JYU Reports 49

Mari Puurunen

BLOODLESS BUT DEADLY

Information warfare in Russian military science research

JYU REPORTS 43

Mari Puurunen

BLOODLESS BUT DEADLY

Information warfare in Russian military science research

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2024

Cover illustration: Juuso Laasonen

Permanent link to this publication: http://urn.fi/URN:ISBN:978-952-86-0338-2

ISBN (PDF)
URN:
ISBN: 978-952-86-0338-2
DOI: 10.17011/jyureports/2024/49
ISSN 2737-0046

Contents

Abstract

This report examines the terminology of Russian information warfare from the annexation of Crimea and the start of the war in Eastern Ukraine until 2023. The report is based on the analysis of articles on information warfare published between 2014 and 2023 in two of the most prominent Russian journals on military science, Vestnik Akademi Voennyh Nauk and Voennaya Mysl. The terminology is categorised in the report in line with the Russian Armed Forces Dictionary into information warfare objectives, resources and means. The terminology was found to be extensive and constantly evolving, providing the Russian government with political latitude, which it has made use of, for example, in Ukraine since spring 2022. The Russian perspective on information warfare is holistic, and several terms of Anglo-Saxon origin have been adopted to refer to centuries-old Russian warfare concepts. Information warfare is seen as part of a civilisational struggle between Russia and the collective West, which varies in intensity and manifestations. Russia makes no distinction between war and peace. After the war of aggression launched by Russia in 2022, a shift to a kind of post-truth era has emerged, where facts are of secondary importance and the focus is on elements related to an individual's information processing, emotions and decision-making, which are subject to the influence of information warfare. In this phase of information warfare, it is crucial to saturate the information space with content that serves Russia's strategic objectives in the long run. As of spring 2022, the political rhetoric of the Russian regime has been integrated into research publications, reflecting a broader shift in Russian society towards totalitarianism.

1 INTRODUCTION

One of the most prominent Russian military historians of the 20th century, Anton Antonovich Kersnovsky, presented in his work The Philosophy of War (1939, pp. 104-108), a theory of the division of the human mind into two parts, one being intellectual and the other based on willpower.[1] In Kersnovsky's view, the ideal state for a soldier is a perfect balance of these two elements. Kersnovsky's works on the history of the Russian army are part of the foundation of Russian military historiography. In his works, he argued that the existence of war is an indispensable part of human civilisations, and that the only way to end war is to end human life on Earth. Despite his radical views, Kersnovsky has remained a part of the Russian military-political discussion because of the portrayal of the human being in his work mentioned above.

As we move into the 2020s, Kersnovsky's concepts have been described as mental warfare (in Russian ментальная война, mental'naya voina), although the term is not used in the original work. Andrey Ilnitsky, a long-time advisor to the Russian Defence Minister, politician and researcher, referred to Kersnovsky's work in an interview with the Russian Armed Forces weekly Zvezda in April 2021. According to Ilnitsky, Kersvnovsky's theory of the human mind is about the struggle between understanding or information and willpower, where willpower always wins over understanding and information. In contrast to previous descriptions of information warfare, what is interesting is Ilnitsky's view of the nature of information as well as the Russian information environment. The second half of decision-making, what Kersnovsky had previously described as the mental or intellectual side, had been transformed in Ilnitsky's interview into information. According to him, the

[1] In his work, Kersnovsky uses the terms ум and воля, the first of which directly translates as mind or intelligence, and the second as will.

current information state is also a complex world in which individuals make decisions deprived of the capacity for critical thinking, under outside influence.

According to Ilnitsky, mental warfare is not about manoeuvring in the grey area between war and peace, as the American hybrid warfare strategies imply, but rather, as Kersnovsky sees it, a war of civilisations that is constantly ongoing. Ilnitsky describes mental warfare as taking place in today's "post-truth" world, in which people have been alienated from critical thinking, and in which public opinion, emotions and the subconscious are actively manipulated. This differentiates it from cyber and information operations. Mental warfare, as described by Ilnitsky, has gained popularity as a research topic in Russian military science publications since 2021.

This report presents an overview of Russian information warfare terminology from the start of the war in Eastern Ukraine in 2014 until 2023. The data for the analysis was compiled from articles dealing with information and warfare published in two of the most prominent military science journals, Vestnik Akademi Voennyh Nauk and Voennaya Mysl.[2] In this article, the term information warfare was chosen as an overarching term to describe the Russian government's attempt to systematically control the information space for the following three reasons: (1) information warfare is a direct translation of the Russian terms most commonly used in research, (2) other terminology related to information warfare can be somewhat organically arranged under the umbrella concept of information warfare, and (3) unlike Western countries, Russia does not distinguish between wartime and peacetime information activities, which are seen as a weapon to achieve political goals at the expense of individuals, social groups and states (Berzina 2018, p. 162). Ulrika Franke (2015, p. 10) has also highlighted the lack of systematic translation of terms used in information warfare between Russian and English. According to Franke (2015, p. 10), the term information warfare is also no longer actively used in NATO or the United States, so it has an appropriate "foreign ring".

According to the Russian Armed Forces Dictionary, information warfare consists of information as an objective, resource and means (Военный энциклопедический словарь 2024, Информационная война). This distinction is also used in the subheadings of this report, but it is worth noting that Russian thinking on information warfare is characterised by its comprehensive nature and adaptability to political needs, which means that the distinction itself is not immutable or categorical.

[2] in Russian Вестник Академии военных наук; Военная Мысль.

In Russian research, there has been an increase in the study of information warfare since 2014, and the latest spike in the number of published articles dates to spring 2022, when Russia launched a large-scale and illegal war of aggression against Ukraine. In addition to the numbers, the research field also reflects a certain shift to a time of crisis or conflict. Since the spring of 2022, the diversity of the published articles, especially in regards to the definitions of terms, has decreased, and top-down political rhetoric seems to have increasingly taken over research content concerning the causes, consequences and objectives of the war.

2 ON INFORMATION WARFARE

The aim of influencing the thinking, judgement and beliefs of the individual has also always been a part of Russian warfare. The range of means available for information warfare expanded significantly in the 1990s with technological advances, and the Gulf War is seen in the Russian research literature as the first example of a "modern information war" (Novikov & Golubchikov 2017). The Russian narrative of the US attempt to incite information warfare in third countries not only furthers Russia's superpower aspirations, but also shapes military science research (Clark 2020).

The information dimension of warfare became a more prominent topic of discussion in Russia around the time of the occupation of the Crimean Peninsula and the outbreak of the war in eastern Ukraine in 2014. A characteristic feature of research on information warfare in Russia is its focus almost entirely on describing the information operations of Western countries, such as the United States and the United Kingdom, with Russia actively playing the role of a victim. The Russian research field of information warfare covers a wide range of themes, which in Western research are often categorised under the research themes of hybrid and information influence, strategic communications, cyber warfare, psychological warfare and disinformation.

In the broader field of research, information warfare research is often positioned in the context of future warfare research. Thus, it is to be assumed that Russia is trying to proactively predict future developments. Indeed, part of the Russian information warfare narrative is the bitterness, carried over from the Soviet era, about the West's advantage in technological development. Russia sees itself as being at a disadvantage when it comes to new technologies, and the West as trying to hinder Russia's technological development. Russia sees technological development as one of the pillars of its superpower thinking. (See Thomas 2014; Puurunen, 2021.)

The Russian military scientific research field uses an extensive terminology to describe the phenomena of information warfare, the diversity of which has been

increasingly discussed within the scientific community since 2014 (Kuleshov et al. 2014). One of the most active researchers on hybrid warfare, retired officer and member of the Russian Military Academy Aleksandr Bartosh (2022), argued in an article published in January 2022, a month before the start of Russia's large-scale war of aggression, for a clarification of terminology for the complex phenomenon to be understood in decision-making. Other authors who have commented on the clarification of terminology are Chekinov and Bogdanov (2015), Lata et al. (2019), Ilnitsky (2021), Karavayev & Sukhanov (2022) and Belokon (2022). The themes of Russian information warfare have also been studied by Pynnöniemi (2020, 2019, 2018), Kari (2019), Pynnöniemi and Kari (2016), Vasara (2020), Giles (2023, 2016), Giles and Akimenko (2020), Pomerantsev and Weiss (2014), Berzina (2018, 2019), Franke (2015), Panarin (2006) and Thomas (2004).

During the 2000s, information has also become an increasingly important aspect of security also in Russian strategic guidance documents, such as the latest National Security Strategy (2021) and the Concept of the Foreign Policy of the Russian Federation (2023). In both documents, Russia's national interests and strategic objectives are stated in the same phrasing as “the development of a safe information space, the protection of Russian society from destructive information-psychological impact”.

Also, in the previously published Military Doctrine (2014), information influence emerged as an overarching theme of the document due to the invasion of Crimea and the war in Eastern Ukraine (Krieg 2023, 122–123, Pynnöniemi & Mashiri 2015). The military doctrine also highlights the notion of technological backwardness compared to the West. In fact, the 2021 National Security Strategy presents technological development as one of the most important actions to improve information security in Russia. The notion of technological backwardness is also highlighted in the Information Security Doctrine of the Russian Federation (2016). In Russia’s view, the strategic balance has tipped in favour of the West, thus threatening Russia’s position as a superpower. The doctrine defines Russia’s national interests and threats with regard to information security, as well as measures to minimize the threats and strengthen security. The document also describes information security arrangements as part of Russia’s national security.

The doctrine, in common with other strategic guidance documents, does not separate the cyber dimension from the information dimension, but rather considers it part of it. Threats to information security include information-psychological and information-technical operations, the latter of which refers to the cyber dimension of information security, and the former to activities related to an individual’s cognition.

Furthermore, the Russian view of information warfare does not distinguish between war and peacetime activities, but rather sees information warfare as an ongoing struggle that affects the whole of society (Pynnöniemi 2019, 216). Russia also uses rhetorical means in an attempt to shift the playing field in its favour by presenting the collective West as the aggressor. One of the clearest ways is to use proprietary terminology which is a part of strategic communication both domestically and abroad. By presenting itself as a victim of information warfare, Russia opens up opportunities for so-called defensive actions to protect its sovereignty and achieve its strategic objectives.

3 INFORMATION WARFARE AS AN OBJECTIVE

From the Russian perspective, information and the information space are seen as part of a centuries-long zero-sum game between the superpowers, where the losers are those, whose messages do not spread widely and do not produce the desired results for the propagator of the messages. In contrast, the winning countries are able to control the future direction of the losing countries and to define their worldview, values and interests as they wish.

Information as an objective is largely manifested in the Russian debate as an attempt by the West to weaken Russia through the means of information warfare. In the debate on the objectives of information warfare emerge, the topics of controlling the new generation wars (Russian: новое поколение войны, novoe pokolenie voini) or future wars (Russian: война будущего, voyna budushchego), reflexive control and its necessity in managing the information space, and the cross-century duration of the information warfare time span. Vasara (2020, pp. 44, 78) defines reflexive control as influencing decision-making in order to induce an opponent to make a decision that is predetermined and advantageous to the influencer, seemingly independently, by manipulating the information that the opponent receives. Alternatively, decision-making can either be blocked or slowed down (Vasara 2020).

From the Russian perspective, information warfare is part of the long-term struggle between civilisations. Marichev et al. (2021) describe geopolitical projects of mental warfare as long-term series of events measured in decades and centuries. They define the politics of history and the sovereign right of the state to write its history as among the most essential objectives of information warfare. Thus, the objective of mental warfare is to destroy the self-consciousness of a people, and to transform its spiritual and civilisational foundation. The narrative of the struggle between civilisations takes its place in the Russian political discourse as part of

arguments that see Russia as separate from the rest of Europe and "Western civilisation". This juxtaposition is a continuation of the ideological juxtaposition of the Cold War era, and it also supports the Russian view of the sphere of interest in Eastern Europe. (See Joenniemi 2008; Pynnöniemi & Jokela 2020.)

Since Russia launched its large-scale and illegal attack on Ukraine in February 2022, a concept that has gained prominence is that of mental warfare, where the act of "consciousness renewal" directed at communities, groups and individuals leads to the subjugation of the targeted group of people when an external aggressor destroys the "idea" that unifies the group (Karavayev & Suhorov 2022). In a publication of the Russian Academy of Military Sciences, Ovsyannikova (2022), a Candidate of Pedagogical Sciences, describes the vulnerability of Russian youth in particular to Western information warfare, which is seen as resulting, among other things, in forgetting the historical events of their own country, rejection of traditional moral values and indifference to the common interest of society. The language of the article largely follows the Russian political canon concerning the causes and consequences of war, and the appeal for the requirement to put the interests of the Russian state before selfish, individualistic interests unambiguously reflects Russia's development into a totalitarian state following the war of aggression.

Russia's information warfare is also aimed at its own citizens, who are likewise being deprived of independent thought by replacing it with state-controlled information. These views on information warfare are not new, having already appeared in the 2016 Doctrine of Information Security. Instead, the harsher rhetoric and increasingly delusional claims of, for example, "cleansing the region of the Ukronazis" or "ending the neo-Nazist activities of the United States" (see, e.g., Karpovich 2022, Ovsyannikova 2022, Manoilo 2022, Kulakov 2023) indicate an increasingly open shift of military academy scholars and military publications into Putin's vertical of power and a general trend towards totalitarianism. Such narratives feed the Russian public's mistrust of foreign countries and provide an opportunity to justify Russia's actions with the objective of winning the ostensible Western-led information war.

According to research professors at the Military Academy of the General Staff of the Armed Forces of the Russian Federation, Chekinov and Bogdanov (2015), the wars of the future will be decided by a skillful combination of military, non-military and special non-violent means, which will be used in combination with political, economic, informational, technological and environmental means, mainly employing information superiority. According to the comprehensive and holistic Russian view, information warfare will be the starting point and a key element in future wars. One of the objectives of information warfare is to defeat the opponent in the information

space without engaging in combat. Kulakov (2023) refers to this kind of warfare as "bloodless but deadly".[3]

An essential part of information warfare is also the theory of reflexive control, which has been studied in Russia (and previously in the Soviet Union) since the early years of the Cold War. The development of new technologies as well as Russia's aggressive foreign policy towards post-Soviet states have restored the model of reflexive control to the heart of Russian operations and information warfare (Thomas 2004). Reflexive control is used to influence an opponent's decision making by feeding manipulated information to the opponent. Through the burdening of the decision-making process by limiting available options and time, the aim is to direct the opponent to making decisions that are convenient for the influencer. Reflexive control can impair or potentially paralyse the opponent's decision-making capacity. (See Vasara 2020, p. 35.)

In his article on future wars, Kulakov (2023) describes algorithms as a new form of technical implementation of reflexive control. In what are referred to as "algorithmic wars", the value of information is no longer in its qualitative or quantitative aspects, but rather in how information is received, used, processed, analysed, stored and distributed to achieve certain objectives and solve specific problems. According to Russian researchers, the international information space has become militarised, which has led to the rise in popularity of the term information warfare. The information space is seen as one of the theatres of warfare, and its control is essential to achieve the objectives of war.

The information space is seen as one of the arenas of war, and its control is essential to achieve the objectives of warfare. In contrast with the Western way of thinking, the Russian perspective looks further into the future, beyond generations. Thus, to support information warfare, Russia is totalitarianising and militarising its own population to respond to a perceived external threat. At the same time, it seeks, through information warfare, to place external actors under "reflexive control". The purpose is to induce seemingly independent actors to make decisions that are favourable to Russia by means of carefully selected information feeds.

[3] «бескровную, но смертельную».

4 INFORMATION WARFARE AS A RESOURCE

In Russian thinking, information is also seen as a resource for achieving the objectives of information warfare. Akimenko and Giles (2020), who have studied these themes of information and cyber warfare, refer to the domain of information warfare. In this article, information warfare resources include both the central concept of information space and the domains of information warfare, including information-psychological warfare, cyber warfare and hybrid warfare, which is strongly related to the topic.

In the Doctrine of Information Security of the Russian Federation (2016), information space (Russian: информационное пространство, informatsionnoe prostranstvo) is defined as a combination of information, objects of informatisation, information systems and websites, communication networks and information technology. In addition, the information space includes actors that produce and process information, develop and use the technologies mentioned above and safeguard information security, as well as mechanisms that regulate social relations in the information space. Informatisation (Russian: информатизация, informatizatsiya) is a term used to refer to social development in which the development of information technologies is coupled with social, economic and technical processes. Through its foreign and security policy, Russia seeks to exploit the informatisation development of societies in order to weaken their cohesion. (See Pynnöniemi & Kari 2016.)

The information space is seen as an abstract field where the battle is waged with competing narratives against opposing views. From a Russian perspective, inseparable parts of the information space include both information operations and cyber warfare (Giles 2016, p. 9). According to the information security doctrine, to maintain a strategic balance, Russia's sovereignty in the information space must be safeguarded so that Russia can pursue its national interests. Information and its

security are seen as the foundation of Russia's foreign and security policy. (See Kari 2019, p.78; Pynnöniemi & Kari 2016.)

The struggle taking place in the information space is referred to in Russian military studies and political rhetoric using a number of terms, which partly support each other, but also overlap. The umbrella term used in this article, information war or information warfare (Russian: информационная война, informatsionnaya voyna), is the term most often used in Russian research to describe the struggle for control of the information space between Russia and the "collective West".

What is significant is that most of the articles published on the subject treat information war specifically as an attack by the West on Russia. Another indication of this is the very often used term information counter-struggle (Russian: информационная противоборство, informatsionnaya protivoborstvo). See, for example, Chekinov & Bogdanov 2015, Bartoš 2018, Gryzlov & Pertsev 2015. In both English- and Finnish-language research, the term, often translated simply as information warfare, ignores the Russian intentionality of presenting Russia in the information war as a target of attack and a defender. Instead, the term should be translated as counter-confrontation or counter-struggle. Previous authors on the topic include Giles (2016), Ristolainen (2017) and Pynnöniemi (2019). In contrast, the concept of information influence, which is often used in Finnish research literature, does not appear in the Russian articles at all, because information activities directed at another state are, fundamentally, hostile with harmful intent. In the Russian leadership's worldview, war is an ever-present condition, with varying intensities and arenas of warfare. Thus, information is a weapon, the use of which is, in principle, always a combative action. In fact, in Russian research, the term informatsionnaya borba (Russian: информационная борьба) appears alongside information warfare and counter-struggle, which could be loosely translated as information combat (see, e.g., Dylevski et al. 2016).

Two arenas of warfare, psychological warfare and cyber warfare, are also seen as a specific resource for information warfare. Psychological warfare is also often described using the aforementioned term counter-struggle, linking it to information-psychological operations. Information-psychological counter-struggle is defined as the psychological influence exerted on the civilian population and/or military personnel of another state in order to achieve political and military objectives. Thus, consciousness at both the population and individual level is under influence. (See Kuleshov et al. 2014; Giles 2023, pp. 34–35.)

The consciousness of the individual has increasingly been the focus of information warfare research, especially towards the 2020s. According to Ilnitsky (2021), the information space today is full of "necessary" content that can be used to

manipulate both individuals and large masses of people. In this way, it is possible to influence both human emotions and decision-making. Russia's way of operating in these areas of information warfare is to identify the opponent's weaknesses, which it then seeks to exploit to its own advantage. Ilnitsky (2021) describes a trend originating in the United States of a division in democratic societies, which he says is driven by radical feminism, the anti-racist movement and the green transition, among other influences. These and many other dividing lines in societies are being used by Russia against the open democracies of the West. In his theory of mental warfare, Ilnitsky (2021) describes information warfare as being simply about influencing people's minds, a struggle for consciousness (Russian: борьба за сознание, borba za soznanie). (See Ilnitsky 2021 and Karavayev & Sukhanov 2022.)

According to Ilnitsky (2021), mental warfare is divided into two elements used to influence people's minds. The information element consists of a reformation of the information space, knowledge and facts, in which all elements of information are subject to regulation and change. This modification of information concerns all available information from news sources to research data, education from pre-primary to university and content from television programmes to archive sources. Thus, information is "corrected" according to what produces favourable results in achieving victories in information warfare (Ilnitsky 2021). This "correction of information" has manifested itself in the Russian war of aggression as an intermittent cacophony of different narratives as well as contradictory content, which, from a Western point of view, may even appear as lies that have been pushed to the point of being ridiculous. More relevant, however, is the longevity of the narratives and the occupation of the information space, which are believed to create disbelief among the citizens of both Ukraine and its supporters as the war is prolonged and its costs increase.

The psychoemotional element is based on the manipulation of consciousness, states of mind and emotions, instead of the manipulation of information. The objective of this manipulation is to influence an individual to accept a particular assessment, view or opinion on a critical issue. An individual, group or society is exposed to the intended inputs without the target being aware or understanding what the manipulation is leading to. This reformation of consciousness (Russian: переформатирование сознание, pereformatirovaniye soznaniye) is discussed to some extent in the Russian research literature, often in connection with the patriotic education of children in Russia. (See Ovsyannikova 2022.)

The resources of information warfare also include cyber warfare, often identified in Western research as a separate field of warfare. In Russian texts, cyber warfare is more naturally characterised as being part of information warfare and "network warfare", where the arena is not only information networks and critical

infrastructure, but also ordinary social media platforms (Sheremet 2016, Chvarkov & Lihonosov 2017). At the core of this thinking is the value of information itself, rather than the various channels through which it is transmitted. Information is created, processed and shared in the cyber environment in the same way as in the rest of the world. Consequently, in Russian research, cyber warfare or the cyber dimension do not stand out as a strong separate theme, but rather appear in connection with the cyber activities of foreign states or when talking about technical implementations of information warfare. Cyber warfare does not constitute a separate entity in Russian information warfare, and its broad range of applications differs from Western thinking on cyber warfare. Since cyber warfare is not seen as a clearly defined form of warfare, it opens up the possibility for Russia to combine cyber activities with other means of information warfare, such as the use of disinformation, kinetic and electronic warfare, and measures to exert pressure directly on state leadership. (See Akimenko & Giles 2020.)

A significant terminological debate in the Russian discussion on future wars is the definition of hybrid warfare and hybrid means. The term hybrid (Russian: гибрид, gibrid), which is clearly of foreign origin, became common in Russian debate after a speech given by Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, to the Russian Academy of Military Sciences in 2013. The speech was also published in the Voenno-Promyshlennyi Kurier newspaper, which publishes weekly news on the Russian military-industrial complex (Gerasimov 2013). In his speech, Gerasimov described changes in modern warfare and the range of means available in future wars, especially the combination of "non-military means" (Russian: невоенные меры, nevoennye mery) with military force. Gerasimov listed information as one of the means along with political, economic and humanitarian means, for example. (See Pynnöniemi & Jokela 2020.) These means had already been identified, for example, in a previous update of the military doctrine in 2010, but in Gerasimov's speech they were reportedly combined for the first time under the term hybrid warfare.

In the Russian context, the use of the hybrid term, which has received widespread international attention, reveals the culmination of Russian strategic thinking in attempts by the West to destabilise Russia politically, rather than in the tactical aspects of warfare. Another essential aspect of the debate on hybrid warfare is that it is centred in the Western countries, which are waging war against Russia by non-military means. Exactly the same rhetorical setup can be seen in the debate on information warfare.

In contrast to the Western view, Russia sees information as a multifaceted resource with a wide range of uses. The concept of information warfare appears in

Russian discourse in many different forms, but its underlying meaning remains the same. Running alongside information-psychological warfare, cyber warfare, as well as hybrid warfare, are part of holistic Russian views on the nature of information.

5 INFORMATION WARFARE AS A MEAN

The Russian holistic understanding of information warfare requires a wide variety of means. The Russian debate on information warfare identifies a large number of ways in which Russia sees the West attacking it in the information space. By examining this debate, we can try to understand Russian perspectives on the threats that Russia perceives itself to be facing.

One of the means of information warfare that is most often mentioned in the Russian debate are the “colour revolutions”. This refers to the changes of power that took place at the beginning of the 21st century in countries that gained independence from the Soviet Union, such as Georgia, Ukraine and Kyrgyzstan, and which were unfavourable from the Kremlin’s point of view and in some cases chaotic. The colour revolutions resurfaced in the debate with the invasion of Crimea and the war in Eastern Ukraine in 2014, and, since then, they have become partly synonymous with hybrid warfare in Russia. The Russian view is that especially the United States is inciting colour revolutions near Russia's borders, with the aim of creating controlled chaos (Russian: управляемый хаос, upravlyaemyy khaos) in the country, intended to bring about a coup d'état. (Berzina 2019.) According to Gerasimov (2016), colour revolutions are based on information technologies which are used to manipulate the population’s potential for protest along with other non-military means.

In addition to the colour revolutions, Russia sees the West as trying to weaken Russia through the use of what is referred to as soft power (мягкая сила, myagkaya sila). The term refers to non-military activities. In Russian research literature, soft influence is defined as “the capacity to achieve desired outcomes by attracting an opponent to your side or neutralising an opponent through peaceful means” (Chvarkov & Lihonosov 2017).

Soft influence is based on prevalent sociocultural factors such as culture, values, traditions, concepts, symbols and myths. Soft influence uses a wide range of measures, including culture, information, gathering of intelligence, networks and psychology. The intention is to change the psychological state of an individual, an ethnic group, a religious community or the population of a country.

(See Chvarkov & Lihonosov 2017.)

The goal of using non-military means is to achieve a geopolitical victory over the opponent, resulting in the disintegration and dissolution of the opponent's state institutions, the loss of its territory and resources, and the fracturing of the civilisational, religious, cultural and national identity of the state's population. This "model of state disintegration" has been described by former member of the Duma, political scientist Alexey Podberezkin in his book Probable scenario of the development of the international situation after 2021 (2015).[4] This topic has been analysed by Puistola and Voinoff (2023).

According to Chvarkov and Lihonosov (2017), researchers from the General Staff of the Armed Forces of the Russian Federation, it should be strongly emphasised that such a victory in a geopolitical confrontation is irreversible and historically indisputable, as the losing side ceases to exist. The use of soft power is also noted as being one of the most effective means currently available in international geopolitical warfare for weakening existing and potential enemies.

The "weapons" or main means of information warfare are roughly divided into the information-psychological weapon and the information-technical weapon. Both of these are covered by the term information weapon (Russian: информационное оружие, informatsionnoye oruzhie), which is described in the Armed Forces Dictionary as including technical intelligence, mass media, information security, mind control equipment and other non-lethal means. (Военный энциклопедический словарь 2024, Средства информационной борьбы («Информационное оружие»)). Key features of the information-psychological weapon and information-psychological warfare are their continuity and their independence of the relationship between the parties. Information-psychological warfare is a manifestation of the permanent struggle for existence between civilisations, and the use of the information-psychological weapon does not require open conflict, but rather it is a tool for winning the information struggle. (See Akimenko & Giles 2020; Kivimäki 2017.)

The term information-technological weapon roughly reflects what is called cyber warfare in the West. At the heart of Russian thinking, information as an

---

[4] Вероятный сценарий развития международной обстановки после 2021 года.

objective, a resource and a means manifests itself as a device in the form of cyber influence, which is seen especially as a technical implementation of information warfare, a way of using information as a means to an end. Consequently, cyber warfare cannot be separated into its own field of information warfare. (See Akimenko & Giles 2020.) However, it is worth noting that, just like the information-psychological weapon, Russia also uses the information-technological weapon outside open conflicts.

One theme that has also emerged in the Finnish debate on information warfare is disinformation (Russian: дезинформация, dezinformatsiya), which is understood in a broader and more comprehensive way in the Russian debate compared to the West. According to Zaritsky and Chvarkov (2022), researchers from the General Staff of the Armed Forces of the Russian Federation, disinformation is the most important tactical, operational and strategic element of modern warfare, intended to misdirect the enemy's command, reduce its ability to make decisions, control the situation and monitor the overall state of affairs. According to them, disinformation is now understood as (1) a method of deliberately disseminating false (modified, distorted) information about objects, their structure and function, and (2) the imitation of actions based on this information, (3) protecting one's own objects containing critical information and misleading an opponent with the information so that the opponent will make decisions favourable to the party disseminating disinformation, and (4) information, material and documents containing information intended to mislead the target of influence (decision-makers, government and military officials, business leaders, etc.).

The basis of using disinformation is the repetition of unreliable and provocative information in various communication channels until the information space becomes saturated. Thus, Zaritsky and Chvarkov describe disinformation as a form of Russian strategic deception, maskirovka (Russian: маскировка, lit. masking, disguise).[5] According to the Russian Armed Forces Dictionary, disinformation is a form of masking, consisting of specific prepared information designed to create false impressions in the opponent's mind about the activities of real troops and objects, and to divert the opponent's intelligence activities to secondary and false targets. Disinformation is used by providing false, distorted or outdated information to an opponent's intelligence through existing or specifically created channels, including the media. (See Zaritsky and Chvarkov 2022.) The Russian Information Security Doctrine of 2000

[5] Maskirovka, or strategic deception, was already part of the strategic methods of the armed forces in the Soviet era.

defines strategic deception as part of Russia's information defence, in which the purpose of deception is "to develop means of strategic and operative deception, both counterintelligence and electronic countermeasures, together to improve the means of countering active operations of propaganda, information and psychological warfare".

The 2016 doctrine no longer contains this wording, but the centuries-old tradition of strategic deception has almost certainly not disappeared from the Russian repertoire.

6 CONCLUSIONS

The purpose of this report was to explore Russian information warfare terminology, and the meanings attached to the terms since 2014.

Russian information warfare terminology is a diverse and ever-evolving set of expressions used to describe, from a Russian perspective, aggression against Russia in the context of a struggle between superpowers. The Russian conceptual view of information warfare is based on ideological, historical, cultural and philosophical factors that are used to explain modern wars (Panarin 2006). There is also a difference in the perception of the timescale of information warfare, with Russia seeing information warfare as a struggle that has been going on for centuries and still continues. Therefore, countermeasures should also be based on long-term planning and anticipation rather than on a reactionary approach.

Most of the terms used in the Russian discourse are derived from Western debate, but there are also a number of original, rhetorically significant terms, such as information counter-struggle. The diversity of terms and a certain sense of ownership of terms, common in Western research, also characterises the Russian debate, with harmonisation efforts being made, especially as of spring 2022. With the exception of a few of the most common terms used to refer to information warfare, the terminology is used flexibly to describe a wide variety of information operations. What all these terms have in common, however, is the underlying Russian worldview, according to which the West is seen as making use of the information space to subjugate Russia in the struggle between the superpowers.

The loose definition and diversity of terms also provides leeway for strategies and tactics. As of spring 2022, a change in terminology can also be seen to reflect the situation that has arisen as a result of Russia's war against Ukraine. Many articles published on information warfare include the term "special military operation" in their keywords, and the premise of the research is almost always the information warfare activities of the United States against Russia. From 2022 onwards, however,

there can be seen a kind of extension of the power vertical into information warfare research, as political rhetoric enters the research publications. The transition of Russian society back to a totalitarian system resembling the Soviet era is also reflected in the call for an ideological system to guarantee information security (Yegorov et al. 2023).

Following Russia's large-scale and illegal attack on Ukraine, the Russian information space has become narrower and more one-sided: With the official canon of the causes, consequences and objectives of the war, the Russian political leadership has created a harmonised narrative where there is no room for truth. At the same time, Russia seeks to exploit the freedom of speech and expression in Western societies by creating and reinforcing dividing lines in them. In Russia, the world is seen as having entered an era in which information plays a central role, but truth has lost its importance. Thus, the narratives that have the greatest capacity to penetrate and saturate the information space become the "truth".

From the Finnish perspective, Russia's information warfare activities should be taken seriously and should be addressed jointly by the authorities, the civil society as well as the commercial and industrial sector. The seriousness of the issue should also be reflected in the terminology. Instead of information influence, there should also be a discussion in Finland about information warfare, or at least hostile state-run information influence. A change in terminology would also redirect our thinking to confront information warfare in a way that reflects its seriousness.

Literature

Primary sources

Bartosh, A. A. (2018). Стратегия и контрстратегия гибридной войны. Военная Мысль, № 10, 5–20.

Bartosh, A. A. (2022). Законы и принципы гибридной войны. Военная Мысль, № 10, 6–14.

Belokon, S. P. (2022). Информационные аспекты прогнозирования угроз военной безопасности Российской Федерации Information aspects of forecasting threats to the military security of the Russian Federation. Вестник Академии Военных Наук, № 4(81), 40–46.

Dylevsky, I. N., Zapivahin, V. O., Komov, S. A., Korotkov, S. V., & Krivchenko, A. A. (2016). О диалектике сдерживания и предотвращения военных конфликтов в информационную эру. Военная Мысль, № 7, 3–11.

Gerasimov, V. V. (2016). Организация обороны Российской федерации В условиях применения противником «традиционных» И «гибридных» методов ведения войны The Russian federation defense organization in the conditions of the enemy application the traditional and “hybrid” methods of the war fighting. Вестник Академии Военных Наук, № 2(55), 19–23.

Gryzlov, V. M., & Pertsev, A. B. (2015). Информационное противоборство. История и современность. Informational confrontation. History and modernity. Вестник Академии Военных Наук, № 2 (51) 2015(51), 124–128.

Ilnitsky, A. M. (2021). Ментальная война России. Военная Мысль, № 8, 19–33.

Yegorov, S. V., Zhdanov, M. A., & Lukashin, A. V. (2023). Роль идеологии в построении эффективной системы обеспечения информационной безопасности государства в современных условиях. Военная Мысль, № 9, 21–29.

Karavaev, I. N., & Sukhanov, P. V. (2022). Ментальная война как новый вид противоборства Mental war as a new kind of confrontation. Вестник Академии Военных Наук, № 2(79), 42–45.

Karpovich, O. G. (2022). Информационная война против России в условиях осуществления специальной военной операции Information war against Russia in the context of a special military operation. Вестник Академии Военных Наук, № 2(79), 10–13.

Kulakov, A. A. (2023). Задачи информационной политики Российской федерации в условиях «гибридной войны» с коллективным западом Russian federation information policy objectives In a “hybrid war” with the west.

Вестник Академии Военных Наук, № 1(82), 17–25.
Kuleshov, Yu. E., Zhutdiev, B. B., & Fedorov, D. A. (2014). Информационно-психологическое противоборство В современных условиях: теория и практика Information-psychological warfare in modern conditions: Theory and practice. Вестник Академии Военных Наук, № 1(46), 104–110.
Lata, V. F., Annenkov, V. A., & Moiseev, V. F. (2019). Информационное противборство: Система терминов и определений Informational countemeasures: Against the system of terms and definitions. Вестник Академии Военных Наук, № 2(67), 128–138.
Manoilo, A. V. (2022). Информационные диверсии в конфликте на Украине Information sabotage in the conflict in Ukraine. Вестник Академии Военных Наук, № 4 (81) 2022(81), 54–58.
Marichev, M. O., Lobanov, I. G., & Tarasov, E. A. (2021). Борьба за ментальность — тренд современной войны. Военная Мысль, № 8, 48–55.
Novikov, V. K., & Golubchikov, S. V. (2017). Анализ информационных войн за последние четверть века Analysis of information war in the last quarter of a century. Вестник Академии Военных Наук, № 3(60), 10–16.
Ovsyannikova, O. A. (2022). Противоборство в информационной войне (на примере украинского кризиса) Confrontation in the information war (on the example of the ukrainian crisis). Вестник Академии Военных Наук, № 2(79).
Sheremet, I. A. (2016). Противодействие информационным и кибернетическим угрозам Informational and cybernetic threats contradiction. Вестник Академии Военных Наук, № 2(55), 29–34.
Chekinov, S. G., & Bogdanov, S. A. (2015). Прогнозирование характера и содержания войн будущего: проблемы и суждения. Военная Мысль, № 10, 41– 49.
Chvarkov, S. V., & Lihonosov, A. G. (2017). Новый многовекторный характер угроз безопасности России, возросший удельный вес «мягкой силы» и невоенных способов противоборства на международной арене New polivectoral character of the Russia security threats, the increasing specific weight of the “soft force” And the ways of contradiction on the international arena. Вестник Академии Военных Наук, № 2(59), 27–30.
Zaritsky, V. N., & Chvarkov, S. V. (2022). Дезинформация и манипуляция в гибридных действиях. Disinformation and manipulation in hybrid actions. Вестник Академии Военных Наук, № 4(81), 76–84.

Russian documents

Doctrine of Information Security of the Russian Federation. Доктрина информационной безопасности Российской Федерации. Approved by Decree of the President No.
646. (2016). http://www.scrf.gov.ru/security/information/document5/
Doctrine of Information Security of the Russian Federation. Доктрина информационной безопасности Российской Федерации. Approved by Decree of the President No.
1895. (2000). https://base.garant.ru/182535/
National Security Strategy of the Russian Federation. Стратегии национальной безопасности Российской Федерации. Approved by Decree of the President No.
400. (2021). http://actual.pravo.gov.ru/content/content.html#pnum=0001202107030001
Military doctrine of the Russian Federation. Военная доктрина РФ. Approved by Decree of the President No. 146. (2010). http://kremlin.ru/supplement/461
Military doctrine of the Russian Federation. Военная доктрина РФ. Approved by Decree of the President No. 2976N. (2014). http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf
The Concept of the Foreign Policy of the Russian Federation. Концепция внешней политики Российской Федерации. Approved by Decree of the President No. 229. (2023).
https://mid.ru/ru/foreign_policy/official_documents/1860586/ The Concept of the Foreign Policy of the Russian Federation. Концепция внешней политики Российской Федерации. Approved by Decree of the President No. 640. (2016).
http://static.kremlin.ru/media/acts/files/0001201612010045.pdf

Other materials in Russian

Герасимов, V. V. «Ценность науки в предвидении». (2013). Военно-промышленный курьер.
https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html
Ильницкий, А.: «Ментальная война за будущее России». (2021). Еженедельник
«ЗВЕЗДА». https://zvezdaweekly.ru/news/20214211636-jxgHZ.html Керсновский, А. А. (1939). Философия войны.

Министерство обороны Российской Федерации, Военный энциклопедический словарь" Информационная война". Retrieved 7 May, 2024, from https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5211@morfDictionary

Министерство обороны Российской Федерации, Военный энциклопедический словарь Средства информационной борьбы («Информационное оружие»).

Retrieved 8 May, 2024, from https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14342@morfDictionary Панарин, И. Н. (2006). Информационная война и геополитика.

Подберезкин, А. И. (2015). Вероятный сценарий развития международной обстановки после 2021 года. Moscow State Institute of International Relations MGIMO, The Ministry of Foreign Affairs of the Russian Federation.

Research literature

Akimenko, V., & Giles, K. (2020). Russia's Cyber and Information Warfare. *Asia Policy*, *15*(2), 67–75. https://doi.org/10.1353/asp.2020.0014

Berzina, I. (2018). The Narrative of "Information Warfare against Russia" in Russian Academic Discourse. *Journal of Political Marketing*, *17*(2), 161–175. https://doi.org/10.1080/15377857.2018.1447762

Bērziņa, I. (2019). Weaponization of "Colour Revolutions". *Journal of Political Marketing*, *18*(4), 330–343. https://doi.org/10.1080/15377857.2019.1678905 Clark, M. (2020). *The Russian View of Future War: Unconventional, Diverse, and Rapid* (RUSSIAN HYBRID WARFARE, pp. 15–24). Institute for the Study of War. https://www.jstor.org/stable/resrep26547.5

Franke, U. (2015). *War by non-military means: understanding Russian information warfare*. https://dataspace.princeton.edu/handle/88435/dsp019c67wq22q

Giles, K. (2016). *Handbook of Russian information warfare*. NATO Defence College Research Division.

Giles, K. (2023). *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine*. Royal Institute of International Affairs. https://doi.org/10.55317/9781784135898

Joenniemi, P. (2008). Introduction by guest editor: Russia's narrative resources. *Journal of International Relations and Development*, *11*(2), 121–127. https://doi.org/10.1057/jird.2008.9

Kari, M. J. (2019). Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to

Cyber Threats. *JYU Dissertations*. https://jyx.jyu.fi/handle/123456789/65402

Kivimäki, V.-P. (2017). The cyber-enabled information struggle: Russia's approach and western vulnerabilities. *FIIA briefing paper*, *220*, 7.

Krieg, A. (2023). *Subversion: the strategic weaponization of narratives*. Georgetown University Press.

Pomerantsev, P., & Weiss, M. (2014). *The menace of unreality: how the Kremlin weaponizes information, culture and money*. https://dataspace.princeton.edu/handle/88435/dsp014m90dx90f

Puistola, J.-A., & Voinoff, S. (2023). Vakaus vastaan vaikuttaminen. Puolustusvoimien tutkimuslaitos, Tutkimuskatsaus 03–2023.

Puurunen, M. (2021). *Sotatieteiden akatemian roolista sotilasdoktriinien valmistelussa: uhkien perusteet*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 3: Työpapereita, nro 23. https://www.doria.fi/handle/10024/181639

Pynnöniemi, K. (2019). Information-psychological warfare in Russian security strategy. In *Routledge Handbook of Russian Security*. Routledge.

Pynnöniemi, K., & Jokela, M. (2020). Perceptions of hybrid war in Russia: means, targets and objectives identified in the Russian debate. *Cambridge Review of International Affairs*, *33*(6), 828–845. https://doi.org/10.1080/09557571.2020.1787949

Pynnöniemi, K., & Kari, M. J. (2016). Russia's New Information Security Doctrine: Guarding a besieged cyber fortress. *FIIA Comment*, *26*. https://www.fiia.fi/wp-content/uploads/2017/04/comment26_russia_s_new_information_security_doctrine.pdf

Pynnöniemi, K., & Mashiri, J. (2015). *Venäjän sotilasdoktriinit vertailussa: Nykyinen versio viritettiin kriisiajan taajuudelle*. The Finnish Institute of International Affairs.

Ristolainen, M. (2017). Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West. *Journal of information warfare*, *16*(4), 113–131.

Thomas, T. (2004). Russia's Reflexive Control Theory and the Military. *The Journal of Slavic Military Studies*, *17*(2), 237–256. https://doi.org/10.1080/13518040490450529

Thomas, T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies*, *27*(1), 101–130. https://doi.org/10.1080/13518046.2014.874845

Vasara, A. (2020). *Theory of reflexive control: origins, evolution and application in the framework of contemporary Russian military strategy*. National Defence University.

Appendices

Appendix 1 Key terms in Russian, transliterated and in English

Term in Russian	Transliteration	English translation
борьба за сознание	*borba za soznanie*	struggle for consciousness
война будущего	*voina budushchego*	future wars
гибридная война	*gibridnaya voina*	hybrid war; hybrid warfare
дезинформация	*dezinformatsiya*	disinformation
информатизация	*informatizatsiya*	informatisation
информационная безопасность	*informatsionnaya bezopasnost*	information security
информационная борьба	*informatsionnaya borba*	information struggle
информационная война	*informatsionnaya voina*	information war; information warfare
информационная операция	*informatsionnaya operatsiya*	information operation
информационная сфера	*informatsionnaya sfera*	information sphere; information space
информационное оружие	*informatsionnoe oruzhie*	information weapon
информационное пространство	*informatsionnoe prostranstvo*	information space
информационное противоборство	*informatsionnoe protivoborstvo*	information counter-struggle
информационное превосходство	*informatsionnoe prevoshodstvo*	information superiority
информационно-психологическое оружие	*informatsionno-psikhologicheskoye oruzhiye*	information-psychological weapon

информационно-психологическое противоборство	*informatsionno-psikhologicheskoye protivoborstvo*	information-psychological counter-struggle
информационно-техническое оружие	*informatsionno-tekhnicheskoye oruzhiye*	information-technical weapon
киберпространство	*kiberprostranstvo*	cyberspace
когнитивное оружие	*kognitivnoye oruzhiye*	cognitive weapon
маскировка	*maskirovka*	strategic diversion; lit. disguise
ментальная война	*mentalnaya voina*	mental war; mental warfare
мягкая сила	*myagkaya sila*	soft power
невоенные меры	*nevoennye mery*	non-military means
непрямые действия	*nepryamye deystviya*	indirect actions
новое поколение войны	*novoye pokoleniye voyny*	new generation wars
переформатирование сознания	*pereformatirovaniye soznaniya*	consciousness reformatting
психологическая война	*psikhologicheskaya voyna*	psychological war; psychological warfare
рефлексивное управление	*refleksivnoye upravleniye*	reflexive control
сетецентрическая война	*setetsentricheskaya voyna*	network-centric warfare
управляемый хаос	*upravlyayemyy khaos*	controlled chaos
цветная революция	*tsvetnaya revolyutsiya*	colour revolution

Russia sees information warfare as part of an ongoing struggle between the West and Russia that can only end in the ultimate annihilation of one side. In the Russian debate, the means of information warfare are seen as the most essential part of the wars of the future, in which military action is directed especially at the population of the target country. By influencing the populations of democratic states, Russia aims to sow the seeds of doubt and widen existing divisions in order to weaken internal cohesion within the states.

This report describes the terminology used in Russian information warfare over the last ten years. This period includes the annexation of Crimea, the war in eastern Ukraine and Russia's large-scale war of aggression against Ukraine. During this time, information warfare has become one of the most popular topics in military research in Russia.

This report is part of the results of the KILPI project at the University of Jyväskylä. KILPI is a development project for training and research in cognitive and information psychology security. The aim of the project is the comprehensive development of Finnish expertise in the field and the creation of opportunities for networking and pooling of expertise among actors in the field. The project is funded by the Ministry of Education and Culture.

ISSN 2737-0046
ISBN 978-952-86-0338-2

9 789528 602118

JYU Reports 49
University of Jyväskylä
2024