IRREGULAR WARFARE CENTER

INSIGHTS

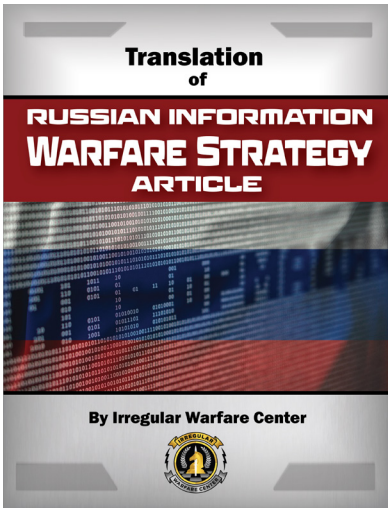
Vol. 1, No. 11, December 2023

Russian Information Warfare Strategy:

New IWC Translation Gives Insights into Vulnerabilities

This Irregular Warfare Center (IWC) Insights article introduces and builds upon the IWC's new translation of a Russian military article titled "Informational Support for National Security: Information Warfare Strategy." This article, originally published in the 2016 issue of the Russian academic journal *"National Security/nota bene,"* gives new insights into how Russian scholars and practitioners view information warfare. Written by one of Russia's *most prolific authors* on hybrid and information warfare and a member of Russia's Academy of Military Sciences, Alexander Bartosh, the article reveals the similarities of Russian information warfare strategy in 2016 and 2022 and certain narrative vulnerabilities in the Russian approach. The translation can be requested *here*.

EXECUTIVE SUMMARY: Recognizing and responding to Russian Operations in the Information Environment (OIE) requires understanding the strategic intent behind their information warfare strategy. First, this IWC Insights will begin by examining a past example of Russian OIE and how the West responded. Second, the article analyzes how the Western understanding of Russian information warfare strategy has evolved over time, as well as some misconceptions about it that have pervaded. Third, it analyzes some of the key concepts raised in a translated article from Russia on information warfare, and how they can be connected to ongoing events in Ukraine. Finally, it will briefly discuss some potential vulnerabilities in Russia's information warfare approach and how they can be taken advantage of to counter such strategies. As revealed in the translated article, Russia's information warfare capabilities are reactive to Western OIE approaches and, therefore, may be vulnerable to new Western initiatives.



IWC MISSION: The IWC serves as the central mechanism for developing the Department of Defense's (DOD) irregular warfare knowledge and advancing the Department's understanding of irregular warfare concepts and doctrine in collaboration with key allies and partners.

J.D. MADDOX
IWC Subject Matter Expert
Operations in the Information Environment

ANDREW LIFLYANDCHICK
IWC Russia Analyst

EXAMPLES OF RUSSIAN INFORMATION WARFARE AND INITIAL WESTERN RESPONSES

On 21 May 2016, two protest groups faced off in Houston near an Islamic cultural center to demonstrate competing opinions on Texas' future. Both groups, one which was protesting the perceived Islamization of Texas, and the other in support of the Islamic community, had been organized on Facebook pages. At first glance, this seemed like a normal and innocuous part of the U.S. political process. Unbeknownst to most participants, however, both Facebook pages had been created by Russian actors seeking to exacerbate political discord in the United States. This event was not an isolated case; it was a part of a coordinated effort by Russia to meddle in the U.S. elections, both in the social media space and in the physical domain.

Russia's aggressive use of Operations in the Information Environment (OIEs, also known as information operations) before, during, and after the U.S. election of 2016, as well as during the invasion of Crimea in 2014, brought the world's attention to the pivotal role that OIEs play in the new era of strategic competition. Empowered by the rapid development of social media and artificial intelligence, information warfare has evolved from a niche option that could only reach limited interest groups to a powerful asymmetric tool with the potential to impact society at all levels simultaneously. As a result of these events, analysts in many Western countries, including the United States, began recognizing the severity of this emerging threat. The general sentiment in the West at the time was that Russia had become the new master in the fields of hybrid and information warfare and that countries such as the United States had fallen behind. Research began into how foreign countries conduct OIEs and how these operations can be countered. For this purpose, the mission set of the U.S. Department of State's Global Engagement Center (GEC) was expanded from a primarily counterterrorism communications role to one aiming to, "recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests." Their subsequent research has resulted in numerous publicly available reports revealing the inner workings of Russian disinformation and propaganda networks.

However, the lack, in 2016, of preparation and understanding of information threats was not universal. The Baltic States, for example, having a long history of being a target of Russian influence efforts, were able to provide a much more rapid and robust response to Russian disinformation surrounding the invasion of Crimea in 2014. This included using pre-existing legal frameworks to quickly take down Russian broadcasts that spread disinformation, boosting existing government strategic communication structures, and tightening media rules and regulations. Perhaps most importantly, this response did not come solely from the government, but included industry, academics, media, and private citizens by creating collaborative networks, such as the volunteer cyber elves movement, which empowered regular civilians to contribute to the fight against foreign-led disinformation.

UNDERSTANDING RUSSIAN INFORMATION WARFARE STRATEGY

Although much progress has been made in understanding Russian OIEs on the tactical and operational levels, understanding Russian information warfare strategy as a whole has proven more challenging. Much of the modern understanding of Russian information operations can be traced to the popularization of the 2013 translated remarks by the Russian Chief of the General Staff, Valery Gerasimov. These remarks would become the basis of what is now known as the "Gerasimov Doctrine." These remarks have often been misinterpreted and mischaracterized, with one of the misconceptions being the notion that these ideas were in some way new and that they were representative of the entirety of the Russian literature on the subject. Unfortunately, the lack of general access in the West to alternative Russian sources on the subject, and the lack of a clearly defined information warfare doctrine

in Russia, has made these misconceptions difficult to correct. The information warfare strategy article recently translated by the IWC is one part of an extensive continuum of Russian and Soviet academic and military works on information warfare strategy. It offers a more in-depth look into Russian information warfare strategy than what can be found in the Gerasimov Doctrine, by not only offering a definition of information warfare and the end goals it seeks to achieve, but also conceptualizing how it fits in scenarios of hybrid warfare and color revolutions. When taken in the context of other Russian theoretical work on the subject, a much more nuanced picture can be seen.

To truly understand the Russian Way of Information Warfare, it is first necessary to address and overcome some key misunderstandings. First of all, as evidenced in the article translated by the IWC, Russia has long held the view that, when it comes to information warfare, it is constantly playing defense. Not only do Russian officials assume that they are the constant target of information attacks but, by 2016, having witnessed a series of liberal "color" revolutions across the world, they felt that Moscow was severely behind in its hybrid warfare strategy and capabilities. This is the primary argument underlying Gerasimov's 2013 article, which is not, as it is often seen, a framework for Russian hybrid warfare strategy, but rather an interpretation of perceived Western actions. In other words, the same fears of inadequate preparations that arose in the United States following the events of 2014 and 2016 were present in Russia for many years before that.

Second, neither Valery Gerasimov nor Russia were the first to understand the importance of hybrid warfare and the pivotal role that information operations play in it. Throughout the Cold War, Soviet practitioners had developed extensive experience and expertise in conducting disinformation campaigns targeted at foreign audiences. One such example was Operation Denver, later dubbed "Operation INFEKTION," a coordinated campaign in the 1980s between the KGB and their allied intelligence services to spread disinformation in the United States on the origins of the HIV/AIDS virus. By falsely claiming that the virus was a result of US government weapons research, and that it had been intentionally released to target select minority groups, Russian intelligence attempted to sow discord and distrust. Much of the groundwork that informs Russian hybrid and information warfare strategy today comes from leading Soviet and early post-Soviet theoreticians. As a result, these sources should be part of the conversation whenever this question is discussed.

Finally, despite Gerasimov's article being referred to as a "doctrine," it is by no means the type of universal, standardized doctrine that is familiar to U.S. and NATO practitioners. In fact, Russia's approach to information warfare in recent times has become increasingly decentralized. Throughout the Russo-Ukraine War, military bloggers have become a critical component of Russia's propaganda ecosystem. Due to the need to respond rapidly and adaptively to events on the ground, and to their pro-Ukrainian counterparts, these bloggers, even if they maintain government connections, do not always follow the Kremlin's directions or protocol. Some prominent bloggers have even been allowed to criticize failures of the Russian Armed Forces, something that seems unthinkable in a traditional top-down directed model. Of course, strict oversight remains in place, and if these comments cross the Kremlin's bottom line, then direct action is taken to remove such threats.

Likewise, future Russian foreign-targeted OIEs appear to be shifting toward proxy operations, including semi-independent and strategically-chosen influencers on social media, rather than using a directly-controlled team of professionals, as was the case in 2016 with Yevgeny Prigozhin's "troll factory" that worked to interfere in the U.S. elections. A recent report by the Latvia-based NATO Strategic Communications Centre of Excellence chose the term "strategy without design" as a way to describe Russia's approach to information warfare. While this indirect approach has notable advantages, such as an increase in responsiveness, it also opens up the Russian propaganda ecosystem to external influence and manipulation. The report discovered that while bloggers commonly copied the official narratives

of the Kremlin, sometimes the opposite was true—narratives proposed by the bloggers would later be adopted officially as the government's position. While, previously, the thought of influencing Russian leadership and society seemed an uphill battle, this decentralization of information may provide opportunities for those seeking to manipulate narratives inside Russia.

INSIGHTS OFFERED BY THE TRANSLATION

Yet, despite the Kremlin not always providing a clear step-by-step strategic plan, this does not mean that there is no strategic intent behind Russia's information warfare. It is important to understand that Russia views hybrid warfare, and by extension information warfare, as an all-out war with the survival of the nation at stake. Take, for example, the definition of information warfare offered in the article translated by the IWC:

"...information warfare is a set of methods, through a coordinated concept and plan, to influence all segments of an enemy's population and government in order to distort their worldview, to weaken and destroy the foundations of their national identity and way of life, with the goal of disrupting their ability to resist aggression."

Compared to Gerasimov's vision, which was only a broad outline, this definition is much more explicit and aggressive in its description of what, in the opinion of the author, the end goal of information warfare should be. While such goals should be rightfully seen as anathema to Western values, countering the threat of Russian OIEs requires fully recognizing that their understanding of the topic is fundamentally different. To address this threat, special preparations are needed. An effective defense must also include taking advantage of existing Russian vulnerabilities, albeit for different reasons than those proposed in their definition of OIEs.

In the translated article written by Alexander Bartosh, one of Russia's most prolific authors on hybrid and information warfare and a member of Russia's Academy of Military Sciences, he argues that two classic conventional warfare strategies, attrition and annihilation, can also be applied to information warfare. While this dual categorization of warfare strategy is perhaps outdated, Bartosh's framework, when applied to Russian information warfare before and after its invasions of Ukraine, can give interesting insights into the strategic intent behind Russia's actions.

RUSSIAN APPLICATION OF AN INFORMATION WARFARE STRATEGY OF ATTRITION

The information warfare strategy of attrition, as described by Bartosh, is a series of gradual OIEs and influence campaigns targeted at national leaders, the populace, and servicemembers, with the goal of distorting and eventually replacing a country's national values and priorities. This long-term strategy, which in Bartosh's opinion is ideal in a hybrid war scenario, is quite similar to that employed by Russia in 2014 to prepare the information environment in Crimea and Eastern Donbass for a quick and relatively smooth invasion.

A similar setup was attempted before the Russian invasion of Ukraine in 2022. For many years prior to the invasion, Kremlin officials and media sources had been gradually pushing the narrative that Russians and Ukrainians were a single people, and that the state based in Kiev did not have the right to exist. In his now infamous 2021 speech, "On the Historical Unity of Russians and Ukrainians," Russian President Vladimir Putin made Russia's position on Ukrainian sovereignty abundantly clear. Using a skewed interpretation of history, Putin sought to distort the worldview of not only domestic audiences by providing a potential future justification for aggression, but also international and especially Ukrainian audiences, by attempting to convince them to support Russia's worldview and policies. Introducing these narratives and making them easily recognizable to the target audiences was a

process that took time. The theories and arguments for a unified "*Russkiy Mir*" (Russian World) and a "*Novorossiya*" (New Russia) had been popularized over the course of decades. For example, the Russkiy Mir Foundation, established in 2007 and ostensibly a network of Russian culture and language centers, became a vehicle for the targeting of ethnic Russian diaspora in countries such as Ukraine. The goal was to then use these communities as a vector to influence their society and leadership. This strategy of using Russian ethnic minorities as a driver for information and influence operations bore fruit during the invasion of Crimea in 2014, but this was in part due to a lack of understanding of OIE strategy and countermeasures on the part of the Ukrainian government, and in part due to the irregular nature of the invasion itself. In 2022, however, these tactics turned out to not be sufficient, as the Ukrainian populace demonstrated a strong willingness to resist the invaders. As a result, this has forced Russia to adopt the second, shorter-term strategy of information warfare described by Bartosh: one geared towards annihilation.

RUSSIAN APPLICATION OF AN INFORMATION WARFARE STRATEGY OF ANNIHILATION

In classical military understanding, a strategy of annihilation involves taking direct action to defeat an enemy and permanently prevent their resurgence. In the information environment, according to Bartosh, this means seizing full control of a target's information networks and infrastructure through the use of coordinated information, psychological, and cyber operations (in Russia, both cyber and psychological operations are considered as part of information warfare). This then clears the path for what Bartosh describes as "overthrowing the government and transferring the country under external control," something that the Kremlin fears the West will attempt in Russia.

Russia has attempted to employ these tactics during previous invasions. Notably, cyber attacks were conducted during the Russo-Georgian War of 2008. Timed in tandem with conventional military operations, these attacks temporarily knocked out a large number of key government, news, and private sector websites, which severely hindered the ability of the Georgian government to communicate with the public. Likewise, Russia has done its utmost to exert control over information infrastructure in Ukraine. In occupied areas, Moscow has shut down previous internet service providers and replaced them with networks that route all data through Russian servers, thus allowing tight control and censorship over the information that Ukrainian citizens can access. The fight for control over information and communication infrastructure in Ukraine became a top priority for both sides. The Ukrainian government turned to the private sector and requested the company SpaceX to give both military personnel and civilians in the country access to the company's network of Starlink satellites. These satellites have been used during the war to provide a significantly more secure option, both for civilians and the military, to communicate information. However, this introduces its own security issues, as it allows external actors to hold some level of influence over military decision-making. This was demonstrated by the company's decision to refuse an emergency request to support a Ukrainian drone attack, thus effectively forestalling the operation.

Yet, even if Russia had been successful in achieving full control of the information space in Ukraine, this does not answer the question of how Russia would attempt to achieve the second aspect of a strategy of annihilation: permanently "disrupting their ability to resist aggression." As the aforementioned definition proposed by Bartosh reveals, one possible method of achieving this is to "weaken and destroy the foundations of their national identity and way of life." In the misguided calculations of the Kremlin, if Ukrainians were to begin seeing themselves as Russians, their willingness to resist would decrease. This explains some of the Russian activities in the occupied territories of Ukraine. These have included attempts to erase the usage of the Ukrainian language, destruction of religious and cultural sites, and the indoctrination of schoolchildren in occupied territories.

COUNTERING RUSSIAN INFORMATION WARFARE STRATEGY

The more we learn about Russian information operations, the more vulnerable they appear to be. As the fight in Ukraine has demonstrated, Russia's previously perceived superiority in information warfare can be undermined, and in some cases overcome, by a country with significantly less resources and OIE capabilities. An expert understanding of the country and the proactive targeting of narrative vulnerabilities can provide an effective defense against information and influence operations. For too many years, the U.S. has approached IO from a reactive and defensive viewpoint. While the West should by no means engage in OIEs with the same destructive intentions as Russia does, that does not mean that there are no strategic vulnerabilities in their approach that can be exploited. While designing new strategies to counter Russian OIEs, the following must be kept in mind:

- **Avoiding Biases**—An accurate understanding of how malign actors view information warfare is critical to the development of countermeasures. During this process, it is important to avoid mirror imaging, and recognize that not all countries approach and define the information environment in the same way.
- **Identifying Structural Weaknesses**—Bartosh implies that even Russian IO analysts, as well as practitioners, may lack a clear understanding of "the national values and interests of our state and on their scientifically established hierarchy and priority levels." This, along with the NATO Strategic Communications Center report, suggests that Russia's command and control system for information might be more vulnerable than previously thought.
- **Creating an Adaptive Response Structure**—Information warfare in an age of social media requires quick and adaptive responses to events on the ground. Russia has found that, against an active opponent, a government bureaucracy with a long chain of command is not capable of winning an information war alone. Any response should include not only a whole-of-government approach, but also industry, civil society, academic institutions, allies, and partners.
- **The Role of Cultural Institutions**—Cultural institutions, whether willing or not, cannot avoid being drawn into competition over information when it targets society at all levels. While understandably prioritizing their own security first, these institutions can also, when they choose, proactively become a part of shaping narratives and countering disinformation. This topic will be examined in more depth in a future IWC Insights article.
- **Targeting Narrative Vulnerabilities**—While recent polls seem to indicate that the majority of Russians still support continuing the War in Ukraine, there is a significant diversity in opinion on the topic in Russia. Many factions disagree on the direction the war should take, and many others only support it due to fear of reprisals. The divisions being exacerbated by the war create narrative vulnerabilities in the Russian information environment that may have not existed beforehand.

In conclusion, there are many potential lessons and opportunities that can be gleaned through direct examination of new Russian sources, such as the article translated by the IWC. These ideas should become the basis of further discussion on Russian narrative vulnerabilities and how they can be used to counter Russian information warfare strategy. While Russian sources often refer to all of Russia's OIE as defensive in nature, this does not mean that they do not expose the logic and intent behind the Kremlin's proactive use of OIE and influence campaigns abroad. After all, when it comes to the Russian Way of Information Warfare, the best defense is a good offense.

The views expressed are those of the author(s) and do not necessarily reflect the official position of the Department of Defense, Defense Security Cooperation Agency, or the Irregular Warfare Center.