„Defence and Science“ № 4 (2025)
www.defenseandscience.eta.edu.ge

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

SPECIFIC FEATURES OF INNOVATIVE TECHNOLOGICAL SUPPORT IN MODERN WARFARE

Kakha Phutkaradze[1]
https://orcid.org/0000-0001-9222-0673
Petre Gelashvili[2]
https://orcid.org/0009-0005-1558-0321
doi.org/10.61446/ds.4.2025.10474

Article History:
Received 07 September 2025
Accepted 14 October 2025
Published 25 December 2025

ABSTRACT

The article examines technological and informational innovations in modern warfare as factors exerting an increasingly significant influence on national security. It analyzes military and strategic concepts based on network integration, digital intelligence systems, and forms of information-psychological influence. The study compares the practical implementation of technological warfare models by the United States and NATO, as well as by Russia and China. Particular attention is devoted to the role of information-psychological operations (PSYOPS), which, together with next-generation technological tools, determine the structure and dynamics of the modern battlefield. In the context of Georgia, the significance of this topic lies in the fact that national security effectiveness depends not only on military potential but also on the protection of cyberspace, data management systems, and the strengthening of informational resilience. The conclusion emphasizes that the integration of technological innovations into the defense system requires strategic vision, digital transformation, and enhanced international cooperation.

Keywords: Innovative technologies, National security, Network-centric operations, Cybersecurity, Hybrid warfare, Information-psychological influence.

[1] Associate Professor of Bachelor's Program in Defense and Security of LEPL David Aghmashenebeli National Defence Academy of Georgia, Doctor of Social Science,
[2] Assistant Professor of Bachelor's Program in Defense and Security of, LEPL David Aghmashenebeli National Defence Academy of Georgia, PhD in International Relations

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

INTRODUCTION

Modern military conflicts are increasingly based on technological and informational innovations that are transforming the nature and structure of warfare. As the battlefield evolves, the role of physical force is diminishing, while the possession of information, speed, and precise analysis is becoming a decisive advantage.

In this reality, technological support for warfare has become the principal determinant of a national security system. Its purpose is not only the modernization of armaments, but also the strategic, operational, and tactical integration of all levels of combat into a unified digital system.

The “Network-Centric Warfare” (NCW) model, formulated by the U.S. Department of Defense in the 1990s, represents the foundation of this philosophy. It is based on the idea that the rapid and accurate exchange of information creates a shared picture of the battlefield, reduces decision-making time, and increases overall effectiveness.[3]

For Georgia, such an approach is critically important, as the country’s primary security challenges are directly linked to the protection of the informational domain, the prevention of cyberattacks, and the optimization of technological resources

In this context, it is relevant to analyze the historical-theoretical foundations and intellectual roots of the aforementioned direction, as well as to examine its economic-technological parallels, technological and operational aspects, international experience, philosophical-strategic interpretations, and the challenges and perspectives facing Georgia.

At the same time, attention must be paid to the strategies, tactics, and unique methods employed in recent years by various states in the field of military and information-psychological confrontation.

MAIN PART

Given the current stage of human history and the existing architecture of global geopolitics, it is natural that the analysis of the key issues of this research should focus on

[3] Alberts, D. S., Garstka, J. J., & Stein, F. P. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

three states—the United States, Russia, and China—along with the North Atlantic Alliance (NATO), as the actors possessing the greatest traditions and potential in Network-Centric Warfare (NCW), and on Georgia, which has been both one of the victims of confrontation conducted through this method (the final stage of the USSR, culminating in the August 2008 war and continuing to the present day) and a prospective target.

The Russian military theorist Yevgeny Messner wrote as early as 1959 that “modern war encompasses the entire society, where the boundary between soldiers and the population disappears.” This observation represents a kind of prediction of the contemporary network-centric model, in which the battlefield is no longer confined to the front line but extends into the social, economic, and informational domains.[4]

“In the 1980s, Marshal Nikolai Ogarkov developed the idea of a ‘military-technical revolution,’ which emphasized the role of information technologies in transforming the battlefield.”[5]

As for the American perspective, in U.S. military theory NCW was defined as a transition from **“platform-based warfare”** to **“network-based warfare.”** ***Admiral Jay Johnson*** called this “the most important military revolution in the last 200 years.” Experts and scholars of the field likewise note that informational superiority generates operational superiority, enabling the achievement of significant results with limited resources.[6,7]

The Chinese approach is well reflected in the 1999 publication Unrestricted Warfare, where Chinese military theorists ***Qiao Liang*** and ***Wang Xiangsui*** emphasize that war is no longer confined solely to the military arena. It also encompasses the economic, informational, technological, and psychological domains. This approach directly corresponds to the logic of NCW.[8]

[4] B. Zelenko, "К вопросу о сетецентрических войне и мире (некоторые аспекты). Власть." *Власть.* 2022.
[5] Ibid
[6] avid S. Alberts, John]. Garstka, Frederick P. Stein. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority.* CCRP Publication Series.
[7] Vice Admiral Arthur K. Cebrowski, USN, and John H. Garstka. 1998. "Network-Centric Warfare - Its Origin and Future." *US Naval Institute*
[8] Xiangsui, by Qiao Liang and Wang. 1999. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, February.

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

Through the theoretical and conceptual analysis of Network-Centric Warfare, it is based on the notion that the free and rapid exchange of information creates **“information superiority.”**

The main principles of NCW are:

- **Information sharing:** all combat units, sensors, and command posts are integrated into a unified network.
- **Common Operating Picture (COP):** all participants have a real-time updated view of the operational environment.
- **Decentralized decision-making:** subunits are granted greater autonomy, as they have precise and rapidly updated information.
- **High efficiency with limited resources:** through the use of so-called **“smart power”,** it is possible to achieve significant results with minimal force.

The foundation of this concept is the transition from **“platform-based warfare”** to **“network-based warfare”** — a shift that ***Admiral Jay Johnson*** described as the most significant stage of military revolution in the last 200 years.[9]

The implementation of Network-Centric Warfare is impossible without a technological foundation, and it is therefore natural that we must also examine its technological and operational aspects.

Main components:

- **Sensors and intelligence:** satellites, unmanned aerial vehicles, radars, electronic warfare **(EW)** systems, and other cybersecurity platforms;
- **Communication networks:** radio communication, satellite communication, navigation systems - **GPS, GLONASS, Galileo, BeiDou, NavIC, QZSS,** and fiber-optic systems;
- **Data analysis:** artificial intelligence and Big Data analytics;
- **Cyberspace:** defensive and offensive capabilities simultaneousl.

[9] Alberts, D. S., Garstka, J. J., & Stein, F. P. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series.

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

At the operational level, NCW (network-centric warfare) provides the capability to:

- to ensure rapid response;
- to synchronize different branches of the armed forces;
- to paralyze the adversary's informational infrastructure.

When discussing network-centric warfare, it is also impossible not to draw economic-technological parallels. For example, **Wal-Mart's**[10] business model is based on the rapid collection and distribution of information, which gives the company a competitive advantage. The same principle operates in the military sphere: sensor networks, data processing, and battlefield synchronization create operational superiority. The example of the financial sector is also important, since here the instantaneous dissemination of information determines the circulation of trillions of dollars. Accordingly, in the military domain, the speed of information exchange may likewise become the defining factor between success and failure.

As for international experience, it can be presented as follows:

USA

- The NCW concept was officially formulated in the 1999 publication "Network-Centric Warfare: Developing and Leveraging Information Superiority" (Alberts 1999) (Network Centric Warfare: Developing and Leveraging Information Superiority). Its practical continuation is the **Joint All-Domain Command and Control (JADC2).** The U.S. Department of Defense has conducted at least two major exercises using **JADC2**. The first took place in Florida in December 2019 and focused on repelling cruise-missile attacks. The exercise involved aircraft of the Air Force and Navy, including F-22 and F-35 fighter jets. The second exercise was held in July 2020. During the operation, the U.S. Air Force maintained communication with Navy vessels deployed in the Black

[10] Founded in 1962 in the United States by brothers Sam and James "Bud" Walton, the transnational corporation that operates a network of hypermarkets across the U.S. and 23 other countries is a global leader in both revenue volume and employment.

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

Sea.In addition, special operations forces from eight NATO member states coordinated joint actions aimed at repelling a **(JADC2)**[11].[12]

NATO

- **NATO** exercises demonstrate that a unified operational system based on the networked model significantly enhances the effectiveness of multinational operations.

Russia

- In the 1990s, Russia adopted American experience and developed its own model. Since 2014, operations conducted in Ukraine have demonstrated that information-psychological influence has become a central element of military strategy. Gerasimov's doctrine reflects precisely this integrated approach.[13] [14] [15]

China

- China is developing an "information-networked" model based on the comprehensive mobilization of national resources. Its central principle is the strategic paralysis of the adversary through informational dominance.

It is impossible to discuss **NCW** without focusing on information-psychological operations **(PSYOPS),** which today are as significant as traditional combat operations.

As the Russian example shows, these operations aim to:

- the demoralization of society;
- *the dissemination of disinformation;
- the stimulation of fear and uncertainty;
- the discrediting of international support.

If we attempt a philosophical-strategic interpretation of NCW, we can assume that in the contemporary reality even "war through media" has become possible, where the

[11] A concept developed by the U.S. Department of Defense, the essence of which lies in integrating information flows coming from all branches of the armed forces into a unified network operating on the basis of artificial intelligence, and which connects all domains (land, air, sea, space, and cyberspace.

[12] R. Hoehn, John. 21 января 2022. *Joint All-Domain Command and Control (JADC2). .* Congressional Research Service, Federation of American Scientists.

[13] Gerasimov, V. 2013. "The Value of Science is in the Foresight. ." *Military-Industrial Courier .*

[14] Thomas, T. 2015. "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations." *The Journal of Slavic Military Studies, 28(4).*

[15] Darczewska, J. 2014. "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study." OSW Report.

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

informational domain itself has become the battlefield. According to ***Boris Zelenko***, network-centric warfare is not merely a military-technical doctrine. It is part of a new global order, in which dominance in the informational space also determines political outcomes. In his view, “network-centric war and peace” creates a hybrid reality, where the boundaries between the military and civilian spheres dissolve.[16]

This interpretation shows that NCW requires not only military-strategic analysis but also philosophical and cultural understanding.

To summarize the research, let us address the challenges facing Georgia and the prospects associated with this direction, which are as follows:

Main challenges:

- Technological lag compared to advanced military countries;
- Weaknesses in cybersecurity systems;
- Insufficient control over the informational domain.

Prospects::

- Strengthening cooperation with international partners (NATO, the U.S., the European Union);
- Developing Georgia’s own military cybersecurity and defensive capabilities;
- Integrating information security into the national education system.

CONCLUSION

Network-centric warfare is a unity of technology, strategy, and psychological influence. It has already become one of the central challenges to national security including in Georgia. Confronting it requires a comprehensive approach that includes:

- **Strengthening informational resilience;**
- **Systemic development of cybersecurity;**
- **Strategic cooperation with international partners.**

[16] Zelenko, B. 2022. "К вопросу о сетецентрических войне и мире (некоторые аспекты). Власть." *Власть.*

ISSN 2720-8710 (Print)
ISSN 2960-9658 (Online)

Ultimately, it must be stated that a country's security today depends on its ability to manage military, informational, and cybersecurity challenges in an integrated manner.

BIBLIOGRAPHY

Alberts, D. S., Garstka, J. J., & Stein, F. P. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority.* CCRP Publication Series.

Darczewska, J. 2014. "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study." OSW Report.

David S. Alberts, John]. Garstka, Frederick P. Stein. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority.* CCRP Publication Series.

Gerasimov, V. 2013. "The Value of Science is in the Foresight. ." *Military-Industrial Courier .*

R. Hoehn, John. 21 января 2022. *Joint All-Domain Command and Control (JADC2). .* Congressional Research Service, Federation of American Scientists.

Thomas, T. 2015. "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations." *The Journal of Slavic Military Studies, 28(4).*

Vice Admiral Arthur K. Cebrowski, USN, and John H. Garstka. 1998. "Network-Centric Warfare - Its Origin and Future." *US Naval Institute.*

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

Zelenko, B. 2022. "К вопросу о сетецентрических войне и мире (некоторые аспекты). Власть." *Власть.*