

National Defence University

Department of Warfare

Series 2: Research Reports No. 19

Russian Concept of War, Management and Use of Military Power

Conceptual Change

Pentti Forsström (ed.)



Finnish National Defence University

Russia Seminar 2022

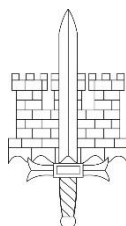


MAANPUOLUSTUSKORKEAKOULU
SOTATAIDON LAITOS
JULKAISUSARJA 2: TUTKIMUSSELOSTEITA NRO 19

NATIONAL DEFENCE UNIVERSITY
DEPARTMENT OF WARFARE
SERIES 2: RESEARCH REPORTS NO. 19

**RUSSIAN CONCEPT OF WAR,
MANAGEMENT AND USE OF MILITARY POWER
– CONCEPTUAL CHANGE**

PENTTI FORSSTRÖM (ED.)



NATIONAL DEFENCE UNIVERSITY
DEPARTMENT OF WARFARE
HELSINKI 2022

Pentti Forsström (ed): *Russian Concept of War, Management and Use of Military Power – Conceptual Change*

Maanpuolustuskorkeakoulu

Sotataidon laitos

Julkaisusarja 2: Tutkimuseloiteita nro 19

National Defence University

Department of Warfare

Series 2: Research Reports No. 19

Editor:

Pentti Forsström

Writers/speakers:

Dima Adamsky, Justin Bronk, Pentti Forsström, Lester W. Grau, Oscar Jonsson, Michael Kofman, Santeri Kytöneva, Aristide LaVey, Leonid Nersisyan, Rod Thornton with Marina Miron, Jyrki Terva, Jukka Viitaniemi, Juha Wihersaari

Recent publications in PDF format: <http://www.doria.fi/handle/10024/73990>

Cover image: FNDU

Pictures and illustrations: Authors

© FNDU & Authors

ISBN 978-951-25-3287-2 (pbk.)

ISBN 978-951-25-3288-9 (pdf)

ISSN 2343-5275 (print)

ISSN 2343-5283 (web)

Maanpuolustuskorkeakoulu – Sotataidon laitos

National Defence University – Department of Warfare



This work is licensed under the Creative Commons BY-NC 4.0 International License. To view a copy of the CC BY-NC 4.0 license, visit <https://creativecommons.org/licenses/by-nc/4.0/deed.en>

PunaMusta Oy
Joensuu 2022
Finland



CONTENTS

Klaus Ilmonen

SPEECH BY MANAGING DIRECTOR OF THE MANNERHEIM FOUNDATION ON THE EVE OF THE SEMINAR.....	iii
--	-----

Pentti Forsström

1. INTRODUCTION TO THE PUBLICATION	1
--	---

Pentti Forsström

2. INTERPRETATIONS ON THE DEVELOPMENT OF THE RUSSIAN CONCEPT OF WAR.....	4
---	---

Dima Adamsky

3. COMMAND AND CONTROL CULTURE À LA RusSE.....	14
--	----

Leonid Nersisyan

4. NEW RUSSIAN STRATEGIC WEAPONS AND MISSILE DEFENCE SYSTEMS – CHANGE OF THE BALANCE?.....	16
---	----

Jukka Viitaniemi

5. STRATEGIC ACTIONS OF THE ARMED FORCES – CONCEPTUAL ANALYSIS	25
---	----

Jyrki Terva

6. SCHRÖDINGERS CAT IN EASTERN UKRAINE – HOW RUSSIA’S WAR IN UKRAINE CREATES AND DESCRIBES NEW RUSSIA-WEST CONFLICT	32
--	----

Juha Wihersaari

7. EVGENY MESSNER’S THEORY OF SUBVERSION WAR VS. HYBRID WARFARE.....	33
---	----

Oscar Jonsson (and Bryce Johnston - absent from the seminar)

8. RUSSIA’S REVOLUTION IN INTELLIGENCE AFFAIRS.....	43
---	----

Rod Thornton and Marina Miron

9. INTERFACE BETWEEN ARTIFICIAL INTELLIGENCE AND CYBER. CREATING REVOLUTION IN MILITARY AFFAIRS? THE RUSSIAN MILITARY’S UTILISATION OF ARTIFICIAL INTELLIGENCE TO ENHANCE ITS CYBER OPERATIONS: THE CURRENT STATE OF PLAY	62
--	----

Jonna Alava

10. REPRESENTATIONS OF WOMEN SOLDIERS IN RUSSIAN ARMED FORCES 2008–2021.....	72
---	----

Aristide M. LaVey

11. ADMIRAL USHAKOV: A STUDY OF RUSSIAN POWER PROJECTION	73
--	----

Santeri Kytöneva

12. JUSTIFYING THE USE OF FORCE: RUSSIA’S SPIRITUAL AND NATIONAL SECURITY	81
--	----

Justin Bronk

13. DEVELOPMENTS IN RUSSIAN COMBAT AIR SPENDING AND LIKELY
OPERATIONAL IMPLICATIONS..... 89

Lester W. Grau (and Charles K. Bartles)

14. RUSSIAN MANEUVER DEFENCE AND THEIR CONCEPT OF THE
FRAGMENTED BATTLEFIELD 102

Michael Kofman

15. ON PRESENT WAR IN UKRAINE - KEYNOTE 2..... 112

CONTRIBUTORS..... 115

SPEECH BY MANAGING DIRECTOR OF THE MANNERHEIM FOUNDATION ON THE EVE OF THE SEMINAR

Klaus Ilmonen

I am very happy to welcome you all to the Mannerheim-Museum on behalf of the Mannerheim-Foundation.

The foundation manages the estate of the Marshal of Finland and, in line with his will, primarily supports participation in international post graduate programs for Finnish officers. The foundation also owns and manages the Mannerheim-museum.

Marshal Mannerheim had a long military career in service of the Russian Empire before Finnish independence and developed a deep understanding of Russia, which helped him guide Finland through difficult times. We feel that developing deeper understanding of Russian politics and security fits very well with the goals and values of the foundation. The foundation has been very pleased to have the opportunity to support the establishment of the Chair in Russian security policy and has continued to follow and support related research initiatives - including the current conference.

We are very happy that the conference has attracted leading scholars in the field and that we can join forces to better understand the security dynamics of our neighbour and the region. It must be satisfying for a scholar that the importance of one's subject of research is widely recognized and is at the centre of public interest – in the case of Russian security policy there may be another side to the coin, however, and one would prefer the subject matter to be far less topical than it is today. Nevertheless, understanding the drivers underlying Russian policy is paramount for developing our own policies and increasing the prospects of peace and security.

Maybe a very brief reflection is allowed on the status of Finnish debate on Russian security matters for our foreign guests. These have traditionally been uncomfortable subject matters for political leaders, but it has been observed that the debate is generally becoming healthier than before. There has been some discussion again around the concept of Finlandization. The mere mention of the term has been against official policy in past decades, but I have a sense that this time around there has been a better recognition than earlier of the full scope of what this concept has entailed for Finland and a readiness to challenge former narratives in domestic politics. There has also been a clear change in how our political leadership communicates in matters related to Russia and security. The president of the Republic, Sauli Niinistö, has publicly referred to an obscure proverb that “Cossacks will take everything that is not firmly tied-up”. This actually accurately describes current Finnish policy and provides concrete guidance for keeping one's house in order to increase one's security – a position much changed from past days.

As a final observation it can be noted that we are in the middle of the Olympic season with recent national successes. One would hope nations would focus on competing on sports arenas rather than elsewhere. However, there appears to be an established Russian practice not quite in the spirit of the games to start mayhem in connection with Olympic Games – in Georgia in 2008 at the start of the Beijing Olympics and in Crimea in 2014 during the Sochi Olympics. In this respect there is a more ominous

proverb used in Finland: “There is no two without a third”. We are all keeping close watch on the geopolitical situation throughout the Olympic Games and will continue do so thereafter as well.

I welcome you again to our museum and also wish you all a successful conference and valuable discussions on indeed very topical matters tomorrow at the conference and also during the course of this evening.

Klaus Ilmonen, LL.D.

Managing director of the Mannerheim Foundation

1

INTRODUCTION TO THE PUBLICATION

Pentti Forsström

This publication consists primarily of articles presented in the annual Russia Seminar 2022 organised by the Department of warfare of the Finnish National Defence University (FNDU) and titled as “Russian Concept of War, Management and Use of Military Power – Conceptual Change”. The aim of the Seminar was to raise a discussion on Russian military policy and military power. The focus of the seminar was on the Russian concept of ”war” – that is – the use of lethal military force in order to achieve certain political objectives. It should be noted that the publication is not an exhaustive presentation of all the aspects related to the concept of war. This leaves room for themes and questions to be researched also in the future.

The use of force is one of the two main functions of the Russian military power, the other one being deterrence, which was discussed at the Russia seminar 2021¹. The objective of deterrence is to influence the consciousness of the adversary - to change adversary’s behaviour and make it relinquish possible ideas of aggression or threat to use military power against Russia. In the 2021 seminar the main emphasis was on the military aspects and prerequisites of preventing a war.

As we know now, at the time of writing these lines, in May-June 2022 – these aspects and methods of deterrence conducted by Russia and its military during the past year were not only aimed at preventing war, but also, they were actual preparations for a war. Furthermore, despite the fact that these means and capabilities were partly escalatory and threatening by nature, they did not enable Russia to achieve its political, military-political or military objectives. Regarding Ukraine, or more broadly the security structure of Europe, they were set by Russia, perhaps, intentionally on a level which was clearly unacceptable. In this manner Russia could justify to Russian people – after the launch of the operation – that there is no other solution than to conduct “a special military operation” in Ukraine.

In this introductory chapter I will briefly introduce the articles or presentations of this report which were contributed in the seminar. All the presentations and discussion can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s>.

D.Mil.Sc., Lt. Col. (ret.) **Pentti Forsström** in his keynote presentation explores the Russian definition of war and its conceptual changes in Russian military thought. Forsström also focuses on the Russian perception of war through structure, nature, and orientation. One result of this is that the geopolitical changes and limitations in military power have forced Russia to implement different means in safeguarding its

¹ See: Pentti Forsström (Ed.) 2021: Russian Concept of Deterrence in Contemporary and Classic Perspective, National Defence University, Department of Warfare, Series 2: Research Reports No. 11. The permanent address of the publication: <https://urn.fi/URN:ISBN:978-951-25-3250-6>.

military security compared to the Soviet idea of strategic echelons of conventional armed forces.

Professor **Dimitry Adamsky** presents an in-depth analysis on possible changes in the way how Russia implements the elements of mission command within its ranks. The key notions in professor Adamsky's presentation revolve around the questions of how much Russian command and control is shifting from the traditional Soviet-style inflexible way of troop command to more adaptive means and ways of practicing C2 on the future battlefields.

Military Analyst **Leonid Nersisyan** discusses Russian strategic weapons and missile defence systems on the notion of how much these aforementioned systems will change the balance between Russia and NATO. Nersisyan argues that although Russia is investing considerable number of resources in the research and development of the weapon systems in question, the proliferation of new strategic weapons and missile systems will not change the balance of power but will provide more political leverage in interstate relations.

M.Mil.Sc, PhD Researcher, Major (ret.) **Jukka Viitaniemi** in his presentation clarifies the key concepts of Strategic Actions of Armed Forces. The main argument of Viitaniemi is that in order to better understand Russian way of strategic scale operations, the western audience should learn the key concepts and their definitions.

PhD Researcher **Jyrki Terva** in his presentation operationalises the quantum approach to international relations theory and analyses the relation between the West and Russia. Terva focuses on the main fracture points in the conflict especially in the shade of key events in Ukraine after 2014 and the formularisation of Minsk treaties. He expands on the idea that treaties have become the Schrödingers cat in a box, meaning that it appears different depending on the perspective in question.

PhD Researcher, Colonel (ret.) **Juha Wihersaari** presents on the topic of Messner's theory of the subversion war and the Russian hybrid war. Wihersaari's definition on Russian hybrid war combines different sources on the topic. His findings on similarities and differences between Messner's theory and Russian hybrid war lead to the conclusion that these two concepts can be seen as closely related to each other.

Dr. **Oscar Jonsson** presents an overview to the topic of Russian intelligence from the perspective of artificial intelligence. In his article "*Russia's Revolution in Intelligence Affairs: From natural stupidity to Artificial Intelligence*", Jonsson argues that emerging innovations in the fields of machine learning and AI-tools will force changes in the way intelligence is conducted. The author concludes that the debate on artificial intelligence in military affairs should include more elements of intelligence processes instead of emphasizing solely autonomic weapon systems.

Dr. **Rod Thornton** and Dr. **Marina Miron** in their research explore the current situation of how the Russian military utilises Artificial Intelligence (AI) to enhance its offensive cyber operations. Researchers discuss the reasons at the strategic level on why Russia is emphasising the development of AI to enhance its offensive cyber capability. In the end of the chapter there are considerations on the effects of the Russian invasion of Ukraine on the military's ability to deploy AI in weapons systems and technologies.

PhD Researcher **Jonna Alava** in her presentation analyses the representations of Russian women soldiers in the contemporary setting. She argues that key functions of the representations are to morally support male soldiers, legitimise warfare and produce a female workforce for mainly auxiliary tasks in the military.

Independent Researcher **Aristide M. LaVey** in his chapter presents his research on the topic of visual information and cultural power projection. The focus of the presentation is on the spiritual power projection via the personage of the naval saint Adm. Fedor Fedorovich Ushakov. Lavey argues that in order to understand the religious dimension of patriotism, the Western audience should familiarise with Ushakov's role in Russian military-religious culture.

Research Intern **Santeri Kytöneva** (FNDU) presents the results of research conducted on Mahkmut Gareev's usage of the concept of spiritual security, concluding that Gareev sees the phenomena as an important part of national security with growing importance in the future. Kytöneva evaluates the implications in the shade of Russia's recent strategic planning documents. In addition, Russian military theorists' views are categorised on the issues of state security, closely related to spiritual security. Finally, new venues for research on the topic of justifying the use of force are considered.

Senior Research Fellow **Justin Bronk** (RUSI) provides in his presentation "*Developments in Russian combat air spending and likely operational implications*" a pervasive insight into the Russian Air Force's (VKS) aircraft procurement and considers how these new capabilities will change the way Russia engages against its perceived adversaries. Bronk argues that despite the fact that Russia pursues to highlight the existence of emerging weapon systems, its primary focus will remain in updating the existing capabilities.

Dr. **Lester W. Grau** (and Dr. **Charles K. Bartles**)² examine in their presentation the concept of Russian maneuver defense and the concept of fragmented battlefield. Maneuver defense differs totally from the Western Corps-level concept of mobile defense. Researchers are giving an in-depth analysis of Russian concept of fragmented battlefield in defence and in attack. One conclusion is that improvements in technology have made the potential future battlefield more deadly and fragmented. Russia is currently looking at adjusting tactics to fight effectively and survive on the future battlefield.

Michael Kofman concentrates in his keynote speech on his views on the situation and the current (16 Feb 2022) crisis between Russian and Ukraine practically on the eve of the Russian "special military operation" in Ukraine. His perception was that a principal decision might have been made by the Russian political leadership on the use of military force.

² This article was first published in *Infantry* in Fall 2021 as "Russian Future Combat on a Fragmented Battlefield" by Lester W. Grau and Charles K. Bartles. It has been modified for presentation and publication by the National Defence University of Finland.

2

INTERPRETATIONS ON THE DEVELOPMENT OF THE RUSSIAN CONCEPT OF WAR

Pentti Forsström

The presentation made by Pentti Forsström in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 20:00.

Introduction

When planning the themes of the Russia seminars in the spring of 2019, we thought that the theme for 2020 would be “The Deterrence” and for 2021 “The use of military force”. As we know the pandemic changed our plans and we postponed the seminars for one year. So, we did not anticipate how actual in real world the chosen themes would be. When I wrote the introduction to the last year’s publication, I concluded the topic as “the Russian deterrence – preventing or preparing for war”. I could not imagine how incisive it actually was. The year before the 24th of February 2022 and the time after that date, are offering a good amount of empirical material on the Russian way of waging war, which I think, is perhaps the only positive issue in this situation.

The situation of today is apparently a result of a long-term development. Already in the middle of 1990s, general Anatoly Klimenko, serving at that time in the Strategic research centre of the Russian General staff, wrote that, in the relations between the West and Russia there was a slow advancement towards “*a confrontational situation similar to the Cold war*”. He argued this prediction would come true if NATO accepts new members and ignores Russian’s security concerns¹.

In this respect, the current situation has been evolving for the past 25 years, but the question is, what happens tomorrow? In 2017 the Chief of the Russian General staff, Army general Valery Gerasimov stated in the assembly of the Academy of Military sciences that “*the war has always been a “sputnik” for mankind...and one of the factors for a state’s development*”.² How right he was – but the development can proceed either to a negative or to a positive direction. Many people in Europe at the moment are of the opinion that a war is not “behind the mountains”, a perception which is created intentionally by Russia³. Russia is not explicitly stating this, but the facts speak for themselves.

¹ General Klimenko served at that time at the Military-strategic Research Center of the General Staff and referred to an article by D. Trenin: “Russia and the West...” in *Международная жизнь* № 1/1996.

² Gerasimov V.V.: *Современные войны и актуальные вопросы обороны страны*. Вестник академии военных наук 2(59) 2017, p. 9.

³ See: LtCol(GS), PhD Petteri Lalu (2016): *On war and perception of war in Russian thinking*. https://puolustusvoimat.fi/documents/1951253/2208221/PVTUTKL_160525_DOS_J_tutkimuskatsaus_on_war_and_perception_of_war_in_Russian_thinking.pdf/2d81a143-9e98-4194-92aa-86157e84b291/PVTUTKL_160525_DOS_J_tutkimuskatsaus_on_war_and_perception_of_war_in_Russian_thinking.pdf?t=1464597041000 p.1.

We should consider the following question - in this situation is there such a contradiction, the solution of which would be reached by using military power? And are all the other non-military means already proven fruitless? Furthermore, the next question would be logic, but to a certain extent speculative – what would Russia achieve by using military power? Theoretical approach would be in trying to examine the grounds and reasons, detonators, the notion of victory, the end-state, consequences etc. and what comes to the military - what would be the military-strategic objectives respectively?

My perception is, as we speak, that Russia is conducting a real exercise and a test of the strategic deterrence as a proactive function and trying to find out the limits for actions of this kind. In a way I see some similarities between the situation of today and the situation in the spring of 2014 when Russia invaded the Crimean Peninsula. I am not certain that Russia really anticipated the consequences. These current actions definitely do not contribute to foster a détente or trust in Europe - quite the opposite.

My presentation consists of three parts: Firstly, I discuss some theoretical aspect and bring up some highlights from the debate in Russia concerning the notion of war. In the second part I will discuss the questions of war, what instruments are used, how they have changed and how they change the concept of war in broad terms. Finally, I will draw some conclusions.

Theoretical background

It is worth noting that in the middle of 1990s the Chief of the General staff Army general Viktor Samsonov brought up his definition of war, by saying “*a war is means to achieve political goals by solving disputes between states by using political, economic, financial, diplomatic, informational, technological and other means combined (в союзе) with the threat of use or with the direct use of military power*”.⁴ Despite of the fact that this definition did not end up as an official definition, it gives an idea of the thoughts within the military leadership at that time and how close the definition is to the current situation. The important term was “the combination”, but apparently at that time of the definition was too belligerent.

The debate, the variety of perceptions on the concept of war and the incompleteness in terms of the definition were tangible, because it was 2017 when Army General Valery Gerasimov stated that “*the definition of the notion of war is not written in the official documents*”⁵. This refers to the fact that the definition of war is a political act, every state defines it according to one’s own basis⁶ and it doesn’t have any permanent state of matter – every war is thus different from others as for example Army general Mahmut Gareev has mentioned⁷.

⁴ Самсонов В. Н. (1996): Иная трактовка понятия войны. Независимая газета № 243 от 26.12.1996.

⁵ Герасимов Валерий (2017): Мир на гранях войны. Военно-промышленный курьер от 13 марта 2017.

⁶ See: Кокошин А.А., Веселов В.А., Лисс А.В., Фисенко И.С. (2015): Современные войны и военное искусство. Некоторые социологические и политологические аспекты. ЛЕЛАНД, Москва, p. 29. Probably Russia will not suggest to the international community that the conventions related to war should be opened and the contents redefined.

⁷ Гареев М.А. (1999): Характер войн будущего. Стратегическая стабильность № 1/1999. Löydettävissä: <http://sipria.ru/pdf/ss1911.txt> (20.4.2004, 7.2.2022).

The Russian approach to the concept of war is to see it in a political and a military dimensions which both refer to the objectives. The official typology according to military doctrines from 2010 onwards in its turn defines war by using scale and objectives. Also starting from that time, there was a new concept introduced – a military conflict – which includes all types of war and also an armed conflict. This division refers to the threat perception and can be explained from the systemic perspective to security and also with the needs and resources from the military planning's perspective.

The legacy of von Clausewitz, defining a war as a political instrument, has not been denied, although the only type of war which is assessed and commonly declared in speeches and official documents to have a minor probability is a large-scale war. Despite of its level of probability, a large-scale war is one of the foundations and a justification for military preparations. In Russian military thinking a large-scale war includes all resources and capabilities in terms of military potential.

Despite of the challenges regarding the definition of war, I will examine the Russian perception of war through three factors: structure, nature, and orientation. The structure is understood as consisting of the essential, permanent components of the phenomenon and the relations between them. The structure of war consists of the subject, the instrument and its utilisation, the object and the aim. The nature of war is perceived as changing due to different factors relating to war. The orientation refers to the object and the influence directed towards it.

Especially the development of technology and weapon systems causes changes, as a matter of fact, inclusions to the practical means of warfare and to the theoretical basis for them. It is apparent that the change in the nature of war would affect also the notions of “military power, art of war, armed battle and violence”. The changes in the nature of war will cause changes in the orientations of influence towards the object respectively.

The debate on the concept of war

Traditionally in Russia, the concept of war has been understood in accordance with the Clausewitzian definition as one, among others, means of politics. The concept is firmly attached to terms such as uncertainty, unpredictability, surprise and the use of violence⁸. The ultimate goal has been the coercion of the adversary to obey the will of the winner. In practical terms, the goal was to force the leadership of the adversary to a situation without options, the area has been occupied and the military force destroyed or forced to a stage of not being capable to continue the war.

In the last Soviet encyclopedia, the definition of war heavily emphasized the role of the state, its militarized organisations and the obligation of the whole society and people when it comes to participation in waging war. Along with the armed battle, the use of other means (political, diplomatic, economic, financial, informational, etc.) in achieving the aims was also included.⁹

The collapse of the Soviet Union did not cause any substantial changes to the definition of war. The Soviet ideological emphasis of the concept was replaced with refer-

⁸ Jyri Raitasalo & Joonas Sipilä (2004): Sodan määrittelystä – käsitykset sodasta sodankäynnin taustalla. MPKK:N strategian laitos, julkaisusarja 4 n:o 18, p. 1-2.

⁹ Военный энциклопедический словарь, Военное издательство, Москва, 1986, p. 151.

ences to an informational battle. Other parts of the definition were left mostly unchanged, and the essential prerequisite for war was still the armed battle.¹⁰ So, the use of other than military means in the concept is nothing new.

In the first decade of the 21st century, the nature of war was one of the main topics in the military scientific debate. Different “schools of thought” can be found within the debate, or rather, various viewpoints emphasising different issues related to the nature of war. One of these was the so-called official school, the other was a sort of conservative block, putting emphasis on the current resources and the use of multiple means, and the third represented a futuristic point of view stressing for example the role of new high-precision weapon systems. These approaches to warfare were not mutually exclusive, on the contrary, they brought up different elements which can be found today.

One interesting detail is that in the General staff academy during the years 2008–2009 war was perceived as a combination of using all means and instruments available towards achieving the defined political goals.¹¹ So, this approach was even more belligerent than that by Viktor Samsonov 10 years earlier. In this respect the main idea of the theory of warfare was the systemic approach. Basically, war as a system consists of two opposite parties being at the same a subject on the one hand, and on the other hand an object to the other party’s influence. According to this approach, the international relations between the actors are basically a constant competition and defending one’s own interests without using armed force.

Despite of the debate, the changes in the encyclopedia of 2007 were rather mild. The reference to the role of the society was not so strict as in the Soviet version, apparently because of the change in the threat perception (or in the potential). The larger the scale of the war in question, the bigger the role of the supporting functions of the society. The armed battle was and still is the core element of war in various definitions.¹² In this respect the war is not defined solely with the use of military force. What comes to the use of non-military means, its primary goal seems to be in creating favourable conditions for waging war and for the use of military force. Hence the war is defined by the functions of the society¹³. This largely forms the essence of the so-called strategic deterrence.

Army general Valery Gerasimov noted already in 2017 that there were still two approaches to the debate. One being the classic approach to the essence and contents of war and the other one emphasising the need to rethink the nature of war and take into consideration also other means and instruments in addition to armed battle.¹⁴ It is not too far-reaching to conclude that the debate has come to an end, because two years from this speech in the assembly of the Academy of Military Sciences (2019) he said that “*the principle of warfighting is the coordinated use of military and non-military means with*

¹⁰ See: Valeri Gerasimov (2013): Ценность науки предвидении. Военно-промышленный курьер № 8(476) за 27 февраля 2013 года.

¹¹ Ярыгин Ю.В. (2006): Характер современных войн. Военная Академия Генерального Штаба Вооруженных сил Российской Федерации (ВАГШ ВС РФ), Москва, р. 6, 8-9.

¹² Военный энциклопедический словарь, Военное издательство, Москва, 2007, р. 154.

¹³ See also: О.М. Горшечников, А.И. Малышев, Ю-Ф. Пивоваров (2017): Проблемы типологии современных войн и вооруженных конфликтов. Вестник Академии военных наук № 1(58) 2017, р. 53.

¹⁴ Герасимов В.В. (2017): Современные войны и актуальные вопросы обороны страны. Вестник Академии Военных наук, № 2(59) 2017, р. 10.

the decisive role of armed forces"¹⁵. Furthermore, the starting point for the war is thought to be the beginning of use of armed and other means of violence¹⁶. It is evident that non-military means are used constantly in politics already in the so-called peace time.

The use of non-military means in politics can generate problems and contradictions, for the solution of which the use of military means might be considered. This is why the Russian military officials argue that the non-military means have to lean on military power. One explanation could be that the main (only) means for Russia's influence is the military power. The concept of the strategic deterrence fits to this approach and the essence of it would be the creation of favourable conditions for war. Furthermore, this could be the basis for the relation 4:1 between non- and military means presented by Valery Gerasimov in 2013¹⁷.

In Russian military thought on war there are at least five issues which seem to be fairly permanent:

- the existence of war and its role as political means is not disputed¹⁸
- Russia will use all resources and means at its disposal to safeguard its military security
- the role of armed battle is essential for the war¹⁹
- the possibility of escalation up to the large-scale war with nuclear weapons, and
- an opposite party in a war is a state or coalition of states.

If these "requirements" are not met, then the question is about armed conflict or conflict in general.

As mentioned, the Russian thinking is usually based on systemic approach as a method. Accordingly, war as a phenomenon includes a subject, action, an instrument, and an objective. The basic idea is that an instrument must have a purpose, a function and an objective for action.

Concerning Russia and in particular the Armed Forces as a subject, there have been only few structural changes after the collapse of the Soviet Union. There is the high command, the Armed forces and other militarized organisations etc. The responsibilities, tasks, and activities of the state military organisation have been shaped and

¹⁵ Валеры Герасимов: векторы развития военной стратегии. Красная звезда от 4 марта 2019 г. Gerasimov used wording: Основной «нашего ответа» является «стратегия активной обороны»...»предусматривает комплекс мер по упреждающей нейтрализации».

¹⁶ Violence is defined not only as physical impact on another person, but also as coercion of the opposing party, use of power against the will of the opposite party, misuse or illegal use of power. See: Ушаков Д.Н. (под ред.) (2006): Толковый словарь русского языка. «АСТ, Астрель, Хранитель», Москва, p. 393. See also: <http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=12849@morfDictionary> (13.1.2016, 3.2.2022)

¹⁷ Валерий Герасимов: Ценность науки в предвидении. Новые высоты требуют переосмыслить формы и способы ведения боевых действий. Военно-промышленный курьер № 8 (476) за 27 февраля 2013 года.

¹⁸ Вахрушев В.А. (1999): Локальные войны и вооруженные конфликты: характер и влияние на военное искусство. Военная мысль № 4, 1999, p. 20.

¹⁹ Махмут Гареев (2013): Предчувствовать изменения в характере войны. Военно-промышленный курьер, №. 20, May 29, 2013. See also: О.М. Горшечников, А.И. Малышев, Ю.-Ф. Пивоваров (2017): Проблемы типологии современных войн и вооруженных конфликтов. Вестник Академии военных наук № 1(58) 2017, p. 53.

finalized over time of course. This applies to the whole of the state military organisation.

When discussing the possible objects of warfighting, Russia has quite extensive experience. The potential and the real adversaries are mentioned in the military doctrine. The opposite parties have been occasionally real when looking at the conflicts in the Caucasus, Central Asia and Syria, not to mention the “internal adversaries”. As of 2014 the threats and dangers formed by an object are mentioned quite unequivocally²⁰ in real terms.

As for the functions of the instrument, in practical terms military power and armed forces, is twofold – to guarantee the security by deterring the threat on one hand and neutralize the source of threat (aggression) on the other. Taking into consideration the combat readiness of the Armed forces, one could say that in this context the red line between peace and war is literally between “the finger and the trigger”.

When it comes to the development of the Russian military organisation during the past more 10+ years, it has been assessed, that instead of focusing solely on the phenomenon of “*irregular warfare*”, Russia has concentrated on also developing capabilities in terms of “*conducting conventional warfare between developed states*”²¹. In this regard, the threat perceptions have served as a foundation for strategic military planning, reforming the Russian armed forces and the military machine in general.

The change of the instrument

Russian Armed Forces have been modernised significantly over the past 15 years in terms of activities and military hardware. The reform of 2008 affected almost all of the services and branches of the Russian Armed Forces. The main elements composing the military power were thoroughly renovated: command and control, organisations, personnel, composition of units, training, weaponry and equipment, housing, logistics etc. The goals set for different components in order to increase the combat capabilities, readiness and the level of modern weaponry have been mainly achieved.

The past 10 years have been a period of enhanced rearmament, modernisation of weaponry, and a huge number of military exercises. In this respect Russia made a choice to primarily rely on hard – rather than soft – power and to put emphasis on military force²². Russia now has a streamlined, more mobile, and partly professional military, equipped with relatively high percentage of modern weapons²³. Nevertheless, there are problems in terms of manning the units and financing also in the future. In total, one can assess that the discrepancy between military threats and capabilities to

²⁰ Forsström Pentti (2016): Venäjän sotilasdoktriinien kehittyminen Neuvostoliiton hajoamisen jälkeen (in Finnish). National Defence University, Department of Warfare, Series 3: Working papers n:o 3, p. 21–22. (<http://www.urn.fi/URN:NBN:fi-fe2016051712438>)

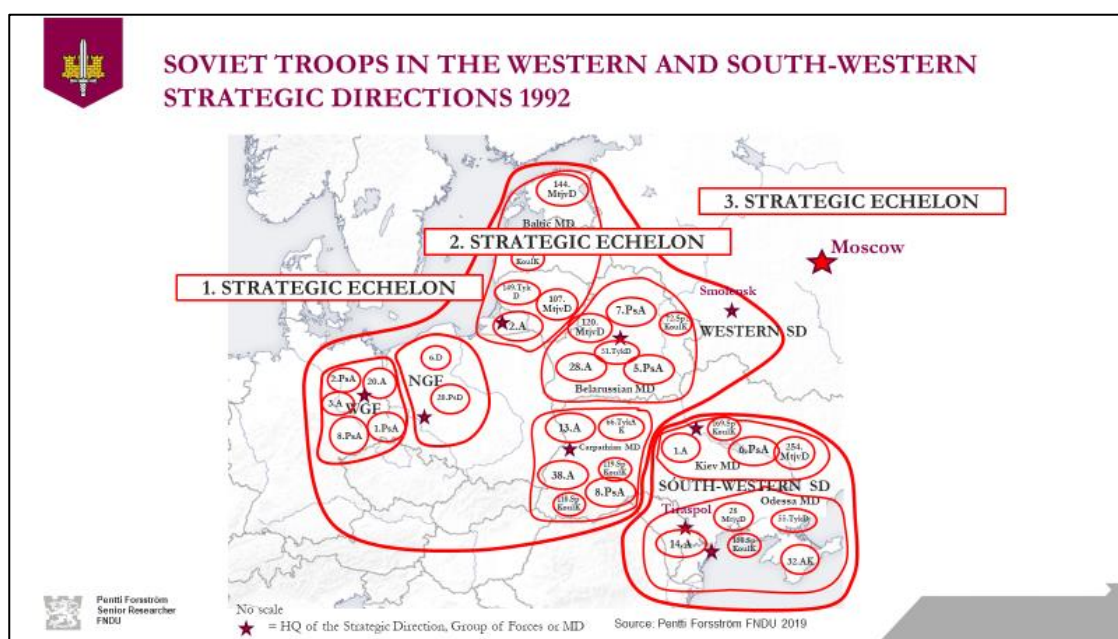
²¹ Rod Thornton (2015): The Changing Nature of Modern Warfare. Responding to Russian Information Warfare. The RUSI Journal, Volume 160, 2015 - Issue 4.

²² See: John R. Deni (ed.) (2018): Current Russia Military Affairs. Assessing and Countering Russian Strategy, Operational Planning, and Modernisation. US Army War College, SSI, p. 36.

²³ See also; Martin Russell (2021): Russia's armed forces, Defence capabilities and policy. European Parliamentary Research Service. p. 1. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689370/EPRS_BRI\(2021\)689370_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689370/EPRS_BRI(2021)689370_EN.pdf) (3.2.2022). The EU assessment is rather generic.

respond these threats have been significantly reduced in different dimensions of warfare.

If one has to choose one achievement, it would perhaps be the combat readiness and readiness as a whole, with the exception of the so-called strategic reserves. One must have noticed also that the density of troops in the Western Russia is somewhat different to the other parts of Russia. The readiness is the answer to rapidly emerging threats on the one hand and a factor enabling the blurring of the line between peace and war on the other hand²⁴.



Picture 1. Soviet Forces in the Western TVD after the collapse of the SU

As a principle this is by no means a novelty, it was already in use not only in the nuclear forces, but also at least in the 1st Strategic echelon of the Warsaw pact Armed Forces. The other guiding principle was to construct the echelons in a very deep strategic formation consisting of the Groups of forces with unequal capabilities. The most efficient and new weaponry and equipment was deployed in the first Strategic echelon. Russia today does not hold the same geographical possibility to organize the group of forces according to the same principle of echelons. The lack of this possibility has to be compensated with something else.

²⁴ Pentti Forsström (2019): Venäjän sotilasstrategia muutoksessa. Tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen. NDU Series 1: Research publications No 32, p. 416. See also: John R. Deni (ed.)(2018: Current Russia Military Affairs. Assessing and Countering Russian Strategy, Operational Planning, and Modernisation. US Army War College, SSI, p. 36.



PRINCIPAL STRUCTURE OF RUSSIAN DETERRENCE/IMPACT



Picture 2. Russian principle of means of deterrence and impact

When it comes to the nuclear forces – the development and the rearmament are still some of the top priorities for Russia when assessing the level of so-called modern weapons²⁵. There are at least two tendencies when it comes to the nuclear forces: first, maintaining capacity by replacing the older versions of weaponry, and the second, developing capabilities to overcome the challenge of ballistic missile defence systems²⁶ (Avangard, Sarmat). Also, the dual-purpose principle is heavily put into practice (Poseidon, Kinzhal, Tsirkon).

The reformation of the conventional forces has resulted not only in increased combat readiness but also in the creation of larger and more powerful, manoeuvrable formations and in their rearmament with modernized and partly newly produced weapon systems. This applies to all the services and branches of the Armed Forces. The basis for readiness has been achieved by recruiting professional soldiers. The conscript system served mainly for the purpose of forming strategic reserves, and it is maintained particularly in the light of a large-scale war.

The change of the armed battle

In the following part, I will briefly discuss changes in the armed battle, defined as fighting with the use of weapons. Its nature, scale and means depend on the weaponry at one's disposal²⁷. During the last decade the Russian Armed forces have been quite determined and successful not only in terms of developing the weaponry and equipment. The conceptual basis for this change was created in the 1990s. Already then, few tendencies in the development of the armed battle were identified. The most

²⁵ Congressional Research Service: Russia's Nuclear Weapons: Doctrine, Forces, and Modernization, Updated September 13, 2021. (<https://sgp.fas.org/crs/nuke/R45861.pdf>)

²⁶ See: John R. Deni (ed.) (2018): Current Russia Military Affairs. Assessing and Countering Russian Strategy, Operational Planning, and Modernisation. US Army War College, SSI, p. 31.

²⁷ <https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=12869@morfDictionary> (3.2.2022)

remarkable of them being the enlargement of the battlespace and the growing importance of information, very generally speaking.

Conceptual shifts are partly based on the development of digital technologies and artificial intelligence at a very large scale. These are named as some of the key future drivers regarding changes in the armed battle. The initial period of war and battle has a substantial and critical significance for the outcome of a battle in Russian military thinking. Informational superiority in command and control of the troops and weapon systems are the focal objectives to be achieved.²⁸

At the shift of the millennium, the representatives of the Strategic research centre of the General staff stated that the development of information technologies and technology in general is no less than “revolutionary”. This creates the basis for developing a new generation of instruments for armed battle.²⁹ The development was assessed to proceed in a direction where different arms- and supportive systems function independently³⁰.

In 2013 Valery Gerasimov stated that in the future battlefield the asymmetric actions will increase, and in addition to this, the special operation forces and internal opposition will form a front in the whole depth of the adversary. In addition to this, the operations will be conducted by manoeuvrable combined group of forces which are operating in a common intelligence and information space. Information warfare and far-reaching fire power without physical contact are used in order to achieve the objectives and paralyze the objects. Given these actions, high-precision weapon systems, robot technology and new means of impact based on artificial intelligence play the leading role. Nonetheless Gerasimov mentioned that one must not forget one’s own traditions despite of the fact that the level of art of war is fading, and the division between defensive and offensive actions is even more difficult to define.³¹

In 2017 Valery Gerasimov mentioned that the non-military actions define the preparation of war and the waging of it. These actions were even regarded as the essential elements of the traditional armed battle. In this respect, it seems that the top of the Russian military has accepted the fact that it is not only the armed battle that defines the nature of modern war but also the complex selection of other non-military means. Especially the influence of information in forms of psychological and technical impact is increasing.³²

One feature concerning the nature of war in the Russian debate remains unchanged – the role of armed battle is still regarded as organic and the most important factor. Developing the instruments and the capabilities is for the Armed forces top-priority.

²⁸ Круглов В.В., Сосновский М.Е. (1998): О тенденциях развития вооруженной борьбы. Военная мысль № 2/1998, р. 39-43.

²⁹ Горбунов В.Н., Богданов С.А. (1999): О характере вооруженной борьбы в XXI веке. Военная мысль № 3/2009, р. 2-15.

³⁰ Горбунов В., Богданов С. (2009): Вооруженная борьба будущего. Некоторые характерные черты ее содержания. Российское военное обозрение № 1 (60) 2009. Löydettävissä: <http://www.coldwar.ru/rvo/012009/voorujennaja-borba-buduschego.php> (20.10.2015).

³¹ Герасимов В.В (2013): Ценность науки в предвидении. Военно-промышленный курьер № 8 (476) от 27.2.2013. See also: Герасимов В.В (2015): Генеральный штаб и оборона страны. Военно-промышленный курьер № 4 (522) от 5.2.2015.

³² В.В. Герасимов (2017): Современные войны и актуальные вопросы обороны страны. Вестник Академии военных наук № 2(59) 2017, р. 10.

It is obvious that a specific weapon system can even change the concept of operations and warfare in general. For example, according to Frederik Westerlund, Russia will be able to introduce stand-off-reconnaissance-strike concept.³³ This idea was brought up by Vladimir Sliptshenko speaking on the 6th generation warfare in which the long-range, high-precision missile systems play a significant role.

As mentioned, Russia does not have the same strategic depth in the West as the Soviet Union had, which would enable it to execute the principle of strategic echelons with real troops and formations. It is obvious that there is a military need for this sort of a concept – “the farther away – the better”. This could be a motive in Russia’s intentions to create a system which could compensate for the lack of traditional strategic depth.

Conclusion - «Война войной, а обед по расписанию»

The change in the perceptions of war and warfighting in Russia has reached a point, where, as the Defence minister Sergei Shoigu noted, “*the new generation conflicts are an entity of classic and asymmetric means of armed battle, where battles are high-speedy and there is no time to correct mistakes*”. Furthermore, he continued that “*the creation of a new theory for warfighting and military actions has to be the main mission in the near future*”.³⁴

Different means and weapons, when put together, create possibilities and can be used in preventive or proactive manner. In this regard, the use of informational, electronic, and cyber capabilities is safer, while they, perhaps, do not exceed the red line of warfare, but yet might have nearly as disruptive impact as the traditional kinetic weapons.

I would like to raise a question – are we today witnessing the elements of the Russian concept of “active defence strategy” launched by Valery Gerasimov in 2019?

As Andrew Monaghan wrote: “*it is time to move beyond thinking of Russian activity as blurring the lines between war and peace and towards thinking of it as blurring the lines between the offensive and defensive*”³⁵. I would add to this that the blurring of the lines should be examined also in the sphere of Russian Art of war. This could serve as a starting point on elaborating the theme for the annual Russia Seminar 2023.

I wish everyone the most fruitful discussions and informative seminar – Also, I thank you all for your contributions to this seminar.

³³ See: John R. Deni (ed.) (2018: Current Russia Military Affairs. Assessing and Countering Russian Strategy, Operational Planning, and Modernisation. US Army War College, SSI, p. 38.

³⁴ https://function.mil.ru/news_page/world/more.htm?id=12237313@egNews (3.2.2022) Выработка новой теории ведения войн должна стать основной задачей в ближайшее время, заявил Министр обороны России генерал армии Сергей Шойгу, выступая на научно-практической конференции с руководящим составом Вооруженных Сил РФ, 18.06.2019.

³⁵ Andrew Monaghan (2020): How Moscow Understands War and Military Strategy, CNA Occasional Paper. November 2020, p. i. <https://www.cna.org/reports/2020/11/IOP-2020-U-028629-Final.pdf>.

3

COMMAND AND CONTROL CULTURE À LA RUSSE

Dima Adamsky

The presentation made by Dima Adamsky in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 55:00.

Abstract

Is the Russian military cultivating command and control practices associated with the concept of “mission command” within its ranks? This presentation examines the possibility of an ongoing shift in the current Russian combat management procedures, especially on the tactical-operational levels, towards embracing the mission command culture. It outlines the sources, drivers and extent of this discontinuity in the Russian command and control (C2) tradition, the doctrinal knowledge driving it, related training methods and combat practices, and the consequences of this phenomenon for Russian military theory, organizational structures, and force buildup.

Historically, among other cultural traits, the Russian military tradition has had two proclivities. First, its tactics have been inclined toward a centralized command scheme and averse to *mission command culture* – a combat management style where commanders share with their subordinates the intent of the mission, and delegate to them freedom of action in choosing the ways to execute it, based on the subordinates’ ability to understand the context of the executed combat tasks. Second, it has tended to innovate by *conceptual anticipation*, a process whereby top military theoreticians imagine future war deductively during peacetime, and the armed forces are then transformed accordingly. It has been disinclined to innovate through *battlefield adaptation*, where lessons learned in a bottom-up, inductive manner, from the lower levels of command, result in a major transformation of the military system during wartime. These tendencies are often interrelated: while armed forces that practice centralized command are relatively better off in military futuristic, the skills associated with mission command usually enable to embark more effectively on *battlefield adaptation*.

Declarations by the Russian military brass, operational evidence and modernization initiatives suggest that the Russian military may be departing from the above customs. Besides the traditional traits of its military art, the Russian *modus operandi* in recent conflicts has resembled *mission command* practice and the *battlefield adaptation* style. Russian forces have demonstrated a flexible operational approach, innovated through trial and error, experimented displaying a tolerance to failure, modified combat planning in response to dynamic developments, delegated decision-making authority to the lower levels of command, learned and promptly adjusted and in some cases radically departed from the accepted procedures. All of these phenomena are uncharacteristic of the Russian style of war, as Western observers traditionally have perceived it. That said, the Russian high command is cultivating these developments within the ranks.

If the above assertion about the emergence of a *mission command culture* is even partly accurate, it may be a harbinger of a major change in the Russian style of war. However,

as of this writing, these significant developments have been underexplored. This presentation seeks to fill this void and focuses on the following questions: To what extent has the Russian military demonstrated such traits of tactical behavior as *mission command*, *battlefield adaptation*, and *operational improvisations*, which conventional wisdom views as alien to its tradition? If to any significant extent, how does the Russian military cultivate within its ranks mission command skills and procedures, and how do these inform concepts of operations and force buildup within the currently modernizing Russian military? If these are not just programmatic announcements and episodic wartime adjustments, but a profound transformation of the military's mindset and a shift in its organizational climate, what will be the cultural, institutional and political enablers and obstacles to implementing this change?

NEW RUSSIAN STRATEGIC WEAPONS AND MISSILE DEFENCE SYSTEMS - CHANGE OF THE BALANCE?

Leonid Nersisyan

The presentation made by Leonid Nersisyan in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 1:39:00.

Since 2018, Russia has announced and is developing several new strategic weapons and assets, some of them are considered unique¹. At the same time, a number of missile defence systems are being developed in secrecy, part of which also have anti-satellite functions.

The main questions are whether the new systems affect the balance of power and pose threat to nuclear deterrence existing between Russia and USA/NATO and what are the real goals of achieving these weapons. These issues are becoming even more important on the background of Russo-Ukrainian war and the ongoing crisis in Russia-West relations.

Classification of new strategic systems

New systems can be divided to categories by their function and nature:

- Hypersonic weapons, which include Avangard glider, GZUR hypersonic missile, Zircon anti-ship missile and Kinzhal aeroballistic missile.
- RS-28 Sarmat liquid propelled intercontinental ballistic missile (ICBM)
- Poseidon nuclear-powered, and nuclear-armed unmanned underwater vehicle
- Burevestnik nuclear-powered cruise missile
- Peresvet lasersystem
- Missile defence systems, which include S-500, S-550, Nudol, A-235 Moscow defence, Aerostat anti-ballistic missile system.

Also, on basis of open-source research and the nature of the projects systems can be divided to those which development and serial production can be described as realistic and feasible, and those which are questionable and most probably unreliable.

For example, the RS-28 Sarmat ICBM is really needed by the Russian Strategic Rocket Forces to replace the aging R-36M2 Voevoda and is not an overly sophisticated project, as it is an upgraded version of Voevoda. Also, very realistic is the Kinzhal air-launched missile, which is however a tactical system, although the Russian authorities present it differently. The Avangard hypersonic glider is also feasible as it is on

¹ Presidential Address to the Federal Assembly, March 1, 2018. <http://en.kremlin.ru/events/president/news/56957>

experimental duty², but the value of this system is still unclear given its high weight (3-4 standard nuclear warheads could be used instead of this glider).

On the other hand, some systems seem to have problems in the process of the development and questionable value in general. First, that are Burevestnik nuclear-powered cruise missile and Poseidon nuclear-powered torpedo. Both of projects are on early prototypes testing stage and there are many questions to the cost-effectiveness of these systems. It will take many and many hours for Poseidon to reach USA shore and its contribution to the preemptive or retaliatory nuclear strike is very doubtful compared to much cheaper and simpler ICBMs and SLBMs. Same can be said about Burevestnik: Russia possess long-range air-launched Kh-101/Kh-102 cruise missiles which can reach almost every target without use expensive and complex miniature onboard nuclear reactor. Se problem with it is not only the price, but also maintenance and questions about possibility of conducting test launches without spreading too much radioactive elements.

Sarmat ICBM is out of schedule

The liquid-fueled heavy Sarmat ICBM, is going to replace the aging R-36M2 Voevoda missile. The new missile resembles the previous one; however, new technologies will contribute to the facilitation of the system exploitation, and to decrease in the time period from receiving of the attack order to the missile launch (it will be less than one minute). Besides, the ICBM will be capable of carrying new hypersonic glide vehicles or just greater number of regular warheads, if compared to Voevoda (not less than 10).

Moreover, Sarmat will be configured for sub-orbital flight of almost unlimited range, which will allow attacking the enemy from any direction³. Timely development of Sarmat is vital because of the ageing of R-36M2 Voevoda ICBMs and the need for their routine replacement. Otherwise, the strategic nuclear potential of Russia will be significantly decreased.

At this point Sarmat only completed the ejection tests stage with 3 launches completed in 2017-2018 and first full-fledged test launch completed in April 2022⁴. According to Sergey Shoigu's statement in summer 2021, Sarmat was going to be tested in 2021 and 2022 and enter service in the end of 2022⁵, which is already an unreachable goal. Other official plans were stating five Sarmat test launches in 2022, which also doesn't seem feasible. Moreover, the open sources are showing that there is a trial going on with the designers of control system of the missile because of violation of scheduled work⁶. The cause of that is lack of needed Russian components and Western sanctions closing the availability of high-quality electronics.

² “Andrew Osborn, 2019. Russia says it has deployed first hypersonic nuclear-capable missiles”. Reuters. <https://www.reuters.com/article/us-russia-nuclear-missiles-idUSKBN1YV1M1>

³ Dmitry Kornev, 2021. “Waiting for the Sarmat (В ожидании Сармата)”. New Defence Order. Strategy, №3 (68). <https://dfnc.ru/arhiv-zhurnalov/2021-3-68/v-ozhidanii-sarmata/>

⁴ Mike Wall, 2022. “Russia conducts 1st full flight test of new 'Sarmat' intercontinental ballistic missile”. Space.com <https://www.space.com/russia-test-launch-sarmat-icbm>

⁵ “First Sarmat ICBM regiment to enter service in late 2022 — Missile Forces commander”. TASS. <https://tass.com/defense/1376805>

⁶ <https://t.me/warbolts/779>

On that background, a more realistic prognosis of Sarmat being operational sounds as 2024–2025. At the same time, it should be noted that Russia is already building infrastructure for the new ICBMs at the 302nd Regiment of 62nd Missile division in Krasnoyarski Krai which shows the will to start the rearming process as soon as possible⁷.

Kinzhal Hypersonic Air-Launched Missile

Generally, the Kinzhal missile is an air-launched missile very similar to the 9M723 ballistic missile which is part of the Iskander-M short-range ballistic missile system⁸.

Certainly, one cannot fully classify Kinzhal as a hypersonic weapon – it is still a ballistic missile, and these missiles have already reached such speeds before. At the same time, it is also not really a strategic weapon, as Russian officials try to show it.

However, the idea of adapting 9M723 Iskander-M missile for the needs of aviation is quite sound – it does not require too much investment, and it solves key tasks: precision strikes on the most important enemy targets protected by the layered air defense and missile defense systems. The maximum flying range of the missile itself remains one of the disputed questions – we can definitely say that it is at least 1000 km, as it was officially stated about one of the test launches⁹. The high speed of the missile, which reaches Mach 10, makes target engagement time very low adding Russian Armed forces a new long-range instrument for any kind of conflict. If we consider average speed of the missile at Mach 7 it will only take 6 mins to engage a target at the range of 1000 km.

The missile has already been tested in the Southern Military District with the MiG-31BM converted supersonic interceptor aircraft as a launch platform¹⁰. In the end of 2021 Sergei Shoigu stated that a regiment of MiG-31K is created in Russian VKS. It is noteworthy that MiG-31K is noticed to have drills together with Tu-22M3 bombers – and last time that happened in Syria in February 2022¹¹. Most probably that testing is connected to the plans of having MiG-31K integrated in Navy aviation for countering surface targets – in that case operations with Tu-22M3 doesn't seem strange. Also, there are long-standing discussions and rumors on development of Kinzhal missile modification for Tu-22M3 itself. Also, it should be noted that several Kinzhal missiles were used in the war with Ukraine, but there is not much information available on effectiveness of these strikes.

⁷ <https://t.me/warbolts/843>

⁸ “The Kinzhal airborne missile system. Project history, characteristics and expert opinion (Авиационный ракетный комплекс "Кинжал". История проекта, характеристики и мнение экспертов)". TASS. <https://tass.ru/info/7235539>

⁹ “Defence Ministry reports successful test of Kinzhal missile in challenging weather conditions (В Минобороны сообщили об успешных испытаниях ракеты "Кинжал" в сложных метеоусловиях)". TASS. <https://tass.ru/armiya-i-opk/6139382>

¹⁰ <http://militaryrussia.ru/blog/topic-896.html>

¹¹ “Tu-22M3 and MiG-31K with Kinzhal missiles deployed to Syria to participate in Russian naval exercises (Ту-22М3 и МиГ-31К с ракетами "Кинжал" перебросили в Сирию для участия в учениях ВМФ РФ)". TASS. <https://tass.ru/armiya-i-opk/13714005>

Another actively promoted hypersonic weapon is the Zircon anti-ship missile. It has been undergoing trials since at least 2012, when the first drop tests were carried out from a Tu-22M3 bomber, while flight tests began in 2015 at the Nenoksa test range¹².

Reliable information about the missile is scarce, and even a short video recording releases does not reveal much information about it. Clearly, after exiting from the 3S14 vertical launcher, the missile is accelerated by a solid-propellant booster to the supersonic speeds required to activate its ramjet/scramjet engine. Given that the missile reaches a speed of Mach 8, on the first sight it can be assumed that a scramjet is used.

But the information from one of the latest tests of Zircon gives another view: missile was launched on target at a range of 450 km, and according to the Chief of the General Staff of the Russian Armed Forces, Valery Gerasimov, the Zircon flight time was 4.5 minutes. Based on this data, the average missile flight speed about Mach 4.86 and the maximum speed is reached only on the final part of trajectory, most probably by the use of solid-propellant booster¹³. Apparently, this approach allows the missile to be powered by a ramjet engine, the development and production of which is not under a question. The Zircon's firing range is probably around 600 km or slightly more.

The third hypersonic cruise missile being developed is known as GZUR (гиперзвуковая управляемая ракета - abbreviation for Hypersonic Guided Missile in Russian). Information about work on this project appeared for the first time in open sources in 2017. The missile is being developed by the Raduga Design Bureau (City of Dubna) and will be able to reach a speed of Mach 6 with a maximum range of 1 500 km when launched on a high-altitude trajectory. There is a serious lack of information on how development of the missile is going on and its definitely out of schedule as it was planned to enter service in 2020¹⁴.

Hypersonic Glide Vehicle – Is Russia the First in the World to use it?

Russia, China, and the United States have been actively developing hypersonic glide vehicles for a rather long time in order to equip their ICBMs with it. However, Russia has already 6 Avangards operational in 13th Orenburg Rocket Division, in 2022 the second regiment of those systems will be formed¹⁵.

The Avangard consists of an UR-100N UTTKh silo-based liquid-propellant intercontinental ballistic missile (ICBM) (NATO classification SS-19 Mod 3 *Stiletto*) combined with a new hypersonic glide vehicle, which previously appeared in open sources as Object 4202 and 15Yu71. The glider was developed by NPO Mashinostroyeniya and

¹² “Developers reveal hypersonic cruise missile above 6M (Минобороны успешно испытало гиперзвуковую ракету "Циркон")”. Interfax. <https://www.interfax.ru/russia/730342>

¹³ Leonid Nersisyan, 2021. “The Need for Speed.” Air Warfare, issue 3. The Shephard Press Ltd. https://editions.shephardmedia.com/2021/06/09/aw-03-21-hypersonic-weapons/pugpig_index.html

¹⁴ <http://militaryrussia.ru/blog/topic-562.html>

¹⁵ “А second regiment of hypersonic Avangards will be on duty by the end of 2022 (Второй полк гиперзвуковых "Авангардов" заступит на дежурство до конца 2022 года)”. TASS. <https://tass.ru/armiya-i-opk/13676241>

is believed to have undergone at least seven tests, most recently on 26 December 2018¹⁶.

Unlike conventional ICBMs, the Avangard hypersonic glider enters the atmosphere noticeably earlier and switches from a ballistic trajectory to gliding. Its speed at re-entry reaches Mach 27 (also typical for regular ICBM warheads), which begins to decline rapidly during the glide phase (the vehicle has no propulsion of its own). It can be assumed that in the final phase of flight it will be at no more than Mach 8-10.

Such speeds, combined with its nonballistic trajectory and some manoeuvrability, make the Avangard inaccessible to existing air and missile defence assets. Of particular note is the ability to achieve more accurate guidance on target, through a controlled flight path, which theoretically could allow the future use of conventional precision-guided intercontinental-range warheads.

Another interesting question is how the Yasnensk site is equipped with the UR-100N UTKh, as the last 30 of these missiles known to be in service are deployed at the Tatischev launch site (in the Saratov region, hundreds of kilometres away). The idea of moving heavy liquid-propellant ICBMs from one base to another initially sounds absurd.

Nevertheless, in recent years Avangard has been tested from launchers at Yasnensk where the newer R-36M2 Voyevoda ICBMs are based. The answer appears to be that Russia bought 30 stockpiled *Stilettoes* from Ukraine in 2002-04¹⁷. The technical condition of these ICBMs at the time allowed them to be kept operational until at least 2020 and even beyond. Accordingly, it is logical to suppose that 12-20 of these missiles have been modified into Avangards and kept in empty silos for R-36M2 ICBMs. This is the view of the author, reached after a conversation with Dmitry Kornev, an independent military expert specialising in Russian strategic armaments.

It is obvious that the Avangard, in its current form, is a temporary, transitional solution. The UR-100N UTKh is old (production ended in 1985), and despite its reliability, it does not have an infinite lifespan. There is a high degree of probability that the future carrier of hypersonic gliders will be the RS-28 Sarmat advanced heavy ICBM.

It is possible that due to the increased payload of the Sarmat (twice as high as that of the UR-100N), it will be able to carry two or three gliders at once. However, even after the RS-28 enters service, only a small fraction of them will be equipped with hypersonic gliders, while the rest will have conventional nuclear warheads. They are cheaper, and most importantly lighter – the RS-28 will be able to carry at least ten of them.

At the current stage of development of anti-ballistic missile systems, large-scale production and deployment of hypersonic gliders with nuclear payloads makes no practical sense: they are heavier than regular warheads and their use actually reduces the power of the armed forces. Conventional hypersonic gliders, which in the more dis-

¹⁶ “History of the Avangard missile system (История создания ракетного комплекса "Авангард)". TASS. <https://tass.ru/info/5955357?>

¹⁷ “Source: The first carriers of Avangard hypersonic units will be UR-100N UTKh missiles (Источник: первыми носителями гиперзвуковых блоков "Авангард" станут ракеты УР-100Н УТТХ)". TASS. <https://tass.ru/armiya-i-opk/5047200>

tant future could hit targets across the globe within 30 minutes, may be much more useful, but the Russian defence industry is not ready for production of the complex guidance systems needed to provide high enough precision.

Combat Laser System

Peresvet Combat Laser System was shown for the first time in 2018 by the President of Russia. From that time no official information on the functions of the system had been disclosed.

Later, in August 2018, following from comparison of a video record published by the Minister of Defense and satellite images, one of the OSINT specialists discovered that the systems were situated in launch sites of the Russian Strategic Missile Forces, where ICBMs are located. In view of this, it was supposed that the task of Peresvet can also include flashing the optics of Earth observation satellites and missile early-warning satellites. Later the comprehensive OSINT research of Bart Hendrickx¹⁸ showed that this was a right interpretation – Peresvet function is to dazzle electro-optical reconnaissance satellites and dual-use Earth remote sensing satellites and it is still a question if it can be used versus early-warning satellites, which are on high geostationary orbits. There are already 5 missile divisions equipped with Peresvet. Most probably the system is planned to use during two possible scenarios: 1) Signs of imminent attack on Russian ICBM arsenal and 2) The Russian plans of first attack on other state. In both scenarios Peresvets will help to mask the movement and location of Mobile ICBMs.

Air and Missile Defence Systems

Talking about Russian missile defence systems there is no need to go deep into technical details, as not many of them are known and some are a matter of discussion.

S-500 system main purpose is tactical missile defence. Officially it can engage targets 200 km high and 500 km far¹⁹. These specifications are more or less close of those of U.S. THAAD system. Both systems can't engage ICBM warheads, but at the same time can add real capabilities versus tactical missiles which can be widely used by enemy in local and regional wars. From that perspective S-500 project is very practical but is not connected to strategic balance.

Another question is what is S-550 system announced by Sergey Shoigu in the end of 2021. It could be some further development of S-500, or a cheaper and simpler version of S-500, like S-350 relate to S-400²⁰. There is yet no reliable information on that project available.

Other well-known and widely discussed system is the Nudol, which is considered nowadays more as an anti-satellite (ASAT) system and has been tested once with a real satellite interception. There is almost no information on the system coming from

¹⁸ Bart Hendrickx, 2020. Peresvet: a Russian mobile laser system to dazzle enemy satellites. The Space Review. <https://www.thespacereview.com/article/3967/1>

¹⁹ “The Sword of Damocles and Prometheus: what threats the S-500 must parry (Дамоклов меч и Прометей”: какие угрозы должен парировать С-500)”. TASS. <https://tass.ru/opinions/12677175>

²⁰ “Details of Russia's latest S-550 SAM system revealed (Раскрыты подробности о новейшей российской ЗРС С-550)”. Lenta.Ru. <https://lenta.ru/news/2021/11/24/s550/>

Russian official sources and even the data on test launches comes from mostly from U.S. intelligence. It is difficult to imagine real combat use of such an ASAT system in a local conventional war, but there is one real problem it may cause: the test interceptions generate space debris which is making difficulties for the civilian space projects²¹.

Modernisation of A-135 Moscow missile defence system to the A-235 is going on during last years. The new version has upgraded interceptors, which according to some sources are not carrying nuclear warheads any more due to the better guidance system²². At the same time, the system is initially made to counter single ICBM warheads and is not capable of stop a full-scale ICBM/SLBM strike. Most probably, same can be said about the mysterious Aerostat strategic ABM system. It is only known that Aerostat is being developed by Moscow Institute of Thermal Technology (MIT) and it never been mentioned officially. It could be a part of the prospective A-235 Moscow missile defence system – the new long-range interceptor. There is a probability, that system is based on one of the MIT existing ICBMs (i.e. RS-24 Yars) and has an exoatmospheric kill vehicle instead of warheads. Also, the system may use mobile launchers²³.

Unmanned Underwater Vehicle – Implementation of the Idea of the 1950s'

The idea to create a giant nuclear-powered torpedo with a tremendously powerful thermonuclear charge appeared in the USSR as early as the 1950s. The project was called T-15 and has actively been promoted by Andrey Sakharov, one of chief Soviet scientists and then a future political dissident. The technologies of those times didn't allow for the creation of a compact nuclear propulsion system, and there were also problems with naval carriers for such a huge object.

However, modern technologies ensured the implementation of this old concept – the Poseidon nuclear-powered submarine drone was 'accidentally' demonstrated on the Russian TV in 2015 and then officially announced by Vladimir Putin in 2018. Earlier mass media reported of the range of Poseidon as equal to 10,000 km, submergence depth of 1 km and the rate of sailing up to 185 km/h²⁴.

The carrier platform for this unmanned underwater vehicle is the project 09852 Belgorod nuclear-powered submarine which already started test in the sea. In the official televised footage, the submarine is carrying both nuclear-powered torpedoes, and Klavesin-2R-PM unmanned underwater vehicle (this vehicle is capable of implementing various ISR tasks such as mapping of the sea bottom, and possibly affecting the underwater communication lines)²⁵.

²¹ Theresa Hitchens, 2022. "Russian ASAT debris imperils DoD, NRO sats, while ISS risks increase: COMSPOC". Breaking Defense. <https://breakingdefense.com/2022/01/russian-asat-debris-imperils-dod-nro-sats-while-iss-risks-increase-comspoc/>

²² <http://militaryrussia.ru/blog/topic-354.html>

²³ Bart Hendrickx, 2021. "Aerostat: a Russian long-range anti-ballistic missile system with possible counter-space capabilities". The Space Review. <https://www.thespaceview.com/article/4262/1>

²⁴ "Russia releases first video footage of new Kanyon/Status-6 nuclear torpedo". Naval Today. <https://www.navaltoday.com/2018/07/19/russia-releases-first-video-footage-of-new-kanyon-status-6-nuclear-torpedo/>

²⁵ "Putin shows off Russia's latest nuclear weapons (Путин показал новейшее ядерное вооружение России)". Novaya Gazeta. https://youtu.be/oo_zuzBvVxg?t=77

The real stage of development of Poseidon is unknown, but the technological complexity shows that most probably it is far from serial production. The real effectiveness of this concept is very questionable as it will take many hours or even days to reach USA shore in the event of full-scale nuclear war. Retaliatory strike of this way is not adding much difference to the full-fledged use of ICBMs and SLBMs. At the same time system can add some effective damage to naval bases if we are talking about a first attack (in connection with timely used ICBMs and SLBMs).

Burevestnik Nuclear-Powered Cruise Missile – Implementation of the Cold War Concept

The Burevestnik nuclear-powered cruise missile had never been mentioned before the Putin's announcement in 2018²⁶. Judging by the announcement and the footages shown, this system is new and unprecedented. According to this concept, the small-size nuclear power plant on board of the missile ensures almost unlimited range capability. The real state of preparedness of this missile is still unclear (as well as its actual testing with the reactor onboard). The actual cost of such a missile may become the problem, as well as its limited use – it is clear that Moscow is not going to use nuclear-powered weapons in local conflicts. Its other drawback is a necessity of the staff permanent work with the nuclear-powered missiles, which requires the provision of effective radiation safety. One another problem is that the testing of nuclear-powered missile is very dangerous.

According to the official version, the tests were conducted at the end of 2017 at the Central Testing Ground of the 12th Main Directorate of the Ministry of Defense in Novaya Zemlya Archipelago, where the nuclear power plant reached the planned capacity and ensured the required level of thrust. Later, one of Russian independent experts found out that the test launch was conducted from a launcher located near Pankovo, Novaya Zemlya. Apparently, the cruise missile prototype flew about 100 km. Evidently, a United States officials had issued a statement that confirmed that the US had observed a small number of Russian nuclear cruise missile tests and had seen them all crash²⁷.

In July, 2018, the Ministry of Defense of Russia has demonstrated a video from the plant where Burevestniks are produced²⁸. The video shows only the head part of the missile, its most interesting “details” not being disclosed yet.

At this point there are currently no real tasking for such a missile – the existing system of the US National Missile Defense is far from being able to handle the Russian retaliatory strike by means of the intercontinental ballistic missiles (ICBM) and submarine-launched ballistic missiles (SLBM). As the first-strike weapon, the system does not have so many advantages over the Russian air-launched cruise missiles Kh-

²⁶ Presidential Address to the Federal Assembly, March 1, 2018. <http://en.kremlin.ru/events/president/news/56957>

²⁷ David E. Sanger, Andrew E. Kramer, 2019. “U.S. Officials Suspect New Nuclear Missile in Explosion That Killed 7 Russians”. New York Times. <https://www.nytimes.com/2019/08/12/world/europe/russia-nuclear-accident-putin.html>

²⁸ “The Burevestnik nuclear-powered cruise missile (Крылатая ракета с ядерным двигателем «Буревестнику»)”. Russian Ministry of Defence. <https://youtu.be/okS76WHh6FI>

101/Kh-102, capable of flying according to various estimates from 4 500 to 5 500 km.

Conclusions

- RS-28 Sarmat is the most important project as it must replace aging R-36M2 ICBMs
- Strategic ABM systems won't be able to counter USA or China massive nuclear strike in foreseeable future
- Kinzhal airborne ballistic missile is not a strategic system. At the same time, it can be highly effective in any type of conflict, decreasing target engagement time
- Avangard hypersonic glider in nuclear configuration is not adding capacity to Russian nuke-triade. Before the creation of highly effective ABM systems Avangard is only decreasing the number of warheads per ICBM
- Peresvet laser system is being widely deployed, but the exact functions are still a matter of question
- S-500 system can add anti-tactical ballistic capacity to Russian troops and create another echelon of defence – the longest-range one
- Poseidon and especially Burevestnik don't look as feasible projects. Both of them can't break the existing balance between Russia and USA.

Therefore, it can be considered that the main reason for investing in the most complex and miscellaneous strategic weapons and partly the strategic ABM systems have more a political than military value. These systems are allowing Russia to have a high-level dialogue with USA and keep the military superpower status, also serving as bargaining chip in further Arms Control negotiations. They also have a vast internal policy function, as the greatness of Russian Armed Forces and especially its nuclear component is widely used in the state propaganda.

The abovementioned systems are not going to change the existing balance of power and affect the existing nuclear deterrence. Also, many of the projects may never move further from prototype stage. On the background of Russo-Ukrainian war even the political role of these weapons is hardly affected, as the strategic stability negotiations are not possible in foreseeable future, at the same time the already standard Russian nuclear threatening policy is not effectively deterring USA and NATO from providing a full-fledged support to Ukraine.

At the same time, Russia may gain feasible ASAT capabilities with the combination of Nudol, Peresvet and orbital satellite intercepting systems. This may lead to further arms race in this domain. On that background, the tests and real combat interceptions of low-orbit satellites may form too much "space junk" and in that way make serious problems for civilian space projects.

5

STRATEGIC ACTIONS OF THE ARMED FORCES – CONCEPTUAL ANALYSIS

Jukka Viitaniemi

The presentation made by Jukka Viitaniemi in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 2:08:00.

Abstract

The aim of this working paper is to provide information on the operations of the Russian armed forces, especially at the strategic scale. This working paper focuses on key concepts by looking at the evolution and change of their official definitions from Soviet times to the present day, ending with the current official definitions. The main aim of the working paper is to create definitions for those concepts for which no official definition has been published.

The analysis of the definitions shows that the basic concepts of strategic action or their precursors date back to the 1950s and 1960s, when they were characterized by the proliferation of nuclear weapons. The partition of strategic actions of the armed forces seem to have emerged in the early 1960s and have basically remained the same to this day. This partition, or mainly its outline, consisted of nuclear missile strikes, act of wars on the ground, covering from the enemy's nuclear strikes, and act of wars at sea. Today, the strategic actions of the armed forces are defined as strategic operation in a theatre of military action, strategic airspace operations in strategic airspace directions, and strategic operations of the nuclear forces. It should be noted, however, that there is no official public definition for the concept of strategic operation in a theatre of military action and its sub-concepts: strategic operations in a continental theatre of military actions and the strategic operations in an oceanic theatre of military actions in Soviet and modern military dictionaries or military encyclopedias.

Keywords

Russia, armed forces, strategic actions of the armed forces, strategic operation, concept, logical thinking, conceptual analysis, Hegel, Marx

Introduction

The purpose of this article is to provide an overview of the strategic actions and strategic operations of the Russian armed forces, emphasizing the concepts that explain them. The aim is to provide tools for observing strategic exercises of the Russian armed forces and at the same time to place the concepts in a historical context. With the help of concepts or more specifically with the help of their definitions, it is possible to analyze more systematically strategic exercises and real-life operations of the Russian Armed Forces. The article also supports other research prepared at the National Defense University.

It can be stated that the concepts play a central role in Russian military science and, in particular, in the logical understanding and thinking. In the Soviet Union in the 1970s, the main forms were considered to be the concept (Понятие), judgement (Суждения) and syllogism (Умозаключения). In the Military Science Work of the Time, the term “concept” was defined as follows:

”Понятие есть такая форма мышления, которая отражает общие, существенные свойства предметов, их связей и отношений. В отличие от форм чувственного познания, отражающих конкретные предметы, понятия представляют собой абстрактные образы, в которых отражаются общие существенные, необходимые свойства, связи многих предметов.”¹

Another important form of abstract thinking is judgement, which is an idea that embodies any feature and connection of an object to other objects through the association of concepts. Unlike concepts, judgements express anything about their characteristics, connections, and relationships. Correspondingly, conclusion was defined as a form of thinking through which truthful judgements provide new information about the things and phenomena of the objective world in a logical way.

In 1991, the book *Culture of Military Thought* was published, in which one subchapter dealt with logic and the shaping of the military science concept and judgement. According to the beginning of the chapter, thinking is realized through the concept, and the understanding of military objects and phenomena is realized through the formation of the concept and their use. In particular, the concept was seen as the basis for forming other forms of thinking; judgement and syllogism and it is seen to reflect the nature of things and phenomena.

Judgement was seen as an idea of a real object and a phenomenon that confirms or denies something related to its features or relationship to other objects and phenomena. Judgement combines and compares concepts. This allows syllogisms to be drawn about objects and phenomena. The syllogism was formulated as a logical basic form of indirect thought, the essence of which consists of one or a few judgements in the thinking process and which creates new information about objects and phenomena.

It has also been written in recent years about logical thinking and its significance in military science. Major General Mahonin criticized in his year 2018 article, *Strategic Thinking and Strategic Analysis: Approaches to Understanding Terms*, a poor understanding of the rules of logic and the formation of concepts in general. According to him, practice has shown that there are not many people in the scientific community who understand the basics of the rules of thinking. These rules form the basis of logic - the correct (rational) thinking of philosophical science. Concepts, judgements and syllogisms make it possible to organize the information received correctly and at the same time build it on top of an existing information system and make it available for later use. The first group of rules of logic relates to the terminology discussed in the section on concepts. Since all disciplines, including military science, have their own terminology, it must be formed according to the rules of logic.

In 2021, an article written by Lieutenant General Mahnin was published in the Journal of the Academy of Military Science, titled *Enhancing Education: A Cognitive Approach*.

¹ И.Е. Шавров и М.И. Галкин, соім., *Методология военно-научного познания* (Москва: Военное издательство Министерства обороны СССР, 1977), 165.

The theme of logical thinking was also sidelined in that article. Forms of logical thinking were defined as the concept, judgement and syllogism. The concept is considered to be a basic form of logical thinking that reflects only the essential, general features in objects, while rejecting secondary features. Based on the concepts, judgments and syllogisms are formed. Accordingly, a judgement confirms or repeals something and includes definitions of terms. The concept and the judgement are interrelated because they form a syllogism.

In practice, the family tree of the threefold division of logical thinking in the philosophy of science of present-day Russian military science dates back to Georg Wilhelm Friedrich Hegel (1770-1831) through Karl Marx (1818-1883). The threefold division of logical thinking presented above can be traced at least to Hegel's work *The Science of Logic (Wissenschaft der Logik)* and more specifically to its second part, titled Subjective Logic or the Doctrine of the Concept (Die subjective Logic or Die Lehre vom Begriff). In that section, the first section, Subjectivity (Die Subjektivität), can be found, which is further divided into three consecutive chapters: the concept (Der Begriff), the critique (Das Urteil) and the conclusion (Der Schluß). A quick analysis of Hegel's texts shows that the model and logical process of logical thinking in Russian military science is at least more reminiscent of Hegel's ideas than that presented in Marxist-Leninist philosophy.

The logical thinking of Russian military science as a process largely resembles that outlined by Hegel, in which logical thinking is more of a process than a single, detached series of independent events. Marxism-Leninist philosophy, and especially its illogicality, have certainly influenced, at least in the early decades of the Soviet Union, the philosophical debate in the science of military science, which seems to have taken on more correct form of logical thinking since the 1970s. In both Russian military science and Hegel's subjective logic, concepts play a key role. Without the concept, there is no logical thinking.

Materials

In time, the analysis of definitions begins from the 1960s, with the most significant source being the book *Military Strategy*, which first edition was published in 1962 by Marshal of the Soviet Union S.D. Sokolovsky. Due to the growing importance of nuclear weapons, the book looks at the military strategy heavily from the perspective of nuclear weapons, but despite this, the book can be considered one of the waypoints of the Russian military strategy.

According to history, Sokolovski met with Communist Party Secretary-General Nikita Khrushchev for instructions on how to write the book. The instructions were short: "*Write so that they will be turned from terrified to half-dead there.*" However, this does not significantly reduce the value of the work in question. The above-mentioned period has also been supplemented by intelligence reports produced by the CIA at that time and obtained through human intelligence, as well as a book summarizing the history of Russia's military strategy. The weakness of the intelligence reports produced by the CIA is that they have been translated into English. Because of that, it is impossible to know verbatim what terms have been used and what their Russian definitions are. The next temporal fixed point is 1976-1980, when the last Soviet Military Encyclopedia was submitted, and 1983 and 1986, when the first and second editions of the Military Encyclopedic Dictionary were published. The purpose of the choices is to

bring the latest definitions from the Soviet era into comparison. The next time point is the turn of the millennium, when the *Military Encyclopedic Dictionary of Strategic Missile Forces* was published in 1999 and the first Russian military encyclopedia was published in 1994-2004.

Methods

This working paper is a basic descriptive traditional conceptual analysis that aims to describe the concept of strategic actions and other closely related concepts and their changing meanings and definitions in the Russian printed and electronic official military encyclopedia and dictionaries from 1979-2022. This literature has been supplemented when necessary by other sources.

The conceptual analytical process consists of four steps. The first step is to build a knowledge base that looks at who has previously considered the site and its surrounding areas, and what results have been achieved. In the second stage, an external analysis takes place, during which the concepts under review are distinguished from other closely related concepts and located in relation to their upper concepts. In the third stage of internal analysis, several views on the same concept are presented, reflecting on and detailing them. In the final fourth stage of drawing conclusions, old concepts are adopted or modified, or new ones are formed.

Discussion

On the basis of the external analysis, a total of 12 concepts were selected among the other closely related concepts by means of a distinction. At the same time, they were identified in relation to their upper concepts, of which the concept zero is “strategic actions of the armed forces”.

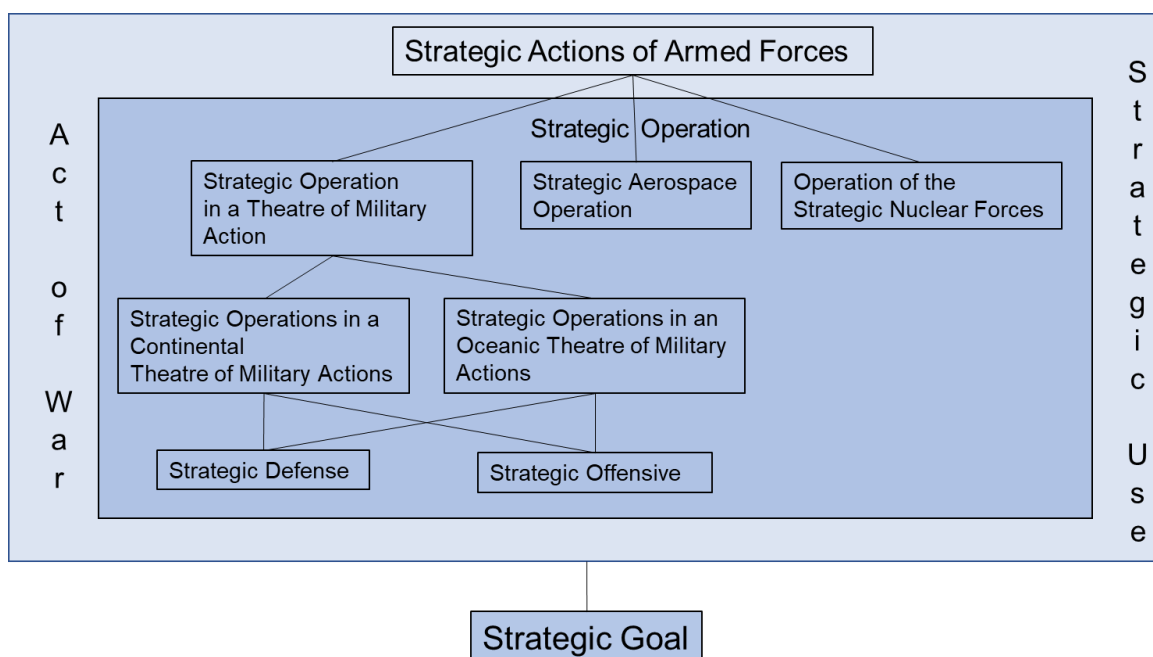
The 12 concepts mentioned above are listed below:

0. Strategic Actions of Armed Forces (СТРАТЕГИЧЕСКИЕ ДЕЙСТВИЯ ВС)
1. Strategic Use (СТРАТЕГИЧЕСКОЕ ПРИМЕНЕНИЕ)
2. Strategic Operation (СТРАТЕГИЧЕСКАЯ ОПЕРАЦИЯ)
3. Act of War (ВОЕННЫЕ ДЕЙСТВИЯ)
4. Strategic Defense (СТРАТЕГИЧЕСКАЯ ОБОРОНА)
5. Strategic Offensive (СТРАТЕГИЧЕСКОЕ НАСТУПЛЕНИЕ)
6. Strategic Goal (СТРАТЕГИЧЕСКАЯ ЦЕЛЬ)
7. Operation of the Strategic Nuclear Forces (СТРАТЕГИЧЕСКАЯ ОПЕРАЦИЯ ЯДЕРНЫХ СИЛ (СОЯС))
8. Strategic Aerospace Operation (СТРАТЕГИЧЕСКАЯ ВОЗДУШНО-КОСМИЧЕСКАЯ ОПЕРАЦИЯ)
9. Strategic Operation in a Theatre of Military Action (СТРАТЕГИЧЕСКАЯ ОПЕРАЦИЯ НА ТВД)

10. Strategic Operations in a Continental Theatre of Military Actions
(СТРАТЕГИЧЕСКАЯ ОПЕРАЦИЯ НА КОНТИНЕНТАЛЬНОМ ТВД)

11. Strategic Operations in an Oceanic Theatre of Military Actions
(СТРАТЕГИЧЕСКАЯ ОПЕРАЦИЯ НА ОКЕАНСКОМ ТВД)

One of the results and conclusions of this chapter can also be considered the visual concept map, which describes the author's understanding of the relationships between concepts. Although the location of the visual concept map would be more logical at the end of this chapter, it will be presented next before examining the individual concepts. The aim of this is to give the reader a road map on the basis of which the movement between concepts can be perceived and facilitated in his mind. The concepts discussed in this article can be found in the colored boxes on the concept map.



Picture 1. Visual concept map made by author

Strategic actions are not defined in military dictionaries or military encyclopedic dictionaries published between 1983 and 2007. In the current definition, the strategic actions of the armed forces are seen as a form of use of the armed forces, and a more detailed definition can also be found below it. Forms of use of the armed forces (формы применения) in the current definitions include peacekeeping operations during peacetime and special operations of forces in internal armed conflicts and strategic operations during the wartime. Special forms of use of the armed forces include military deterrence and strategic deployment in peacetime and wartime.

The strategic actions of the armed forces as part of their use of the armed forces are currently defined as follows. The operation of strategic nuclear forces has been added to the definition, and previously separately recorded strategic operations in the ocean and continental theatre of military actions are very likely sub-concepts of the concept of strategic operation in the theatre of military action.

”Стратегические действия ВС - форма применения ВС в войне, представляющая собой совокупность согласованных и взаимосвязанных по целям, задачам,

месту и времени стратегических операций, проводимых последовательно или одновременно для достижения поставленных стратегических целей. Проводятся в форме: стратегических операций на театре военных действий (ТВД); стратегической воздушно-космической операции на стратегическом воздушно-космическом направлении; стратегической операции ядерных сил.”²

Conclusion

It could be said that without the concept logical thinking there can be no science, this naturally also applies to military science. Concepts form, or more precisely their definitions, the parts with which we try to describe our surrounding world more comprehensibly and at the same time the language in which we discuss each other. The conclusion applies not only to the scientific community but to all of us. Concepts also form the platforms on which we transfer and store information. Definitions of concepts consist of words, terms, and other concepts written together, being a central element in all human communication.

The concepts play an important role in the philosophy of science, applying also to Russian military science, and especially in logical thinking, which has its roots all the way back to Hegel. This has not always been the case, as the actual sharpening has taken place since the 1970s, when current interpretations began to take shape. This development of ideas could not be slowed down, let alone definitively confused by Marxist-Leninist philosophy. As a result, it is safe to say that the logical thinking associated with the philosophy of science in Russian contemporary military science actually stems from Hegel's philosophical ideas, thus being at least a degree freer from the burden of political interpretations and ideas.

The Russian and also the Soviet military concepts can be rightly described very well defined and documented. Due to its breadth and, in addition, the multidimensional nature of the concepts, it is justified, when examining Russian military skills, to master the official concepts that are of interest to or linked to them. More specifically, one of the first steps in researching Russian strategy, operational art, or tactics must be to identify and master the official concepts and definitions that are central role in the research in question. Based on experience, this significantly speeds up the acquisition of further data and the actual analysis. Only after this is it justified to map out different interpretations of the definitions of the concepts or suggestions for improvement and other reflections related to the definitions and their subject matter, for example, from Russian military scientific publications. Starting work, for example, directly on interpretations of definitions or informal definitions of concepts may, from a material point of view, be misleading from the outset and thus significantly slow down the completion of a study in progress.

During the analysis process, public official definitions were found for the key concepts of strategic actions and further for strategic operations. This only reached a basic level in terms of concepts and their definitions. As a result, it would be justified to further explore the concepts in a later study, such as the sub-concepts of strategic operations and their definitions.

²”Формы применения Вооруженных Сил”.

There is no public official definition of the concept of a strategic operation in the theatre of military action with its sub-concepts. As this is a key concept, it is justified to form a definition based on the available sources. The main sources used are CIA intelligence reports from the 1970s, supplemented by current definitions of other concepts. One of the challenges in developing a definition is its many similarities with its sub-concepts of strategic operation in the continental theatre of military action and strategic operation on the oceanic theatre of military action.

The following is the author's definition of a strategic operation in the theatre of military action, stylistically designed to resemble Russian concepts:

Strategic operation in a theatre of military action is the main form of strategic actions of armed forces, forming the whole of operations, strikes and battle actions conducted by strategic missile forces (in a nuclear war), fleets, fronts (armies) and by commands and formations of different services of the armed forces, coordinated by objective, mission, place, and time and which is carried out by common idea and plan under the general command of the Supreme High Command and under the direct command of the force commander in a theatre of military action to achieve the strategic goals in a theatre of military action. By nature, the operation can be defensive or offensive and it is divided into strategic operation in a continental theatre of military actions and strategic operation in an oceanic theatre of military actions.

Strategic operation in a theatre of military action may include strategic missile forces strikes, long-range aviation's air-operations, fronts (armies) operations, fleets naval-operations, air-operations for destruction the air-enemy, airborne and anti-airborne operations, special operations and air-defence operations. Their goal is the destruction of enemy group of forces in a theatre of military action, intercept enemy's air-strikes by air-defence forces, the destruction or seizing of military-industrial complexes' in a theatre of military action, disturbing the enemy's mobilization, disturbing the enemy's governmental command and control and seizing the vital areas.

6

SCHRÖDINGERS CAT IN EASTERN UKRAINE – HOW RUSSIA’S WAR IN UKRAINE CREATES AND DESCRIBES NEW RUSSIA- WEST CONFLICT

Jyrki Terva

The presentation made by Jyrki Terva in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw-7vg&t=3263s> starting from 4:09:00.

EVGENY MESSNER'S THEORY OF SUBVERSION WAR VS. HYBRID WARFARE

Juha Wihersaari

The presentation made by Juha Wihersaari in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 4:44:00.

Introduction

Russian Colonel Evgeny Eduardovich Messner was remarkable Russian military thinker who has significant influence on Russian hybrid warfare. He was a trailblazer in the theory of modern warfare. He created in 1959 his theory of subversion war. It was so radical, that next similar theory was born in the USA first 30 years later.

Messner's theory of subversion war became known as late as in the beginning of this century. He was the only notable Russian military thinker who belonged to white officers. That is why he lived decades under the radar in Argentina and never in Soviet Union. Messner's theory of subversion war is usually referred as a root of hybrid warfare. However, more accurate exploration reveals that *subversion war is de facto hybrid warfare without modern technology*.

Biography and Writings of Evgeny Messner

Messner was born in 1891 in Odessa, where he spent his childhood and youth. He started his physics studies in 1909 in the Novorossisk university, but after the first year he decided to fulfill his dream to become an officer and enrolled to army. After graduation from Artillery Academy in 1912 he started his officer career in the 15th Artillery Brigade, where he served next four years, including the first years of the First World War. In 1916 Messner was ordered to Nikolayev War Academy. After graduation in February 1917 he was ordered to serve in the 15th Infantry Division. Messner was division's last Chief of staff and he served on that post until demobilization of the 15th Infantry Division in year 1918.¹

After demobilization, he joined the White Army and fought the Red Army in Ukraine during years 1918-1920. At the end of his war path in Russia Messner served as division's Chief of staff in the Wrangel Army and was promoted to colonel.²

In 1920 he emigrated to Beograd in Yugoslavia with several other white officers from Russia. In Beograd, he started writing about theory of war, taught emigrated Russian officers in higher military courses and defended his doctoral thesis in military sciences.

¹ Fridman, Ofer: *Russian Hybrid Warfare, Resurgence and Politicisation*, Oxford University Press, Oxford, 2018, p. 49-51

² Fridman (2018), p. 51

In the Second World War Messner served in Wermacht's propaganda (e.g. psychological operations) posts in the Balkans.³

After the capitulation of Germany, Messner emigrated again; this time to Buenos Aires, Argentina, where a lot of Germans and, also Russian officers, emigrated to. In Buenos Aires, he founded South American branch of the Institute for the research of war and peace in Buenos Aires and continued his career as military thinker and writer. Messner died in Buenos Aires in 1974.⁴

Messner had two active writing periods in his life. First period was between the world wars. It started in 1925 and ended in 1939, peak being from 1937 to 1938. During this period, he wrote about service and ethics of officer, art of war, Spanish Civil War, actual and potential crisis. The second active period was between 1959 and 1974 when Messner developed his famous theory of subversion war. Based on open source information Messner's writings were first found in Russia at the end of 1990 and only after that in the Western World.⁵

Undoubtedly Evgeny Messner was very talented, hardworking officer and researcher, but the secret of his open-minded military thinking laid on his exceptionally broad experience of psychological operations in multiethnic, multinational, multilingual and sectarian wars in Balkans and Russia.

Theory of Subversion War among other theories of war

The new element in Messner's theory of subversion war is information, which Messner defined the fourth dimension of warfare already in 1959. Western and Russian war theorists made the same conclusion much later. The most similar theory is the fourth-generation warfare, which was created by William S. Lind and group of US Marine Corps officers in 1989.⁶ Another developer of the theory of the 4th generation warfare was US Marine Corps Colonel Thomas X. Hammes. He wrote his first analysis in 1994.⁷ It is interesting an observation that all the developers of 4th generation warfare theory are from US Marine Corps, where officers serve all over the world and are more familiar with people from different cultures and religions than in other services.

On the Russian side the first warfare theory in which information had special importance, was the theory of the 6th generation warfare.⁸ It was developed in 1999 by Russian Major General Vladimir Slipchenko and described net-centric warfare e.g. the "informatization" of conventional warfare and the development of precision strike systems. Slipchenko looked back at Ogarkov's "revolution in military affairs" with "weapons based on new physical principles" and saw "Desert Storm" as a first indication of the appearance of such capabilities.⁹ The sixth generation was basically "only" an evolution version in the line of conventional warfare theories. Equivalent

³ Fridman (2018), p. 51-52

⁴ Fridman, (2018), p. 52

⁵ Месснер, Е,Э.: *Хочешь мира, победи мятежевойну*, Русский путь, Москва, 2005, p. 6-7

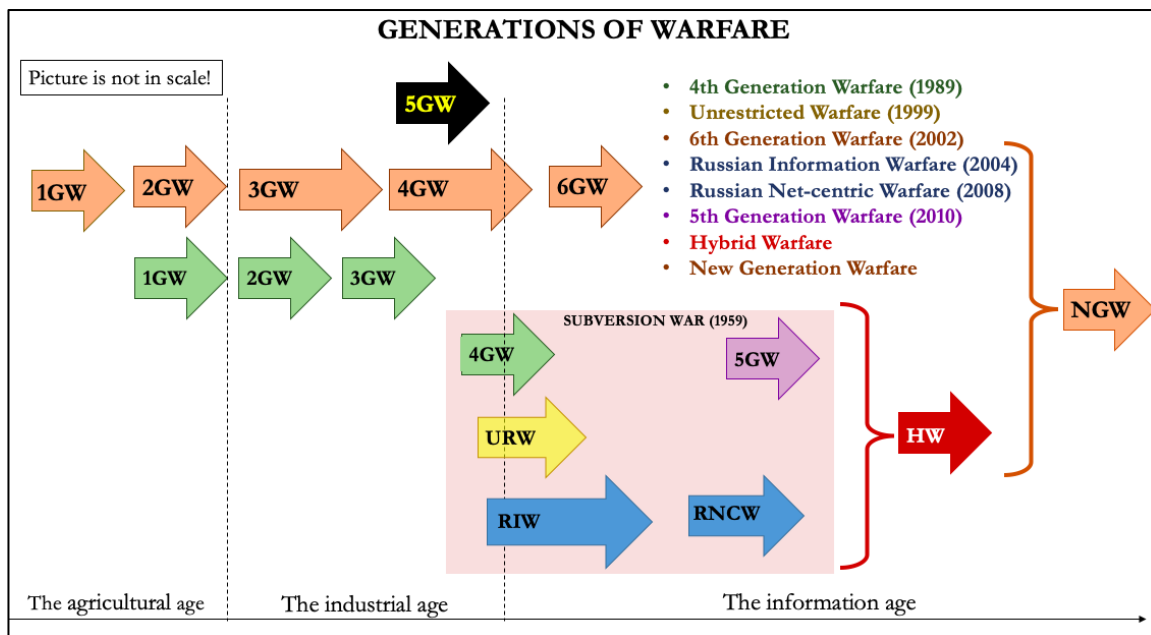
⁶ Lind, William S & Nightengale, Keith & Schmitt, John F. & Sutton, Joseph W. & Wilson, Gary I.: *The Changing Face of War: Into the Fourt Generation*, Marine Corps Gazette, October 1989

⁷ Hammes, Thomas X.: *The Evolution of War: The Fourth Generation*, Marine Corps Gazette, September, 1994

⁸ Слипченко, Владимир Иванович: *Войны шестого поколения. Оружие и военное искусство будущего*, Вече, 2002

⁹ Kipp, Jacob W.: *Russian Sixth Generation Warfare and Recent Developments*, Eurasia Daily Monitor, Volume: 9, Issue: 17, 25.1.2012

new theories to subversion war and the 4th generation warfare appeared in Russia first in connection to the annexation of Crimea.



Picture 1. Soviet Forces in the Western TVD after the collapse of the SU

After the theory of the 4th generation of war, several theories in which information plays key role and which are considered as roots of hybrid warfare appeared. In 1999 two Chinese Colonels Qiao Liang and Wang Xiangsui published their book about Unrestricted Warfare.¹⁰ Eleven years later American psychologist Daniel H. Abbot defined for the first time the theory of 5th generation warfare.¹¹ In Russia studying of information as a crucial part of warfare started in the first decade of 21st century. Igor Panarin, Russian military thinker and retired colonel with KGB background, started to process theory of Russian information warfare. After him Russian philosopher and political analyst Aleksandr Dugin defined Russian net-centric warfare.

Hybrid warfare appeared into military discourse in 2002, when William J. Nemeth used the term in his Chechnya War analysis.¹² However, hybrid warfare had become public knowledge originally, when Frank Hoffman analyzed Hezbollah actions in Lebanon Second War in 2006.¹³

Russian new generation warfare is assessed to be the combination of 6th generation warfare and hybrid warfare.¹⁴ Even broader definition can be found in writings of Pakistani officers and war scholars. It is based on the theories of 4th and 5th gener-

¹⁰ Qiao, Liang & Wang, Xiangsui: *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, February, 1999

¹¹ Abbot, Daniel H.: *The Handbook of 5GW*, Nimble Books LLC, Ann Arbor, 2010

¹² Nemeth, William J.: *Future war and Chechnya: a case for hybrid warfare*, Naval Postgraduate School, California, Monterey, 2002, Nemeth was at that time major in US Marine Corps.

¹³ Hoffman, Frank: *Lessons from Lebanon. Hezbollah and Hybrid War*, The Foreign Policy Research Institute (FPRI), 2006, Hoffman was at that time Lieutenant Colonel in US Marine Corps.

¹⁴ Fridman, (2018), p. 141-142

ation warfares and according to it hybrid warfare covers all the warfare generations from 1st to 5th.¹⁵

Subversion war vs. 4th generation warfare

In these first warfare theories where information is the most important element and which were revolutionary in comparison to previous theories of conventional warfare, certain similarities and differences can be seen. Both theories were developed by analyzing the same period which started after the Second world war. Naturally Messner's time window was narrower, but conclusions are very similar.

After the Second world war all wars that begun were small wars, not big. According to theory of subversion war one big war was split into small wars and these small proxy wars were led by super powers. In the theory of 4th generation warfare small wars were part of de-colonization process, in which newborn states' borders were too artificial to survive. Especially inter-religious collisions and poverty caused liberation movements to be born and escalation into liberation or civil wars. In many cases Soviet Union supported these kinds of movements.

Messner's point of view was perhaps more objective, because he analyzed small wars being outside of alliances. Lind and his group of U.S. Marine Corps officers tried to foresee new threats for USA. Due to this they had more defenders' point of view. However, the big conclusion was the same – information has become the fourth domain of warfare. In subversion war information is used in order to destroy adversary nation's will to fight and typically super power is behind the local attacker in civil war. In fourth generation warfare weaker attacker's ultimate target is to influence super power's political leadership, which is afraid of next elections and give up under public pressure. It usually takes 20-30 years to be able to gain that kind of pressure among adversary's nation¹⁶. Messner had similar time frame in his last writing when he evaluates time for cultural revolution¹⁷.

Lind and his group assessed that future wars are wars between cultures. In Western world it would mean war between Christian and Islamic culture.¹⁸ Messner assessed Cold War situation basically the same way, but he did not use word culture. Cold War was war between [Christian] West and Communist Soviet Union. Taking into consideration that atheism was a dogma and had a status of religion in Soviet Union, we can define Cold War as war between Christianity and Atheism. According to Russian war scholars Russian hybrid war is war between Russian and Western culture¹⁹ e.g., between Orthodox Christianity and European Ecumenical Christianity.

¹⁵ Nisar, Maaz: *5 GW and Hybrid Warfare its implications and response options*, Escola de Comando e Estado-Maior do Exército, (School of Command and General Staff of the Army), Rio de Janeiro, 2018, p. 22-27

¹⁶ Hammes, Thomas X.: *Insurgency: Modern Warfare Evolves into a Fourth Generation*, Strategic Forum, Institute for National Strategy Studies (INSS), No. 214, January, 2005, p-6-7

¹⁷ Месснер, Е.Э.: *Хочешь мира, победи мятежвойну*, Русский путь, Военный университет, Москва, 2005, p.157-161

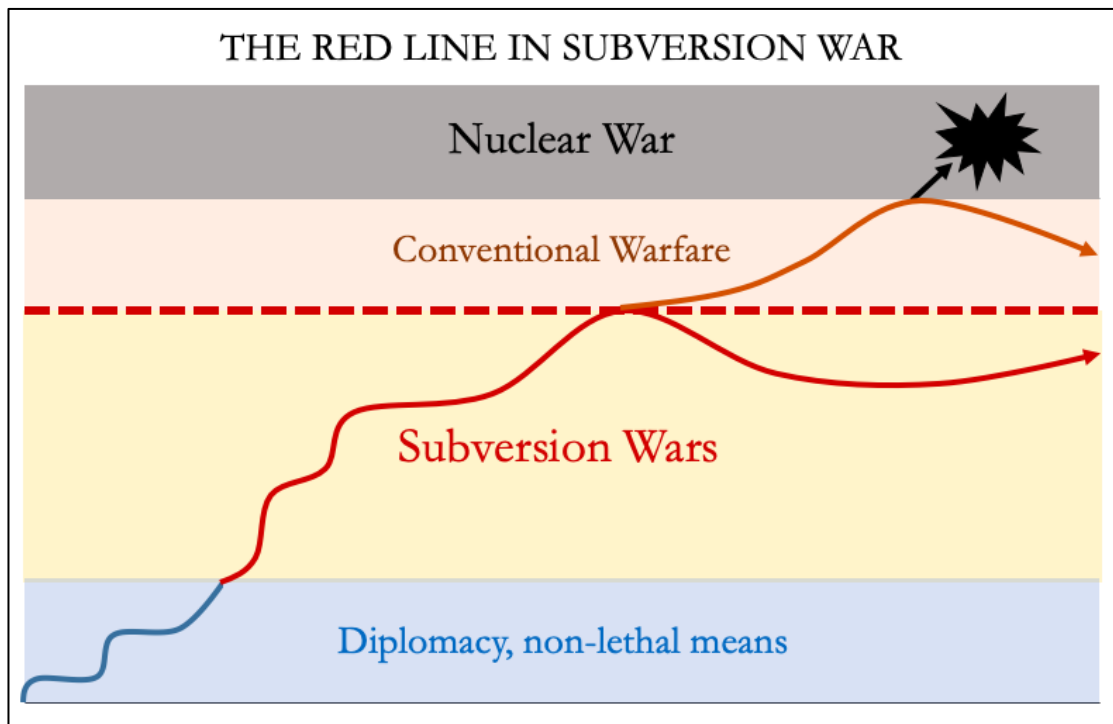
¹⁸ Lind, William S. & Schmitt, John F. & Wilson, Gary I.: *Fourth Generation Warfare: Another Look*, Marine Corps Gazette, December 1994, p.36

¹⁹ Баргош, Александр Александрович: *Стратегия и контрстратегия гибридной войны*, Военная Мысль, No 10, 2018, p. 11

In both theories importance of information increased radically with time. In his first writing in 1994 Hammes defined information operations only to support military campaigns in fourth generation warfare. Thirteen years later he assessed the opposite: military operations support information campaign, which has the key role in fourth generation wars. The same change in information's importance is seen in Messner's analysis from 1959 to 1971.

The Red Line in Subversion War

In addition to rise of information into the 4th dimension of warfare the reason for the born of subversion war is critical. Since the beginning of the peace treaty of Westphalia there has been distinct line between war and peace. After Second World War nations were tired of fighting and two superpowers had brand new overwhelming nuclear weapon, which made them almost invulnerable. Only another nuclear power posed threat. In his analysis Messner came to two crucial conclusions: 1) Only superpowers or alliances can conduct war; 2) War between superpowers could easily escalate into nuclear war which would destroy the whole world.



Picture 2. The red line in subversion war

In order to avoid this path to self-destruction superpowers started to conduct wars in form of small wars. For superpower the best and the safest way was to avoid open conventional war and instead organize several proxy wars, and not be official party. This is one of the most important principles in hybrid warfare, not being official party in a war. Cyber warfare and use of private military companies are examples of this rule.

Parameters of Hybrid Warfare

There are four elements in hybrid warfare: modes of warfare, dimensions, tactics and strategy. However, the definition of hybrid warfare is determined merely by modes

and dimensions. In his master thesis Manon van Tienhoven based his summary definition on the three distinguished hybrid warfare scholars: Frank Hofmann, Russel W. Glenn and John J. McCuen.²⁰ They all are Americans with military background.

Aleksander Bartosh is a Russian warfare scholar and retired colonel. He writes actively and his articles regularly publish for example in Voennaja Mysl and in Voenno-Promyshlennyi Kurier. At the moment he is the most authoritative Russian war scholar studying hybrid warfare.

Modes of Hybrid Warfare

The three hybrid warfare scholars together identify eight different modes of warfare: conventional capabilities, irregular tactics, terrorism, criminal activities, political, economic, information, and social. These four can be divided into the physical modes of warfare, the first four; and the conceptual modes of warfare, the latter four.²¹ This definition is later referred as basic definition.

Modes	Messner	Bartosh	Definition
(Conventional warfare)		(X)	X
Irregular warfare	X	X	X
Terrorism	X	X	X
Criminal activity	X	X	X
Political means	X	X	X
Economical means	X	X	X
Social means	X	X	X
Information means	X	X	X

Picture 3. The modes of hybrid warfare

Conventional warfare is one of the contested concepts used to describe hybrid warfare, since conventional capabilities are associated with the military capabilities of the state. This definition includes the following three indicators: 1) the usage of army, navy, and air force; 2) joint combined arms maneuver warfare; 3) firepower intensive conflicts.²² Bartosh argued that most crucial difference between conventional and hybrid warfare lies in the use of armed forces. In conventional war armed forces are used to defeat enemy, but in hybrid warfare armed forces are used 1) together with non-military modes such as information and psychological operations and ruining enemy's economy; 2) to isolate and besiege enemy in war of attrition in order to break enemy's will to fight; 3) together with cyber operations; 4) as a tool of traditional diplomacy in anti-terrorist campaign.²³ As explained above, already in 1959 Messner had come to the

²⁰ Hoffman served in the US Marine Corps, but Glenn and McCuen in the US Army.

²¹ Van Tienhoven, Manon: *Identifying Hybrid Warfare*, Leiden University, Crisis and Security Management, Political Administration, Master Thesis, 2016, p. 17

²² Van Tienhoven (2016), p. 19

²³ Бартош, No 10 (2018), p. 6

conclusion that conventional warfare does not at all belong to subversion war.²⁴ Both Bartosh and Messner write about warfare of state. In Bartosh's definition second point is close to conventional use of armed forces, but Messner is restricted on proxy war without attackers' straight connections to subversion war.

According to the basic definition three indicators have been derived to identify *irregular warfare*: 1) guerrilla tactics, 2) insurgency, 3) credibility and legitimatization.²⁵ When Bartosh describes strategy of hybrid warfare he writes "on the certain moment the attacker begins armed operations by using local insurgents, mercenaries and private military companies. Armed forces of the attacker state have only supportive role".²⁶ In Messner's first analysis of subversion war in 1959 there are two specified forms of irregular warfare. Partisan troops, which are mobilized among local people in enemy's rear area and uprising.²⁷ Ten years later he does not give them major role.

Terrorism is the third concept that is used to describe hybrid warfare. The indicators of this mode of warfare are: 1) an act of violence that produces widespread disproportionate emotional reactions such as fear and anxiety, 2) violence is systematically usually directed against symbolic targets, 3) the violence conveys messages and threats in order to communicate and gain social control.²⁸ Bartosh writes quite thinly about the use of terrorism in hybrid warfare. He, of course, sees terrorism as part of hybrid warfare, but warns that international terrorism is difficult to control.²⁹ For terrorism it is better to use capable fifth column³⁰, which is much more reliable and easier to control. Messner has the same understanding. Terrorism is an essential part of subversion war. According to him terror acts are conducted 1) by small special operation force groups, which are transported to enemy's rear area; 2) by groups of local fifth column, which are capable for terror acts.³¹

To *criminal activities* belong the following: 1) smuggling, 2) illicit transfers of advanced weapons, 3) exploitation of gang networks.³² Bartosh does not deeply discourse criminal activities, but sees organized crime as elementary mode of hybrid warfare.³³ His definition matches the basic definition, because organized crime, beyond any doubt covers all the sectors of the basic definition. In Messner's latest analysis of subversion war he emphasizes criminal activity and terrorism as main modes of subversion war.³⁴

According to the basic definition, the *political means* as a mode of warfare, are the intended use of political means to compel an opponent to do one's will, based on hostile intent.³⁵ Bartosh counts political means as one of the modes of hybrid warfare.³⁶

²⁴ Месснер, Е.Э.: *Хочешь мира, победи мятежевойну*, Русский путь, Военный университет, Москва, 2005, р. 90-91

²⁵ Van Tienhoven (2016), p. 19

²⁶ Бартош, No 10 (2018), p. 4

²⁷ Месснер (2005), p. 91

²⁸ Van Tienhoven (2016), p. 19

²⁹ Бартош, Александр Александрович: *Трение и износ гибридной войны*, Военная Мысль, No 1, 2018, p. 8-9

³⁰ Бартош, No 10 (2018), p. 4

³¹ Месснер (2005), p. 91

³² Van Tienhoven (2016), p. 19

³³ Бартош, No 10 (2018), p. 6

³⁴ Месснер (2005), p. 162

³⁵ Van Tienhoven (2016), p. 20

³⁶ Бартош, No 1 (2018), p. 11

Messner assesses political means as a mode of subversion war in each of his writings beginning from 1959.³⁷ Traditionally political means are a matter of course.

In the basic definition the *economic means* as a mode of warfare as the use of, or the threat to use, economic means against a country in order to weaken its economy and thereby reduce its political and military power.³⁸ Bartosh states for example that on the strategic level hybrid warfare includes also manipulation of enemy's economy and finances.³⁹ In Messner's analysis economic means have same weight as political means. They are seen a mode of subversion war in each of his writings beginning from 1959 in each of his writings beginning from 1959.⁴⁰

Basic definition of *information means* as a mode of warfare is old. Van Tienhoven decided to use the definition of the U.S. Department of Defense from 1996: Actions taken to achieve information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.⁴¹

According to Russian definition information warfare consists of two types: 1) information-psychological warfare (to affect the personnel of the armed forces and the population), which is conducted under conditions of natural competition, i.e. permanently. This is close to western definition for *information warfare*, 2) information-technology warfare (to affect technical systems which receive, collect, process and transmit information), which is conducted during wars and armed conflicts. *Cyber warfare* covers information-technology warfare well.⁴²

Bartosh writes that strategic goal of information warfare is to influence on ideology and for this reason it is the most important mode in the area of culture and ideology.⁴³ The most important goal of strategy of subversion war is to psychically conquer enemy's nation e.g. discredit enemy's ideological basis, convince enemy attacker's ideology is superior and make enemy adapt attacker's ideology.⁴⁴

Social means as a mode of warfare determines the support and control of three groups that are: 1) conflict zone population, 2) home front population, 3) international community.⁴⁵ In Bartosh's writings social means are not emphasized but the point is easily seen in his writings.⁴⁶ In subversion war psychological support and control are key elements.⁴⁷

³⁷ Месснер (2005), p. 74, 76, 103, 109, 114, 135

³⁸ Van Tienhoven (2016), p. 20

³⁹ Бартош, No 10 (2018), p. 5

⁴⁰ Месснер (2005), p. 74, 76, 103, 109, 114, 135

⁴¹ Van Tienhoven (2016), p. 20

⁴² Giles, Keir: *Handbook of Russian Information Warfare*, NATO Defence College, 2016, p. 9

⁴³ Бартош, No 10 (2018), p. 10

⁴⁴ Месснер (2005), p. 132

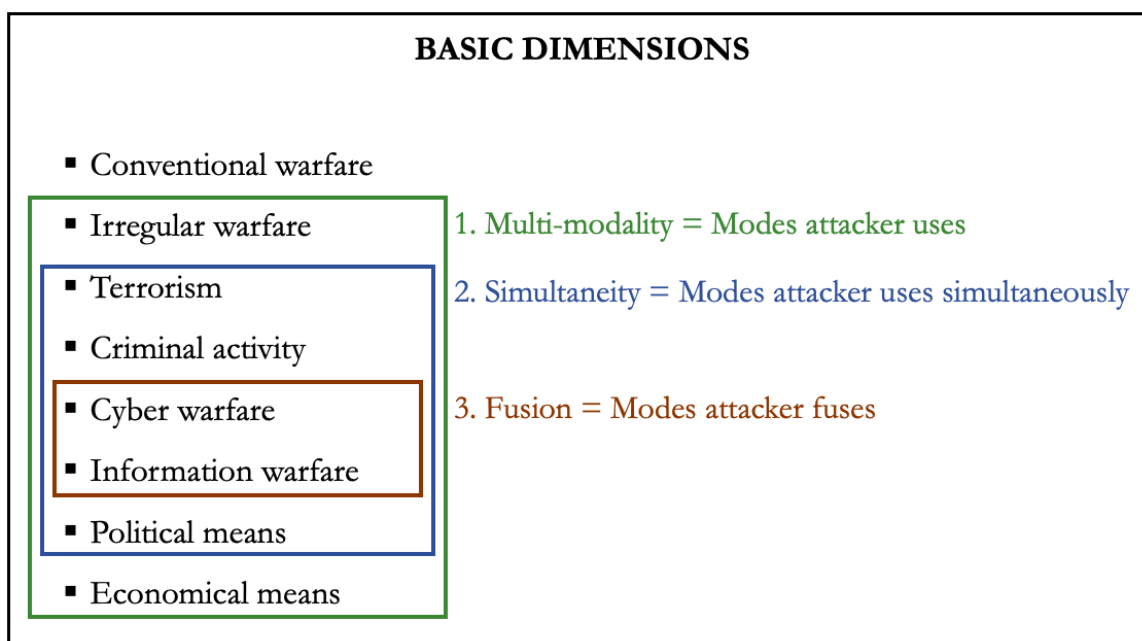
⁴⁵ Van Tienhoven (2016), p. 20

⁴⁶ Бартош, No 10 (2018), p. 13

⁴⁷ Месснер (2005), p. 131-132

Dimensions of Hybrid Warfare

Per the basic definition, there are four dimensions of hybrid warfare mentioned in the basic definition: multi-modality, simultaneity, fusion, and catastrophic. First, *multi-modality* can be defined as the extent to which an adversary can mix and apply different modes of warfare. Secondly, *simultaneity* is the extent to which an adversary applies simultaneously different modes of warfare. Thirdly, *fusion* means the extent to which an adversary fuses the different modes of warfare toward its own advantage.⁴⁸



Picture 4. The basic dimensions of hybrid warfare

Fourthly, *catastrophic* can be perceived as the impact on the environment: Any natural or man-made incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions.⁴⁹

Per Bartosh in hybrid warfare could be seen man-made technological and ecological catastrophes on civil or military objects, massive terrorist attacks on traffic connections (e.g. large air and sea ports) causing a lot of casualties, and assassinations of political leaders, which could break enemy nation's will to continue fighting.⁵⁰

Messner deals critically with man-made catastrophes but he does not judge them. For example, by destroying dam with a (nuclear) bomb and drowning the whole town could cause more psychological harm than physical damages to enemy. In worst case the act only makes enemy's nation angrier and more willing to fight. However, Messner disapproves nuclear weapons. He stressed that nuclear strike is too disgusting an

⁴⁸ Van Tienhoven (2016), p. 16-17

⁴⁹ Van Tienhoven (2016), p. 16-17

⁵⁰ Бартош, No 1 (2018), p. 10

act: Even own people usually reject it and it backfires. More important thing of course is judgment from international community.⁵¹

On the base of the above made analysis of modes in Messner's writings, two first dimensions, multi-modality, and simultaneity, are used in subversion war.

Conclusion

Messner's theory of subversion war fulfills basic criteria of hybrid warfare. Theory of subversion war is written 1959 and beyond any doubt it is the first theory that covers above mentioned criteria. After this conclusion will be researched how and if the theory of subversion war is related to theories of earlier (Soviet) war scholars and to later theories which are connected hybrid warfare.

⁵¹ Месснер (2005), p. 131-132

RUSSIA'S REVOLUTION IN INTELLIGENCE AFFAIRS¹

Oscar Jonsson (and Bryce Johnston - absent from the seminar)²

The presentation made by Oscar Jonsson in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 5:57:30.

Artificial Intelligence (AI) is seen as a critical technology by the Russian leadership in transforming the nature of great power competition and military conflict. As AI is primarily an analysis, pattern-recognition and decision-making tool, this paper investigates how it can impact Russian intelligence affairs. This paper argues that the application of AI will generate such an impact in the speed, breadth, depth, and decentralization of intelligence affairs that it will constitute a revolution in intelligence affairs. AI will do so by discovering patterns hitherto unseen, by collecting and analyzing unprecedented amounts of data, and by being able to automate and decentralize collection and analysis. Whilst the technology and desire for such revolution is already in place, organizational and doctrinal change have not been implemented to such a degree to confirm that a revolution in Russian intelligence affairs has taken place. Nonetheless, the tipping point is rapidly approaching.

Introduction

The saying “knowledge is power” is attributed to Sir Francis Bacon and runs to the core of intelligence work. While the statement is not completely correct³, it underlines the importance of knowledge in strategy. Any way of increasing your knowledge about an enemy - his plans, his technology, and his weaknesses - offers the opportunity to set oneself ahead. This underlines the core business of intelligence affairs. This paper sets out to investigate how AI can impact Russia’s intelligence and security services.

As states transitioned from industrial economies to digital ones, the character of great power competition changed as well. Rather than solely being in the hands of governments and armed forces, large parts of geopolitical confrontation are being played out in the digital and private domain.⁴ The modern economy runs on innovation,

¹ In this footnote 1 the “publication” refers to this article:



This publication was funded by the Russia Strategic Initiative, U.S. European Command. The views expressed in this publication do not necessarily represent the views of the Department of Defense or the United States government.

² Bryce Johnston is a West Point graduate and Fulbright scholar. He holds a MSc in International Development from the IE University and a BS from the United States Military Academy. He currently serves as an officer in the U.S. Army TRADOC. The views expressed in this article do not necessarily represent the views of the U.S. Army or the United States.

³ Power is more about how you leverage that knowledge and to influence outcomes rather than just to possess knowledge.

⁴ Jonsson, O., et al. (2020). *The New Digital Domain: How the Pandemic Reshaped Geopolitics, the Social Contract and Technological Sovereignty*, Madrid: Center for the Governance of Change. <<https://docs.ie.edu/cgc/IE-CGC-The-New-Digital-Domain.pdf>>, (accessed 15 March 2022).

knowledge and data rather than the control of territory and resources. Therefore, the “process of collecting and organizing information is now a tremendous source of economic, political and cultural power. Data makes us more malleable, easier to predict, and extremely prone to influence”.⁵ This underlines the rise of Big Tech-companies who are relying on vast amounts of data to influence behavior (mostly consumer behavior). The data economy poses both notable challenges for how intelligence services should adapt in the 21st Century, but also opportunities to influence an adversary.

Decades ago, the key difficulty in intelligence affairs was information scarcity. Adversaries, such as the Soviet Union, were seeking to operate in the dark while traveling and foreign media was restricted. Human intelligence assets, such as illegalists, took time and effort to recruit as well as to use, while counterintelligence entailed closely monitoring movements of diplomats and other dignitaries. Intelligence affairs was difficult, costly and analysts had to make do with the limited amount of information extracted.

Today, the problem is the opposite. The virtual explosion of open-source material coupled with the increasing capabilities have turned the challenge from accessing more information to narrowing what information to use. It is a classic case of when the amount of information crosses over to noise, and only makes analysis more difficult. The key potential game-changer in the intelligence domain that can mitigate this is the use of Artificial Intelligence (AI). It offers unparalleled opportunities to reshape parts of the classic intelligence cycle to improve the OODA-loop (Observe, Orient, Decide, Act) and for offensive operations.

The Russian President Vladimir Putin stated that “*whoever becomes the leader in [AI] will become the ruler of the world*”.⁶ This statement has often been blown out of proportion; he was speaking for school children rather than his senior strategists. However, the importance of AI for the Russian leadership is genuine.

Russia is providing the largest threat to the European security order since the collapse of the Soviet Union and is in its essence a security and intelligence-led state. Many of its key leaders have their background in the services.⁷ Moreover, the institutions and processes defining Russia’s threat perception and grand strategy are heavily defined by the security and intelligence perspective⁸.

Nonetheless, research has so far, in our opinion, failed to grasp the full potential of AI in intelligence affairs. Existing studies are lacking by: 1) overlooking the implications of AI or only applying it in a narrow sections of intelligence affairs⁹,2) focusing

⁵ Smyth, S. (2019). “The Facebook Conundrum: Is it Time to Usher in a New Era of Regulation for Big Tech?”, *International Journal of Cyber Criminology*, 13(2), p.578.

⁶ RT. (2017). “Whoever leads in AI will rule the World: Putin to Russian children on Knowledge Day”, 1 September, <<https://www.rt.com/news/401731-ai-rule-world-putin/>>. (accessed 15 March 2022).

⁷ Meister, S. (2019). “The Domestic and Foreign Policy Nexus”. In Kanet, R. (Ed.), *Routledge Handbook of Russian Security*. Milton Park: Routledge.

⁸ Bacon, E. (2019). “The Security Council and Security Decision-Making”. In Kanet, R. (Ed.), *Routledge Handbook of Russian Security*. Milton Park: Routledge.

⁹ Allen, G & Chan, T. (2017). “Artificial intelligence and national security”. *Belfer Center for Science and International Affairs*, July <<https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>> (accessed 15 March 2022); Degaut, M. (2016). “Spies and policymakers: Intelligence in the information age.” *Intelligence and National Security*, 31(4), pp. 509-531; Thornton, R & Miron, M. (2020) “Towards the ‘third revolution in military affairs’ the Russian military’s use of AI-enabled cyber warfare” *The RUSI Journal*, 165(3), pp. 12-21; Kurliak, M. (2018). “Applying the Revolution in Military Affairs to Intelligence”. *The Journal of*

on how it can entail change only within the current system (that is to say, an evolution and not a revolution)¹⁰, 3) failing to account of the blurring sectors of private and public fusion of intelligence¹¹, 4) not investigating the Russian perspective on AI and intelligence collection.¹² As argued by Fink, “while there is much breathless media coverage of specific military systems with features of AI and autonomy, more serious and comprehensive analysis remains scarce”.¹³

However, the gaps are also understandable as the analysis of AI and its impact in intelligence affairs is fraught with difficulties. Not only is the vast share of AI’s promise ahead of us, but intelligence is the most obscure business which makes assessing its impact even harder. Whilst discussions on military theory, military strategy and operations are characterized with a relatively high degree of transparency in Russia, the reverse is true for intelligence services.

This does not lessen the need to understand the topic but rather the opposite. Nonetheless, it decreases the degree of certainty with which conclusions can be drawn. With this caveat, this paper will set out answer the question of *how will AI revolutionize Russia’s intelligence affairs?* It will do so by relying on a fourfold combination of: existing research on the revolution in intelligence affairs (mostly Western-centric); the current frontier of AI-development; the views of Russian theorists and doctrines; and lastly, the available material on the Russian application of AI. Put together, this seeks to allow for an illustration and discussion of the current state of affairs.

The State of Intelligence Affairs

In the past decade, intelligence organizations have faced shifting geopolitical tensions and rapid technological change. While Western intelligence has mostly focused on their traditional role of providing actionable insights to decisionmakers, Russian intelligence and security services have often taken a more active role in trying to shape world politics.

Intelligence, Conflict, and Warfare, 1(1); Gioe, D, Goodman, M. S. & Stevens, T. (2020). “Intelligence in the Cyber Era: Evolution or Revolution?” *Political Science Quarterly*, 135(2), pp. 223-224.

¹⁰ Boelens, M. (2017). “The Revolution in Intelligence Affairs: Problem Solved?.” *Perspectives on Military Intelligence from the First World War to Mali*. TMC Asser Press, pp.119-143; Payne, K. (2018). “Artificial Intelligence: A Revolution in Strategic affairs?” *Survival*, 60(4), pp. 7-32; Uri B & McDermott, R. (2008). “Change the Analyst and Not the System: A Different Approach to Intelligence Reform”. *Foreign Policy Analysis*, 4(2), pp. 127–145; Duyvesteyn I, De Jong, B. & van Reijn, J. (2015). *The Future of Intelligence*. London-New York: Taylor and Francis.

¹¹ Barger, D. (2005). “Toward a Revolution in Intelligence Affairs.” *Rand Corporation*, <https://www.rand.org/pubs/technical_reports/TR242.html>, (accessed 15 March 2022); Lahneman, W. (2007). “Is a revolution in intelligence affairs occurring?” *International Journal of Intelligence and Counterintelligence*, 20(1), pp. 1-17; Brown, Z. (2018). “Adaptive Intelligence for an Uncertain Age.” *Defense Threat Reduction Agency*.

¹² Vinci, A. (2020) “The Coming Revolution in Intelligence Affairs.” *Foreign Affairs*, 31 August, <<https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs>>, (accessed 15 March 2022); The notable exceptions that investigates Russia is Morgus, R., 2019, “The Spread of Russia’s Digital Authoritarianism”, in Wright (Ed.), *Artificial Intelligence, China, Russia, and the Global Order*, Maxwell: Air University Press; as well as Edmonds, J. et al (2021) “Artificial Intelligence and Autonomy in Russia”, Center for Naval Analysis, May, <https://www.cna.org/CNA_files/centers/CNA/sppp/rsp/russia-ai/Russia-Artificial-Intelligence-Autonomy-Putin-Military.pdf> (accessed 14 January 2022); For China, see Kania, E. “Chinese Military Innovation in the AI Revolution.” (2019). *The RUSI Journal*, 164(5-6), pp. 26-34.

¹³ Fink, A. 2021. “Russian Thinking on the Role of AI in Future Warfare”, *NATO Defense College*, 8 November, <<https://www.ndc.nato.int/research/research.php?icode=712>>, (accessed 15 March 2022)

The Global War on Terror led Western intelligence services to increase both the scope and intensity of their intelligence collection, but not always for greater insights. An illustrative example of U.S. intelligence efforts in Iraq and Afghanistan is that they collected biometric data without a clear idea of how it could add value.¹⁴ While the U.S. had access to hundreds of terabytes of biometric data in the region, they could not quite use the data in its raw form. Intelligence work has often been compared to finding a needle in a haystack, and in this case, their collection efforts only succeeded in increasing the size of the haystack.

Another example comes from the Pentagon's Joint Improvised Explosive Device Defeat Organization (JIEDDO), which sought to use big data to tackle the application of improvised-explosive devices in Iraq and Afghanistan. Even with the billions of dollars spent on acquiring and analyzing data, the Pentagon ran into the limitations to what degree that data could support decision-making.¹⁵ Despite the wealth of data available to them, the organization lacked the ability to make sense of it in an actionable manner.¹⁶

Today, the priority for Western intelligence agencies has returned to great power competition. Governments, organizations, and private citizens can capture more data than ever before. The intelligence cycle relies heavily on human labor and recent increases in productivity have been due to technological advances that allow intelligence professionals to cycle through this process quicker. Even with these improvements, the human analysts may not be quick enough to deal with the myriad threats posed in an increasingly connected world. Shifts in technology have over the last two decades have increased the amount of data available from a multitude of sources: cheaper satellites, more powerful processors, and smaller batteries have allowed for the proliferation of sensors in space and on the Earth.

Intelligence services face several challenges as they attempt to remain relevant in the 21st Century. Manpower shortages and resource constraints make it impossible to monitor all threats simultaneously. Decision-makers are also suffering from information overload.¹⁷ Even though the intelligence services have more data than ever to help make sense of complicated issues, their ability to process and disseminate this data are often limited. Finally, intelligence professionals are trying to outrace open-source information which often reduces the depth of their analysis.¹⁸ If the intelligence community hopes to remain relevant in an era of great power competition, they will need to adopt new processes and technologies that will allow them to increase the breadth, depth, and speed of their intelligence work.

¹⁴ Boone, J. (2010). "US army amasses biometric data in Afghanistan." *The Guardian*. 27 October <<https://www.theguardian.com/world/2010/oct/27/us-army-biometric-data-afghanistan>>, (accessed 15 March 2022)

¹⁵ Atherton, K. (2017). "When Big Data went to war — and lost", *Politico*. 12 October <<https://www.politico.eu/article/iraq-war-when-big-data-went-to-war-and-lost/>>, (accessed 15 March 2022)

¹⁶ Sadowski, R. 2008. "Joint Improvised Explosive Device Defeat Organization: Anomaly or Future Roadmap.", *Army War College* <<https://apps.dtic.mil/sti/citations/ADA479728>>, (accessed 15 March 2022).

¹⁷ Winter, D. (2019). "Too much information? The new challenge for decision-makers," *Financial Times*. 13 December, <<https://www.ft.com/content/407f74b2-dfa8-11e9-b8e0-026e07cbe5b4>>, (accessed 15 March 2022).

¹⁸ Zegart, A & Morell, M. (2019). "Spies, Lies, and Algorithms: Why US Intelligence Agencies Must Adapt or Fail. Foreign Affairs", June, <<https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms>>, (accessed 15 March 2022).

The Intelligence Cycle

The intelligence cycle reflects a quite centralized and highly standardized process of intelligence affairs which serves as an illustration of the constituent parts of intelligence. The most common representation involves six steps: planning, collection, processing, analysis, dissemination, and evaluation. The origins of the cycle first took shape in the post-war period when management sciences sought to standardize corporate procedures to make them more efficient. By standardizing the intelligence cycle, Western intelligence organizations increased scalability and benefited from improved efficiency and interoperability as analysts within different programs had a common language through which they could communicate.

This standardization also affects the kinds of information that the intelligence community seeks. According to the office of the Director of National Intelligence for the United States, the main sources of information are classified into six types: signals intelligence (SIGINT), images intelligence (IMINT), measurement and signature intelligence (MASINT), human intelligence (HUMINT), open-source intelligence (OSINT), and geospatial (GEOINT). In most Western states, intelligence organizations are centered on one of these six types of intelligence so that they could gain from the benefits of specialization. While this made them effective at handling their specific type of information, it made it difficult for agencies to collaborate and share information across the INT-disciplines. The failure to share information was cited in the 9/11 Commission Report as a main factor for why the United States failed to thwart the attacks on the World Trade Center and the Pentagon. For instance, Zegart showed how before the attack, the efforts to focus on the rising threat of terrorism did not translate to the organizational changes necessary to prepare agencies.¹⁹ Information sharing has improved today, but the volume of data and the increased pace of global events has stretched the limits of human ability.

Artificial Intelligence (AI)

What AI consist of is, like any other important concept, disputed. It consists of a myriad of different techniques of machine learning with pattern and image recognition, Natural Language Processing (NLP), unsupervised learning, and more. This paper will apply a general definition that captures the essence of AI as it seeks to get computers to perform tasks that have hitherto only been performed by humans.²⁰ Many of these technologies are indeed decades old. As put by Jensen:

Much of what constitutes the basket of technologies we discuss herein under the “artificial intelligence” banner is not new, we sit at an inflection point wherein AI systems—powered by rapid scientific advances and poised to receive massive, comprehensive funding from governments around the world—will be made to interact with both one another and human institutions in unprecedented fashion.²¹

¹⁹ Zegart, A. (2006) "An empirical analysis of failed intelligence reforms before September 11." *Political Science Quarterly*, 121 (2), pp.33-60.

²⁰ Ertel, W. (2018). *Introduction to Artificial Intelligence*. London: Springer.

²¹ Jensen, B. (2019). “Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence”, *International Studies Review*, 22(3), pp.528.

This paper will illustrate several examples on how AI has managed to automate cognitive tasks that once were the sole domain of humans. First, machine learning allows computers to improve their own algorithms in the face of new data. Machine learning can be supervised or unsupervised. Supervised machine learning techniques require labeled and unlabeled data. The goal is to train the computer on the labeled data so that it can develop rules that will help it sift through the unlabeled data. This kind of machine learning is useful for detecting known patterns in new datasets and performing tasks that require algorithms that can adapt to new situations.

Unsupervised machine learning finds new patterns in data. If one wants to explore a dataset but doesn't know what they should look for, this kind of machine learning model can come up with novel patterns and find relationships that a human might miss.²² This is similar to deep learning where computers create their own rules from unstructured data. By creating these rules, computers can then perform predictive analysis to determine future outcomes.

Neural networks allow computers to mimic the processes of the brain to perform complex tasks such as natural language processing and computer vision. Neural networks rely on different nodes to parse through information.²³ The connections between these nodes allow computers to complete complex tasks that approximate human abilities. Computer vision allows machines to "see" images in the same way humans can. Computers can then identify information about the image, sort it into categories, or adjust the image to fit certain criteria.²⁴ NLP allows understanding verbal and written communications without the need to manually encode every word or phrase into the computer's memory.²⁵ This enables computers to extract information from text, compile texts with similar features, and even create new text.

Beyond scraping information, AI could also be used to automate decision making processes. A study by Kahneman and Sunstein suggests that experts are often worse than algorithms at making consistent judgements.²⁶ They found that human judgment is noisy; given the same inputs and same processes, even experts produce different outputs. In many cases, algorithms could replace experts in making these judgements. By delegating these tasks to an algorithm, organizations would benefit from quicker and more consistent judgements.

While it is hard to predict exactly which domains where AI outperform humans, we can ascertain that some of this delegation is already taking place in the private sector. Bridgewater, one of the most successful hedge funds, is famous for being a machine-driven manager.²⁷ Since its inception in 1970, founder Ray Dalio would convert his thoughts to algorithms to standardize their investing process by adopting algorithmic

²² Celebi, M. (2016). *Unsupervised Learning Algorithms*. Berlin: Springer International Publishing.

²³ Schmidhuber, J. (2015) "Deep Learning in Neural Networks: An Overview." *Neural Networks*, 61, 85-117.

²⁴ Egmont-Petersen, M, de Ridder, D. & Handels, H. (2002). "Image processing with neural networks—a review." *Pattern Recognition*, 35(10), pp. 2279-2301.

²⁵ Brill, E, & Mooney, R. (1997) "An overview of empirical natural language processing." *AI Magazine*, 18(V), pp.13.

²⁶ Kahneman, D, Rosenfield, A. M., Gandhi, L. & Blaser, T. (2016). "Noise." *Harvard Business Review*, pp.38-46.

²⁷ Herbst-Bayliss, S.(2021) "Top hedge funds earn \$63.5 billion in 2020, highest in a decade: LCH data", *Reuters*, 25 January, <<https://www.reuters.com/article/us-hedgefunds-returns/top-hedge-funds-earn-63-5-billion-in-2020-highest-in-a-decade-lch-data-idUSKBN29U00R>>, (accessed 15 March 2022)

decision making throughout the company.²⁸ Bridgewater is working on automating all of the day-to-day operations of the company by handing it over to an AI who studied the habits of their employees. The Principles Operating System (PRiOS) is an attempt to migrate decision-making into algorithms that can be used to hire, fire, or promote workers.²⁹ This is but one example of a tool that could provide decentralization in intelligence affairs. Rather than work through a chain of command that has limited time and limited attention, a product could be evaluated at once and allow for analysts to create relevant products without the need for a large network of human oversight.

AI and Intelligence Affairs

The Revolution of Intelligence Affairs (RIA) is a direct analogy to the discussions of a Revolution in Military Affairs (RMA).³⁰ This paper relies on a definition of the RIA along the lines of Andrew Marshall who emphasized that an RMA was not just about technology but also requires a change in doctrines and organization³¹. Marshall emphasized the cultural aspect of such revolutions; states can have the same technology but face different military problems and use different doctrine in solving those problems. Therefore, a revolution should be analyzed in those three constituent parts.

Nonetheless, the RIA is often treated by scholars as a standalone process. First, the proliferation of information technology that propelled humanity into the information age caused scholars to look at how this technology would affect intelligence services.³² This became a focus with both the surprise of 9/11 and the subsequent Global War on Terror.³³ The most comprehensive document on the RIA leans into organizational changes rather than technological ones.³⁴ Likewise, research into how AI will affect international affairs focuses on the technologies analytical, predictive, and operational capabilities, but it does not focus on intelligence affairs.³⁵

Algorithms will be most helpful for intelligence by increasing the speed, breadth, depth and decentralization of collection and analysis. AI can perform the rote task of formatting raw data such as imagery or human intelligence reporting while combining separate streams of data into connected databases so that information on individuals or organizations can be linked across sources. Once this data is processed, AI can sift

²⁸ Dalio, R. (2018). *Principles*. New York: Simon and Schuster.

²⁹ Kopfstein, J. (2016). "An AI 'Brain' Is Micro-Managing Staff At World's Largest Hedge Fund." *Vocative*, 27 December <<https://www.vocativ.com/387603/ai-brain-bridgewater-associates/index.html>>, (accessed 15 March 2022).

³⁰ Kurliak, M. 2018. "Applying the Revolution in Military Affairs to Intelligence," *The Journal of Intelligence, Conflict, and Warfare*, 1 (1).

³¹ Marshall, A. 1993. "Some Thoughts on Military Revolutions", *Office of the Secretary of Defense*, 23 August. <<https://stacks.stanford.edu/file/druid:yx275qm3713/yx275qm3713.pdf>>, (accessed 15 March 2022).

³² Herman, M. (2001). *Intelligence Services in the Information Age*, London: Routledge; Berkowitz, B & Goodman, A. (2001). *Best Truth: Intelligence in the Information Age*. New Haven: Yale University Press.

³³ Lahneman, W. (2007). "Is a revolution in intelligence affairs occurring?" *International Journal of Intelligence and Counterintelligence*, 20(1), pp.1-17; Liaropoulos, A, "A (R)Evolution in Intelligence Affairs? In Search of a New Paradigm", *The Research Institute for European and American Studies*, 100, pp.20; Denécé, J.E. (2014). "The Revolution in Intelligence Affairs: 1989–2003," *International Journal of Intelligence and Counterintelligence*, 27(1), pp.39.

³⁴ Barger, D. *op. cit.* pp. 163; see also Payne, K. (2018). "Artificial intelligence: A Revolution in Strategic Affairs?" *Survival*, 60(5), pp.7-32.

³⁵ Cummings, M. L et. al. (2018). "Artificial Intelligence and International Affairs." *Chatham House*, <<https://www.chathamhouse.org/sites/default/files/publications/research/2018-06-14-artificial-intelligence-international-affairs-cummings-roff-cukier-parakilas-bryce.pdf>>, (accessed 15 March 2022). pp.7-18.

through the datasets to find trends and patterns. While this portion cannot be completely automated, AI could be used to help separate signals from noise so that human operators can narrow their attention to the most important insights from the data. This becomes especially important as the volume of processed data increases.

Here, we will suggest some civilian examples to illustrate the promise of AI. A solution for hospitals and doctors with limited time was suggested by Harari who imagined a solution where each person has their own AI doctor.³⁶ In his view, a small number of human medical professionals could monitor a vast network of AI doctors who provide personalized service to thousands of patients every day. This doctor would monitor their health in real time using biometric sensors and alert the patient if it detects signs of disease. Because every AI doctor would be connected to a central network, they would have access to the latest medical research as soon as it is released as well as to large repositories of data collected by other AI doctors. This would allow for patients to have access to accurate and personalized medical care at scale. This analogy could be used for intelligence collection and algorithms in general, as well as HUMINT case officers in particular to monitor GPS, biometric data and phone activity.

Intelligence systems using AI will increase the productivity of individuals so they can widen the scope of their work. Machine learning will help to collect more information in less time by automating many of the steps that human operators must go through to grab data from these sources. Automated analysis has long been viewed to classify features in models and is already being used by oncologists to identify types of cancers.³⁷ There are a variety of ways that this technology can disrupt current intelligence processes. Algorithms can process satellite images to determine if there is evidence of military mobilizations in a predetermined location.

By delegating this rote task to an algorithm, human operators can focus on collecting more relevant information for their decision makers. As it stands now, human operators must go through a long process to set up collection priorities which incentivizes them to set broad collection aims.³⁸ Instead, operators can use algorithms to determine which criteria are most important.

AI can also increase the depth and accuracy of collection. This analytical power also lends itself to a deeper reach in terms of data collection that produces insights which would be difficult for the traditional intelligence. One early example is from Target. In 2012, an advertisement algorithm from Target that assigned users a “pregnancy prediction score” had revealed a teenager was pregnant before her father knew. The interesting part is how little data Target needed to come to this conclusion, whereas

³⁶ Harari, N. (2017). "Reboot for the AI revolution." *Nature News*, 76(550), pp.324.

³⁷ Batory, D, Benavides, D. & Ruiz-Cortes, A. (2006). "Automated analysis of feature models: challenges ahead." *Communications of the ACM*, 49(12), pp.45-47; Huiyan Luo et al. (2019). "Real-Time Artificial Intelligence for Detection of Upper Gastrointestinal Cancer by Endoscopy: A Multicentre, Case-Control, Diagnostic Study," *The Lancet Oncology*, 20(12), pp.1645–54, .

³⁸ Walsh, P. & Miller, S. (2016) "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden" *Intelligence and National Security*, 31(3), pp.345–68.

the teenager's father had significantly more data.³⁹ Even if human analysts had access to this data, it is unlikely that they would be able to make sense of it.⁴⁰

Algorithms outperform human counterparts in many sections by cutting down on bias in decision making. For instance, experiments have shown that decisions on whether a defendant awaiting trial should be allowed to pay bail or not due to the risk of relapse is more accurate than by a judge (who, again, have access to more data).⁴¹ Judges may be biased to decide against a defendant simply because they look like a previous defendant who skipped bail. Another study showed that parole decisions were highly correlated with judges' meal breaks, as they were more lenient shortly after their breaks and became harsher as the day went on.⁴² Algorithms are not influenced by environmental factors (even though they might suffer from other biases).

The integrated nature of AI also allows for the intelligence community to adjust the scope of analysis that they perform. As AI detects patterns in the data stream, it can communicate with sensors to focus on the data streams that are most relevant to these patterns. Further, AI can better collaborate between different data streams as each of the separate INTS would be under the supervision of one entity. This allows for AI to expand the scope of the cycle so that patterns found from one INT can affect collection efforts in another. Depending how deeply integrated this AI system is, it can also pull data from different departments so that military intelligence organizations can infuse their analyses with relevant information concerning political, economic, or cultural issues that may shape the battlefield.

These changes in technology will disrupt the current intelligence cycle by allowing it to run in real-time with less need for human intervention and free up manual labor. AI can make parts of the intelligence process almost instantaneous; rather than having a collection officer, a data processor, and an analyst, AI can within defined data sets do all roles at once. This decentralized structure would rely on automated decision gates that allow for a quicker authorization for collection and dissemination as seen in the Bridgewater example. Automating approval processes could also improve the quality of decisions throughout the organization.

Lastly, AI can allow agencies to decentralize decision making processes. One of the biggest decentralizing aspects of digital technology is the increase in open-source data. Over 98% of all the world's information has been digitized and created an estimated 44 zettabytes of data available on the web.⁴³ Private firms have recognized this opportunity and the open source intelligence market is forecasted to reach over \$6

³⁹ Marx, G. (2016). *Windows into the soul: Surveillance and society in an age of high technology*. Chicago: University of Chicago Press.

⁴⁰ Taleb, N. (2007). *The Black Swan: The impact of the highly improbable*. New York: Random House.

⁴¹ Corbett-Davies, S, Goel, S. & González-Bailón, S. (2017) "Even imperfect algorithms can improve the criminal justice system." *New York Times*, 20 December, < <https://www.nytimes.com/2017/12/20/upshot/algorithms-bail-criminal-justice-system.html>>, (accessed 15 March 2022). Thaler, R, & Sunstein, C. (2004). "Market efficiency and rationality: The peculiar case of baseball", *Michigan Law Review*, 102(6), pp.1390-1403.

⁴² Danziger, S., Levav, J. & Avnaim-Pesso, L. (2011). "Extraneous factors in judicial decisions" *Proceedings of the National Academy of Sciences*, 108(17), pp.6889-6892.

⁴³ Eldridge, C, Hobbs, C. & Moran, M. (2018). "Fusing algorithms and analysts: Open-source intelligence in the age of 'big data'", *Intelligence and National Security*, 33(3), pp.394.

billion by 2027.⁴⁴ Some of these private firms are beginning to rival the secret work done by the established intelligence community.⁴⁵ Using open-source information, many private organizations have been successful in finding information that has eluded the gaze of the intelligence community. The most well-known example may be Bellingcat, a collective of researchers, journalists, and investigators who have released reports on the actions of the Russian intelligence, Russian chemical attacks in Syria and their information operations in Ukraine.⁴⁶

Intelligence in the Russian Context

The first critical thing to understand about the role of intelligence and security in the Russian context is that they are not a peripheral activity far removed from power. Rather, the intelligence and security services are at the core of power in Russia. This is not a novelty but it is continuous from the Soviet Union. Today, “it is clear that the security services in Russia today are as critical and central as they were under communism”.⁴⁷ The Soviet Union was characterized as a system with “an overarching concern with ‘enemies’ both internal and external. Security and extirpation of real or presumed threats become the premier enterprise of such systems”.⁴⁸

The centrality of internal and external enemies has manifested itself in the Russian vertical of power, and in particular in the principal role of the Security Council (SC). The SC has emerged as one of Russia’s most powerful institutions and has been placed at the core of strategic planning.⁴⁹ It might sound bureaucratic, but Russia’s strategies are key in achieving their grand strategic goals and consist of the whole spectrum of key concepts, strategies and doctrines for Russia including for socio-economic development and energy, as well as foreign policy and military doctrine.⁵⁰

Despite its broad mandate, the SC is heavily dominated by representation from the security and intelligence services. It is led by Nikolay Patrushev who was the head of the FSB between 1999–2008 and holds the central bureaucratic power.⁵¹ Putin reportedly starts his days with an intelligence briefing by the Federal Security Service (FSB)

⁴⁴ Valuates Report. (2021) “Global Open Source Intelligence (OSINT) Market Size, Status and Forecast 2021-2027”, < <https://reports.valuates.com/reports/QYRE-Auto-29O5948/global-open-source-intelligence-osint>>, (accessed 15 March 2022).

⁴⁵ Brown, Z & Medina, C.A. (2021). “The Declining Market for Secrets”, *Foreign Affairs*, March 9, <<https://www.foreignaffairs.com/articles/united-states/2021-03-09/declining-market-secrets>>, (accessed 15 March 2022).

⁴⁶ Ilyuk, Y. (2019). "Journalistic Investigations in the Digital Age of Post-Truth Politics: the Analysis of Bellingcat's Research Approaches Used for the (Re) construction of the MH17 case" *Perekrestki*, 1, pp.56-78.

⁴⁷ Gustafson, K. C., (2016), “Protecting the New Rome: Byzantine Influences on Russian Intelligence”, in Davies, P & Gustafson, K. C., *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere*, Washington DC: Georgetown University Press.

⁴⁸ Dziak, J. (1988) *Chekisty: A History of the KGB* (Lexington: Lexington Books), P.4

⁴⁹ Monaghan, A. (2017), *Power in Modern Russia*, Manchester: Manchester University Press, p.21

⁵⁰ Stanovaya, T. (2020). “Pyat Putinskikh elit na fone tranzita (Five of Putin’s elites against the background of transition)”, *Moscow Carnegie Center*, February 27. <<https://carnegie.ru/2020/02/27/ru-pub-81158>>, (accessed 15 March 2022).

⁵¹ Schulmann, E., & Galeotti, M. (2021). “A Tale of Two Councils: The Changing Roles of the Security and State Councils During the Transformation Period of Modern Russian Politics”. *Post-Soviet Affairs*, 1–20.

and the Foreign Intelligence Service (SVR)⁵². Moreover, the military intelligence (GRU) and the Federal Protective Service (FSO) also regularly update the president.⁵³

If we dig deeper into the threat perception of the Russian elites, we find that it is strongly influenced by intelligence and security service perspective. The threats that have risen most clearly on the agenda the last decade are from non-military means and includes the fear of color revolutions and information-psychological warfare.⁵⁴ The new National Security Strategy (NSS) from 2021 include focus on “unfriendly countries are trying to use socio-economic problems in the Russian Federation to destroy its internal unity, instigate and radicalize a protest movement, support marginal groups and divide Russian society. Indirect methods aimed at provoking long-term instability within the Russian Federation are increasingly being used”.⁵⁵ The NSS also focuses on how “Russian spiritual, moral and cultural-historical values are under active attack by the U.S. and its allies”;⁵⁶ and also how they saw that “information and psychological sabotage ...increasing the threat of the Russian Federation losing its cultural sovereignty.”⁵⁷

The key trends that are stipulated in the NSS and also echoed in the military doctrine - which is hierarchically subordinate to the NSS - are focused on threats to regime security. This is essentially a task for the intelligence and security services, and the backdrop with which we need to understand the Russian development of AI.

Russian views of AI

Even though Putin’s statement that the leader of AI will rule the world has been worn out, it is not unique. At a meeting at Sberbank in 2019, he said that “if someone can secure a monopoly in AI – well, we all need to understand the consequences – he will be the ruler of the world”.⁵⁸ The meeting also included plans for creating a strategy for AI development, which was approved later during the year. Putin has also in other places emphasized the key role of the technology for the future of power. For the conference Journey through Artificial Intelligence, he stated that Russia “must, and can, become one of the global leaders in the sphere of AI. This is a question of our future, the place of Russia in the world”.⁵⁹

The Russian Strategy for Science and Technology underlined the role of AI in the coming decade to stabilize Russia’s position in the world economy. It calls for

⁵² Galeotti, M. (2016), “Putin’s Hydra: Inside Russia’s Intelligence Services”, *European Council on Foreign Relations*, 11 May, <[https://ecfr.eu/wp-content/uploads/ECFR_169 - PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf](https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf)>, p.12.

⁵³ Ibid. p.12

⁵⁴ Jonsson, O. (2019). *The Russian Understanding of War: Blurring the Lines Between War and Peace*, Washington DC: Georgetown University Press.

⁵⁵ President of the Russian Federation, (2021a), “Strategiya natsionalnoy bezopasnosti Rossiyskoy Federatsii (National security strategy of the Russian Federation)”. Decree 400. July 2, <<http://publication.pravo.gov.ru/Document/View/0001202107030001?index=0&rangeSize=1>>, Point II.20

⁵⁶ Ibid. II.49

⁵⁷ Ibid. II.88

⁵⁸ BBC. 2019. “Putin zanyalsya iskusstvennym intellektom. Chto obsuzhdalos' na pervoy vstreche (Putin took up AI. What was discussed at the first meeting)”, 30 May, <<https://www.bbcrossian.com/russian/news-48463710>> (accessed 15 March 2022).

⁵⁹ President of the Russian Federation. 2019. “Konferentsiya po iskusstvennomu intellektu (Conference on Artificial Intelligence)”, 9 November, <<http://www.kremlin.ru/events/president/news/62003>>, (accessed 15 March 2022).

“transition to advanced digital, intelligent production technologies, robotic systems, new materials and design methods, the creation of systems for big data processing, machine learning and artificial intelligence”.⁶⁰ This mirrors the position in Russia’s NSS as well. AI is seen as a tool to ensure Russia’s economic security and to “increase labor productivity, modernize industrial enterprises and create high-tech jobs”.⁶¹ A subsequent point puts AI as a priority for science and technological development in Russia.⁶²

Above the specific mentions of AI, the NSS also makes references to new technologies of which AI is a critical part. It states that new technologies will contribute to the creation of weapons, military and special equipment with previously unattainable characteristics that will transforming power rivalries between states.⁶³

The Russian strategy on AI - with the formal title National Strategy for the Development of Artificial Intelligence Over the Period Extending up to the Year 2030 - was approved in October 2019 and set out key terms and key priorities. It defined AI as “a set of technological solutions that makes it possible to simulate human cognitive functions”.⁶⁴ Thereafter, it emphasizes Russia’s strengths in physics, mathematics and programming among universities and academic publications.⁶⁵ The strategy is mostly general and focuses on the educational and economic aspects of AI. One key characteristic is the continuing emphasis on AI’s importance as a decision-making technology. It is listed as the first priority for basic science research⁶⁶, as well as strengthening the application of AI for planning, forecasting, management and decision-making processes.⁶⁷

While the public doctrines are authoritative and confirms the importance of AI, they say little how it in practice will impact security and intelligence affairs. Therefore, it is useful to survey some key theorist’s views. There is a wide-ranging debate on how both emerging technologies in general and AI in particular will impact strategic affairs. One illustration comes from Major-General (ret) Burenok, a prominent military theorist and President for the Academy of Rocket and Artillery Sciences. Before that, he worked at the Ministry of Defense’s Central-Science Research Institute (TsNII) which provides the impetus to much of Russia’s thinking of modern war. He argued that AI will not only change war, but also the essence power as: *“The creation and development of systems of artificial intelligence is currently becoming one of the most important areas of scientific and technological progress, the very fundamental technology that can radically change the nature of not only*

⁶⁰ President of the Russian Federation. 2016. “Strategy for the Scientific and Technological Development of the Russian Federation”, Presidential Decree No.624.

⁶¹ President of the Russian Federation, (2021), “Strategiya natsionalnoy bezopasnosti Rossiyskoy Federatsii (National security strategy of the Russian Federation)”. Decree 400. July 2, <<http://publication.pravo.gov.ru/Document/View/0001202107030001?index=0&rangeSize=1>>, Point 67.6

⁶² Ibid. Point 76.14

⁶³ Ibid. Point 72

⁶⁴ Ibid. Point 5a

⁶⁵ President of the Russian Federation. 2019. ”Natsionalnuyu strategiyu razvitiya iskusstvennogo intellekta na period do 2030 goda (National Strategy for the Development of Artificial Intelligence Over the Period Extending up to the Year 2030)”. <<https://base.garant.ru/72838946/>>, (accessed 14 March 2022). Point 13

⁶⁶ Ibid. Point 30

⁶⁷ Ibid. Point 21a

armed struggle, but also the whole essence of power confrontation between states, including economic, information and cyber war."⁶⁸

In particular, Burenok saw a strong contribution from AI in “self-learning systems for analyzing and predicting the development of the geopolitical situation, assessing threats, the probability and methods of enemy attack, the possible composition of forces and characteristics of the weapons used, and possible damage of infrastructure”.⁶⁹ These are all core intelligence tasks which he is calling for. Burenok then listed the priorities for AI, which revolved around intelligence, command and control.⁷⁰ Interestingly, Burenok also emphasized that a lot of pioneering AI in the US were taking place among private firms, and he listed Google, Apple, Salesforce, and IBM, which could be read as a reminder of the Russian system where government is pioneering research.

Another example of the perception of AI can be taken from Colonel General Zarudnitsky, who is heading the Military Academy of the General Staff. Previously, Zarudnitsky was, among other things, chief of the Main Operations Directorate, of the central positions in the Russian Armed Forces. Zarudnitsky saw that AI was so impactful that it could even change the roles of the Russian Armed Forces in that “both military and non-military means of confrontation, primarily with the use of artificial intelligence technologies, causing the emergence of promising forms of employment of the RF Armed Forces — from a strategic operation of general-purpose forces and an operation of strategic deterrence forces to a global military campaign”.⁷¹

For him, he also saw a clear role of AI in intelligence and subversion. He argued that “psychological weapons are the weapons of tomorrow. They are aimed at manipulating society, the cultural environment, the national mentality through behavior algorithms using reflexive control techniques”.⁷² Lastly, Zarudnitsky saw the application of AI for autonomy and continued to call for the development of AI “capable of self-learning and analysis of big data sets for application in various fields — from reconnaissance and weapons control to strategic forecasting and decision making”.⁷³

While it is clear that there is a strong agreement in theory that AI will impact the essence of global competition, power and war, the major question is how this holds up in practice.

Russia’s Applications of AI

If we start from Putin’s statement that the leader in AI will rule the world, we have to ask how Russia is holding up against its international competition. At the present moment, Russia’s AI industry does not position them to be this leader. An investigation by Russia’s National Technology Initiative Competence Center for Artificial Intelligence to the Moscow Institute of Physics and Technology came with the

⁶⁸ Burenok, V.M. 2021. “Iskusstvennyy intellekt v voyennom protivostoyanii budushchego (Artificial intelligence in the military confrontation of the future)”. *Voennaya Mysl'*, No.1, p.109.

⁶⁹ *Ibid.* p.108.

⁷⁰ *Ibid.* p. 109.

⁷¹ Zarudnitskiy, V.B. 2021. “Kharakter i sodержaniye voyennykh konfliktov v sovremennykh usloviyakh i obozrimoi perspektive (Character and content of armed conflicts in modern conditions and near-term perspective)”. *Voennaya Mysl'*, No.1, p.44.

⁷² *Ibid.* p.39.

⁷³ *Ibid.* p.43.

conclusion that Russia lagged behind the world leaders (the US and China) in supporting domestic AI capabilities.⁷⁴ Due to the small size of their economy, Russia is outspent by about 350 to 1 by China on AI research.⁷⁵ The US and China spends seven times more on AI as a percentage of their GDP than Russia.⁷⁶ The report further concludes that Russia will have to triple the country's AI research and development budget to be able to compete with the leaders of AI.

Even though Russia has an unusually high degree of research and the development controlled by the government, much of its progress has taken place in the private sector. The main leader in the Russian Government's approach to AI has been Sberbank. Last year, Sberbank unveiled a second AI supercomputer that is supposed to bolster their technology profile.⁷⁷ At the same time, other key Russian actors have been less successful in pioneering AI. The defense conglomerate Rostec has largely ignored AI in favor of other priorities.⁷⁸ Yandex - Russia's equivalent to Google and the national leader in AI - has so far been left out of national AI planning due to governmental distrust of the firm.⁷⁹ The larger Russian political economic system with lacking rule of law and protection of property has also made it unlikely for new start-ups to find success in Russia.⁸⁰ Moreover, Russia faces a shortage of software engineers and has seen many young workers seek employment outside of their borders.⁸¹

Nonetheless, despite these challenges Russia has plenty of potential to build their AI capacity in the coming years. They certainly have the intellectual capacity with a strong tradition of the natural sciences, mathematics in programming as emphasized in their National AI-strategy. Indeed, in the International Collegiate Programming Competition (ICPC) where over 3,000 universities compete, Russian universities have won every single year the last decade.⁸²

The promise of AI and has already pressured the Russian government to start organizational change. For instance, the Russian Ministry of Defense has announced in 2021 that they will create a special AI department by 2022 with its own budget.⁸³ The Ministry of Defense has also started a close cooperation with the Ministry of Education and Sciences as well as the respected Academy of Sciences. The three entities agreed upon a number of priorities to develop AI, which included: creating a

⁷⁴ National Technology Initiative Competence Center for Artificial Intelligence. (2021.) "Artificial Intelligence Almanac: 2020 Index Report." *Center for Security and Emerging Technology*. December 6. Via <<https://cset.georgetown.edu/publication/artificial-intelligence-almanac-2020-index-report/>>, (accessed 15 March 2022).

⁷⁵ Ibid.

⁷⁶ Ibid.

⁷⁷ Marrow, A. (2021). "Russia's Sberbank, enhancing AI offering, unveils second supercomputer." *Reuters*. November 11. <<https://www.reuters.com/technology/russias-sberbank-enhancing-ai-offering-unveils-second-supercomputer-2021-11-11/>>, (accessed 15 March 2022).

⁷⁸ Petrella, S. Miller, C. & Cooper, B. (2021). "Russia's artificial intelligence strategy: the role of state-owned firms." *Orbis* 65(1), pp.75-100.

⁷⁹ Ibid.

⁸⁰ Dear, K., (2019). "Will Russia Rule the World Through AI? Assessing Putin's Rhetoric Against Russia's Reality." *The RUSI Journal* 164 (5-6), pp.36-60.

⁸¹ Ibid.

⁸² Wikipedia. (2022). "International Collegiate Programming Contest", <https://en.wikipedia.org/wiki/International_Collegiate_Programming_Contest>, (accessed 9 March 2022).

⁸³ Nadibaidze, A. (2022). "Russian Perceptions of Military AI, Automation, and Autonomy. *Foreign Policy Research Institute*, January <<https://www.fpri.org/article/2022/01/russian-perceptions-of-military-ai-automation-and-autonomy/>>. P.22

consortium on Big Data and AI analysis; creating a fund for analytical AI; creating a state system for training AI; creating a lab for testing AI solutions; creating a national AI-center; building a system for monitoring AI-development abroad; and using AI for wargaming activities.⁸⁴

This mirrors another initiative by Russia's Fond perspektivnykh issledovaniy (Advanced Research Agency), which in the Presidential decree (ukaz) is tasked with pioneering research for the Russian Armed Forces and for the power ministries.⁸⁵ It was setup to meet the need for "a radical organization to aggressively pursue risky innovation projects in the most promising areas".⁸⁶ That included specific mentions of the need to implement a public-private partnership in emerging technologies. The Advanced Research Agency has also been complemented by a military "technopolis" to pioneer technological development for the Russian Armed Forces, which also entails AI as a key priority.⁸⁷

The most notable contribution to Russia's progress in AI would be a partnership with China. The Russia-China Investment fund is already seeking to create technoparks that would emulate China's model for technological innovation. The fund has invested in companies such as Megvii which offers machine learning and facial recognition software.⁸⁸ Russia has already invested in autonomous vehicles for military use with sophisticated AI systems to "see" the environment.⁸⁹ Pivoting these technologies for use in information warfare could allow Russia to gain outsized effects from their small AI industry.⁹⁰

There are roughly three components needed for progress in AI: data, algorithms and people. It is clear that Russia does have the talent pool needed, so the question continues to data and algorithms. Relevant data is needed to be able to train the algorithms, and in terms of data, the Russian leadership have implemented far-reaching technologies for mass surveillance. Most significant is the SORM system created in the late 1990s, which allows for the interception of all telephone and internet communications. It enables the FSB to "control centers connected directly to operators' computer servers". To monitor particular phone conversations or Internet communications, an FSB agent only has to enter a command into the control center located

⁸⁴ Ministry of Defense of the Russian Federation. 2018, "Konferentsiya «Iskusstvennyy intellekt: problemy i puti ikh resheniya — 2018 (Conference 'Artificial Intelligence: Problems and Their Solutions – 2018)' <<https://mil.ru/conferences/is-intellekt.htm>>, (accessed 15 March 2022).

⁸⁵ Fond perspektivnykh issledovaniy. 2022. "Dokumenty (Documents)", <<https://fpi.gov.ru/about/documents/41/>>, (accessed 14 March 2022).

⁸⁶ Zysk, K. 2021. "Defence innovation and the 4th industrial revolution in Russia", *Journal of Strategic Studies*, 44:4, p. <544.

⁸⁷ President of the Russian Federation. 2018. "Ukaz: O sozdanii voennogo innovatsionnogo tekhnopolisa 'Yera' (On the creation of the military innovative technopolis 'Yera')", No 364. <<http://krem-lin.ru/acts/bank/43213>>, (accessed 15 March 2022).

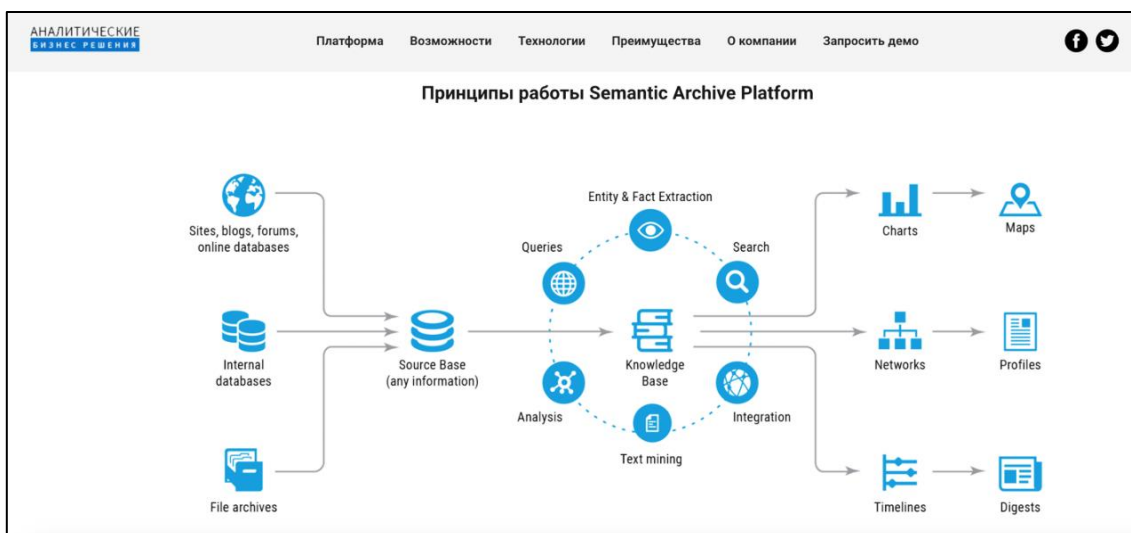
⁸⁸ Russia-China Investment Fund. (2021). "Portfolio Companies", <<http://rcif.com/en/portfolio-companies.htm>>, (accessed 15 March 2022).

⁸⁹ Horowitz, M. C. 2018. "Artificial intelligence, international competition, and the balance of power", *Texas National Security Review*, 1(3), pp.36-57; Edmonds, J. et al (2021) "Artificial Intelligence and Autonomy in Russia", *Center for Naval Analysis*, May, <https://www.cna.org/CNA_files/centers/CNA/sppp/rsp/russia-ai/Russia-Artificial-Intelligence-Autonomy-Putin-Military.pdf>, (accessed 15 March 2022).

⁹⁰ Konaev, M. & Bendett, S. 2019. "Russian AI-Enabled Combat: Coming to a City Near You?". *War on the Rocks*, <<https://warontherocks.com/2019/07/russian-ai-enabled-combat-coming-to-a-city-near-you/>>, (accessed 15 March 2022).

in the local FSB headquarter”.⁹¹ The SORM network relies on black boxes that “mirror online traffic, sending the original on to its intended destination and a copy of all traffic to FSB-owned and -operated servers”.⁹² The Russian government is also significantly expanding its reliance on facial recognition.⁹³ The new facial recognition software Sphere has for instance led to the detainment of over 2,000 people already.⁹⁴

The SORM-system allows the Russian intelligence services to access vast amounts of data that can be leveraged together with AI technologies. One such implementation comes from the Analiticheskiye Biznes Resheniya (Analytical Business Solutions) who offers a platform called the Semantic Archive Platform (SAP) that is being leveraged by the Russian security services.⁹⁵ The SAP is a multi-source analytics tool that includes gathering data (including unstructured) from social networks, media, forums and more through automated crawlers.⁹⁶ Additionally, the SAP (according to its website) combines it with data on bank transfers, phone calls and text messages, which are all surveilled in Russia. This has, of course, been within the reach of intelligence services for a long time, but there is a unique addition in that the platform offers both automated data collection (increases the breadth of collection), data integration (combining different data flows) and automated analysis (increases the speed and depth).



Picture 1. The Semantic Archive Platform

With this combination of data and analysis, the SAP provides network analysis, mapping of people, events and objects as well as the relations between them. This product

⁹¹ Soldatov, A., & Borogan, I., “Russia’s Surveillance State”, *World Policy Journal*, 30(23), pp.23-30.

⁹² Morgus, R., 2019, “The Spread of Russia’s Digital Authoritarianism”, in Wright (Ed.), *Artificial Intelligence, China, Russia, and the Global Order*, Maxwell: Air University Press. P.91

⁹³ Human Rights Watch, 2020, “Russia Expands Facial Recognition Despite Privacy Concerns”, 2 October, <<https://www.hrw.org/news/2020/10/02/russia-expands-facial-recognition-despite-privacy-concerns>>, (accessed 15 March 2022).

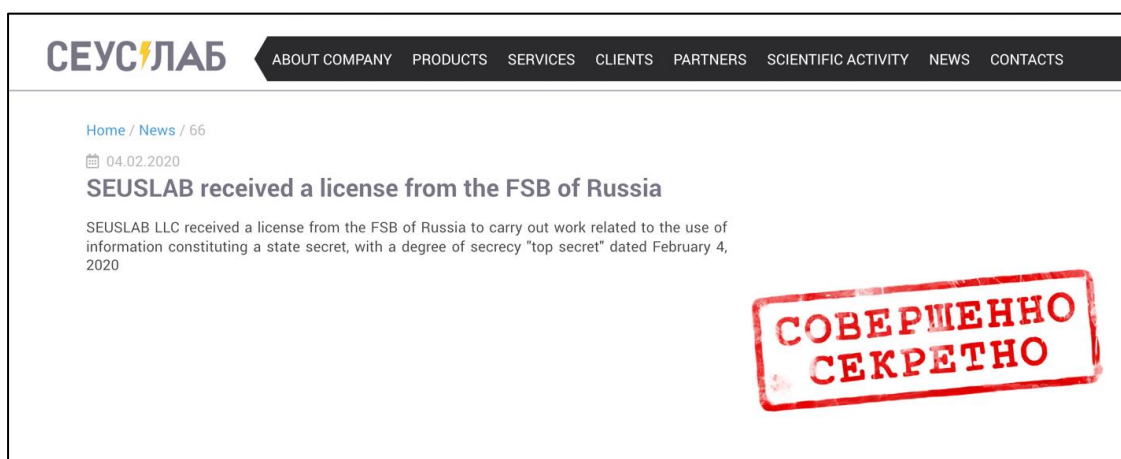
⁹⁴ CNA. 2022. “AI and Autonomy in Russia – Newsletter”, No.30, January 24. <https://www.cna.org/CNA_files/PDF/AI-and-Autonomy-in-Russia-Issue-30-January-24-2022.pdf>, (accessed 9 March 2022).

⁹⁵ Morgus, R., 2019, “The Spread of Russia’s Digital Authoritarianism”, in Wright (Ed.), *Artificial Intelligence, China, Russia, and the Global Order*, Maxwell: Air University Press. P.92

⁹⁶ Semantic Archive Platform. 2022. “Platforma (The Platform)”, <<http://www.anbr.ru/>>, (accessed 15 March 2022).

thus holds the promise for the security and intelligence services to translate their large-scale surveillance and abundance of data, into actionable intelligence in an automated and decentralized manner. Nonetheless, it is unclear how well they are solving that task in practice.

Another example of the application of AI to the security services is Zeus Lab, who since 2012 has a stated mission to “developing software and hardware solutions designed to protect Russian statehood and culture”.⁹⁷ In doing this, Zeus Lab offers “special software solutions ... [for] law enforcement agencies, government bodies and enterprises of the military-industrial complex of the Russian Federation”. Zeus Lab is openly communicating about having received a clearance by the FSB to work with classified material up to Top Secret.⁹⁸ They are also stating that their software is being used by governmental agencies in 39 of the Russian Federations regions.



Picture 2. Zeus Lab’s license (automated translation)

While the information about their products is less transparent than the SAP, Zeus Lab is still communicating that they are using neural networks to train algorithms to track and analyze the use of social networks.⁹⁹ Their stated research priorities are: analysis of information processes in social networks; development of methods for assessing the state of information confrontation; and automation of big data analysis.¹⁰⁰

It is thus clear that Zeus Lab, like *Analiticheskiye Biznes Resheniya*, offers ways to cut through the massive amounts of data generated to filter out actionable intelligence. What is more transparent is that Zeus Lab’s interaction with governmental agencies. The company participates in a number of governmental fora on topics of digital policing in information and communication technologies, information confrontation, and how using AI in the online domain can strengthen security and intelligence services.

⁹⁷ Zeus Lab. 2022. "ООО Seuslab", <<https://seuslab.ru/>>, (accessed 15 March 2022).

⁹⁸ Zeus Lab. 2022. "Kompaniya «SEUSLAB» poluchila litsenziyu FSB Rossii (Zeus Lab received license from FSB)" <<https://seuslab.ru/news/66>> (accessed 15 March 2022).

⁹⁹ Zeus Lab. 2022. "Zaregistrirrovana baza dannykh dlya klassifikatsii roley polzovateley sotsialnykh setey (Registered database to classify the roles of social network users)" <<https://seuslab.ru/news/76>> (accessed 15 March 2022)

¹⁰⁰ Zeus Lab. 2022. "Nauchnyye Isskedovaniya (Scientific Research)" <<https://seuslab.ru/science>> (accessed 15 March 2022)

Both the examples of Zeus Lab and *Analiticheskiye Biznes Resheniya* show that the Russian intelligence and security services are seeking to integrate the private sector in applying AI solutions to help their intelligence efforts.

Discussion

This study seeks to show how intelligence is a key activity for the Russian leadership, and that AI holds the greatest promise to reform it. AI can solve the problem with an abundance of data and a limited amount of analytical power to make sense of it. AI can, and will, solve it in four ways. First, it increases the speed of data collection, processing, and analysis. Second, it allows for intelligence agencies to increase the scope of their collection efforts by including and analyzing vast data streams. Third, it enables intelligence services to look at targets in greater depth, and with algorithms outcompeting human operators in parts. Fourth, it adds an element of increased decentralization, where steps of the traditional intelligence cycle is delegated and automated.

With this in mind, the question is how far Russian intelligence affairs have come in translating the promise of AI into practical reality. As stated above, a real revolution in intelligence affairs is not only about technological progress, but also requires the change in organization and doctrine to leverage its full potential. Below, we will assess these in turn.

Technology

Technology is the most straightforward part of this trilogy to assess. Many of the examples mentioned above from the civilian applications are years old, and some are decades old. The ability to implement AI solutions for analysis and decision-making are known, commercially available and used by the Russian government and private sector.

The section on Russia's applications shows how AI tools are used to make sense of big data, fusing different data streams and providing automated analysis. Moreover, the talent pool in Russia with leading universities and academic publications bears witness of the fact that there is an access to the technology needed. That being said, the U.S. and China are still far ahead of Russia in actual progress in AI. While Russia is doing well in AI's constituent parts – data, algorithms and people – they have so far failed to translate preconditions to output.

Organization

To leverage the benefits of AI, organizational change is needed, particularly as AI is a general purpose-technology that is pioneered in the private sector. This poses notable problems for Russia where a large majority of the research is guided by the state, done by state institutes and often for state purposes. There has been a recognition in both Russian doctrines and among theorists that a much stronger public-private partnership is needed in this regard. However, that is easier in theory, and in particular as intelligence and security services are by their nature the most secretive agencies.

Russia's leader in AI – Yandex – is seemingly not trusted by the government, which have focused their efforts on Sberbank. Sberbank might be a competent actor, but they are a bank and limited by the nature of the data they possess. Yandex is an

equivalent to Google that has a search engine, maps, e-mail, a browser and other e-services, which makes their data significantly more useful for intelligence purposes. This is why both Yandex and Google have such a powerful insight on how to influence individuals (consumer) behavior. The quality of AI is highly dependent on the quality of the data.

There have been notable attempts of organizational change to leverage the use of AI. Indeed, “the Russian authorities are creating public-private consortiums to facilitate collaboration between the private high-technology sector and civilian academic institutions on the one hand and military and security institutions on the other”.¹⁰¹ Examples includes the Ministry of Defense creating a special AI-unit, the joint venture by the Ministry of Defense and Education together with the Academy of Sciences, and a number of private AI-companies working directly with the security and intelligence services.

Similarly, as in the case with technology, we can register an ambition that is manifested in a number of initiatives but have yet to materialize in concrete results.

Doctrine

A change in doctrine requires an update in the set of institutional knowledge, procedures and beliefs. Needless to say, it is the hardest component to assess from the outside. This study rather mirrors the conclusion of a study of Russia’s wider attempt to pioneer the technologies of the fourth industrial revolution, of which AI is a key component. Zysk concluded that “despite grand ambitions, new initiatives, and modifications of the traditional defense innovation model to incorporate civilian and private-sector innovation, Russia struggles to leverage 4IR technologies due to structural and circumstantial constraints and a lack of resources relative to near-peer competitors, the US and China.”¹⁰²

Moreover, in terms of translating doctrine and organization, this study also agrees with the results from a study by the Russian Center for Policy Research (PIR) into the Russian application of AI. In it, Kozylin argued that we are at an inflection point where “perhaps we are approaching a moment when decision making on defense and security will be increasingly delegated to artificial intelligence as a necessary measure”.¹⁰³ This study agrees with the sentiment in both aspects as it has 1) not yet happened, but also that 2) there is such amount of attention and initiatives that that point is rapidly nearing.

The application of AI in the Russian intelligence and security services will mirror the old saying on how one becomes bankrupt “first gradually then suddenly”. Russia’s revolution in intelligence affairs will progress the same way.

¹⁰¹ Zysk, K. (2021) “Defence innovation and the 4th industrial revolution in Russia”, *Journal of Strategic Studies*, 44:4, p.552.

¹⁰² Ibid.

¹⁰³ Kozylin, V. (2019. “Militarization of AI”, *Stanley Center for Peace and Security*, July, <<https://stanley-center.org/wp-content/uploads/2020/05/MilitarizationofAI-Russia.pdf>>, (accessed 15 March 2022).

INTERFACE BETWEEN ARTIFICIAL INTELLIGENCE AND CYBER. CREATING REVOLUTION IN MILITARY AFFAIRS? THE RUSSIAN MILITARY'S UTILISATION OF ARTIFICIAL INTELLIGENCE TO ENHANCE ITS CYBER OPERATIONS: THE CURRENT STATE OF PLAY

Rod Thornton and Marina Miron

The presentation made by Rod Thornton in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 6:27:00.

Abstract

The aim in this chapter is to explore the current situation in terms of the Russian military drive to utilise Artificial Intelligence (AI) to enhance its offensive cyber operations. It firstly considers why the Russian military puts such emphasis on the need to develop an AI-enhanced offensive cyber capability. The concentration here is on the strategic level use of this particular capability – against state adversaries – rather than at the operational or tactical levels. It also focuses only on the offensive capabilities of AI-enhanced cyber, not the defensive. Finally, this chapter will consider how the ability of the Russian military to engage in AI-enhanced offensive cyber operations will have been affected by the fall-out from the Russian invasion of Ukraine.

Caveats, of course, abound when investigating how the Russian military might wish to employ its offensive cyber capabilities and how AI might be utilised to enhance them. There will inevitably be a degree of opacity surrounding these issues. The Russian military will want to keep them secret. This chapter thus goes forward on the understanding that it is relying on open-source material and that a degree of extrapolation has had to take place.

The concentration here is on the use of offensive cyber by the Russian military itself. While the internal security body, the FSB,¹ and the Foreign Intelligence Service, the SVR² both have roles to play in the Russian state's cyberspace operations, they are seen to play second-fiddle to the military. It is the military that is regarded as the lead offensive cyber protagonist and the one that has some degree of control over the cyber activities of the other two services.³ Indeed, the head of the Russian military,

¹ Federalnaya Sluzhba Bezopasnosti [Federal Security Service]. This operates using the APT28 hacker group and others such as Turla and Palmetto Fusion.

² Sluzhba Vneshnei Razvedki. This operates mainly using the APT29 group.

³ Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Anchor Books, 2020); Bilyana Lilly and Joe Cheravitch, 'The Past, Present and Future of Russia's Cyber Strategy and Forces,' in *20/20 Vision: The Next Decade*, T. Jancarkova, L. Lindstrom, M. Signoretti and I. Tolga (eds), (Fallinn: NATO, 2020), https://ccdcoe.org/uploads/2020/05/Cy-Con_2020_8_Lilly_Cheravitch.pdf.

General Valerii Gerasimov, has given the impression that it is his military that is the coordinating body for all the state's offensive cyber actors.⁴

When talking of the military and offensive cyber operations these are conducted by its principal intelligence arm, the Main Intelligence Directorate or GRU.⁵ The GRU, of course, does not have a critical mass in terms of numbers of cyber operatives to generate the scale of cyberattacks that would create strategic effect. But it can call on any number of civilian hackers either through the St Petersburg-based Internet Research Agency (IRA),⁶ through the services of ad hoc 'patriotic hackers' or even through those hackers press-ganged into providing services for the GRU.⁷

The importance of warfare in cyberspace

There is a belief within both the Kremlin and the Russian military that it is 'information' that will be the truly effective strategic weapon in the coming decades when it comes to what United Kingdom official documents refer to as the 'intensifying international competition' between Russia and NATO and its core states.⁸ Within Russian official political and military publications actual kinetic conflict with NATO is generally judged to be a highly unlikely possibility. Rather, the main weapon that will be used against Russia is non-kinetic in form and it is information.⁹

President Vladimir Putin has himself expressed the concern that Russia is being subject to an information warfare campaign directed from 'the West' that can have dire consequences for his country. He has noted that, 'Russia cannot be defeated, it can only be torn apart from within'.¹⁰ He was referring to the fact that Russia could be destabilised through the inciting of what Russian military doctrine refers to as the 'protest potential of the population'.¹¹ *Khaos* may result.¹² This could be incited in Russia by, in essence, NATO's utilisation of information supplied over cyber means – social media sites and media outlets. It is a considerable fear of the Kremlin that the

⁴ Valerii Gerasimov, 'Vektory Razvitiya VoЕННОi Strategii [Vectors of Military Strategy Development]," *Krasnaya Zvezda*, 4 March, 2019, <http://redstar.ru/vektory-razvitiya-voennoj-strategii/>.

⁵ The GRU (or Glavnoe Razvedyvatel'noye Upravleniye) should more accurately be referred to as the GU (Glavnoe = Main Directorate of the General Staff of the Armed Forces of the Russian Federation). But the abbreviation GRU remains in use.

⁶ Dimitry Volchek, 'Inside the "Propaganda Kitchen" – a former "Troll Factory" employee speaks out', RFERL, 29 January 2021, <https://www.rferl.org/a/russian-troll-factory-hacking/31076160.html>.

⁷ Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington D.C.: Georgetown University Press, 2021); Jolanta Darczewska, 'Russia's Armed Forces on the Information War Front,' *OSW Studies*, no. 57 (2016), https://www.osw.waw.pl/sites/default/files/prace_57_ang_russias_armed_forces_net.pdf.

⁸ 'Global Britain in a Competitive Age. The Integrated Review,' CP 403, HM Government, March 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

⁹ S. P. Rastroguyev, *Formula Informatsionnoi Voiny* [Formula of Information War] (Moscow: Biblioteka Rasovoi Mysli, 1999).

¹⁰ Andrew Roth, 'Putin accuses west of "coming with its missiles to our doorstep"', *The Guardian*, 23 December 2021, <https://www.theguardian.com/world/2021/dec/23/putin-accuses-west-coming-with-missiles-doorstep>

¹¹ Ministry of Defense of the Russian Federation, *Voennaya Doktrina Rossiiskoi Federatsii* [Military Doctrine of the Russian Federation], Kremlin, 26 December, 2014, <http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>;

¹² S.G. Chekinov and S.A. Bogdanov, 'Voyennoye Iskusstvo na Nachal'nom Etape XXI Stoletiya: Problemy i Suzhdeniya' [The Art of War at the Beginning of the 21st Century: Problems and Opinions], *Voennaya Mysl'* [Military Thought], No.1, 2015, <http://elibrary.ru/contents.asp?issueid=1365492>

Russian government could be brought down by mere information¹³ – information which may be no more than the truth.

Such forms of ‘attack’ are, in Russian military thinking, all part of ‘information warfare’ (*informatsionnaya voyna*). This form of warfare is seen to have two elements: the ‘cyber psychological’ (*kiber-psikhologicheskii*) and the ‘cyber technical’ (*kiber-tekhnicheskii*). In this military’s view, and in contrast to the thinking in NATO states, cyber warfare is considered to be more of psychological weapon than a technical one. As a writer in one Russian military-focused journal had to point out to his readers, ‘Some experts erroneously call cyber warfare a transformation of another type of confrontation - psychological operations. This is partly true, but the very concept and set of tools involved in cyber warfare is much broader than in psychological operations.’¹⁴ The idea being that this author’s readers had to be made aware that this form of warfare – cyber – has other aims than just creating psychological effect – it has technical targets as well.

Obviously, in cyber-psychological attacks use is made of social media and even information supplied over mainstream media. The cyber technical form is the one more akin to the Western notion of a ‘cyberattack’. Here the information in IT systems would be targeted. As the world becomes increasingly digitised, the high dependence on cyberspace is creating both opportunities and vulnerabilities (as was the case in Estonia in 2008).¹⁵ Principal targets in any strategic-level, state-sourced, IT-focused cyberattack would be the likes of banking systems, energy infrastructure and transportation links. Societal disruption will ensue, again possibly to the point of creating *kekhaos*. The fear expressed in Russian circles is again that Russia could also be the target of such an attack launched by NATO states. Thus Moscow sees itself as being under threat from NATO-launched offensive cyber threats in both forms – the cyber-psychological and the cyber-technical – that can generate serious effects on the way the country functions. The word used most often in Russian military writings on this subject is that the country will be ‘destabilised’ to the point where it can be subject to the leverage of NATO actors – in essence, defeated.¹⁶

Russia itself, of course, is working from the same song sheet. The weaponisation of information is also important in Russian strategic thinking and as an offensive tool it can, in turn, ‘destabilise’ the countries of its NATO adversaries. Moscow can also use information warfare in cyberspace to theoretically gain the same effects by weakening its own state opponents internally such that they either no longer pose a threat to Russia or are, indeed, weakened to a degree where Russia holds strategic leverage over

¹³ Andrei Ilnitski, ‘Bezgranichnye Kibervozmozhnosti [Limitless Cyber-possibilities].’ *Izvestiya*, June 17, 2019, <https://iz.ru/888988/andrei-ilnitckii/bezgranichnye-kibervozmozhnosti>.

¹⁴ Alex, ‘The Russian army is betting on Artificial Intelligence’ *Voennaya Platforma*, 10 February 2021, <https://www.militaryplatform.ru/7410-rossiyskaya-armiya-delaet-stavku-na-iskusstvennyy-intellekt.html>.

¹⁵ Jasper, *Russian Cyber Operations*, pp. 32-35.

¹⁶ Valerii Gerasimov, ‘Genshtab Planiruyet Udary [The General Staff Plans Strikes],’ *Voenna-Promyshlenniy Kur’er*, 9, no. 772, 12 March, 2019, <https://vpk-news.ru/articles/48913>; Lyudmila V. Gundarova, ‘Kto Finansiruyet Tsvetnyye Revolyutsii na Postsovetском Prostranstve [Who Finances Colour Revolutions in the post-Soviet Space],’ *Nezavisimoe Voennoe Obozrenie*, 15 January, 2016, https://nvo.ng.ru/concepts/2016-01-15/1_revolutions.html; ‘S “Tsvetnykh Revolyutsiy” Hotyat Snyat’ Kamuflyazh [They Want to Remove Camouflage from ‘Colour Revolutions],’ *Kommersant*, 3 April, 2015, <https://www.kommersant.ru/doc/2679357>; ‘Rossiya Obvinila NATO v Podgotovke “Tsvetnykh Revolyutsiy” [Russia Blamed NATO for Preparing ‘Color Revolutions],’ *Lenta*, 2 July, 2019, <https://lenta.ru/news/2019/07/02/sovbez/>.

them. They would then be, again to borrow from the Russian military lexicon, ‘neutralised’.¹⁷

The state body tasked with carrying out both forms of cyberattacks is, as noted, the Russian military. This military has readily turned to the use of information warfare in cyberspace as a means of weakening core NATO states from within and, in particular, to undermine the unity of NATO as an alliance. This fits in well with the overall asymmetric thinking adopted by this military over the last two decades or so.¹⁸ There is a realisation that the Russian armed forces are much weaker than the collective forces of NATO. Thus, if this military is to ever prevail over NATO then it has to employ means – at all levels of warfare, but particularly at the strategic level – that avoid any symmetrical clash of forces on any battlefield. The thinking is that NATO needs to be ‘defeated’ at the strategic level *non-kinetically* and *before* any clash of actual arms takes place.¹⁹

The importance of AI

In its efforts to ‘neutralise’ adversary states through the use of information warfare there would naturally be a search by this Russian military for ways of increasing the power of such a form of warfare. Here is where AI comes in. AI when applied in both cyber-technical and cyber-psychological attacks holds the promise of fundamentally improving their ability to generate strategic effect.

AI-driven cyber-attacks are assumed to have a much higher success rate than those using traditional approaches²⁰ and, what is more, with a much smaller chance of detection.²¹ Thus, in the cyber technical sphere, there is a fear (in Russia) that the Third World War could be over ‘within a few seconds if one state, using AI technologies, takes control of all the main life support systems of rival countries.’²² And as another Russian author expresses it, any military organisation using AI in this way can actually create a ‘doomsday technology’.²³

¹⁷ A.V. Kartapolov, ‘Uroki Voennykh Konfliktov, Perspektivy Razvitiya Sredstv I Spocobov ikh Vedeniya. Pryamye I Nepryamye Deystviya v Sovremennykh Mezhdunarodnykh Konfliktov [Lessons of Military Conflicts and Prospects for the Development of Means and Methods for their Conduct. Direct and Indirect Actions in Contemporary International Conflicts],’ *Vestnik Akademii Voennykh Nauk*, no. 2 (2015), <http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/737-vestnik-avn-2-2015>.

¹⁸ Kartapolov ‘Lessons of Military Conflicts’.

¹⁹ S. Chekinov and S. Bogdanov, ‘Asimmetrichnie deystviya po obespecheniyu voennoy bezopasnosti Rossii [Ensuring Russian military security by asymmetric means],’ *Voennaya mysl’* no. 3 (2010): 13-22; S. Chekinov and S. Bogdanov, ‘Vliyaniye Nepryamykh Deystviy na Kharakter Sovremennoy Voyny [The impact of indirect methods on the nature of modern warfare],’ *Voennaya mysl’* no. 6 (2011): 3-13; S. Chekinov and S. Bogdanov, ‘O Kharaktere I Soderzhanii Voiny Novogo Pokoleniya [On the Character and Content of New-Generation Wars],’ *Voennaya Mysl’* 22, no. 4 (2013): 13–24; Kartapolov, ‘Lessons of Military Conflicts.’

²⁰ Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova, ‘The Emerging Threat of AI-driven Cyber Attacks: A Review,’ *Applied Artificial Intelligence*, 2022, DOI: [10.1080/08839514.2022.2037254](https://doi.org/10.1080/08839514.2022.2037254), p. 23.

²¹ Ben Buchanan, John Bansenmer, Dakota Cary, Jack Lucas, and Micah Musser, ‘Automating Cyber Attacks,’ Center for Security and Emerging Technology, November 2020, <https://doi.org/10.51593/2020CA002>, pp.13-14.

²² Ilnitski, ‘Bezgranichnye Kibervozmozhnosti’

²³ ‘Tekhnologii “Sudnogo Dnya”’: Vooruzhennyye Sily Rossii Vnedryayut Iskusstvennyy Intellect [Doomsday Technologies: Russia's Armed Forces Introduce Artificial Intelligence], Yandex.ru, 16 March 2018, <https://zen.yandex.ru/media/menweapon/tehnologii-sudnogo-dnya-voorujennye-sily-rossii-vnedriaiut-is-iskusstvennyi-intellekt-5aab65d67ddde892fdb118ed>.

The Russian side wants to make sure that they are in a position to create what is known as ‘first mover advantage’;²⁴ where whoever is the first to develop truly significant forms of AI-enhanced cyberattacks will be the side that wins ‘within a few seconds.’²⁵

Aside from the threats associated with AI-driven cyber-technical attacks, there is also the more nuanced psychological dimension created by the use of AI in the cyber-psychological domain. Here AI can be used ‘to create “fake news”, post fake press releases on government websites and central banks, create artificial reality online, change the video content of TV shows to influence the minds of citizens and force politicians to make “necessary” decisions.’²⁶ In other words, AI can make cyber-psychological attacks much more powerful than is possible with traditional forms of cyberattack.

This use of AI to target the so-called cognitive space has been explored since 2012.²⁷ Indeed, multiple studies have demonstrated the success of AI’s persuasive effects on human agents.²⁸ Some current examples of the use of AI for malicious purposes to target the cognitive space – be it related to a person or a whole country – include smart bots in information campaigns, phishing and deepfakes.²⁹ The current proliferation of AI-based software enabling the creation of deepfakes is, in particular, seen as posing a significant threat/opportunity.³⁰ A recent manifestation of such a deepfake sourced to Russia was the creation of a ‘false’ Ukrainian President Volodymyr Zelensky at the beginning of Russia’s ‘special military operation’ in Ukraine. This video was supposed to show Zelensky asking his troops to surrender.³¹ Had this deepfake been created in a more professional manner, it could have caused excessive confusion, even leading to the actual blanket surrender of Ukrainian forces.

AI development in Russia

Given that AI when used in the information warfare realm offers, at least in theory, to win wars almost immediately and without firing a shot, then a world-wide development race has been evident for some years now. The major states – notably the

²⁴ Indermit Gil, ‘Whoever leads in artificial intelligence in 2030 will rule the world until 2100’, Future Development, Brookings, 17 January 2020, <https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/>

²⁵ Ilnitski, ‘Bezgranichnye Kibervozmozhnosti.’

²⁶ Ibid.

²⁷ Shouqi Li, Fangcheng Long and Yongchang Wang, ‘Probe into Principles of Expert System in Psychological Warfare’, in DS. Huang, Y. Gan, P. Gupta & M.M. Gromiha (eds). *Advanced Intelligent Computing Theories and Applications. With Aspects of Artificial Intelligence. ICIC 2011. Lecture Notes in Computer Science*, vol 6839 (Berlin: Springer, 2012), https://doi.org/10.1007/978-3-642-25944-9_43, pp. 333-340.

²⁸ Christoph Bartneck, Christoph Lütge, Alan Wagner & Sean Welsh, ‘Psychological Aspects of AI,’ in *An Introduction to Ethics in Robotics and AI* (Cham: Springer, 2021), https://doi.org/10.1007/978-3-030-51110-4_7, pp. 55-60.

²⁹ *Malicious use of artificial intelligence*, Moscow: Newstex, 2020, <https://www.proquest.com/blogs-podcasts-websites/malicious-use-artificial-intelligence/docview/2472245285/se-2>

³⁰ Konstantin A. Pantserov, ‘The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability,’ in *Advanced Sciences and Technologies for Security Applications* (Advanced Sciences and Technologies for Security Applications) (Springer Nature 2020), https://doi.org/10.1007/978-3-030-35746-7_3, pp. 37-55; *Artificial intelligence and new threats to international psychological security*, Moscow: Newstex, 2019, <https://www.proquest.com/blogs-podcasts-websites/artificial-intelligence-new-threats-international/docview/2253712763/se-2>.

³¹ Tom Simonite, ‘A Zelensky Deepfake Was Quickly Defeated. A Next One Might Not Be,’ *WIRED*, March 17, 2022, <https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/>.

United States, China and Russia – are in a rush to be the first to field AI-enhanced offensive cyber capabilities. To be second in this race risks, as noted, being open to actual annihilation as a state.³²

Putin himself has been, over the last few years, constantly encouraging the responsible authorities in his country to improve its AI capabilities in general. He wants Russia to be the world leader in terms of AI development: ‘Russian leadership’, he said, ‘on this topic [of AI] – is, without exaggeration, the most important.’³³ It is the ‘most important topic’ and yet he did not look to scientific, educational or industry bodies within Russia to take the lead in terms of AI R&D in the country. Instead, he called on his military to take on this responsibility.³⁴ First Deputy Minister of Defence Ruslan Tsalikov confirmed this was the case. In Russia, he said, it is the armed forces that are ‘currently leading in almost all of the technological breakthrough areas’ in relation to AI.³⁵ By 2018, the Russian Ministry of Defense was stressing the importance of developing AI which would help it win the cyber wars of the future. According to Yuri Borisov, the then Deputy Defence Minister, ‘[s]uch a concept as cyber war has become a reality today. Today all battles are played out not on the battlefields, they are first played out in the information space. Whoever can control it, whoever is able to organize counteraction in the right way – he will be the winner today.’³⁶ In a similar fashion, the current Defence Minister Sergei Shoigu has called for closer cooperation between the military and the civilian sector to accelerate the development of AI. In his view, AI would help defend Russia both in the technological as well as the economic spheres.³⁷

Although the military is nominally the lead actor when it comes to developing AI in Russia, it can call on a significant body of highly knowledgeable civilian scientists and engineers. Russia, indeed, is perceived to have perhaps the best intellectual capital when it comes to the development of AI.³⁸

³² Colin Demarest, ‘NATO Launches AI Initiative to Ensure Tech Advantage,’ *C4ISRNET*, 18 May 2022, <https://www.c4isrnet.com/artificial-intelligence/2022/05/18/nato-launches-ai-initiative-to-ensure-tech-advantage/>; Mark Pomerleau, ‘Pentagon’s AI Center to Field New Psychological Operations Tool,’ *C4ISRNET*, 11 September 2020, <https://www.c4isrnet.com/artificial-intelligence/2020/09/11/pentagons-ai-center-to-field-new-psychological-operations-tool/>; Ben Noon & Chris Bassler, ‘How Chinese Strategists Think AI Will Power Military Leap Ahead,’ *Defense One*, 17 September 2021, <https://www.defenseone.com/ideas/2021/09/how-chinese-strategists-think-ai-will-power-military-leap-ahead/185409/>.

³³ Quoted in Andrei Kolesnikov, ‘Honoured Artist: How Vladimir Putin Digitised German Gref,’ *Kommersant*, 11 November 2019, <https://www.kommersant.ru/doc/4154715>.

³⁴ ‘Vooruzhennyye Sily RF Vnedryayut Tekhnologii Iskusstvennogo Intellekta’ [Russian Armed Forces Introduce Technologies of Artificial Intelligence], *Voennyye Materialy* [Military Materials], (undated but in March 2019), <https://warfiles.ru/176763-vooruzhennyye-sily-rf-vnedryayut-tehnologii-iskusstvennogo-intellekta.html>.

³⁵ Kolesnikov, ‘Honoured Artist’.

³⁶ Borisov quoted in ‘The development of artificial intelligence is necessary for the successful conduct of cyber wars’, Russian Ministry of Defence, 14 March 2018, https://function.mil.ru/news_page/person/more.htm?pid=12166660@egNews&print=true.

³⁷ ‘Shoigu Zayavil, Chto Voennyye I Grazhdanskie Uchenyye Dolzhny Sovmestno Razrabatyvat’ Tekhnologii Iskusstvennogo Intellekta [Shoigu Stated That The Military and Civilian Scientists Have To Jointly Develop AI Technologies].’ *Business Gazeta*, March 14, 2018, <https://www.business-gazeta.ru/news/375400>.

³⁸ Anastasia Korol, ‘Why Russian programmers are the best’, MyKeytoRussia, 2022, <https://mykeytorussia.com/edited-why-russian-programmers-are-the-best/#:~:text=Russian%20coding%20teams%20successfully%20represent,Collegiate%20Programming%20Contest%E2%80%9D%2013%20times;Victoria%20Ryabikova,Why%20are%20Russian%20programmers%20the%20best%20in%20the%20world?>; Victoria Ryabikova, ‘Why are Russian programmers the best in the world?’, *Russia Beyond*, 1 June 2021, <https://www.rbth.com/science-and-tech/333855-why-are-russian-programmers-best-in-the-world>.

This push to develop systems that will aid the Russian military's application of information warfare is accepted at the very top. The head of the military, General Gerasimov has specifically stated that, 'the study of issues of the preparation and conduct of information actions is *the most important task of military science* [emphasis added].³⁹ He is not privileging the development of better missiles or robots or any other weapons systems – he wants, most of all, the better development of cyber-psychological and cyber-technical tools.

The Ukraine experience

Over the last decade or so, much concern has been felt in Western military defence and security circles in regard to the threat posed by Russian offensive cyberspace operations. And if these were to be enhanced by AI then this threat level could be raised exponentially. Perhaps Russia could win a war 'in seconds'. But this concern seems to have been dissipated to a significant degree by events in Ukraine. While there has been a substantial number of Russian offensive cyber operations against Ukrainian targets,⁴⁰ the expected level, given all the prior hype,⁴¹ has failed to materialise (at least at the time of writing in June 2022). Russia, 'the most aggressive cyber actor in the world' has not lived up to its reputation. And while there was some evidence of AI-enhanced offensive cyber activities there was, again, not the degree expected. As one observer put it, 'aside from Russian influence campaigns with their much-discussed "deep fakes" and misinformation-spreading bots, the lack of known tactical use (at least publicly) of AI by the Russian military has surprised many observers.'⁴²

This could all obviously be a case of the Russian military simply not having the AI capabilities that had previously been assigned to it by many Western analysts (and even its use – as mentioned earlier – of deepfakes has been judged to be pretty amateurish⁴³). But it could also, however, be a case that Ukrainian cyber defences (with some assistance from the West) have proved stronger than anticipated. And it all, of course, could be because – as the former NATO supreme commander, Admiral James Stavridis, has said – '*Putin [is] saving massive scale non-deniable cyber-attacks for a later stage of the conflict*'. *This would, he presumes, be in retaliation for when Western 'sanctions really start to bite*'.⁴⁴ This may, indeed, have come to pass after this chapter here has been published.⁴⁵

³⁹ Gerasimov, 'Vektory Razvitiya Voennoy Strategii.'

⁴⁰ Raphael Satter, Christopher Bing and James Pearson, 'Microsoft discloses onslaught of Russian cyber attacks on Ukraine,' *Reuters*, 27 April 2022, <https://reuters.com/technology/microsoft-discloses-onslaught-russian-cyberattacks-ukraine-2022-04-27/>.

⁴¹ Ryan Browne, 'The world is bracing for a global cyberwar as Russia invades Ukraine,' *CNBC*, 25 February 2022, <https://www.cnbc.com/2022/02/25/will-the-russia-ukraine-crisis-lead-to-a-global-cyber-war.html>.

⁴² Eric Tegler, 'The vulnerability of AI systems may explain why Russia isn't using them extensively in Ukraine,' *Forbes*, 16 March 2022, <https://www.forbes.com/sites/erictegler/2022/03/16/the-vulnerability-of-artificial-intelligence-systems-may-explain-why-they-havent-been-used-extensively-in-ukraine/?sh=5ecf559837d5>

⁴³ Max Mason, 'Deepfakes and espionage, but no cyber apocalypse from Ukraine invasion,' *Financial Review*, 9 May 2022, <https://www.afr.com/policy/foreign-affairs/deepfakes-and-espionage-but-no-cyber-apocalypse-from-ukraine-invasion-20220425-p5afvt>.

⁴⁴ Catherine Philp, 'Putin armed cyberattack aimed at me, says former MI6 chief,' *The Times*, 26 May 2022, <https://www.thetimes.co.uk/article/putin-aimed-cyberattack-at-me-says-former-mi6-chief-sir-richard-dear-love-xtlq83cql>

⁴⁵ Kari Paul, 'Russia's slow cyberwar in Ukraine begins to escalate, experts say,' *The Guardian*, 2 April 2022, <https://www.theguardian.com/world/2022/apr/01/russia-ukraine-cyberwar>; 'The world holds its

However, the lack of major cyber attacks could also be a matter of the Russians wanting, as it were, to ‘keep their cyber powder dry’ for a more significant future conflict – i.e., one with the lead countries of NATO itself. That is, the Russian military would not want to expose just what cyber capabilities it does possess because their use against Ukrainian targets would alert NATO cyber specialists. The cyber *modus operandi* employed by the Russians would, to a degree, highlight where the cyber vulnerabilities of certain NATO states themselves might lie, and for which defences have not been prepared. If forewarned by Russian cyberattacks NATO could be forearmed. Thus alerting NATO cybersecurity personnel through its activities simply to make some, albeit quite significant, gains against Ukraine might not serve the long-term strategic aims of Moscow.⁴⁶ For what is vital for the Russian military, and something central to its doctrinal thinking, is to retain the ability, with its offensive cyber tools, to generate major shock and thereby cause strategic paralysis in any targeted state.⁴⁷

Thus, when looking at the reasons for the supposed lack of offensive cyber operations by the Russian military against Ukraine, the reasons for it may be seen as not exactly clear-cut.

The effect of the war on Russian AI development

However, what does seem clear is that the Russian invasion of Ukraine and the consequences of it will inevitably have had an effect on the military’s ability to deploy AI across a range of weapons systems and technologies. Included here, of course, will be those related to the use of AI in offensive cyber capabilities. These effects can, from a Russian perspective, be seen as both positive and negative in character.

In terms of the positives, the Russian military will doubtless have gained more data from its experiences in Ukraine. One of the problems for the Russian armed forces in terms of developing any enhanced weapons and weapon systems based on Machine Learning (ML) AI is that there has been of a lack of training data. The best data for the development of ML with military connotations comes from operations against an enemy. As Gregory C. Allen expresses it, ‘NATO has provided weapons and equipment to Ukraine that offers the best opportunity yet to collect operational training data for new AI models and more diverse military AI applications.’⁴⁸ The same will be true in the cyber realm. Data could be collected from the activities of not just Ukrainian cybersecurity actors but also those of NATO as well. All such data-gathering by the Russian military can only help to improve its future AI algorithms for use in various spheres across a range of systems,⁴⁹ including, of course, in cyberspace.

breath for Putin’s cyberwar,’ 23 March, 2022, *Politico*, <https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440>.

⁴⁶ Jaspreet Gill, ‘Russia may be holding cyber capabilities in reserve, so US must keep its shields up: Experts,’ *Breaking Defence*, 14 March 2022, <https://breakingdefense.com/2022/03/russia-may-be-holding-cyber-capabilities-in-reserve-so-us-must-keep-its-shields-up-experts/>.

⁴⁷ Shimon Naveh, *In Pursuit of Military Excellence. The Evolution of Operational Theory* (Frank Cass, London, 1997).

⁴⁸ Gregory C. Allen, ‘Russia probably has not used AI-enabled weapons in Ukraine, but that could change,’ *Center for Strategic and International Studies*, 26 May 2022, <https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change>; <https://ria.ru/20220414/tekhnika-1783437321.html>

⁴⁹ Alexandr Kruglov, Alexei Ramm and Evgenii Dmitriev, ‘Sredstva PVO Obyedenyat Iksusstvennym Intel-
lektom [Air Defence Systems Will be United Using Artificial Intelligence],’ *Izvestiya*, 2 May 2018,

While there does seem to be this one positive in terms of the development of AI in Russian military systems, there are several negatives. First, in the wake of the conflict in Ukraine a great many foreign high-tech firms with interests and investments in Russian AI development are now cutting their links with Russia. The investment they had been provided along with the high-tech components they supplied are now lost, including those that could be used, however tangentially, in military applications. The Russian government will now have to provide more of its own investment funds and, crucially, have to find its own source of microchips and microprocessors. And then there are the general post-invasion sanctions, of course, imposed by the West. These will further limit Russian access to high-tech components. There is also now bound to be less contact with Western academics and fewer opportunities for Russian academics and engineers to interface with and gain knowledge of Western practices and technologies.⁵⁰

Another natural follow-on effect of the invasion is that skilled Russians involved in both the development of AI and in the cyber security and defence fields are now leaving Russia. They are and will be seeking employment abroad where they can continue their work unhindered by sanctions and by academic and technological limitations. Their skills are in high demand. Many will go to the West but others will be drawn to high salaries in China.⁵¹ According to Jonathan Vanian, since 2014 when Russia annexed Crimea and occupied much of the Donbas, ‘50,000 to 70,000 Russian IT workers have left the country because the sanctions have cut off access to technologies that they need to do their jobs.’ The brain-drain evident since then is now likely to reach very significant proportions. Some 70,000 to 100,000 are expected to follow. They have left, post invasion, for the likes of Armenia, Turkey, Georgia and the United Arab Emirates. It has been a veritable exodus.⁵²

Russia may, indeed, have the world’s best mathematicians and programmers that could boost the country’s development of AI systems – including those related to AI-enhanced offensive cyber - but they are no use to Russia if significant numbers of them move abroad. Obviously, however, those skilled personnel who are actually working in the defence sector may not be allowed to leave.

Overall, and while the Russian military will have more data now on NATO’s cyber potential, the general post-invasion dynamic is that Russia is bound to lose now in the scramble to gain ‘first mover advantage’ or even, possibly, to be anywhere close to matching advances in the United States or China. As one analyst puts it, *‘With the weight of Western sanctions crippling parts of the Russian economy, the consensus seems to be that Moscow’s ambitions of being a major player in the development of machine learning, robotics, natural language processing and other artificial intelligence (AI) tools are functionally dead.’* This has led

<https://iz.ru/733333/aleksandr-kruglov-aleksei-ramm-evgenii-dmitriev/sredstva-pvo-obediniat-iskusstvennyy-intellektom>.

⁵⁰ Jonathan Vanian, ‘Invading Ukraine has upended Russia’s AI ambitions - and not even China may be able to help,’ *Fortune*, 25 March 2022,

<https://fortune.com/2022/03/25/russia-ai-sanctions-ukraine-china/>

⁵¹ Ibid.

⁵² Cade Metz and Adam Satariano, ‘Russia’s tech industry faces “brain drain” as workers flee,’ *The New York Times*, 13 April 2022, <https://www.nytimes.com/2022/04/13/technology/russia-tech-workers.html>

to a headline in one US journal that reads '*Russia's AI industry faces collapse*.'⁵³ Indeed, it may.

The future

With Russian offensive cyber in mind, there is perhaps one particular consequence of the Ukraine conflict that NATO states might be wary of. This is that Moscow's military, having experienced such setbacks on the battlefield, and having become yet more conscious of its inferiority vis-à-vis the forces of the Alliance, might now put even more emphasis on its asymmetric activities. Included here might be an increased emphasis on using AI-enhanced offensive cyber to achieve strategic effect. The Russian military might increase its 'cyber aggression.'⁵⁴ And it might want to impress on its civilian masters in the Kremlin that, if Russia is to prevail in any future major conflict with NATO, it must strike first. It must 'neutralise' its NATO adversaries before, the thinking might run, those adversaries might try to neutralise it. And the most likely tool in this respect in the Russian armoury will still probably be, and despite the Ukraine experience, the use of an AI-enhanced cyberattack – most notably in a cyber-technical form.

⁵³ Brendan Bordelon, 'Russia's AI Industry Faces Collapse,' *Digital Future Daily*, 8 August 2022, <https://www.politico.com/newsletters/morning-tech/2022/03/08/russias-ai-industry-faces-collapse-00014998>.

⁵⁴ Christopher Whyte, 'Russia's AI setbacks will likely heighten its cyber aggression,' *CSO*, 14 April 2022, <https://www.csoonline.com/article/3656957/russias-ai-setbacks-will-likely-heighten-its-cyber-aggression.html>.

10

REPRESENTATIONS OF WOMEN SOLDIERS IN RUSSIAN ARMED FORCES 2008–2021

Jonna Alava

The presentation made by Jonna Alava in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=xGvzdwIdZ5M> starting from 27:30.

11

ADMIRAL USHAKOV: A STUDY OF RUSSIAN POWER PROJECTION

Aristide M. LaVey

The presentation made by Aristide M. LaVey in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=xGvzdWIdZ5M> starting from 52:00.

Imagery is one of the most powerful tools available for informing internal and domestic audiences and for influencing foreign audiences.

—U.S. Department of Defense Joint Publication 3-0
Joint Operations

Introduction

This article introduces research that I am developing on the topic of visual information and cultural power projection, specifically Russian military and spiritual power projection via the image of Admiral Fedor Fedorovich Ushakov.



Picture 1. Image of Ushakov in Moscow (Photo by A.M. LaVey)

Ushakov was born in 1745 into a military family. He attended naval cadet training in St. Petersburg and after serving as a midshipman in the Baltic Fleet, transferred to the Don-Azov Flotilla and then to the Black Sea Fleet where he spent most of his career.

Ushakov distinguished himself in the Russian-Turkish Wars and was Catherine the Great's military governor and

head of the admiralty in Crimea in 1783, eventually became the commander of Sevastopol and the Black Sea Fleet. After the Mediterranean campaigns of 1794-1800, he returned to St. Petersburg and served on the headquarters staff and commander of the Joint Forces Baltic fleet, before becoming the head of the Russian Imperial Navy.

After Catherine’s reign and then Paul I’s, Alexander I had little interest in Ushakov and his last seven years were unpleasant for the admiral who did not care much for staff work, so he retired in 1807 to Tambov, in present day Mordovia. During his retirement he was asked to return to duty for the Patriotic War of 1812, but instead funded and built hospitals for wounded veterans. He died in 1817.

Ushakov is known as a skillful tactician, developing and updating Russian naval doctrine and for never losing a battle. The admiral was rehabilitated in the 1940s by Stalin and later canonized by the Russian Orthodox Church in 2001.



Picture 2. Image of Ushakov in Moscow (Photo by A.M. LaVey)

That last bit of information might be surprising for some. How could a career military serviceman become a saint?

Hagiographer V.D. Ovchinnikov (2016) wrote that after having his heart broken as a young lieutenant, Ushakov devoted 100 percent of his energy to his troops and their families, his country and the navy. He spent

his pay on troop welfare and this was especially documented during his time in Crimea. Later he gave all of his pension to wounded veterans and the local monastery. Ushakov was known for his modesty, self-sacrifice and a real love for his troops. During the Mediterranean campaigns, he was known as a liberator and defender of Christians.

In a 2007 *Voice of Russia* broadcast, hagiographer Valery Ganichev said that “Ushakov was canonized not for his military heroism—this isn’t enough in itself for canonization—but for the way he managed to convey the image of a true Christian in conditions of battle, serving his duty on the frontlines, yet always ready to sacrifice his life for others. This is why his memory lived on among the people.”

In 2015 I was a member of a detachment of paratroopers from the U.S. Army’s 173rd Airborne Brigade embarked upon the British Royal Navy warship H.M.S Ocean in the Baltic Sea, for BALTOPS, the annually recurring multinational exercise designed to increase interoperability of allied and partner forces in the Baltic region. My job as a strategic communications officer was to gather and disseminate information in support of that mission.



Picture 3. The icon of St. Fedor Ushakov can be seen in the upper left corner between the first and second soldier in this photo of the HMS Ocean chapel. (Photo by the UK Ministry of Defense)

It was aboard the Ocean that I first met Admiral Ushakov. Visiting the ship's library next to St. Michael's Chapel I was surprised to see a Russian Orthodox icon hanging in the chapel. Who was this haloed man in a military uniform? A framed letter hung nearby introduced me to the admiral and gave a short biography, also mentioning that the icon was a gift from a group of visiting Russian naval officers.

After that experience, I kept seeing images of Ushakov everywhere I went. I expected to find him in St. Petersburg as he had been educated there and spent most of his career there when not at sea. I saw his image on icons in churches all over the city and his commanding statue at the Naval Cathedral of St. Nicholas in Kronstadt. In museums in the northern capital and in Sevastopol I saw his likeness, heroic portraiture and massive stone busts, as well as personal artifacts.



Picture 4. Two images of Ushakov in St. Petersburg (Photos by A.M. LaVey)

I directly encountered his bodily relics in his carved, wooden nautical-themed casket located at his shrine located at the Sanaksar Monastery of the Nativity of the

Theotokos in Temnikov, in the western part of the Republic of Mordovia. I have yet to visit the Cathedral of Saint Fyodor Ushakov, the first of his name, located in the republic's capital of Saransk, but I have seen images of the commanding edifice that anchors the central square.

These places, directly associated with Ushakov, I expected to find him, but it was the places where I did not expect to find him that surprised me. I observed a surprising number of his images in landlocked Moscow, likely a place he never visited, but this is perhaps understandable as it is the capital of the modern Russian Federation. But what about the Garrison Church of St. Nicholas in Brest, the Convent of St. Elizabeth in Minsk, the Cathedral of the Nativity in Riga, multiple churches in Odesa, and of course a British warship?

It is my belief that promoters of official Russian culture—the troika of church, military and political leaders—are actively using the image and personage of Ushakov as a tool for soft power projection in order to propagate an example of an ideal Russian—a righteous Orthodox warrior.

In my research I hope to introduce Russia's most recent military saint and the important role he plays in Russian culture, highlighting the ideological relationship between the Russian church, military and state. Using the semiotic framework of J.M. Lotman and Tartu Moscow Semiotic School, specifically the role of artistic information and the semiotics of culture, I will bring attention to how his image is being used for cultural power projection and analyze the visual aspects of Russian information operations in the ever-changing Russian infosphere.

Theory

Semiotics is a cultural metalanguage that allows for the unification of the different structures of visual culture and military science. One of the foundational understandings of the Tartu School is the semiotic system, the functions of which is the modeling of the world. Natural languages, for example Finnish, English and Russian, are a group's primary modeling system and gives the members of that group a sense of their cultural structure. Secondary modeling systems are extralinguistic sign systems that groups use to construct cultural texts that mediate information, such as music, dance and in this instance, religious art. The semiotics of culture is the study of these secondary modeling systems. Russian hagiographic texts cannot be studied in isolation, and thus it is necessary to determine their place within the Russian world and its cultural system.

Why is the understanding of religious art important to military science? Art is a communicative system and what Lotman called the highest incarnation of culture (1977). Art serves as a modeling system that can organize and create the way we see the world and our reality, and is a distinct and perhaps universal method for analyzing the different cultures of the world. American military doctrine (2018) also recognizes visual information as one of the most powerful tools available for informing domestic audiences and for influencing foreign audiences. Imagery of this long dead imperial admiral would have no meaning in contemporary society without the usage, remediation, and recontextualization of his image (Ibrus and Ojamaa 2018).

Lotman's concept of the semiosphere—a cultural space where semiosis happens—for micro, meso and macro-level target analysis. I suggest that there are multiple

targets, including the Russian semiosphere (military, church and citizenry), Orthodox semiosphere (Russian, the Near abroad and worldwide), military semiospheres (Russian as well as foreign via military-diplomacy, and international cooperations and operations) and the non-Russian mediasphere.

Ushakov's role in Russian culture

The majority of my observed examples are religious icons, but the cult of Ushakov is also supported by the church and state with numerous military, educational and community groups that bear his name, as well as events like Ushakov Youth Olympiads, held at state schools and partnered with local military and religious officials.

Ushakov is also featured on many Russian postage stamps. Stamps are state-sponsored iconic texts and are powerful symbols that communicate national ideals inside and across Russian borders. Most Ushakov philately is from Russia, but a recent example, issued by the Dniester Moldovan Republic, is seemingly out of place. The first day of issue ceremony was held at the Cathedral of the Nativity in Tiraspol, and was attended by state and religious leaders who called Ushakov a powerful Russia figure and a wonderful example for devout believers (TSV 2020).

Since his canonisation in 2001, numerous visual representations, including churches, memorials, statues, stamps and icons have proliferated not only in Russia, but also throughout the Mediterranean, the Black Sea and the Russian world. Recent state-funded additions include three images in the Main Cathedral of the Russian Armed Forces finished in 2020, and a wooden military chapel built in 2018 and a newer 2020 memorial at the Russian naval logistics base in Tartus, Syria (Ministry of Defence of the Russian Federation 2020).



Picture 5. Three examples of philatelic Ushakov: Russia, Dniester Moldovan Republic and the USSR.

Soviet films introduced many to Ushakov, in fact Patriarch Kirill, at a 2019 blessing of a new church dedicated to St. Fiodor in the Moscow region¹, mentioned that he was fascinated by the actions of the man and it was the first color film he saw (Press service of the Patriarch of Moscow and all Rus 2019). Modern documentaries (and social media platforms, such as TikTok) produced by military and religious broadcasters continue to bring the word to a new generation to be amazed by Ushakov's undefeated military record, piousness and patriotism.

Recent Russian-language academic literature about Ushakov focuses on military culture, especially themes of patriotism, morality and the spiritual development of military personnel (Levchuk 2016, Didov 2014). Other research lists Ushakov as the source of all Russian military-diplomatic activities (Rassokho-Anokhina 2013), and defines Russia's place in international affairs, especially in Crimea, the Black Sea and the Balkans (Kovalenko 2019, Gnedneva & Chernykh 2016). Many others highlight Ushakov's useful position in the pantheon of Russian military saints, as it relates to the development of contemporary Orthodox culture in the armed forces (Smirnov 2016, Panichkin 2017, N.E. Ratnikov & R.O Rosina 2012).

Patriotism, along with politics, war and international relations is written into the Russian Orthodox Church's social catechism, *Bases of the social concept of the Russian Orthodox Church*; and is suggested that religious patriotism is a sacred duty for all Orthodox Christians who are called to follow in the path of the holy saints before them in their love for, and dedication to, the fatherland (Kirill 2003).

While there is certainly a push to increase spiritual life in Russia, there is another type of practice, targeting not-so-religious adherents to what researcher Elena Kahla defines as cultural, rather than religious Orthodoxy, which is the embedding of national ideas into symbols which manifests themselves in memory politics and cultural production (2016).

Ushakov in the west

Ushakov is generally unknown outside Russia, even to Russianists. An English-language literature review netted very little, just a few mentions in Russia's Mediterranean campaigns (McNight 1965), Crimea (Kozelsky 2014) and his connection to religious nationalism (Fomina 2019), but most instances refer to the Russian or Soviet warships named after him.

Additionally, the admiral's name often appears on the English-language mediasphere relating to the presentation of the Ushakov Medal to foreign servicemembers, often for their service in the Arctic Convoys. The Russian Embassy in London notes that the medal has been awarded to more than 3,300 foreigners (2015).

There are popular reports of his sainthood, its application as the patron saint of nuclear bombers, and also religious and culture media, including those financed by the Russian state and Orthodox evangelists.

¹ The liturgy was attended by military officials from the Ministry of Defense, government officials the Duma and the security services, as well as religious leaders, such as the chairman of the Synodal Department of Youth Affairs. <http://www.patriarchia.ru/db/text/5552433.html>.

Closing

There is much active and recent Russian-language scholarship on Ushakov's place in contemporary military and religious society, but yet he remains invisible to outside scholars. I put forth that in order to understand the religious dimension of patriotism that drives Russian policy, we must know Ushakov and I hope my research will do just this.

Questions from the audience

Q1: How is the theme of sacrifice present in your work?

A2: Ushakov not only made personal sacrifices for his men and their families throughout his career, and especially in Crimea, but during the Mediterranean Campaign he offered himself and paid ransoms in exchange for the lives of captured French soldiers. This is the type of servicemember every military wants—someone who is willing to sacrifice himself for the mission.

Q2: Why do you think Ushakov is emphasized over other saints with military connotations, such as Saint Elijah, Saint Alexander Nevskii or Saint Fiodor Stratilat?

A2: Contemporary servicemembers are able to identify more with Ushakov than Saint Elijah, because there is a realness to him and because he is the only “modern” military saint of our times. He is often called the saint in shoulder straps (epaulets with military rank), and his hagiography tells of his life and the struggles of military life in a very real way.

References

- Didov, P. V. 2014. “Moralnyi kodeks pravoslavnogo voina.” *Istoricheskiye, filosofskkiye, politicheskkiye i yuridicheskkiye nauki, kulturologiia i iskusstvovedeniye. Voprosy teorii i praktiki* 11 (1): 70-75.
- Ibrus, I., and M. Ojamaa. 2018. “The Creativity of Digital (Audiovisual) Archives: A Dialogue Between Media Archaeology and Cultural Semiotics.” *Theory, Culture & Society* 37 (3): 49-70. doi:10.1177/0263276419871646.
- Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland. 2015. “Update on the progress of the Ushakov medal campaign.” *Ushakov Medal*. <https://rusemb.org.uk/ushakov/>
- Gnedneva, A. R., and V. D. Chernykh. 2016. “Rol F.F. Ushakova v sozdanii Azovskodonskoy flotilii.” *Sovremennyye problemy gumanitarnykh i obshchestvennykh nauk* 4 (2): 11-16.
- Fomina, V. 2019. *Dead Heroes and Living Saints: Orthodoxy, Nationalism, and Militarism in Contemporary Russia and Cyprus*, Doctoral thesis. Budapest: Central European University.
- Joint Chiefs of Staff. 2018. *Joint Publication 3-0 Joint Operations*. Washington, DC: Department of Defense. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.
- Kahla, E. 2016. “Third Rome Today or State Church Collaboration in Contemporary Russia.” Edited by T. Nygaard. *Russia and the Nordic Countries: State, Religion, and Society*. <http://dansk-norsk.no/uploads/files/Report-State-religion-society.pdf>.
- Kirill (Metropolitan of Smolensk and Kaliningrad). 2003. “Tserkov i mir—osnovy sotsialnoy kontseptsii Russkoy Pravoslavnoy Tserkvi.” *Doklad mitropolita Kirilla na IX Rozhdestvenskikh chteniyakh*.

- Kovalenko, V. I. 2019. "Fedor Fedorovich Ushakov (vzglyad politologa)." In *IV mezhdunarodnogo nauchnogo foruma, 75-letiyu Krymskoy nastupatel'noy operatsii 1944 goda i 5-letiyu vossoyedeniya Sevastopolya i Kryma s Rossiei*. Sevastopol: Sevastopol State University.
- Kozelsky, M. 2014. "Religion and the crisis in Ukraine." *International journal for the Study of the Christian Church* 14 (3): 219-241. doi:10.1080/1474225X.2014.957635.
- Levchuk, S. V. 2016. "Admiral F.F. Ushakov: Grazhdanstvennost, pravstvennost, patriotizm." *Innovatsionnoye obrazovaniye I ekonomika* 21:55-58.
- Lotman, J. M. 1977. *The structure of the artistic text*. Translated by R. Vroon. Ann Arbor: University of Michigan.
- McNIGHT, J. L. 1965. *Admiral Ushakov And The Ionian Republic; The Genesis Of Russia's First Balkan Satellite*, Doctoral thesis. Madison: The University of Wisconsin—Madison.
- Ministry of Defence of the Russian Federation. 2020. "V siriyskom Tartuse sostoyalos torzhestvennoye otkrytiye byusta vydayushchegosya russkogo flotovodtsa admirala Fyodora Ushakova." *Novisti*, 2020.
- Ovchinnikov, V. D. 2016. *Admiral Fiodor Ushakov: Cviatoi pravednii vojn*. Iaroslavl: Akademiia 76.
- Panichkin, A. F. 2017. "Svyatoy admiral." *Morskoy sbornik* 8 (2045): 88-91.
- Press service of the Patriarch of Moscow and all Rus. 2019. "Slovo Sviateishogo Patriarcha Kirilla v Nedeliu 27-iyu po Piatideciatnitye posle liturgii v khrame pravednovgo voina Feodora Ushakova v Iuzhnom Butove g. Moskvy. *The Russian Orthodox Church*. <http://www.patriarchia.ru/db/text/5552419.html>
- Rassokho-Anokhina, V. N. 2013. *Gosudarstvennaia voyennaia, voyenno-diplomaticheskaiia i blagotvoritelnaia deyatelnost admirala Fedora Fedorovicha Ushakova*, Doctoral thesis. Moscow: Military University of the Ministry of Defense of the Russian Federation.
- Ratnikov, N. E., and R. O. Rosina. 2012. "Svyatyte polkovodtsy: kanonizatsiya i pochitaniiye." *Zashchita otechestva i tsennosti patriotizma v russkoy kul'ture, istorii i sovremennom vospitanii*, 302-314.
- Smirnov, Y. N. 2016. "V pamyat o svyatykh voynakh: nagrody velikoy otechestvennoy voyny." *Tsentri i periferiya* 4:4-10.
- TSV. 2020. "Marka s Ushakovim." YouTube. <https://www.youtube.com/watch?v=eZr2BtupVqI>.
- Voice of Russia. 2007. *The Christian Message from Moscow: Saint Blessed warrior Fyodor Ushakov*, Radio broadcast. Rossiya Segodnya.

JUSTIFYING THE USE OF FORCE: RUSSIA'S SPIRITUAL AND NATIONAL SECURITY

Santeri Kytöneva

The presentation made by Santeri Kytöneva in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=xGvzdwIdZ5M> starting from 1:15:00.

Introduction

This article is a continuation of research done in the fall of 2021. The conducted research focused on analysing articles written by Mahkmut Gareev (1923–2019) mainly released in Russian military science journals. The end result was an academic paper in Finnish on the concept of spiritual security. In conclusion the earlier article traces the genealogy of spiritual security to early 2000's in Gareev's articles. Gareev sees spiritual security as part of information security with growing importance in the future.¹

The seminar article following the presentation given at Russia seminar 2022 concentrates on the topic of spiritual security and the justification of the use of force. In this article I will conceptualise the phenomena described in Gareev's articles as spiritual security. Spiritual security will then be connected into the discussion surrounding the justification of the use of force. The article also builds on categorisation put forward by the Norwegian military science researcher Tor Bukkvoll into three schools of thought in Russian military science: traditionalists, modernists and revolutionaries.²

This taxonomy is developed here in the context of state security. Main reason for developing this taxonomy is to clarify the discussion on the importance of spiritual security and connect it into the justifying the use of force.

The structure of the article is the following. Firstly, I define the following key concepts: spiritual security and information security. I will explain how these concepts are interlinked and how their meaning has evolved in the context of Russian strategic thought. Secondly these concepts will be connected to the traditionalist theoreticians, following a categorisation given by Tor Bukkvoll in a 2011 released article.³ Thirdly theoretical assumptions on spiritual security are presented and tied together into the logic underlying the justification of force in Gareev's thought. I will put forward a hypothesis that the dominant view on many of the current theoretical debates on state security is one of the traditionalists. Finally, I will consider the way in which these spiritual factors can possibly be used in order to justify the application of military force.

¹ Kytöneva 2021

² Bukkvoll 2011

³ Bukkvoll 2011

The three main arguments of the article, which I will elaborate on are the following: Firstly, spirituality is gaining further importance in Russia's strategic planning documents and practical measures. Secondly, traditionalists, who dominate the current debate on the issues of spiritual security, argue for further centralized state control. Thirdly, spirituality is connected to justifying the application of military force, for both the citizens and the soldiers. Aim here is to elaborate on the logic underlying the justification of force.

Spiritual security

Spirituality as a concept remains elusive. It can be approached from individual experience of felt connection towards a greater idea. However, the focus of this presentation is more on the group-centric state defined spiritual and its usage in justifying certain measures. Contents of spirituality vary depending on the time period, target audience and the use of the concept. Some definite background can be set here on the contemporary Russian state endorsed spirituality: contemporary Russian state-defined spirituality is closely intertwined with Orthodox Christianity and patriotism.

The focus here will be on spiritual security (духовная безопасность), which is a concept that Gareev has used in his publications in military scientific journals. It is therefore a concept up on which some theoretical debate can be found in the Russian military scientific community. Gareev defines spiritual security as part of information security. The concept is closely connected to protecting the memory of the Great Patriotic War and Russian spiritual foundations. In order to clarify the elusive concept of spirituality, attention should be directed towards narratives of the past Russian wars and the way in which they are utilised in the military setting.

Gregory Carleton describes the Russian identity to have a performative aspect in the sense of deeply embedded pride in defending the nation, protecting the faith and saving the continent. Russian national pride is deeply intertwined with orthodox Christianity both in the past and present.⁴ Spiritual aspects and their collective foundations appear then to be connected into war and Christianity.

Spiritual security at the state level aims towards maintaining unity in national ideas of great importance, therefore securing a strong and well-defined spiritual foundation. At the level of the individual soldier this means maintaining high morale and readiness to self-sacrifice. It is a feature of Russian strategic culture with long roots in past wars spanning over decades. The Russian soldier is presented as extremely persistent and in spiritual strength superior to the competition.

Spiritual security in Russia's strategic planning documents

The three Russian strategic planning documents I will briefly consider in their newest form are the following: Doctrine of Information Security (2016), National Strategy (2021) and The Military Doctrine (2014). The aim is to bring forward the issues of spiritual security and their context in the Russian strategic documents. The 2021 released National Strategy includes a separate section on protecting the traditional Russian spiritual and moral values, culture and historical memory. The Doctrine of Information Security of The Russian Federation defines national interests in the informa-

⁴ Carleton 2017, 63–64

tion sphere. Noteworthy is that this doctrine also focuses on critical infrastructure and other interests of Russia in the information sphere, but I will not consider these in the context of this article. The corruption of Russian spiritual values is noted as a threat in the information sphere.

The military doctrine lists activities undermining spiritual and patriotic traditions as a main internal threat. Active measures are required to defend these national interests. The logic of defending national interests and justifying different measures is something I will return on later in the presentation. The official Russian doctrine on information security defines information security as the implementation of legal measures used to predict, contain and eliminate informational threats in order to ensure the rights of the citizens.⁵ The information security doctrine approved by the president of the Russian federation in 2016 lists measures and their strategic goals. The doctrine defines information security as part of the national security of Russian federation.⁶

The information security doctrine defines one national interest to be the preservation of cultural and moral values of the Russian Federation.⁷ This claim is also repeated in the 2021 National strategy of the Russian federation, where strengthening traditional Russian spiritual and moral values is defined as one of its national interests. The strategy also notes preserving the cultural and historical heritage as one of national interest.⁸ One of threats identified in the doctrine on Russian information security is the influence on values of the young people.⁹

A strategic goal highlighted in the doctrine on information security is the neutralisation of means aimed at undermining the historical and patriotic values tied into defending the fatherland.¹⁰ On the grounds of these official doctrines the phenomena underlying spiritual security comes in light as a problem of information security with growing importance in the near future, which parallels closely what Gareev wrote on the topic earlier.¹¹

⁵ The Doctrine of Information Security of the Russian Federation 2016 "информационная безопасность Российской Федерации (далее - информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;"

⁶ The Doctrine of Information Security of the Russian Federation 2016 "30. Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации."

⁷ The Doctrine of Information Security of the Russian Federation 2016 "... а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;"

⁸ Russian National Security Strategy 2021 "7) укрепление традиционных российских духовно-нравственных ценностей, сохранение культурного и исторического наследия народа России;"

⁹ The Doctrine of Information Security of the Russian Federation 2016 "Нарастает информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей."

¹⁰ The Doctrine of Information Security of the Russian Federation 2016 "А) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества."

¹¹ Kytöneva 2021

The hierarchical structure of these three concepts can then be noted to be the following:



Picture 1. Classifying Russian military theorists on issues of state security

Now in order to explain the underlying thinking in these documents, I will return to the aforementioned classification of Russian military theorists. In his article Tor Bukkvoll categorises Russian military theorists into three schools of thought: traditionalists, modernists and revolutionaries. Bukkvoll presents this cat-

egorisation in the context of military technological resource allocation and its relation to personnel resources in the army. Traditionalists and modernists believe that the nature of war remains fundamentally unchanged regardless of technical developments. Traditionalists highlight that new technology should not come at the expense of manpower. Modernists however value reallocation of resources to technology in some cases. Revolutionaries believe in fundamental change in the nature of war that comes with the development of new technologies.¹²

In this article I will extend the categorisation into debate on state security and issues of spiritual security. The aim is to offer a positive definition to traditionalists' thinking. I argue that the traditionalists desire stricter state-controlled implementation of spiritual security. Traditionalist theorists recognise the need for spiritual security as a separate domain of national security. Non-traditionalist theorists on the other hand do not necessarily desire stricter control and therefore also do not see the need to conceptualise and develop measures regarding spiritual security.

Traditionalist school of thought

Bukkvoll names Mahkmut Gareev as one traditionalist theoretician.¹³ Gareev was the first president of the Russian Academy of Military Sciences (Академия военных наук) and widely published author. Mari Puurunen clarifies the link between Gareev's publications and the development of the official strategic planning documents in her working paper, concluding that Gareev influenced the development of Russian military doctrines as an influential theorist.¹⁴ Gareev is also recognised as a traditionalist in the taxonomy developed here.

Traditionalists in the context of state security can be characterised by the following theoretical assumptions: firstly, the need for a strong state. Secondly, they maintain the importance of ideological unity. Thirdly, traditionalists see protecting the memory

¹² Bukkvoll 2011

¹³ Bukkvoll 2011

¹⁴ Puurunen 2021

of past wars as an important task. Finally, traditionalists desire actions in protecting and strengthening what are defined as Russian values.

Traditionalists see the role of the state as critical and undeniable in building and strengthening ideology, a viewpoint repeated by Gareev, Ilyin and Uryupin¹⁵ Gareev repeatedly stresses in his writings the need for a separate state organ in handling issues of spiritual security.¹⁶ Traditionalists desire actions toward state-controlled ideology at the root of patriotism. Strong state is seen as necessary by traditionalists and this is closely related to the next theoretical assumption.

Traditionalists see the absence of ideology as a harmful state. The underlying reasoning is that an ideological void will most likely be filled from the outside, possibly with anti-Russian content. The state of ideological void is seen as a harmful state of matters by traditionalists. Ilyin and Uryupin argue that void in the sense of ideology needs to be avoided, or it will be most likely filled from the outside.¹⁷

Without a collective national idea, the traditionalists see perceived threats such as colour revolutions and globalisation actualising further. Both of these threats are seen as driven from outside and being harmful to Russian values. Traditionalists seek to uphold a strong collective national idea in order to combat these issues raising from a possible state of ideological void.

The role of history in strengthening the moral of the soldiers and citizens is central. Traditionalists emphasise the history and memory of the Great Patriotic War. In the matter of past wars traditionalists highlight the role of veterans' stories and see great importance in enhancing a certain narrative in their memory. In his book Gregory Carleton presents the story of the Great Patriotic War as a one with significant strength in building unity between Russian people.¹⁸ Story is told that the people of Russia are matched up against great evil and forced to fight it in order to bring back the good into the world. And the Russians although suffering great sacrifices, succeed in this. The war still plays a great role in defining the Russian collective identity through sacrifices made and ultimately Russia defeating the evil forces.

This story of the war plays a great role in being a uniting the idea at the root of the Russian collective identity. It is seen by traditionalists as an idea too strong to give up on. An idea uniting the people to the land that signifies the meaning of spiritual over material, a viewpoint also written down in the most recent national strategy. Carleton clarifies well the fact that the Great Patriotic War is seen as a sacred event in multiple sources and protecting the war from heresies on many fronts is required.¹⁹ This is also a key focus of Gareev in his collection of works released in a book titled *Battles on the Military-Historical Front*.²⁰

Gareev, Ilyin and Uryupin frame globalisation and the spread of Western values as a threat to Russian spiritual values. Ilyin and Uryupin return to Soviet times in idealising manner as examples of desirable patriotic education. Increasing the need for patriotic

¹⁵ Y. D. Ilyin & V. N. Uryupin 2022, Gareev 2010

¹⁶ Kytöneva 2021

¹⁷ Y. D. Ilyin & V. N. Uryupin 2022

¹⁸ Carleton, G. (2017). *Russia: The story of war*. Cambridge, Massachusetts; London, England: The Belknap Press of Harvard University Press, 2017.

¹⁹ Carleton 2017, 101

²⁰ Gareev 2010

education is something that the traditionalist thinkers desire. Russian tradition according to Gareev is something unique, a feature that needs to be protected.

Summarising traditionalists' theoretical assumptions

Traditionalists aim for deep unity in a national idea built on collective values. State-controlled ideology is justified through history and the perceived greater good in protecting a certain idea of Russia. This idea of Russia is deeply intertwined in the past wars and the struggle of the soldiers and citizens who fought in them. It also lends itself to framing foreign forces as enemy images.

Traditionalists stand for stricter control and active measures on state security. Many of the mechanisms that are put into practice and that underlie the logic of these measures are from Soviet times. Traditionalists highlight the role that morality of the soldiers plays in the outcomes of wars. This going back to past wars and a deep historical tradition of seeing the Russian soldier as spiritually superior to the enemy. Ensuring spiritual security according to traditionalists requires active measures for example in the production of historical education material, controlling harmful media and controversial views especially on the topic of past wars.

At the practical level strengthening spiritual security can mean the following: organising events, directing films, building historical narrative, conceptualising certain images of the enemy. Spiritual security in Gareev's writings brings forward the importance of protecting the memory of the Great Patriotic War, defining spiritual security as part of information security, and raising patriotism in the citizens and the soldiers.

Justifying the use of force

First returning to Gareev's logic underlying the application of military power. Gareev sees the use of military power justified on the basis of sovereign state defending its national interests. Now a key question to raise is, what kind of violation of national interests is great enough to justify the use of force. Defining a key threshold in theory is extremely difficult. However, this is a topic I would like to raise for discussion. Can harmful interference to the patriotic values and Russian spiritual values be interpreted as a violation of national interests that requires defending?

What I have conceptualised in this article as spiritual security is closely related to national ideas with ideological priority. The content of these ideas is built in accordance with the state leaders, the armed forces and the church enjoying mutual support. Strengthening these ideas is important for justifying the use of force both for the soldiers and citizens. Spiritual security is developed in accordance with the national security. The main sphere of logic from which the usage of force can be justified is the requirement to defend national interests: spiritual factors are especially interesting in this line of thought due to them being in contact with ideas seen as a holy and undeniable, with them comes the ability to justify the different measures and control.

Complicated issues of defining the actual content of spirituality and the threshold for the application of military power remain great challenges. Unity is secured on the basis of unchallenged ideological foundations and centralized control. Attention should be put into understanding these centralized power structures and their function in justifying the application of military power.

Traditionalists aim for deep unity in a national idea built on collective values. Ensuring spiritual security according to traditionalists requires active measures in the production of historical education material. State-controlled ideology is justified through history and the greater good in protecting a certain idea of the Russia. This idea of Russia is deeply intertwined in the past wars and the struggle of the soldiers and people who fought them. It offers the basis for also seeing other starting points as hostile, therefore lending itself to building enemy images.

Gareev puts great emphasis on sovereign states' need to protect their national interests. A state that does not protect its national interests is not sovereign. What I have conceptualised in this article as spiritual security is closely tied to patriotism and the ability to uphold the readiness to defend the fatherland through collective unity. Strengthening this unity is important in justifying the use of force both for the soldiers and citizens.

Concluding remarks

Eleven years after Tor Bukkvoll published his article it seems that traditionalists still hold the dominant view within many military scientific debates, one of which being the one on spiritual security. The growing role of spirituality is highlighted in the recent Russian national strategy and theoretical debate on the topic. The future may hold even stricter policies on activities harmful to Russian spiritual values.

Traditionalists seek an ideal that is a united and resilient state, where interests are shared between leaders and population. Answers to threats corrupting unity are seen as centralizing control. Traditionalists see it as critical for state security to maintain a strong government and a strong spiritual base.

Questions and answers

Q: What about revolutionaries in the context of state security? Is coexistence of these views possible in some cases or are they mutually exclusive?

A: Further research needs to be done on the revolutionaries' role and conceptualising the non-traditionalists line of thought. It is by no means certain that traditionalist' thinking remains dominant theoretical view in the future. In my view co-existence of traditionalists' views on state security and revolutionaries' views in other lines of military thought is also possible.

Q: What is the role of sacrifice in the context of this presentation?

A: Sacrifice is an important concept related to all the presentations in our session. Ideas strong enough to warrant sacrifice at the individual level are of the greatest strength. The readiness of the individual ready to self-sacrifice is in my view is an ideal that is desired by the traditionalists.

References

Bukkvoll, T. (2011). Iron Cannot Fight – The Role of Technology in Current Russian Military Theory. *Journal of Strategic Studies*, 34:5, 681–706.

Carleton, G. (2017). *Russia: The story of war*. Cambridge, Massachusetts; London, England: The Belknap Press of Harvard University Press, 2017.

Gareev, M. (2008). Национальные интересы и национальная безопасность России на современном этапе. Вестник Академии Военных Наук No.1, 8–22.

Gareev, M. (2010). *Сражения на военно-историческом фронте*. Moskva: INSAN, 2010.

Пуйн Y. D. & Урупин V. N. (2022). Патриотизм - Духовная Основа Национальной Безопасности России. Военная Мысль, No. 1, 47–64.

Kytöneva, S. (2021). Voimankäytön oikeutuksen lähtökohtia: Venäjän hengellinen ja kansallinen turvallisuus Garejevin mukaan. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 3: Työpapereita nro 24.

Puurunen, M. (2021). *Sotatieteiden akatemian roolista sotilasdoktriinien valmistelussa – Uhkien perusteet*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 3: Työpapereita nro 23.

Official documents

Doctrine of Information Security of the Russian Federation. Approved by Decree of the President of the Russian Federation on December 5, 2016 No. 646.

Russian Military Doctrine 2014, Approved by the President of the Russian Federation on December 25, 2014 No. Pr.-2976.

Russian National Security Strategy 2021, Approved by decree of the President of the Russian Federation on July 2, 2021. No 400.

DEVELOPMENTS IN RUSSIAN COMBAT AIR SPENDING AND LIKELY OPERATIONAL IMPLICATIONS

Justin Bronk

The presentation made by Justin Bronk in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyas-Buw7vg&t=3263s> starting from 8:20:00.

The combat air (fast jet) fleets of the Russian Aerospace Forces (VKS) have been heavily modernised since 2010, as part of successive state rearmament programmes. During the same period, the Russian aircraft industry has also pursued a range of next generation combat aircraft and weapons programmes. This analysis of the procurement patterns of the most recent state armament programmes is intended to shed light on the likely balance of advanced fourth generation platforms and more exotic next generation programmes in the future force structure of the VKS over the coming decade. This is important because the shape of the force will heavily influence the nature of the threat posed to potential adversaries by the VKS itself, and also dictate the likely proliferation patterns of Russian combat aircraft to non-Western aligned states.

Fighter and Strike Fleet Modernisation

The VKS has been comprehensively re-equipped over the past decade with three primary types of modern fast jet, all derived from the T-10 ‘Flanker’ airframe. The key air superiority type is the Su-35S, which is currently Russia’s most potent fully operational frontline combat aircraft. Following its first flight in 2008, the VKS ordered an initial tranche of 48 aircraft in 2009 and a subsequent tranche of 50 aircraft in 2015. The latter order was reportedly completed in May 2021, giving the VKS a total inventory of 98 fighters.¹ One Su-35S crashed in July 2021, and eight have been assigned to the Russian Knights aerobatic display team, leaving 89 aircraft for operational training and frontline use – largely as a replacement for Soviet-era Su-27s.² In early 2021 Defence Minister Sergei Shoigu announced that a further contract had been signed for around 70 billion rubles to cover the delivery of an unspecified additional number of Su-35S.³ Assuming a unit price of somewhere in the region of \$35 million, this would be sufficient to cover around 24 additional aircraft.

¹ Anton Lavrov and Roman Kretsul, ‘Авиаполку прибыло: юг России и Кавказ укрепят истребителями Су-35’ [The air regiment has arrived: the south of Russia and the Caucasus will be strengthened by Su-35 fighters], *Izvestia* (3 May 2021) <https://iz.ru/1158724/anton-lavrov-roman-kretsul/aviapolku-pribylo-iug-rossii-i-kavkaz-ukrepiat-istrebiteliami-su-35> accessed 8 February 2022.

² Aviation Safety Network, ‘ASN Wikibase Occurrence # 266179’, (31 July 2021), <https://aviation-safety.net/wikibase/266179> accessed 9 February 2022.

³ Anton Lavrov and Roman Kretsul, ‘Авиаполку прибыло: юг России и Кавказ укрепят истребителями Су-35’ [The air regiment has arrived: the south of Russia and the Caucasus will be strengthened by Su-35 fighters], *Izvestia* (3 May 2021) <https://iz.ru/1158724/anton-lavrov-roman-kretsul/aviapolku-pribylo-iug-rossii-i-kavkaz-ukrepiat-istrebiteliami-su-35> accessed 8 February 2022.

A parallel, and less ambitious, air superiority modernisation programme to upgrade Soviet-era Su-27P/SM aircraft to Su-27SM(3) standard appears to have ceased at 12 airframes in 2018, alongside an additional 12 newly built Su-27SM(3) aircraft which were delivered between 2009 and 2011.⁴ In light of this, and the unknown but significant number of remaining Su-27 aircraft in service, it seems reasonable to assume that limited-rate Su-35S production will continue through the 2020s to replace the remaining Su-27P/SMs as they are retired.

Alongside the air superiority focussed Su-35S, the most numerically significant combat air modernisation programme has been the acquisition of Su-30SM(2) multirole fighters since 2012. Originally developed as an export product from the Su-27UB twin seat trainer, the Su-30 family had great success on the global export market throughout the 2000s and 2010s. This success provided Sukhoi with significant funding for the development and integration of more modern radars, thrust-vectoring engines and avionics, and as a result the VKS has been able to purchase the modern multirole Su-30SM in significant numbers from 2012. As of mid-2021, approximately 130 Su-30SMs have been delivered to the VKS and the Naval Aviation regiments.⁵ The Su-30SM(2) is now the primary multirole fighter of the VKS and Naval Aviation fleets, and has been used to replace older Su-27s and Mig-29s as the backbone of Russian fighter strength.⁶ It is also replacing Su-24 bombers in some units and being discussed as controllers and wingmen for Su-70 UCAVs alongside the more advanced but troubled Su-57 low-observable fighter.⁷ The VKS also took delivery of twenty Su-30M2 fighters between 2009 and 2012.⁸ These aircraft lack the canards, thrust vectoring engines and PESA radar of the Su-30SM/SM(2) family, and are significantly less capable.

The latest model of the Russian Su-30 family is the Su-30SM(2), which includes the same Irbis-E PESA radar and AL-41F engines as featured on the Su-35S. In 2021 an order was placed for new build examples, with reported numbers varying between 21 and slightly over two dozen.⁹ The Russian Defence Minister stated that the order for these new Su-30SM(2) aircraft and 25 Yak-130 advanced jet trainers would cost a little over 100 billion rubles, which suggests a unit cost in the region of \$35 million for a

⁴ Leonid Nersisyan, 'Russian Combat Aviation: Procurement, Modernization, and Future Outlook', *CNA Occasional Papers* (December 2020), p. 7-9. https://www.cna.org/CNA_files/PDF/IOP-2020-U-028810-Final.pdf accessed 9 February 2022.

⁵ Roman Kretzul and Anna Cherepanova, 'Тяга к лучшему: истребители Су-30СМ получают сверхмощный апгрейд', [Thrust for the best: Su-30SM fighters will receive a heavy-duty upgrade], *Izvestia* (2 May 2021), <https://iz.ru/1159091/roman-kretcul-anna-cherepanova/tiaga-k-luchshemu-istrebiteli-su-30sm-poluchat-sverkhmoshchnyi-apgreid> accessed 9 February 2022.

⁶ For example see 'Курский авиаполк с «алжирскими» МиГами получит Су-30СМ' [Kursk air regiment with "Algerian" MiGs will receive Su-30SM], *Lenta* (28 November 2016), <https://lenta.ru/news/2016/11/28/kursk-su30/> accessed 9 February 2022.

⁷ 'Истребители Су-30СМ2 поведут в бой беспилотники' [Su-30SM2 fighters will lead drones into battle], *Izvestia* (9 February 2022), <https://iz.ru/1288747/2022-02-09/istrebiteli-su-30sm2-povedut-v-boi-bespilotniki> accessed 11 February 2022.

⁸ Leonid Nersisyan, 'Russian Combat Aviation: Procurement, Modernization, and Future Outlook', *CNA Occasional Papers* (December 2020), p. 10. https://www.cna.org/CNA_files/PDF/IOP-2020-U-028810-Final.pdf accessed 9 February 2022.

⁹ Leonid Nersisyan, 'Russian Combat Aviation: Procurement, Modernization, and Future Outlook', *CNA Occasional Papers* (December 2020), p. 10. https://www.cna.org/CNA_files/PDF/IOP-2020-U-028810-Final.pdf accessed 9 February 2022.

new Su-30SM(2).¹⁰ A major upgrade programme has also been agreed to upgrade a large but so far undecided number of existing Su-30SMs to the Su-30SM(2) standard between 2021 and 2027.¹¹ However, the cost of this upgrade programme has not been disclosed. Since the suggested aim is to upgrade the majority of Su-30SMs to SM(2) standard, this programme to upgrade and standardise Su-30 engines and avionics around those of the Su-35S fleet is likely to represent one of the major investment pillars for Russian combat air modernisation efforts during the 2020s. Upgraded Su-30SM(2) aircraft will soon serve with both the VKS and Naval Aviation regiments.

The third core combat air acquisition programme which has been central to VKS modernisation over the past decade is the Su-34 strike bomber, or frontal bomber in Russian terminology. The Su-34 was developed as a specialised bomber variant of the T-10 Flanker airframe with a twin crew in a side-by-side cockpit, a PESA radar optimised for operations against ground targets, retractable forward looking 'Platan' target acquisition and laser designation system and various other modifications to improve its capability as a long-range strike asset. It fulfils a similar high-end tactical strike role within the VKS to that performed by the F-15E Strike Eagle in the US Air Force fighter fleet. Production contracts as part of the state armament programmes until 2020 was for 124 Su-34s.¹² In June 2020, a contract was signed for the production of 24 new and slightly upgraded Su-34 'NVO version' as part of ongoing efforts to replace the remaining Su-24M Fencer bombers.¹³ In addition, production of a significantly upgraded Su-34M version is already underway, with eight units scheduled for delivery at the end of 2021.¹⁴ The stated intent of the 2027 Russian state armament plan is to produce sufficient Su-34Ms to enable the full replacement of the remaining Su-24M bombers and Su-24R maritime reconnaissance aircraft. Although the Su-24M fleet has been upgraded with the SVP-24 'Gefest' continuously computed release point (CCRP) bombing system and has seen extensive service in Syria, the type is considered outdated. To this end, the current contract covers the production of 76 additional Su-34Ms by 2027, which would result in an eventual fleet of over 200 aircraft by the end of the 2020s.¹⁵ It remains to be seen how quickly and how many of

¹⁰ Anton Lavrov and Roman Kretzul, '«Сухого» место: новейшие истребители поступят в морскую авиацию' ["Dry" place: the latest fighters will go to naval aviation "Izvestia" learned the details of the contract for the purchase of combat vehicles Su-30SM2], *Izvestia* (22 April 2021), <https://iz.ru/1154899/anton-lavrov-roman-kretzul/sukhogo-mesto-noveishie-istrebiteli-postupiat-v-morskuiu-aviaciiu> accessed 9 February 2022.

¹¹ Roman Kretzul and Anna Cherepanova, 'Тяга к лучшему: истребители Су-30СМ получают сверхмощный апгрейд', [Thrust for the best: Su-30SM fighters will receive a heavy-duty upgrade], *Izvestia* (2 May 2021), <https://iz.ru/1159091/roman-kretzul-anna-cherepanova/tiaga-k-luchshemu-istrebiteli-su-30sm-poluchat-sverkhmoshchnyi-apgreid> accessed 9 February 2022.

¹² Yefim Gordon and Dmitriy Komissarov, *Russian Tactical Aviation since 2001* (Manchester: Hikoki Publications, 2017), p. 290.

¹³ 'The Ministry of Defense signed a three-year contract for the construction of about 20 front-line Su-34', *TASS* (8 June 2020), <https://tass.ru/armiya-i-opk/8676891> accessed 9 February. See also 'В авиаполках Су-34 сформируют дополнительные эскадрильи', [Additional squadrons will be formed in Su-34 air regiments], *Izvestia* (9 December 2021), <https://iz.ru/1261834/2021-12-09/v-aviapolkakh-su-34-sformiruiut-dopolnitelnye-eskadriili> accessed 9 February 2022.

¹⁴ Anton Lavrov and Bogdan Stepanov, 'Показаться на высоте: полки бомбардировщиков усилят эскадрильями Су-34', [Appear on top: regiments of bombers will be strengthened by squadrons of Su-34], *Izvestia* (9 December 2021), <https://iz.ru/1261713/anton-lavrov-bogdan-stepanov/pokazatsia-na-vysote-polki-bombardirovshchikov-usiliat-eskadriiliami-su-34?destination=node/1261713> accessed 9 February 2022.

¹⁵ Anton Lavrov and Roman Kretzul, '«Сухой» воздух: Минобороны закупит Су-34 усовершенствованной версии' ["Dry" air: the Ministry of Defense will purchase the Su-34 improved version], *Izvestia* (29 May 2020), <https://iz.ru/1016971/anton-lavrov-roman-kretzul/sukhoi-vozdukh-minoborony-zakupit-su-34-usovershenstvovannoi-versii> accessed 9 February 2022.

the early production Su-30 aircraft will be upgraded to at least Su-34 'NVO', if not Su-34M standard. However, the strong performance of the Su-34 over Syria and the fact that it is one of the only elements of the VKS force structure to routinely employ a wide range of precision guided munitions makes this expensive production and modernisation plan one of the most likely VKS priorities for sustained funding during the 2020s.

All three 'Flanker' derived types which have formed the backbone of VKS fighter and frontal bomber acquisition efforts since 2010 feature relatively modern and capable passive electronically scanned array (PESA) radars and digital avionics.¹⁶ In terms of weapons, they are compatible with the standard R-73, R-27ER/ET and R-77-1 air-to-air missiles in the VKS inventory, and can carry a wide range of unguided and precision-guided air-to-ground missiles, bombs and rockets for ground attack and strike missions. However, the lack of targeting pods or laser self-designation capabilities on the Su-35S and Su-30SM(2) family significantly limits their effectiveness against ground targets that are mobile, do not easily show up on radar or are not pre-planned. All Russian Flankers have very large signatures in the radar, infra-red and electro-optical bands of the electromagnetic spectrum. They are also currently limited to very powerful PESA radars, without modern low-probability of intercept/low-probability of detection (LPI/LPD) capabilities. The latter is a significant disadvantage compared to Western competitors which increasingly feature active electronically scanned array (AESA) type radars and significantly more advanced passive electronic support measures (ESM) target detection and tracking capabilities.

More limited numbers of modernised Mig-29SMT/35 and Mig-29K/KUB fighters have been procured for the VKS and Russian Naval Aviation since 2009. The Mig-29K was originally developed as a navalised version of the Mig-29M, but lost out to the Sukhoi Su-33 in Russian Naval Aviation service. However, it was purchased by the Indian Navy, and when it became necessary to procure a replacement for the Su-33 in the mid-2010s it was cheaper for the Russian Navy to purchase Mig-29K/KUBs rather than paying to restart the Sukhoi production line. Consequently, a contract for 24 aircraft was placed in 2012 and these had all been delivered by 2015.¹⁷ However, the Russian Navy's only aircraft carrier is now stuck in a troubled refit and repair cycle during which there was a major fire onboard and the only drydock capable of accommodating it sank.¹⁸ Furthermore, one of the Mig-29Ks crashed during the type's first frontline cruise in the Mediterranean in 2016.¹⁹ Consequently, Naval Aviation combat aircraft procurement is now heavily focused on acquiring land-based squadrons of Su-30SM(2) and Su-34Ms rather than carrier fighters.

¹⁶ Yefim Gordon and Dmitriy Komissarov, *Russian Tactical Aviation since 2001* (Manchester: Hikoki Publications, 2017), p. 83-115.

¹⁷ Mikoyan Aircraft Corporation, 'МиГ-29КУБ - 9 лет в небе' [MiG-29KUB - 9 years in the sky], (20 January 2016), <http://www.migavia.ru/index.php/ru/novosti/press-relizy/553-mig-29kub-9-let-v-nebe> accessed 10 February 2022.

¹⁸ Tyler Rogoway, 'Russia's Accident-Plagued Aircraft Carrier Is On Fire (Updated)', *The War Zone* (12 December 2019), [Russia's Accident-Plagued Aircraft Carrier Is On Fire \(Updated\) \(thedrive.com\)](https://www.thedrive.com/news/12-december-2019/russia-s-accident-plagued-aircraft-carrier-is-on-fire) accessed 23 February 2022.

¹⁹ Sam LaGrone, 'Russian Carrier-based MiG-29K Fighter Crashes in Mediterranean; Shows Potential Gaps in Capability', *US Naval Institute News* (14 November 2016), <https://news.usni.org/2016/11/14/russian-carrier-mig-29k-fighter-crashes-mediterranean-shows-potential-gaps-capability> accessed 10 February 2022.

The VKS has placed even less priority on Mikoyan fighters as part of its modernisation than the Naval Aviation force. In 2007, a batch of Mig-29SMTs built for export to Algeria was rejected due to quality control concerns. To save face, the Russian Ministry of Defence agreed to purchase them, and so 28 single seaters and six trainer aircraft were supplied to the 14th Guards Fighter Regiment (GvIAP) at Kursk between 2009 and 2010.²⁰ However, despite public pronouncements of satisfaction with the new type, and the fact that it had only recently received these ostensibly modern, capable and newly manufactured multirole fighters, the 14th GvIAP was quietly re-equipped with Su-30SMs between 2016 and 2018.²¹ Furthermore, commercial satellite imagery from February 2022 of Kursk airbase shows that 33 of the Mig-29SMTs previously flown by the 14th GvIAP are now inactive and parked on peripheral hardstand areas of the base.²² This suggests that the VKS does not see significant value in transferring these aircraft to re-equip other fighter units, although there still regiments flying Soviet-era Mig-29s and Su-27s which are badly in need of replacement. Following the re-equipment of the 14th GvIAP, the only active VKS unit equipped with the Mig-29SMT is the 116th UTsBP [Training Centre of Combat Applications], which provides adversary support for training purposes to the rest of the VKS frontline.²³ Although there have been token purchases rumoured for the follow-on Mig-35 derivative of the Mig-29 family, the practical investment choices made by the VKS suggest that there is little future for this once iconic Soviet-era fighter line. Instead, the Flanker family is now dominant across most combat air mission sets.

Alongside the 'Flanker' types, the VKS has also invested significantly in major mid-life upgrade programmes for two Soviet-era workhorses. Most notably this includes a series of contracts signed in 2011, 2014 and 2019 to overhaul and upgrade 110 of the huge Mig-31B and Mig-31BS interceptors to the much more capable Mig-31BM/BSM standard.²⁴ The BM/BSM upgrade added a new RP-31AM radar, Zaslon-AM fire control system, Baghet-55 mission computer and the TKS-2M tactical datalink.²⁵ It also provides compatibility with the new R-37M very long range air-to-air missile.²⁶ Importantly, the new fire control system, mission computer and datalink were designed to allow the Mig-31BM to exchange target data with surface-to-

²⁰ Yefim Gordon and Dmitriy Komissarov, *Russian Tactical Aviation since 2001* (Manchester: Hikoki Publications, 2017), p. 118-123.

²¹ 'Курский авиаполк завершил перевооружение на истребители Су-30СМ' [Kursk Aviation Regiment completes re-equipment with Su-30SM fighters], *TASS* (27 December 2018), <https://tass.ru/armiya-i-opk/5959229> accessed 10 February 2022.

²² <https://www.google.com/maps/@51.755088,36.2995663,2338m/data=!3m1!1e3> captured 10 February 2022.

²³ Yefim Gordon and Dmitriy Komissarov, *Russian Tactical Aviation since 2001* (Manchester: Hikoki Publications, 2017), p. 124.

²⁴ Yefim Gordon and Dmitriy Komissarov, *Russian Tactical Aviation since 2001* (Manchester: Hikoki Publications, 2017), p. 130-133. And 'Минобороны РФ подписало новый контракт на модернизацию МиГ-31' [The Ministry of Defense of the Russian Federation signed a new contract for the modernization of the MiG-31], *Interfax* (8 January 2019), <https://www.interfax.ru/russia/645309> accessed 10 February 2022.

²⁵ Yefim Gordon and Dmitriy Komissarov, *Russian Tactical Aviation since 2001* (Manchester: Hikoki Publications, 2017), p. 128.

²⁶ Douglas Barrie, 'Russia's Foxhound finally gets its bite back', *IJSS Military Balance Blog* (30 April 2019), <https://www.ijss.org/blogs/military-balance/2019/05/russia-foxhound-upgrades> accessed 8 February 2022.

air missile (SAM) units, to greatly extend the range at which the ground based integrated air defence system (IADS) can engage low-flying targets.²⁷

There are now approximately 100 Mig-31BM/BSM aircraft in VKS service, and the Ministry of Defence signed a new contract in 2021 to complete the upgrade process for the remaining 20 or so Mig-31B/BS airframes which are still in use.²⁸ Russia has also retained more than 100 non-airworthy Mig-31 airframes in long term storage. The VKS now plans to upgrade at least some of these to Mig-31BM standard and return them to service during the 2020s, with a likely fleet target of around 150 modernised interceptors.²⁹ The large size, high fuel consumption, stresses incurred during high performance flight and comparatively small fleet size of the Mig-31 ensures that it is an expensive asset to operate. Furthermore, the state of many of the older airframes means that upgrade work at the Sokol factory has been more time consuming and expensive than initially hoped. Up to 50% of the structural area of airframes required replacement due to corrosion, and the upgrade process involves replacing all wiring, avionics, rubber components and fitting a completely new electronic fly-by-wire control system in place of the mechanical one.³⁰ While concrete figures on the 2019 and 2021 contracts are hard to find, the 2014 contract for 50 upgraded aircraft was valued at over 30 billion rubles, or around \$8 million per aircraft.³¹ Since 2014, however, inflation caused by the dramatic devaluation of the ruble and a slower pace of upgrade work will have significantly increased real costs. As such, a real-terms cost of around \$15 million per aircraft is the likely minimum for the more recent Mig-31BM/BSM upgrade contracts.

Despite its cost and somewhat old-fashioned design the Mig-31BM (and the more specialised Mig-31K hypersonic missile launch platform sub-type) remains a priority for the VKS. With its long range, interoperability with the ground-based IADS and ability to engage targets including low-flying cruise missiles and helicopters from well inside Russian airspace, the 'Foxhound' provides unique capabilities which cannot easily be replaced. In January 2021, Rostec did confirm the existence of a long-rumoured programme to develop a successor to the Mig-31BM, designated the 'Advanced Aviation Complex for Long-Range Interception' (PAK DP).³² PAK DP is nominally forecast to enter service in the early 2030s and feature a stealthy airframe, even more impressive high-altitude performance than the Mig-31, new hypersonic missiles and potentially a laser weapon. However, the modernisation programme for Mig-31BM/BSM will only be completed around 2027. Furthermore, there is no con-

²⁷ Justin Bronk, 'Russian and Chinese Combat Air Trends' *RUSI Whitehall Reports*, 3-20, (October 2020), p. 27., <https://static.rusi.org/russian-and-chinese-combat-air-trends-whr-final-web-version.pdf> accessed 10 February 2022.

²⁸ 'Модернизированные МиГ-31 обеспечат безопасность Северного морского пути' [Modernized MiG-31s will ensure the safety of the Northern Sea Route], *TASS* (24 November 2021), <https://tass.ru/armiya-i-opk/13027683> accessed 10 February 2022.

²⁹ Илья Крамник, 'Новые крылья ВВС России' [New Wings of the Russian Air Force], *Izvestia* (5 December 2017), <https://iz.ru/679043/ilia-kramnik/novye-krylia-vvs-rossii> accessed 10 February 2022.

³⁰ 'Модернизированные МиГ-31 обеспечат безопасность Северного морского пути' [Modernized MiG-31s will ensure the safety of the Northern Sea Route], *TASS* (24 November 2021), <https://tass.ru/armiya-i-opk/13027683> accessed 10 February 2022.

³¹ 'Минобороны заключило контракт на модернизацию 50 МиГ за 30 млрд рублей' [The Ministry of Defense signed a contract for the modernization of 50 MiGs for 30 billion rubles], *RIA* (27 November 2014), <https://ria.ru/20141127/1035386047.html> accessed 10 February 2022.

³² 'МиГ-31БМ: птица высокого полета' [MiG-31BM: high-flying bird], (22 January 2021), <https://rostec.ru/news/mig-31bm-ptitsa-vysokogo-poleta/> accessed 10 February 2022.

firmed funding allocation for PAK DP within the state armament programme 2027, and without major investment there is little reason to expect a faster and more successful next-generation development programme than previous efforts including Su-57 and the next-generation bomber (PAK DA). Therefore, the Mig-31BM will remain a core element of VKS air defence capabilities without a replacement for the foreseeable future.

The second soviet-era fast jet fleet which has seen significant upgrade work is the Su-25 ground attack aircraft. The VKS has upgraded 84 of its remaining roughly 200 Su-25s to Su-25SM standard, and approximately 30 others to a further-improved Su-25SM3 version.³³ The Su-25SM upgrade programme involved fitting modern avionics, improved infra-red/TV sensor and laser designator in the nose and adding the capability to carry and launch a wide range of radar, laser and TV-guided air-to-ground missiles, bombs and rockets. It was intended to last the type until its envisaged out of service date of 2020.³⁴ The more advanced Su-25SM3 standard added a significantly more capable Vitebsk-25 self-protection suite which includes electronic warfare pods and missile-approach warning system, and a GLONASS navigation/attack system.³⁵ The SM3 programme gained urgency after the shoot-down of a Su-25SM in Syria in February 2018 by a man-portable air defence system (MANPADS), which was judged to be evidence of unacceptable vulnerability. Despite the upgraded navigation and self-protection suite of the Su-25SM3, the contracted upgrade rate remains at a minimal 4 per year.³⁶ The primary reasons for the Su-25 being retained in service is that it is cheap to operate and that there is no suitable replacement immediately available.

The Flanker-family fighter acquisition programmes and Mig-31 modernisation programme represent a successful effort by the Russian combat aircraft industry to leverage a range of cutting edge late-Soviet era technologies which had been kept on life-support as limited research and development programmes throughout the lean decades of the 1990s and 2000s. Other examples of this include the success in developing the long-troubled R-77 and R-37 active radar-seeking air-to-air missile (AAM) to a level of maturity where both have entered service in limited numbers with frontline units in the shape of the R-77-1 and R-37M.³⁷ However, efforts to develop new programmes to keep pace with the latest generation of American (and Chinese) fighter and Western sensor, weapon and avionics technologies have proven far more challenging for Russian industry. In particular, the Su-57 ‘fifth generation’ fighter, Su-70 ‘*Okhotnik-B*’ combat UAV have yet to prove they have a viable place in the VKS frontline order of battle.

³³ Vladimir Karnozov, ‘Further Improved Su-25SM3 Redeploys to Syria’, *AIN Online* (22 March 2019), <https://www.ainonline.com/aviation-news/defense/2019-03-22/further-improved-su-25sm3-redeploys-syria> accessed 11 February 2022.

³⁴ Vladimir Karnozov, ‘MAKS 2011: Upgrade of Sukhoi Su-25 Extended to Two-Seat Version’, *AIN Online* (22 August 2011), <https://www.ainonline.com/aviation-news/defense/2011-08-22/maks-2011-upgrade-sukhoi-su-25-extended-two-seat-version> accessed 11 February 2022.

³⁵ Yefim Gordon and Dmitriy Komissarov, *Russian Tactical Aviation since 2001* (Manchester: Hikoki Publications, 2017), p. 70-76.

³⁶ Vladimir Karnozov, ‘Further Improved Su-25SM3 Redeploys to Syria’, *AIN Online* (22 March 2019), <https://www.ainonline.com/aviation-news/defense/2019-03-22/further-improved-su-25sm3-redeploys-syria> accessed 11 February 2022.

³⁷ Douglas Barrie, ‘Russia’s Foxhound finally gets its bite back’, *IJSS Military Balance Blog* (30 April 2019), <https://www.ijss.org/blogs/military-balance/2019/05/russia-foxhound-upgrades> accessed 8 February 2022.

Next-Generation Systems

The initial order for 52 Su-57 ‘fifth generation’ fighters in the 2010 state armament programme were steadily reduced between 2015 and 2019. In terms of production-quality aircraft, the order was dramatically reduced to 12 aircraft for a single squadron in 2015, then six aircraft in 2017 and finally to two aircraft in 2018.³⁸ At that point the total production (including prototypes) by 2027 was to be 15 aircraft, with no intent to put the Su-57 into series production for the foreseeable future. The justification offered at the time was the Su-35S was so capable that mass production of the Su-57 was not required. In reality, the most likely cause was a combination of protracted and troubled development, disappointing radar signature and sensor performance characteristics and the rising unit costs of at least 3 billion rubles or around \$40 million each.³⁹

In May 2019, however, President Putin announced that a 20% reduction in unit price had been agreed with industry to enable the VKS to purchase 76 Su-57s during the same period without allocating any additional funding.⁴⁰ The maths behind this claim is transparently defective. Furthermore, no confirmation has followed on contracts being signed to cover more than a slight increase in the slow existing Su-57 production rate. In December 2020, Defence Minister Shoigu stated that the VKS expected to have received 22 Su-57s by the end of 2024, with the remaining 54 presumably presently unfunded and envisaged for production between 2025 and 2028.⁴¹ As of January 2022, however, only four series-production Su-57s have been delivered to the VKS and the first one crashed during its acceptance flight tests.⁴² Furthermore, the Su-57 is still considered to need ‘modernisation’ before it can fully meet VKS needs. This includes full integration of the new OSNOD datalink and other equipment into the fire control system to enable cooperative engagements between the Su-57 and ground-based S-400/500 SAM systems.⁴³ Production of a definitive combat-ready Su-57 with the new Saturn ‘Izdeliye 30’ engine, OSNOD and other avionics upgrades is tentatively scheduled for 2025.⁴⁴

³⁸ Илья Крамник, ‘Предполетные ожидания: когда Су-57 заступят на боевое дежурство’ [Pre-flight expectations: when the Su-57 will take up combat duty], *Izvestia* (11 April 2019), <https://iz.ru/866427/ilia-kramnik/predpoletnye-ozhidaniia-kogda-su-57-zastupiat-na-boevoe-dezhurstvo> accessed 9 February 2022.

³⁹ Илья Крамник, ‘Полтриллиона за господство в воздухе: сколько стоит партия Су-57’ [Half a trillion for air supremacy: how much does a batch of Su-57 cost], *Izvestia* (18 May 2019), <https://iz.ru/878906/ilia-kramnik/poltrilliona-za-gospodstvo-v-vozdukhe-skolko-stoit-partiia-su-57> accessed 11 February 2022.

⁴⁰ ‘Putin says 76 Su-57 jets to be purchased before 2028’, *TASS* (15 May 2019), <https://tass.com/defense/1058494> accessed 11 February 2022.

⁴¹ Antony Angrand, ‘Russia: 22 Su-57 in service by the end of 2024’, *Air and Cosmos International* (22 December 2020), <https://aircosmosinternational.com/article/russia-22-su-57-in-service-by-the-end-of-2024-3049> accessed 11 February 2022.

⁴² ‘Russian Aerospace Forces received two more Su-57 in late 2021’, *Janes* (24 January 2022), <https://www.janes.com/defence-news/news-detail/russian-aerospace-forces-received-two-more-su-57-in-late-2021> accessed 11 February 2022.

⁴³ Anton Lavrov and Alexey Ramm, ‘Обменным курсом: «Сухие» смогут наводить на цели зенитные комплексы’ [Exchange rate: “Dry” will be able to direct anti-aircraft systems to targets], *Izvestia* (7 May 2021), <https://iz.ru/1159173/anton-lavrov-aleksei-ramm/obmennym-kursom-sukhie-smogut-navodit-na-tseli-zenitnye-kompleksy> accessed 11 February 2022. See also ‘Testy systemu łączności Su-57’ [Tests of the Su-57 communication system], *Defence 24* (20 September 2019), <https://defence24.pl/przemysl/testy-systemu-laczności-su-57> accessed 11 February 2022.

⁴⁴ ‘Производство модернизированного варианта Су-57 может начаться в 2025 году’ [Production of the upgraded version of the Su-57 may begin in 2025], *TASS* (8 August 2021), <https://tass.ru/armiya-i-opk/12085969> accessed 11 February 2022.

In terms of potential combat capabilities once mature, the basic Su-57 has the potential to solve most of the outstanding deficiencies of the current Flanker family as advanced 4th generation fighters. The questionable surface finish, imperfectly hidden engine fan-blades, leading-edge vortex controller (LEVCON) surfaces and actuators, non-faceted infra-red scan and track (IRST) sensor ball and engine housings all significantly reduce its potential low-observable qualities to well below those of American or even Chinese competitors. Despite these features, there is no doubt that it has the potential for a radar cross section which is at least an order or magnitude lower than existing VKS frontline types. However, it is questionable whether the achievable level of radar cross section and sensor complexity will deliver sufficient practical benefits to justify its increased cost for the VKS, when considered against the advanced threats the Su-57 will have to face in the late 2020s and beyond.

There are no indications that UAC has managed to solve the many challenges with the complex multi-array N036 Byelka AESA radar system, and the fact that ‘modernisation’ of the avionics is considered essential is evidence to the contrary.⁴⁵ It is also worth noting that South Korea has agreed to US Government demands that it halt exports of gallium arsenide semi-conductors to Russia. This means a critical component for both the N036 and Irbis-E radars is now cut off, with no domestic substitute immediately available.⁴⁶ In the somewhat unlikely event that the full complement of 76 production-standard Su-57s are delivered, they will be sufficient to equip only three frontline regiments, which will receive the bulk of their allotted 24 aircraft each in the late-2020s.⁴⁷ By this stage, any low-observable properties will have been dramatically degraded by the modern AESA radars, cooperative multi-static detection and tracking techniques and dramatic increases in processing power introduced progressively on Western aerial, maritime and ground-based platforms since the Su-57 was designed. The difficulties faced by the much better-funded US Air Force in maintaining the F-22 Raptor’s availability and low-observable coatings (even after decades experience operating stealth aircraft) also do not bode well for the VKS’s ability to maintain the Su-57 in frontline service.⁴⁸

The other major next-generation programme of note is the Su-70 ‘*Okhotnik-B*’ unmanned combat aerial vehicle (UCAV) – a subsonic flying wing design in the 20-ton class. The first prototype flew in August 2019, and a second airframe with significantly improved surface finish and engine nozzle configuration was unveiled in December

⁴⁵ ‘Источник назвал сроки начала производства истребителя Су-57’ [The source called the timing of the start of production of the Su-57 fighter], *Izvestia* (9 August 2021), <https://iz.ru/1204510/2021-08-09/istochnik-nazval-sroki-nachala-proizvodstva-istrebitelia-su-57> accessed 11 February 2022.

⁴⁶ ‘Sanctions Buster: South Korea Must Stop Supplying Gallium Arsenide to Russia’s JSC-Phazotron-NIIP’, *Global Defense Corp* (13 January 2022), <https://www.globaldefensecorp.com/2022/01/13/sanctions-busting-south-korea-must-stop-supplying-gallium-arsenide-to-russias-jsc-phazotron-niip/> accessed 11 January 2022.

⁴⁷ Bogdan Stepovoy, Alexey Kozachenko, Alexey Ramm and Andrey Fedorov, ‘Сны полка: для истребителей Су-57 создают особые военные подразделения’ [Dreams of the regiment: special military units are created for Su-57 fighters], *Izvestia* (20 May 2019), <https://iz.ru/879224/bogdan-stepovoi-aleksei-kozachenko-aleksei-ramm/sny-polka-dlia-istrebitelei-su-57-sozdaiut-osobyie-voennye-podrazdeleniia> accessed 11 February 2022.

⁴⁸ Stephen Losey, ‘Aircraft mission-capable rates hit new low in Air Force, despite efforts to improve’, *Air Force Times* (26 July 2019), <https://www.airforcetimes.com/news/your-air-force/2019/07/26/aircraft-mission-capable-rates-hit-new-low-in-air-force-despite-efforts-to-improve/> accessed 11 February 2022.

2021.⁴⁹ The Su-70 is currently in the early phase of flight and systems testing, and both prototypes are still primarily remotely piloted machines despite a plan to develop a heavily automated control and attack system in the coming years.⁵⁰ Doctrinally the *Okhotnik-B* is designated as a 'heavy strike drone' that is intended to engage a range of ground-based and aerial target sets in conjunction with the Su-57.⁵¹

The Ministry of Defence has specified an ambitious development timetable for the Su-70. The target date is late-2022 for the completion of initial ground-tests and flight-trials, and 2024 for the delivery of the first production airframes to the VKS.⁵² This is likely to prove an overly ambitious target. Russian industry will face major hurdles in developing the Su-70 prototypes into a viable frontline UCAV design. The vulnerability of datalinks makes remotely-piloted aircraft generally unsuitable for combat against adversaries with potent electronic attack capabilities, which is why UCAVs intended for high-intensity conflict must have high levels of in-flight autonomy.⁵³ The designers of the Su-70 are well aware of this and are planning to incorporate a high level of autonomous combat capability.⁵⁴ However, this will require unprecedented levels of autonomous navigation, sense-and-avoid capability, target detection, classification, prioritisation and attack capability, and a totally new C2 system and broader force integration architecture. This are all things that Russian industry has never mastered before, and which even the US and China have only partially achieved. The United States and China have also both demonstrated repeatedly that moving from a promising looking series of flying demonstrators to a stable frontline fleet is extremely time-consuming and resource intensive, especially for low-observable aircraft. Space, weight, power and computing power (SWAP-C) is a significant constraint when weapons systems, sensors, communications arrays and fuel for combat operations need to be fully self-contained within a clean, low-observable airframe. Furthermore, thermal management, sensor placement and the relationship between airframe materials and the various frequencies and wavelengths of friendly and hostile sensors are huge challenges which need to be overcome to field practical stealth combat aircraft.

If the Su-70 does enter service in significant numbers, it is envisaged as a force multiplier to be directed in flight by accompanying fighters. However, single seat pilots are likely to face serious capacity limitations attempting to control flights of Su-70s in combat. This is why the plan for tactical cooperation between Su-70 and Su-57

⁴⁹ 'Военный эксперт рассказал о возможностях беспилотника С-70 «Охотник»' [Military expert spoke about the capabilities of the S-70 "Hunter" drone], *Izvestia* (14 December 2021), <https://iz.ru/1264245/2021-12-14/voennyi-ekspert-rasskazal-o-vozmozhnostiakh-bespilotnika-s-70-okhotnik> accessed 11 February 2022.

⁵⁰ 'Летчик-испытатель рассказал о возможностях беспилотника С-70 «Охотник»' [Test pilot spoke about the capabilities of the S-70 "Hunter" drone], *Izvestia* (21 February 2021), <https://iz.ru/1128115/2021-02-21/letchik-ispytatel-rasskazal-o-vozmozhnostiakh-bespilotnika-s-70-okhotnik> accessed 11 February 2022.

⁵¹ 'Источник назвал дату начала испытаний беспилотника «Охотник»' [The source called the date of the beginning of tests of the drone "Hunter"], *Izvestia* (21 January 2022), <https://iz.ru/1281282/2022-01-24/istochnik-nazval-datu-nachala-ispytanii-bespilotnika-okhotnik> accessed 11 February 2022.

⁵² 'Russia rolls out first flight prototype of state-of-the art Okhotnik heavy strike drone', *TASS* (14 December 2021), <https://tass.com/defense/1375043> accessed 11 February 2021.

⁵³ Justin Bronk, 'Next Generation Combat Aircraft: Threat Outlook and Potential Solutions', *RUSI Occasional Papers* (2 November 2018), [Next Generation Combat Aircraft: Threat Outlook and Potential Solutions | Royal United Services Institute \(rusi.org\)](https://rusi.org/next-generation-combat-aircraft-threat-outlook-and-potential-solutions) accessed 23 February 2022.

⁵⁴ 'Летчик-испытатель рассказал о возможностях беспилотника С-70 «Охотник»' [Test pilot spoke about the capabilities of the S-70 "Hunter" drone], *Izvestia* (21 February 2021), <https://iz.ru/1128115/2021-02-21/letchik-ispytatel-rasskazal-o-vozmozhnostiakh-bespilotnika-s-70-okhotnik> accessed 11 February 2022.

involves an as-yet non-existent two-seat variant of the latter.⁵⁵ The prospects are unlikely for either a twin-seat Su-57, or single seater with sufficiently mature avionics to make controlling Su-70s in flight practical under combat conditions until at least the late 2020s. An awareness of this is probably the reason behind a recent contract announcement which shows that twin-seat Su-30SM2s will also be configured to control Su-70s.⁵⁶

The declared funding within the 2027 state armament programme is manifestly inadequate to cover the myriad of promised acquisition, upgrade and development programmes across the various armed services. This means that hard choices will have to be made between continuing the acquisition and modernisation of proven and mature platforms for the VKS and betting large sums on unproven and immature systems like the Su-70 (and Su-57). The limited rollout of the Link-16 equivalent 'OSNOD' datalink to replace the older TKS-2 and TKS-2M has also so far only been confirmed for the Su-57 and Su-30SM2.⁵⁷ Given the centrality of seamless datalink connectivity for the planned Su-70 concept of operation, the lack of detail on wider OSNOD rollout does not bode especially well for the viability of a UCAV fleet as a core part of the VKS frontline in the 2020s or early 2030s.

Conclusions

When considering the likely nature of the threat which the combat air fleets of the VKS can pose to Western air arms over the coming decade, it is important to look at the actual procurement dynamics underpinning Russia's undeniably impressive fighter modernisation drive. During the 2010s the VKS received almost 100 new Su-35S fighters, more than 150 Su-30M2 and Su-30SM(2) multirole fighters and around 130 Su-34 strike fighters. Production of these types continues at a significant rate, and iterative upgrade programmes are also underway. The unique Mig-31BM/BSM fleet already sits at around 110 upgraded interceptors, and contracts have been signed which should see the modernised fleet hit at least 130 in the next few years, with an intent to reach around 150 by 2027. The majority of these fighters are at least equipped with the TKS-2 or TKS-2M datalinks, and the latest standard of Su-30SM2 is equipped with OSNOD – Russia's equivalent to the ubiquitous NATO Link-16 system.

There has been less priority given to Su-25SM upgrades, and even less to the Mig-29/35 series. Neither is seen as a major component of future VKS combat power against state opponents. However, the situation is even less promising for the next-generation combat air programmes at present. The constant programme slippage, unclear funding provisions, immature systems and rapidly degrading potential stealth advantages of the Su-57 stand in stark contrast to the mature Su-35, Su-30SM2 and Su-34M programmes which are delivering real combat power to the VKS alongside the venerable but still potent Mig-31BM/BSM. The Su-70 represents a potentially

⁵⁵ 'Russia rolls out first flight prototype of state-of-the art Okhotnik heavy strike drone', *TASS* (14 December 2021), <https://tass.com/defense/1375043> accessed 11 February 2021.

⁵⁶ 'Истребители Су-30СМ2 поведут в бой беспилотники' [Su-30SM2 fighters will lead drones into battle], *Izvestia* (9 February 2022), <https://iz.ru/1288747/2022-02-09/istrebiteli-su-30sm2-povedut-v-boi-bespilotniki> accessed 11 February 2022.

⁵⁷ Charlie Gao, '1 Thing The Russian Military and Its Stealth Fighters Can't Fight Without', *The National Interest* (1 April 2021), <https://nationalinterest.org/blog/reboot/1-thing-russian-military-and-its-stealth-fighters-cant-fight-without-181752> accessed 11 February 2022.

potent, but currently unproven and deeply immature asset that is designed for a VKS ecosystem of twin-seat Su-57s and ubiquitous OSNOD connectivity that does not yet exist. If it is developed for service in significant numbers, it may offer a relatively cost-effective way to boost VKS striking power in more contested areas. However, it will only be ready for service in the late 2020s at the earliest, and will serve in relatively specific roles alongside Su-30SM2s rather than Su-57. Meanwhile, more exotic projects such as the Su-75 'Checkmate' fighter⁵⁸, PAK DA next generation bomber⁵⁹ and PAK DP next generation interceptor⁶⁰ remain firmly in the realm of unfunded future ambitions and should be left out of medium-term Western threat assessments.

In terms of air-to-air weaponry developments, the VKS has successfully caught up with the older NATO AIM-9M/L Sidewinder and AIM-120B/C AMRAAM series of short and medium range air to air missiles with the R-73M and R-77-1. However, it does not have a direct answer to the latest generation of Western missiles such as the AIM-132 ASRAAM, AIM-120D AMRAAM and Meteor, or to the Chinese PL-15. As such, Russian fighters remain largely out-matched in terms of practical engagement ranges by NATO fighter equipped with such weapons. However, the VKS has begun to field the R-37M very-long range missile with the Mig-31BM fleet, and this weapon can be carried and launched by Flanker-type fighters if required.⁶¹ However, in practice limited stocks, high unit costs and the centrality of the Mig-31BM mission for territorial defence probably ensure that the R-37M will remain a specialist weapon. Nonetheless, the VKS now regularly deploys fighters to conflict zones and along airspace borders with relatively modern R-77-1 and R-73M air-to-air missiles which can pose a real challenge to many NATO fighters. It can also support those fighters with a modernised, albeit relatively small, A-50M AWACS fleet to provide greatly enhanced wide-area situational awareness, target acquisition and coordination.

Importantly, however, VKS flying hours remain low compared to the leading NATO air forces, with 120 hours a year on average in elite units such as the 16th UTsBPr.⁶² Across all VKS fixed wing types, flying hours for pilots in 2018 averaged 100 hours.⁶³ In 2021, Naval Aviation pilots flew an average of just under 100 hours per year, which was reported as an increase on the figures from 2020.⁶⁴ Western fighter pilots struggle to stay combat-capable across the broad range of multi-mission tasks they are assigned despite getting 180-250 live flying hours per year, access to modern high-fidelity

⁵⁸ John Parachini and Peter Wilson, 'Is Russia's Su-75 'Checkmate' Aircraft a Case of Vapor Marketing?', *The RAND Blog* (6 January 2022), <https://www.rand.org/blog/2022/01/is-russias-su-75-checkmate-aircraft-a-case-of-vapor.html> accessed 8 February 2022.

⁵⁹ *TASS*, 'PAK DA demonstrational model to be ready by 2023' (2 August 2021), <https://tass.com/defense/1321611> accessed 8 February 2022.

⁶⁰ Gareth Jennings, 'Russia launches PAK DP development to replace MiG-31', *Janes* (25 January 2021), <https://www.janes.com/defence-news/news-detail/russia-launches-pak-dp-development-to-replace-mig-31> accessed 8 February 2022.

⁶¹ Thomas Newdick, 'Russian Air-To-Air Missile Tests Signal Potential New Capabilities For Flanker and Felon', *The War Zone* (5 October 2020), <https://www.thedrive.com/the-war-zone/36899/russian-air-to-air-missile-tests-signal-potential-new-capabilities-for-flanker-and-felon> accessed 11 February 2022.

⁶² Piotr Butowski, *Flashpoint Russia: Russia's Air Power: Capabilities and Structure* (Czech Republic: Harpia Publishing, 2019), p. 33.

⁶³ 'В командовании Военно-воздушных сил ВКС подвели итоги за 2018 год' [The command of the Air Force of the Aerospace Forces summed up the results for 2018] *Department of Information and Mass Communications of the Ministry of Defense of the Russian Federation* (4 December 2018), https://function.mil.ru/news_page/country/more.htm?id=12206756@egNews accessed 11 February 2022.

⁶⁴ 'Палет российских военных летчиков увеличился' [The flight time of Russian military pilots has increased], *VPK News*, (10 November 2021), <https://vpk-news.ru/news/64588> accessed 11 February 2022.

simulators and benefiting from superior cockpit and system ergonomics in their aircraft.⁶⁵ With such low flying hours and dramatically lower investment in modern simulator facilities than most NATO opponents, the average Russian frontline combat pilot will struggle to use the equipment at their disposal to its full potential in a complex combat environment. Furthermore, most VKS training flights are relatively simple 2-ship or 4-ship sorties, with a high proportion of navigation and target-simulation flights in cooperation with ground-based SAM units.⁶⁶ The lack of international training opportunities such as the Red Flag or Blue Flag series is also a significant limitation on the ability of VKS crews to regularly gain experience in high-end scenarios within complex and congested airspace.

The proportion of precision guided munitions used in the air-to-ground strike mission remains generally low across the VKS as a whole, but in the Su-34 force it is now routine and a wide variety of guided munitions are available for most likely combat tasks. However, the lack of targeting pods or sufficient flying hours to stay fully mission ready across a wide range of precision munitions limits the multirole capabilities of most Russian fighters against dynamic targets or targets of opportunity. Nevertheless, they have many options for striking fixed pre-planned targets, or ones which present a solid and easily identifiable radar signature. As such, the threat which the VKS can pose to such fixed or large, hard targets should not be underestimated in scenarios where adversary air forces are unable to effectively deny them access to contested areas.

In summary, the VKS has modernised its core fighter fleets and weaponry to the point where it can qualitatively and quantitatively overmatch state opponents that are unable to field the latest generation of Western fighters and missiles in quantity. This provides the Russian government with a valuable capability to projecting the threat or reality of significant air power against non-NATO member states in Russia's periphery. Ukraine is currently being conspicuously threatened by modernised VKS combat air capabilities, which are now in a completely different league to those deployed against Georgia in 2008.⁶⁷ What the VKS modernisation programme has not achieved is any form of qualitative parity with the latest and best fighter or strike fighter capabilities fielded by NATO air forces. However, this is ultimately not necessary or intended within Russian doctrine. Against NATO air power, Russia will rely first and foremost on its dense and highly capable ground-based IADS to both shield its own ground forces, protect its airspace and allow VKS combat air assets to commit to individual offensive and defensive engagements where and when favourable circumstances permit.

⁶⁵ Author interviews with RAF Typhoon instructor pilots at RAF Coningsby (July 2021), US Air Force F-15E instructor pilots at RAF Lakenheath (September 2021), French Air Force Mirage 2000C instructor pilots at Orange-Caritat Airbase (August 2021).

⁶⁶ Author interview with senior NATO fighter force commander, 9th February 2022.

⁶⁷ Justin Bronk, 'Ukrainian Air Defence Options in the Event of a Russian Attack', *RUSI Commentary* (8 February 2022), <https://rusi.org/explore-our-research/publications/commentary/ukrainian-air-defence-options-event-russian-attack> accessed 11 February 2022.

RUSSIAN MANEUVER DEFENCE AND THEIR CONCEPT OF THE FRAGMENTED BATTLEFIELD

Lester W. Grau (and Charles K. Bartles)¹

The presentation made by Lester W. Grau in the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 9:10:00.

Improvements in technology have changed battlefields in the past and probably also in the future making them more deadly and fragmented. Russia, mindful of history as a serious part of their practice of military science, is considering adjusting tactics to fight effectively and survive on that future fragmented battlefield. Over time, technology has concentrated the battlefield and located it on open terrain, then centuries later greatly expanded the battlefield and moved it to difficult terrain. Battles used to be compact events fought within the visual range of the contending commanders. Units used to march into battle in formation and fight shoulder-to-shoulder. Battlefields were chosen where terrain would not interfere with positioning the forces. Arrows flew while infantry advanced in close order with shield, spear and sword at the ready. Combat was close and frequently highly lethal. Then technology intervened.

Gunpowder and the bayonet allowed the infantryman to fight both the midrange and close battle. Still, muskets were inaccurate, so marching columns still moved close to each other and fought standing up and shoulder-to-shoulder. Rifled muskets appeared during the Crimean War with devastating results. The musket-armed Russians were decimated during the Battle of Inkerman (5 November 1854) by rifle-armed British infantry.² Unfortunately, this vital lesson of Crimea had to be relearned in the carnage of the initial period of the American Civil War.

Both sides of the American Civil War were initially trained in Napoleonic tactics-based on the smooth-bore musket and more-lethal bayonet. But the rifled musket was far more lethal at a much greater range. Soldiers learned the value of firing from a rifle pit, trench or behind a barricade. It was dig or die. Battlefields expanded and commanders seldom saw the entire battlefield. Semaphore and telegraph extended the ability of commanders to command. Battles lasted over days and weeks instead of hours. Rail transport proved vital to the logistics of war. In 1873, Major Wilhelm von Scherff published *Studien zur neuen Infanterie-Taktik* [The New Tactics of Infantry] while teaching tactics at the Prussian Military Academy. His book was based on his observations during the 1870-1871 Franco-Prussian War, which saw the wide use of cartridge ammunition, accurate rifles, machine guns and artillery. The result was “the void of the battlefield”. The combatants were widely dispersed and the distance

¹ This article was first published in *Infantry* in Fall 2021 as “Russian Future Combat on a Fragmented Battlefield” by Lester W. Grau and Charles K. Bartles. It has been modified for presentation and publication by the National Defence University of Finland.

² Report from General Menshikov to Emperor Nicholas I cited in Mungo Melvin, *Sevastopol's Wars: Crimea from Potemkin to Putin*, New York, Osprey Publishing, 2017, p. 218-219.

between the front lines had expanded. Further, while weapons were far more lethal, casualty rates lessened and many more bullets were expended per casualty induced.³

The increased lethality of weapons was not the sole reason for dispersion of forces on the battlefield. The telegraph and the radio allowed commanders to control forces over a greatly expanded area. The steam engine, internal combustion engine and the airplane allowed forces to move quicker over that expanded area. Armored vehicles provided a degree of protection as a sort of mobile firing pit. The density of US combat formations fell from 3,883 men per square kilometer to 404 in World War I and 36 in World War II.⁴ Of course, this varied by theater, geography, terrain and force, but the battlefield was becoming increasingly empty.

Thanks to technology, massing in space is getting more hazardous on the modern battlefield against near-peer competitors. This was a Soviet concern and is now a Russian concern.

Operation Desert Storm (17 January 1991 – 28 February 1991) had a major impact on military affairs. The US-led coalition thoroughly defeated Iraq, although Iraq had a larger, modern armed force. Iraq lost 8-10,000 combatants compared to the 300 casualties of the coalition. The coalition, particularly the United States, had a distinct advantage in satellite technology, communications technology and computer technology, plus, there were not too many places to hide large weapons and facilities in the open spaces of Kuwait and Iraq. Technology, training and getting everything in place before initiating combat played a major role in the coalition victory. The lesson learned by smaller, less powerful militaries was not to fight powerful, technologically-advanced forces in terrain that was optimum for modern maneuver war, but to move the fight to those areas where technology and maneuver is hampered or negated—mountains, jungles, deep forests, swamps and urban areas. This works well for countries that have an abundance of difficult terrain, but countries are stuck with the terrain they own or occupy.

Fragmented Combat

Much of Russia terrain is wide plains, interrupted by large, slow-moving rivers, forests and swamps. The road system is underdeveloped, and trafficability in European Russia is hampered by the very muddy roads of the fall and spring *razputitsa*. Although the Soviets fought the “Great Patriotic War” [World War II against the Germans] with thousands of kilometers of tied-in trenches and fairly linear lines of combat, the wars of the future would change and the Soviet Union prepared itself for non-linear or fragmented (*ochagovyy*) combat.⁵ The Soviet General Staff's view of future war envisioned dynamic, high-tempo, high-intensity land-air operations which would extend over vast expanses and include new areas such as space. Tactical combat would be even more destructive than in the past and would be characterized by fragmented [ochagovyy] or non-linear combat. The front line would disappear and no safe havens

³ James J. Schneider, “The theory of the ‘Empty Battlefield’”, *The RUSI Journal*, Volume 132, Issue 3, 1987, p. 35.

⁴ Trevor N. Dupuy, *The Evolution of Weapons and Warfare*, Indianapolis: Bobbs-Merrill Company, Inc, 1981, p. 312.

⁵ Lester W. Grau, “Soviet non-linear Combat: The challenge of the 90s”, Soviet Army Studies Office, Fort Leavenworth, September 1990, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a231789.pdf>.

or "deep rear" would exist. Nuclear war would be avoided at all costs, as it could escalate to strategic exchange and the "destruction of all the world's people."

In the 1950s-1960s, the Soviets envisioned future war as a nonlinear, nuclear battlefield where atomic weapons created maneuver corridors through which Soviet ground forces advanced to conduct meeting battles. The tempo of the offensive provided flank security to the attacker who maintained the initiative by advancing deep into the communications zone of the enemy. Due to the expected wide-spread use of nuclear weapons.

Combat would be exceptionally dynamic and highly maneuverable, forcing subunits to change rapidly from attack to defense and back again, and to change its combat formations frequently. Attacks would develop irregularly with the absence of a continuous front line and would be conducted in wider zones along axes. Under these conditions, combat would have a fragmented [ochagovyy, non-linear] nature at the various troop echelons.⁶

Indeed, "the broken nature of the front line, the presence of intervals and gaps formed in the enemy's combat formation by nuclear strikes, and the conduct of the attack along axes create favorable opportunities for the employment of maneuver."⁷

The US Vietnam War and the later Soviet and US wars in Afghanistan were clearly non-nuclear but also non-linear. In the 1970s and 1980s, the Soviets re-envisioned future large-scale war as being fought conventionally under nuclear-threatened conditions and adapted tactics and reemphasized operational art in order to meet this new vision. The Soviets conceptualized non-linear battle as separate "tactically independent" battalions and regiments/brigades fighting meeting battles and securing their flanks by obstacles, long-range fires and tempo. There would be no safe areas and combatants would suffer heavy attrition. Large units, such as divisions and armies, might influence the battle through employment of their reserves and long-range attack systems, but the outcome would be decided by the actions of combined arms battalions and regiments/brigades fighting separately on multiple axes in support of a common plan and objective. Attacks against prepared defenses would be a rarity, as neither side would be able to tie in their flanks or prepare defenses in depth.⁸

The fragmented defense is usually constituted on a wide front with significant gaps between defensive concentrations, strong points, lines and positions. This creates the possibility that an attack will quickly breakthrough into the depths, conduct flank attacks or envelopments and break the defense into pieces. Consequently, the brigade or division in the greater depths of the defense supplements its routes of maneuver while securing communications with airborne, air assault and diversionary reconnaissance groups. They rapidly emplace mine and demolition obstacles, and [conduct artillery] fires at the rear of the penetrated unit to their front in order to counter enemy maneuver and cause the enemy to regroup and resupply....When conducting a fragmented defense, it is necessary to consider the possibility that subunits and units may be surrounded and separated from the main body. It is absolutely necessary to

⁶ D. F. Loza, G. I. Garbuz and I. F. Sazonov, *Motostrelkovyy batal'on v sovremennom boyu* [The motorized rifle battalion in contemporary combat] (Moscow: Voenizdat, 1965), p. 4.

⁷ Ibid.

⁸ V. G. Reznichenko, B. I. Vorobyev, N. F. Miroshnichenko, *Тактика* [Tactics], Moscow: Voenizdat, 1987, p. 60.

constitute a 360° defense in which every element is tactically self-sufficient. It is also necessary to constitute a reserve.⁹

In the event that the enemy penetrates into a city, the fight may become fragmented. Subunits must conduct a determined fight to retain every building. Firing positions located in the upper floors may destroy the enemy located next to the defended building but also fire on distant targets in order to prevent the approach of the enemy reserve. Special attention must be paid to establishing flanking fires and interlocking fields of fire.¹⁰

21st Century tactical combat-brigade defense

Since the collapse of the Soviet Union, Russia has fought two wars in break-away Chechnya, fought a brief engagement in Georgia, re-annexed Crimea, supported a Russian separatist movement in Ukraine and provided direct aid and support to the government of Syria in its war of survival. Russia has changed its ground force structure to primarily a military district-combined arms army-brigade structure and revamped its approach to conventional maneuver war fought under nuclear-threatened conditions.¹¹ Improvements in technology have made the potential future battlefield more deadly-and fragmented. Russia is currently looking at adjusting tactics to fight effectively and survive on the future battlefield.

A sudden illness prevented me from speaking at last year's Finnish National Defence University Russia Seminar, however, my article, "Continuities of Russian Military Thought, Military Reform, Military Strategy and Aleksandr A. Svechin," was published in the proceedings.¹² I noted that Svechin advocated a maneuver defense when the Soviet Union confronted a powerful enemy. Conducting a deliberate withdrawal while engaging the enemy with artillery and limited counterattacks would debilitate the enemy, stretch his supply lines to the breaking point. When the enemy attack culminated, the Soviets should launch a series of powerful counterstrokes to defeat the enemy. This worked against Napoleon and, after a series of bad initial decisions, led to Hitler's defeat by the Soviet Union. Svechin's theories are popular with many leading Russian generals as many recently published articles attest to.¹³ Russian maneuver defense employs their decided advantage in artillery to reduce attacking strength continually while yielding ground until they arrive at a position favorable for a determined defense. Maneuver defense differs totally from the Western Corps-level concept of mobile defense.

⁹ Ivan N. Vorobyev, *Тактика – искусство боя* [Tactics-the Art of War], Moscow: Voenizdat, 2002, p. 584-585.

¹⁰ Ibid, p. 689.

¹¹ Lester W. Grau and Charles K. Bartles *The Russian Way of War: Force Structure, Tactics and Modernization of the Ground Forces*, <https://community.apan.org/wg/tradoc-g2/fmso/p/fmso-bookshelf>

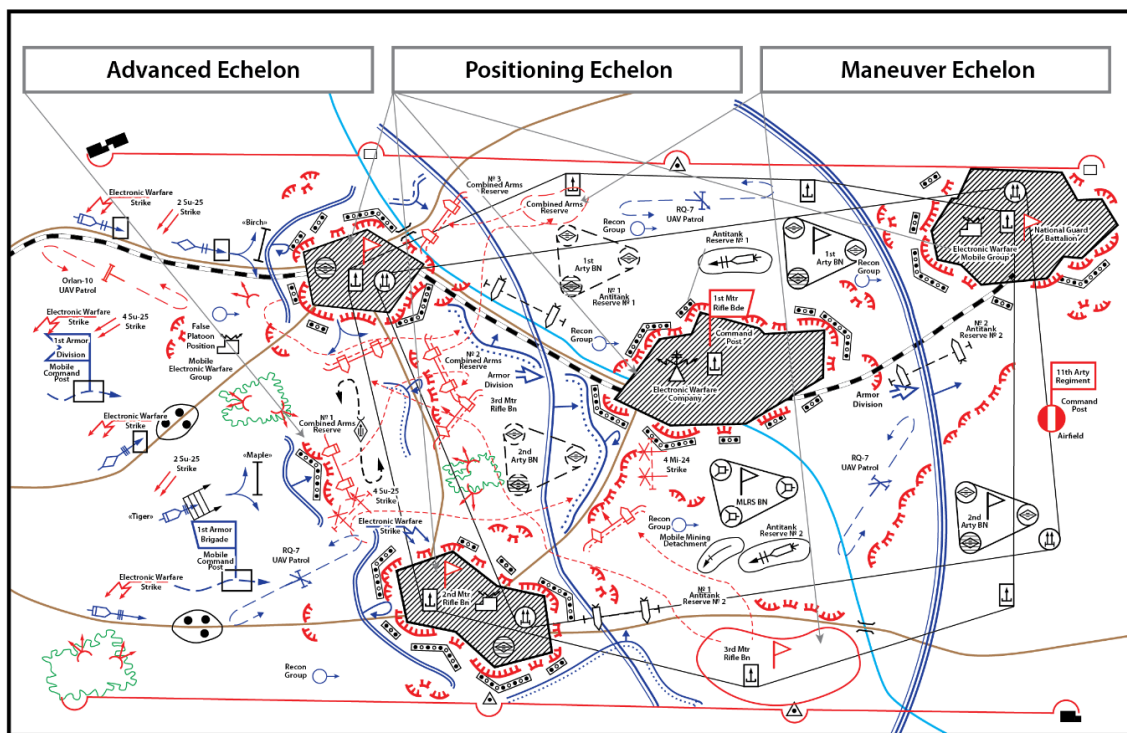
¹² Lester W. Grau, "Continuities of Russian Military Thought, Military Reform, Military Strategy and Aleksandr A. Svechin," *Russian Concept of Deterrence in Contemporary and Classic Perspective*, Helsinki: Finnish National Defence University, 2021, p. 63-75.

¹³ Lester W. Grau and Charles K. Bartles, "The Russian Army and Maneuver Defense", published in *Armor* 19 May 2021. https://www.benning.army.mil/armor/EArmor/content/issues/2021/Spring/2Grau_Bartles21.pdf

Republished in *Armor*, Winter 2020 https://www.benning.army.mil/armor/earmor/content/issues/2022/Winter/ARMOR_Winter_2022_edition.pdf

Improvements in technology have made the potential future battlefield more deadly-and fragmented. Russia is currently looking at adjusting tactics to fight effectively and survive on the future battlefield.

This conceptual layout postulates how a Russian independent motorized rifle brigade might conduct a fragmented defense against an enemy tank division using US equipment. The Russian force has apparently conducted a maneuver defense back to an area conducive to fragmented combat. The defense is divided into an Advanced Echelon, a Positioning Echelon and a Maneuver Echelon. The advanced echelon is constituted for maneuver combat and ambushes; disruption of the enemy's organized attack; and the creation of conditions to turn or draw the enemy attack in a predetermined direction with the goal of destroying him. The positioning echelon is constituted to repulse the enemy advance by inflicting casualties, retain important areas or facilities in the defensive area and create the necessary conditions for the actions of the maneuver component. The maneuver echelon is constituted to cover intervals between defensive concentrations and open flanks; destroy penetrating enemy with fire from occupied positions (firing lines) and counterattacks; to prevent enemy encirclement of defensive concentrations; and to combat enemy diversionary forces.



Picture 1. Russian brigade defends against a US Armor Division¹⁴

The map scale is not indicated, but it is clearly wider than five kilometers and much deeper. The defense sits astride two east-west axes. The northern is a road and single-track rail axis passing through three villages. The southern is a road passing through a village. A motorized rifle battalion each defends the eastern-most villages. The third

¹⁴ S. I. Pasichnik, A. S. Garvardt and S. A. Sychev: “Перспективы развития способов боевых действий общевойсковых формирований тактического звена” [Prospect for the development of methods of combat action by the Combined Arms tactical formations], *Вестник Академии Военных Наук* [Journal of the Academy of Military Science], January 2020, p. 39.

motorized rifle battalion is split into a northern and southern assembly area ready to maneuver where needed. The tank battalion has attached a company to each of the motorized rifle battalions. The two howitzer battalions are forward in temporary firing positions while the multiple launcher battalion occupies its primary firing positions.

In the north, the enemy attacks along the road and rail line with a tank and mechanized infantry company where it is met with electronic jamming, two SU-25 ground attack aircraft, two howitzer concentrations, an ambush and standing artillery barrage "Birch". An Orlan-10 UAV monitors this enemy attack. The town is defended by the 1st Motorized Rifle Battalion, a tank company and air defense assets. The attack is thwarted. In the center, the enemy tank division mobile headquarters is attacked by electronic jamming, an MRLS artillery concentration and four SU-25 ground attack aircraft. An enemy tank battalion attacks on a northeast feeder road to the northern town where it is met with a howitzer fire concentration, a MLRS-delivered FASCAM mine field and an ambush. South of this, an attacking mechanized infantry battalion is met with an air strike by two SU-25 ground attack aircraft, a double moving barrage "Tiger" and standing artillery barrage "Maple". The attacking battalion goes on line only to encounter a mine field and defenses from the combined arms reserve, flanking fire from an ambush and four Mi-24 attack helicopters, and close air defense from a 2K22 "Tunguska" gun/missile track. To the south, the attacking enemy First Mechanized Infantry Brigade, supported by a RQ-7 "Shadow" UAV, is met with electronic jamming, an artillery howitzer concentration, a MLRS-delivered FASCAM mine field, two ambushes and the defenses of the 2nd Motorized Rifle Battalion in the southern town. The 2nd Battalion is augmented with multiple air defense and electronic warfare assets. The attack against the southern village also fails.

The attacking enemy in the north takes up positions outside the northern village and tries to bypass it. Its northern bypass is stopped by a combined arms reserve counter-attack from the 2nd Motorized Rifle Company of the 3rd Motorized Rifle Battalion. Its southern bypass attempt makes headway and causes the withdrawal of the center reserve forces into prepared positions at the mouth of a fire sac between the northern and southern villages. The second howitzer battalion begins to displace by battery to its primary firing positions. A counterattack by the 3rd Motorized Rifle Battalion stops the enemy advance in the center. The enemy tank division builds up its forces for a push in the center while conducting electronic jamming and UAV and ground surveillance. The first howitzer battalion begins to displace by battery to its primary firing positions. When the enemy attack resumes, the combined arm reserve and 3rd Motorized Rifle Battalion withdraw from the fire sac to hold the shoulders of the sac from prepared positions and with the antitank reserve. Four Mi-24 helicopter gunships attack the enemy. The enemy attack is again stopped by the defenses surrounding the third village. The third village holds the brigade and 3rd battalion main CPs. The MRLS battalion begins to displace by battery to alternate firing positions. The 11th Aviation Regiment has displaced to another airfield. The 11th Artillery Regiment is positioned around the airfield to provide supporting fires for the defending Russian brigade. The depleted enemy tank division skirts the third village and attacks along the rail and highway line toward the fourth village which is held by a Russian National Guard battalion and a company "*bronegruppa*" from the second battalion.

Commentary: How successful the brigade defense has been, depends on how much of the enemy division it was able to kill or disable. The defense is more lethal than the

attack if the correlation of forces and means is right and sufficient supplies and ammunition are at hand. Built-up areas are easier to defend than open area, so the brigade chose to create strong points in the villages and use fires and a series of prepared positions and counterattacks to weaken the enemy moving through the more-open terrain. The Russians employ a fire sac where possible and did so in this example. A fire sac allows the defender to engage the point and flanks of an enemy attack simultaneously. The defense employs artillery and aviation to engage the attacking enemy. Control of own air defenses when friendly forces are flying overhead is dicey. Normally Russian close air support is deployed on the flanks or flies a marked route over the ground force.¹⁵ Widespread electronic countermeasures are employed in this example, indicating that much of the Russian defense is fiber-optic or wire-based. (The presence of full-time professional internal security troops from the Russian National Guard indicates that this fight is in Russia or very near her borders. Fiber-optic networks are increasingly common in Russian populated areas and the military has a system of buried wire drop-boxes installed in key areas of military interest.) The attacker is faced with the dilemma of continuing his advance, leaving intact enemy forces on his line of communications, committing follow-on forces to deal with the villages or reducing each of the urban strongpoints in a lengthy attrition fight.

Much has been written in Russian professional military journals about the use of the maneuver defense in conventional maneuver war under nuclear threatened conditions. The maneuver defense also faces the fragmented battlefield, but fights a long attrition battle, trading space for time and terrain advantage while leading to a culminating stationary defense from which a counter offensive can be launched. The above alternate defense relies on the strength of the urban defense combined with fires, rapidly-laid obstacles, electronic combat and counter attacks. It is somewhat reminiscent of the recent experience of fighting in Syria and Iraq with the forces of ISIS.

21st Century tactical combat-brigade attack

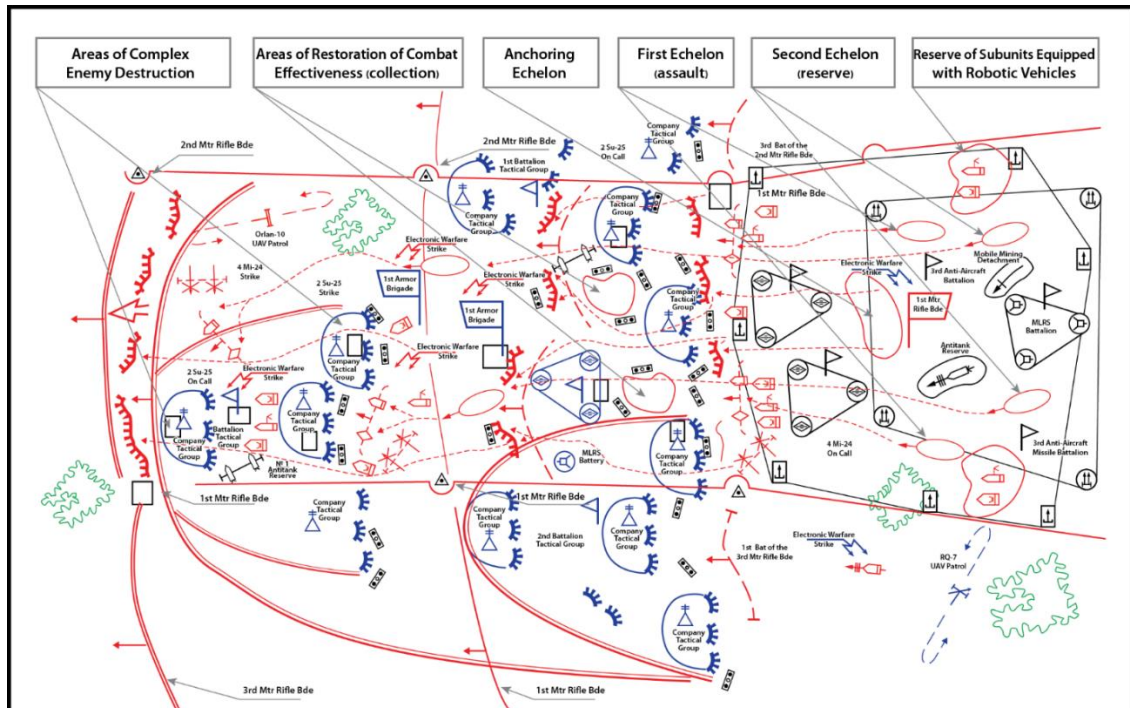
The decisive aim of an attack is to achieve the complete destruction of the enemy throughout the entire depth of his defense, which reinforces synchronized actions in time and the missions of autonomous tactical formations.¹⁶

This conceptual layout postulates how a Russian Separate Motorized Rifle Brigade might attack as part of a three-brigade Combined Arms Army offensive in an attack from positions in close contact. It focuses on the actions of the 1st Separate Motorized Rifle Brigade as it engages part of the enemy 1st Tank-Mech Brigade which is organized into battalion and company tactical groups. The second brigade attacks to its north and the third brigade attacks to its south. The brigade will face six+ company tactical groups, a howitzer battalion, and a MRL battery. The attack is divided into a First (Assault) Echelon, an Anchoring (consolidation) Echelon and a Second (Reserve) Echelon. The First (Assault) Echelon attacks and captures enemy objectives

¹⁵ Lester W. Grau and Charles K. Bartles, "Russian Aviation in Support of the Maneuver Defense", *Aviation Digest* October-December 2018 issue. https://www.rucker.army.mil/aviationdigest/assets/archive/AVN_DIG_2018_10-12.pdf.

¹⁶ S. I. Pasichnik, A. S. Garvardt and S. A. Sychev: "Перспективы развития способов боевых действий общевойсковых формирований тактического звена" [Prospect for the development of methods of combat action by the Combined Arms tactical formations], *Вестник Академии Военных Наук* [Journal of the Academy of Military Science], January 2020, p. 40.

forward of the line of contact and in the depths. The Anchoring Echelon is constituted to retain important areas, lines and points that that would deny enemy deep maneuver and counter attacks. The Second (Reserve) Echelon is constituted to replace assault subunits that have lost their combat potential, to augment strength, destroy the enemy, resolutely retain military objectives and develop the high tempo of the advance.



Picture 2. Russian Separate Motorized Rifle Brigade attacks part of an enemy Tank-Mech Brigade¹⁷

Again, there is no map scale indicated. The attack has an intermediate objective at the rear of the two forward defending companies and a subsequent objective of the rear of the enemy brigade defense. The brigade attacks with two reinforced battalions on line. The tank battalion is attached to the attacking units. The two howitzer battalions are positioned close to the attacking battalions, while the multiple rocket launcher battalion is further back. Two SU-25 ground attack aircraft are on-call to strike on the northern flank of the attack while four Mi-24 helicopter gunships are on call on the southern flank. The antitank battalion and engineer battalion follow the attack.

The assault battalions attack the northern and southern companies in sector, leaving the artillery to pound the middle company while the assaulting battalions bypass the middle company. The enemy brigade CP and artillery battalion are forced to withdraw. The 3rd Battalion (the anchoring echelon) pushes through the bypassed enemy middle company and seizes two assembly areas for disabled equipment, wounded personnel, prisoners and personnel separated from their subunits. The northern assaulting battalion pins the defending enemy reserve company in place and bypasses it to reach and push through the immediate objective. The southern attacking battalion

¹⁷ S. I. Pasichnik, A. S. Garvardt and S. A. Sychev: “Перспективы развития способов боевых действий общевойсковых формирований тактического звена” [Prospect for the development of methods of combat action by the Combined Arms tactical formations], *Вестник Академии Военных Наук* [Journal of the Academy of Military Science], January 2020, p. 41.

pushes forward to the immediate objective and continues on to attack a leading company of the enemy brigade rear. It is supported by four Mi-24 attack helicopter gunships, electronic jamming and reinforced by the brigade reserve.

The northern battalion pushes through to bypass a defending enemy and to attack the last enemy reserve company. The battalion is supported by four Mi-24 attack helicopters, two SU-25 ground attack aircraft, an Orlan-10 UAV and electronic jamming. The southern attack battalion completes the destruction of its company and continues to push through the enemy brigade area to capture or destroy its trains.

Commentary: This is not the fight described in current Russian Army regulations. The brigade attack destroys four of the six+ companies in its AOR. The bypassed two companies are damaged and held in position by the consolidation echelon or have retreated. This new element, the Anchoring or consolidation echelon, polices up the battlefield and helps reconstitute the force. This is very much an aviation, artillery and electronic warfare fight with their fires enabling maneuver. The maneuver is fluid and leaves intact but mangled enemy behind as it pushes to the objective. The tanks are integrated as part of the first echelon and perhaps the reserve. Of particular interest is the presence of subunits equipped with robotic vehicles. The Russians have been developing robotic tanks and other systems for use in the close fight or long-range surveillance. In this example, they appear to be robotic tanks and mine-clearing robots that initially follow the two initial attacks as well as constituting two mobile reserves. Evidently, when the attack meets stiff resistance, the robots deploy forward to kill the enemy or absorb his fire while counter-fire pinpoints and destroys the resistance and to clear paths through minefields. The Journal of the Academy of Military Science—a part of the General Staff that conceptualizes future war published these examples. From the technology depicted, this is near-term future war. It is not the battle described in the Russian regulations, but reflects the impact of Syria and technology advances on the military thinkers. How to mass this three-brigade offensive in this era of detect-destroy technology is a puzzler. This attack is from positions in direct contact—not the favored form of attack for Russian forces, but common in the fighting in Syria.

There is nothing fragmented about this attack. Presumably, this situation occurred from advancing through a fragmented battlefield involving road marches and meeting battles until an enemy encounter resulted in one or both sides going to ground in a hasty defense. The enemy force is formidable enough to require the massing of three brigades by the combined arms army to defeat it.

Conclusion

Technology will continue to expand and empty the battlefield and move it into difficult terrain. The Soviets were quick to realize the value of robotics to augment manpower. The T-62 (introduced in 1961) was the last Soviet/Russian tank to have a four-man crew. The T-64 (fielded in 1964) had an autoloader and a three-man crew. The autoloader enabled the T-64 to maintain a low silhouette, 38-ton weight and employ a 120mm main gun. Current Russian tank design engineers are working on reducing the size of a tank turret and creating a future tank with a two-man crew. Autonomous robots, such as UAVs, are a fairly recent innovation in the Russian armed forces. The use of autonomous robots for conducting ambush and delivering artillery fire are being studied. Tactical directed energy weapons are being developed to protect and

attack optics and optical-electronic systems as well as front-line combat, where such systems could increase the lethality of antitank weapons by 20-30%. Tactical directed energy weapons could also increase the lethality of artillery fire and air defense weapons. This technology might prove effective against UAVs.¹⁸ The concept of robot tanks, controlled by a master tank, has occasionally shown up in Russian writings.

Russia is preparing its forces to fight conventional maneuver war under nuclear-threatened conditions, however it is considering different tactics for different conditions including difficult terrain and advancing technology. Russia's recent conflicts have had an impact on this consideration, especially their recent efforts in Syria.

¹⁸ S. I. Pasichnik, A. S. Garvardt and S. A. Sychev: “Перспективы развития способов боевых действий общевойсковых формирований тактического звена” [Prospect for the development of methods of combat action by the Combined Arms tactical formations], *Вестник Академии Военных Наук* [Journal of the Academy of Military Science], January 2020, p. 41-42.

ON PRESENT WAR IN UKRAINE - KEYNOTE 2

Michael Kofman

As a keynote-speaker Michael Kofman presented his analysis on the 16th of February 2022 regarding the situation in Europe, Russian military preparations and possible development towards a war. His presentation of the Russia Seminar 2022 can be found on the FNDU YouTube-channel: <https://www.youtube.com/watch?v=ywyasBuw7vg&t=3263s> starting from 10:32:00.

Here you may find slightly shortened transcription of the presentation:

Michael Kofman: I will speak briefly on how I see the situation surrounding the current crisis. I will try to make the talk more interesting and be a bit provocative. In my view, the Russian military build-up that we have seen tells us that the leadership of Russia has directed the armed forces to prepare for a large-scale military operation in Ukraine. That is as much as we can glean from the intentions of Russia. Some see this military build-up as a bluff and others see it as a long drawn out game of diplomacy. I personally do not think this is a bluff and I have grown pessimistic about diplomatic solutions. Personally, I am pessimistic about the trajectory of the situation. I am concerned that the political leadership may have already made the decision to conduct a large-scale military operation in principle.

Where are we now?

We are at a situation where masses of troops have stationed and moved themselves to final staging areas. These areas are manned with personnel, support and logistics. These are all the aspects you would expect to see from a military that is actually positioning itself for a military operation, not just an exercise. Overall more than 150 000 troops have been situated. That is not counting the Russian led forces in the Donbass region, the separatists, Rosvgardia units or other auxiliaries. Despite positive signals earlier this week, all I have seen so far is Russian units playing the deployment show game. Some units are rotating around but I have not seen any signs of de-escalation or anything that could to me suggest positive developments.

Looking at the crisis briefly, from my point of view, I think this crisis is not about the NATO or Ukraine, but about both the NATO and Ukraine. We are here in part because Moscow sees Ukraine as part of a Russian geopolitical space and a buffer state in a strategy of extended defence. Russia also wants to relitigate the post-cold war order in Europe. The Russian interpretation of what it should be is rather different than ours. Russia would like the United States in particular to agree to a revised European security architecture where Russia has a veto over the security arrangements. From the Russian point of view, they see current order created at a time of Russian weakness and absence on the continent. As many of you may know and believe, Moscow fundamentally sees itself as a system determining power in Europe and believes it should have a say over the security arrangements. These supersede the ability of

other states to make them independently. Final point on this, I think the issue of NATO is first a political one, because it cements this order of exclusion and expands it, reducing Russia's ability to achieve influence in former Soviet states. The issue is also a military one, military and defence planners are not the local analysts. They focus on capabilities because intentions can change. When they talk about NATO, they are talking about the US power projection on the continent. The conversation is not about one single thing, because this is not a monocausal crisis.

Security guarantees

I am sceptical about potential progress and the earnestness here. It is a very strange case. First in March-April 2021, the Russian military employed many units and issued some red lines, but in the discussions later in the spring they did not make any demands. It was a strange case in the course of diplomacy. There were no tremendous Russian demands back then. Russia has said they do not believe in the US security assurances. Why are they then suddenly asking for legal guarantees they believe the US will abandon one day? There is a problem: the US congress or legislature in Europe is not likely to ratify an agreement with Russia based on these demands.

Diplomatic efforts in December 2021 seem very improvised. The central demands Russia has for security guarantees are obvious non-starters for the West. Russia has been asking for things they know they cannot attain. Diplomacy seems highly performative in this case. Releasing a treaty to the public is not usually how diplomacy is done. Serious diplomacy is usually conducted behind closed doors.

Turning to the issue of why now?

I see it as a case of two overlapping issues. First is the interaction between Ukraine and Russia. Moscow wants a say over Ukraine's strategic orientation, but also aspects of Ukraine's domestic policy. Secondly as they say, Russia looks to block further NATO expansion and roll back its defence collaboration with Ukraine and potentially even other states who are not NATO members.

To me the approximate causes of the standoff are political turns in 2020 and 2021. After being visibly open to dialogue, Zelensky's administration dashed a lot of hopes for Russian compromise and took a hard turn. Westward hard line was chosen by Ukraine. Russia is concerned of Ukraine becoming a platform for power projection.

Other factors to consider are that Russia is in a stable situation economically, it has a war chest. Russian leaders are also confident politically. Russian military has the potential to conduct a large-scale operation. Russian political leaders may hold certain war optimism. Political leaders often have a very different calculus to military professionals. Leaders are often very optimistic or pessimistic about the prospect of a conflict. When the political leaders choose to use force, it is not because they think force is a good option. They begin to rationalise, what are enduring costs of inaction and they start believing that the use of force may be inevitable. There is an argument that Moscow is just fishing for what they can get, but if that is the case, they should take the money and run at this point. Russia can not back down without some external and internal audience costs at this point. If Russia backs down, people will say that it was either bluffing or the more likely argument was that Moscow was deterred. In this case Russia will be seen as highly aggressive and resistible at the same time.

Turning to military options

Given the stakes and likely costs of a military operation in this case. Any Russian military operation would likely have to achieve political gains that would give Russia the ability to enforce implementation in Ukraine. Just hurting the military in Ukraine would not achieve any political goals. The purpose for political leaders to use military force is to achieve political goals. If Russia does use force it is likely to be a very dramatic large-scale military operation. It may involve an attempt at regime change in Ukraine. We are not going to see something small and repeat of the earlier military action, because this would not achieve any political goals easily.

Question and answers:

Question: What is your perception of the internal strength of both the local and the federal government in Ukraine?

Answer: First we should appreciate that very likely there is another shoe to drop in the saga, where Russia would never be contemplating a military operation in Ukraine if Russia did not have plan on how to use certain regional elites. I do not think they plan to actually fight seriously for cities. Nothing consumes manpower faster than urban warfare. But this depends on the reaction of the elites, this is bit of a Schrodinger's cat scenario, you do not know what is going to happen until the worst-case scenario unfolds. My sense of it is that they assume, they will be able to manage the situation without substantial amounts of urban warfare. The Russians may count on the fact that locals may ultimately stabilise many of these areas. Most likely the Russians are optimistic about the amount of resistance they would face. Most likely we are also optimistic about the levels of resistance and the truth will end up being somewhere in the middle.

Question: Could you hypothesize the next steps from the victory day? If looking at the best-case scenario from Russian point of view, how would the future look like? How do you see the way in which people in Moscow see the potential Western reactions and what do you think are their assumptions either explicit or implicit?

Answer: I am going to do what I hate to do, be speculative. Here is my best guess on what is happening on the Russian end. First, it is contingent on how the fight goes. They have several options for a possible military operation and it depends on whether they manage to achieve a pro-Russian government. Potentially they could pursue a very expensive option, if things do not go as planned. They are likely going to try to have the Ukrainians do the actual stabilization, for some people that may seem ridiculous. Also, I think the Russians are expecting the United States and Europe to be self-deterred from actually doing the worst in terms of economic sanctions. Economic collateral damage would be significant. For Russia the next steps depend on how the possible operation goes. In worst case they look partition the country a long a line that makes sense for them. That is going to very expensive option for Russia.

CONTRIBUTORS

Pentti Forsström, DScMil, LtCol (ret.), is a member of the Russia research group and a Senior Researcher at the Finnish National Defence University. He has a General Staff Officer's Degree from year 1997 and he served in the Finnish Defence Forces till 2017. Forsström's military experience includes several positions in Military Intelligence and Strategic Research in Finland and five years abroad. In 2009 he graduated from the General Staff Academy of the Russian Armed Forces. During the last two years in active military service, he finalized his doctoral dissertation on the development of Russian military strategy. In 2019 he was appointed as a senior researcher in the Russia research group. His current research interest focuses on Russian Military in general and the Art of War.

Dmitry (Dima) Adamsky is a Professor at the School of Government, Diplomacy and Strategy at the Reichman University, Israel. His research interests include international security, cultural approach to IR, and American, Russian and Israeli national security policies. On these topics he has published several dozens of articles in the leading world academic journals. His books *Operation Kavkaz* and *The Culture of Military Innovation* (Stanford UP, 2010) earned the annual prizes for the best academic works on Israeli security. His book *Russian Nuclear Orthodoxy: Religion* (Stanford UP) won the 2020 ISA best book award in the category of Religion and IR. His forthcoming book with Stanford UP *Deterrence a la Russe* (2022) deals with Russian art of coercion. His current book-length project - *The Commissars* - deals with the nexus of the military, politics and ideology in contemporary Russia.

Leonid Nersisyan is a defence analyst and CEO at Armenian Research and Development Institute. He also holds experience in consulting and research. His research interests include CIS countries' armed forces and defence industry.

M.Mil.Sc., Major (ret.) **Jukka Viitaniemi** is a senior researcher at the National Defence University. Jukka Viitaniemi's military experience includes several positions in the Finnish Army and in Military Intelligence in Finland and abroad. His current research focuses on Russian Military Strategy. Viitaniemi is also a doctoral researcher at the FNDU.

Jyrki Terva is a doctoral researcher at the university of Tampere. He has focused on international relations and Russia in his research. He is currently on a study leave from his diplomatic position at the Ministry of Foreign Affairs.

Colonel (ret.), **Juha Wihersaari** is a doctoral researcher of the Russia Research Group at the FNDU. He has the General Staff Officer's Degree from 1993 and he served in the Finnish Defence Forces until 2015. Wihersaari's military experience includes positions mainly in military intelligence, where he served 26 years. Since 2016, Wihersaari has been the owner and director of a small intelligence and security company.

Oscar Jonsson is Director for Phronesis Analysis and researcher at the Swedish Defence University. He holds a PhD from the Department of War Studies at King's College London and is the author of *The Russian Understanding of War* (Georgetown University Press).

Rod Thornton, PhD, is an Associate Professor working for King's College London at the UK's Defence Academy at Shrivenham. He has served in the British Army and has lived and worked in both Kyiv and Moscow. He teaches across a range of courses and subject areas, mostly related to the Russian military and strategic studies. He is the author of several articles on the Russian military more broadly and on its information warfare activities more specifically. His latest article (with Marina Miron) is entitled 'Winning future wars: Russian offensive cyber and its vital importance in Russian strategic thinking', will appear in *Cyber Defense Review*. He is currently writing a book on the Russian armed forces.

Marina Miron, PhD, is an Honorary Research Fellow in the Defence Studies Department of King's College London. As well as works on counter-insurgency she has several publications in the sphere of Russian information warfare. She has worked on several projects related to emerging technologies including the use of drones and the development of offensive and defensive cyber tools in the context of information warfare as used by Russia and China. She has lectured to UK MoD audiences on 'Information Warfare' and on 'Human Augmentation'. Currently, she is focusing on the integration of AI into military technologies within the framework of grey-zone warfare. She is also currently working on a UK MoD-related project on the ethics of human augmentation in a defence context.

Jonna Alava, M.A. is a doctoral researcher at the University of Helsinki and a member of the Russia Research Group at the National Defence University since August 2019. Her article-based dissertation examines gender aspects in the military-patriotic education in Russia. The first article 'Russia's Young Army – Raising New Generations into Militarized Patriots' analysed discourses in which the legitimization of the military-patriotic youth organization 'Yunarmiya' is constructed. The second article examines the representations of female soldiers in the Russian armed forces. The latest article deals with the nationalist transformation of Russian patriotic education during the war.

Aristide M. LaVey is a visual information scientist specialising in eastern Slavic art. His recent article "Reading Belarus: The evolving semiosis of Belarusian textiles" and forthcoming article "Archiving the digital semiosphere: A case study in Belarus" analyse the use of textiles and digital protest art in the period surrounding the 2020 Belarusian presidential election. LaVey served in the U.S. Army for ten years as a paratrooper and strategic communications officer, mostly in Europe and Iraq.

Santeri Kytöneva is working as a research assistant at the Finnish National Defence University. He has focused on topics surrounding the Russian definition of war, justification of force and information security.

Justin Bronk is Senior Research Fellow for Airpower and Technology in the Military Sciences team at the Royal United Services Institute (RUSI) in London. He is also Editor of the RUSI Defence Systems online journal. Justin's particular areas of expertise include the modern combat air environment, Russian and Chinese ground-based air defences and fast jet capabilities, unmanned combat aerial vehicles and novel weapons technology. He has written extensively for RUSI and a variety of external publications, as well as appearing regularly in the international media. Justin is a part-time doctoral candidate at the Defence Studies Department of Kings College London and holds an MSc in the History of International Relations from the London School

of Economics and Political Science, and a BA (Hons) in History from York University.

Lester W. Grau, PhD, Lieutenant Colonel (ret.) is a Senior Analyst for the Foreign Military Studies Office (FMSO). Grau has served the U.S. Army for 52 years and his military experience includes, for instance, service in Vietnam War and later teaching and research. Grau's research focuses on tactical, operational and geopolitical subjects and Russian military. His latest publications include: *Russian Engineer Reconnaissance in Icy River-crossing Conditions*, published by Engineer January-April 2020; *Activities of the Russian Ground-Based Contingent in Syria*, Russia's War in Syria: Assessing Russian Military Capabilities and Lessons Learned, co-authored with Charles Bartles, Foreign Policy Research Institute, September 2020; *The Russians Train for Arctic Riverine Operations*, published by Marine Corps Gazette November 2019.

Charles K. Bartles is an analyst and Russian linguist at the Foreign Military Studies Office at Fort Leavenworth, Kansas. His specific research areas include Russian and Central Asian military force structure, modernization, tactics, officer and enlisted professional development, and security assistance programs.

Michael Kofman is a Director of the Russian Studies Program at CNA and a Kennan Institute Fellow at the Woodrow Wilson International Center. Previously he served at National Defence University as Program Manager. Kofman's research focuses on security issues in Russia and Eurasia, and he has published numerous articles on the Russian military, Russian strategy, doctrine, combat operations, and security issues in Russia and Eurasia. "The Ogarkov Reforms: The Soviet Inheritance Behind Russia's Military Transformation", *CCW Russia Brief* 2019: 5, p. 10–12 is one of his latest publications.

National Defence University

Department of Warfare
PL 7, 00861 HELSINKI

Puh. +358 299 800

www.mpkk.fi

ISBN 978-951-25-3287-2 (pbk.)

ISBN 978-951-25-3288-9 (pdf)

ISSN 2343-5275 (print)

ISSN 2343-5283 (web)

SOTATAIDON YTIMESSÄ



Puolustusvoimat
The Finnish Defence Forces