The American Journal of Political Science Law and Criminology
ISSN 2693-0803 Volume 07 - 2025

Theoretical Analysis of The Phenomenon of Information Wars in The Era of Globalization

[1] Aliyev Jakhongir Erkinjon o‘g‘li
[1] Tashkent State University of Oriental Studies, Department of "International Relations", Doctoral candidate, Uzbekistan

Received: 30th Oct 2025 | Received Revised Version: 20th Nov 2025 | Accepted: 02th Dec 2025 | Published: 14th Dec 2025

Volume 07 Issue 12 2025 | Crossref DOI: 10.37547/tajpslc/Volume07Issue12-05

Abstract

The process of globalization has led to an unprecedented increase in the exchange of information between states, societies, and individuals due to the rapid development of modern information technologies. This process has not only strengthened integration in economic, social, and cultural spheres but has also created new opportunities and challenges. Along with the expansion of the global information space, the risks associated with information security have also grown. In particular, phenomena such as information attacks, disinformation campaigns, cyberattacks, and psychological manipulation have become serious threats today, not only in military and political spheres but also in areas such as economic competition, social stability, and the preservation of cultural identity. Consequently, information wars are now considered a crucial issue in ensuring the national security and sovereignty of states in the modern world.

This article provides an in-depth analysis of various forms of information warfare and their strategic objectives. Information wars are examined as a tool employed by states or groups to safeguard their political, economic, or ideological interests. In this process, methods such as spreading disinformation, orchestrating cyberattacks, exerting psychological pressure, and manipulating through mass media play a crucial role. Through these methods, attempts are made not only to control public opinion but also to destabilize the internal stability of states and weaken their position in the global arena. The article illustrates with examples how these mechanisms operate and how they impact the global information space.

In conclusion, it is demonstrated that in the context of globalization, protecting the national information space and creating a stable media environment are among the key principles in combating information wars. In this process, states must be capable of not only ensuring their own information security but also actively participating in the global information space and defending their interests. The article emphasizes the necessity of comprehensively studying the problem of information wars and developing effective strategies against them, which is becoming increasingly crucial in the modern world.

Keywords: Information warfare, disinformation, media manipulation, cyberattacks, national content, information security, global communication, information sovereignty.

Cite This Article: Aliyev Jakhongir Erkinjon o‘g‘li. (2025). Theoretical Analysis Of The Phenomenon Of Information Wars In The Era Of Globalization. The American Journal of Political Science Law and Criminology, 7(12), 29–34. https://doi.org/10.37547/tajpslc/Volume07Issue12-05

1. Introduction

The process of globalization has become one of the most significant and influential trends of the 21st century. Due to the rapid development of modern information technologies, the physical and spiritual boundaries between countries, societies, and individuals around the world are gradually disappearing. The widespread use of the Internet, digital communication tools, and social networks has brought information exchange to an

unprecedented level. This has enabled people to access the information they desire at any time and place. For instance, it has become possible to send messages from one corner of the world to another in a matter of seconds, follow news in real-time, or explore diverse cultures. However, this process brings not only positive changes but also serious risks. Along with the expansion of the global information space, problems related to the quality and reliability of information within it are also becoming more acute. Today, alongside factual reality, manipulated, misinterpreted, or blatantly false information is actively spreading. This situation has created a favorable environment for information warfare, transforming it into a strategic tool aimed at undermining the socio-political stability of specific states or societies.

Information warfare today extends beyond traditional military domains and is actively conducted in virtual and media spaces. While competition was previously carried out primarily through armed forces or economic resources, establishing control over information and directing it towards one's own interests has now become the main means of gaining supremacy in the modern world. States, large corporations, and even individuals are striving to advance their political, economic, or personal interests by managing information flows. For instance, it has become possible to alter the opinions of millions of people, influence their behavior, or even interfere in political processes through false messages disseminated on social networks or targeted advertising campaigns. In this process, states are employing not only overt but also covert methods to weaken their competitors.

Modern information wars do not only target political and military objectives, but also encompass economic, social, and cultural spheres. Through cyberattacks, critical infrastructure - such as banks, energy systems, or government websites - can be rendered inoperable, which has a high likelihood of seriously undermining economic stability. Psychological manipulation is employed to turn the public against each other, intensify social tensions, or disrupt national unity. Media influence is used in attempts to damage the image of certain groups or states, aiming to discredit them in the international arena. For instance, deliberately disseminated false information can increase distrust within society and potentially incite protest movements against the government.

Furthermore, information warfare poses a threat to cultural identity. As dominant cultures and languages prevail in the global information space, there is a risk of small nations losing their unique characteristics. In this process, local cultures are being marginalized through manipulative means, with externally influenced values being instilled in their place. Consequently, information warfare is becoming a battleground not only for political or economic competition but also for the protection of cultural sovereignty. States are compelled to strengthen their national information space and create a reliable media environment to counter external forces attempting to influence the consciousness of their citizens.

The complexity of information warfare lies in the fact that it is often conducted in covert and hard-to-detect forms. For example, messages spread through fake accounts on social networks or comments managed by so-called "troll factories" can distort reality. Additionally, personal data is being analyzed using artificial intelligence and big data technologies to develop tailored manipulation strategies. This makes information warfare increasingly effective and dangerous.

As a result, in the context of globalization, information warfare has become an integral part of the modern world. It directly influences the success of states not only in foreign policy but also in internal stability and development. Therefore, to combat these threats, states need to take measures such as ensuring their own information security, developing a national media system, and improving the digital literacy of citizens. Only in this way will it be possible to protect one's interests in the global information space and maintain a stable society.

2. Methodology

Within the framework of scientific research on the significance of information warfare in the formation process, a number of theoretical, methodological, and practical approaches have been developed by foreign and local scientists. In this regard, the works of scientists such as A. Muminov, H. Rajabov, B. Milner, I. Nonaka and H. Takeuchi, P. Senge, V. Bukovich, K. Wiig, D. O'Leary, D. Snowden, Y. Vovk, M. Martynenko, A. Degtyar and M. Bubliy, A. Nalyvayko, N. Butenko, N. Smolinska, I. Hrybyk, and S. Leonov are noteworthy.

At the same time, it is important to emphasize that at the beginning of the 21st century, understanding the place and role of information warfare in the context of modern hybrid warfare requires increasing attention.

Today, "information warfare" is a multifaceted concept that incorporates diverse elements from various fields of knowledge, forming a theoretical model capable of complex and effective explanation. The most commonly used terms within the framework of information warfare include: information security systems, information superiority, information dominance, protection of critical infrastructure, operational security, and others. As a result of the rapid development in the field of information technology, information wars are becoming increasingly complex and more effective. Their influence on national values, social self-awareness, and other important factors may go unnoticed for a long time; in some cases, this process is almost imperceptible. The party engaging in information warfare can effectively carry out its actions by exploiting the interconnectedness and interdependence of systems within modern infrastructures.

Information warfare is considered one of the most serious threats to national security. This threat is essentially related to the achievement of absolute supremacy in the information sphere by any state. Such supremacy allows for influencing the actions of citizens, the political elite, and the military, as well as manipulating public opinion. Information warfare expands the battlefield: in this type of war, there is no traditional front line. It is impossible to precisely determine when information influence is being exerted, and it is also difficult to directly observe or expose information operations. Therefore, it is nearly impossible to detect such attacks, and the authors of these operations remain unknown.

Researcher A. Tulepov describes the information war as follows: "Currently, the information war is intensifying rapidly. Information warfare is the ideological influence exerted on an opponent to achieve various goals. An information attack is an attempt to shape public consciousness through malicious means by influencing the opponent" . Through this definition, he tried to reveal the essence of information warfare. According to him, information warfare is a means of ideological influence, with its main goal being to influence the public consciousness of the opponent. One of the most important aspects of this process is information attacks, which are aimed at forming misconceptions about existing political institutions in society through lies, disinformation, and manipulation.

The term “information warfare” was first used in a 1976 report titled "Weapons Systems and Information Warfare" prepared by American scientific consultant Thomas Rona for Boeing Company. In his work, the author emphasized that information infrastructure was becoming a key component of the US economy and noted that it could become a vulnerable target not only during wartime but also in peacetime. The publication of T. Rona's report sparked widespread discussions in the US press, and the topic attracted the interest of American specialists working with classified materials. By the 1980s, the US Air Force began actively discussing this subject. By that time, the concept that information could be used not only as a target but also as a weapon had become widespread.

Similarly, Russian researcher Y. Vostretsova, like American scientist Winn Schwartau, divides information warfare into three forms based on scale. She specifically highlighted the following directions of global information attacks: influencing individual, group, and public consciousness using mass media; influencing decision-making systems in socio-political, economic, and military spheres. In Y. Vostretsova's book “Fundamentals of Information Security” information warfare is classified into four categories: political, financial-economic, diplomatic, and military. This classification demonstrates the complex nature of information warfare and its impact across various fields.

According to Doctor of Political Sciences H. Rajabov, the damage inflicted on a particular country as a result of a traditional war can be calculated over a specific period of time. However, it is practically impossible to identify and eliminate the consequences of information warfare within a given timeframe. Along with the technical aspects of the damage caused by information warfare, there are also ideological aspects that cannot be limited by time. In this regard, the higher the level of effectiveness of information wars for the attacker (aggressor), the greater the damage to the defender.

Currently, alongside concepts such as "information attack" and "information warfare," the term "psychological warfare" is also widely used. This term was first introduced to science by the English historian and military theorist John Frederick Charles Fuller in 1920. In the process of studying the First World War, J. Fuller emphasizes that during the war, states not only engaged in armed conflicts but also exerted information and psychological pressure on each other. He particularly stresses the importance of psychological warfare,

viewing it as an integral part of modern wars.

Manuel Castells, in his book "Communication Power," analyzes the role of the information space in governing society. According to Castells, in the era of the Internet and social networks, information flows have become the primary means of shaping consciousness. He refers to information wars as "a new weapon of the digital age" and substantiates their spread through global communication networks with examples.

It is becoming increasingly evident that the interpretation of information warfare by researchers and experts as merely a part or logical continuation of traditional warfare does not align with today's reality. This is because signs of information warfare are appearing even in regions where traditional wars are not being waged. These instances are now being viewed as a modern manifestation of cultural and ideological aggression. The general purpose and content of information warfare during active military operations differ significantly from those during periods without traditional warfare.

3. Results

As globalization interconnects the world and accelerates information exchange, information warfare is becoming an increasingly crucial tool for protecting and influencing states' strategic interests. This process affects not only traditional military and political spheres but also broader areas such as economic competition, preservation of cultural identity, and maintenance of social stability. In the modern era, information warfare has evolved from simple propaganda to more complex and dangerous forms, creating new threats for states and societies.

The rapid development of modern technologies, particularly the widespread use of social networks, the increasing capabilities of artificial intelligence, and the emergence of deepfake technologies, has fundamentally altered the methods of conducting information warfare. Now these wars are waged not only through words and images, but also via digital platforms, complex algorithms, and manipulations that directly influence human consciousness.

Analyses indicate that creating and developing national content is considered one of the most effective strategies in combating information warfare.

Disinformation is one of the most dangerous weapons in today's information warfare, and its negative consequences are clearly visible in several crucial areas. Diminished trust in information, the proliferation of inaccurate or manipulated data undermines public confidence in official sources, creating a vacuum in the information space. Furthermore, propaganda and false information can intensify conflicts within society and incite hostility between groups.

4. Discussion

The boundless flow of information and the advancement of digital technologies are compelling nations to safeguard and fortify their information spaces, as these spaces hold strategic importance not only for national security but also for economic stability and societal cohesion. Information warfare is no longer confined to traditional military or diplomatic arenas; it is now extensively employed to manipulate global economic processes, mold public consciousness, and influence the internal political stability of states. At present, information warfare is exerting its impact across various domains and is being utilized as a strategic weapon in the following directions:

Mass media is being extensively utilized to expand global spheres of influence. Major powers, such as the United States and Russia, are actively employing international media platforms in attempts to sway each other's political processes. Information streams targeted at global audiences are being shaped through networks like CNN and other U.S. channels, as well as Russian outlets such as RT or Sputnik. This process serves not only to alter the image between states but also to shift the balance in international relations.

The widespread use of social networks has simplified the process of influencing political processes. For example, cases of manipulating election results through fake accounts, bots, and propaganda campaigns are on the rise. Claims of Russian interference in the 2016 US elections or disinformation campaigns during the Brexit process are clear examples of this. Manipulations spread through social networks are serving to intensify polarization and populist movements in society.

In today's globalized information age, developing countries such as Uzbekistan need to develop their own strategies to counter these threats of information warfare. Currently, the country needs to focus on the following areas to ensure information security:

Developing local media platforms and increasing content based on national values is an important method of protection against foreign information influence. This process serves to preserve the cultural identity of the people and increase immunity to manipulations. It is also necessary to invest in and expand technological capabilities to make local media platforms competitive in the digital world. At the same time, mechanisms for filtering and controlling foreign information flows should be developed.

It is necessary to focus on strengthening the legal framework for regulating the state information space and combating disinformation, adopting new laws in this area, and adapting existing ones to modern requirements.

Implementation of special educational programs to improve media literacy and develop the population's critical information analysis skills. This process is especially aimed at increasing the younger generation's ability to identify fake information on social networks. These programs should cover not only young people, but all age groups and teach them how to protect themselves from information manipulation.

Modern technologies are being introduced in the field of cybersecurity to protect national information systems. This will help safeguard government agencies, banking systems, and critical infrastructure from cyberattacks.

In the context of globalization, information wars present a complex challenge for states, affecting not only external threats, but also internal stability and economic development. To counter these threats, Uzbekistan must continue strategic measures, such as strengthening its national media and cybersecurity infrastructure, educating the public on safe navigation in the digital world, and developing international cooperation. This approach not only protects the country from current threats but also helps it secure a strong position in future global information competition.

5. Conclusion

The process of globalization has expanded the global information space and intensified the interdependence of states and societies. Due to the development of information technologies, competition between states is escalating not only in economic or military spheres, but also in the information domain. The results of this study demonstrate that information warfare occupies a central position in the national security policies of modern states.

Analysis has shown that information warfare is not limited to propaganda or disinformation, but is conducted through various forms (cyberattacks, deepfakes, psychological pressure, information blockades, and social manipulation). In this process, it was determined that the creation and strengthening of national content is the primary condition for ensuring information security.

The research results led to the following important conclusions:

1. The intensification of information warfare - states are conducting extensive disinformation campaigns using social networks, mass media, and artificial intelligence.

2. The urgency of cybersecurity strategies - in response to the expansion of information warfare, states are developing new strategies to protect their information infrastructure.

3. National content is the fundamental cornerstone of information sovereignty - strengthening the national information space is emerging as an effective means of defense against foreign information onslaughts.

4. The necessity of improving society's media literacy - developing the media culture of the population is crucial for combating disinformation and strengthening information security.

In the future, Uzbekistan should implement the following strategies:

Strengthening information policy - developing new legislative acts to protect the national information space and counter foreign manipulations.

Developing the national media system - enhancing the competitiveness of domestic media and promoting them in the international arena.

Developing special programs to combat disinformation - enhancing society's ability to detect fake news and fostering a critical approach to information among the population.

Strengthening cybersecurity infrastructure - protecting state information systems and improving the national cybersecurity strategy.

In the context of globalization, information wars are having a serious impact on the national security and

social stability of states. The following areas are of paramount importance for ensuring information sovereignty:

1. Creating and promoting national content - the primary strategy for combating foreign information attacks.

2. Developing information policy - the state should introduce new legislative norms to ensure information security.

3. Increasing media literacy in society - it is crucial to raise public awareness to combat fake news and disinformation.

4. Strengthening cybersecurity infrastructure - it is necessary to protect information systems of government institutions and the private sector.

In the future, Uzbekistan and other countries should develop international cooperation in combating information warfare, devise new strategies in line with advancements in information technologies, and strengthen information policies to protect national interests.

References

1. А. Муминов. Ўзбекистон: Ахборотлашган жамият сари. Т.: - Turon-zamin ziyo‖ нашриѐти 2013. Б-132.
2. Vacca W., Davidson M. (2019) The Regularity of Irregular Warfare. Parameters.
3. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / — Екатеринбург : Изд-во Урал. ун-та, 2019. — 204 с.
4. Rajabov H.I. Globallashuv sharoitida davlatning axborot siyosati (O‘zbekiston Respublikasi misolida). Siyosiy fanlar bo‘yicha falsafa doktori (PhD) ilmiy darajasini olish uchun bajarilgan dissertatsiya.- T., 2018. – B.32.
5. Nye, J. S. (2004). Soft Power: The Means to Success in World Politics. PublicAffairs. (pp. 89, 112, 121)
6. Castells, M. (2009). Communication Power. Oxford University Press. (pp. 32, 45, 97, 157)
7. Mahmudov, T. (2020). Milliy axborot xavfsizligi va uning tahdidlariga qarshi kurash. Toshkent: Sharq. (pp. 55, 65)
8. Mohamed, A. (2018). Cyber Warfare in the Middle East: Tactics and Strategies. Routledge. (pp. 63, 79, 89)
9. Pomerantsev, P. (2014). Nothing is True and Everything is Possible: The Surreal Heart of the New Russia. PublicAffairs. (pp. 112, 143, 154)
10. Glenn R.W. (2019) Thoughts on “Hybrid” Conflict. Small Wars Journal.
11. Duginets, G., & Busarieva, T. (2021). The role and place of the information war in the modern hybrid war. Naukovi zapysky TNU imeni V. I. Vernadskoho. Seriia: Ekonomika i upravlinnia, 32(71), 4, 1-5. https://doi.org/10.32838/2523-4803/71-4-1
12. Tulepov A. Internetdagi tahdidlardan himoya. Toshkent: Movarounnahr, 2015. B. 15.