

SOCIAL AND POLITICAL PHILOSOPHY



UDC 101.1 : 316 : 355.01

Original Theoretical Research

<https://doi.org/10.23947/2414-1143-2026-12-2-18-23>



Information Warfare in Modern Conflicts

Ivan Yu. Partyshev

Institute of Service and Entrepreneurship (Branch) of Don State Technical University,
Shakhty, Russian Federation

✉ ivanpartysev@gmail.com

Abstract

Introduction. The use of information as a tool of influence has ancient roots. The information wars of the first half of the 20th century served as a kind of prelude to the emergence of modern information wars. The destructive impact of information wars on both the collective public consciousness and the individual can be more significant than that of open armed conflicts. The purpose of this article is to analyze the modern information confrontation waged by adversaries, as well as to identify its specific characteristics and tools.

Materials and Methods. The theoretical and methodological foundation of this study is a set of general scientific and socio-philosophical methods. The methods employed include analysis and synthesis, the dialectical method, comparative and systemic analysis, and the historical-genetic approach.

Results. Modern information warfare arises in the context of a developed information space, since it is precisely within this space that the consciousness of the masses is shaped, emotional states are influenced, and the ideological framework for further aggressive actions is established. Information pressure in modern warfare includes the internalization of certain behavioral patterns into the mass consciousness, as well as the manipulation of information processes, information management systems, and enemy information.

Discussion and Conclusion. First-generation methods of information warfare were aimed at undermining the stability of an adversary's command-and-control systems, while second-generation methods are aimed at manipulating public opinion. Third-generation methods focus on the use of information networks. There are four main areas of research in information countermeasures: psychological, normative, conflict studies, and technological.

Keywords: information, information warfare, hybrid warfare, information confrontation

For Citation. Partyshev I.Yu. Information Warfare in Modern Conflicts. *Science Almanac of Black Sea Region Countries*. 2026;12(2):18–23. <https://doi.org/10.23947/2414-1143-2026-12-2-18-23>

Оригинальное теоретическое исследование

Информационное противостояние в современных войнах

И.Ю. Паргышев

Институт сферы обслуживания и предпринимательства (филиал) Донского государственного технического университета,
г. Шахты, Российская Федерация

✉ ivanpartysev@gmail.com

Аннотация

Введение. Использование информации в качестве инструмента воздействия имеет древние корни. Информационные войны первой половины XX в. являлись своеобразным прологом к возникновению современных информационных войн. Разрушительное воздействие, наносимое информационными войнами как массовому общественному сознанию, так и человеку в отдельности, могут быть значительнее, чем открытые вооруженные столкновения. Цель статьи – анализ современного информационного противостояния, осуществляемого антагонистами, а также выявления его специфики и инструментария.

Материалы и методы. Теоретической и методологической основой исследования является комплекс общенаучных и социально-философских методов. Применяются методы анализа и синтеза, диалектический метод, сравнительный и системный анализ, историко-генетический подход.

Результаты исследования. Современная информационная война возникает в условиях развитого информационного пространства, поскольку именно в нем формируется сознание масс населения, настраивается эмоциональное состояние, создается смысловая нагрузка дальнейших агрессивных действий. К информационному давлению в современной войне относится интериоризация в массовое сознание определенных паттернов поведения, а также воздействия на информационные процессы, информационно-управляющие системы, информацию противника.

Обсуждение и заключение. Средства первого поколения ведения информационной войны были направлены на уменьшение стабильности систем управления соперника, средства второго поколения направлены на манипулирование сознанием масс. Средства третьего поколения актуализируют использование информационных сетей. Существуют четыре основные направления исследования информационного противодействия: психологическое, нормативистское, конфликтологическое и технологическое.

Ключевые слова: информация, информационная война, гибридная война, информационное противостояние

Для цитирования. Партышев И.Ю. Информационное противостояние в современных войнах. *Научный альманах стран Причерноморья*. 2026;12(2):18–23. <https://doi.org/10.23947/2414-1143-2026-12-2-18-23>

Introduction. Every war begins with an information campaign. Every war continues with ongoing information support. Every war comes to an end, yet the victory reports continue to be broadcast for a long time afterward. War and information are always intertwined. This inseparable link between war and information is undeniable, even in the context of modern warfare. The goal of information warfare is to impose on the enemy a narrative that presents the situation in a favorable light. It is quite evident that the topic of information warfare is currently an extremely sensitive one for Russian society. Information warfare always affects the entire society, and in the case of the special military operation, this information war is still far from over.

The use of information as a tool of influence has ancient roots, and the practice of waging information warfare stretches back deep into history, hundreds and thousands of years ago. The most famous treatise on the “fog of war” is “The Art of War”, written two and a half thousand years ago by the Chinese military commander and strategist Sun Tzu [1]. The Trojan War, dating to the 13th century BC, can also be cited as an illustration. Another historical precedent demonstrates the tactics employed by Genghis Khan’s armies in the 13th century AD. To demoralize the enemy and persuade cities to surrender, the Mongol conquerors actively spread terrifying rumors of the total annihilation of the population if they refused to surrender. Such a psychological attack significantly reduced resistance and accelerated the process of territorial conquest, underscoring the importance of information warfare on the outcome of military campaigns

But it was in the 20th century that information warfare between adversaries grew exponentially. First, World War I demonstrated the unique potential of information to influence one another [2]. The opposing coalitions (both the Franco-Anglo-Russian and the Austro-German-Italian) employed the means and methods of information warfare in the form of “jingoism,” social and religious demagoguery, portraying their participation in military conflicts as a forced, purely defensive action. At the same time, despite the widespread use of propaganda, disinformation, and the printing of millions of leaflets, the official authorities were primarily concerned with anti-government sentiment within the troops (this applies to both Germany and the Russian Empire).

World War II demonstrated to the world the unprecedented nature of the information pressure exerted by opposing sides on one another, as well as the internal information pressure on the population. General Charles de Gaulle wrote the following about this period in his memoirs, “France at War”: “We are about to face a powerful enemy... We face difficulties of a moral and material nature... We will have to contend with a host of objections, accusations, and slanderous claims...” [3, p. 230]. The constant psychological manipulation of the population in the Third Reich yielded negative results – according to the memoirs of Soviet aircraft designer A.S. Yakovlev regarding his stay in prewar Germany, all the Germans he met, regardless of social status, exuded a sense of “immeasurable superiority” over representatives of other nations. A state of social schizophrenia and constant paranoia became commonplace in Nazi Germany. Any form of critical reflection or attempt to rationally comprehend reality was suppressed by the repressive apparatus. In 1927, Harold Lasswell, analyzing the prevailing situation, asserted the primacy of propaganda in influencing people during wartime [4]; he emphasized that its use entails the systematic dissemination of certain ideas, doctrines, or information with the aim of shaping public opinion or manipulating the actions of individuals or groups.

Overall, this brief historical overview shows us that the information warfare of the first half of the 20th century, in the context of the world wars, was one of the components of ideological confrontation and, by employing various technologies of information influence to achieve its primary objective, served as a kind of precursor to the emergence of modern information warfare.

In discussing the intensification of information wars in the 21st century, it should be noted that the information society serves as the primary environment for their emergence and development. Indeed, the information society, as a new type of society, gives rise to new forms of conflict: information wars. Since the second half of the 20th century, information has become a powerful, tangible resource that is even more valuable than natural, financial, labor, and other resources. Information has become a commodity that is bought and sold. Information has turned into a weapon; information wars arise and end. Theorists of the information society concept have actively discussed this, in this context, it is necessary to highlight the work of Canadian professor Marshall McLuhan, who argued that under the influence of electronic mass media, the world is transforming from a “global village” into a “global theater,” where everyone plays roles assigned to them by the structures of audiovisual teleculture. Moreover, according to M. McLuhan, these structures can be regarded as universal laws of existence and consciousness that regulate the lifestyle, activities, and thinking of people living in different countries but in the same historical eras [5, p. 199]. And it was M. McLuhan who was among the first to apply the concept of “information warfare,” proposing the innovative thesis: “true total war is war by means of information.” He demonstrated that modern military conflicts are primarily waged in the information sphere.

In traditional warfare, psychological warfare (as the experience of the two world wars has shown) merely accompanies military operations, providing motivation to fight and justifying the necessity of war. In modern wars, however, psychological confrontation takes on a dominant role. This involves a significant shift in the focus of confrontation and conflict from its physically intense component to the psychological and informational, to processes in the realm of consciousness and human emotions.

In modern warfare, the information component plays a leading role. At its core, the information conflict is an integral part of the ideological struggle. A distinctive feature of this conflict (often referred to in academic literature, as well as in popular and political discourse, as “information warfare”) is that it does not directly lead to bloodshed, destruction, and the like. However, the damage inflicted by information wars on both the individual psyche and the collective public consciousness is, in terms of scale and significance, fully comparable to that of armed conflicts, and at times even exceeds their consequences.

The purpose of this article is to analyze the contemporary information warfare waged by adversaries in the context of modern warfare, as well as to identify its specific characteristics and tools.

Materials and Methods. The theoretical and methodological foundation of this study is a set of general scientific and socio-philosophical methods, as well as the achievements of global and domestic scholarship in this field. Methods of analysis and synthesis were applied at all stages of the research, as they ensured the internal consistency of the whole and its parts.

In our study of information conflicts, we employed a dialectical method that allows us to analyze information wars as they unfold, driven by internal contradictions. Systematic and comparative analysis made it possible to identify patterns in the unfolding of modern information confrontation, as well as the interrelationship and ambivalence of the processes occurring in society that predetermine the development of information wars.

The structural-functional approach has made it possible to identify patterns of information warfare by focusing on the interconnection between information security and modern information warfare. The historical-genetic approach has made it possible to identify the essence of the phenomenon of information warfare from a historical perspective.

Results. A distinctive feature of modern warfare is that it is waged in a globalized world, where the world has been brought closer together by intensive communication, and the increasingly close nature of interactions between nations also contributes to the growth of conflicts between them. Russian scholars I.V. Goncharova, V.F. Nicevich, O.A. Sudorgin note that “the causes of the transition to a new type of warfare were the collapse of the bipolar world, the growing threat of international terrorism, and the erosion of ethnocultural identity within the United States itself and a number of countries following in the wake of its policies” [6, p. 20]. It is difficult to disagree with this view, since the unfolding of modern information conflicts takes place amid social turbulence, constant social and political transformation, and the metamorphosis of cyberspace, which serves as a key arena for information conflict.

Modern information warfare arises as a result of the exponential development of the information space. Therefore, a number of contemporary scholars (S.I. Samygin, A.M. Rudenko, V.V. Kotlyarova) emphasize that “at present, information-psychological wars are becoming the foundation of all other wars, preceding them or proceeding in parallel, determining the success or failure of their outcome” [7, p. 49]. Without social media, outside the global communication space, modern

information warfare would be meaningless, since it is precisely within this space that the consciousness of the masses is shaped, emotional states are set, and the semantic context for further aggressive actions is created.

In today's world, information technology is an integral part of warfare, notes I.N. Panarin. Information warfare is a key component of the modern globalization process, and without an understanding of its nature, it is impossible to fully assess the consequences of globalization pressures [8, p. 18]. I.N. Panarin identifies the main areas of information pressure, which scholars have identified as the political and financial-economic spheres, the innovative development of the economy and society, as well as the diplomatic and military spheres. It is quite possible that virtually all spheres of society are affected by information warfare, and the advantage lies with those who are informationally powerful, due to the availability of new technologies, creativity, technical means, and speed of response.

Modern information technology not only provides access to information relevant to the recipient but also offers opportunities for interactive communication, including with those who disseminate that information. This makes it possible to adjust the information based on the socio-psychological reaction it elicits. The interactive nature of information exchange is most clearly evident in the functioning of social media, which often contributes to the growth of terrorist threats (cyberterrorism), mass hysteria, xenophobia, and other negative social phenomena.

One of the key features of the information society is "network logic", which explains the concept of the "network society" [9, pp. 42–43]. Networks connect people, institutions, and even entire states through numerous links. They form the foundation of the global network society, as they permeate the entire social and economic structure. In conducting a philosophical analysis of the problem of cyberterrorism in social networks within the context of modern hybrid threats, representatives of the Rostov philosophical school (E.E. Nesmeyanov, A.M. Rudenko, and V.V. Kotlyarova) emphasize that "information, by exerting a regulatory influence on human behavior through the formation of worldview attitudes, can distort true goals, interests, and needs" [10]. Modern technologies have the ability to influence information; modern technologies are characterized by the effect of "ubiquitous influence"; all systems that use information technologies are subject to "network logic," which allows them to influence a multitude of processes and organizations.

Dorothy Denning, an expert at the U.S. Center for the Study of Terrorism, believes that information warfare is primarily directed at technical resources [11]. According to D. Denning, the internet is now considered a powerful lever of informational pressure for altering the domestic and foreign policy courses of any state, and she identifies three types of activity in this regard: social activism, hacktivism, and cyberterrorism. The scholar derives her typology of information wars, classifying them as defensive and offensive, each of which has its own mechanisms, technologies, methods of conduct, and so on. Thus, defensive information warfare is characterized by the presence of a series of filters located along the "lines of attack," while offensive information warfare is characterized by the presence of these very "lines of attack."

The following two fairly broad categories of measures can be attributed to information pressure in modern warfare:

- influencing military personnel and the civilian population with the aim of instilling certain behavioral patterns in the collective consciousness;
- opportunities for technical and technological influence on information and control systems and on the information transmitted by the enemy, regardless of the means employed.

Modern warfare has a number of fundamental characteristics: the formation of a vast socio-informational and cultural space as a powerful mechanism for shaping reality (what is presented in a certain way is considered real, while true facts are rejected or ignored; a peculiar construction of an illusory pseudo-reality); the contradictory stance of state structures and/or their inability to recognize the scale of real threats; the absence of a reliable and effective international security system; the ability to frame information warfare as a conflict between value-based models of order and to influence the understanding of the current state of the world as a shift in paradigms of strategic thinking.

The "information noise" accompanying military operations, whether through suppression, the creation of deliberately contradictory interpretations, or simply a cover-up, significantly hinders the formation of a clear perspective on military events. A prime example of such information pressure is the bombing of the RTS television center in 1999. [12]. At that time, a representative of the North Atlantic Alliance announced that they had struck the "brain" of President Slobodan Milošević's military apparatus, despite the fact that sixteen employees of the television center had been killed. In modern information warfare during the conduct of special military operations, as T.N. Rastorgueva notes, "The methods used by Russia's geopolitical opponents on the Maidan are effective precisely because they are based on a deep understanding of human nature and sensory perception" [13, p. 60]. It should be noted that in modern information warfare, the initiative for offensive information influence tactics is taken by the opponents of the Russian Federation. Consequently, a critically important aspect in this regard is the improvement of information security policy.

Discussion and Conclusion. In today’s world, as the role of information and the means of transmitting it in people’s lives continues to grow, so too does the number of methods and techniques used to wage information warfare. The evolution of such methods points to a gradual shift in the generations of information warfare tools. First-generation tools were aimed at undermining the stability of the adversary’s command and control systems, while second-generation tools are aimed at manipulating public opinion. In recent years, third-generation information warfare tools have become widespread, characterized by the effect of “rapid decisive actions.” It is precisely among these third-generation information warfare tools that cyber warfare is on the rise.

The current stage of research into information warfare is characterized by a reevaluation of existing concepts, a search for new ones, and the development of innovative methodological approaches. In total, four established approaches can be identified. The normative school of thought, one of the earliest methodological approaches in American scholarship on the conduct of information warfare, interprets information warfare specifically as an information confrontation between antagonistic parties in the context of armed conflict.

The second approach is the psychological approach, according to whose methodological framework information warfare is defined as a comprehensive, open, or targeted, implicit informational influence exerted by opposing sides, encompassing a system of forms, means, and methods of influencing adversaries.

The third school of thought is the conflict studies approach, whose proponents view information warfare through the lens of military and political confrontation. Representatives of the fourth, technological, school have focused their research on a meticulous examination of the technical component, as they believe that in information warfare, the enemy’s technical capabilities will become the primary arena of engagement and the key target.

The foregoing leads to the conclusion that it is necessary to modernize information security policy, which serves as a fundamental factor capable of effectively countering the challenges of information influence.

References

1. Sun Tzu. *The Art of War*. Translated from the English by M. Mikhailova. Moscow: AST Publishing House; 2024. 256 p. (In Russ.)
2. Duz S. Information warfare became the “main weapon” of that First World War. *Zvezda Weekly*. January 12, 2019. (In Russ.) URL: <https://zvezdaweekly.ru/news/2019191119-W7bIY.html/> (accessed: 06.10.2025).
3. *World War II as Recalled by W. Churchill, S. de Gaulle, C. Hull, W. Legu, and D. Eisenhower*. Edited by E.Y. Troyanovskaya. Moscow: Politizdat; 1990. 558 p. (In Russ.)
4. Lasswell H.D. *Propaganda technique in World War I*. Translated from the English by V.G. Nikolaev. Moscow: INION RAS; 2021. 236 p. (In Russ.)
5. McLuhan M. *Understanding media: the extensions of man*. Translated from the English by V.G. Nikolaev. Moscow: KANON-Press-C; Zhukovsky: Kuchkovo Pole; 2003. 464 p. (In Russ.)
6. Goncharova I.V., Nicevich V.F., Sudorgin O.A. Information Warfare as a Tool of Political Confrontation in the Modern Multipolar World. *RUDN Journal of Public Administration*. 2024;11(1):19–31. (In Russ.) <https://doi.org/10.22363/2312-8313-2024-11-1-19-31>
7. Samygin S.I., Rudenko A.M., Kotlyarova V.V. Historical and Philosophical Understanding of the Problem of Information Security. *Society and Power*. 2016;58(2):47–51. (In Russ.)
8. Panarin I.N. *Information Warfare, PR, and World Politics*. Москва: Moscow: Goryachaya Linia-Telecom; 2006. 352 p. (In Russ.)
9. Castells M. *Communication power*. Translated from the English by N.M. Tylevich and A.A. Arkhipova. Second edition, revised. Moscow: Higher School of Economics Publishing House; 2017. 590 p. (In Russ.)
10. Nesmeyanov E.E., Rudenko A.M., Kotlyarova V.V. Sociocultural analysis of cyberterrorism in social nets within the problems of information safety of Russian society. *Science Almanac of Black Sea Region Countries*. 2015;(4):1–5. (In Russ.)
11. Denning D. E. Stuxnet: What Has Changed? *Future Internet*. 2012;3(4):672–687. <https://doi.org/10.3390/fi4030672>
12. Pechurov S.L. “Allied force” of the aggressor: features of the military action against Yugoslavia in 1999. *Military Historical Journal*. 2009;3:15–19. (In Russ.)
13. Rastorgueva T.N. Information Warfare as a Mechanism of Societal Destabilization: Analysis of Manipulative Technologies Through the Prism of Emotional and Semantic Perception. *Theories and Problems of Political Studies*. 2025;14(1A):52–64. (In Russ.)

About the Author:

Partyshev Ivan Yurevich, postgraduate student, Institute of Service and Entrepreneurship (Branch) of Don State Technical University (147, Shevchenko St., Shakhty, 346500, Russian Federation), [ORCID](#), [SPIN-code](#), ivanpartysev@gmail.com

Conflict of Interest Statement: the author declares no conflict of interest.

The author has read and approved the final version of manuscript.

Об авторе:

Партышев Иван Юрьевич, аспирант, Институт сферы обслуживания и предпринимательства (филиал) Донского государственного технического университета (Российская Федерация, 346500, г. Шахты, ул. Шевченко 147), [ORCID](#), [SPIN-код](#), ivanpartysev@gmail.com

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

Автор прочитал и одобрил окончательный вариант рукописи.

Received / Поступила в редакцию 16.01.2026

Reviewed / Поступила после рецензирования 30.01.2026

Accepted / Принята к публикации 02.02.2026