "throw down" codes to intercontinental ballistic missiles (ICBMs) in case the nations leadership was rendered helpless and unable to transmit codes to the Kazbek launch system.

In times of tension, the system (and the officers in a bunker) might be activated in an "advance preparation" fashion. The Perimeter system would apparently be used not only if contact was lost with the leadership but if special sensors also indicated "radioactivity, seismic shocks, and atmospheric overpressure," all signs of a nuclear strike. In that sense the system was semiautomatic, as its use still rested on people in the bunker making a final decision. An automatic system was also contemplated (a "Dead Hand") but apparently discarded, since it relied solely on computers and took people out of the launch process.[324]

In 2011, in the journal *Military Thought*, it was reported that there were prospects for what was termed a "military (combat) Internet" in the Russian Armed Forces. Information was viewed as a decisive factor in achieving strategic and operational-tactical superiority over an adversary on the battlefield. Information superiority enables speed and timely decision-making on the modern battlefield. Improvements in the strategic control system through installing digital and telecommunications equipment was designated as priority one for these reasons.[325] It was noted that many people writing on this subject tend to support development of a new Russian segment, Intranet Russian Federation" and that it "could be protected against outside threats and have no risks of dependence on foreign assistance in technical problem fixing."[326]

Consideration Nine: Battlefield Influence Operations

On the battlefield, operations in cyberspace have signaled Russia's entrance into an entirely new type of warfare. It is, according to experts, a combination of information and information infrastructure designed and used on the battlefield to shape, generate, transform, transit, use, and store information in computers and computer networks. Cyberspace is essential for operations in any modern control system and is the most prioritized element of a battlespace in the broadest sense. The authors of one article noted that the "formation of cyberspace as a new realm of combat operations called for a revision of ideas held about the forms and methods of combat actions and the content of command and control over tactical military formations."[327] Some of the forms and methods were said to be cyber-warfare, cyber-engagement, cyber-action, and cyber-attack.[328]

In 2014, Major General (retired) Kh. I. Sayfetdinov wrote on battlefield operations. He defined information warfare as the conscious employment of information to enable the user to achieve his

---

[323] See D. E. Hoffman, *The Dead Hand* (New York: Doubleday, 2009), pp. 150-154 for a worrisome discussion of the Perimeter project.
[324] Ibid.
[325] V. F. Samokhin, V. N. Lukyanchik, and A. N. Artyushenko, "Prospect for a Military (Combat) Internet in the New Look Russian Armed Forces," *Voennaya Mysl' (Military Thought*) No. 8 2011, pp. 57-60.
[326] Ibid.
[327] V. I. Kuznetsov, Yu. Ye. Donskov, and A. S. Korobeynikov, "About the Question of the Role and Place of Cyberspace in Modern Military Operations," *Voennaya Mysl' (Military Thought*), No. 3 2014, pp. 14-16.
[328] Ibid.

political, economic, military, or any other goals.[329] The objective of such operations is to gain and hold information superiority over an adversary and to create favorable conditions for the Armed Forces. Operations must be conducted constantly, in peacetime and wartime.[330] Information operation tasks include monitoring information sources to detect, assess, and predict information-related threats to Russia; deceiving adversaries as to Russia's plans and intentions; disorganizing the adversary's government and military command and control capability; impairing the psychological stability of adversary forces; and maintaining the morale and psychological state of friendly forces.[331] Subsystems of an information operations system would include the ability to attack an adversary's technical information capabilities and protect friendly systems from adversary attacks; software and hardware capabilities; reconnaissance, to include electronic reconnaissance capabilities; electronic warfare; and psychological warfare against an adversary, while protecting friendly forces from similar attacks by an adversary.[332]

In 2016, Colonel K. A. Trotsenko discussed operational-tactical control levels. Initially he discussed the basic structure and understanding of information confrontations in Russia. His explanation contained the familiar division of information operations into information-technical (computers, electronics, etc.) and information-psychological (influencing the public and armed forces of an adversary). He added that this definition is strategic. At the tactical and operational levels, the focus is more on organizing control and electronic warfare capabilities.[333] Attaining a tactical goal can be determined by the degree of information superiority one has over an opponent and the time available to forestall adversary actions. He explains:

> Informational confrontation in preparing and conducting tactical actions is, therefore, to imply a set of measures for organizing and effecting control, reconnaissance, electronic warfare, security, tactical camouflage, fire destruction of the adversary control systems, use of highly maneuverable units and certain kinds of maneuvers coordinated in terms of time, place, mission, and aimed at achieving superiority in controlling, deceiving, and forestalling the adversary in its actions.[334]

Conclusions

This article was designed to show that Russia's approach to cyber and information operations is thoughtful and innovative, focused on being covert and manipulative, and yet still repetitious due to its use of specific concepts from Soviet days. Thoughtful in that it integrates new technologies, concepts, and approaches to cyber affairs as they develop; covert and manipulative in the many ways it attempts to force its objective reality on other populations through reflexive control and other mass media methods; and repetitious in that many of the techniques used earlier are still adaptable to current conditions as Russia continues to divide information warfare into information-technical and information-psychological aspects.

This is a far cry from where Russia first started in the early 1990s, when its information and cyber advantages were almost nonexistent. During a September 1995 conference in Moscow, for example, Russian information expert V. I. Tsymbal stated that the use of information warfare

---

[329] Kh. I. Sayfetdinov, "Information Confrontation in the Military Sphere," *Voennaya Mysl' (Military Thought)* No. 7 2014, p. 38.
[330] Ibid., p. 39.
[331] Ibid., pp. 40-41.
[332] Ibid., p. 41.
[333] K. A. Trotsenko, "Information Confrontation at the Operational-Tactical Level of Control," *Voennaya Mysl' (Military Thought*) No. 8 2016, p. 20.
[334] Ibid., p. 21.

forces against Russia would be considered a military phase of conflict, even if there was no loss of life. More ominously, he added:

> In studying the potential catastrophic consequences from an enemy's use of strategic IW systems on, for example, the economy or government control…we must unequivocally declare that in the case of their use against Russia, we reserve the right to conduct a first strike (nuclear) against the IW system and forces which are directing that weapon, and then also against the aggressor-government.[335]

The warning was unambiguous. There apparently was a desire to use the conference to transmit a message to the US leadership, if it hadn't made its way there earlier through other channels, that the thought of an information warfare attack on Russia's weak infrastructure would be an act of war leading to a devastating attack on the other side. Whether the conference message reflected actual operational plans or was used simply for deterrent purposes is not known. Today, since Russia has developed numerous information and cyber specialists, it is less likely that Russia would answer a cyber-attack against its infrastructure with a nuclear strike. It would be more likely that Russia would unleash its own powerful information strike against such an adversary.

The analysis prompts a host of questions and suppositions about what Russia's end goals might be. Specifically, US attention should focus on Russia's desire to achieve information superiority in the initial period of war; Russian attempts to manipulate "objective reality" to its benefit; the continued application of specific media tactics and reflexive control deception; and the various templates Russia is developing, either wittingly or unwittingly, to achieve their goals. For the U.S., these issues should become priority considerations. Understanding where Russia is heading, what techniques of persuasion they are using, and how they are shaping a future potential battlefield are all important considerations. There is also one other very important fact to keep in mind and that is for analysts to stop trying to mirror image U.S. thinking onto Russia's way of conducting military affairs. Russia has its own priorities, concerns, and way of military thought. It is only through a conceptualization of Russia's framework of military thought that its actions can be understood. Without that lens, analysts are likely to be led down some false roads.

Russia continues to add more military muscle in the form of information and cyber-driven equipment. It also continues to worry incessantly about NATO. Russian activities, as a result, need to continue to be monitored closely. Some actions need to be confronted directly, either through negotiations or through the development and implementation of new US security measures. A greater focus on the contours of Russian military thought would also be of the upmost importance in trying to decipher where that nation's leadership is taking them.

---

[335] V. I. Tsymbal, "The Concept of Information Warfare," Presentation at a September 1995 conference in Moscow, Russia, p. 7, attended by the author of this work.

8 Electrons, Underwater Cables, Satellites, and Creative Thought: The Russian Military's Invisible Information Environment

> In the event of a global conflict it is extremely important to destroy the enemy's group of satellites in order to deprive him of communications, navigation, and the capability to conduct reconnaissance. Thus, the idea of creating such interceptors appears. In the USSR, for example, tests were conducted during which one satellite approached another and exploded, striking the target with fragments.[336]

Introduction

A few months ago, a U.S. Army general sat behind a table and looked at a map of Russia. He said he could visualize where the Russian brigades might be located in each military district on this purely cartographic representation. What he didn't know, and what he asked about, was "what can't I see."

The following discussion offers one assessment of things not visible, focusing on the multi-dimensional information environment. It is a difficult one to assess. During the Cold War, we all knew the intent of a tank and who the potential enemies were. In the information age, ascertaining the intent of an electron and where it originated (an adversary or surrogate) present much more difficult challenges in assessing who really may or may not have attacked whom. It is also difficult to observe items that are out of sight (electronic networks, satellites, and underwater cables, all key sources of information and communications) and whether they are being inspected or manipulated by foreign entities.

Overview

Russia's military has stepped quickly into the information age, developing information troops and information science companies along with a vast array of new precision weaponry and reconnaissance means (unmanned aerial vehicles, satellites, etc.). The military is cooperating with numerous domestic information and computer assets (Kaspersky, Dr. Web, etc.). These forces, along with the aerospace and electronic warfare branches, are developing ways to watch or manipulate adversaries by learning to disorganize command and control entities; inspect or neutralize satellites; tap into underwater cables; develop information, space, and ocean theaters of military operations (TVDs) from which actions spring; make advance preparations for an initial period of war; forecast the impact of the information age on war's conduct; and other related activities.

The vast majority of this chapter's content addresses Russia's current approach to acquire and control new operational capabilities. The newer strategies and conduct of operations are listed first below, as they utilize new scientific discoveries to uncover innovative ways to use reconnaissance assets, precision weaponry, military art, or deterrence theories. Perhaps more important is how Russian theorists have expanded their vision for employing such assets to the entire planet. Two components of Russia's breakout of information warfare's components that have also been present since the 1990s, information-technical and information-psychological developments, are also discussed.

---

[336] S. Valchenko, N. Surov, and A. Ramm, "Russia Sends Inspector into Orbit: Military Test Operations of Maneuvering Identification and Intercept Satellite," *Izvestiya Online*, 26 October 2017.

Near the end of the chapter the international strategies that have been used for years are discussed. Two more contemporary documents (2011 *Conceptual Views* and 2014 *Military Doctrine*) demonstrate the carry-over of specific goals from the 1990s into the contemporary era that Russia still hopes to achieve. These documents are centered around rules, regulations, and terminology for the use of information resources. Early United Nation presentations by Russian experts focused on defining information weapons and other terms. Such goals are still sought after today, as the documents clearly indicate. An April 2018 presentation by Russian General Major Igor Dylevskiy, an information warfare expert, demonstrates the contemporary application of the same process.

Russia's military approach to the information age is thus clearly multi-dimensional and requires continuous study. The following outline represents the order in which topics are presented in this chapter:

- Information assets and strategies
- Information's role in the initial period of war
- Strategic operation for the destruction of critically important targets (SODCIT)
- Forms and methods of information use
- Information and digital deterrence
- Information troops
- Information-technical and information-psychological capabilities
- Reinstating political-military officers in the force
- The military's 2011 *Conceptual Views* and 2014 *Military Doctrine*
- General Major Igor Dylevskiy's 2018 presentation at the 6th Moscow conference on international security

Each topic is highlighted in **bold** below so that readers can quickly find sections in which they may be more interested.

Newer Developments

Information Strategies

There are three key points to analyze when considering Russian information strategies. First is the scale of such operations. Russian analysts indicate that information's capabilities, not surprisingly, have expanded from specific territories to a planetary scale. It is now possible to hit targets with either missiles or electrons anywhere on the planet. Perhaps Russia's discussion of an information TVD is where the focus of a planetary concept of operations can be found. A second point is that for an information strategy to be successful, information superiority must be attained, and that involves the capability to interrupt, if necessary, an adversary's information flows. In this regard Russia is focusing on the carriers of information, namely underwater cables, satellites, and electronic warfare means, as issues to control if it is to thwart the command and control capabilities of a foreign force. Third, there remains the ability to construct information flows, not interrupt them, and deceive an opponent with information specially developed for their consumption. Such capabilities are referred to in Russia as the reflexive control of an opponent. All of these points are explained in greater detail below.

Writing in 2010, Russia analyst S. G. Chekinov noted that "Orbiting weapons capable of hitting key military targets at any point of the planet would give a global dimension to armed struggle."[337] His reference to the global dimension of armed struggle has been restated by others and indicates a theoretical move from considering warfare on a strategic scale to a planetary one. Information strategies involving the global information space use information and digital assets to influence situations and decision-makers. In 2013 Russia's *Army Journal* published an article by General-Major Vladimir Slipchenko, who was known for his creative thought. Slipchenko wrote that superiority over an opponent was only possible after superiority in information, mobility, and rapidity of reaction were assured. Precise fire and information effects against economic structures and military objectives were required. Slipchenko referred to this mode of conduct as noncontact war. Most important of all he stressed that, in such war, information confrontations would be continuous and would leave the operational and strategic levels and acquire a planetary scale. However, such confrontation's principal goal remains to be the maintenance of one's own information security and the lowering of a potential enemy's security.[338] Chekinov and Slipchenko are not alone in thinking about planetary concepts of influence.

Concepts such as information strategies and wars on a planetary scale are developed in the bowels of the General Staff in Moscow. Russian General Staff Chief Valery Gerasimov, quoting Soviet military theorist Alexander Svechin in regard to strategy, has noted on occasion that each situation has a logic all its own. That is, strategy's makeup is not fixed but entirely flexible. It depends on creative thought to best utilize the circumstances under consideration, and choices will remain hidden until utilized. With an array of missiles, satellites, underwater cables, and electronic networks before it, strategies are dependent on the creativity and innovation of commanders to exploit the situation at hand.

Underwater cables and satellites play huge roles as assets whose locations may be known but their location so widespread (planetary) that they can only be watched intermittently, perhaps when a warning sounds. It is not only their location, but also their function that may be invisible. Until such equipment's function is discussed openly or is actually utilized (or is inspected by a foreign entity), its function remains a secret. The same doubts apply to the application of military art. How forces will be used remains a secret until they are deployed.

With regard to underwater cables, a 2014 Russian report stated that the oceanographic research ship Yantar can submerse to a depth of over 6,000 meters. The range of tasks it can resolve is broad and interesting, such as "the retrieval of information from the NATO counties' underwater intercontinental communications cables along which our 'partner's' most secret and sensitive information is transmitted."[339] A 2017 British report noted that Russia could use not only the Yantar but also underwater drones to attack network cables carrying Internet and telephone communications around the world.[340] Another 2017 report of Russian origin noted that the Yantar is a "unique floating dock for mini-submarines and unmanned submersibles" and that they are cable of connecting to information cables on the bottom of the sea.[341] A 2018 Russian report stated

---

[337] S. G. Chekinov, "Predicting Trends in Military Art at the Start of the 21st Century," *Voennaya Mysl'* (*Military Thought)*, No. 7 2010, pp. 19-33.
[338] V. Slipchenko, "Information Assets and Information Confrontation," *Armeyskiy Sbornik (Army Journal)*, No. 10 2013, pp. 52-53, 55. The author would like to thank Dr. Harold Orenstein for his translation of this article.
[339] Unattributed report, "Secret 'Rus' Surfaces Successfully," *Argumenty Nedeli Online*, 17 December 2015.
[340] David Brown and Tom Parfitt, "Russian Navy Ship Yantar Can Sever Internet Cables," *The Times* (Electronic Edition), 17 December 2017.
[341] Andrey Riskin, "Which Secrets Is the Russian Intelligence Ships Yantar Seeking on the Bottom of the Mediterranean Sea?" *Nezavismaya Gazeta Online*, 10 October 2017.

that the U.S. was particularly concerned about protecting underwater communications and that their damage could cause wide-scale disorganization in communications.[342] Obviously the Russians are aware of the sensitivity associated with these cables.

Information flows can also be disturbed by anti-satellite (ASAT) weaponry. Satellite observation or destruction topics have been under discussion in Russia for over 60 years. While there are several types of satellite disruptions, the first for discussion is the Tirada-2S, because it is designed to interfere with information flows. The system is supposedly capable of radio-electronic suppression or jamming of communication satellites, to include the complete disabling of the satellites.[343] The Tirada is ground based, suppresses an adversary's electronic apparatus by means of an impulse, and likely receives target designation from Russia's Missile Attack Warning System. The new Russian combat laser, the Peresvet system, blinds satellites[344] and may have a similar function, among others, as the Tirada.

There are other satellite types in the Russian inventory that, while not directly affecting information flows, will perform such activities simply due to the consequences of their other functions. In 2017 Russia announced it had developed both "killer satellites" and maneuvering inspection satellites that approach and inspect other satellites. As one military expert noted:

> In the event of a global conflict it is extremely important to destroy the enemy's group of satellites in order to deprive him of communications, navigation, and the capability to conduct reconnaissance. Thus, the idea of creating such interceptors appears. In the USSR, for example, tests were conducted during which one satellite approached another and exploded, striking the target with fragments.[345]

The inspection could, utilizing the visible, infrared, and ultraviolet bands, collet data and transmit it to a control center.[346] If the data indicates the satellite is conducting communications, the control center could send a message to the Tirada to disable it. The inspector satellite could also be equipped with electronic intelligence collection or accommodate attack weapons, "whether it be an energy gun, micro-missiles, or simply a bag of nails."[347] A late 2018 report noted that there are various kinds of ASAT weaponry in Russia's inventory. The ASAT Kontakt missile can be launched from a MiG-31 aircraft; the S-500 Prometey air defense missile system is designed to intercept orbital vehicles; and the Nudol space missile is part of the A-235 missile defense system, capable of interceptions at ranges up to 1500 kilometers.[348]

REB capabilities are another way to interrupt information flows. Referring again to Chekinov's explanation of 21st century military trends, he noted the following:

> Electronic warfare devices are, therefore, placed side by side with nuclear and conventional weapons and electronic warfare itself turns from a kind of operations (combat) support into one of the key elements of combat operations. In the light of past experience, the share of electronic suppression in disorganizing the enemy's control system and undercutting his

---

[342] Aleksey Ivanov, "Russian Navy May Deprive United States of Communications," *Rossiyskaya Gazeta Online*, 22 June 2018.
[343] No author or title provided, *Interfax* (in English), 9 January 2019.
[344] Aleksey Abaturov, "Russian 'Sweepers' of Near-Earth Space: Tirada, Nudol, and Kontakt," *Yezhenedelnik Zvezda*, 20 November 2018.
[345] S. Valchenko, N. Surov, and A. Ramm, "Russia Sends Inspector into Orbit: Military Test Operations of Maneuvering Identification and Intercept Satellite," *Izvestiya Online*, 26 October 2017.
[346] Vladimir Tuchkov, "Russia's Killers: Who Already Finds Themselves in the Sights: Moscow is Creating a Grouping of Orbital Spacecraft Called Killer Satellites," *Svobodnaya Pressa*, 30 March 2018.
[347] Ibid.
[348] Abaturov, "Russian 'Sweepers'…"

> combat potential accounts for about a third. In the longer run, it may rise and have a more significant impact on the efficiency of air force attacks and strikes by other weapons.[349]

REB has become a major method to deny communications and information flows to opponents and to disorganize them. REB Chief General-Lieutenant Yuriy Lastochkin, for example, mentioned REB's ability to disorganize adversary troops and weapons eight times in a 2017 article.[350] He and two other authors described how operational art is developing in conjunction with improvements in weaponry and ways to conduct combat. Capabilities, it was noted, have always determined methods. Weapon improvements have resulted in new operational tasks for REB and allowed the force to both disorganize adversary troops and weapons and repulse aerospace attacks.[351] Destroying circuitry, distorting or destroying information, or simple electronic suppression all contribute to the C2 disorganization effort.[352] REB methods will be a main way to cause chaos in an adversary's C2.

Russian theorists understand that the ability to interrupt information flows or to use information to deceive an opponent are methods that must be developed and prepared in peacetime. It requires mapping an opponent's information network and, if possible, collecting intelligence on such systems in order to be able to disrupt or influence them at a moment's notice. Such access allows Russian forces to prepare to gain the initiative in what they term as the initial period of war.

Information's Role in the Initial Period of War (IPW)

An 11 January 2018 *Wall Street Journal* article discussed Russian hacking successes against the U.S. power grid. Robert Silvers, former assistant secretary for cyber policy at Homeland Security, noted that "what Russia has done is prepare the battlefield without pulling the trigger."[353] There is hardly a better description of Russia's IPW concept.

Being prepared for the initial period of any war has been a constant focus for the Soviet Union and now Russia. Most likely this is a direct result of lessons learned from the Soviet experience in WWII, when the nation was not properly prepared to go to war with Germany and experienced early setbacks. Now in the age of information, where information superiority is so crucial to success, the IPW has taken on added important.

An important discussion of information and the IPW was conducted on the pages of *Voennaya Mysl'* (*Military Thought)*. The IPW was defined as when warring states conduct operations before the start of war to achieve objectives or to create favorable conditions for committing their main forces.[354] Outer space, information warfare, and new weapon capabilities all help inform the shape needed for the IPW. These weapons enable sides before the start of operations to conceal the status and intent of their armed forces and the nature of any planned attacks. More importantly "In all likelihood, the aggressor country is to be expected, still in peacetime, to launch a wide-scale

---

[349] Chekinov, "Predicting Trends…"
[350] Yu. Lastochkin, Yu. Koziratsky, Yu Donskov, and A. Mororescu, "Combat Employment of EW Forces as an Element of Ground Force Operations," *Voennaya Mysl'* (*Military Thought)*, No. 9 2017, pp. 18-25.
[351] Ibid.
[352] Ibid., p. 24.
[353] Rebecca Smith and Rob Barry, "Russian Hack Exposes Weakness in U.S. Power Grid," *The Wall Street Journal*, 11 January 2018, pp. A1, A9.
[354] S. G. Chekinov and S. A. Bogdanov, "Initial Periods of War and their Impact on a Country's Preparations for Future War," *Voennaya Mysl'* (*Military Thought)*, No. 11 2012, p. 16.

targeted information operation and intense reconnaissance activities, including a set of related and closely coordinated actions."[355]

It was noted that the IPW of new-generation wars will be decisive for the outcome of a future war. Such wars will include the launching of information operations, to include technical and psychological attacks along with electronic operations. Information operations and electronic and fire strikes disorganize government systems, demoralize populations, and prevent leaders from rallying forces to repel aggression.[356] The attainment of information superiority is required in areas such as the mass media in order to stir up chaos and confusion in an adversary's government and military management. The main effort in the information struggle is to be directed against an adversary's government and military control systems, while providing protection to national information resources from adversary influences.[357] Russian IPW preparations include broadcasts to prepare the economy and public for war; the mobilization of reserves; the relocation of military units; the broadcast of false information to deceive adversary reconnaissance; and a campaign to inform the public about the adversary's motivations and intentions.[358]

Perhaps due to concern for the US's cyber security in the IPW, the US Federal Bureau of Investigation (and earlier, the government of Ukraine) decided to no longer tolerate the sale of the Russian-produced Kaspersky anti-virus solutions, a product sold in stores and advertised on prominent radio stations in the US. A recent *Wall Street Journal* article noted that the Kaspersky anti-virus solution has been on a Defense Department watch list of potential problems since 2004. In 2013 the Defense Intelligence Agency issued a Pentagon-wide threat assessment about the company. US officials note that the firm's products were used as a tool for spying on systems in the US.[359]

Proper IPW preparation includes planning for the immediate implementation, whether preemptively or after conflict erupts, of strategic operations to destroy critically important targets. These plans help Russian forces ensure it can attain the initiative in future confrontations.

Strategic Operations to Destroy Critically Important Targets (SODCIT)

Russia's military doctrine of 2014 noted that information can impose an effect on the enemy to the full depth of his territory in global information space. This makes the U.S national military objective of deterring "state adversaries from threatening the U.S. homeland and U.S. interests while assuring the security of allies"[360] take special note.

Cyber operations, which seemingly are without borders, are most likely one aspect of Russia's SODCIT concept, as it allows Russia to affect an enemy to the full depth of his territory in global information space. The SODCIT concept implies deep reach into an opponent's rear area and threats there to political, economic, military, and information infrastructures and targets of strategic significance. There is very little in the open military literature about this concept, but it has apparently been discussed in Russia for several years and, due to its strategic implications, is extremely important yet close hold.

---

[355] Ibid., p. 24.
[356] Ibid., p. 25.
[357] Ibid., p. 27.
[358] Ibid., p. 26.
[359] Paul Sonne, "Russian Firm Was Long Seen as Threat," *The Wall Street Journal*, November 18-19, 2017, p. A2.
[360] C. M. Scaparrotti, *United States European Command: Theater Strategy*, 2016, p.6.

In 2010, a *Red Star* article noted that changes in the nature of wars would be reflected in the various forms in which the Armed Forces are used. The article's author, Marina Yeliseyeva, wrote that "The **strategic operation to destroy critically important facilities** has been developed."[361] Retired Colonel General Viktor Barynkin added "it has become expedient to combine strategic defensive and offensive operations and strategic operations in the ocean theater of hostilities into a single strategic operation."[362] This appears to border on a planetary and not a strategic operation.

In 2013 the journal *Air-Space Defense* published an article on forms and methods of combat in space. It added "space" to Barynkin's strategic operation noted above, stating:

> It is possible to use various space systems in support of each of these operations. Thus, supporting a **strategic operation to destroy critically important enemy targets** necessitates the use of space-based means of reconnoitering these targets; electronic intelligence assets; meteorological reconnaissance assets in the interests of a proper selection of attack weapons and their combat employment methods; and space-based navigation, communications, relay, and strike evaluation systems.[363]

A 2014 article that mentioned the SODCIT concept was found in *Military Thought*. It stated that determining combat missions, mixes, methods, and variations of long-range precision-guided munitions (PGMs), which are supported by an information infrastructure) employment in operations can be presented according to a priority-ranked subprocess:

- Determination of parameters of the concept of organizing the planning and conduct of demonstration strikes by long-range PGM;
- Substantiation of variations of the concept of limited strikes for deescalating the military conflict and compelling the enemy to cease armed confrontation;
- Development of the concept of the **strategic operation to destroy critically important enemy facilities**.[364]

The authors added that in the makeup of the special mathematical and software support (SMPO) for employing long-range PGM forces, a central place must be set aside for use against systems of complex-structure targets. Calculations must be oriented toward correlating the combat capabilities of long-range PGM groupings with weapon targets; and optimization problems can be used to solve operational issues, to include:

- Determination of the mix of long-range PGM forces (weapons) for performing missions of destroying key facilities in RF Armed Forces general-purpose force operations;
- Determination of the mix of long-range PGMs for participation in a **strategic operation to destroy critically important facilities [strategicheskaya operatsiya po porazheniyu kriticheski vazhnykh obyektov] (SOKVO).**[365]

Finally, in 2015 the Aerospace Forces (VKS) noted that its missions were to do the following: reconnoiter the aerospace situation; uncover the beginning of an aerospace air and missile attack; notify state and military command and control entities about it; repel aggression in the aerospace

---

[361] Marina Yeliseyeva, "Lessons for All Time," *Krasnaya Zvezda (Red Star) Online*, 27 October 2010.
[362] Ibid.
[363] Vasiliy Y. Dolgov,and Yuriy D. Podgornykh, "Space As a Theater of Military Operations: On Possible Forms and Methods of Combat Employment of Space Command Forces and Assets," *Vozdushno-Kosmicheskaya Oborona Online*, 10 April 2013.
[364] A.A. Protasov, V.A. Sobolevskiy, and V. V. Sukhorutchenko, "Planning the Use of Strategic Weapons," *Voennaya Mysl'* (*Military Thought)*, No. 7 2014, pp. 9-27.
[365] Ibid.

sphere; protect command and control facilities of top echelons of state and military command and control, administrative-political centers, industrial and economic areas, and important facilities of the country and troop groupings against attacks from space and from the air; **destroy critically important enemy facilities** and troops by employing conventional and nuclear weapons (the term "strategic operation" was missing but by adding the term "nuclear," strategic operations seem to be implied); provide air support and support to combat operations of troops of Armed Forces branches and combat arms; and support launches of spacecraft (MBR [ICBM] launches) and their control in orbital flight.[366]

Thus, while the term is used sparingly, it has been observed in specific places. It's use in conjunction with aerospace forces or precision-guided munitions is significant, since they both possess long-reach capabilities to the depth of an adversary's territory anywhere on the globe. Russian planetary warfare theorists must find such concepts intoxicating.

Forms and Methods[367] of Information's Use

A consistent element of a Russian planners thought process is to examine the forms and methods of a capability's use. This element applies to information topics as well, as demonstrated by S. A. Komov who a few years ago wrote an article "On the Methods and Forms for the Conduct of Information War" and by the many authors after him who covered similar ground. In a recent Russian military article on the army's military-political instructional plan for 2019, forms and methods were mentioned prominently in several categories.[368]

A definition of a form and a method along with their use in an information sense is listed below:

> A "form" is an organization, which in regard to information warfare could include international media elements such as *Russia Today or Sputnik* or military developments, such as the creation of cyber and electronic warfare "science companies;" a cyber corps, which was announced in 2013 but for which no further information has been provided; information operation forces, announced in 2017; and the Advanced Research Foundation, Russia's equivalent to the US's Defense Advanced Research Projects Agency. These forms or organizations implement methods.
>
> "Methods" are broken into two parts, weaponry and military art. Weaponry includes hackers, reflexive control techniques, trolls, disinformation, deterrence capabilities, killer satellites, and other agents of destruction or influence. Military art includes the use of indirect and asymmetric capabilities to achieve specific goals, such as the exploitation of the West's free press or an indirect attack on the cyber infrastructure of another nation. Russia's excellent contingent of algorithm writers ensures that the nation will be strong for years to come in writing software as weapons that can eavesdrop, persuade, or destroy.[369]

---

[366] Viktor Bondarev interview by V. Kutishchev, "Russian Aerospace Forces," *Armeyskiy Sbornik (Army Journal)*, No. 3 2017, pp. 33-34.

[367] For a discussion of Russia's forms and methods of operations, see Timothy Thomas, "Russia's Forms and Methods of Military Operations: The Implementors of Concepts," *Military Review*, May-June 2018, pp. 30-37.

[368] No author provided, "Instructional Plan for the Military-Political Preparation of the Armed Forces of the Russian Federation in 2019," *Armeyskiy Sbornik (Army Journal0*, No. 11 2018, pp. 91-101, as downloaded from https://dlib.eastview.com on 16 January 2018.

[369] Statement by Mr. Timothy L. Thomas, at the time Senior Analyst, Foreign Military Studies Office, Fort Leavenworth, Kansas before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, First Session, 115TH Congress, On Russia's Information War Concepts, March 15, 2017.

It is important to continue to study information forms and methods of conflict. They can be some of the most subliminal or deceptive forms of manipulation and are always being updated in Russian information warfare circles.

Information and Digital Deterrence

In both 2015 and 2016 Ukraine's power was turned off due to a cyber-attack that, to Ukrainian experts, originated in Moscow. The so-called "Black Energy" malware causing the events has also been spotted on the US grid, according to a 2017 *Wired* article. The author summed up the events in the following manner:

> By turning the lights out in Kiev—and by showing that it's capable of penetrating the American grid—Moscow sends a message, warning the US not to try a Stuxnet-style attack on Russia or its allies like Syrian dictator Bashar al-Assad. In that view, it's all a game of deterrence.[370]

It is important to know how Russia both defines and employs its deterrence concepts, so that issues don't escalate out of control simply due to a misunderstanding of terminology or practice. Russian and US understandings of terms like nuclear deterrence, nonnuclear deterrence, and information deterrence may differ—or not exist in both nations. It is well-known that a key component of EUCOM's theater strategy is to deter conflict.

There have been several Russian military or civilian ways to define deterrence in the past decade. In 2008 retired General of the Army Makhmut Gareev, the President of the Academy of Military Science, defined strategic deterrence as an asymmetric approach and part of a set of interrelated political, diplomatic, information, economic, military, and other measures that deter, reduce, or avert threats and aggressive actions by any state or coalition of states with threats of unacceptable consequences as a result of retaliatory actions.[371] In the Russian Defense Ministry's 2011 *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space*, deterrence was seen to exist as a conflict prevention asset in information space in the following way:

> Deterrence and conflict prevention: develop an information security system for the Russian Federation's Armed Forces that can deter and resolve military conflicts in information space; remain in a constant state of readiness; expand the group of partner states; conclude, under UN auspices, a treaty on international information security; establish control over the escalation of conflict; take priority steps to counter the development and spread of a conflict; neutralize factors leading to the conflict's spread; and shape public opinion means to limit the ability of instigators to further escalate the conflict.[372]

In 2012, in *Military Thought*, two authors noted that deterrence types are those involving the threat of force or those that are nonmilitary and indirect (asymmetrical). A force can be either offensive or a powerful defensive task force; it could be an ultimatum; or it could be the use of an information campaign to mislead an adversary about Russia's ability to confront aggression and thereby deter him from acting.[373] In 2015 Russia's *National Security Strategy* defined strategic deterrence as the

---

[370] Andy Greenberg, "Lights Out," *Wired*, July 2017, p. 61.
[371] M. A. Gareev, "Strategic Deterrence: Problems and Solutions," *Krasnaya Zvezda (Red Star),* No. 183, 8 October 2008, p. 8, as downloaded from Eastview.com on 17 March 2010.
[372] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministry of Defense of the Russian Federation*, 2011.
[373] S. G. Chekinov and S. A. Bogdanov, "Initial Periods of War and their Impact on a Country's Preparations for Future War," *Voennaya Mysl'* (*Military Thought)*, No. 11 2012, p. 26.

result of interrelated political, military, military-technical, diplomatic, economic, information, and other measures, to include maintaining the capacity for nuclear deterrence.[374]

To deter or counter threats (which appear to include the US's Prompt Global Strike concept; a global Anti-Ballistic Missile (ABM) system; color revolutions; cyber-attacks; and an ISIS threat to the south) to Russia, Putin's staff is employing some old methods and developing new ones. Naturally nuclear deterrence remains at the top of the list of ways to counter threats from the US. Russia has two terms for deterrence, *sderzhivanie* and *ustrashenie.* The military uses the former much more often than the latter and defines it as containment, used to limit the development of weapons or the use of military activities. The latter is defined as deterrence through intimidation or fear. In effect, the terms seem to be complimentary. Frightening someone can result in their containment. Containing someone can result in their being frightened.

A 2016 discussion of deterrence in the information age appeared in the journal *Military Thought*. It was written by several Russian information specialists, with recommendations as to how to avoid information age conflict. On the one hand, the authors note, deterrence is based on the build-up of a state's military capabilities, while on the other hand, preventing military conflicts is often based on the proportional reduction of military potentials. It appears that the joint functioning of these two items are required to stabilize the international situation.[375] However, new means for deterring conflict are evolving. While the Cold War primarily witnessed nuclear deterrence, a period of nonnuclear deterrence has followed with an emphasis on precision weaponry. A potential new deterrent trend that has appeared is "hostile information" (information-technical, information-psychological) activities that can violate state sovereignty or interfere in a state's internal affairs.[376] The authors made a reference to the 2014 edition of Russia's *Military Doctrine* under the section titled "organization and conduct of the information struggle," where a task of the Armed Forces was stated to be the development of forces and means of information confrontation which can deter opponents. "Means" of information confrontation (struggle) the authors listed include the following:

- Technical reconnaissance resources (used to obtain information by allocating parameters of various types of physical fields);
- Information resources (information used to influence knowledge, moral values, motives, and behavior stereotypes of individuals, collectives, and the public consciousness in order to form certain behaviors);
- Psychotronic resources (make it possible to covertly control consciousness, psychological processes, and the behavior of people);
- Special hardware and software effects (computer viruses, worms, and Trojan programs used to steal, destroy, and/or modify information of databases, block their access, or breach computer functions);
- And resources for protecting information (technical, cryptographic, and software resources designed to limit the acquisition of information due to leakage).[377]

---

[374] "The Russian Federation's National Security Strategy," *President of Russia Website*, 31 December 2015.
[375] I. N. Dylevskiy, V. O. Zapivakhiyn, S. A. Komov, S. V. Korotkov, and A. A. Krivchenko, "On the Dialectic of Deterrence and the Prevention of Military Conflicts in the Information Age," *Voennaya Mysl'* (*Military Thought)*, No. 7 2016, p. 5. The author thanks Dr. Harold Orenstein for his translation of this article from Russian into English.
[376] Ibid., p. 6.
[377] Ibid., p. 8.

New means of strategic deterrence now include information weapons, the authors note. There must be a method for selecting targets according to a "cost effectiveness" criteria. The effect of attacks on the economy, financial systems, and the information infrastructure must be monitored. Since information weapons can be employed in conjunction with precision guided weapons, one must determine the necessary quantity of resources for nonnuclear (precision and information) deterrence. Finally, the thoughts of an adversary's leadership must be considered, that is, a nonnuclear attack could cause an adversary to resort to nuclear or nonnuclear means.[378]

Russia has employed other forms of information deterrence. In November 2015, Russian TV used information as a deterrent when it carried images of supposed "top secret" schematics of a Russian naval torpedo, the Status-6. The torpedo allegedly carries nuclear warheads and supposedly can travel up to 10,000 kilometers, making it capable of striking the western shores of the US and creating a tsunami in the process. The Russian press labeled this action as "deliberate stove piping" to deliver an information bomb. The torpedo would be impossible for either Prompt Global Strike or a Global ABM to detect or intercept. Of interest is that the torpedo's development may not even be complete,[379] but just the suggestion of such a capability can help to deter an opponent, who is uncertain as to the validity of the claim.

In 2017 Russian military expert Valery Mukhin noted that the use of inspector satellites can serve as a serious deterrent. This is because with the system, Russia can check on whether the stated functions of a satellite are true or not. Such a satellite can maneuver between orbits and is effective in peacetime.[380]

A lack of information can serve as a deterrent as well. A Russian satellite "parked itself between two Intelsat satellites in geosynchronous orbit for five months this year" and maneuvered at times to within ten kilometers of these vehicles.[381] Roscosmos declined to comment on the matter, and the Russian Defense Ministry said it would "look into the situation."[382] This maneuvering's lack of specific information as to the satellite's goals "implied" (that is, it lacked information) capabilities (attack, reconnaissance, inspection?) that could not be ascertained. Thus, the absence of information can serve as a deterrent just as much as its presence.

With regard to legal deterrence, Russia is using the UN to support its legal claims to areas it says are within the nation's proclaimed "national interests." This applies to the Arctic, where Russia has spent much time and money mapping the Arctic Sea. If Russian representatives can prove their case with images or numbers, based on digital mapping of the area, it may be able to reserve for itself exclusive access to the region's oil and gas riches. Russia would, in effect, deter other nations from the region through the use of digital (information) assets.

Perhaps more importantly, Russia wants a United Nations resolution on specifics of the information sphere. This includes criteria for types of information effects and acts of aggression; a way to regulate the identification and authentication of sources of information effects; and standards for investigating information effects to include a method for collecting evidence.[383]

---

[378] Ibid., pp. 8-9.
[379] Konstantin Sivkov, "Essential and Sufficient: Status-6 System Leaves an Adversary No Choice," *Voyenno-Promyshlennyy Kuryer Online (Military-Industrial Courier Online)*, 2 December-8 December 2015.
[380] S. Valchenko, N. Surov, and A. Ramm, "Russia Sends Inspector into Orbit: Military Test Operations of Maneuvering Identification and Intercept Satellite," *Izvestiya Online*, 26 October 2017.
[381] No author or title provided, *Interfax* (in English), 12 October 2015.
[382] Ibid.
[383] "On the Dialectic of Deterrence…," p. 10.

A conclusion to be reached here is that Russia has noticed that technological progress is changing the means and parameters by which to deter an opponent. Russia's leaders appear to believe that by exposing weapon capabilities, as Putin did in his March address to the nation describing new weaponry and as Russia had done earlier with its Status-6 torpedo, that the threat can be neutered through what might be termed information deterrence, that is, stating again and again that no analogous systems exist in the world to counter Russian equipment. The nature of international relations is changing as well, as we are now much more connected globally than ever before—by the media, satellites, and optical fiber. Russia is working to create a system of strategic deterrence that takes advantage of these changes, both nuclear and nonnuclear, to contain and intimidate its neighbors and their partners.

One final consideration for the future is whether artificial intelligence or quantum computer discoveries will add an unexpected type of deterrence, that being deterrence based on a capability to gaze into any adversary's cyber system. The military has invested in a host of new technologies that will enable Russia to influence events in directions they desire on the battlefield. Rostelecom will test a data transmission network using quantum technologies in early 2019, according to one report.[384]

The military has been writing about artificial intelligence since 1996, when they published such an article in *Armeyskiy Sbornik (Army Journal*). President Putin's official website noted that the main goal of a new park titled Era Technopolis is to create military artificial intelligence systems and supporting technologies. This will be a place for young scientists of technical capabilities to work.[385] Worries abound, of course, of the consequences of using artificial intelligence. For example, Russia's Deputy Speaker of the Duma stated that the speedy preparation of laws concerning artificial intelligence are needed soon. There are ethical issues to consider as well as ways to compensate for robotic mistakes or how to handle copyright laws. There will also be increased social tensions as jobs are lost to robots.[386]

The military, however, doesn't see these issues as too constraining. Deputy Defense Minister Yuriy Borisov noted that "artificial intelligence technologies will help to provide effective countermeasures in information space." "Whoever can control this [information space], whoever organizes countermeasures in the right way, is the victor."[387] As weapons and the nature of conflicts change, he notes, high-speed, high-precision, and high-performance is needed, and artificial intelligence helps provide these attributes.[388]

In September 2018 there was an added discussion of the Advanced Research Foundation and its work on artificial intelligence. The Deputy General Director of the foundation, Sergey Garbuk, said he understands artificial intelligence to be "technologies that allow for accomplishing a number of applied tasks that man accomplishes well owing to his natural intellectual capabilities."[389] Intellectual tasks are identifying shapes, processing human speech, separating objects against complex backgrounds, and predicting the behavior of complex systems. Competitions organized by the foundation so far have been dedicated to converting complex

---

[384] No author or title provided, *Interfax* (in English), 17 October 2018.
[385] *Official Website of the Russian Federation President* (in English), at http://en.kremlin.ru, 23 February 2018.
[386] No author or title provided, *Interfax* (in English), 10 January 2018.
[387] No author listed, "Development of Artificial Intelligence is Essential to Conduct Cyberwarfare Successfully," *Ministry of Defense of the Russian Federation*, 14 March 2018.
[388] Ibid.
[389] Interview conducted by Igor Yermachenkov with Sergey Garbuk, no title offered, *Advanced Research Foundation*, 26 September 2018.

Russian speech to text, facial recognition in complex conditions, creating aerospace imagery interpretation technologies for identifying concealed structures, and technologies for the automated smart monitoring of an operator's manual operations to spot deviation from established technique routines.[390]

Information Troops

Russian military expert Aleksandr Perendzhiyev, working for the Association of Military Political Scientists, noted that victory is now forged in virtual space as much as on the battlefield. Former Soviet KGB Analysis Directorate Chief Vladimir Rubanov noted that "information space realistically is becoming a sphere of military activity on an equal basis with theaters of military operations on land, at sea, and in aerospace."[391] As a result the development of information operation troops became another priority, especially since Russia felt it was lacking specific forces on the modern battlefield, where information space was playing an ever-larger role.

In February 2017 this shortcoming was rectified when Defense Minister Sergey Shoygu stated that information operation troops had been created. They are, he noted, more effective and stronger than the old directorate known as counterpropaganda. Further, an information conflict class is now reportedly taught at the General Staff Academy. Shoygu stated that the troops must distinguish themselves through offensive actions, and that cyberspace is an area of responsibility for information troops. Stating that he does not intend to call hackers to arms, he still sees advanced specialists in cyber technology as "indispensable," and he also sees a mission for propaganda specialists.[392] Currently three prominent specialists have carried much of the propaganda work load for the nation, and they must be supplemented with new support mechanisms. They are, in the Foreign Ministry Information and Press Department, Mariya Zakharova; in the Defense Ministry Press Service and Information Directorate, Major General Igor Konashenkov; and in the Presidential Press Secretary, Dmitriy Peskov.[393]

Control over the activities of troops online is another area of interest to Russian military policy. The most recent law "On the Status of Servicemen" states that army personnel are forbidden to disclose on the Internet or in the mass media any information "about themselves and their colleagues which could reveal their official assignment, the details of their official activities, or their basing location."[394] Photographs, videos, and geotags on social networks were specifically mentioned. Odnoklassniki (classmates), VKontakte (in contact), and Facebook were websites and social networks particularly mentioned as those not to use. The ban does not extend to citizens who have been discharged from the Armed Forces.[395] Monitoring will also be conducted on the online activities of students at military institutes. The InfoWatch Traffic and the Device Monitor programs reportedly can detect confidential files in a stream of data as well as disloyal employees, according to Yekaterinburg-based website Znak.com.[396]

---

[390] Ibid.
[391] Mariya Latsinskaya, Aleksandr Braterskiy, and Ignat Kalinin, "Russia Sent Troops onto the Internet: Shamanov Explained Why Information Operations Troops Are Necessary," *Gazeta.ru*, 22 February 2017.
[392] Oleg Odnokolenko, "Shoygu Orders Information Troops to Take Offensive. Military Propaganda Body Comes into Operation in the Defense Ministry," *Nezavisimaya Gazeta Online*, 27 February 2017.
[393] Ibid.
[394] Marina Yurshina, Tatyana Berseneva, and Aleksandr Kruglov, "The Secret Selfie: Military Banned from Writing about Themselves on Social Networks," *Izvestiya Online*, 23 October 2018.
[395] Ibid.
[396] No author or title listed, *Znak.com*, 23 October 2018.

In addition to correcting these internal issues, the military's intelligence service, the GRU (Russian Military Intelligence Service), has been involved in a host of influence operations abroad and there appears to be no restriction on their activities. A January 2017 edition of *Moscow Defense Brief*, titled "Russian Information and Cyber Operations," stated that the GRU's 12th Main Directorate may be responsible for information warfare and cyber operations. The same report noted that in 2012 Russia's Defense Ministry established a Cyber Command, that is, five years before Shoygu announced the development of information troops. The command's objectives were stated to be global and large-scale information operations, targeting both individual provinces and entire countries or continents.[397]

One important accusation of GRU activity was a report in *The Daily Beast* that stated Guccifer 2.0, an alleged hacker who provided WikiLeaks with stolen emails from the Democratic National Committee, was a GRU operative. Attempting to appear as a lone Romanian hacker, Guccifer on one occasion failed to "activate the VPN client before logging on. As a result, he left a real, Moscow-based Internet Protocol address in the server logs of an American social media company."[398] The IP address allowed U.S. investigators to identify Guccifer 2.0 as a GRU officer and the address (Grizodubovoy Street in Moscow, GRU Headquarters) where he worked.[399]

Information-Technical and Information-Psychological Capabilities

For at least the past 25 years, Russia has broken its information war theory into information-technical and information-psychological categories. Today, the two aspects are more integrated than ever before. For example, an information-technical cyber-attack against another nation's banking industry exposes or manipulates data about the banking industry that causes fear or even information-psychological panic in the general population. Or consider how the exposure of an information-technical achievement such as the Status-6 torpedo (now known as Poseidon), which can be nuclear armed, could have an enormous impact on the information-psychological stability of a US coastal region that could be a target of such a torpedo. They work together.

In 2015 retired Russian officers S. G. Chekinov and S. A. Bogdanov stated that, for future war goals to be successful, an information strategy is required that secures information superiority over an adversary. This can be accomplished in the media realm by stirring up chaos and confusion in a country and instilling ideas of violence, treachery, and immorality to demoralize the public.[400] Such information-psychological attacks require, from Russia's perspective, that all mass media be placed under government control and direct the main efforts in the information struggle against a probable aggressors' government and military control systems. Information superiority can even create conditions for a government to achieve its political objectives in peacetime.[401] In regard to information-technical attacks, chaos can be increased when attacks are launched against the hardware and software of an adversary's information and telecommunication environment in order to damage it.[402]

---

[397] Aleksey Ramm, "Russian Information and Cyber Operations," *Moscow Defense Brief*, No. 1 2017, pp. 16-17.
[398] Spencer Ackerman, "Exclusive: 'Lone DNC Hacker' Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer," *The Daily Beast*, 26 September 2017.
[399] Ibid.
[400] S. G. Chekinov and S. A. Bogdanov, "The Initial Periods of Wars and their Impact on a Country's Preparations for Future War," *Voennaya Mysl'* (*Military Thought)*, No. 11 2012, pp. 26-27.
[401] Ibid., p. 27.
[402] Ibid., p. 25.

A 2017 article in the *Journal of the Academy of Military Science* in Moscow stated that hiding from the powers of influence is difficult, since they are developing both conscious and subconscious influences on people.[403] Technologies of influence are now capable of producing information-psychological and information-technical effects that outdo the effects of armament systems and hardware. The goal of information action is to redirect forces from destroying an adversary to unconditionally subjugating him. Some influence actions are equivalent to the use of military force.

Modern power, the authors add, rests on an inventory of the following means (or strategy) to wage information war realistically. They are arranged here in three groups: primary information warfare means, information support means, and the regular armed forces. All play different information-technical and information-psychological deterrent roles:

A. Primary: training groups to plan and wage information war; developing information warfare theory and a record of waging it; legal frameworks that allow for information warfare to be waged in peacetime and wartime; development of organized structures for waging information warfare; and the use of world-renowned academics.
B. Support: technical intelligence; specialized intelligence service; navigation aids; electronic warfare capabilities; information-telecommunications network development; high-speed computers and complex software; worldwide internal media centers; human rights organizations; and a movie industry, audiovisual industry, and computer (virtual) games industry.
C. Regular: strategic nuclear forces; ballistic missile defense systems; precision-guided munitions; naval forces; and special forces.[404]

Information warfare is now a preferred method of attack, since it can be used liberally while nuclear weapons cannot. New forms and methods of information's use will be applied based on 21st century technological breakthroughs. The basis for long term success will be preparing key groups of personnel for waging information warfare. Future information power will be based on preparing young people to compete in information warfare studies, specifically mathematics and physics in high schools. These topics will increase in the number of hours taught by two hours each week.[405]

The terms information-technical and information-psychological are still used widely today by officers as prominent as General Staff Chief Valeriy Gerasimov. In Gerasimov's 2018 presentation to the Academy of Military Science, for example, he noted that the roles of both information-technical and information-psychological actions are expanding.[406] At other times, these two aspects of information warfare are often implied but not directly stated. For example, in the 2011 document titled *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space*, discussed above, the authors subdivided the definition of information war into four parts. The relationship of the parts to the information-technical and information-psychological components is obvious. The first part was confrontation designed to cause damage to information

---

[403] V. K. Novikov and S. V. Golubhikov, "Analysis of Information War in the Last Quarter of a Century," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 3 2017, p. 10.
[404] Ibid., p. 14.
[405] Ibid., p. 16.
[406] Valeriy Gerasimov, "The Influence of the Contemporary Nature of Armed Struggle on the Focus of the Construction and Development of the Armed Forces of the Russian Federation. Priority Tasks of Military Science in Safeguarding the Country's Defense," *Vestnik Akademii Voennykh Nauk (The Journal of the Academy of Military Science)*, No. 2 2018, p. 18.

systems processes and resources, and to critically important structures (information-technical). The second was confrontation with the objective of undermining the political, economic, and social systems of Russia (could include active measures, information-technical, or information-psychological measures). The third objective was to carry out massive psychological manipulation of the population to destabilize it and the state (information-psychological). Finally, the objective of the confrontation was to compel a state to make decisions that are in the interests of its adversary (which is a reference to a component of disinformation, namely reflexive control).[407] Some recent information-technical and information-psychological observations follow.

Information-Technical

The information-technical aspect of Russia's information war theory has been well covered regarding weaponry. Most weaponry today possesses some degree of information-technical quality and relies heavily on algorithm use. Such developments include cyber forces, precision-guided weaponry, satellite functions, electronic warfare equipment, radars, and numerous other pieces of equipment that employ digital components. Covered here are the information-technical systems that drive information security issues for the Defense Ministry.

There were several technological issues that help Russia ensure the acquisition of information superiority for its internal systems. In 2016, the military completed a "closed data transfer segment" communication system that is independent from the Internet. It is accessible only on special licensed computers using a Defense Ministry dedicated operating system.[408] In May 2018 it was noted that either this project or one very similar to it had "received a boost" in the form of a budget item to "provide for the creation of an integrated communications network for the needs of national defense, national security, and law enforcement."[409] Russian Communications and Mass Media Minister Nikolai Nikiforov stated in the article that it was possible to create a backup Internet infrastructure element in Russia.[410]

Other technical issues were under discussion as well. First, the Defense Ministry reported it no longer trusts the Windows operating system, relying instead on the Russian Astra Linux operating system. The Russian Federation's National Defense Operations Center is based on this system. It is envisioned that one day the system will be loaded on special smartphones and tablets. The security system includes Russian-made Elbrus, Baykal-T1, and Komdiv processors, the heart of a generation of supercomputers. It was further noted about Astra Linux that:

> The operating system kit includes the office application LibreOffice. The Pergament electronic document management system is used for secure communications. It is possible to install the Panorama geoinformation application to create and edit digital maps and city plans. The operating system is compatible with such popular Russian software products as the 1S accounting system and the Kaspersky and Dr. Web anti-virus programs.[411]

Second, Russia is making progress in the development of quantum cryptology systems and post-quantum cryptographic systems. They are essential for protecting information, such as future

---

[407] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministry of Defense of the Russian Federation*, 2011, p. 5.
[408] No author or title provided, *RT Online* (in English), 13 February 2018.
[409] No author or title provided, *Interfax* (in English), 11 May 2018.
[410] Ibid.
[411] Aleksandr Kruglov and Aleksey Ramm, "Military Says Goodbye to Windows: Defense Ministry Will Put Russian-Produced Operating System on Service Computers," *Izvestiya Online*, 9 January 2018.

attacks generated by an adversary's quantum computers.[412] One recent report noted that Russia expects its first quantum computer to appear in the fall of 2021. It will have not less than 50 qubits, and be capable of creating more accurate weather forecasts, have the ability to crack codes and set up complex passwords, and improve predictions of new material science, engineering problems, and the properties of pharmacological drugs.[413]

Third, a park-complex known as the Era Technopolis is under construction. Its objectives include developing innovative technology, helping to reduce the time required to build arms and special equipment, and educating highly skilled personnel for military research institutes. The Technopolis is stated to work for the "Russian army elite" and is designed to ensure the nation's lead in the military-technical sphere. It is organized into three clusters, scientific-research, scientific-educational, and scientific-production. The Era Technopolis is another step on the way to reinstate central research institutes and applied research in military institutions.[414]

Russia has developed 12 different science companies, one of which is dedicated to information security. These companies include specially selected young draftees out of a university who are allowed to perform their military duty alongside experts in the field from the military-industrial complex, enabling them to learn from skilled scientists. The information security company has been working for three years. The company has several functions: it helps perform research and along with mathematicians helps validate the use of various cryptographic protocols and devices; conducts research in special communications and various kinds of electronic equipment; and conducts research along with systems programmers working in the information security field. The company allows young people to become involved in a military science environment, expand their cooperation with defense enterprises, and improve the quality of scientific work and protect state secrets.[415]

Finally, Russia's Defense Ministry had developed a closed access "military Internet" (the term "Intranet" was not used in the article describing the system). As computerized processes have risen along with the number of information sources, such a system helps shape a safe information and telecommunication infrastructure using technology based on domestic developments.[416] The first indication of this system came in 2016, in a *Red Star Online* report:

> The deployment by the Armed Forces of Russia of a military Internet, a communications system officially named 'Classified Data Transmission Segment' (ZSPD), has been completed. The military network is not connected to the global Internet, and all computers connected to it have protections against connections to uncertified flash drives and external hard discs.[417]

Military personnel reportedly have their own electronic mail service, and the military Internet has its own websites. The networks home page is accessed at the "mil.zs" address. Access is available on certified computers, which work on the Armed Forces Mobile System. It is the State Secrets

---

[412] No author provided, "Ministry of Defense Ponders Development of Quantum Cryptology Machines," *RIA Novosti*, 1 February 2018.
[413] Mariya Nedyuk, "A Quantum Computer Will Appear in Russia Three Years from Now. It Was Previously Anticipated that this Would Take Five Years," *Izvestiya Online*, 7 May 2018.
[414] Inna Sidorkova, "Military Skolkovo: Why Shoygu is Building a Technopolis in Anapa," *RBK Online*, 13 March 2018.
[415] Yevgeniy Miroshnichenko, "Company of Creative Thought; This Scientific Unit Has Trained Effective Personnel in the Field of Information Security for Three Years," *Krasnaya Zvezda (Red Star) Online*, 20 September 2017.
[416] No author or title provided, *Interfax* (in English), 18 September 2018.
[417] Vladimir Zykov and Aleksey Ramm, "A Military Internet has Appeared in Russia: The Classified Data Transmission Segment Allows Ministry of Defense Components to Safely Exchange Secret Information," *Krasnaya Zvezda (Red Star) Online*, 19 October 2016.

Protective Service, also known as the Eighth Directorate of the General Staff, that performs the certifications. The American example, the authors note, had many holes with different protocols and networks under different management. So many connections to the Internet allowed someone like Edward Snowden to do serious damage to the US. The Russian article stated that it is the hope of the military to avoid such damage.[418]

Later it was announced that the Russian military-industrial complex will get their own secret Internet, designated as the "Protected Communication System" (Sistema Zashchishchennykh Svyazey or SZS). Work on the system was to have been completed at the end of 2017. Both defense enterprises and science companies will use the system and be able to transmit data with at least 10 Mbps of bandwidth. Only special Astra Linux operating systems using the Armed Forces Mobile System will work on the network.[419]

Information-Psychological

Information-psychological measures are discussed often in Russian military journals. These discussions rarely make front page news in the West, but they are vitally important to understanding an authoritarian regime. Military officers consider information-psychological aspects of information warfare to no longer be "add-ons" but rather as key components of waging war. The articles do not discuss what Russia is doing but rather what they believe the West is doing to Russia.

The discussion below begins with a 2015 article from the journal *Military Thought*, followed by three articles from the *Journal of the Academy of Military Science (AMS)* (all three from 2017), and two 2018 articles from *Army Journal*. The articles describe what Russia believes are Western attempts to destabilize Russian society's values and incite a color revolution there. Westerners would consider the list of methods that Russia authors state the former is using against the latter to be just what the latter is doing to the former!

A 2015 article in the journal *Military Thought* discussed the information-psychological aspect of information warfare. The authors described information as a strategic national resource that penetrates all spheres of life, making it problematic to collectively protect the security of individuals, society, the state, and its institutions. The authors defined information warfare (IW) in ways that they believe an adversary would use the concept against Russia. These ways included the use of technologies to create deliberately false information or distort existing information. Such IW use is designed to influence the civilians and servicemen of other states through the spread of information; and to damage information-related processes and systems of an adversary to achieve information superiority.[420] An information impact is achieved, they note, by distorting facts or imposing emotional perceptions favorable to the influencing side. The use of information vacuums and alien ideas are practiced, and there are attempts to involve Russia in unwanted conflicts, to induce public hatred among Russians toward their own state, or to stage a color revolution. An image of Russia is thereby produced that is tyrannical, backward, and aggressive.[421] The use of misinformation or slanted information helps promote a defeatist mood. The downing of the Malaysian airliner in July 2014 is indicative of this type of activity.[422] [Note: again, this is how

[418] Ibid.
[419] Vladimir Zykov and Aleksey Ramm, "Defense Enterprises to Get Their Own Internet—Secret Technical Information to be Shared on the Protected Network," *Izvestiya Online*, 31 October 2016.
[420] I. V. Puzenkin and V. V. Mikhailov, "The Role of Information and Psychological Means to Ensure the Country's Defense Capability," *Voennaya Mysl'* (*Military Thought)*, No. 7 2015, p. 11.
[421] Ibid., p. 12.
[422] Ibid., p. 13.

Russia is interpreting events for their soldiers. As is well known, an international forum has condemned the Russian version of events and directly blamed Russia or the insurgents for the tragedy, but Russian theorists refuse to accept this proven view.].

The rest of the article was more general, describing the power behind today's use of information technology. Information's spread through the Internet and social media can destroy values, culture, and language on the one hand; or be used in systems to precisely control advanced weaponry. The authors note that the center of gravity is shifting. It no longer lies with the use of power alone but is shifting to information methods and means using covert and other subtle capabilities. War in general is becoming super technological where informatization and automated systems are now crucial to victory. Information parameters are determining the efficiency of modern weapons, especially those involved in electronic warfare.[423] Information confrontation has become so great that the period between war and peace is being obliterated. Cold Wars are gaining in scale and political effect. Information infrastructures are under constant threat of major disasters. An opposing force can now cause accidents, disorganize state governance and the functioning of financial systems, and cause defeat by merely actuating specific information or cyber components via computer networks.[424]

In the first 2017 *AMS* article, it was stated that technological enslavement had replaced military colonization as the primary method to acquire territory.[425] Manipulating people involves the creation of information and images, where the image becomes more important than the content itself. Recoding the consciousness of a population is a major aspect of the information revolution, and the object of such influence is the subconscious.[426] Here the power of narratives and meanings play a large role. Social technologies are a set of forces and means interconnected by smaller goals (psychological, informational, and ideological) aimed at achieving the stated larger goal, regardless of the interests and aims of the society and the population being acted upon.[427] Using these technologies to destroy statehood involves destroying traditions, religious norms, common ethno-cultural characteristics, networks that integrate central and regional relations, and the education system. This is accomplished with the use of hidden subversive technologies and tools for destroying internal bonds of statehood; and ensuring the absolute geopolitical domination of the aggressor state over the attacked country's state system and depriving it of economic and resource-based self-sufficiency, among other issues.[428] The author described how a color revolution, a term applied to the methods used to create regime change (in Ukraine it was called the orange revolution and in Georgia the rose revolution), is initiated:

- The socio-political and economic system of a country is destabilized, plunging it into a state of "controlled chaos."
- Conditions are created for "managed chaos" within the transformed state system to attract an opposition center.
- The aggressor focuses efforts on creating a new state system.

---

[423] Ibid., p. 14.
[424] Ibid., p. 15.
[425] V. N. Remarchuk, "The Destruction of the Modern State System by Means of 'Social Technologies'," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2017, p. 46. The author would like to thank Stephen Hunnewell for his help with this translation.
[426] Ibid., p. 47.
[427] Ibid., p. 48.
[428] Ibid., p. 49.

- Finally, the aggressor resolves that task of strengthening state institutions of the country under its control by forming, training, and equipping the power and administrative structures of the once-attacked state.[429]

In the second *AMS* article from 2017, the authors stated that the age of information warfare has become an objective reality for all nations. Information's "technological mode" stimulates diverse capabilities for information-psychological influence on people, to include the ability to move the behavior of society's consciousness in a needed direction.[430] Revolutionary situations are created in target states, which then permit regime change. The goal of information actions is to redirect the interests of the population toward unconditional subjugation. This is a multi-directional approach of a non-military character, and it can be equivalent in results to the direct use of military force.[431]

More importantly, the authors list an inventory of 21 capabilities (both information-technical and information-psychological) that modern powers require in order to wage information warfare without regard for the United Nations and other world states. The inventory initially listed several branches of service but then listed several IW means: technical intelligence; specialized intelligence services; navigation aids; electronic warfare capabilities; global communication systems; and high-speed computers and complex software. Specific IW components were:

- International media centers
- Military bases abroad
- Numerous human rights organizations and human rights activities abroad
- A movie industry and an industry to produces computer (virtual) games
- Private military companies
- Systematic training for how to plan and wage information warfare
- A theory about information warfare and track record of waging it
- A legal framework that allows for information warfare to be waged during times of peace and war
- Organized structures for waging information war
- The need to use world-renowned academics, such as Nobel laureates[432]

Information-psychological aspects of warfare will no longer be viewed as "add-ons" but rather as key components of waging war, the authors note. It is a preferred method of attack and it will be used in training for and waging information warfare, and in scenarios. Forms and methods of its application will rely on 21st century breakthrough technologies. Training key groups of personnel for waging information warfare will be the basis for long-term success. Increasing the number of hours dedicated to mathematics and physics in high schools will provide Russia with future power in the information sphere.[433]

In the third article from 2017 in *AMS*, the authors listed the principal reasons and condition for the escalation of the information struggle to the level of information warfare. Sixteen reasons were listed, but only a few were related to information issues. They included the following information-escalation-related reasons: there has been an increase in resources devoted to influencing human

[429] Ibid., p. 50.
[430] V. K. Novikov and S. V. Golubhikiv, "Analysis of Information War in the Last Quarter of a Century," *Journal of the Academy of Military Science*, No. 3 2017, p. 10. Dr. Harold Orenstein translated this article from Russian into English.
[431] Ibid.
[432] Ibid., pp. 13-14.
[433] Ibid., p. 16.

consciousness and subconsciousness, with the end goal being behavior control; the hegemony of the West in nanotechnology, biotechnology, information and telecommunications technology, energy, and science as a whole on the basis of a new technical structure—information—has caused other nations to respond in kind; and the fact that information warfare can make any state vulnerable to a revolutionary situation via an integrated use of the effects of various information resources and technologies.[434] The authors, in their conclusion, noted that three categories (technical resources for intelligence; resources and technologies that produce information-technical and information-psychological effects; and methods and forms for their employment) now make it possible to wage war in a nonviolent fashion.[435]

In September 2018, the journal *Armeyskiy Sbornik* (*Army Journal*) published an article on the topic of information-psychological warfare, which the authors labelled as a type of "undeclared war." The discussion noted that such wars have no concept of front and rear, since a country's entire population and its state apparatus are targets. The authors prioritized six strategic priorities that an opponent can use to achieve its objectives, namely, worldview, chronology, fact-based, economic, weapons of genocide, and weapons of annihilation, in that order.[436] Information-psychological effects are part of waging fourth-generation wars (4GW), whose objective is to crack open an opponent's culture code and subordinate an opponent to one's will. This strategy was used in Iraq, Afghanistan, Libya, Syria, and Ukraine by the US. Thus, again, this article, like the others, addresses what the authors view as the West's or US's strategy.[437]

Eight principles of this strategy were listed: asymmetric conflict; mobility; web site interactions; "war without rules"; chaos; special effects; autonomous or semi-autonomous combat teams; and the individualization of responsibility or "victory without management." The authors then stated that the US's Military Information Support Operations (MISO) is a 4GW strategy. The latter, they add, proposes a wide set of technologies that form MISO tactics and aim to exhaust the military and financial resources of an enemy country. These tactics include the illegal application of standards of domestic and international law; economic and political sanctions, such as organizing color revolutions, demonstrations, rallies, and so on; tactics of terror, such as the organization of rebel movements; tactics of destroying family values; and high-speed operations, such as high-tech psychological warfare consisting of the manipulation of the mass media.[438] The authors concluded the following:

> Information-psychological warfare affects the unconscious, irrational states of people, their emotions, feelings, instincts, prejudices, preconceptions, and the mythological constructs of the population of a potential enemy…This is achieved through the mass introduction to people's awareness of a multitude of false stereotypes of perception and thought, and of perverted notions about views dominating their environment as well as about events occurring in the world.[439]

For those Western analysts following Russian propaganda and media/social network manipulation, it appears these authors are discussing Russian tactics and not those of MISO.

---

[434] V. K. Novikov, S. V. Golubchikov, and V. V. Zakharov, "The Principal Reasons and Conditions for the Initiation and Conduct of Information Warfare," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science*), No. 4 2017, pp. 30-31. The author would like to thank Dr. Harold Orenstein for his translation of this article from Russian to English.
[435] Ibid., p. 32.
[436] I. Sitnova and A. Polyakov, "Fourth-Generation War: Priorities, Principles of Strategy, and Tactics," *Armeyskiy Sbornik (Army Journal*), No. 9 2018, pp. 5-8.
[437] Ibid.
[438] Ibid.
[439] Ibid.

The next issue of *Armeyskiy Sbornik* continued the discussion. The initial pages of the article continued to lambast Western propaganda, noting that the West's ideological warfare is guided by the thoughts of Goebbels; that statesmen tell bald-faced lies and express hatred toward Russia; and that you can declare anyone to be a hero, even a fuehrer called Adolph. US pilots were accused of bombing schools, infirmaries, and hospitals.[440] Perhaps such vitriol is designed to support the moral-psychological hardening of soldiers toward those in the West, especially considering the restoration of deputy commanders of political affairs in the Armed Forces, as described below.

The article stated that western civilization has developed a fourth-generation weapon to be used against its enemies. The West affects people via the use of social psychology, information, and disinformation, which are multiplied by the capabilities of the Internet. The young are a target of such activities. What is required to confront the threat is a strong ideology, one that helps people understand the essence of events occurring in the world.[441]

At the end of the article, the author noted that America or the Europeans will try to prepare the consciousness of the Russian population to accept alien values and ideology. Success here will mean a faster path to a "bloodless" seizure of the state. The West, to accomplish this, must prepare the Russian population to be anti-Russian in the following way:

> First, undermine trust in state authority, plant doubt as to its legitimacy, then subject national, spiritual, moral, cultural, and social traditions to criticism, and then the mechanism of overthrowing old idols and deifying new ones is turned on. In that way the coming generation turns in time into the principal destructive force within its own country.[442]

To counteract such efforts the restoration of a strong ideology is required. The underestimation of ideology's role in bringing up Russian citizens causes concern. Ideology allows people "to gain an understanding of the essence of a particular event."[443] Without ideology, agitation, and propaganda, it is impossible to think that a future statesmen or political figure can move Russia forward. Ideology, it is noted, "represents a part of the social consciousness in which views, ideas, theories, and teachings of one class or another about society and social relations are systematized and theoretically substantiated."[444] It seems as though this is not being recalled often enough in Russia today, the author concludes.[445] To a Western mind, the author's statements are reminiscent of what was preached by Soviet commissars.

Reinstating Political-Military Officers in the Force

On 30 July 2018 President Putin appointed the former head of the Western Military District (and former head of the Chief of the Operations Directorate of the General Staff), Colonel General Andrey Kartapolov, as Russian Deputy Defense Minister and Chief of the Main Military-Political Directorate (GVPU) of the Armed Forces.[446] The directorate, a new one, indicates that Russia's military is falling back on an old system of political officers to handle the impact of nonmilitary trends (social media, etc.) on a soldier's morale. The development of a strong patriotic education

---

[440] V. Kutishchev, "In Order for the Enemy Weapon to Misfire…: We Continue the Conversation about Fourth-Generation War," *Armeyskiy Sbornik (Army Journal)*, No. 10 2018, pp. 10-16.
[441] Ibid.
[442] Ibid.
[443] Ibid.
[444] Ibid.
[445] Ibid.
[446] No author or title provided, *Interfax* (in English), 30 July 2018.

in soldiers is required in the opinion of the Ministry of Defense. Kartapolov will be working to improve the moral and the psychological stability of servicemen through the directorate.

In 1991 Russia's military political headquarters was named the Main Military Political Directorate of the USSR Armed Forces, tasked to work on the morale and psychological state of servicemen. In 1992 the directorate was renamed as the Main Administration/Directorate for Personnel Work. However, over two decades later it has been deemed inappropriate to handle the many issues that now complicate the life of young servicemen, such as their access to information on the Internet.

In February 2018 the idea of creating a Main Administration for Political Work was proposed. The rationale for the new proposal was that Armed Forces personnel need an explanation regarding the levers of cyber-systems and information-propaganda being used against them to undermine their moral character[447] and discredit the image of Russia, part of what some see as a global information and psychological confrontation. The administration would be an expanded version of the Main Directorate for Personnel Work (*главного управления по работе с личным составом* [ГУРЛС or GURLS]). GURLS organized education activities, emotional and psychological support, and discipline work. It facilitated state-patriotic education of personnel, implemented measures for the social protection of servicemen, organized cultural and leisure-related work, and coordinated interaction among various agencies and religious associations.[448] Subordinate to the organization is the Russian Federation Armed Forces Center for Military Patriotic work, the Russian Federation Armed Forces center for Psychological Work, and the 49th Equipment and Facilities Center.[449]

An August report stated that the new Main Military-Political Directorate will affect the Defense Ministry's mass media system. The question asked was whether the military newspapers of the military districts and fleets should be transferred to the new organization. This would ensure complicity of tasks and goals across the military. Only the main military newspaper, *Krasnaya Zvezda (Red Star)* would remain independent of military-political entities.[450]

In early September 2018 Kartapolov noted that the protection of soldier's patriotism is needed because there is an undisguised information war being conducted against Russia, composed of propaganda, deception, and the suppression of Russia's point of view, which can change society's conscience and have serious consequences.[451] He did not, however, offer any examples. He added that the military-political agencies will work with the population as well as the military, in particular with the youth and younger generation. One of the reasons for reinstituting the Main Military-Political Directorate, he observed, were the shortcomings observed during the conflict in Syria. He stated that "We saw that in the phase of the accomplishment of combat mission, those methods, techniques, and forms, which were set forth in the system, did not fully operate and were

[447] No author listed, "An Expert Has Defined the Mission of the Armed Forces' Military-Political Directorate," *RIA Novosti*, 30 July 2018.
[448] No author listed, "Source: The Defense Ministry Is Planning to Revive the Main Political Directorate," *RIA Novosti*, 5 February 2018.
[449] No author listed, "Main Military Political Directorate Set Up at Ministry of Defense. Colonel General Andrey Kartapolov Appointed as Chief of Directorate," *TASS*, 30 July 2018.
[450] Aleksey Ramm, Aleksandr Kruglov, Bogdan Stepovoy, and Roman Kretsul, "Directorate of Patriotism: Main Military-Political Directorate Is Being Established in the Defense Ministry and in Other Security Departments," *Izvestiya Online*, 1 August 2018.
[451] Sergey Valchenko, "Political Workers Will Teach Soldiers to Love the Homeland and Will Defend It from Information Subversion. The Main Political Directorate Chief: 'No Commissars or Lenin Rooms Whatsoever'," *MK Online* 5 September 2018.

not as effective."[452] He identified a shortcoming in what he termed the "socio-state training programs."[453]

Kartapolov noted that the administration is similar to its Soviet predecessor but minus the communist party component. The Soviet system developed methods, modes, and forms of conveying important information to soldiers. The content will be different from Soviet times, but the forms and methods will remain the same. This is needed to confront the information war around Russia and the alteration of society's political consciousness, according to Kartapolov. It offers information protection for personnel and molds servicemen with a firm conviction of the necessity to serve the Fatherland.[454]

The ideological base will be the history of Russia, the cultural tradition of its people, and the conviction that Russia must live and develop. A main cathedral for the Armed Forces is being built that will be a training center for military clergy. Belief in God and belief in the cause of service to the motherland are very close, and chaplains can mold a soldier's belief in God and political officers will mold belief in the country and the rightness of his cause. The latter must also work with social networks, as the tablet must become the political worker's weapon. Subordinate to the administration are two suborganizations, the Culture Department and the Directorate for Work with Citizens' Appeals.[455]

There are three stages to forming the military-political agencies. Phase one is the formation of the Main Military-Political Directorate, which was to be completed as of 1 October 2018, including the recertification of current employees. The second stage was to be completed by 1 December 2018, when a system of military-political agencies is formed. The third stage will be completed sometime in September 2019, when a system of cadre training is complete. Cadre will be focused on a particular branch of service or combat arm. Work with individuals will replace working with groups. In the end, priests and political-workers will be at the front, in the trenches. Psychologists are planned to be military and not civilian personnel, and it is even possible to have political officer positions at the platoon level. It is envisioned that the position of deputy commander for military-political work must become a desirable step to molding future major military commanders.[456] The role of the clergy will be expanded as well, with Kartapolov noting that the church will be called upon to serve as a center of spiritual education and as a center of historical enlightenment.[457]

In November 2018, it was reported that company deputy commanders for political affairs were posted in motorized rifle companies, and they will report directly to company commanders. They will have numerous duties:

- Instill in subordinates a deep understanding of the state's policy in guaranteeing defense
- Developing in servicemen patriotism and loyalty to military duty and the military oath
- Be responsible for professional training and ideological convictions

---

[452] Ibid.
[453] Ibid.
[454] Viktor Demin interview with Andrey Kartapolov, "Kartapolov— 'We Will Borrow the Best from the Soviet System, But We Will Change the Content'," *Zvezda (Star) TV Online*, 10 September 2018.
[455] Demin, Ibid.
[456] Ibid.
[457] Mariya Tomilenko, "To Strengthen the Army's Spirit," *Krasnaya Zvezda (Red Star) Online*, 7 September 2018.

- Understand their direct subordinate's allegiance to religious confessions, individual psychological, emotional, political, and military-professional qualities and special traits
- Ensure that no drugs are used, or excessive liquor consumed
- Maintain contact with relatives and friends of soldiers and sergeants performing draft service
- Organize leisure activities and amateur performance groups
- Prepare weekly reports about distinguished servicemen for the formation's newspaper, radio newsreel, and wall news display
- Instill in soldiers' confidence in their weapons and readiness to perform combat tasks in any conditions
- Identify soldiers with a bad attitude and set them on the true path[458]

New equipment will be supporting the military-political directorate. Recently Russia announced the fielding of a multimedia all-terrain vehicle that has educational and psychological warfare potential. Each military district is to receive two mobile multifunction information systems (PMIK). It is a van that carries multimedia equipment for "educational" work and leisure activity organization. The vehicle can also produce combat news bulletin leaflets, newspapers, rule booklets, and so on in electronic form. Digital products can be disseminated via a Wi-Fi network.[459]

It was noted above that the second stage in forming military-political agencies would be completed by 1 December 2018. Kartapolov stated on 19 December that structures subordinate to the Military-Political Directorate are the Defense Ministry Department of Culture and its organizations and institutions (the Central Museum of the Armed Forces, the Central Academic Theater of the Russian Army, the Central House of the Russian Army, and all creative teams) as well as the Defense Ministry Directorate for Work with Citizens' Appeals. In the same interview Kartapolov discussed the development of the Main Temple of the Armed Forces. It would honor the victory in the Great Patriotic War. A unique complex in the temple's precincts will be called the "Road of Memory" with photos of Muslims, Christians, Jews, Buddhists, and others.[460]

As noted earlier, regarding the restricted use of social networks, the Defense Ministry has recommended that servicemen not only stop using social networks such as Odnoklassniki, VKontakte, Facebook, and others but also to switch off geolocation services on mobile phones and abstain from Internet posts. Officials warn that foreign intelligence services monitor user data, which could lead to operational failure. Soldiers were asked not to post inappropriate interethnic or interfaith messages, and relatives of soldiers were asked not to circulate information about the service activities of their soldiers.[461] Instead of smartphones, officers and servicemen have been advised to use push-button phones that do not have photo or geolocation capabilities but can send SMS messages.[462]

---

[458] Aleksey Ramm, Aleksey Kozachenko, and Bogdan Stepovoy, "The Main Military-Political Directorate Will be Responsible for the Climate: Company Deputy Commanders for Political Affairs Are Back in the Army: The First Political Officer Posts Have Been Created in the Armed Forces," *Izvestiya Online*, 8 November 2018.
[459] Aleksandr Kruglov and Aleksey Ramm, "Military Educators Have Received Multimedia All-Terrain Vehicles. Advanced Technologies Are Being Used for Informing Soldiers and Organizing their Leisure Activities in Field Conditions," *Izvestiya Online*, 11 March 2018.
[460] Aleksandr Pinchuk, "Political Officers Called on to Stand Alongside Soldiers," *Krasnaya Zvezda (Red Star) Online*, 19 December 2018.
[461] Aleksandr Kruglov and Bogdan Stepovoy, "Soldiers and Officers Have Been Taught How to Communicate Safely on the Internet," *Izvestiya Online*, 13 February 2018.
[462] No author or title provided, *Interfax* (in English), 16 February 2018.

A final point of note is that the November 2018 issue of *Armeyskiy Sbornik (Army Journal)* contained a long article on the military-political teaching plan for the year. It covered specific topics for officers, soldiers who entered the Armed Forces via contracts, and soldiers who were drafted.[463]

Older Concepts Still in Vogue

The information age, as demonstrated above, is full of new means for confronting or deterring an opposing force. However, there remains in the Russian road map a strong desire to implement several thoughts that first germinated in the 1990s but were never approved by an international organization. There were several presentations that Russia made at the United Nations in regard to rules and regulations that it felt nations should be required to follow in the information age as well as definitions of specific terminology. At the time it appeared to U.S. representatives that such terminology requirements would be designed to limit what the U.S. could do and so no agreement was ever reached.

Russia's military has continued to discuss topics similar to those they first advanced in the UN in their official documents. Two important documents are discussed here. The first is a 2011 document on information space. The second is an update of information-related concepts in the 2014 Military Doctrine of Russia, the latest it has written at the current time. It offered their view of information space in a 2011 document and several thoughts were updated in the 2014 military doctrine. Supporting these views was General Major Igor Dylevskiy's presentation at the 6th International Security Conference in Moscow in 2018. His presentation, also summarized below, demonstrates the continuity in Russian information goals over the past 25 years.

Conceptual Views of the Activities of the Armed Forces of the Russian Federation in Information Space (CV) 2011

This is the first official document from the Russian Ministry of Defense that discusses the emergence of a global information space, defined as "The sphere of activity related to the generation, development, conversion, transmission, use, and storage of information, which influences *inter alia* the individual and public consciousness, the information infrastructure, and the information itself."[464]

The *CV* defines the terminology, principles, rules, and confidence-building measures of information space from the military's point of view, adding that in the Russian Armed Forces an "integral system has now evolved which is designed to ensure effective deterrence, prevention, and resolution of military conflicts in information space."[465] Unfortunately Russia often violates many of the principles and rules it lists.

- Principles: The principle of legality notes that the RF is guided by the norms of international law which calls for abiding by respect for national sovereignty (in Crimea and Donbass Russia did not abide by this point), non-interference in the internal affairs of other states (hacking in most European countries nullifies this point), and non-use of force or the threat of force. International humanitarian law limits the indiscriminate use of information

[463] No author provided, "Instructional Plan for the Military-Political Preparation of the Armed Forces of the Russian Federation in 2019," *Armeyskiy Sbornik (Army Journal)*, No. 11 2018, pp. 91-101, as downloaded from https://dlib.eastview.com on 16 January 2018.
[464] "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," *Ministry of Defense of the Russian Federation*, 2011, p. 5.
[465] Ibid., p. 4.

weapons (the latter are defined in the CV as "information technologies, systems, and methods used to wage information warfare") and the prohibition of treacherous methods of waging information warfare.[466] Other principles are as follows:

- A "priority" principle is to collect relevant and reliable information regarding threats as well as the protection of information resources.[467]
- The "integration" principle attempts to utilize all resources, to include staff activities and troop operations involving intelligence gathering, operational deception, electronic warfare, communications, secure and automated command and control, staff information work, and the protection of information systems against all types of effects.[468]
- The "interaction" principle coordinates the work of federal executive bodies.
- A "cooperation" principle aims to create a regime of international law that governs, among other things, military activities of states in the global information space.[469]
- Finally, the "innovation" principle simply seeks out highly skilled personnel to resolve information security problems.[470]

- Rules: The first rule is associated with "deterrence and conflict prevention." This rule should include a system:

  - To deter conflicts in information space
  - Keep resources in a state of readiness to confront information space threats
  - Organize cooperation among partner states
  - Conclude a UN treaty on international information security;
  - Take measures to detect early conflicts in information space
  - Control factors over the escalation of a conflict
  - Counter conflict developments
  - Prevent conflict from spreading
  - Neutralize factors leading to conflict
  - And explain causes and origins of conflict to the international community[471]

  The second rule is about conflict resolution. Conflicts are to be decided through negotiations and reconciliation, are to be prevented whenever possible, and are to exercise individual or collective self-defense rights in a crisis phase in information space. Retaliatory actions are to be determined taking into account other states security, forces are to be deployed on other state's territories in accordance with international law, and Russian and foreign media are to be kept informed of the evolving situation.[472]
- Confidence-building measures: These measures include exchanging concepts for ensuring security in information space, exchanging information about crisis events and threats in information space, and consulting on issues of concern to the parties.[473]

---

[466] Ibid., pp. 6-7
[467] Ibid., p. 7.
[468] Ibid., p. 8.
[469] Ibid., pp. 8-9.
[470] Ibid., pp. 9-10.
[471] Ibid., pp. 10-12.
[472] Ibid., pp. 12-13.
[473] Ibid., p. 14.

Military Doctrine 2014

This document noted several ways that information had become important. Two external information trends were noted, one a shift of military dangers and military threats into information space; and the other the use of information and communication technologies for military-political objectives, such as carrying out actions that contradict international law and aim at the sovereignty, political independence, and territorial integrity of states.[474] Internal information dangers included attempts at disorganizing not only the functions of state authorities but also the information infrastructure of the Russian Federation; and activities that have an information effect on the population, above all on the young, for the purpose of undermining the historical, spiritual, and patriotic traditions of Russia.[475]

The doctrine noted that features of modern conflicts were the integrated use of force and information and other nonmilitary measures; the use of information management systems; and the ability to impose a simultaneous effect on the enemy to the full depth of his territory in global information space.[476] In order to deter conflict, state of the art information technologies are required to lower the risk of information and communications technologies being used for military-political objectives in contradiction to international law and the sovereignty of nations.[477] With regard to military organizations, information interaction among federal executive authorities and others is required; and information security systems must be upgraded.[478] Finally, with regard to armaments, information confrontation forces and assets must be developed; information exchange systems must be upgraded so that Armed Forces information space is unified with Russian Federation information space; and information-control systems must be created and integrated with fire control systems and automated command and control entities of strategic, operational-strategic, operations, operational-tactical, and tactical scales.[479]

The doctrine deemed it necessary to develop a dialogue with other nations on their approaches to opposing military dangers and threats. In this way large-scale use of information and communications technologies for military-political purposes could be spotted before they rise to a point where conflict is inevitable.[480]

General Major Dylevskiy's Presentation at the 6th Moscow International Security Conference

General Major Dylevskiy is well-known for his multiple articles in Military Thought on Russian and US information operations. He is someone who understands Russia's position and focus well. His 2018 presentation at the International Security Conference was in many respects a reiteration of points that Russia has been making about information technologies either since the early 1990s at the United Nations (UN) or after "color revolutions" that transpired around the world after 2000. The presentation contained three basic points of discussion. The first was his concern over regimes being overthrown with modern technologies. He noted that disinformation, extremist statements, racist flash mobs, and cross-border computer attacks on critically important facilities can cause social explosions. Technologies can have the ability to produce information-psychological influence and result in color revolutions. Of great interest was his comment that informational-psychological influences resulting in color revolutions are "far more destructive for a country's

---

[474] "Military Doctrine of the Russian Federation," *President of Russia website*, 26 December 2014, sections 11 and 12l.
[475] Ibid., sections 13a, 13c.
[476] Ibid., sections 15a-c.
[477] Ibid., sections 21a, 21s.
[478] Ibid., sections 35b, 35j.
[479] Ibid., sections 46c, 46d, and 46g.
[480] Ibid., section 55f.

economy, social sphere, and other spheres of vital activities than those that result from the destruction of individual critically important facilities."[481] It is surprising that his comments would underscore the importance of information-psychological actions. It can take months or years to change someone's information-psychological character, whereas destroying a critical facility can be accomplished in a matter of minutes or hours once a decision is made. Russia's focus on information-psychological activities appears to border on paranoia at times, as the discussion of Russia's perception of the West's information-psychological advances against Russia was described earlier.

Dylevskiy's second point of discussion was his focus on special information technologies, resources, and methods that are termed information weapons. Discussions of information weapons and attempts to control them have been examined in Russia for many years. The Shanghai Cooperation Organization offered the definition of information weapons above. Such weapons can: establish oversight over an opponent; interfere in the operation of an opponent's automated systems and certain types of arms; influence armed forces' command and personnel; and influence the population.

The third point of discussion was Dylevskiy's request for additional laws to reduce the likelihood of information weapons being used in an attack. In particular he asked if Article 51 of the UN charter allowed for the right of self-defense or collective defense in case of an information attack. However, there is no definition, he noted, of an international law term "armed attack involving the use of information weapons." Further, if an attacker is a person not acting under orders from a state structure but as a terrorist, extremist, or mercenary, then they cannot be regarded as a source of an armed attack as the UN now defines it. Thus, at the moment, there is no clarity as to whether there is a basis for carrying out retaliatory attacks using information weapons against an undefined or unclear source of an information attack.

Dylevskiy expanded his presentation with a discussion of the information sphere, which has no defined borders as the physical environment does. Russia's Information Security Doctrine notes that the information sphere comprises the

> Sum total of information, hardware and software facilities, information systems, Internet websites, communication networks, information technologies entities whose activities are connected with forming and processing information, with developing and using those technologies, and with guaranteeing information security, as well as the aggregate of mechanisms for regulating the corresponding social relations.[482]

However, both traditional weapons and information technologies can impact information-sphere assets. Such impacts should be considered an act of aggression and qualified as an infringement of another state's sovereignty, he notes. Again, however, this depends on an identification of the source of the attack. Finally, he discussed a state's responsibility for the use of information weapons. Here he again cites a lack of law, since combatants are no longer just the armed forces of two states but could be defined in numerous categories (private armies, terrorists, insurgents, etc.) of combatants. A definition of a combatant operating in information space needs to be made in accordance with an international law methodology.[483]

---

[481] Unattributed transcript, "Theses from a Speech by Major General Igor Dylevskiy, Deputy Chief of the Russian Federation Armed Forces General Staff Main Operations Directorate, at the 6th Moscow Conference on International Security," *www.mil.ru*, 5 April 2018.
[482] Ibid.
[483] Ibid.

This is not the first time that Dylevskiy had discussed these issues. In 2015, for example, he and four other information experts described what they felt was needed to assure information security. They covered many of the same issues that Dylevskiy would discuss in his 2018 address. Initially the authors blamed NATO and the US for information being used by terrorists to train and recruit people, for the use of information as a weapon against Iranian nuclear facilities, and for the use of information as a subversion technique that generated "color revolutions" that overthrew leaders.[484] The authors promoted the concept of an "information weapon nonproliferation regime" as a result. They also noted that there are numerous technical and legal issues to solve.[485]

Information weapon varieties that the authors listed to be curtailed in 2015 were:

> Electromagnetic weapons (radio jammers, electromagnetic pulse weapons, and directed energy weapons); software weapons (computer viruses, computer works, Trojan programs, hidden management utilities, and so on); and hardware weapons (bookmarks to permit unauthorized access to computer information, download and transmit it to an addressee, and mount attacks against computer networks to modify or destroy information stored and circulating in them).[486]

An international information weapons nonproliferation regime was defined as follows:

> A system of patterns, principles, norms, rules, and procedures for preventing the proliferation of information weapons codified in international agreements and national laws, and also international and national agencies involving all members of the world community and nongovernmental organizations. They have total prohibition of information weapons as their end goal.[487]

The rest of the article focused on the need for dialogue, confidence building measures, exchanging national concepts of security assurances in the information environment, prompt exchange of information about critical events, and consultations on information environment activities. The principle of equal and inseparable security of all member of the world community should also be upheld.[488]

Conclusions

There are many items associated with the information age that one cannot see. While electrons running through wires are the most invisible in terms of both intent and location, other information resources or components, perhaps hidden by location or in the development stage, only become apparent after their expression and discovery in new armaments. While General Staff thinking is available in some instances, for the most part it remains hidden as well.

Western analysts will need to follow closely Russian future war forecasts, developments in military art, and the formation of information-related forms and methods of warfare. Thought is always the first to enter battle and Russia's military encourages creativity and innovation in military art.

---

[484] I.N. Dylevsky, V. P. Elyas, S. A. Komov, A. N. Petrunin, and V. O. Zapivakhin, "Military-Political Aspects of the State Policy of the Russian Federation in the Area of International Information Security," *Voennaya Mysl'* (*Military Thought)*, No. 1 2015, pp. 11-12.
[485] Ibid., pp. 12-13.
[486] Ibid., p. 15.
[487] Ibid.
[488] Ibid., p. 16.

Another important area of concern is Russian thoughts on the IPW and an evolving interest in planetary warfare. First, Russian hackers appear to be involved in trying to place malware in the circuits of a broad swath of nations in Europe and North America. There is hardly a nation in either that has not been touched. Success in planting malware helps assure information superiority in times of conflict and allows Russia to maintain an advantage in the IPW. It offers opportunities for the initiation and application of a concept such as SODCIT in times of conflict. The information age has offered Russia's excellent and talented group of algorithm writers a leg up in surveilling and reconnoitering other nations systems, especially when backed by an authoritarian regime. Second, in regard to planetary warfare, while the concept is seldom mentioned (Chekinov and Slipchenko may be the only ones to mention the idea specifically to date) Russian declarations of information, space, and oceanic theaters of military operations signify a planetary interest in planning, as does Russian interest in the global information space. Satellites and cables enable nations to reach out and touch another nation on the other side of the globe with precision and force as never before.

Some of the items listed in this overview were suggested in Russia's 2016 *Information Security Doctrine*, a political directive. Five initiatives in the document offered ways to ensure information security in the defense arena. These initiatives were: strategic deterrence and preventing military conflicts originating from the use of information technologies; improving the system of information security, to include information warfare forces and assets; forecasting, detecting, and evaluating information threats; protecting RF interests in information space; and neutralizing information and psychological attacks.[489] All of these items have been developed further, as the discussion above indicates.

Thus, Russia's current approach to contesting or controlling the multi-dimensional information environment is expansive. It is a mixture of old and new strategies. Overall, it is fair to say that Russia's military is keeping in step with new advances in scientific achievements and how they can be used in weapon applications. Some uses are deceptive while others are opaque. There is much to be on guard against, both seen and unseen.

Information strategies now in use include updated reflexive control mechanisms, new disorganization planning, indirect and asymmetric uses of nonmilitary activities, and new and creative uses of military art. Russian theorists have developed different varieties of information deterrence (media, legal, satellite inspections, etc.) to keep adversaries at bay. Such work indicates that the Defense Ministry intends to employ all types of information resources to help deter any opponent from infringing on what Russia determines to be its territorial sovereignty, whether it be former USSR territory or new resources in the Arctic. Russia supports such efforts with information troops.

Russian information operations have long been broken into information-technical and information-psychological subsections, and this tendency continues. The former can have an offensive or defensive technical character and is associated not only with information systems but also with the components that enable precision-guided and other types of weaponry. The information-psychological aspect is more specifically designed to warn and protect military personnel and the population from information-psychological offensives that potential adversaries might conduct. The Defense Ministry is clearly worried that its soldiers could be influenced by adversaries, almost to the degree of paranoia. Otherwise, why would they have decided to reinstitute its tradition of a

[489] "Information Security Doctrine of the Russian Federation," *President of Russia Website*, Edict No. 646. Dated 5 December 2016.

military-political officer directorate, which is charged with protecting the moral and patriotic fervor of servicemen.

It should be noted that the military's 2011 *Conceptual Views* and 2014 *Military Doctrine* (the latest doctrine) offered some of the more traditional guideposts and terminology. These views were supported by the 2018 presentation of information warfare expert General Major Dylevskiy, making it clear that Russia has not given up on pursuing old goals while developing new ones.

Russian theorist Sergey Chekinov noted the following in 2010:

> The dialectical development of modern armed struggle processes is a reason to argue that the information component of armed struggle will be given a greater weight in 21st century wars. Its significance will rise because the troops will be supplied with weapon systems based on wide-scale employment of information technologies, quick-acting reconnaissance and communication systems, automated troops and weapon control systems, electronic warfare systems, and so on.[490]

Chekinov's thoughts, and those of others, correctly forecasted some of the changes that information technologies would bring. This paper attempted to bring the impact of those and other information components to the forefront. It appears that Russia is using technologies and working in peacetime to "prepare to deter" by implementing its IPW and disorganization theories and working to achieve new forms and methods of employing information-aided military art to gain the initiative in potential conflicts. It continues to research the use of nonmilitary information power as well. What is important is understanding how Russia's military thinks about future conflict and how it will apply its theories. All in all, there is much to contemplate and work to be done by the West if it is to comprehend just what Russia is up to.

[490] Chekinov, "Predicting Trends…"

9 Russia's Military Discusses the Definition of War

In the Western media the combination of such methods has received the name 'hybrid warfare.' However, **it is still premature to use this term as an established one**.[491]

Introduction

Russian General Staff Chief Valery Gerasimov, in March 2017, noted about war that "In the Russian Federation Military Doctrine it [war] is called a form of the resolution of interstate or intra-state contradictions with the employment of military force."[492] In the first half of 2017, however, a detailed study was underway in Russia to ascertain if contemporary technologies and conditions had caused war's definition to change. Warfare is now so destructive (via precise targeting capabilities and increased yields) and transparent (via satellite imagery, sensors, listening devices, etc.) that force on force warfare between major nations possessing these capabilities appears less likely than during Cold War times, although it is not ruled out in areas like the Baltics.

In 2017 Russian military experts, from active and retired officers to candidates for doctoral dissertations, conducted a serious discussion of potential ways to reconsider "war" in line with these developments. The discussion appears to have started in 2016 when, for example, Russia's General Staff Academy held a conference on the meaning of the term "warfare" under current conditions. A session of the Security Council of Russia the same year also considered the issue of war's definition, analyzing the characteristics and trends in war's emergence and evolution. These initial discussions apparently kicked off a far-ranging interchange among experts.

The experts did not agree on a new determination of war. Instead, they conducted a far-ranging discussion, with some analysts stating that military means alone have not totally disappeared, especially when major powers (Russia; the US) confront lesser powers (Ukraine; Iraq, respectively), while other experts elevated nonmilitary means of warfare to a new level of importance and even envisioned the potential for such means to capture territory or cause political change. Gerasimov planned to convene a forum in August 2017 to discuss the results of the interchanges. No report from that meeting has ever surfaced.

Due to the absence of a conclusive statement regarding war, this article has two parts. Part one covers two short discussions of war since the detailed 2017 discussion period. Included here are a description of war from a 2018 article in the *Journal of the Academy of Military Science*; and a description of war from Russian General Staff Chief Valery Gerasimov's 2019 presentation before the Academy of Military Science that was published in the paper *Red Star*. These articles suggest that war's definition has indeed expanded. Gerasimov's presentation was particularly startling for its numerous references to the term "waging war." Part Two covers in some detail the 2017 discussion among military analysts.

The 2018 and 2019 Discussions

It is unknown if these two articles were the result of the 2017 discussions, but it is possible. The first article represents a summary of numerous nonmilitary aspects of the contemporary period,

---

[491] V. V. Gerasimov, "Modern Wars and Real Questions in Regard to the Country's Defense," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2017, p. 11. Dr. Harold Orenstein translated this article from Russian into English.

[492] Valery Gerasimov, "The World on the Brink of War. It Is Not Enough to Take Account of Today's Challenges. Future Challenges Need to Be Forecasted," *Voyenno-Promyshlennyy Kuryer Online,* 15 Mar 2017 - 21 Mar 2017.

while the second article describes in no uncertain terms how to wage war in an updated, classical form.

In mid-2018, two authors wrote on the topic "The Typology of Warfare: Foundations of Philosophical Analysis." They defined war as armed struggle between states, different social groups (classes), or peoples (nations).[493] In the past, nuclear weapons began discussions of changes in war's nature. Such weaponry changed the sense that war could actually be a continuation of politics by other means, since political goals could hardly be achieved if mankind would be destroyed. This led to a search for new forms and methods of conducting war.[494] Classical war has withdrawn to the background, but the presence of nuclear weapons has not ensured a state's sovereignty and integrity. This is because, according to the authors, contemporary times are generating warfare types that earlier were just wild fantasies—cyber warfare, network-centric warfare, psychological warfare, and biological warfare. Information, economic, and terrorist warfare is becoming natural. Such new-type war, the authors note, can begin without notice or a declaration of war.[495]

Military coercion is changing, the authors believe, due to the involvement of large international organizations and even corporations. The latter are manipulating minds and making the consciousness of the individual and society an object of coercion as a way to help control the geopolitical situation. Conflicts are shifting to a "low intensity" phase, where electronic weapons are as dangerous as nuclear ones and their use is much cheaper. New fronts of warfare are cultural, ethnic, religious, and so on. A clear boundary between war and peace is absent. States can "use the tactics of irregular formations" and "irregular formations can use existing advanced technologies."[496] Thus, this article focused on war's changing nature.

General Staff Chief Gerasimov's article was focused on both military and nonmilitary issues. He often discussed "war" in his presentations over the years at the Academy of Military Science. For example, in a comparison of his seven speeches at the Academy, the words/phrases "forms and methods," "nonmilitary," "asymmetric," "information," "command and control," and "war" were examined for their frequency of use. In each case from 2013-2019, the word used most often was "war," except in 2014, when command and control was used more frequently.

Gerasimov used the term "war" 12 times in his 2018 presentation, with references to topics such as a state of war, future war, local war, declared, or undeclared war. There were also references to the definition of strategy, which Gerasimov had defined by noting that as each war has a logic all its own.[497] His 2018 presentation was more notable for its focus on future war and for its use (three times) of the term "comprehensive destruction" of an enemy force.

In 2019 Gerasimov used the term "war" 27 times. Uses were in relation to 15 different topics, some used more than once, from preparing war, preventing war, or future war to the kinds, nature, state, or outcomes of war. However, the term "waging war" and "wage war" stood out, for they

---

[493] E. Yu. Shakirova and A. Yu. Cherepanov, "The Typology of Warfare: Foundations of Philosophical Analysis," *Vestnik Adademii Voennykh Nauk (Journal of the Academy of Military Science*), No. 3 2018, pp. 16-17. Dr. Harold Orenstein translated this article from Russian into English.
[494] Ibid., p. 18.
[495] Ibid., p. 19.
[496] Ibid., p. 20.
[497] See, for example, Harold Orenstein, "Russian General Staff Chief Valery Gerasimov's 2018 Presentation to the General Staff Academy," *Military Review*, January-February 2019, pp. 130-138.

were used eight times (waging war was only used twice in all of his preceding presentations combined) as follows:

Waging War

- The principle of waging war is based on the coordinated use of military and nonmilitary measures, with the deciding role of the Armed Forces, has seen development under today's conditions.
- Therefore, a search for rational strategies of waging war against a varying enemy acquires priority importance for developing the theory and practice of military strategy.
- We need to clarify the essence and content of military strategy and the principles of preventing war, preparing for war, and waging war.
- But all the same, questions of preparing for and waging war, above all by the Armed Forces, comprise the main content of military strategy.

Wage War

- Military strategy as a science, ". . . the art of command and control," originated at the beginning of the last century and was developed based on research of the experience of wars. In a general form strategy represents ". . . a system of knowledge and actions to prevent, prepare for, and wage war."
- They [the West] are preparing to wage wars against a "high-tech enemy" using precision-guided munitions [PGM] from the air, sea, and space, with the active conduct of information warfare.
- Under these conditions our Armed Forces must be prepared to wage wars and armed conflicts of a new type using classic and asymmetric methods of operations.
- The development of strategy as a science must encompass two directions: the development of a system of knowledge about war and the improvement of practical activities to prevent, prepare for, and wage war.[498]

The overall topic of Gerasimov's 2019 presentation was vectors of strategy. Thus, the presentation should stand out for its focus on military and nonmilitary methods of implementing strategy and should be closely studied. Russia's response to US actions is the strategy of the active defense, he noted, which envisages a set of measures for the preemptive neutralization of threats to national security. The issue of preemption conjures thoughts once again of the importance of the IPW, where preparations are made in advance for the potential future application of wartime methods. Gerasimov added that the development of strategy as a science must encompass the development of a system of knowledge about war.[499] Thus, as late as March 2019, he still was insisting on more information about war's modern-day characteristics, going so far as to request a "system of knowledge" about war.

[498] Presentation of Valery Gerasimov, "Vectors for the Development of Military Strategy," *Krasnaya Zvezda (Red Star) Online*, 4 March 2019.
[499] Ibid.

The 2017 Debate on War

The 2017 discussion that preceded the two articles above was long, broad, and deep. For example, warfare was under examination in a host of military journals, to include the *Vestnik Akademii Voennykh Nauk (AVN or the Journal of the Academy of Military Science (AVN)*, *Voennaya Mysl' (VM or Military Thought)*, *Armeyskiy Sbornik (AS or Army Journal)*, and others. *AVN'*s first issue of 2017 was particularly fruitful, offering eight warfare-related articles on topics such as war's interpretation and aspects, and its nature, essence, and strategies. The second *AVN* issue of 2017 contained four such articles, with the main one being the address of General Staff Chief Valeriy Gerasimov on the essence of modern wars at the Academy's annual conference.

Military Thought, while containing fewer articles with "war" in the title, did publish four papers by May 2017, to include one by Colonel (retired) S. G. Chekinov and Lieutenant-General (retired) S. A. Bogdanov on war's nature and content. These two retired officers authored the 2013 new-generation warfare article that caused such a stir in the West and resulted in the assembly of entire teams to study their concept. Other *Military Thought* authors in early 2017 discussed preparations for war and the topic of coalition war, while *Army Journal's* July edition discussed war's levels of classification. While all of the articles mentioned are not covered here, those considered the most important are. The topic was under the microscope in a number of venues.

There are many defining points in these 2017 articles to consider. Here are a few:

- Gerasimov, when discussing hybrid war in March, noted that "In the Western media the combination of such methods has received the name 'hybrid warfare.' However, **it is still premature to use this term as an established one**."[500]
- General of the Army Makmut A. Gareyev and retired Major-General Nikolay I. Turko stated that Russia has the right "to declare a state of war not only if it is necessary to fulfill international treaties, but also as the result of an assessment of the scale and degree of threats" to its national security (with respect to the economy, to ideology, or the information sphere).[501]
- More colorfully, Aleksandr A. Bartosh stated, by analogy, that "a **color revolution**, similar to a poisonous mushroom, can grow in soil well manured by those who wage **hybrid wars**."[502]
- Aleksandr I. Kalistratov listed **nine ways for Russia to counter the hybrid war** activities of the West.[503]
- Valeriy Kiselev noted that "**behavior wars**" involve manipulating behavior algorithms, habits, activity stereotypes, and so on that have been installed in us by our social groups, biographies, and cultural environment.[504]

---

[500] V. V. Gerasimov, "Modern Wars and Real Questions in Regard to the Country's Defense," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2017, p. 11. Dr. Harold Orenstein translated this article from Russian into English.
[501] M. A. Gareyev and N. I. Turko, "War: a Contemporary Interpretation of its Theory and Practical Realities," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2017, p. 9. Dr. Harold Orenstein translated this article from Russian into English.
[502] A. A. Bartosh, "Adaptive Strategies of Information Warfare (Part 2)," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2017, p. 58. Dr. Harold Orenstein translated this article from Russian into English.
[503] A. Kalistratov, "War and Modern Times: Modern Wars: Let's Explore the Classification," *Armeyskiy Sbornik (Army Journal)*, No. 7 July 2017, p. 9.
[504] Valeriy A. Kiselev, "For What Kinds of Conflict Should the Armed Forces of Russia Prepare?" *Voennaya Mysl'* (*Military Thought*), No. 3 2017, p. 37.

- Chekinov and Bogdanov continued to stress that military means were still the most prominent way to conduct war, noting in 2017 that "the main specificity of war **remains acts of violence**." However, they also described the change from the era of human societies to the era of super societies and its designed and managed wars, "a **new-type of war**."[505]

This article will examine the views of these authors and others about war's emerging trends and definitions. The discussion begins with a look at *AVN's* articles, starting with Gerasimov's and the tasks he imposed on the Academy of Military Science. A summary of the main points of several other journal articles follows.

Three clear lines of thought emerge: that nonmilitary issues and nontraditional methods have risen in importance and must be considered in conjunction with military ones when warfare is contemplated; that war's essence, in spite of nonmilitary issues, remains armed conflict; and that hybrid war continues to be refuted by several authors as a Russian method of fighting, stating instead that hybrid war is a Western way of war that Russia must confront. Instead Russian theorists are focusing on new-type war.[506] Other popular topics that are discussed include asymmetric, indirect, and information warfare strategies.

Articles in the Journal of the Academy of Military Science (AMS)

Chief of the General Staff General Valeriy Vasil'evich Gerasimov

General of the Army Valeriy Vasil'evich Gerasimov is the Chief of the General Staff of the Armed Forces of the Russian Federation. He is a member of the Russian Federation's Security Council and a Hero of the Russian Federation. There is much to learn from his 2017 presentation at the Academy of Military Science, which is devoted to developing **trends** in the application of military force, both military and nonmilitary. Gerasimov noted that the Russian Federation's 2014 Military Doctrine defined war as a form of resolving interstate or intrastate conflicts by using military force. This definition is under analysis, based on as his comments in this presentation.

One of the primary issues he addresses is activities that do not fall under the definition of aggression. He states that "In the Western media the combination of such methods has received the name 'hybrid warfare.' However, it is still premature to use this term as an established one."[507] This has been a consistent theme of Russian military officers over the past several years, that it is the West that is using hybrid wars, not Russia. President Vladimir Putin recently supported Gerasimov's point. He stated in an interview in May 2017 with the *Le Figaro* newspaper that there is no need "to think up mythical Russia threats, hybrid wars, and so on. These are your [the West's] own fancy, and then you scare yourselves, and based on that formulate a policy prospect."[508]

Gerasimov stated that conflicts now feature changes in the **ratio** of various types of struggle (military, economic, etc.) to the overall political success of a war. The cost of armaments plays a role in the choice of **methods** for military action. New **forms** for applying force have appeared,

---

[505] S. G. Chekinov and S. A. Bogdanov, "The Evolution of the Essence and Content of War in the 21st Century," *Voennaya Mysl'* (*Military Thought)*, No. 1 2017, p. 43.
[506] See the articles by Gerasimov, Derbin, Dolgopolov, Kalistratov, Chekinov/Bogdanov, Semenov, and Kiselev.
[507] V. V. Gerasimov, "Modern Wars and Real Questions in Regard to the Country's Defense," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2017, p. 11. In accordance with the five aspects of Russian military thought (trends, forecasts, correlation of forces, forms, and methods) these terms are in **bold** print where used by Gerasimov, along with the concept of new-type war.
[508] No author or title provided, *Interfax* News Agency (in English), 30 May 2017.

such as the digital mass media and social networks, while information dominance remains an "indispensable pre-requisite of combat actions."[509]

Gerasimov noted that the analysis to date indicates that boundaries between the state of war and peace are being erased. For example, in Syria the USA and NATO used hybrid methods of fighting, which were described as the simultaneous use of traditional and non-traditional actions of military and nonmilitary assets. Hybrid actions use slogans designed to defend democracy or insert democratic values into a country without violence. The protest potential of the population is the "implementer" of these methods, using nonmilitary forms and means with unprecedented technological capabilities that can trigger the collapse of a state's vital functions, such as in the energy, banking, economic, information, or other spheres.[510] However, this hasn't changed Gerasimov's views on war's overall nature, as he added "the essence of wars in modernity and in the foreseeable future will remain the same. Their main feature is the presence of an armed struggle."[511] Here he means violent military actions.

In August of 2017 a roundtable was held at the "Army-2017" forum, where the topic "Contemporary Warfare and Armed Conflict: Characteristics and Features" was discussed. This appeared to signal that there would be some form of closure on the topic of war and its evolving nature.[512] No summary of that forum has been produced to date.

Forecasting future threats remains an important instrument of military thought, as it is a way of strategically calculating what capabilities are required to contain emerging threats and dangers. Fulfilling these requirements also helps restore the nation's confidence in the Armed Forces.[513] The Syrian experience required, Gerasimov notes, practices that always couldn't rely on military science. Many operations were resolved on the spot, indicating Russia has "shown skill in waging a **new-type war**, organizing coalitions, and working with partners"[514] and demonstrating that Russia could carry out operations in a remote theater.

Gerasimov closed his speech by offering what he considered to be military science's priority tasks in the coming months. First is the necessity of studying new **forms** of confrontation and effective **methods** for countering them. Second is determining measures to counter "hybrid" wars aimed at Russia. Third, it is necessary to study the features of contemporary military conflicts and develop effective **forms and methods** of operating under various conditions. Finally, organizing forces on remote theaters of military operations (Arctic?) requires separate research.[515]

General of the Army Makhmut Akhmetovich Gareyev and General (retired) Nikolay Ivanovich Turko

General of the Army Makhmut Akhmetovich Gareyev is the President of the Academy of Military Science and Major-General Nikolai Ivanovich Turko (retired) is one of his closest coworkers and a Doctor of Military Science. Gareyev is purportedly the officer who developed the concept known as the operational maneuver group, according to Russian officials. He fought in the World War II battle for Kursk and he also participated in the war in Afghanistan in the 1980s. Turko taught a

[509] Gerasimov, "Modern Wars…," p. 10.
[510] Ibid., p. 11.
[511] Ibid.
[512] Ibid.
[513] Ibid., p. 12.
[514] Ibid.
[515] Ibid., p. 13.

series of courses at the General Staff Academy in Russia where he was a professor. He wrote often on information-related topics.

These authors noted that war, as a rule, is an armed clash of various states or a coalition of states with the aim of resolving antagonistic conflicts rising between them.[516] But the main feature of contemporary war's first phase no longer is an armed clash. Rather it is the active employment of "harsh" nonmilitary means in combination with "soft" nontraditional means (first and foremost, information), where the goal is to redistribute the roles and functions of countries instead of the destruction of the enemy. The political process is raised to a second (higher) phase of war when military means are employed.[517] Thus these authors see two phases to war, one nonmilitary and one described as the use of military operations.

In phase one, the mass employment of cybernetic and radio-electronic resources aim to disorganize the entire economic and financial system of opposing countries. The potential moral and psychological subversion of some countries from within, as happened with the collapse of the Soviet Union and other countries, can occur due to the use of information technologies.[518] Some scholars believe war is already underway in peacetime.[519]

Contemporary conditions have changed the manner in which war is unleashed, although Russia's laws still indicate that war begins with the commencement of military operations. For example, Article 18 of the Federal Law of the Russian Federation "On Defense," adopted on 3 July 2016, states the following according to the authors:

> A state of war is declared by federal law in case of an armed attack against the Russian Federation by another state or group of states, as well as in case of the necessity of fulfilling the Russian Federation's international agreements. Wartime begins at the moment of the declaration of a state of war or at the actual commencement of military operations, and expires at the moment of the declaration of the cessation of military operations, but no sooner that their actual cessation.[520]

Gareyev and Turko then call for changes to the law, noting that Russia has the right "to declare a state of war not only if it is necessary to fulfill international treaties, but also as the result of an assessment of the scale and degree of threats" to its national security (with respect to the economy, to ideology, or the information sphere). They added as justification that NATO's 1949 concept allowed for the participation of armed NATO formations beyond its territories in case of an interruption in the flow of vitally important resources.

The complexity of the contemporary international situation serves as a basis for increasing the country's readiness to repel clearly hostile acts by military and nonmilitary means. In regions where there are antiterrorist operations, a "military situation" or an "emergency situation" may be introduced. Presently there is no defense if an opponent employs cybernetic, information, psychological, or other effects against Russia's population. The appropriate retaliatory actions should be coordinated at the government level, with each country able to declare a state of war

---

[516] M. A. Gareyev and N. I. Turko, "War: a Contemporary Interpretation of its Theory and Practical Realities," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2017, p. 4.
[517] Ibid., p. 5.
[518] Ibid., p. 6.
[519] Ibid., p. 7.
[520] *Federal'nyi zakon "Ob oborone" (s izmeneniiami na 3 iiulia 2016 g.) (redaktsiia, deistvuiushchaia s 1 ianvaria 2017 g.). www.docs.cntd.ru.*

proceeding from its own national interests.[521] The task for the scientific community is to grasp the essence of warfare.[522]

Alexander Vladimirovich Dolgopolov

Colonel Alexander Vladimirovich Dolgopolov is a graduate of the Higher Military Aviation Electronic School in Kharkov. He served as a navigator-operator on long range aircraft and chief of staff of an air regiment. In 2010 he became the deputy chief of the Center for Military and Strategic Studies of the Military Academy of the General Staff.[523] It is not known if he is still in that position.

He wrote that there exist unanswered questions with respect to the nature and essence of war, which requires clarification on contemporary war's definition due to the new means and methods for its conduct.[524] Such clarification was also the case in the past. A. Snesarev and Alexander Svechin, two renowned Russian and Soviet military theorists at the beginning of the 20th century, made significant contributions to the development of the "science of war." In their research they noted that war as a phenomenon "is the consequence of not only political, but also economic and social relationships."[525] Thus they understood that war was not just a military function. Svechin in particular noted in his two-volume work, *Strategy in Classic Military Works*, that "war is conducted not only on an armed front, but also on class and economic fronts."[526] Snesarev, in his 1926 review of Svechin's *Strategy*, noted that war can be waged not only by the sword, but also by other means such as agitation, crushing of the enemy's economy, or the reconstitution of one's own forces.[527]

Dolgopolov singled out four basic directions that are influencing the formation of a new approach to warfare. First is the appearance of new actors (persona, subjects). He states that "To some degree war is a continuation of politics not only of a state, but also of civilized formations (non-existent or quasi-states)."[528] An example of this would be the so-called "Islamic State," which essentially is not a state. A second direction is the development of new military-theoretical concepts, such as partisan warfare, terrorist, or asymmetric warfare, where one of the subjects of war is not a state but could even be a nongovernmental organization. In the past, if the essence of war's goals was based on expanding one's living space and consolidating economic power, today's priority appears to be ensuring political influence and domination in all regions of the world.[529]

A third direction determining the essence of modern war is the rapid development of high technologies. They are revolutionizing the means of military force and changing how to conduct war, such as via noncontact confrontations. Finally, the fourth direction is the appearance of new spheres and corresponding methods of confrontation, which are undoubtedly conditioned by the mass introduction of information and communication technologies into theory and practice. No

---

[521] Gareyev and Turko, p. 9.
[522] Ibid., p. 10.
[523] A. V. Dolgopolov and S. A. Bogdanov, "The Evolution of Warfare Forms and Methods in a Network Centric Environment," *Voennaya Mysl'* (*Military Thought)*, No. 2 2011, p. 49.
[524] A. V. Dolgopolov, "A Contemporary Understanding of the Essence and Content of War," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science),"* No. 1 2017, pp. 41-42. Dr. Harold Orenstein translated this article from Russian into English.
[525] Ibid., p. 42.
[526] A. Svechin (ed.), *Strategiia v trudakh voennykh klassikov* (Strategy in classic military works), Moscow: Gosudarstvennoe voennoe izdatel'stvo, 1926, as cited in Dolgopolov, "A Contemporary…," p. 42.
[527] Dolgopolov, "A Contemporary…," p. 45.
[528] Ibid., p. 44.
[529] Ibid.

less important is the wide dissemination of other types of confrontation (economic, information, political, etc.) within the framework of war.[530] The latter includes the alteration/breakdown of the consciousness of the opposing side, also known as *консциентальная война*. Its goal is to shift the orientation of a person's values and is not conducted with the employment of military force, but rather actions in the information domain. Thus, changes in war's essence is being conditioned by both the substantive broadening of the means (especially nonmilitary) of confrontation and by changes in the order and sequence of employing military and nonmilitary means during war.[531]

The culminating stage of war to Dolgopolov, as with Gerasimov, remains the employment of the means of armed struggle. The armed forces' employment is the obligatory condition for defining "war."[532] As a result there are now two views on war to consider, while the truth may be found somewhere in the middle:

> One (the classical, traditional) view consists of the fact that the principal subject of military science, together with issues of the development of the armed forces, their technical equipping, military economy, and military training and education, is armed struggle. The other (expanded) point of view sees as the subject of military science warfare both as a whole and on the same level as armed struggle; it proposes other types of struggle (information, diplomatic, economic, cybernetic, etc.) as a subject for research.[533]

In contemporary military conflicts, indirect and asymmetric methods of operation are being employed more and more. This circumstance conditions the necessity of studying the capabilities of various types of confrontation in the interests of safeguarding military security and waging war.[534] Dolgopolov added that these ideas have been confirmed, for the most part, essentially being the content of the concept of the "new type" war (hybrid war: Dolgopolov's insert), which has appeared in military conflicts in Iraq, Libya, and Syria.[535] Here he appears to be highlighting US methods.

Evgeniy Anatol'evich Derbin

Evgeniy Anatol'evich Derbin is a Major-General in the reserves and a professor on the information security cadre at the Russian Government Linguistic University. He stated that his article was an attempt to understand the possibilities and ways of getting out of a situation of conceptual stagnation about the concept of war. He noted that interpretations of international legal standards about war are obsolete, since they associate war with the entry into a certain state of relations between states, and pair this with a public "declaration." Further, war is paired with the employment of a specific type of resources for pressuring the enemy, as determined by the technological wave of innovation—traditionally, means of physical destruction. He adds that at present, "when resolving conflicts among states this ceases to be a required condition for the achievement of a goal, inasmuch as the capabilities of means of destruction have now moved beyond the boundaries of the destruction of the physical capabilities of the living force."[536]

---

[530] Ibid., pp. 44-45.
[531] Ibid., p. 45.
[532] Ibid., p. 46.
[533] Ibid., p. 47.
[534] Ibid.
[535] Here Dolgopolov appears to be referring to the article of Colonel-General Andrey Kartapolov in the *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2015, pp. 26-36.
[536] A. V. Derbin, "Methodological Aspects of an Analysis of the Essence of Contemporary War," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2017, pp. 11-12. Dr. Harold Orenstein translated this article from Russian into English.

States, classes, and individuals are seeking unchallenged control over resources in order to dominate in spheres of interest using human, economic, military, and even legal resources. Derbin lays blame on the West for this circumstance, stating that its traditions correspond to intolerant attitudes toward the existence of "evil," insisting that it must be destroyed due to its existence. Eastern traditions, on the other hand, confront evil and take into account the interests and values of the other side (or evil). This indicates to Derbin that Russia cannot have allies, partners, or friends in the form of states or representatives of Western civilization.[537]

Derbin adds that technological advances in political, economic, and military capabilities allow for aggressors to dispense with methods of armed struggle from the past.[538] He also offered a variant of, in his words, a "new-type" of warfare in which he discussed various stages of a conflict in a table/figure under the title "Variant for Assessing the Development of the Military-Political Situation and Conflict Resolution by Implementing Forms and Methods of Hostile Actions."[539]

Aleksandr Georgievich Semenov

Aleksandr Georgievich Semenov is a candidate of technical sciences and a senior scientific official. He discussed the nature and content of war from, as he noted, an evolutionary point of view. However, his article focused on what he termed the West's desire to impose on all countries "its matrix of governance, consumerism, and socio-economic hierarchy leveraging a wide arrangement of achievements in economics, science and technology, and other areas."[540] He states on two occasions that globalization is the new-type of war being waged by the West against the world, and he added later that the West's goal is to create a unipolar world between 2020 and 2040.[541] He lists numerous tools that characterize this type war. They are: peaceful civilians; mass media; countries' leadership; management capabilities; psychological, informational, and communication resources; socially oriented forms and methods of work with the masses; cyber-technologies; precision weapons; terror; money; bribery; blackmail; threats; sanctions; lies; setups; and so on.[542] He summed up his Western diatribe in the following manner:

> Globalization is the reason for the destruction of countries and for profound changes in the mental and moral makeup of people all over the world. Peace on the planet can be maintained based on an alternative belief system different from that of the West…While in those times [medieval and prehistoric] there were no moral, ethical, and humanitarian rules of war, today these rules are violated and used as leverage to accuse the opposing side of violations. This type of practice is characteristic of a number of Western countries, terrorists, organizations, and their sponsors.[543]

Aleksandr Aleksandrovich Bartosh (2016)

Aleksandr Aleksandrovich Bartosh is the director of the Information Center for Questions of International Security at Moscow's Government Linguistic University. His article focused on information warfare issues and offered suggestions on how to apply them against the West's proclivity, in Bartosh's opinion, to use information technologies (IT) to develop and succeed in

---

[537] Ibid., pp. 13-14.
[538] Ibid., p. 15.
[539] Ibid., p. 17.
[540] A. D. Semenov, "War: Its Essence and Content from an Evolutionary Point of View," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2017, p. 31. Dr. Harold Orenstein translated this article from Russian into English.
[541] Ibid., pp. 31-32, 34.
[542] Ibid., p. 33.
[543] Ibid., p. 34.

the use of color revolutions and hybrid war. This article was published in 2016. It is used here because Bartosh published a second, follow-on article with the same title in 2017.

Subversive IT methods, in his opinion, have led to increasingly chaotic international relations due to today's competitive environment. This environment has fostered new types of conflicts combining traditional military power with political, IT, financial, and other components.[544] These developments are centered on the activities of the United States, who inspired, he believes, the coup d'état in Ukraine. Indirect strategies are on the rise as well, with the West setting up color revolutions and hybrid wars that introduce controlled chaos with military power no longer the only player.[545] Now nations are manipulating perceptions and falsifying historical facts through the use of IT. Information war uses IT and the mass media to achieve geopolitical goals. It is also used in warfare in order to gain unilateral advantages in collecting, processing, and using information on the battlefield.[546]

Bartosh underlined the purpose of his article when he stated that it focusses on information-war strategies pertaining to subversive information-psychological operations against a country. The U.S. and NATO, he believes, support the consistent execution of subversive cyber operations as part of their information war strategies. These strategies, when viewed as a key military-political tool, are characterized by deliberate and planned measures that affect the awareness of all social groups to distort perceptions and disorganize any countermeasures against aggression. Color revolutions are used against a relatively small range of targets, while hybrid war's scale can reach an entire population of a country over a long period of time. In summary, Bartosh adds, "one of the principal targets of information war is public and individual awareness and the subconscious, especially that of the youth, elites, and military service members."[547]

Two definitions of information war were provided in the article. The first was that of information warfare specialist Igor N. Panarin, who stated that

> Information war is a multifaceted strike, i.e., a combination of IT operations against the adversary's government and military control system and the military-political leadership, which even in peacetime would produce favorable decisions for the initiating side, and during conflict would completely paralyze the adversary's control infrastructure.[548]

Bartosh felt that Panarin's definition was balanced in regard to its human and technical aspects.

The second definition, by A. M. Sokolova, defined information war as an IT and media realm standoff. It is designed to achieve political goals:

> Information war is a combination of measures to achieve superiority over the adversary by affecting its IT systems, processes, and networks, as well as the public and individual, including military service members, awareness and subconscious while at the same time protecting one's own IT environment.[549]

Bartosh summarized this section by noting that today's political realities call for an extended use of IT and communication technologies in conflicts with the involvement of intelligence agencies. Information war is now an assault on the information space of an opposing side to achieve strategic

---

[544] A. A. Bartosh, "Adaptive Strategies of Information Warfare (Part One)," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2016, p. 85. Dr. Harold Orenstein translated this article from Russian into English.
[545] Ibid., p. 86.
[546] Ibid., p. 87.
[547] Ibid., p. 88.
[548] Ibid.
[549] Ibid.

goals. Here the focus is on undermining cognitive aspects of activities in a victim country, where belief systems are destroyed and fake economic and moral assumptions implanted. Color revolutions and hybrid wars are examples, he notes, of "multifaceted conflicts characterized by the purposeful and adaptive use of military force, economic strangulation, and subversive IT operations."[550] Adaptability is the key characteristic for any information war strategy, defined as "the ability to provide an adequate response to a changing environment or to request from lower level systems," a process of adjusting capabilities and their use to fit a changing environment.[551]

Adaptive management uses a managed chaos strategy based on adjusting the purpose of IT operations for changing external or internal circumstances to reach a goal with the required effectiveness. The use of several types of adaptive strategies can be part of a unified plan for waging information war.[552] The strategies of obliteration and exhaustion are discussed in Bartosh's 2017 article, which is next.

Aleksandr Aleksandrovich Bartosh (2017)

This article focused on the use of information warfare and technology activities that are designed to cause regime change through, in author A. A. Bartosh's words, either obliteration or exhaustion strategies in conjunction with color revolutions and hybrid war. Clearly the target of these strategies is, in Bartosh's opinion, Russia. He states, for example, that "we can conclude that the hybrid war against Russia has been waged for an extended period of time, with information technology warfare being its most important component."[553] Further he adds that adversaries using hybrid war tactics combine indirect measures with a threat of military aggression against Russia, forcing the country into more military expenditures.[554]

Bartosh notes that color revolutions and hybrid wars are conflicts that combine traditional military power with other components (political, financial, etc.). These latter components are enhanced by indirect strategies designed to drill conflicting information into the minds of the people and the ruling elite that utilize the following components:

- A discussion of internal corruption
- A list of perceived internal grievances, such as differences in income levels, the inadequacy of the elite group, lack of upward-mobility, and health care, education, judiciary, social security, ethnic, and inter-religious problems
- A list of perceived external issues, such as instability and discontent fueled by foreign and national media
- The introduction of distorted historical and ideological ideas, falsely interpreted values and interests, and emotional appeals and slogans based on national identity[555]

[Author: this summation sounds like what the Russians are doing to the West. Obliteration is paired with color revolutions and exhaustion is paired with hybrid below]

---

[550] Ibid., p. 89.
[551] Ibid.
[552] Ibid., p. 90.
[553] A. A. Bartosh, "Adaptive Strategies of Information Warfare (Part 2)," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2017, p. 58. Dr. Harold Orenstein translated this article from Russian into English.
[554] Ibid., p. 59.
[555] Ibid., pp. 56-57.

The use of these tactics qualifies, in Bartosh's opinion, as a strategy of obliteration due to the quick pace and implementation of conflicting information, which can be enhanced through information-psychological technology activities.

For color revolutions, this would mean the dynamic overthrow of government and the resulting regime change. To expedite the process, at some point an event is staged (e.g., provoke law enforcement into using unnecessary force, highlighting unjust judicial decisions, etc.) and the "manipulated masses make their uncompromising demands upon authorities." There is no planned defeat of the armed forces in this scenario.[556] The initial stage of the strategy of obliteration involves the painstaking collection of information and can take a very long time. This is followed by a powerful head-on strike over a short period of time (just a few weeks in some cases) to achieve some significant political outcome.

If the obliteration strategy does not work, then an aggressor will shift to a hybrid strategy focused on exhausting the target nation though the use of a wide range of measures, especially cyber strikes designed to inflict an indirect exhaustion effect. By weakening one's resources, an aggressor state causes psychological instability capable of disrupting the unity and integrity of the target state. Bartosh notes that "an important role under this strategy is given to ruining traditional moral values and reformatting cultural life and belief systems."[557] Exhaustion strategies apply sanctions, break up the ruling elite, undermine the economy, and diminish the will of the population, with the objective being to force the target country into exorbitant military expenditures.[558]

Bartosh adds that once a critical decision point is reached about instituting a coup d'état, the situation transitions back to a strategy of obliteration by initiating a color revolution.[559] An interesting analogy he uses is that a color revolution, similar to a poisonous mushroom, can grow in soil well manured by those who wage hybrid wars.[560] Thus he implies that a color revolution can occur either on its own or as a follow-on to hybrid war actions. Exhaustion and obliteration strategies are a destructive tandem (moving from obliteration to exhaustion and back to obliteration) that target critical elements of today's world and create chaos in target countries.[561]

One conclusion Bartosh reaches is that information warfare capabilities that target large segments of Russia's population make it an urgent task to develop information-psychological warfare countermeasures and methods of controlling and defending cyberspace. "The effectiveness of today's Russian strategy of countering information warfare," he notes, "to a large extent depends on a clear awareness and cognizance of our national values and interests as well as scientific justification of their hierarchy and prioritization."[562] National values must be promoted (especially culture and belief systems), a sense of historic memory and self-identity restored, a "soft" force developed to counteract subversive strategies of information warfare, and a model designed for delivering preventive information-psychological technology counter-strikes.[563]

Nikolay Nikolaevich Bolotov

---

[556] Ibid., p. 56.
[557] Ibid., p. 57.
[558] Ibid., p. 58.
[559] Ibid., pp. 57-58.
[560] Ibid., p. 58.
[561] Ibid.
[562] Ibid., p. 59.
[563] Ibid., pp. 60-61.

Nikolay Nikolaevich Bolotov is a Doctor of Military Science and colleague at the scientific research laboratory for information security at the Military Academy of the General Staff of the Armed Forces of the Russian Federation. His article examined war in the information sphere.

Bolotov writes that war is understood as the totality of armed struggles with violent actions as its principal and decisive means. Other means of pressure, such as nonmilitary actions, work only with large military forces in reserve, which forces the weaker side to subordinate itself to the will of the other side.[564] However, one sphere of struggle or war that is found in both military and nonmilitary operations is confrontations in the information sphere.

Information warfare is understood to be operations undertaken to achieve information superiority via effects on an enemy's information and information systems, while protecting ones own systems. The importance of information has elevated it to the form of an independent type of weaponry. An information weapon is a means for destroying, distorting, or stealing large amounts of information, and extracting from it the necessary information after penetrating its security system. Such weapons can be secretly employed, cause irrecoverable damage without violating another nation's borders or sovereignty, employ both military and civilian cyber forces, and involve minor losses and high effects. Such weapons are basically invisible, nonlethal, selective, and scalable.[565] Their goal is to achieve information superiority, defined as attaining and maintaining a favorable situation in the information sphere for the resolution of operational tasks of force groupings. It is characterized by the superior functioning and stability of one's information structures over those of a potential opponent. Bolotov notes that only after achieving information superiority can other tasks (air, land, sea, and space) be resolved. Information-related tasks include obtaining intelligence, gaining unsanctioned access to an opponent's information resources, disseminating disinformation, suppressing elements of an opponent's information infrastructure, and destroying or disrupting information systems.[566]

Before conflict erupts, an information situation is developed that is favorable to the operations of one's own forces. Once military operations commence, all restrictions, including those concerned with observing norms and laws, are removed. Electronic strikes and the use of high-tech weapon strikes against important targets of an enemy's information infrastructure are delivered and information operations forces and means are brought into action. The following statement was then made:

> Recently, technologies acquired a new development regarding the rendering of information-psychological pressure on the mass consciousness, with the aim of manipulating public opinion. This has been confirmed by the experience of military actions in Syria, where the US and its allies, enemies of the legal President of Syria Bashar Assad, who is waging an irreconcilable war against ISIS, unleashed a large-scale war against him in the information sphere, with the goal of toppling the legal government.[567]

Bolotov accused the West of preparing specially prepared disinformation to influence public opinion; and accused Western news resources of regularly spreading lies and half-truths. Western methodology involves having foreign officials cite nongovernmental sources that convey Russian participation is some event. Then Western mass media spins the attack, contending that Russia's

---

[564] N. N. Bolotov, "The Essence and Content of the Concept of 'War in the Information Sphere,'" *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2017, p. 23. Dr. Harold Orenstein translated this article from Russian into English.
[565] Ibid.
[566] Ibid., p. 25.
[567] Ibid., pp. 26-27.

actions are crude and ineffective. Information is streamed through fabricated information packages. The side affected is unable to conduct their own information clarification work, since they must concentrate their efforts on verifying these packages and preparing rebuttals.[568] [Author: from a Western point of view, this method tracks precisely with what Russian propaganda and their legion of trolls attempt to accomplish with disinformation efforts aimed at the West.]

Bolotov concluded his article with two interesting thoughts. First, he stated that information sphere operations resolve tasks that are comparable in scale and importance with tasks that are resolved using fire resources, thus appearing to equate information operations with war-type activities. Second, he noted that information operations "in the future need to be viewed as a promising independent type of combat operation, through which decisive results can be achieved."[569]

Articles in the Journal *Military Thought*

Sergey Gennad'evich Chekinov and Sergey Alekseevich Bogdanov

Sergey Gennad'evich Chekinov (at last known reference point) is the Chief of the Center for Military and Strategic Studies of the Military Academy of the General Staff of the Armed Forces of the Russian Federation, Professor. He is a Colonel in the reserves. Lieutenant General (reserves) Sergey Alekseevich Bogdanov is a Doctor of Military Science and Professor and is one of the main scientific colleagues at the Center for Military Strategic Research of the General Staff.

These authors believe that it is premature to change the concept of war, even if today it is characterized not only by force alone but also by other, non-violent means to solve international relations issues.[570] Many factors (politics, aims, the projected scale of military operations, and economic, morale, and the psychological potentials of opposing states) affect war's content. They note that:

> The growing role of other forms of struggle (economic, ideological, psychological, informational, and others), in our opinion, does not change the nature of future wars; armed struggle remains the crucial factor in armed struggle, but will be used actively with all other kids of confrontation…this has impacted not only and not so much on the 'physical realm' of the subjects of war (the individual, the army, the state) as much as in the sphere of the spiritual, psychological, mental.[571]

The authors then describe various types of wars. Traditional war occurs when objectives are achieved by forceful actions where unconventional ways merely complement armed forces activities.[572] However, Chekinov and Bogdanov add that traditional war's purpose "lies not in the destruction of an increasing number of military forces of the enemy" but rather in creating conditions "where their use is ineffective," leading to an enemy's total defeat.[573] Contactless war, as the term implies, is another type of war where military, economic, moral, and psychological capabilities of the state allow for the ability to strike a host of different targets. However, it is doubtful that future wars will be contactless in the authors' opinion.[574]

---

[568] Ibid., p. 27.
[569] Ibid., p. 28.
[570] S. G. Chekinov and S. A. Bogdanov, "The Evolution of the Essence and Content of War in the 21st Century," *Voennaya Mysl'* (*Military Thought)*, No. 1 2017, p. 30.
[571] Ibid., p. 32.
[572] Ibid., p. 33.
[573] Ibid., p. 35.
[574] Ibid., pp. 36-37.

An information war is a third type, whose nature and content is to weaponize information, computers, and communications technologies to suppress an enemy or to disorganize its management and introduce chaos. Another goal of information war is to demoralize enemy personnel and the wider population. In the information sphere man's consciousness is also a target of attack.[575] Network-centric warfare is a type of war described as warfare based on nonlinearity, complexity, and chaos and is characterized by rapid control and self-synchronization. However rapid command and control is not the goal here, the authors state, but rather the timely use of strengths and advantages.[576]

Hybrid actions are, in Chekinov and Bogdanov's opinion, becoming the main way to ensure the realization of national interests. They are thought of as a kind of military action and confrontation that allows for the use of indirect actions. It's essence lies in the conduct of hostilities by regular military units and detachments of non-state actors. NATO generals feel this type of warfare offers them a distinct advantage, they add.[577]

Chekinov and Bogdanov also discuss what they term as the Cold War or a new-type of war that is progressing with the process of globalization. The management of a new-type of war is not just for world domination by the West but for controlling processes for its advantage. New-type war uses non-military means such as political pressure, information sabotage, security service work, cunning diplomacy, and speculation on humanitarian issues. It ensures that processes are designed and managed[578] and that the violent "westernization" of other peoples of the world is a main goal of the weapon. New-type war involves not only conquest but the re-division of the world. There exists a state of permanent war of this new-type where distinctions between military and peaceful means disappear. It splits conquered countries into warring parts, creating a "fifth column" for themselves. It is not a war that one perceives but is presented as propaganda to the masses as people try to avoid war. They then make two claims that are at the very least simply bizarre, that "Russia will remain the enemy of the West" and that the West will calm down "only when our country and our people have been relegated to a state worthy of ridicule and contempt."[579]

Finally, the authors briefly discuss environmental wars against humanity, which are those designed for the ownership of vital resources (fertile lands, forests, freshwater sources, mineral resources, oil, etc.) with little compassion for the environmental effects on the population. There will be consumers of natural resources and donor countries.[580]

In conclusion, Chekinov and Bogdanov state that, despite the claims of some for revisions of the essence and content of war, the application of armed force is the main criterion for distinguishing war as a special period of confrontation.[581] Any war has shown that some military and non-military forms of struggle were used. However, the main specificity of war remains acts of violence. The content of change has been in the transition from the era of human societies to the era of super societies and toward designed and managed wars, a new-type of war.[582]

---

[575] Ibid., pp. 37-38.
[576] Ibid., p. 38.
[577] Ibid., p. 39.
[578] Ibid., p. 40.
[579] Ibid., p. 41.
[580] Ibid., p. 42.
[581] Ibid.
[582] Ibid., p. 43.

Valeriy Aleksandrovich Kiselev

Valeriy Aleksandrovich Kiselev is a retired Colonel and professor at the Combined Arms Academy of the Armed Forces of the Russian Federation. He writes that two lines of thought have emerged in regard to how warfare is conducted. First, modern wars are designed to destroy a country's military and its economic infrastructure without the use of ground troops, just aerospace weapons. Second, wars can be conducted to seize territory by eventually relying on ground forces to obtain the war's objectives.[583] In both examples, the use of precision weaponry begins the active phase of conflict after being preceded by diplomatic, economic, and financial moves. There is a third type of warfare, however, and it is one that relies on illegal armed formations or private military companies. In all cases Kiselev refers to conflicts in which the US military has been involved.[584]

Illegal armed formations are actually, in Kiselev's opinion, a major element of so-called hybrid warfare. These formations include combat wings of extremist religious organizations, such as Salafism and Wahhabism. Such organizations are joined by two new spheres of combat actions, namely outer space and information. This means that combat will be very different from the past. Kiselev adds that "The presence or absence of assets, methods, and forms of information warfare can significantly affect the outcome not only of a single operation, but also of the entire military action."[585] He adds that for technologically advanced countries, cyberspace can be viewed as an operational environment for combat actions. The latter can be conducted in the form of individual computer network operations or actions can be combined with electronic warfare, psychological operations, and fire damage actions to destroy adversary assets. Such threats can take the form of criminal terrorist organizations, individual hackers, or cyber communities' or even the secret services of some states.[586]

Kiselev believes that in future wars, information confrontation will play a prominent role in the form of a set of measures aimed at exerting influence on the will, emotions, behavior, psychology, and morale of the adversary. Information confrontation implies attacks not only on information but also on information networks, especially those conducting decision-making. Information confrontation's main forms and methods will include psychological operations, ensuring data security, fooling adversaries, electronic warfare, computer network operations, and the physical destruction of adversary assets and targets, among other issues. Information and cyberwar are expected to merge and provide feed-forward and feed-back between psychic changes such as psywars and neurowars. The kinds of warfare he envisions [Author: if was hard to decipher whether he was discussing US or Russian methods] will include technological and information confrontations, behavioral warfare, and internal-policy subversive acts.[587] Behavioral wars drew special attention, as Kiselev described them as a new warfare type, which are the weapons of tomorrow:

> At the core of those is manipulating behavior algorithms, habits, activity stereotypes, etc. that have been installed in us by our social group, and also by our biographies and cultural environment. In short, the instruments for behavioral warfare work by separating the habit

[583] Valeriy A. Kiselev, "For What Kinds of Conflict Should the Armed Forces of Russia Prepare?" *Voennaya Mysl'* (*Military Thought)*, No. 3 2017, p. 37.
[584] Ibid., p. 38.
[585] Ibid., p. 40.
[586] Ibid.
[587] Ibid., p. 41.

> from the previously formed type of activity, the situation that has formed the latter, and using behavior patterns to achieve other objectives.[588]

Kiselev then goes on to state that network centrism has turned into cognitive centrism, which requires more military scientific thought on the issue. He added:

> Talking of cognitive centrism, one should first of all understand what we should teach the troops and especially commanders. And only on the basis of advanced ideas about the nature and content of future warfare can we discover the trends in military thought, the forms and methods of combat actions, and then work out and create a relevant material base for combat operational training with all that in mind.[589]

Future war must envision how long-range hypersonic guided missiles (such as Russia's Yu-71 Glider) will work with reconnaissance and strike systems and electronic warfare systems to both uncover adversary plans and targets and then to take them out with the correct mixture of exposure, control, and destruction means. The reconnaissance and strike systems must be developed in conjunction with precision-guided weapons and not separately.[590]

Finally, Kiselev notes that the ratio between weapons and specialized hardware will continue to increase versus the number of servicemen needed. Technology will continue to determine tactics.[591] Hardware and weapons are not the only factors to consider, he adds, since the value of asymmetric actions to eliminate adversarial advantages continues to rise in importance. Asymmetric actions include keeping preparations for combat actions secret, uncovering adversary weaknesses, focusing on vulnerable places (facilities) of adversaries, and imposing one's own version of conflict on the adversary (one's will). However, imbuing officers and servicemen with high morale remains the most important condition for success in future war. In closing, Kiselev noted that the theory of a new-type war must be elaborated, and it is "vital to develop the theory of asymmetric and indirect actions in conditions when the adversary acts with coalition" groupings where they maintain numerical and technological superiority.[592]

Two Articles on the Classification of War

Two articles in 2017 covered the same topic, the classification of war. The first was published in *Armeyskiy Sbornik (Army Journal*) by Alexander Ivanovich Kalistratov, and the other, by Olge Mikhaylovich Gorshechnikov, Aleksandr Ivanovich Malyshev and Yuriy Fedorovich Pivovarov, was published in *AVN.* The two are compared here for analysis purposes.

Armeysky Sbornik (Army Journal)

Alexander Ivanovich Kalistratov

Retired Colonel Alexander Ivanovich Kalistratov served as a Professor in the Operational Art Department of the Combined-Arms Academy of the Russian Federation's Armed Forces. He is well known in military circles for his work on the history of military art. His work on these and other issues is often prominently positioned in the journal *Military Thought*.

---

[588] Ibid., p. 42.
[589] Ibid., p. 43.
[590] Ibid., pp. 43-44.

[592] Ibid., p. 46.

Kalistravov wrote an interesting article on various ways to think about classifying war in 2017. However, his focus was clearly on defining and discussing hybrid war, as he did not dwell much on war's classifications as originally stated. He described hybrid war as a mixed type of war, combining strategies of indirect actions and crushing opponents. He wrote that 70-80 percent of these type wars use indirect strategies and 20-30 percent use armed violence.[593] The principal method of using them is forcing a crisis using a "fifth column" to create divisions within a state system and thereby deepen the crisis. An armed opposition will then use direct or indirect means to bring a political force to power. He states that the term comes from the United States.[594]

Hybrid wars became especially effective with the powerful development of the mass media and communication technologies, he noted. They enable the opposition to influence human consciousness and the subconscious of masses of people to carry out disobedience and sabotage.[595] Kalistratov identified three forms of hybrid war as follows: when the "fifth column" has for a long time been "preparing the ground" for external aggression conducted under the guise of humanitarian goals and limited employment of military force; when the armed forces of the aggressor destroy a state's infrastructure in a short time, and the "fifth column" sets up the unobstructed takeover of the country's territory and subsequent control of the country; and when the armed forces of the aggressor and the "fifth column" act in sync and successively in the accomplishment of each strategic task. Here, armed force on the part of the aggressor achieves the maximum success under the guise of an "innocent" ideological cover.[596]

The most characteristic features of contemporary "hybrid" warfare were described as follows:

- A change in the correlation of combat and noncombat activities of the opposing sides in favor of the noncombat aspects
- The establishment of control over the system of the state's administration of the country, affecting it by means of "agents of influence" among the ruling elite of the given country and its force structures
- The creation, within the framework of a state system of the victim country, of a special organizational mechanism of "external control," making it possible to establish indirect and covert control over the processes of the vital activities of the side that is subject to aggression
- A long preparatory period associated with the reorientation or destruction of the traditional values of the victim nation, changing them to the psychological attitudes and myths of the active side
- The undermining of the spiritual and moral foundations of the people, with the subsequent destruction of the basic principles of the nation's existence
- The formation of the perception by the mass consciousness of the people that the external aggression is a civilized transformation of a backward society to a different one, one that has a higher degree of development
- The absence of a precise hierarchy and regularity of interaction with the elements of the destructive forces of the victim country in the network structure of the active side

---

[593] A. Kalistratov, "War and Modern Times: Modern Wars: Let's Explore the Classification," *Armeyskiy Sbornik (Army Journal)*, No. 7 July 2017, p. 9.
[594] Ibid., p. 10.
[595] Ibid., p. 11.
[596] Ibid., p. 12.

- The employment of the most effective weapons against critically important targets of the state and against its armed forces, with the strict observation of the restriction on mass employment of contemporary means of destruction
- The conduct of wide-scale armed struggle under an ideological cover. As a rule, this is supposedly a struggle for human rights, for the establishment of democracy in a foreign country, for the freedom of entrepreneurship, against the spread of weapons of mass destruction, for the defense of ecology, etc.
- The "voluntary" transfer of a country's strategically important resources or sections of its territory to a geopolitical enemy under the aegis of a step on the path of the development of society[597]

Of special interest is that in his article Kalistratov used the new-type warfare methodology of Russian Western Military District Commander Colonel-General Andrey Kartapolov to describe hybrid war in 2015, thereby equating the two in his version, and the percentages he used above for indirect and direct strategies also appeared first in Kartapolov's article.[598] He also used General Staff Chief Valeriy Gerasimov's definition of "war" from the latter's address at the Academy of Military Science in March 2017, in which Gerasimov noted that it was too early to classify war as hybrid.[599] Kasistratov asked "How, then, does one oppose the strategies of such hybrid wars? For this, it is necessary to do the following:"

- Maintain the stability of state and social institutions and the public consciousness against any attempts on the part of external and internal forces to distort and transform the country's socio-political system
- Oppose any attempts to destroy sovereignty by means of the employment of various information technologies. It is important to effectively disseminate in real time true information about the state of affairs in the country
- Learn to impose one's own rules of the game and advocate a proper interpretation of events in the global information field
- Maintain at the necessary level the index of the population's public optimism and the stability of personnel in the state apparatus and force structures on the basis of the formation of a national idea and national ideology, and of success in the field of protecting the country's sovereignty and national interests
- Organize effective external and internal intelligence activities
- Take timely and decisive measures to isolate leaders of a destructive opposition, to close mass media organs that are supporting such opposition, and to block financial influxes from abroad
- Introduce martial law in a timely fashion and rigorously implement wartime laws
- Decisively suppress mass disorder and cases of the manifestation of anarchy, sabotage, and disobedience

---

[597] Kalistratov. References he noted with this footnote were those of Manoylo, A.V., "Color Revolutions in the Context of Hybrid Wars," *Pravo i Politika (Truth and Politics)*, No 10, 2015, pp. 1400-1405; Polovenko, O., and Groznyy, O., "Hybrid War: Myth or Reality?" *Krasnaya Zvezda (Red Star)*, 2 February 2015; Polovenko, and R. N. Pukhov, "The myth about 'hybrid war,'" *Nezavisimoe voennoe obozrenie (Independent Military Review)*, 29 May 2015.
[598] Ibid., pp. 12-13.
[599] Ibid., p. 5.

- Maintain the combat capability and combat readiness of the Armed Forces at a level that guarantees the substantial damaging of any potential enemy in case of aggression."[600]

This list could also apply to how the US should counter Russian influence operations.

Journal of the Academy of Military Science

Oleg Mikhaylovich Gorshechnikov, Aleksandr Ivanovich Malyshev, and Yuriy Fedorovich Pivovarov

Olge Mikhaylovich Gorshechnikov is Chief of the Scientific Research Section of Military History at the Military Academy of the General Staff. Aleksandr Ivanovich Malyshev and Yuriy Fedorovich Pivovarov are senior colleagues at the same location.

These authors were clearly anti-Western in their presentation. They noted that radical forces have appeared, where the West has tried to force democracy, create opposition forces, seize power, murder or remove political leaders, dissolve force structure and cause socio-economic instability. They begin by noting that a discussion of the typology of contemporary wars and armed conflicts is due to the fact that conflicts are no longer a simple socio-political phenomenon. Armed struggle today, in their opinion, is the result of a so-called paradox of chaos, where strong armies yield the field of battle to weaker and more poorly organized enemy forces.[601]

A Western method, hybrid operations, is used, they believe, to impose democracy on some regions of the world. Hybrid operations are used to do so. They are described as something that arose at the beginning of the 21st century when traditional and nontraditional ways of fighting were combined. Their chaotic employment can even overcome well prepared force, since they utilize a different space-time model where economic and other forms of struggle begin long before the employment of the means of armed struggle.[602]

Gorshechnikov, Malyshev, and Pivovarov write that, for Russia, military conflict is defined as a form of resolving conflicts with the employment of military force. It encompasses all types of confrontation. The authors see three characteristics of modern military conflicts, with each depending on the goals of the sides: are they aggressive (a threat to peace, an act of aggression to illegal acquire power and/or resources); liberating (defense against aggression, either individual or collective); or peacekeeping (struggle for peace through the employment of armed forces as a third side in the conflict). Armed struggle remains the principal form of confrontation.[603] The authors define war as a socio-political crisis phenomenon that is a special form of resolving conflicts between states, during which the opposing sides, in addition to the forms of struggle during peacetime, shift to armed struggle and a state of action that differs from peace.[604]

Of primary interest in the article was a diagram of how the authors classified modern armed conflicts. The three characteristics of conflict have been mentioned (aggressive, liberating, and

---

[600] Ibid., pp. 14-15.
[601] O. M. Gorshechnikov, A. I. Malyshev, and Iu. F. Pivovarov, "Problems of the Typology of Contemporary Wars and Armed Conflicts," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No 1. 2017, p. 48. Dr. Harold Orenstein translated this article from Russian into English.
[602] Ibid., p. 52.
[603] Ibid., pp. 52-53.
[604] Ibid., p. 54.

peacekeeping). Other attributes, with specific sub elements, were listed as well (see Appendix B for the actual schematic from the *Journal of the Academy of Military Science*):

- **With respect to military-political goals**: military conflict; war (large scale, regional, and local); and armed conflict (international and domestic).
- **With respect to methods of unleashing conflict**: surprise attack; gradual involvement; after strategic deployment; and covert operations.
- **With respect to subjects**: military intervention; civil war; ethnic conflicts; military expansion; and military coup.
- **With respect to medium of conduct**: aerospace, ground, naval, and information.
- **With respect to participants**: coalition, states, and private persons.
- **With respect to the principles of employment of forces**: classical operations; asymmetric operations; network-centric operations; and hybrid operations.
- **With respect to the dynamism of the sides**: maneuver operations; positional operations; retaliatory operations; preemptive operations; and blockade operations.
- **With respect to duration**: blitzkrieg (up to several days); fast-moving (up to several months); protracted (up to several years); and long (more than ten years).
- **With respect to forms**: strategic operations and actions; operations and combat operations; joint special operations and actions; operations to force peace on the aggressor; peacekeeping operations and actions; and counterterrorist operations and actions.
- **With respect to types**: offensive (counteroffensive) operations; defensive operations; armed struggle to reestablish constitutional order; armed struggle against terrorism; and armed struggle against separatism, extremism, and nationalism.
- **With respect to methods of pressure on the enemy**: simultaneous operations; successive operations; taking a region (territory) under control; isolation of a region of military (combat) operations; and sabotage and partisan operations.
- **With respect to the resources employed**: with the employment of nuclear weapons, WMD, or weapons based on new physical principles; and the use of conventional weapons or information-psychological resources.[605]

Conclusions

The extensive Russian military discussion of war above appears to contain two parts upon analysis. First, it describes trends in the world and how those trends and developments are changing war's characteristics and how it is understood and viewed. While many Russians still consider war to be the actual use of military conflict, there is a growing comprehension of a number of nonmilitary issues that have become so powerful that they may be capable of causing territorial or political change. Second, the discussion often refers to the West attacking Russia in the nonmilitary sphere of activity. Westerners reading Russia's discussion believe the attacks are actually what Russia is doing against them. That is, each side sees things differently. Russia states that it is "the attacked,"

[605] Ibid., p. 53.

"the manipulated," or "the victim" of these issues and its leadership sees conspiracies everywhere. The West, however, tends to find Russian charges against the West reflecting exactly what Russia is doing against them, especially attacking and manipulating the West via the media, use of trolls, or use of digits. Russian activities during the 2016 US elections are evidence that these charges against Russia are not farfetched.

The discussion indicated that the study of war in Russia covers, but is not limited to, the following topics: the methods and concepts to fight nonmilitary activities; features of nonmilitary actions; new actors (private armies, illegal groups, etc.) and technologies; war declaration issues; information-technology enhanced exhaustion and obliteration strategies; and the necessity in Russia to develop strong values and nationalist thought to counter information-psychological strikes and the West's hybrid warfare activities. One author noted that information operations can even be considered as an independent type of combat operation where decisive results can be obtained.

After 2017, the discussion of war slowed, probably indicating that specific decisions were made in regard to its definition. Only about four articles a year addressing war were found in publications such as the *Journal of the Academy of Military Science* and *Military Thought* in 2018. Most address war in relation to either hybrid operations of the West or the West's information-psychological actions aimed at Russia. Soon it is expected that Russia will publish a new military doctrine. In that document, the West may find conclusive evidence as to whether, after the extended discussions of 2017, the definition of war has or has not changed. In the meantime, analysts will be wise to become familiar with all of the variants proposed by specialists, as a combination of them may eventually evolve from military decision-makers.

This page intentionally left blank.

10 Russian Forecasts of Future War

Thought is the first to join a battle. Indeed, thought is a weapon…[606]

Introduction

Strategists world-wide study not only the causes of past conflicts but also how to forecast and prepare for new ones. Forecasting the shape of future wars helps determine what capabilities nations require to thwart potential opponents and what issues to include in budget requests. Examining the future war scenarios of other nations obviously can lead to better domestic planning as well. Russian analysts are no exception to such studies. Its theorists constantly pursue an understanding of how war might evolve and unfold.[607]

Russian future war planners input contemporary trends (scientific discoveries, etc.) into their analysis which lead to specific predictions (forecasts) as to how a future war might unfold and what its contents might be. These forecasts are further shaped by the logic of the situational context at hand, such as geopolitical conditions or resource exploitation potential. New forms (organizations, type of operations) and methods (new weaponry and military art) of fighting future conflicts are then considered and chosen, to include a determination of the type of force correlations required to win future war battles.

Forecasting is the key to future war planning because it results in the most likely scenarios future war might take while attempting to avoid the "paths that lead nowhere" and accepting those that "help avoid errors."[608] This requires that Russia update its forecasting predictions on a regular basis to contend with the pace of scientific and other developments. Staying current, for example, helps define ways that cyber or information technology developments, such as the creation of directed energy, precision-guided weapons, and ecological or infrasonic weapons, affect future plans.

Of increasing relevance to forecasting are what Russian officers have long referred to as the IPW. To properly prepare for the evolving IPW environment, operational adjustments are required in peacetime. As one prominent Russian officer, General of the Army Makhmut Gareyev, noted, if conflict is imminent, previously formulated scenarios and models of combat operations will have to be implemented due to the speed and mobility of contemporary operations.[609] Planning tomorrow for a surprise development today (hypersonic weapons) is more than a day late, as the contemporary information environment's impact on the IPW may even result in the conflict's end before it starts, if enough capabilities/resources are destroyed or compromised.

This chapter focuses on the military's objective and openly expressed approach to future war planning. It first examines forecasting theory and how it assists planners in their future war preparations, to include a consideration of how Russia views the shape of the contemporary IPW. It then considers the thoughts of several analysts, to include the Chief of the General Staff, as to future war's components and how it might be conducted.

---

[606] V. D. Ryabchuk, "Problems of Military Science and Military Forecasting under Conditions of an Intellectual-Informational Confrontation," *Voennaya Mysl'* (*Military Thought)*, No. 5 2008, pp. 67-76.
[607] This chapter appeared as an article in the May/June issue of *Military Review*, pp. 84-93.
[608] S. G. Chekinov and S. A. Bogdanov, "A Forecast of the Character and Content of a Future War: Problems and Judgements," *Voennaya Mysl'* (*Military Thought)*, No. 10 2015, p. 49.
[609] Gennadiy Miranovich interview with Makhmut Gareyev, "Knowledge and Skill. Reflections on What Qualities and Skills the Modern-Day Officer Should Possess," *Red Star Online*, 29 September 2017, at http://www.redstar.ru.

Some Views of Russian Forecasters

Forecasting has been a part of Russian military thought for decades. In a 1975 work on the topic of forecasting the term was defined in the following way:

> The study of the military-political situation, the pattern of war in the future, the prospects of developing strategy, operational art, and tactics, the qualitative and quantitative composition of the means of armed conflict (one's own and the enemy's), the prospects for the development of the potential of the war economy in the future, and the forecasting of the enemy's strategic and tactical plans.[610]

Contemporary authors have updated the concept, but only in minor ways. Major General (Res.) V. V. Kruglov, who wrote on forecasting and future war in 1998, 2016, and 2017, noted in 2016 that forecasting prepares the state for the most unexpected vectors of development, predicts global changes for the next 20-30 years, and estimates threats to the country 30-50 years out. Kruglov noted that President Vladimir Putin has requested work on a new, qualitatively different "smart" system of military analysis and planning. Weapon types, the nature of warfare, and better predictions of developments in the military, political, and strategic situations are required.[611]

Kruglov added that developing an armed struggle matrix for forecasters is difficult. The weapons, forms and methods of employing formations, the theater's specific characteristics, and other issues change often. As technological and intellectual standards change, so does the nature of wars and future armed struggles.[612] He recommended that forecasts and assessments be made every three to six months.[613]

In 2017, Kruglov and LTC V. I. Yakupov offered several important points to consider about forecasting's increased importance. They stated:

> The reason is armed struggle is steadily getting more complex, there is synergy between military and nonmilitary confrontation means, and lots of other factors. There are new spheres (continuums) of military confrontation: information-communication, consciental (psychological), and cognitive (area of thinking). Before long new types of weapons will appear and, therefore, also new spheres of struggle (that are not much in evidence or are only forecasted).[614]

The authors ruled out a large-scale war but noted that forecast-based risks may entice confrontations to occur. However, starting such a conflict without a foregone conclusion of success is dangerous. Surefire forecasts are mandated, requiring a solid knowledge of forecasting theory and methodological skills.[615]

The authors explained that an objective difficulty of forecasting is simply the uneven progress of knowledge. With Nano and other technologies increasing by some 35 percent a year, it is difficult to forecast which countries will make what discoveries and what their impact will be on their military forces. Further, the active and covert use of nonmilitary means are extremely difficult to

---

[610] Yu. V. Chuyev and Yu. B. Mikhaylov, *Forecasting in Military Affairs*, Moscow 1975, translated into English by the DGIS Multilingual Section, Secretary of State, Ottawa, Canada (Washington, DC: US Government Printing Office, 1980), p. 14. Published under the auspices of the US Air Force.
[611] V. V. Kruglov, "Military Forecasting: The State, Potential, and Realization of Results," *Voennaya Mysl'* (*Military Thought)*, No. 12 2016, p. 33.
[612] Ibid., pp. 34-35.
[613] Ibid., pp. 35, 38.
[614] V. V. Kruglov and V. I. Yakupov, "On the Methodology of Forecasting Armed Struggle," *Voennaya Mysl'* (*Military Thought)*, No. 4 2017, p. 5.
[615] Ibid., p. 6.

"analyze, consider, and formalize, and this makes even more complex the process of forecasting armed struggle and interstate confrontation."[616] Not mentioned by these forecasters are the expected changes to be wrought by quantum computing, artificial intelligence, and other discoveries, which may double forecasting difficulties.

Forecasting the use of new weaponry with covert (cyber) or surprise characteristics has forced Russian analysts to focus on the growing importance of the IPW. Those nations who gain the initiative in the IPW due to scenarios that are preplanned will be more likely to attain initial success that could even lead to the quick subjugation of an opponent. Most likely Russia's IPW focus is a direct result of the Soviet experience in WWII when the nation was not properly prepared to go to war with Germany and experienced early setbacks. Now, in the age of cyber, information superiority has become crucial to success in the IPW. Russia must begin shaping the information environment (and geopolitical one) to its advantage in peacetime. Efforts can include planting cyber viruses in important systems of an opponent's infrastructure, capturing the electronic warfare frequencies and equipment operating parameters of a potential opponents' equipment, scrambling global positioning system frequencies, or conducting reconnaissance on key underwater cables for espionage or destruction purposes. Diplomatic, economic, and other environments are also potential targets of manipulation to enable victory in the IPW.

Russia's military often discusses the IPW. For example, a 2012 *Military Thought* discussion defined the IPW as operations conducted before the start of war to achieve objectives or to create favorable conditions for committing their main forces.[617] Outer space, information warfare, and new weapon capabilities were said to help create conditions favorable for the IPW. More importantly "In all likelihood, the aggressor country is to be expected, still in peacetime, to launch a wide-scale targeted information operation and intense reconnaissance activities, including a set of related and closely coordinated actions."[618] Thus, if an opponent is expected to perform in such a manner, Russia must either counter these actions or, more likely, take the initiative themselves to achieve control in the IPW. The IPW, the authors note, will include the launching of information operations, which include technical and psychological attacks, along with electronic operations and fire strikes to disorganize government systems, demoralize populations, and prevent leaders from rallying forces to repel aggression.[619] The attainment of information superiority and the use of the mass media will stir up chaos and confusion in an adversary's government and military management and control systems.[620]

In 2015 two authors added their input to the IPW discussion. They wrote that a contemporary military goal is to put an adversary on the verge of defeat at the beginning of hostilities, accomplished by wreaking havoc on its political and economic situation using IT-generated psychological and other types of warfare; and by disabling the adversaries control of the country and armed forces through attacks on strategic installations and infrastructure. The ability to manipulate public opinion and utilize the benefits of nonlethal weapons is also under study.[621]

---

[616] Ibid., pp. 7-8.
[617] S. G. Chekinov and S. A. Bogdanov, "Initial Periods of War and their Impact on a Country's Preparations for Future War," *Voennaya Mysl'* (*Military Thought)*, No. 11 2012, p. 16.
[618] Ibid., p. 24.
[619] Ibid., p. 25.
[620] Ibid., p. 27.
[621] P. A. Doulnev and V. I. Orlyansky, "Basic Changes in the Character of Armed Struggle in the First Third of the 21st Century," *Journal of the Academy of Military Science*, No. 1 2015, p. 46. The author would like to thank Dr. Harold Orenstein for his translation of this article.

Perhaps due to concern for the US's cyber security in the IPW, the US Federal Bureau of Investigation (and earlier, the government of Ukraine) decided to no longer allow the sale of the Russian-produced Kaspersky anti-virus solutions, a product sold in stores and advertised on prominent radio stations. Such products may have offered the ability to insert a virus or logic bomb into a critical information domain that would ensure Russia would have information superiority in an IPW. A recent *Wall Street Journal* article noted that the Kaspersky anti-virus has been on a Defense Department watch list of potential problems since 2004. In 2013 the Defense Intelligence Agency issued a Pentagon-wide threat assessment about the company. US officials note that the firm's products were used as a tool for spying on systems in the US.[622]

Contemplating Future War

After considering the trends in military affairs and how an adversary might use force or the manipulation of context in the IPW, theorists then contemplate how future war might unfold. The following summary from 2012-2018 of future war thought by several Russian military officers and civilians offers significant insights into a future war's potential conduct.

In 2012 G. A. Naletov, writing in the *Journal of the Academy of Military Science*, examined future war's impact on the development of new forms and methods of warfare.[623] Naletov stated that outwardly the forms of military operations have changed little, and include war, armed conflict, operations, strikes, engagements, battles, and combat operations, while their content has changed significantly. Armed struggle is qualitatively different regarding weaponry and methods of their employment. He listed fire-strike, electronic-strike, robotized, aerospace, air-mobile, air-assault, information-reconnaissance-strike, counter-reconnaissance operations, and other actions as some of them.[624]

Naletov observed that combat and noncombat forms of actions are converging; that defensive operations will be more dynamic in terms of maneuver retaliatory-meeting strikes or preemptive strikes; and that future operations will consist of indirect, noncontact, and actively preemptive effects.[625] He stated that it is time to "broaden the arsenal of resources" for conducting armed struggle, to include weapons based on new physical principles (NPP). They will include geophysical, infrasonic, climate, laser, ozone, radiological, accelerator (beam), electromagnetic, directed energy (beam super-precision), nonlethal (against personnel: psychotropic preparations, infrasonic weapons; and against materiel: electromagnetic weapons, resources for radio-electronic suppression and physical effects against computers, biotechnical and chemical resources that corrupt products), and genetic, ethnic, acoustic, and radio-frequency weapons. Speed of decision-making, tempo, and conflict intensity will increase, while temporal parameters (time to accomplish missions) decrease.[626] Operational speed and intensity will not give an enemy time to organize countermeasures. The space domain will increase in importance and the nuclear domain will find its burden somewhat decreased. These, Naletov wrote, "are the principal opinions about the development of new forms and methods of conducting future armed struggle."[627]

---

[622] Paul Sonne, "Russian Firm Was Long Seen as Threat," *The Wall Street Journal*, November 18-19, 2017, p. A2.
[623] G. A. Naletov, "On the Issue of the Development of the Concept of Non-traditional Warfare and Armed Conflicts," *Journal of the Academy of Military Science*, No. 1 2012, p. 29. The author would like to thank Dr. Harold Orenstein for his translation of this article.
[624] Ibid., p. 30.
[625] Ibid., p. 33.
[626] Ibid., pp. 33-34.
[627] Ibid., p. 34.

Authors P. A. Doulnev and V. I. Orlyansky, writing a few years later in the same journal, also noted space's growing importance. Space-based weaponry or military malware used for the first time capitalize on surprise and fully implement other principles of operational art. A critical goal will be to attain space superiority in future wars. The authors stated:

> Therefore, already in the nearest future we can expect the emergence of new forms of military operations in near space—space operations (military actions) aiming to defeat orbital alignments of forces, suppress radio communication systems in space, block orbital alignments of forces and means in specific areas of space, etc.[628]

In 2013 Russia's *Army Journal* published an article that General-Major Vladimir Slipchenko had apparently written before his death a few years prior. It was odd that the article hadn't appeared earlier, as he was one of Russia's most popular military authors in the preceding two decades. Slipchenko wrote that superiority over an opponent was only possible after superiority in information, mobility, and rapidity of reaction were assured. Precise fire and information effects against economic structures and military objectives were required. Slipchenko referred to this as noncontact war. In such war, information confrontations would be continuous and would leave the operational and strategic levels and acquire a planetary scale.[629]

Information confrontation's principal goal is the maintenance of one's own information security and the lowering of a potential enemy's.[630] Recce-strike combat systems will be used extensively to detect and deliver strikes against various target types. This will, from Slipchenko's point of view, radically change the content and nature of warfare, since:

> It will not be masses of forces, but rather recce-strike and defensive combat systems that will clash in such noncontact warfare. Their potentials are characterized not by the quantitative and qualitative superiority of one of the sides, but rather by structural and organizational factors, the uniformity and effectiveness of command and control, and the functional quality of communications and guidance systems and other links in the all-round support of military operations.[631]

He and other Russian analysts stress the importance of structure and organization over quantity and quality.

Also in 2013, General-Lieutenant Victor Vinogradov stated his assumptions as to how war may unfold in the future. The IPW will have a distinctive flavor of surprise and may include the use of weapons based on NPP, tilting war quickly toward the use of weapons of mass destruction.[632] Offense and defense will share the following distinctions:

- The growing role of the first electronic and fire strike
- Resolve in achieving the goals of an operation
- Dynamic and maneuverable style of combat
- A greater role for highly effective strikes
- Tense fighting to seize and hold the initiative
- Sudden changes in the situation and tactics

---

[628] Doulnev and Orlyansky, p. 49.
[629] V. Slipchenko, "Information Assets and Information Confrontation," *Army Journal*, No. 10 2013, pp. 52-53. The author would like to thank Dr. Harold Orenstein for his translation of this article.
[630] Ibid., p. 55.
[631] Ibid., p. 57.
[632] V. A. Vinogradov, "On Tendencies in the Character and Methods of Conducting Operations in a Major War," *Voennaya Mysl'* (*Military Thought)*, No. 10 2013, 27.

- A broader spread of simultaneous combat operations
- And the rising role and significance of protection[633]

Finally, in a nod toward military art, Vinogradov stated that the course and outcome of operations will be affected by a potential adversary's view on the ways that advanced weapons and operations will be used.[634]

In 2015 S. G. Chekinov and S. A. Bogdanov, two of the most popular Russian military authors with wide-ranging expertise (having written on indirect war, asymmetric war, 21st century war, etc.), discussed forecasting and future war in the journal *Military Thought*. Forecasting, they note, reflects how the geostrategic situation is developing, how interstate relations are changing, and how these changes are affecting military art. To achieve its objectives, the military must "abandon decisively" the rigid cannons of modern military art.[635] Perhaps this implies the extended use of more indirect and asymmetric responses to threat perceptions.

Long-term forecasting "has assumed the significance of a national task. Nothing will take the place of long-term forecasting trends in the way in which the geostrategic situation is going…"[636] Forecasting must take into consideration that war's concept is expanding and includes economic, ideological, psychological, informational, and other areas, not just armaments.[637] The authors support the contention that all efforts initially will be tied to the attainment of information superiority, noting that "Information warfare in the new conditions will be the starting point of every action now called the new-type of warfare (a hybrid war) in which a broad use is made of the mass media and global computer networks."[638] Information weapons will paralyze the computer systems that control troops and weapons and deprive the enemy of information transmission functions. Computers will turn into a strategic weapon of future wars.[639]

The authors believe that future wars will begin with a strategic electronic warfare and aerospace attack, augmented with cruise missiles, reconnaissance-strike and -fire delivery systems, and UAVs and robots. The goal is overwhelming superiority everywhere.[640] Speed, synchronization, and concurrency will be decisive factors for military operations, with joint task forces and their strike assets controlled in real time relying on computers, telecommunications, and satellite communications.[641]

The authors then offered a few unconventional thoughts on future war that were also mentioned by Naletov. They stated that unconventional arms might cause earthquakes, typhoons, or heavy downpours leading to the erosion of economies and to the intensification of tension among the population in an adversary country. Further, space-based attack weapons, orbiting battle space stations, automated weapons control, and new weapons of improved destructive power, range, and accuracy will require new forms and methods of warfare.[642] Electromagnetic, information, and

---

[633] Ibid., p. 26.
[634] Ibid., p. 29.
[635] S. G. Chekinov and S. A. Bogdanov, "A Forecast of the Character and Content of a Future War: Problems and Judgements," *Voennaya Mysl'* (*Military Thought)*, No. 10 2015, pp. 42-43.
[636] Ibid., p. 43.
[637] Ibid.
[638] Ibid., p. 44.
[639] Ibid.
[640] Ibid., p. 45.
[641] Ibid., pp. 42-43.
[642] Ibid., p. 44.

infrasonic weapons may be used against forces, economic facilities, government and military control systems, and energy generation centers.[643]

Finally, future wars main distinctions are: weapons designed on NPP; a reduction in the significance of nuclear weapons; strategic operations as the principal form of strategic task fulfillment; and a unified system for collecting and processing information through the integration of space, aerial, and ground reconnaissance capabilities for target allocation. The opening period of a future war with a competent enemy force would last at least a month, according to Chekinov and Bodanov, while the closing period has to conclude as soon as possible.[644]

In 2017 V. A. Kiselev, a professor at Russia's Combined Arms Academy, discussed two lines of thought in *Military Thought* that have emerged about how warfare is conducted today and in the future. First, wars are now designed to destroy a country's military and its economic infrastructure without the use of ground troops, just aerospace weapons. Second, wars still can be conducted to seize territory by eventually relying on ground forces to obtain the war's objectives.[645] In both examples, the use of precision weaponry begins the active phase of conflict after being preceded by diplomatic, economic, and financial moves. Kiselev offered a third type of warfare as well, one that relies on illegal armed formations or private military companies. In each of the cases he cites, Kiselev refers to conflicts in which the US military has been involved,[646] failing to mention that all three types were used by Russia in Syria if one interpolates special forces as ground forces.

Kiselev focused on developments in future war's nature. He stated that

- Outer space and information are two new independent spheres of combat actions.
- Major targets and critical facilities will be attacked by precision fire and electronic and information attacks.
- Reconnaissance-strike systems and electronic warfare systems should be used jointly.
- The technological constituent of future war will be weapons based on new physical principles.
- And information confrontation (in the form of a set of measures aimed at exerting influence on the will, emotions, behavior, psychology, and morale of the adversary) will play a prominent role.[647]

It is expected that information and cyberwar will merge and provide feed-forward and feed-back between what he called Psywars and Neurowars [no further explanation of either term was offered].[648] Behavioral wars drew his special attention, describing them as not only a new warfare type but as the weapons of tomorrow:

> At the core of those [behavior wars] is manipulating behavior algorithms, habits, activity stereotypes, etc. that have been installed in us by our social group, and also by our biographies and cultural environment. In short, the instruments for behavioral warfare work

---

[643] Ibid., p. 46.
[644] Ibid., pp. 47-48.
[645] Valeriy A. Kiselev, "For What Kinds of Conflict Should the Armed Forces of Russia Prepare?" *Voennaya Mysl'* (*Military Thought)*, No. 3 2017, p. 37.
[646] Ibid., p. 38.
[647] Ibid., pp. 39, 43, 44, 44, and 41, respectively.
[648] Ibid., p. 41.

> by separating the habit from the previously formed type of activity, the situation that has formed the latter, and using behavior patterns to achieve other objectives.[649]

In closing, Kiselev noted that the theory of a new-type war must be elaborated, and it is "vital to develop the theory of asymmetric and indirect actions in conditions when the adversary acts with coalition groupings" and maintains numerical and technological superiority.[650] Asymmetric actions include secrecy, finding weak points and vulnerable facilities in an adversary, and imposing one's own version of conflict on an adversary.[651]

General of the Army Makhmut Gareyev, one of Russia's greatest military theoreticians, stated in 2017 that the greatest enemy for the art of war is a "stereotyped and schematic approach."[652] Gareyev noted regarding future war that:

> As far as the operations and hostilities of the future are concerned, it may be assumed that they will differ by their increased scale, the participation of heterogeneous forces equipped with complex heterogeneous combat hardware, a high level of dynamism and maneuverability, the absence of coherent fronts, a dramatically and rapidly changing situation, a fierce struggle to seize and retain the initiative, and a strong electronic warfare element. All this will significantly complicate the command and control of troops and naval forces.[653]

A high level of planning will become the main prerequisite for success and previously formulated scenarios and models of combat operations will have to be implemented due to the speed and mobility of contemporary operations.[654] This appears to be Gareyev's statement that these models and scenarios must be ready for the initial period of war.[655]

At a November 2017 speech to the Defense Ministry Collegium, General Staff Chief V. V. Gerasimov discussed the type of forces Russia should plan to use in case of war. He stated that primary military efforts would continue to be placed on the development of nuclear and nonnuclear forces, the latter specified as precision guided missiles and Kalibr and Iskander-M missiles. Other efforts included an emphasis on ensuring an echeloned system of aerospace defense, improving Russia's command and control system, improving the organizational development of general-purpose forces, creating self-sufficient groupings of troops and forces on strategic axes, and reequipping forces with state-of-the-art systems. Gerasimov discussed the need for increased readiness and arming of the military districts. He noted that improvements were made in UAVs, command and control capabilities, and electronic warfare systems.[656] Gerasimov's comment about increased arming of military districts implies an adjustment of the correlation of forces in each one.

Finally, in 2018, at the Academy of Military Science, Gerasimov produced what he described as the outlines of a probable future war. Such conflicts will feature the extensive employment of precision weapons and other types of new weaponry, such as robot technology. Priority destruction targets will include economic and state control systems, and the information sphere and space will

---

[649] Ibid., p. 42.
[650] Ibid., p. 46.
[651] Ibid.
[652] Miranovich, 29 September 2017, at http://www.redstar.ru.
[653] Ibid.
[654] Ibid.
[655] Ibid.
[656] "Speech by General of the Army Valeriy Gerasimov, Chief of the General Staff of the Russian Federation's Armed Forces/First Deputy Defense Minister of the Russian Federation, at an Open Session of the Russian Federation Defense Ministry Collegium on 7 November 2017," *Ministry of Defense of the Russian Federation Website*, 7 November 2017.

be dynamically involved. Finally, a special role will be afforded to countering communications, reconnaissance, and navigation systems.[657] Gerasimov noted that UAVs, on the one hand, are witnessing the development of future multipurpose complexes that make both reconnaissance and strike tasks plausible. On the other hand, Russian scientists are developing futuristic systems to counter adversarial use of UAVs with weaponry based on NPP.[658] He foresees the use of precision means, including hypersonic, to shift the "principal portion" of strategic deterrence from the nuclear to the nonnuclear forces. The role of command and control organs is increasing in regard to decision-making, and future research must be directed at improving this area.[659] Local war experiences and Syrian operations have given "a new impulse for improving the system of the comprehensive destruction of the enemy."[660] Also of note, Gerasimov used the term "comprehensive destruction" three times in his presentation. In 2013 he noted that nonmilitary means would be used over military ones by a ratio of 4:1. There was scant mention of nonmilitary issues in 2018.

Conclusions

This analysis of Russian future war thinking over the past six years demonstrates that it is an evolving and dynamic process that is continuously being updated. An entire host of various weaponry (NPP, ecological, ultrasonic, etc.) is apparently under development. There were also warnings to Russian analysts to "abandon decisively" the rigid cannons of military art and develop new methods for its conduct.

Three issues stood out from the analysis. First is the necessity to completely plan for the IPW now in peacetime. Specific scenarios are required. Second was the warning that information technology's use in the IPW could end a war before it begins if, for example, information infrastructure or command and control nodes are completely put out of commission. Third, and perhaps most important, was the warning that a contemporary war's destructive nature, due to the growing capabilities of even conventional weapons, could quickly turn decision-makers to the use of weapons of mass destruction. Before long new spheres of struggle (quantum, etc.) not much in evidence yet will appear, making forecasting more complicated. These variables will enter the armed struggle matrix, affecting the forms and methods of combat actions, the theater's specific characteristics, and other issues, such as nonmilitary trends.

Information warfare was stated to be the start point for all new-types of warfare, since even the mass media and global computer networks can get involved. The study of asymmetric, indirect actions, and aerospace operations is important. Finally, future war's priority destruction targets were stated to be economic and state control systems. Gerasimov's conviction that "comprehensive destruction" is required was not reassuring. Future war preparations also would involve assigning a special role to countering communications, reconnaissance, and navigation systems.

Russia will continue to evaluate all aspects of its operating environment and look for places where it can gain an operational advantage in the opening phase of any future conflict. One is reminded

---

[657] V. V. Gerasimov, "The Influence of the Contemporary Nature of Armed Struggle on the Focus of the Construction and Development of the Armed Forces of the Russian Federation. Priority Tasks of Military Science in Safeguarding the Country's Defense," *Journal of the Academy of Military Science*, No. 2 2017, p. 18. The author would like to thank Dr. Harold Orenstein for his translation of this article.
[658] Ibid., p. 19.
[659] Ibid., p. 21.
[660] Ibid., p. 19.

of the wise words of now deceased Russian General Major V. D. Ryabchuk, who noted that "thought is the first to join a battle. Indeed, thought is a weapon…"[661]

[661] V. D. Ryabchuk, "Problems of Military Science and Military Forecasting under Conditions of an Intellectual-Informational Confrontation," *Voennaya Mysl'* (*Military Thought)*, No. 5 2008, pp. 67-76.

11 Russian General Staff Chief Valery Gerasimov: Shaping Russia's Armed Forces and Military Thought

> It is unusually difficult…to predict a war situation. For each war it is necessary to work out a special line of strategic behavior, each war represents a specific case that requires the establishment of its own logic and not the application of some stereotypical pattern.[662]

Introduction

Russia's current Chief of the General Staff, Valery Gerasimov, has now been in charge of the General Staff for over six years. Along with President Vladimir Putin and Defense Minister Sergey Shoigu, he has orchestrated a major upgrade of the Armed Forces. The force is now in possession of thousands of pieces of new equipment and numerous new organizations to improve its command and control. Perhaps as important is that Gerasimov has led a rejuvenation of military thought in Russia, motivating professors and instructors to train officers at the General Staff Academy (GSA) in ways to use their knowledge to develop new concepts in military art and forms and methods of fighting. Officers are encouraged to be innovative and creative in these activities. Gerasimov has also gathered and shared the experiences of the officers and soldiers who have participated in combat operations in Chechnya, Ukraine, and Syria at forums such as the AMS; and he has shared the General Staff's observations of foreign military operations in Afghanistan and Iraq.

The following discussion of Gerasimov's tenure is divided into four parts. First, Gerasimov's background is constructed, which indicates his extensive command responsibilities and experience. Second, Gerasimov has issues with the West. Many, it turns out, are self-generated issues caused by the Russian proclivity to avoid responsibility (for example, its unwillingness to admit responsibility for the shootdown of the Malaysian airliner, generating fake stories that its force is not in Ukraine, etc.). Third, a summary is provided of some of Gerasimov's more important interviews or presentations at localities other than the AMS. Finally, there is a summary of important points from the seven presentations he has made at AMS from 2013-2019, each of which has made a difference in how Russia's military operations are viewed abroad.

Part One: Background

General of the Army Valery Gerasimov was born in 1955 in Kazan. He initially served in tank or motorized rifle assignments. In 1997 he graduated from Russia's General Staff Academy and soon thereafter served in Chechnya. Between 2003 and 2005 he served as the chief of staff in the Far Eastern Military District before becoming the head of the Main Directorate for Combat Training of the Russian Armed Forces. In 2006 he was appointed as the Commander of the Leningrad Region Military District and in 2009 Commander of the Moscow Military District. In 2010 he became a Deputy Chief of the General staff, in 2012 the Commander of the Central Military District, and in November 2012 the Chief of the General Staff and the First Deputy Defense Minister.[663] He apparently commanded the Victory Parade on Red Square, an honor, from 2009-2012. Thus, his command experience is hard to top. Further, he is known for demanding professionalism from the force.

---

[662] V. V. Gerasimov, "Principal Trends in the Development of Forms and Methods of Employing Armed Forces and Current Tasks of Military Science Regarding their Improvement," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, 2013, No. 1, p. 29.

[663] No author or title provided, *Interfax*, 9 November 2012.

As a Deputy Chief of the General Staff Gerasimov helped introduce digital technologies to the force (with a focus on command and control issues), helped create a joint air defense system with the Commonwealth of Independent States (CIS), and helped with negotiations with NATO on military cooperation.[664] He took a special interest in the US's missile defense system, claiming in 2011 that it upsets the strategic balance of nuclear forces.[665] In 2012, speaking at a Defense Ministry conference, he stated that the US system poses a threat to Russia's ability to hit targets in the US. He showed computer generated images of potential flight trajectories to demonstrate that, from his perspective, US defense systems in Poland and Romania were aimed against Russian missiles rather than Iranian ones, as the US had stated. He also stated that the US and Russia should "take advantage of each other's radar capabilities to counter missile threats."[666] Cooperation was not out of the question, and he has continued to meet with US Chairmen of the Joint Chiefs of Staff to this day.

Gerasimov was described by former Russian Strategic Rocket Forces' Main Staff Chief, Colonel-General (retired) Viktor Yesin, as "having excellent creative skills as a leader and efficiency as an organizer."[667] He was expected to do away with the chaos of the recent years that preceded his appointment, in Yesin's opinion. Another complement, an interesting and important one, was paid to him by journalist Anna Politkovskaya, who was gunned down in Moscow by assailants near her apartment. She was a critic of the Chechen conflict and President Putin but wrote that Gerasimov is "a man who was able to preserve an officer's honor" during the war.[668]

President Putin stated that Gerasimov's main tasks would be the "rearmament of the army and the fleet" and improving "both the structure and the command of troops." An additional task would be to organize stable relationships with the defense-industrial complex.[669] Putin had noted that "The situation keeps changing in science and technology and new means of warfare emerge,"[670] which makes Gerasimov's creative skills important to capitalize on new warfare means. On 15 November 2012 Gerasimov was appointed to Russia's Security Council.[671]

Part Two: Gerasimov's Issues with the West

Gerasimov has made numerous outstanding presentations to his officer corps. However, they often include accusations against the West. Gerasimov points out alleged Western threats and dangers to Russia that the West would consider responses to Russia actions, not threats. Gerasimov ignores Russian territorial conquests or half-truths over situational context and blames "color revolutions" directed from the West to detract attention from the Kremlin's land grabs. In spite of overhead images of Ukraine showing Russian vehicles presence or text messages from Russian soldiers on the ground in Ukraine, Gerasimov's military denies the occupation of Ukrainian territory. Former President Ronald Reagan's dictum of "trust but verify" fails to function in the Putin era, since Russia rejects even the results of verification from such images and phone messages. The Kremlin continues to manipulate objective reality to its desire with such rejections of responsibility, which

---

[664] Sofya Shaydullina and Roman Dobrokhotov, "No Mere 'Ceremonial' General Gerasimov," *Slon*, 9 November 2012.
[665] No author or title provided, *RIA-Novosti*, 30 November 2011.
[666] No author or title provided, *Rossiya 24 TV*, 3 May 2012.
[667] No author or title provided, *Interfax* (in English), 9 November 2012.
[668] No author or title provided, *BBC Monitoring* (in English), 9 November 2012.
[669] No presenter or title provided, *Channel One TV*, 9 November 2012.
[670] No author or title provided, *Interfax* (in English), 9 November 2012.
[671] No author or title provided, *Interfax*, 15 November 2012.

has resulted in a backlash from the West in the form of a loss of trust in Russia's civilian and military authorities.

These issues are pointed out here since Gerasimov's discussions of military affairs and his anti-Western statements need to be placed in some sort of situational context. Russian denials are part of a general mindset among Russian leaders, who appear intoxicated with their own paranoia and suspicions that bring out fantasies about Western behavior.

Actions have consequences. Here are several examples. Russia's numerous cyber intrusions, some military, into Western nations have united them against Russia. The latter's denunciations only cause the further deterioration of trust in Russia. Nearly every country in Europe and North America has been a victim of a Russian cyber-attack. The US even gave Russian authorities the names of the Russian military personnel behind the attacks, which indicates Gerasimov was very aware of what operations were being conducted. In other cases, only the Russian military intelligence service was charged.[672] The sum of these charges must number close to 15 countries by now. This is not Ukraine in 2014, where that one nation was affected by Russian pressure on Kiev's leadership. This is 15 or so nations which independently express the same concern for being targeted, and their blame points directly at the same culprit. Such overwhelming evidence has cost Russia not only trust but its credibility as well.

A second example is Western accusations that Russia had violated the INF treaty. It was the cause for the crumbling of the treaty. Russian statements that they have not violated the treaty were met with skepticism, since their credibility is razor thin. Treaties have also crumbled due to the Kremlin's grab of Crimea and insertion of troops into Eastern Ukraine, which Gerasimov blames on the West. Finally, Gerasimov continually notes that Russian weaponry has no analogues in the West. Russia has developed and now uses weapons based on new physical principles that support Gerasimov's intent to construct a nonnuclear strategic deterrence concept that can be used to scare nations into compliance. If there are no analogues to these weapons, shouldn't the West be the one fearing Russia and Russia the one threatening others? If the US was really out to "put Russia in its place" as Gerasimov contends, shouldn't it have done so in the 1990s, when Russia was in its weakest condition in decades and had no high-tech weaponry? The West made no such attempt.

Thus, the reader is warned to keep these points in mind as one examines Gerasimov's many presentations, which describe many advances Russia has made in acquiring new armaments and forces that can deter, in his opinion, any adversary. The work of Russia's military-industrial complex is noteworthy, for sure. But the other side to his presentations is their stark accusations of the dangers and threats associated with Western actions, while ignoring the causes associated with them. The issues raised above do, however, demonstrate how an authoritarian regime's paranoia and suspicion can affect their perceptions of the West and, vice versa, Western perceptions of Russia.

Part Three: Gerasimov's Non-AMS Interviews and Presentations

2012

Gerasimov's late 2012 interviews included a discussion of the academy's importance and a few comments about the military's role in Syria. At a speech on Russian television, speaking about the GSA's anniversary celebration, Gerasimov noted that the academy's focus on strategic studies and

---

[672] In the latter case, see Aruna Viswanatha, Sadie Gurman, and Del Quentin Wilber, "Russian Indicted in DNC Hacking," *The Wall Street Journal*, July 14-15, pp. A1, A3.

economics, the "root cause of any war, any conflict," was important.[673] In a way the interview gave viewers a taste of Gerasimov's interest in nonmilitary issues.

2013

In January 2013 Gerasimov warned against foreign intervention in Syria, which he said would have disastrous consequences for the region. The accumulation of arms, he notes, causes increased risks and can lead to potential provocations as well.[674] A day later he noted that the withdrawal of the International Security Assistance Force from Afghanistan might provoke radical forces in that country.[675] He clearly appeared interested in keeping Syria free from outside influence but was interested in getting help in Afghanistan.

2014

At Moscow's Third International Security Conference, Gerasimov and other military leaders were to discuss "color revolutions" in many areas of the world, especially the Middle East and North Africa. However, much of the discussion focused on Ukraine. A different color revolution is unfolding in Ukraine, he noted, one that is gradually moving toward a civil war. Authorities there are taking an adaptive approach to the use of force against the unarmed population in the East of the country.[676] Naturally, Gerasimov's conclusions vary dramatically from the way the West views the situation there, where the involvement of Russian forces has been demonstrated. It is Russia's involvement and not the use of force by Ukraine against its own people that is the issue.

At the end of 2014 Gerasimov summed up the year. Top priorities were strengthening the nuclear deterrent, rearming with modern weaponry, and establishing forces in Crimea. The top event in his estimation was the development of the National Defense Command Center. The latter allows the Defense Ministry to monitor situations in real time. Also, a Joint Strategic Command focused on the Northern Fleet was set up. Overall Gerasimov stated that the combat capability of the Armed Forces rose by 30 percent.[677] However, Russia's Defense Ministry Press Service and Information Directorate noted that Gerasimov, some two weeks earlier in a meeting with foreign military attaches, used a significant portion of his talk to blame the US and the West for causing instability and he stated that, in great divergence from what is known to be true in the West, that "Russia is not a party to the conflict in Ukraine, since this is directly contrary to its national interests and to the Russian and Ukrainian peoples' many centuries of shared history."[678] Obviously this goes against all of the images from Russian selfies and Western overhead imagery that prove otherwise.

2015

In January Gerasimov focused his attention on responding to the US missile defense system, stating that it had changed the military-political situation. He accused the US of violating the Intermediate-Range Nuclear Forces Treaty (INF) and the Start-3 Treaty. He stated that a military priority was to improve the quality of the strategic nuclear force as a result.[679]

In May 2015 the journal *Armeyskiy Sbornik* published Gerasimov's presentation at the Fourth Moscow Conference on International Security. He stated that it was the US, NATO, and the EU

---

[673] No author or title provided, *Rossiya 24*, 8 December 2012.
[674] No author or title provided, *Interfax-AVN Online*, 16 January 2013.
[675] No author or title provided, *Interfax* (in English), 17 January 2013.
[676] No author or title provided, *Rossiya 24 TV*, 23 May 2014.
[677] No author or title provided, *Rossiya 24 TV*, 29 December 2014.
[678] Defense Ministry Press Service and Information Directorate, "Russian Chief of the General Staff General of the Army Valery Gerasimov Met with Foreign Military Attaches," *Ministry of Defense of the Russian Federation*, 10 December 2014.
[679] No author or title provided, *Interfax*, 30 January 2015.

who were trying "to put Russia in its place" after the latter's principled and independent position regarding the settlement of the situation in Ukraine.[680] Gerasimov noted that NATO is expanding its structure eastward toward Russia's western border. This attitude is destroying the security architecture and the equal security of all states.[681] Borders are also threatened by frozen conflicts in the post-Soviet space, such as the Dniester area in Moldova, Abkhazia and South Ossetia, and Armenia and Azerbaijan. Unfreezing them carries the threat of armed clashes in the area's proximity. The threat of global terrorism cannot be forgotten either.[682]

In December Gerasimov summed up the year as follows: Main priorities are the ability to maintain strategic offensive and defensive forces at levels that provide for the deterrence of aggression against Russia; the need to increase Aerospace Forces and the potential of strike forces and information and command and control systems to support deterrence; and the need for improvements in the system of research and development.[683]

2016

Moscow's Fifth International Security Conference was reportedly designed to discuss problems associated with terrorism, cooperation, security, and the Asia-Pacific region. Color revolutions, Middle East and Central Asia challenges, and the military's role in assuring the stability of countries were also problems to consider.[684] No formal report of Gerasimov's comments has been available, and all that is known of his presentation is included here from a variety of sources. He stated that the Arab Spring has resulted in a migration chaos in Europe; that Russian advisors are helping the Syrian army command plan combat operations; and that terrorism cannot be defeated without military force.[685]

In an article in *Red Star* in September, Gerasimov discussed his impression of Kavkaz-2016, a yearly huge military exercise, this time organized in the Southern Military District. A focus of the exercise was to tackle the topic of territorial defense. The idea is to incorporate into one mission the national economy, personnel from the Defense Ministry, the Ministry of Internal Affairs, the Federal Security Service, National Guard, and Ministry of Emergencies. Mobilization priorities and plans were addressed as well. Information warfare was paid close attention to for the first time. Gerasimov noted that "information warfare is comparable to effective engagement and could at some stage even prevail."[686]

2017

Gerasimov made one of his most important presentations in December of 2017, so this section is a bit longer than the others. In the journal *Military Thought*, he outlined what he had accomplished in fulfilling a plan that President Putin devised and implemented by decree in May 2012. Putin's May Decree was published in full that year in the military newspaper *Red Star*. It noted in particular that the Armed Forces should be equipped up to 70 percent with modern models of arms and special equipment by 2020. Putin's priority developments (in the order they were stated) were the nuclear deterrent forces; air and space defense systems; systems of communication,

---

[680] Valery Gerasimov, "The Military Dangers and Military Threats to the Russian Federation in Contemporary Conditions," *Armeyskiy Sbornik (Army Journal*), No. 5 2015, p. 58.
[681] Ibid., p. 59.
[682] Ibid., p. 62.
[683] No author or title provided, *RIA Novosti*, 14 December 2014.
[684] No author provided, "Russian Defense Ministry to Organize the 5th Moscow International Security Conference on April 27-28*," Interfax* (in English), 14 March 2016.
[685] No author or title provided, *TASS*, 27 April 2016.
[686] Aleksandr Tikhonov, "In the Southwest Sector," *Krasnaya Zvezda (Red Star*) Online, 16 September 2016.

reconnaissance, command and control, and electronic warfare; unmanned aerial vehicles (UAVs); robotized strike systems; modern transport aviation; precision weapons and means of combating them; and systems for the individual protection of service personnel. The Navy received attention to develop the means to protect the Arctic and Far East, and Putin stated that a new system of analysis and strategic planning in the interests of countering threats to national security for 30-50 years was planned for state arms programs.[687]

Gerasimov stated in his 2017 *Military Thought* article that his primary efforts were directed at the readiness of the strategic nuclear and nonnuclear forces, aerospace defense, improving command and control systems, and developing general-purpose forces and creation of self-sufficient groupings. Nonnuclear forces included precision-guided munitions, to include the Iskander-M and the Kalibr missiles.[688] Gerasimov added that "all told, the proportion of state-of-the-art models of arms in the ground, air, and naval strategic nuclear forces was taken to 74 percent."[689] Thus, his comments appeared to be his report card as to how he had fulfilled Putin's directions from 2012 and, if the numbers are correct, he did quite well.

With regard to each area, Gerasimov's article listed several specific systems that were major developments in the past five years. He stated that with PGMs, hypersonic missiles shift strategic deterrence missions from the nuclear to the nonnuclear sphere. The Voronezh and Daryal, Dnepr, and Volga radars were being modernized, helping eliminate gaps in the northern and southern parts of the nation. There were 55 military spacecraft launched in the past five years, which provide communications, intelligence, and navigational information as needed.[690] For the 38 units and subunits activated in the last five years, over 1800 UAVs were delivered to outfit them. They can perform reconnaissance up to 500km in depth and can employ electronic warfare capabilities and support for reconnaissance-strike and reconnaissance-fire delivery loops.[691] Azart radios provided communications in areas where adversary electronic countermeasures were encountered. New electronic warfare models, some nineteen altogether, along with 2000 new-generation complexes came into the inventory, expanding the engagement and countermeasure ranges by some 3.5 times. EW assets on UAVs can block radio communications within a radius up to 100 kilometers.[692] Snap inspections are essentially operational-tactical exercises that rehearse a full package of missions, especially along strategic axes. At this time, two battalions are of contract personnel and a third is manned by conscripts in each regiment and brigade. It was noted that a mandatory requirement was the rehearsal of problems associated with the employment of reconnaissance-fire and reconnaissance-strike loops.[693]

The remainder of Gerasimov's 2017 article focused on Russia's experiences in Syria. Combat experience activated new forms of employing the Armed Forces and methods of conducting operations. The use of reconnaissance-strike and reconnaissance-fire delivery loops developed at the tactical level were discussed.[694] The latter implemented the principle of "one target—one

---

[687] Nikolay Voronin, "Edict of the Russian Federation President 'On the Implementation of Plans and Programs for the Building and Development of the Armed Forces of the Russian Federation and Other Troops, Troop Formations, and Organs and the Modernization of the Defense Industry Complex'," *Krasnaya Zvezda (Red Star)* Online, 8 May 2012.
[688] V. V. Gerasimov, "On Implementing the Executive Orders of the President of the Russian Federation of 7 May 2012, No. 603 and 604, and the Development of the Armed Forces of the Russian Federation," *Voennaya Mysl' (Military Thought)*, No. 12 2017, p. 7.
[689] Ibid., p. 8.
[690] Ibid., p. 9.
[691] Ibid., p. 12.
[692] Ibid., p. 13.
[693] Ibid., pp. 15-16.
[694] Ibid., p. 19.

bomb" where fire engagement was organized on a zonal principle. Near fire engagement zones used the Strelets and the Su-24M bomber. Medium engagement zones (up to 500 Kilometers) used Su-24 bombers and Su-33 fighters using PGMs. Long-range fires included the Kalibr sea launched cruise missiles, Kh-101 air-launched cruise missile, and Tu-22m3 bombers for a fire engagement zone with a radius of 4000 kilometers.[695]

Also, in December 2017 Gerasimov discussed operations in Syria with Viktor Baranets. He stated that the first mission the Armed Forces encountered was identifying and destroying enemy control centers. Gerasimov said the most difficult thing for the General Staff was the organization of collaboration with Syrian government troops and all the various other groups involved. Countering terrorists use of vehicle bombs was another problem, as they would often rush several vehicles at a defensive position or roadblock at one time. Finally, there have been 60-70 UAVs in the air every day in Syria on the average. They help coordinate the use of reconnaissance-strike and reconnaissance-fire loops. Several conferences on the Syrian campaign have been held and a whole series of manuals were published that generalized the experience, according to Gerasimov.[696]

2018

In December 2018 Gerasimov addressed military attaches in Moscow. He stated that there was an increasing potential for conflict and that the struggle for energy, water, food, and other resources was intensifying. The address was similar to the one he provided in 2014 in regard to his criticism of the West. Gerasimov stated that Washington wants to contain Russia and discredit its role in international affairs. He stated that the alleged threat from Russia has caused NATO to increase its military presence close to Russia's borders. He stated that Russia is not increasing the strength of its Armed Forces and is not involved in an arms race (yet in most interviews he underscores Russia's work on new weapons and its plans to increase its force quantitatively). Anything the US is doing or has done in Syria was criticized by Gerasimov during his presentation. He went so far as to say that one Western coalition bombing campaign wiped the city of Raqqa off the face of the earth. The US's irresponsible actions, he added, have demonstrated a compete indifference to the stabilization of the situation there. After this constant bombardment of the West, along with only praise for Russia's efforts in Syria, Gerasimov stated that in 2018 several improvements were made to the Russian Armed Forces. The force's combat potential was raised, nuclear and nonnuclear forces maintained a high level of combat readiness, a layered aerospace defense system was built up, and command and control system training were improved.[697]

Part Four: Presentations at the AMS

Each February or March, a general assembly is held at the Academy of Military Science. The Academy's President, General of the Army Makhmut Gareyev, opens the conference. Gerasimov is the featured speaker. Summarized below are the seven presentations he has made. These presentations initially included numerous tables and graphs, but this habit ended in 2016. Now only a photo of Gerasimov and his presentation are included in the *Journal of the Academy of Military Science*, which publishes his presentation, usually in the first edition of the year.

---

[695] Ibid., p. 18.
[696] Viktor Baranets interview with Valery Gerasimov, "Russian Armed Forces Chief of the General Staff Army General Valery Gerasimov: 'We Broke the Backbone of Terrorism's Shock Forces'," *Komsomolskaya Pravda Online*, 27 December 2017.
[697] No author or title provided, *Ministry of Defense of the Russian Federation Website* (in English), 5 December 2018.

2013 Speech at the AMS—Forms and Methods of Warfare

There were several important aspects of Gerasimov's presentation, the best known of the seven he has made. First, he used the term "new-type military conflicts" to describe conflicts that are comparable in their consequences to "regular" war. The term new-type took hold in the Russian military and has been used by numerous Russian military authors to the present time. Second, he called for the creation of "a holistic theory of asymmetric operations." Asymmetric actions, he noted, include the use of special operations forces, internal opposition to create a "moving front of struggle," and information effects. This, of course, requires Western analysts to understand how Russia further defines asymmetry and the expansion of the concept for military use. Third, he described numerous new trends in the character of war. They were:

- The differences between the states of war and peace are being erased.
- Wars are no longer declared and do not follow stereotypical patterns of the past.
- Safe states territory can be turned into an armed struggle arena in months or days.
- The rules of war have changed.
- Nonmilitary methods to achieve goals have grown. Opposition methods use political, economic, information, humanitarian, and other nonmilitary measures.
- Military methods include covert measures, such as information opposition, peacekeeping, crisis management, and special operations forces.
- Military methods are more dynamic, energetic, and effective[698] using remote, noncontact effects.
- Differences among strategic, operational, and tactical levels of operations (and between offensive and defensive) are being erased.
- Precision weapons, weapons based on new physical principles, and robotics are being introduced into military affairs.[699]

Finally, eleven times Gerasimov referenced a need to develop new forms and methods of warfare. Specifically, he stated that improved forms and methods of information effects were being developed,[700] and that new forms and methods needed to be developed for the following: asymmetric operations and employing force groupings,[701] operating aerospace defense systems and using Russian forces outside its borders,[702] and forms and methods of all-round support systems.[703] Thus, Western analysts need to understand just how Russia understands the terms forms and methods.

Gerasimov's presentation also mentioned, through the use of quotes, two famous Soviet military theorists. They represent, from the Soviet period, how to think about the initial period of war and military strategy, and the concepts appear to have carried over to Gerasimov's present-day thought. He quoted former Division Commander Georgii Samoilovich Isserson as follows:

---

[698] V. V. Gerasimov, "Principal Trends in the Development of Forms and Methods of Employing Armed Forces and Current Tasks of Military Science Regarding their Improvement," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, 2013, No. 1, p. 24. The author would like to thank Dr. Harold Orenstein, who has translated Gerasimov's presentations from 2013-2018.
[699] Ibid., p. 26.
[700] Ibid., p. 24.
[701] Ibid., p. 26.
[702] Ibid., p. 27.
[703] Ibid., p. 29.

> War, in general, is not declared. It simply begins with armed forces that have been deployed beforehand. Mobilization and concentration are associated not with the period after the advent of a state of war, as happened in 1914, but rather unnoticeably, conducted gradually, long before this.[704]

Russian use of cyber issues to infiltrate and map the information infrastructure of another country would fit Isserson's understanding of the initial period of war.

Gerasimov quoted the outstanding Soviet military scholar Alexander Svechin on strategy:

> It is unusually difficult…to predict a war situation. For each war it is necessary to work out a special line of strategic behavior, each war represents a specific case that requires the establishment of its own logic and not the application of some stereotypical pattern.[705]

Gerasimov preceded his quote from Svechin by noting that Russia should not copy foreign experience and try to "catch up with" leading countries. Rather Russia should develop its own forms and methods and rely on military science.[706] Perhaps for this reason Russia has shunned hybrid war for many years and focused more on new-type warfare methods.

There were six tables associated with the presentation. Two of them, "The Role of Nonmilitary Methods in Resolving Interstate Conflicts" and "The Changing Character of Armed Struggle," have appeared often in military journals in the West. The former noted that nonmilitary methods of resolving armed conflict are being used by a ratio of 4:1 over military methods. The latter table listed both traditional and new forms and methods of conflict. The other four graphs were:

- Forms and Methods of Military Operations from the Example of the Afghan War
- Trends in the Development of Robotic Means in the US Air Force
- The Operational Use of Armed Forces Formations Outside the Borders of the Territory of the Russian Federation
- Principal Tasks of Military Science[707]

2014 Presentation at the AMS—Role of the General Staff and Changing Nature of War

The essence of Gerasimov's 2014 presentation was to discuss how the country's defense was organized, with a focus on the role of the General Staff, the changing nature of warfare, and requirements for the military-industrial complex to fulfill. The General Staff's activities were somewhat the same, focused on strategic planning, the Armed Forces' development, and the military organization of Russia as a whole, to include the coordination of the activities of the executive authority. Armed struggle changes included taking into consideration its fast-moving character and employment of military and nonmilitary resources. The use of nongovernmental international organizations and private military companies have acquired greater weight in achieving military-political goals.[708]

In Russia's new Defense Plan, measures for the nation's defense and a shift from a peacetime to a wartime footing were discussed, such as the place, time, directions, forces, means, and resources

---

[704] Ibid.
[705] Ibid.
[706] Ibid.
[707] Ibid., pp. 25-28.
[708] V. V. Gerasimov, "The Role of the General Staff in the Organization of the Country's Defense in Accordance with the New Statue on the General Staff, Approved by the President of the Russian Federation," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 1 2014, pp. 14-15.

required for coordination. A strategic deterrence plan was developed to convince potential aggressors of the futility of any attack on Russian territory. The Defense Plan led the way for the establishment of a new edition of the Statue on Military Planning in the Russian Federation, which specifies the sequence for using the defense plan, the documents that comprise it, and the state organs and military command and control entities that are responsible for developing the documents.[709] The state and military entities were integrated in the National Center for Defense Management.

With regard to the General Staff's leadership of the military-scientific complex, several tasks must be fulfilled. The main one is to recommend the most efficient composition of the Armed Forces and the optimum correlation of forces and means for armed struggle. A second task is forecasting and assessing threats to Russia, exposing them as early as possible in order to create a "comprehensive theory of indirect and asymmetric actions conducted by various federal executive organs."[710] A final task is to develop the forms for employing force groupings and the methods of their operations as well as their optimal composition. This requires a study of combat experiences in various conflicts and highlights new military-technical trends.[711] Special attention is required in the areas of robotics, telecommunication infrastructure, and strategic deterrence and aerospace forces.[712] It is important to develop both military and nonmilitary measures under modern combat conditions and assess their balance. A plan is being developed to form "the fundamental laws of contemporary international confrontation, taking into account the employment of so-called 'soft force.'"[713]

There were eleven tables that were included in Gerasimov's presentation. They were:

- Tasks of the General Staff of the Armed Forces of the Russian Federation
- Changes in the Nature of Armed Struggle
- Changes Introduced into the Federal Law "On Defense" by the 5 April 2013 Version
- The Administrative System of the Military Organization of the Russian Federation
- Forms of Operational Readiness with the Participation of Federal Executive Organs
- The Purpose and Tasks of the Military-Scientific Complex of the Armed Forces of the Russian Federation
- The Development of the Military-Scientific Complex of the Armed Forces of the Russian Federation in 2013
- An Outline of the Structure of the Future Military-Scientific Complex of the Armed Forces of the Russian Federation
- Priority Trends in the Development and Creation of Weapons Systems
- The Formation of a Uniform Base of Scientific Knowledge
- And Trends in the Joint Work of Russia's Ministry of Defense and the Academy of Military Sciences.[714]

---

[709] Ibid., p. 16.
[710] Ibid., p. 19.
[711] Ibid.
[712] Ibid., p. 21.
[713] Ibid., p. 22.
[714] Ibid., pp. 14-22.

The table associated with "Changes in the Nature of Warfare" is listed below. It outlines Russia's understanding of modern conflict and responses to these changes. After the title, the sentence "The use of political, diplomatic, economic, and other nonmilitary measures in combination with the use of military force" was stated, which was followed by the bullets below (the first two entries remind analysts of Russia's strategic operation to destroy critical infrastructure targets):

- Reduction of the military-economic potential of a state by the destruction of vitally important objects of its military and civilian infrastructure
- Simultaneous effects against enemy troops and objectives to the entire depth of his territory
- Armed struggle simultaneously in all physical media and in the information domain
- Command and control of forces and means in a uniform information domain
- Mass employment of precision weapons, large-scale use of special operations forces, robotic systems, and weapons based on new physical principles
- Employment of asymmetric and indirect operations
- Commencement of military operations by peacetime force groupings
- High-maneuver, noncontact combat operations by interservice force groupings
- And participation of the civil-military component[715]

2015 Speech at the AMS—Great Patriotic War Lessons for Today

Gerasimov's 2015 presentation listed lessons learned from the Great Patriotic War (GPW or WW II) and what new duties the General Staff had accumulated over the past 75 years. GPW lessons were as follows:

- State administration organs needed restructuring so that peacetime structures would closely resemble wartime manning, which took too long to establish in the GPW.
- Command and control structures need a uniform system beforehand, so that commanders will understand what decisions can be independently made at the start of enemy aggression, especially after a surprise attack.
- Cooperation must be established among services and branches, to include the creation of interservice force groupings in theaters of military operations and under a unified command in peacetime.
- Technical capabilities of the strategic leadership must be established in peacetime, especially command and control of forces.[716]

To ensure strong command and control, and to institute lessons learned from the GPW, Russia created the National Defense Control Center to ensure state control. The Center is designed to forecast a situation's development, provide information support for leadership decisions, and coordinate activities of federal executive authorities.[717] The 2013 General Staff Decree, which outlined its duties, support this development. The General Staff is charged with strategic planning

[715] Ibid., p. 15.
[716] V. V. Gerasimov, "The Experience of Strategic Leadership in the Great Patriotic War and the Organization of Uniform Command and Control of the Country's Defense under Contemporary Conditions," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2015, p. 12.
[717] Ibid., p. 13.

in the area of defense; safeguarding the state's military security; developing the Armed Forces; commanding and controlling the Armed Forces; coordinating federal executive organs activities; developing a Defense Plan for the Russian Federation; and coordinating the activities of the organs of state authority.[718] To increase state organ leadership capabilities, a special training course was organized at the General staff Academy. Thus, Russia is taking everything it can from the GPW experience that applies and developing military art applicable for the postwar period.[719] Two diagrams were produced as part of the article. One was titled "Analyzing and Forecasting the Development of the Situation," which listed some of the areas that need to be watched; and the "Organs of Strategic Command and Control of the Military Organization of the Russian Federation," which listed some of the areas and centers that monitor the situation or take part in fulfilling requirements.[720]

2016 Presentation at AMS—U.S. Hybrid Issues and Counters to Them

Gerasimov's presentation appeared to have four main parts: to describe the dangers of hybrid war that other nations are implementing; to find a way to work with the US in Syria; to describe organizational changes in the Russian Defense Ministry to combat hybrid's impact; and to inform researchers that new forms and methods of employing various military and nonmilitary activities of territorial defense were required. The latter point thus once again supports Gerasimov's 2013 speech that was oriented on the forms and methods of warfare.

With regard to hybrid war, he noted that methods were changing in the direction of employing political, economic, information, and other nonmilitary measures supported with military measures. The use of internal opposition forces, and partisan and sabotage methods, minimize the need for armed effects. Color revolutions, defined as a state revolution organized from without, are used to achieve military-political goals. The use of such indirect and asymmetric methods deprives an opposing side of sovereignty without the use of military force.[721] These were the Western hybrid threats that Russia was facing.

Gerasimov then discussed the need to work with the US in Syria, stating that only Russia and the US have the power to stop the war, in spite of their varying political interests and goals. He added that both sides have conducted preparatory work so that combat operations may cease immediately, on 27 February 2016. Information was exchanged about a cease fire and a general understanding of borders was reached.

Next Gerasimov underscored the need to consolidate the efforts of all organs of state power to confront hybrid operations. The military alone was not a sufficient answer to the problem. For example, forty-nine organs of state power worked on the Defense Plan for 2016-2020, which indicates that methods other than military ones can be used to confront hybrid actions. Ways were sought to neutralize dangers and threats from abroad, such as hybrid methods of pressure.[722] Finally, Gerasimov stated that the development of forms and methods for the employment of force groupings and procedures for military and nonmilitary actions were required. Command and control elements of the state's military organization are of primary importance for ensuring the

---

[718] Ibid., p. 14.
[719] Ibid., p. 15.
[720] Ibid., pp. 14 and 13, respectively.
[721] V. V. Gerasimov, "The Organization of the Defense of the Russian Federation under Conditions of the Enemy's Employment of 'Traditional' and 'Hybrid' Methods of Conducting War," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2016, p. 20.
[722] Ibid., p. 21.

consolidation of executive authority. The National Center for Command and Control of the Defense of the Russian Federation ensures the country's military-political leadership during a crisis situation.[723]

Gerasimov stated that future research trends included the following: the development of forms of strategic operations for the Armed Forces; improving offensive and defensive forces and the means for struggles in the space and information domains; and developing operational-strategic requirements for weapons and command and control systems.[724] He thus makes it clear that strategic issues are the most important for the AMS and the General Staff to consider.

2017 AMS Presentation—Contemporary War, Elements of Thought

This presentation focused on a discussion of most of the elements of military thought (trends, forecasting, and forms and methods of warfare—strategy was only barely mentioned). Hybrid war was defined as an America proposal that "refers to actions that occur in a period that cannot possibly be associated purely with war or with peace."[725] He defined war in accordance with Russia's Military Doctrine, stating that it is "a form of resolving inter-state or intra-state conflicts with the employment of armed force."[726] He added that in 2016 a discussion on war's concept was organized at the General Staff Academy.[727]

Conflicts between those in the 20th and 21st centuries differ from one another in their composition of participants, weapons employed, and forms and methods of troop activities. In addition, the correlation of the contribution of one type of conflict over another has changed. The US demonstrated its use of new forms in its conflict with Libya, where a no-fly zone, a naval blockade, and the use of private military companies were employed, according to Gerasimov. Social networks were also used to increase the information-psychological impact of the operation. Syria, on the other hand, was described as a US hybrid operation.[728] Gerasimov stated that he considered the use of the term hybrid warfare as an established term to be premature at present.[729]

Gerasimov then described unfolding trends, forecasting issues, and forms and methods of fighting in more detail. Developing trends included the blurring of the line between a state of war and peace; and the broadening spectrum of reasons and approaches for using military force, such as to support a state's economic interests. Methods were discussed next. He stated they are moving in the direction of the extensive use of political, economic, diplomatic, information, and other nonmilitary measures, all supported by the protest potential of a population.[730] The use of forecasting to assess dangers and threats to Russia is also growing. This has moved one task to the top of the list for the country's defense, that being the development of a strong strategic deterrence potential. Deterrence through capabilities, it would seem, both material and spiritual.[731]

Gerasimov stated that Russia's capabilities now include the ability to resolve strategic missions in a remote theater of military operations. The Armed Forces have demonstrated the ability to conduct

---

[723] Ibid., p. 22.
[724] Ibid., p. 23.
[725] V. V. Gerasimov, "Contemporary Warfare and Current Issues for the Defense of the Country," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2017, p. 9.
[726] Ibid., p. 10.
[727] From January to June 2017, there were numerous discussions of war in military publications.
[728] Gerasimov, 2017, pp. 10-11.
[729] Ibid., p. 11.
[730] Ibid.
[731] Ibid., p. 12.

new-type warfare, to include working with allies and organizing coalitions. In closing, he again requested of the AMS to study new forms of inter-state confrontation and to develop effective methods to counter them. This applies to developing counters to hybrid warfare methods of the West. New forms and methods of troop operations under various conditions need study as well, especially the organization of force regroupings in remote theaters of military operations.[732]

2018 AMS Presentation—Future Wars

Gerasimov began this presentation noting that there are three important trends influencing military operations: those affecting the content of operations; those demonstrating an improvement in the system of comprehensive destruction of an enemy; and those showing improvements in weapons developments.[733] He added that the type of Armed Forces required is dependent on the quality of forecasting variants of the military-political situation in the world.[734] In this regard, he noted that the spatial scale of conflict is expanding at a time when the temporal preparation of the Armed Forces is decreasing. Simultaneous and continuous operations are replacing sequential operations, and the borders of theaters of military operations are increasing. Targets now include the economic potential of a country far from the zone of military operations and command and control superiority has become a necessity for winning. Future wars are expected to include precision guided munitions, state control targets, the use of information and space assets, and the need to counter communications, reconnaissance, and navigation capabilities of adversaries. He added that each conflict has its own distinguishing features.[735]

There is now a necessity to develop interservice force groupings for various strategic axes. Work is being done on an automated interservice reconnaissance-strike system that can reduce the time from reconnaissance to strike by 2.5 times. Ground force formations are being manned according to the principle of two battalions of contract workers and one battalion of conscripts. New weaponry will shift the focus from nuclear strategic deterrence tasks to a nonnuclear strategic deterrence force.[736]

Near the end of his presentation, Gerasimov stated that today, scientifically justified recommendations on the employment and development of the Armed Forces are required of the General Staff. This requirement includes the following:

> First and foremost, this involves increasing the authenticity of scenarios being developed and of long-range forecasts of the development of the military-political and strategic situation. Priority tasks for military science must be studying future trends of interstate confrontation, the forms of employment of the Armed Forces, and the methods of conducting operations and combat in future military conflicts. The elaboration of the issue of the content of combat operations at the operational and tactical levels is important.[737]

The content of operations at the operational level most likely is indicative of operational design. In this paragraph Gerasimov covers all of the main elements of developing operations—studying

---

[732] Ibid., pp. 12-13.
[733] V. V. Gerasimov, "The Influence of the Contemporary Nature of Armed Struggle on the Focus of the Construction and Development of the Armed Forces of the Russian Federation. Priority Tasks of Military Science in Safeguarding the Country's Defense," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2018, p. 16.
[734] Ibid., p. 17.
[735] Ibid., pp. 17-18.
[736] Ibid., pp. 19, 21.
[737] Ibid., pp. 21-22.

trends, making forecasts of the strategic situation, developing forms and methods, and applying them to operations.

2019 AMS Presentation—New Thoughts on Military Strategy

Gerasimov's presentation focused on several themes that he had covered in earlier presentations (robotics, UAVs, new weaponry), which left the impression that scientists and theorists weren't getting his message and he thus had to stress those topics again. The tasks of military science, a term he used 16 times, was stated to be one of two main directions of the presentation.

The other direction was the term military strategy, which he used 24 times, and his definition of the term was very different from his previous discussions. In the past, in two different AMS talks, he stated that "each conflict has a logic all its own," which was understood as saying strategy wasn't fixed but depended on the logic of the situation at hand. There was one instance when he came close to stating this expression in 2019, noting that "It is necessary to form principles of a general, universal nature and principles of actions as applied to the situation specifically taking shape."[738]

Throughout this presentation, however, he offered numerous ways of understanding strategy, to include the following:

- Military strategy as a science is the art of command and control.
- Strategy represents a system of knowledge and actions to prevent, prepare for, and wage war.
- A search for rational strategies of waging war against a varying enemy acquires priority importance for developing the theory and practice of military strategy.
- The forms and methods of employing the Armed Forces in support of strategic deterrence is an important aspect of military strategy.
- Military strategy has gone through stages of evolution from a strategy of annihilation, strategy of attrition, and strategies of global war, nuclear deterrence, and indirect actions.
- Russia's response to US actions is the strategy of the active defense, which envisages a set of measures for preemptive neutralization of threats to national security.
- The development of strategy as a science must encompass the development of a system of knowledge about war and an improvement of practical activity to prevent, prepare for, and wage war.
- Strategy must engage in predicting the nature of future war and the development of new strategies for waging them.
- The famous Russian commander Aleksandr Vasilyevich Suvorov noted that "Theory without practice is dead" and this is why it is impossible to imagine the practical activity of military strategy without its scientific substantiation.
- An urgent task of military strategy is the substantiation and upgrading of nuclear and nonnuclear deterrence measures.

---

[738] V. V. Gerasimov, "Vectors of Development of Military Strategy," *Krasnaya Zvezda (Red Star*) Online, 4 March 2019. This presentation of Gerasimov is the only *AMS* article NOT based on his report as published in the *Journal of the Academy of Military Science*, since that journal will not be available for a few months.

- Russia's experience in Syria has played an important role in strategy's development, as fulfilling tasks outside of Russian territory is part of a strategy of limited actions.[739]

Gerasimov listed some additional items in regard to the military's experience in Syria that appear to have more general application. First, he stated that the most important conditions for implementing the strategy of limited actions are winning and holding information superiority; preemptive readiness of command and control and comprehensive support systems; and covert deployment of necessary groupings. Second, new methods of troop actions were substantiated. Military strategy consists of planning and coordinating joint military and nonmilitary actions of the Russian grouping of troops and the force elements of involved states.[740]

Further, Gerasimov underscored four directions for strategy's development. The first involves creating and developing a unified system of integrated forces and assets of reconnaissance, engagement, command and control, and fire control based on state-of-the-art information and telecommunications technologies. The second direction involves the use of military robotic complexes, especially UAVs. The third direction involves countering adversary UAV and PGM use. A deciding role here will be played by electronic warfare forces and assets. Finally, increasing the Armed Forces combat might is a priority direction, determined by the numerical and qualitative composition of the force, its strength and outfitting, its morale and training, and its combat readiness and effectiveness.[741]

Other items deemed important in the theory and practice of military strategy were control over territorial defense missions during times of escalating threats or crisis situation periods; and the substantiation of an integrated system for protecting critically important facilities of a state's infrastructure, when an adversary might try to use attacks on them to destabilize a situation or create chaos and uncontrollability. Finally, Gerasimov stated that new approaches are needed to create ties between the economy and military strategy. Strategy must answer the following questions: "For what kind of possible war and in what directions to prepare the economy? How to ensure its survivability and stability? And how is it more advisable to accommodate facilities of the economy with consideration of their protection?"[742] All of the above concerned strategy.

There were two other aspects of the presentation worthy of note. First, Gerasimov continued his anti-West and anti-US diatribe that he began in December 2018 when he addressed military attaches in Moscow. He stated that geopolitical rivals (who but the US and the West?) are prepared to wage wars using precision-guided munitions and information warfare. The goal of the US, he notes, is to eliminate the statehood of undesirable countries and change the legally elected state authorities (Russia? Venezuela? a contention most European nations and the US would contest). He notes that a "trojan horse" strategy of military operations has been developed by the Pentagon, which few have heard of in the US. It supposedly involves a fifth column of media and other elements to destabilize a situation followed by PGM strikes against important targets. Further, Gerasimov stated that the US and NATO are now at Russia's borders (with no mention of the reason, that Russia has taken Crimea from Ukraine and intervened in the nations Eastern sector);

[739] Ibid.
[740] Ibid.
[741] Ibid.
[742] Ibid.

that the US is destroying arms control treaties (not stating it was due to Russian infractions); and that the US is developing space troops (not mentioning Russian thoughts on the same issue).[743]

Finally, Gerasimov listed several principles for preventing, preparing for, and waging war. Preventing wars are accomplished by foreseeing the military-political and strategic situations and identifying threats and dangers. Advance preparation is accomplished by ensuring constant combat and mobilization readiness. Waging war requires the coordinated use of military and nonmilitary measures. Utilizing surprise and decision-making speed allows Russia to preempt an opponent in case of war and ensures the strategic initiative.[744] These principles are worthy of the interest of Western analysts.

Conclusions

Gerasimov has commanded military districts, served in Chechnya, organized and led the battles in Ukraine and Syria, and helped in the procurement of numerous weapons and other pieces of equipment from the military-industrial complex. He has badgered the officer corps, professors, and academics to update military thought, to identify trends and thus threats to Russia, to propose new theories of strategy and asymmetric war, and to organize counters to a host of potential threats, whether it be UAVs, electronic warfare systems, command and control structures, or satellites. He has talked about new-type war and has only referred to hybrid war when talking about the West and US in particular. He has also bought into the ideology of denying responsibility for his actions, like other Kremlin leaders, causing the military's mindset to resemble that of the Soviet period in many respects.

There are several important take-aways from Gerasimov's numerous presentations that offer areas for Western focus:

- On numerous occasions he has requested that new forms and methods of warfare be developed, whether it be to confront hybrid war capabilities of the West or terrorist actions in Syria or how to confront new conflicts. It is imperative that Western analysts understand just how a form and a method might be defined and further developed. There are very few Western analysts who know what each term means, even though the Russians use the terms repeatedly.
- Russian officers and scientists are told not to stereotype combat scenarios but to be prepared to develop new innovative and creative means of combat. Gerasimov has focused on making officers learn to take the initiative and make decisions in a timely manner. Russian officers are told to understand both classical and asymmetric types of combat. The latter can include new forms of military art. This requires continual study of the changing nature of war.
- Officers are told to be prepared for the initial period of war, which makes them focus their attention on the preparation of the force in peacetime and to focus on attaining information superiority, two items crucial for success; and to make updated calculations of the necessary correlation of forces (qualitatively as well as quantitatively), since the correlation is affected most by information technologies.

[743] Ibid.
[744] Ibid.

- In conjunction with the military-industrial complex, Gerasimov is developing weapons based on new physical principles that will both serve as a counter to an adversary's high-tech weapons and ensure the implementation of strategic nonnuclear deterrence for Russia over potential opponents.

Gerasimov is a worthy Chief of the General Staff, one who is ensuring that Putin and the nation get the type of Armed Forces, both quantitatively and qualitatively, that will ensure the nation's security. Meanwhile, in the West, our hopes are that he doesn't shirk responsibility for his actions and blame them on schemes of Western involvement that are far from reality. He is professional and an officer of integrity, but that doesn't mean his own Soviet- and Russian-inspired mindset couldn't lead him down the wrong path.

12 Conclusions

Introduction

This work has focused on the concepts and elements that compose Russian military thought and how they might be applied. Understanding military thought is important, for an examination of another nation's thought template helps with estimates of what they might do next and why; helps with exposing and eliminating the mirror-imaging of friendly thought patterns onto an opponent; and helps with new ways of thinking about strategy, operational art, and tactics for friendly forces.

Based on the chapters in this report that specified some specific Russian military thought patterns or qualities, the hope is that analysts will be able to discern important elements of Russian thought and how these elements might be applied to new technological developments. A summation of these points is in the first section of these conclusions.

That section is followed by a short examination of whether Russian military concepts coincide with those of the Kremlin. If true it might indicate closer cooperation between the two than originally suspected; or it might indicate that there is a specific tradition of thought in Russia that is applicable to both civilian and military decision-makers. Specific threat stimuli may result in common cultural responses in both military and political cases. Risk-taking, the development of alternate realities, and other methods of conducting operations (indirect, asymmetric, nonmilitary, etc.), for example, appear to be methods that both the military and civilian establishments employ.

Overcoming Western Stereotypes

There are numerous Western journalists and a few military analysts who ascribe Russian actions to be "hybrid" in nature. There are other Western authors who look for Russian activities in the grey zone. These are examples of mirror-imaging the Western thought process onto Russia's and they result in stereotyped responses that miss the focus of Russian activities and planning.

There is a possibility, however, that the Russian term "new-type" warfare is somewhat synonymous with hybrid, since military authors sometimes place the term hybrid in parentheses behind new-type. While this suggestion of some compatibility should be taken into consideration, it is more noteworthy that it is hard to find a prominent military official who clearly endorses hybrid war as a primary Russian concept. Ninety-nine percent of Russian military authors state that hybrid is the type of warfare the West is conducting against Russia.

General Staff Chief Valery Gerasimov noted in 2017 that it was too early to state that what is occurring in military activities is hybrid in nature. President Putin supported Gerasimov's point the same year, stating that there is no need "to think up mythical Russia threats, hybrid wars, and so on. These are your [the West's] own fancy, and then you scare yourselves, and based on that formulate a policy prospect."[745] Russia's April 2019 security conference in Moscow featured a special session on Western concepts, in which hybrid actions and color revolutions were discussed, further buttressing Russian claims that these are methods used by the West against Russia.

In spite of these Western accusations, Russia's military continues to utilize its traditional building blocks of military thought. Gerasimov charges the Academy of Military Science yearly with

[745] No author or title provided, *Interfax* News Agency (in English), 30 May 2017.

developing new forms and methods of thought, and there are recommendations to revisit forecasts of potential war more often, with some analysts recommending such work every 3-5 months.

The elements stressed in this publication attempted to focus the reader's attention on the traditional building blocks that compose the Russian military thought process. In no particular order, the following terms summarize the focal points of the numerous chapters:

- Forecasting
- Forms and methods of fighting
- Correlation of forces
- Disorganizing an enemy force
- Reflexive control
- Asymmetrical and indirect operations
- Equal security
- Military art
- Information-technical and information-psychological actions
- Military and nonmilitary methods of conflict
- New-type warfare
- Operational design
- Trends in warfare
- Deterrence theory's various applications
- Objective reality

These terms represent a solid understanding of Russian military thought. While this report covered the past several years, it is possible to find most of these categories in Russian articles from fifty years ago. They also appear nearly monthly, indicating their priority in the development of military thought. What follows is a quick search from January through April 2019 to demonstrate how often these focal points appear (this is only a random sampling of a few topics and chapters):

With regard to military art, recent applications of the innovative use of military knowledge include roving mortar tactics,[746] a drone with a 12-gauge automatic carbine to take out flying objects,[747] new artillery tactics,[748] and the use of "tank carousels and Syrian embankments."[749] Also, three of the first four issues of *Military Thought* in 2019 had a section titled "Military Art" and each contained two articles related to the topic.

With regard to asymmetric operations, it was noted that the ideal asymmetric response entails a surprise for a potential adversary that causes him "to radically change the ideology of military-technological developments in a specific area of warfare and to incur costs that exceed ours by an order of magnitude of 1-2."[750]

---

[746] Southern Military District Press Service, "Roving Mortar Tactic Used for First Time in Firings at Dagestan Range," *RIA Novosti*, 17 April 2019.
[747] No author provided, "Russian Scientists Armed a Drone with an Automatic Carbine," *RIA Novosti,* 15 March 2019.
[748] Central Military District Press Release, "New Method of Using Artillery Tested at Central Military District Range Near Chelyabinsk," *Ministry of Defense of the Russian Federation*, 11 April 2019.
[749] Viktor Khudoleyev interview with Andrey Sergeyevich Ivanayev, "The Guardsmen Always Strive To Be the Best. The Servicemen of Western Military District's Guards Combined-Arms Army Came Well-Prepared to the Inspection on the Results of the Winter Training Period," *Krasnaya Zvezda online (Red Star Online*), 17 April 2019.
[750] V. V. Selivanov and Yu. D. Ilyin, "The Methodological Basis for Launching Asymmetric Responses in Military-Technological Battles with a High-Technology Adversary," *Voyennaya Mysl' (Military Thought*), No. 1 2019, p. 22.

With regard to GPS Interference, a Murmansk-BN electronic warfare system is being deployed in Kaliningrad, with the capability to suppress command and control channels within a radius of up to 8,000 km.[751] Cyber and information operations were highlighted in a *Military Thought* article, which emphasized the importance of modernizing over-the-horizon radar stations to become important defensive information weapons.[752]

With regard to satellites, Aleksey Ramm, a popular Russian journalist covering Russian military equipment, noted about the Nudol system that "one can assume the Nudol is capable of combatting not only intercontinental missiles but also satellites, and also manned spacecraft."[753]

With regard to mirror-imaging and stereotyping, Issue 2 in 2019 of the journal *Military Thought* included the article "About the Hybrid Nature of Future Wars and Armed Conflicts." It was about Western use of the term hybrid, not Russia's use of hybrid concepts.

With regard to Gerasimov, his 2019 address to the Academy of Military Science noted that Russia is creating a unified system of reconnaissance and attack means in order to "detect and designate a target and launch precision strikes on critical infrastructure on a near-real time scale with strategic and operative-tactical non-nuclear weapons."[754] His comment on striking critical infrastructure, however, leads one to believe Russia IS making military preparations. One is also reminded that Gerasimov used the term "war" 27 times in his 2019 presentation at the Academy.

Western analysts would be better informed about the content and direction of Russian military thought if more attention was focused on these basic elements. Further, understanding how the various elements of Russian thought could be integrated into an operational design is equally important. For example, Russian authors have stated on several occasions that simultaneous operations are one of the future ways to employ weaponry. Such comments should be followed and considered closely. Simultaneous operations that include several of the elements listed above would cause real problems for forces arrayed against Russia's military. Two such examples (hypothetical) follow.

A Russian reflexive control operation could involve a simple three step process: threaten a specific border with troop deployments; watch the response from the other side of the border, where troops are mobilized in specific locations and numbers (the reflexive response, where forces do something for themselves [shore up their defense] that they are actually doing for Russia [showing Russia what forces they would apply against such a buildup]); and then Russia makes adjustments to its correlation of forces in that specific area in order to have an advantage in numbers and capabilities in case of conflict. That is, a Russian reflexive control operation could be used to make adjustments in peacetime to its correlation for forces.

In another example, when tensions have reached crisis proportions on both sides of a border, international observers watch to see who initiates contact and thus which side is more responsible for starting a conflict. When Russia realizes it has an advantage in force correlations, it could consider sending a fake Russian electronic warfare broadcast that Russian forces were moving

---

[751] No author provided, "Deafening Success: EW System to Cover Europe from Near Kaliningrad," *Izvestiya Online (News Online*), 26 April 2019.
[752] A. A. Tsepelev, "Over-The-Horizon Radar Stations as Russian Defensive Information Weapons," *Voyennaya Mysl' (Military Thought*), No. 1 2019.
[753] Aleksey Ramm, "The Army: The Stars in our Sights: What is Known about the New Antisatellite System. Several Countries Are Working on Counters," *Izvestiya Online (News Online*), 19 April 2019.
[754] No author provided, "Single Military Reconnaissance System Intended for Precision Strikes on Critical Infrastructure," *Interfax* (in English), 2 March 2019.

across the border. If EW interceptors on the other side of the crisis think the intercept is real, they would be forced to move troops to the area and thus begin military operations against Russia "before it was too late." In this case an EW intercept could fool an opposing force into acting first, again using reflexive control, and appearing to the world community that Russia was only responding to a conflict started by the other side.

Such examples indicate that it is important to study and understand the elements of an opponent's thought process and how they might utilize their concepts. Hybrid definitions from a Western perspective usually offer a mix of diplomatic, cyber, economic, nonmilitary, and military issues. There is seldom a Western discussion of military art, the disorganization of a force, the forms and methods of warfare, or a force's reflexive control methodology. That is why it is important to have a common understanding of Russian concepts. It may offer a way to see through the fog of concepts, elements, and even terminology.

A current trend is the focus of many nations on artificial intelligence and quantum computing. Such developments will provoke the development of new forms and methods of fighting, new ways to impose asymmetric methods on an opponent, or new developments in the application of military art or reflexive control. The close study of these issues is where an analyst's attention should be focused if they are to uncover the factors that support military decision-making. Hybrid issues, while important to keep in mind, offer less material for analysts to consider when developing an adversary's specific way of thinking.

Are Civilian and Military Thought Patterns Similar in Russia?

In 2019 British author Keir Giles wrote a book titled *Moscow Rules* that describes Kremlin, not military, thought processes.[755] A few of the similarities between Russian military thought covered in this report and in Giles work (referred to hereafter as Kremlin thought, meaning Russia's civilian leadership) are listed here, along with one or two other sources. The paragraphs that follow first list citations from this work, taken from the material above. It is followed by a Kremlin thought example from either Giles book or another source.

This report noted that Russia's military shot down Malaysian airliner MH-17 and has had its forces in Eastern Ukraine for several years now. Russia's military **created their own alternate realities** (they offered numerous ways the incident occurred, all differing from the unanimous Western analysis) and denied involvement in both instances, even though there was overwhelming evidence (voice intercepts of the airliners downing in the first case, overhead imagery of forces on the ground in the second) from the international community that Russia was indeed the culprit in both cases. Russia has offered close to ten different ways the airliner was downed, each according to a version of its alternate realities. Likewise, in regard to forces in Ukraine, Russia continues to deny the presence of soldiers there unless they are those on vacation who feel like fighting against Ukraine. **Giles** noted that Russia's media creates an **alternative reality** that detaches the nation's leaders from Western rationality. Russia's preoccupation is with a subjective notion of truth.[756] Other authors, some of Russian decent, such as Arkady Ostrovsky, offered the same opinion, that Russia's leaders invent their own reality to fit the situation at hand. Ostrovsky's book index even has an entry with the topic "media" and a subtitle under it of "invents reality."[757]

---

[755] Keir Giles, *Moscow Rules*, Brookings Institution Press/Chatham House, 2019.
[756] Ibid., p. 104.
[757] See, for example, Arkady Ostrovsky, *The Invention of Russia: From Gorbachev's Freedom to Putin's War*, Viking Press, 2015, p. 365.

This report noted that one of the most important Russian military themes is to attain information and situational superiority in the **initial period of war** (IPW). Most analysts think we are in the IPW now. **Giles** states that in 2015 President Putin noted that "Fifty years ago, I learnt one rule in the streets of Leningrad: if a fight is unavoidable, you have to **hit first**."[758] One might expect then that if Putin is confronted with a situation where confrontation is unavoidable, he would be prone to hit first. Whether the means to do so would be nuclear or nonnuclear strategic is unclear, but preparations for the IPW would be crucial to success.

This report noted that Russia's military has several historical issues in common with its **Soviet past**, such as the IPW, deep strikes, and military-political officers. The military has consistently offered their own version of events and battles that transpired during the Great Patriotic War (WW II), even in the face of contradictory accounts and historical revelations, which were deemed not worthy of consideration. **Giles** describes how the Kremlin **politicizes** history for its own use and rewrites chapters for schoolbooks, even in light of new and incontrovertible historical evidence to the contrary. The past lives in the present, which is negotiable and malleable for the authorities, but unchallengeable for everybody else.[759] Both the military and the civilian leadership create alternate realities with historical facts.

This report stated that in the 1990s there were numerous Western efforts to **help Russia's military**, especially with explanations of peacekeeping issues, military insurance, and ways that Congress supports the military (explaining Tricare, the Association of the US Army, etc.). Numerous conferences were held in Russia and in the West with the militaries of both sides present and discussing a host of topics (operations other than war, peacekeeping operations of all types, etc.). **Giles** notes that the **Kremlin was also assisted** by numerous developments in spite of Russia's deflated position in the world in the 1990s. These efforts included giving Russia the seat of the USSR on the United Nations Security Council and membership in the G-8.[760] When Russia was at its weakest, the West tried to help put it back on its feet. These efforts are now lost on the Russian leadership, who view any Western advice or advance as a threat.

This report stated that in a discussion of the new meaning of "war," Chekinov and Bogdanov, two of Russia's premier military analysts, stated that there exists a state of permanent war of this new-type where distinctions between military and peaceful means disappear. The West splits conquered countries into warring parts, creating a "**fifth column**" for themselves to use as necessary.[761] General Staff Chief Gerasimov stated that the Pentagon has a strategy whose essence is the active use of the "protest potential of a **fifth column**," which will destabilize a situation along with the simultaneous delivery of precision-guided missile strikes against important targets.[762] **Giles** states that President Putin has used the same term and warned of "actions by a **fifth column**, a disparate bunch of national traitors."[763] Other Kremlin-directed media reports have discussed the use of influence as a **fifth column**.

This report quoted General Staff Chief Gerasimov on numerous occasions. In one of those presentations to the Academy of Military Science, in 2014, he stressed the importance of his **National Defense Control Center**, from which the Armed Forces are controlled. The **Center** is

---

[758] Giles, p. 54.
[759] Ibid., p. 120.
[760] Ibid., p. 168.
[761] S. G. Chekinov and S. A. Bogdanov, "The Evolution of the Essence and Content of War in the 21st Century," *Voennaya Mysl'* (*Military Thought)*, No. 1 2017, p. 41.
[762] Valery Gerasimov, "Vectors of Development of Military Strategy," *Krasnaya Zvezda (Red Star) Online*, 4 March 2019.
[763] Giles, p. 131.

also, **Giles** adds, a "mechanism for all government ministries coming under the command of that same General Staff in time of crisis."[764] When mobilized, all sectors of the economy and all civilian industry will fall under this establishment.

In **this report** it was noted that Russia's military has continually increased military spending to counter the threat of **containment from the West**. **President Putin** has stated the exact same concern. In his December 2014 address to the Federal Assembly of Russia, he noted that "The **policy of containment** was not invented yesterday. It has been carried out against our country for many years…"[765] There is a Russian term for deterrence that translates as containment, thus containment may be understood in Russia as another deterrence method of use against Russia.

This report has stressed that Russia's military believes in the importance of carefully evaluating a situation and, if necessary, take **calculated risks**. In a 1991 military book, risk was stated to be the highest manifestation of a commander's military skill, experience, endurance, and ability to anticipate.[766] In **a *Foreign Affairs* article** in 2016, in regard to Crimea, President Putin reportedly admitted that he carefully weighed the situation unfolding in Kiev, that Russia conceived an operation that was not well-planned, and that the decision to intervene was a **spontaneous one**.[767] The author of this article, Daniel Treisman, stated that Putin told him this at a reception in Sochi in October 2015.[768] Treisman added that he feels Putin is an improviser, gambler, and **risk-taker**.[769]

This report has noted that Russia has specific terms such as trends, forecasting, correlation of forces calculations, forms and methods, and so on that make **Russian evaluations** of potential confrontations **consistent** in regard to the thought pattern that supports their decision-making. Likewise, **Giles** notes that his book "has argued that there are consistent themes throughout Russian history and social and geographic reality that induce its leaders to act in **consistent way**s when faced with challenges."[770] If that is the case, why haven't Western analysts noted these themes in the past? Most likely it is because of a reliance on stereotyped Western terms.

This small example offers some evidence of similar thought within both the Russian military establishment and the Kremlin. Knowing that Russia's leadership engages in the development of alternate realities and subjective versions of truth, Western statesmen and military officials need to be particularly aware of these cultural proclivities. Otherwise, their best intentions may either go nowhere or be manipulated without their understanding.

On 11 April 2019 three eminent US statesmen, George P. Shultz, William J. Perry, and Sam Nunn wrote an opinion piece on nuclear issues for the *Wall Street Journal*. They noted that the risk of nuclear war is still with us, especially in an age where cyber-attacks can take out nuclear warning and command-and-control systems (recalled here is this report's emphasis on the Russian goal to disorganize C2 capabilities of an opponent). The statesmen offered an approach of three steps: address the US's dysfunctional Russia policy; have Presidents Trump and Putin announce a joint declaration that reaffirms that a nuclear war cannot be won and must never be fought; and have the US and Russia discuss a framework for strategic stability that reflects both the current period of global destabilization and emerging military technologies.

---

[764] Ibid., p. 19.
[765] Ibid., p. 196.
[766] Gaivoronsky and Galkin, p. 19.
[767] Daniel Treisman, "Why Putin Took Crimea," *Foreign Affairs*, May/June 2016, p. 47.
[768] Ibid.
[769] Ibid., p. 53.
[770] Giles, p. 159.

The statesmen called for the US and Russia to work toward a mutual vision for a stable world and to identify tools and policy initiatives to get there. The article ended this way:

> It is essential that we re-engage with Russia in areas of common fundamental interest to both nations, including reducing reliance on nuclear weapons, keeping them out of unstable hands, preventing their use, and ultimately ending them as a threat to the world.[771]

These are sound pronouncements. A few weeks later, on 30 April, the same journal published an editorial from the former President of the Soviet Union, Mikhail Gorbachev. He supported the statesmen's position and added more concern and reasons to fear "the madness of nuclear deterrence." Gorbachev noted that technical, human, or computer error could cause the release of nuclear weapons in spite of deterrence concepts. That is, he was stating that even more needs to be done to place checks on nuclear means in an age when, if launched, the speed of today's hypersonic weaponry may prohibit the weapons recall in the case of an accidental launch.[772]

However, talking and agreeing to forms of strategic stability were more conceivable and doable under Gorbachev, it seems. Negotiators today with less experience must deal with a different Russia and their different understanding of reality. For example, for years now Russia's leaders have derided Western accusations (emanating from nearly every European country) that Russia was engaged in the conduct of cyber-attacks against the infrastructure of these nations. Russia either ignored or rejected these allegations as fantasy. Even when Russian attackers were listed by name and agency, Russia only responded with comments that these accusations were just Western ploys and threats with no substance.

Russia said it would never militarize the Arctic, yet it has done just that. This means the West will have to work harder to negotiate with the Putin regime and the latter's suspicious and near paranoid approach to security issues. The Kremlin and its military appear interested in engaging in risk-taking more often than in the past, since Russia now feels powerful again and looks at the West as being weaker than it was. With risk-taking being the "highest manifestation of a commander's military skill, experience, endurance, and ability to anticipate,"[773] commanders such as Putin and Gerasimov may be looking for places to apply such advantages.

Conclusions

The Russian thought process is a complex mixture of vision, deception, deterrence, outright power, innovative thought, preparation, and the development of alternate realities. Vision and foresight heavily influence Russia's focus on ensuring superiority in the initial period of war. Deception includes reflexive control operations and deterrence measures accomplished through legal, information, demonstration, or other means to contain or scare opponents. Power is found in Russia's military-industrial complex, which produces nuclear and nonstrategic nuclear forces, weapons based on new physical principles, and the capabilities to strike deep into the heart of another nation with cyber capabilities. Innovation is most apparent in new applications of military art and the use of disorganization of an opponent's information and C2 capabilities. Preparation is influenced by the Soviet past and Russian presence, from methods passed down through the years

---

[771] George P. Shultz, William J. Perry, and Sam Nunn, "The Threat of Nuclear War Is Still with Us," *The Wall Street Journal*, 11 April 2019, p. A17.
[772] Mikhail Gorbachev, "The Madness of Nuclear Deterrence," *The Wall Street Journal*, 30 April 2019, p. A17.
[773] Gaivoronsky and Galkin, p. 19.

to today's lessons learned from observing foreign armies in action or from their own experiences. Alternate realities and the rewriting of history provide certain rationales for specific situations.

Applying Western-preferred strategies to Russian thought fails to consider the specific vectors of military thought discussed throughout this report. Without an awareness of these various methods of thought it is impossible to comprehend what Russia is doing to its adversaries and how it is planning present and future operations. An awareness of the concepts and elements that compose Russian military thought will help Western analysts to be better prepared for Russia's rejection of objective reality and refutation of all indicators of its complicity in criminal acts. This includes, in hindsight, Russia's rejection of responsibility for affairs like the MH-17 shootdown, the Skripal poisonings, and cyber-attacks, among others.

Russian military thought is based on traditional building blocks. It is also contemplative and interactive with the unfolding technical-based environment before it. Closely following trends and constantly updating forecasts keep the military informed and able to meet new challenges. When specific capabilities are required to confront specific threats to Russia's security, forms and methods are developed to provide the organizations and techniques required, to include the sequencing of events and operational design for successful outcomes.

Overall, Russia's methodology, its wording, particular focus, and the rationale behind its actions differ from military thought in the West. Russia will use many of the items listed in this report to better prepare for its confrontations with future opponents, and hopefully the West will not be one of them. However, it is wise to closely study and consider Russian thought "just in case."

Appendix A Russian Asymmetric Thought and Disorganization

This appendix has three Attachments (1) a short history of the use of the term "asymmetry." (2) an expanded definition of asymmetry. (3) an extended definition of disorganization.

A.1 Attachment One: A Short History of the Use of the Term "Asymmetry"

This section will utilize a bullet format to offer a list of Russian military experts discussing asymmetric actions from 1998-2007.

- 1998: Colonel Sergey Modestov noted that when defending Russia, the nation must seek "optimal forms and means of conducting asymmetrical defensive actions in defending one's own information resource."[774]
- 1999: Major General I. G. Korotchenko, Chair of Military Art at the General Staff Academy, stated that Russia must "depart from the principle of opposing force with force and move to the principle of asymmetrical responses…"[775]
- 1999: Russian Defense Minister, Marshal Igor Sergeyev, stated that the Armed Forces should seek "compensation for avoiding direct military-technical competition with the most developed countries by means of creating 'asymmetrical' means for armed conflict, allowing for the destruction of the most vulnerable functional elements of the main systems and key targets of the enemy's infrastructure…"[776]
- 2000: Russian officers noted that Western European nuclear power plant concentrations were greater than in Russia's European sector, a target density rich asymmetry that Russia could threaten with severe consequences. It simplifies sufficiency calculations for Russia's non-strategic forces.[777]
- 2001: State Duma Deputy Andrey Kokoshin noted that Russia's asymmetric approach to US President Ronald Reagan's strategic defense initiative was "based on who is cleverer, not on the one who makes more iron."[778]
- 2001: Vladimir Slipchenko, responding to the US withdrawal from the ABM treaty, noted that Russia's asymmetric response must include renewed route patrolling by rail-based Topol ICBMs; lifting restrictions under Strategic Arms Reduction Treaty 1 (START 1); relying more on TOPOL-M complexes; and potentially withdrawing from the 1987 INF treaty.[779]
- 2002: Journalist Mikhail Lavrov noted that President Putin, preparing for a US visit in 2001, stated in regard to asymmetry that if the US builds a national

[774] Sergey Modestov, "A Concept for Deep Defense in Information Warfare," *Information Security of Russia*, Moscow 1998, pp. 154-158, paper obtained by the author in Moscow in 1998.
[775] I. G. Korotchenko, "Tendencies in the Modern Development of Military Art," *Military Thought*, No. 1 1999, p. 11.
[776] I. D. Sergeyev, "The Main Factors Which Determine Russia's Military-Technical Policy on the Eve of the 21st Century," *Red Star*, No. 259, 9 December 1999 downloaded from Eastview.com on 18 March 2010.
[777] E. N. Akhmerov, N. F. Kravchenko, and I. I. Sobchenko, "On the Direction of Regional Nuclear Deterrence," *Military Thought*, No. 4 2000.
[778] No author or title provided, *Interfax* (in English), 25 August 2001.
[779] Vladimir Slipchenko, "Missile Defense Again?" *Army Journal*, No. 12 December 2001.

missile defense system, Russia may return to placing multiple reentry vehicles on its ICBMs in place of single warheads.[780]

- 2003: General of the Army Makhmut Gareyev, President of the Academy of Military Science, stated that future warfare would now be more flexible, using more means and methods, including non-military and non-traditional ones. He added that the correlation between direct and indirect actions have changed. The latter involves the extended us of political, economic, and moral-psychological impact on an enemy, designed to supply it with disinformation and undermine its will to fight.[781] [While not using the term asymmetric, he instead uses the terms indirect and non-military.]
- 2004: Retired Major General Vladimir Belous noted that studies show how asymmetric measures are preferable in terms of cost-effectiveness. He offered three missile defense countermeasures: improving strategic offensive arms (such as the capability to maneuver in the boost phase); developing new methods of employing these arms (use of shallow trajectories or decoys); or finding new means and methods of delivering strikes against enemy missile defense system facilities (such as blinding reconnaissance systems).[782]
- 2004: A report noted that a high-ranking Defense Ministry spokesman stated that an asymmetric and state-of-the-art technical system has been developed in Moscow. The Kremlin is thereby not afraid of Western missile defense forces. The weapon's existence will drive down antimissile prices and contracts as well.[783]
- 2005: Colonel Raskin noted that asymmetric war is waged by nonmilitary forms of violence and there is wide use of psychological, environmental, economic and biological effect on an individual state.[784]
- 2005: General of the Army Gareyev wrote that when warfare is conducted against a technologically superior enemy, emphasis must be placed on developing electronic warfare assets and "other cheaper asymmetric means of armed combat" with scenarios and plans that reflect the peculiarities of modern warfare.[785]
- 2006: Colonel Manachinskiy noted that tactics are sometimes based on the resources a side can afford. The weak look for weaknesses in the defense of the strong, much like the battle between David and Goliath. Today that trend is toward insurgent warfare. There may also be an asymmetrical capability of countries to achieve society's mobilization to wage insurgent warfare.[786]
- 2007: Former Russian Security Council Secretary Andrey Kokoshin noted that asymmetric measures will ensure strategic stability, and they should include

---

[780] Mikhail Lavrov, "Asymmetric Strike by the Nuclear Shield," *Prescenter.ru WWW-Text*, 13 March 2002.
[781] M. A. Gareyev, "On Several Characteristic Traits of Future War," *Military Thought*, No. 6 2003, p. 56.
[782] Vladimir Belous, "This Is What I Think: The Answering Move: How Can the American 'Star Wars' be Nullified?" *Labor*, 22 December 2004.
[783] No author listed, "End of the Symmetric World," *Gazeta.ru WWW-Text*, 29 March 2004.
[784] Aleksandr Raskin, "Are Net 'Battles' Coming? We Continue the Discussion on the Nature and Look of Possible Future Wars," *Army Journal*, No. 9 2005, pp. 20-22.
[785] No author or title provided, *Military News Agency*, 16 March 2005.
[786] Aleksandr Manachinskiy, "When the Weak Defeat the Strong. Asymmetrical Wars Are One of the Realities of the Present Day," *Independent Military Review*, 22 December 2006.

technological, operational-strategic and operational-tactical solutions. Russia will not do what the other side is doing but will follow its own path.[787]

- 2007: Mikhail Rastopshin stated that the Topol-M ICBM with maneuverable reentry vehicles is the current asymmetric response to US intrigues. He added that the concept of asymmetry "consists in abandoning a direct counterforce standoff with the militarily developed states by exposing and exploiting the existing vulnerabilities of a potential adversary's current and new armament."[788]

A.2 Attachment Two: An Expanded Definitions of Asymmetry[789]

Asymmetric Operations (Асимметричные действия) – a strategy of struggle by a weak side against a strong one.

In international relations of recent years, the concept of asymmetry is employed most often for the characteristics of conflict between enemies that are unequal with respect to economic development and the level of military force. Asymmetry in international relations attests, as a rule, to their paradoxical nature, when a weak enemy is capable of inflicting serious damage and even imposing his will on a stronger entity, while the latter, despite what would seem to be a clear advantage, cannot always uphold his own interests and subordinates them to the former.

An analysis of the actions of the opposing sides in partisan warfare during different time periods and under conditions of occupation and colonial government and in the course of national liberation movements provided a basis for political scientists and military specialists to assign them to the category of asymmetric actions already in the 1960s. Having identified the coinciding forms and methods of this confrontation in these conflicts, several principal features of asymmetric operations can be determined:

- Unpredictability of the outcome of fighting when there is a clear disproportion of the correlation of forces, means, and capabilities of the side
- Weak side's use of the strategy of seeking the weaknesses of the strong side and its employment of prohibited means of conducting armed struggle and indirect military operation
- Inability of the strong side to uphold his positions or reliably suppress the troops (forces) of a weak enemy

In the majority of such wars (armed conflicts) a weak enemy is incapable of winning a military victory over a strong one. He can, however, as a rule, succeed in dictating the course and content of military operations that are advantageous for himself. In other words, **the use of asymmetric operations often makes it possible for a weak enemy to achieve a political victory**, for the sake of which force, from the point of view of the classical definition of war, is being employed.

Asymmetric Confrontation in Network-Centric Warfare

---

[787] No author or title provided, *Military News Agency* (in English), 13 February 2007.
[788] Mikhail Mikhaylovich Rastopshin, "In the Labyrinth of Asymmetric Responses," *Independent Military Review*, No. 17, 1 June 2007, p. 6, as downloaded from Eastview.com on 17 March 2010.
[789] The "asymmetric operations" definition is from N. N. Tyutyunnikov, *Military Thought in Terms and Definitions, Volume One*, 2018, page 29; and the rest of the asymmetric definitions are from N. N. Tyutyunnikov, *Military Thought in Terms and Definitions, Volume Three*, pages 222-224. The disorganization pages are from N. N. Tyutyunnikov, *Military Thought in Terms and Definitions, Volume One*, 2018, pages 319-320.

- **Asymmetric Threats** (асимметричные угрозы) – the use of the factor of surprise in all its operational and strategic dimensions; the use of weapons by methods that are not planned by the US.
- **Asymmetry** (асимметричность) – countering an enemy in seizing the fire and tactical initiative, preempting him in actions according to the principle "first to recon – first to strike"; employing long- and short-range UAVs throughout the entire depth of the enemy deployment, pairing the actions of means of destruction with reconnaissance-information support systems; employing small recce-strike UAVs, ground recce-strike complexes, and robots; outstripping the enemy's intelligence cycle; employing "network" principles of weapons control; employing energy strikes and weapons based on new physical principles in combination with employing short- and long-range weapons with optic, laser, and radar navigation systems; ensuring dynamism of combat operations in all spheres – on land, in the air, and in the information domain; keeping the enemy constantly stressed; meeting the requirement of a 3-7-fold increase in the depth of information-energy effects against the enemy and 1.5-2-fold increase in the intensity of delivery of a fire strike.

Asymmetric direction of development of weapons and military and special equipment (VVST) under conditions of conducting network-centric warfare (ассиметричное направление развития ВВСТ в условиях ведения сетецентрической войны) – the creation of models that provide short-term effects with the disabling of enemy resources for a specific period of time, and a sudden failure to reproduce enemy network-centric systems, with a shift to "hand" command and control at the tactical level, up to a battalion.

Trends in the development of effective means for countering a probable enemy in network-centric warfare include areas enumerated below.

In the field of **layout solutions** (компоновочные решения) it is necessary to create models:

- That have the ability to distribute properties (functions) across individual elements in their make-up (subsystems, machines)
- That make it possible to form not a linear, but rather a planar order of battle on a sufficiently large area (a "combat swarm")
- That have reduced weight and size characteristics, with the aim of increasing the number of enemy targets

In the field of **improving destructive and suppressive power**, it is necessary to develop resources that provide for:

- Destruction of an air enemy over his own territory—fixed (mobile) air defense resources; UAVs operating against cruise missiles (Roc); tactical weapons of mass destruction at the brigade (battalion, company) level (super low altitude air blast munitions);
- Effects against enemy territory (infrastructure)—fixed (mobile) artillery resources; heavy strike UAVs; tactical weapons of mass destruction at the brigade (battalion, company) level; struggle against enemy network-centric command and control. i.e., the creation of barrier electromagnetic lines with munitions that generate electromagnetic waves over a broad range, e.g., electromagnetic field mines or models for firing rockets designated for dispersing combat elements and aggressive materials or products.

In the field of **protection**, it is necessary to develop resources for the following:

- Protection of subunits based on new physical principles (beam, accelerating "umbrellas" over one's own forces and means);
- Creation of electronic models of VVST;
- Aerosol counteraction that makes it possible to "enwrap" subunits as a whole, up to and including a company;
- "Active" defense—super small rockets and missiles to struggle against enemy mini- and micro-structures; surfaces with "active" protection capable of countering enemy penetration resources or destroying such resources; "guard" mini-, micro-, and nano-robots for the most varied operational habitats, including space, the surrounding environment, and even an organism's cells; flying mine fields on a UAV basis.

In the field of **mobility**, it is necessary to develop resources:

- That operate in three-dimensional space (3D-defense);
- For the dynamic regrouping of models when there is a danger of destruction of the area on which they are located;
- To support defensive maneuvering.

Within the framework of **the organization of command and control** according to the network-centric principle, in the future it will be necessary to create and introduce resources to support the procedure of collective formulation and decision-making, as well as algorithms for representing information in the form of visually oriented dynamic models of the problem being solved, making it possible to enlist the intuitive capabilities and associative thinking of people in the resolution of tasks. This process of reconnaissance-information support turns each combat resource into an information-strike (fire) complex. Here, the disabling of a command post may not affect the combat stability of a military formation for a much longer time, inasmuch as the network-centric principle of information interaction of the executive elements makes it possible for them to maintain the system properties of the force grouping for quite a long period. This is especially important under contemporary conditions, where the ability to disorganize the command and control system has considerably increased. To implement this concept each combat resource should be equipped with a special set of digital resources, including resources for processing information, a navigation system receiver, an ultra-short-wave radio, and radio resources of an automated system for determining location, identification, and data transmission.

A.3 Attachment Three: An Extended Definition of Disorganization

- **Complication of Command and Control** (затруднение управления) – the degree of disorganization of command and control in which information exchange is reduced at different levels of command and control and the centralized operation of the command and control system is disrupted. Loss of command and control of troops does not occur.
- **Disorganization of enemy command and control of troops and weapons** (дезорганизация управления войсками и оружием противника) – the totality of coordinated measures and actions aimed at the substantial reduction of the capabilities or full cessation of the function of his [the enemy's] organs and technical resources of command and control of troops and weapons.

The goal of disorganization of enemy command and control of troops and weapons is depriving him of the ability to organizationally and effectively accomplish combat tasks using his troops and weapons.

The targets of effects when disorganizing enemy command and control of troops and weapons are officials of command and control organs, first and foremost, decision-makers; command posts; resources for obtaining situational information (intelligence resources, resources for covering the situation); automated command and control systems; resources for processing, storing, and displaying information, with their software and information resources; resources for transmitting information (communications [data exchange] resources); telecommunications channels (communications channels, data exchange channels).

- **Fragmentation** (фрагментация) – the basic method for disorganizing command and control. It consists of excluding from the command and control process at a specific stage those elements of the information-command and control system without which, under conditions of a changing operational situation, the development of appropriate command and control actions, their communication, and their implementation are impossible.

Appendix B Russia's Classification of Contemporary Military Conflicts

Outline of the "Basis of Domestic [Russian Federation] Classification of Contemporary Military Conflicts"[790] (Russian version is followed by the English translation of each "number" below).

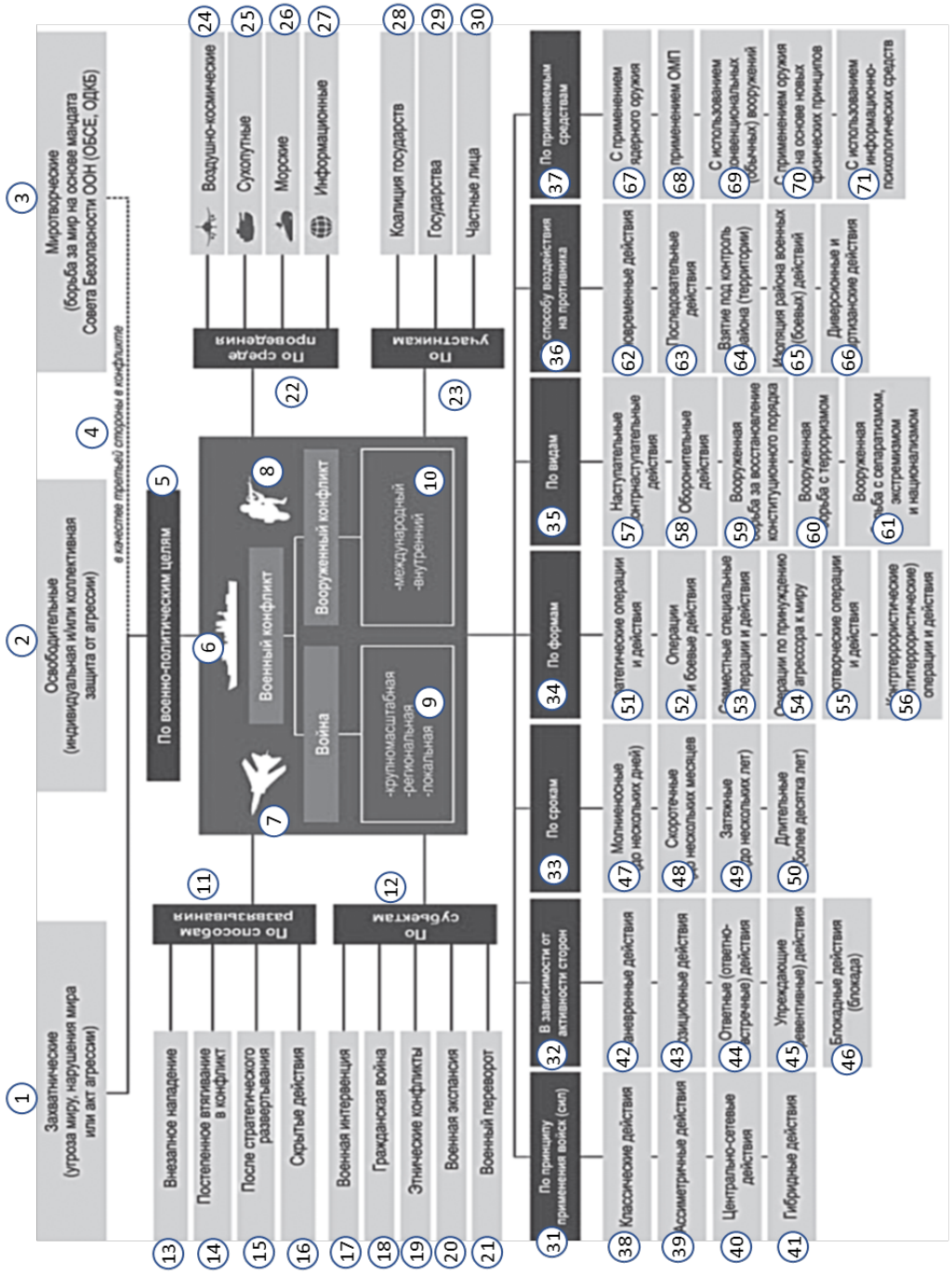


Рис. 2. Основы отечественной классификации современных военных конфликтов

[790] O. M. Gorshechnikov, A. I. Malyshev, and Iu. F. Pivovarov, "Problems of the Typology of Contemporary Wars and Armed Conflicts," *Journal of the Academy of Military Science*, No 1. 2017, p. 53.

Basis of Domestic [RF] Classification of Contemporary Military Conflicts

1. Aggressive (threat to peace, violation of peace, act of aggression)
2. Liberation (individual and/or collective defense against aggression)
3. Peacekeeping (struggle for peace on the basis of a mandate from the UN Security Council, OSCE, CTSO
4. As a third side in a conflict
5. With respect to military-political goals
6. Military conflict
7. War
8. Armed conflict
9. Large scale; regional; local
10. International; internal
11. With respect to method of unleashing
12. With respect to subjects
13. Surprise attack
14. Gradual involvement in conflict
15. After strategic deployment
16. Covert operations
17. Military intervention
18. Civil war
19. Ethnic conflicts
20. Military expansion
21. Military coup
22. With respect to medium of conduct
23. With respect to participants
24. Aerospace
25. Ground
26. Naval
27. Information
28. Coalition
29. States
30. Private persons
31. With respect to principle of employment of forces
32. Dependent on dynamism of the sides
33. With respect to duration
34. With respect to forms
35. With respect to types
36. With respect to method of pressure on the enemy
37. With respect to the resources employed
38. Classical operations
39. Asymmetric operations
40. Network-centric operations

41. Hybrid operations
42. Maneuver operations
43. Positional operations
44. Retaliatory (retaliatory-meeting) operations
45. Preemptive (preventative) operations
46. Blockade operations
47. Blitzkrieg (up to several days)
48. Fast-moving (up to several months)
49. Protracted (up to several years)
50. Long (more than ten years)
51. Strategic operations and actions
52. Operations and combat operations
53. Joint special operations and actions
54. Operations to force peace on the aggressor
55. Peacekeeping operations and actions
56. Counterterrorist (antiterrorist) operations and actions
57. Offensive (counteroffensive) operations
58. Defensive operations
59. Armed struggle to reestablish constitutional order
60. Armed struggle against terrorism
61. Armed struggle against separatism, extremism, and nationalism
62. Simultaneous operations
63. Successive operations
64. Taking a region (territory) under control
65. Isolation of a region of military (combat) operations
66. Sabotage and partisan operations
67. With the employment of nuclear weapons
68. With the employment of WMD
69. With the use of conventional weapons
70. With the employment of weapons based on new physical principles
71. With the use of information and psychological resources

This page intentionally left blank.

Appendix C Acronyms

Term	Definition
4GW	Fourth-Generation War
A2AD	Anti-Access Aerial Denial
ABM	Anti-Ballistic Missile
AMS	Academy of Military Science
ASAT	Anti-Satellite
AVN	Journal of the Academy of Military Science
C2	Command and Control
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance
CIS	Commonwealth of Independent States
COF	Correlation of Forces
CV	Information Space
DIA	Defense Intelligence Agency
EW	Electronic Warfare
FSB	Federal Security Service
GPS	Global Positioning System
GPW	Great Patriotic War (or WW II)
GRU	Russian Military Intelligence Service
GSA	General Staff Academy
GURLS	Main Directorate for Personnel Work
GVPU	Main Military-Political Directorate
IAG	Illegal Armed Groups
ICBM	Intercontinental Ballistic Missile
INF	Intermediate-Range Nuclear Forces Treaty
IPW	Initial Period of War
IT	information technology
IW	Information Warfare
KGB	Committee for State Security
LED	Light-Emitting Diode
MISO	Military Information Support Operations
MLRS	Multi Launch Rocket System
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NPP	new physical principles
PGM	Precision-Guided Munitions
PMIK	Mobile Multifunction Information Systems
RC	Reflexive Control
REB	Radio-Electronic Warfare
RT	Russia Today
SODCIT	Special Operations To Destroy Critical Infrastructure Targets
START	Strategic Arms Reduction Treaty
SZS	Protected Communication System (Sistema Zashchishchennykh Svyazey)

Term	Definition
TO&E	Table of Organization and Equipment
TVD	Theaters of Military Operations
UAV	Unmanned aerial vehicles
UN	United Nations
VKS	Aerospace Forces
VM	Military Thought
VVST	Weapons and Military and Special Equipment
ZSPD	Classified Data Transmission Segment

ABOUT THE AUTHOR

Mr. Timothy L. Thomas (BS, Engineering Science, USMA; MA, International Relations, University of Southern California) is an analyst for the MITRE Corporation, a Federally Funded Research Development Center. Mr. Thomas has conducted extensive research and publishing in the areas of peacekeeping, information operations and war, future war, psychological operations, Russian military thought, forecasting, strategy, and political-military affairs. He was a US Army foreign area officer who specialized in Soviet/Russian studies. His military assignments included serving as an analyst at the Soviet Army Studies Office (SASO) and its follow-on, the Foreign Military Studies Office (FMSO); as the Director of Soviet Studies at the United States Army Russian Institute in Garmisch, Germany; as an inspector of Soviet tactical operations under the Organization for Security and Cooperation in Europe; and as a brigade S-2 and company commander in the 82nd Airborne Division. Before working for MITRE, Mr. Thomas authored three studies on Russia's military while working for FMSO (*Recasting the Red Star, Military Strategy, and Kremlin Kontrol*). He and his wife Christine currently live in Moseley, Virginia.