*Akademik Tarih ve Düşünce Dergisi* *Academic Journal of History and Idea*
*ISSN: 2148-2292*
*12 (4) 2025*

*Araştırma Makalesi | Research Article*
*Geliş tarihi |Received:10.07.2025*
*Kabul tarihi |Accepted:14.08.2025*
*Yayın tarihi |Published:25.08.2025*

**Mahammad Jabrailov**

*https://orcid.org/0000-0002-5812-1900*
*Ph.D. in Philosophy, Associate Professor, Head of the Department of "Philosophical Problems of Digital Development and Artificial Intelligenc" Institute of Philosophy and Sociology, Azerbaijan National Academy of Sciences (ANAS), mehmetsoltanedu@gmail.com*

***Atıf Künyesi | Citation Info***

Jabrailov, M. (2025). Infoimperialism and Security: Cyberattacks, Disinformation, and State Defense Strategies. *Akademik Tarih ve Düşünce Dergisi*, *12* (4), 713-724.

# Infoimperialism and Security: Cyberattacks, Disinformation, and State Defense Strategies

***Abstract***

*This article examines the concept of infoimperialism—the transformation of information technologies into geopolitical instruments—within the context of cybersecurity and strategic information politics in global affairs. Using a methodological framework based on structural realism and constructivism, the study explores how both state and non-state actors leverage disinformation, digital diplomacy, and cyber operations to reshape global power dynamics. The novelty of the article lies in framing infoimperialism not merely as media control but as a form of soft power and technological hegemony in cyberspace. Findings suggest that institutions like USAID play a central role in managing global information flows, thereby influencing geopolitical competition. For countries like Azerbaijan, the article emphasizes the strategic necessity of building institutional and legal mechanisms for information security in an era of digitalized global rivalry.*

***Keywords:*** *Infoimperialism, Cybersecurity, Disinformation, Digital Diplomacy, Geopolitical Competition*

# Enformasyon Emperyalizmi ve Güvenlik: Siber Saldırılar, Dezenformasyon ve Devlet Savunma Stratejileri

***Öz***

*Bu makale, bilgi teknolojilerinin jeopolitik araçlara dönüşümünü ifade eden enformasyon emperyalizmi kavramını, küresel ilişkilerde siber güvenlik ve stratejik bilgi politikaları bağlamında*

*incelemektedir. Çalışma, yapısal realizm ve inşacılık temelli metodolojik bir çerçeve kullanarak, hem devlet hem de devlet dışı aktörlerin dezenformasyon, dijital diplomasi ve siber operasyonlardan yararlanarak küresel güç dinamiklerini nasıl yeniden şekillendirdiklerini araştırmaktadır. Makalenin yeniliği, enformasyon emperyalizmini yalnızca medya kontrolü olarak değil, aynı zamanda siber uzayda yumuşak güç ve teknolojik hegemonya biçimi olarak ele almasında yatmaktadır. Bulgular, USAID gibi kurumların küresel bilgi akışlarını yönetmede merkezi bir rol oynadığını ve bu yolla jeopolitik rekabeti etkilediğini ortaya koymaktadır. Azerbaycan gibi ülkeler için makale, dijitalleşmiş küresel rekabet çağında bilgi güvenliği için kurumsal ve hukuki mekanizmalar inşa etmenin stratejik bir zorunluluk olduğunun altını çizmektedir.*

***Anahtar Kelimeler:*** *Enformasyon Emperyalizmi, Siber Güvenlik, Dezenformasyon, Dijital Diplomasi, Jeopolitik Rekabet*

## Introduction

Since the beginning of the 21st century, geopolitical parameters have been undergoing rapid transformation. In this new era, global developments in information and technology have emerged as central elements shaping both international relations and geopolitical power dynamics. The digital revolution that began in the late 20th century, together with the accelerated growth of information technologies and the widespread use of artificial intelligence, has led to the emergence of a new phenomenon: infoimperialism.

Infoimperialism is increasingly understood as a novel form of imperialism, based not on territorial conquest but on the control of digital information flows, dominance in cyberspace, and the strategic use of global communication tools. The geopolitical role of digital platforms, artificial intelligence technologies, and mass communication infrastructures continues to expand, influencing both the balance of power and the formulation of national security strategies worldwide. Although infoimperialism is rooted in traditional power relations, it diverges significantly from classical imperialism. Whereas classical imperialism sought the occupation of physical territories and the extraction of natural resources, infoimperialism is concerned with controlling the digital information domain and manipulating global information on a large scale. In this regard, major technology companies and digital platforms have become not only economic actors but also political instruments of influence. This study examines the impact of infoimperialism on state security, the mechanisms of cyberattacks and disinformation campaigns, and the defense strategies developed by states in response. Particular attention is devoted to the legal, technological, and cooperative frameworks adopted to strengthen cybersecurity.

## 1. The Rise of Infoimperialism: Digital Hegemony and the Reshaping of National Security Strategies

In contemporary geopolitical processes, states aspiring to become global power centers increasingly employ information resources to steer political outcomes in their favor. Technological innovations and modern cyber capabilities not only drive domestic transformation but also exert significant influence on the international system. As a result, the use of information as a tool of pressure and influence has become a critical global issue.

According to Hikmət Babaoğlu (2013), the phenomenon of infoimperialism defines a new form of global political structure in which power is exercised through the construction of an *infocracy* and the emergence of an *info-elite*. These forces, embedded in the broader logic of capitalist expansion, develop new tools and methods to preserve and extend their influence. Babaoğlu explains:

*"Infoimperialism leads to the rise of a new global infocracy, and infocracy, in turn, gives birth to a new info-elite. These imperial forces, in search of new instruments for the development of capitalism—the substratum of imperialism—are creating a new international political order. Infoimperialism generates unpredictable and complex problems that penetrate even the most unexpected spheres of society. This erosion occurs primarily in the moral domain, exerting such profound influence that even concepts like 'nation' and 'people' undergo fundamental transformation. A new global social pyramid emerges, which is not a classic national-ethnic structure but rather takes the form of an info-cultural hierarchy"* (Babaoğlu, 2013, p. 12).

Babaoğlu's perspective provides a conceptual framework situating infoimperialism as a dominant factor in modern global politics. While classical capitalism focused on controlling material resources, contemporary power structures prioritize control over information flows as a means of attaining economic and political superiority. States and technology corporations that dominate the global information domain constitute the backbone of a new political info-elite. Through the targeted management of information, this elite is capable of reshaping public opinion, manipulating value systems, and even redefining national identities. The restructuring of historical consciousness and cultural identity through information control represents one of the most destabilizing aspects of infoimperialism.

The practical application of infoimperialist strategies can be observed across several geopolitical regions, particularly the Middle East, the South Caucasus, and North Africa. In these

regions, states often demonstrate weak defenses against the growing influence of global actors employing information manipulation as a strategic tool. These dynamics became most visible during the so-called "Arab Spring," where information warfare was used as a method of intervention in countries such as Iraq, Libya, Yemen, and Syria.

For instance, the "Iraq model" presents a clear example of infoimperialism in practice. Following the 2003 U.S.-led military intervention, Iraq retained its formal statehood and borders but underwent significant functional transformations in its governance structure. As Babaoğlu (2013) explains, the occupying powers established a model grounded in the principles of infoimperialism. This model resulted in the fragmentation of Iraqi society into opposing ideological and political camps, generating an internally controlled chaos that served broader geopolitical interests. This demonstrates that the objective of such strategies is not merely to analyze the nature of information but to employ it as a geopolitical weapon—disrupting existing cultural values, creating artificial narratives, and undermining societal cohesion in target countries. Information, in this context, is not a neutral entity but a tool of geopolitical engineering.

As Cəbrayılov (2019) notes, a new generation of professions has emerged, particularly in the virtual realm, as part of this transformation. Among them is digitized foreign policy, which simplifies previously complex diplomatic problems and opens new avenues for global influence through digital means. According to Cəbrayılov:

*"The goal is not to study the nature of information, but to highlight how information is used as a geopolitical tool to weaken national values, suppress unity, create new narratives, and exert pressure. This new informational paradigm produces digitalized fields of practice, including foreign policy, that reshape global interaction patterns"* (Cəbrayılov, 2019, p. 52).

Thus, information becomes both a medium of manipulation within imperialist doctrine and a strategic asset for advancing global power interests. Contemporary research confirms that many states now seek to influence rivals not only through military means but also through information dominance. Achievements unattainable through conventional warfare are frequently pursued via digital disinformation campaigns and cyber influence operations. During the 1980s, the geopolitical power of information became a widely debated subject in Western academic and strategic circles. In the Soviet Union, however, scholarly analysis of this issue remained limited. This can be explained by two factors: first, Azerbaijan, as part of the USSR, was embedded within a unified geopolitical space; second, the transition to an information society coincided with the

final decades of the Soviet era. Nonetheless, the issue of information security in Azerbaijan's post-independence period must now be analyzed in the broader context of global infoimperialist pressure. As global powers seek to control digital information flows and manipulate public opinion, post-Soviet states such as Azerbaijan face a complex web of cyber and narrative threats that require comprehensive defense strategies. In Western countries, the emergence of the concept of the "information society" and the technological progress it generated fundamentally contradicted the principles of communism. Even after works were published emphasizing the historical necessity and social progress of informatization, skepticism toward the power and role of information persisted in the Soviet Union.

A. P. Suxanov, for instance, criticized Western theorists for "fetishizing" the role of information, arguing that the concept of the information society portrayed the individual as helpless, overwhelmed by an ever-growing flood of data, brochures, and books. According to him, bourgeois ideologists framed the role of information in society from an idealistic and technocratic perspective, thereby downplaying the decisive function of productive forces and production relations in social development (Suxanov, 1988). History shows that states that fail to recognize the strategic significance of information struggle to safeguard their geopolitical interests. The collapse of the Soviet Union illustrates the consequences of strategic missteps in information policy. Today, undeclared information warfare presents unprecedented threats to every nation. The rapid expansion of information and communication technologies (ICT)—both in scale and scope—demands new political-scientific responses and agile governance. The trajectory toward an information society is historically rooted in the major informational revolutions of human civilization. Compared to earlier periods, the current role of information in shaping geopolitical relations has vastly expanded. Accordingly, the strategic use of information resources in global politics has become a primary tool for both traditional and emerging international actors to enhance their influence.

Manuel Kastels has analyzed the collapse of the Soviet Union in this context. In *The Information Age: Economy, Society and Culture* (Vol. 1, 2000), he argues that Soviet statism faced severe challenges in transitioning to informationalism. The administrative economy—reinforced by military structures and inefficiency—was ill-equipped to adapt to a system based on the socialized processing of information and the symbiotic interaction between data and production. According to Kastels:

*"Soviet statism encountered a deep structural crisis in the historical context of transition to informationalism. The system, founded under the banner of developing productive forces, failed to cope with one of the most significant technical revolutions in human history. The state's monopoly over information and its confinement of technology within military production could not match the symbiotic interaction between information processing and material production that defines informationalism"* (Kastels, 2000, p. 488).

While Kastels' interpretation may underemphasize broader historical dynamics, the inability to respond adequately to post-industrial transformations—especially regarding the strategic value of information—undoubtedly contributed to the Soviet collapse. This serves as a vital lesson for aspiring global powers: participation in geopolitical processes and the formulation of long-term strategies must include the systematic incorporation of information policy as a central pillar.

New trends in information transfer exert profound influence over global geopolitical configurations. As paradigms of global order evolve, major powers attempt to impose new rules of engagement, while competition among emerging actors grows increasingly fierce. In this environment, open and covert operations—particularly those involving control over information flows—raise serious concerns about the security of smaller states.

Political analysts Bjola and Holmes raise similar concerns. Examining the "borderlands" between Russia and Europe, they highlight the emergence of a new strategic landscape. Comparing current developments with the period leading up to the World Wars, they observe:

*"The process is only beginning, yet it already resembles the trajectory Germany followed in 1914. Powers are being drawn in, and if this continues, many of the well-intentioned information security initiatives pursued by states will fall beyond their control. The buildup of forces has begun, and if this process continues, many of the goodwill initiatives and efforts in the field of information security will fall outside the control of the states themselves"* (Holms & Bjola, 2015, p. 46).

This observation highlights the fundamental shift taking place in global geopolitical dynamics, where information has emerged as a strategic force reshaping state interactions and international cooperation.

The evolution of information into a decisive geopolitical factor has fundamentally altered traditional models of diplomacy and global collaboration. In contemporary international relations, digital communication networks and the virtualization of diplomacy enable states to engage in political dialogue in real time, across digital platforms. The influence of virtual information in

geopolitics is not merely a technological development; it represents a paradigmatic change in how power is exercised and contested globally.

The United States was among the first nations to conceptualize and operationalize information warfare as an alternative to conventional military engagement. In doing so, it reframed "warfare" into a domain where data, narratives, and communication strategies function as weapons of strategic influence. This shift signifies a broader transformation in which the geopolitical "rules of the game" are increasingly being replaced or redefined by information-based technologies and methods. Today, states leverage information as a strategic weapon in their foreign policies, applying pressure, influence, and narrative control to achieve diplomatic objectives without resorting to conventional force. The growing use of these mechanisms in international politics has positioned information infrastructures as central to geopolitical competition, enabling the pursuit of national interests through non-kinetic yet highly consequential means. No state can achieve sustained success in foreign policy without accounting for the strategic role of information in international geopolitics. Efforts to dominate the global information space inevitably provoke resistance from other actors, triggering information conflicts that reshape global and regional power dynamics. Consequently, principles such as national sovereignty, statehood, and information security are increasingly subjected to the pressures of infoimperialist competition.

The United States' pursuit of global geopolitical dominance is not based solely on economic or military superiority. It is equally driven by an ambition to become the world's primary information hub, embedding concepts such as digital diplomacy into the fabric of international relations. Through initiatives such as FAN [full name], the United States seeks to consolidate its informational advantage by establishing unified digital infrastructures for both governmental and intergovernmental operations. From the perspective of infoimperialism, these developments represent deliberate strategies of influence and control over global information flows (IT Strategic Plan, 2010).

Further evidence of this approach can be observed in the activities of the United States Agency for International Development (USAID). According to public disclosures from 2025, USAID provided substantial financial support to international media platforms engaged in shaping global narratives: $3.1 million to *The New York Times*, $8 million to *Politico*, $19 million to *Associated Press*, $9 million to *Reuters*, and £2.6 million to *BBC*. In total, more than 700 media organizations and over 300 NGOs related to media operations received funding, while over 6,000

journalists benefited from USAID programs (Memorandum, 2025). These figures indicate that USAID functions not merely as a development agency but as a strategic actor in global media governance. By allocating resources to leading international news organizations, USAID influences editorial priorities, shapes dominant narratives, and steers public perception in line with U.S. foreign policy objectives. In this respect, its activities can be interpreted as geo-informational rather than purely informational. USAID's actions exemplify how infoimperialism operates through institutional mechanisms. They reaffirm the need to interpret global information flows not as neutral or organic, but as structured instruments of influence serving political, economic, and ideological purposes. As such, media platforms increasingly act as tools in the global competition for narrative dominance and ideological legitimacy. In the context of global information warfare, one of the media's primary functions is the shaping of public opinion. Strategic actors such as USAID employ media resources not only to disseminate information but also to promote selective narratives and restrict alternative perspectives. Evidence suggests that this is a deliberate practice aligned with geopolitical objectives.

One striking example is provided by the article *USAID: A Corruption Hub for Sinister Plans* (2025), which reports that global media campaigns against Azerbaijan during key international events were allegedly supported or coordinated by USAID. These events include the 2012 Eurovision Song Contest, the 2015 European Games, the 44-day Patriotic War (2020), environmental protests on the Lachin Road, and COP29-related media coverage. According to the article, these campaigns sought to damage Azerbaijan's international reputation during moments of national and diplomatic significance. Moreover, USAID—despite decades of occupation of Azerbaijani territories—did not issue statements condemning the occupation or supporting initiatives to address the humanitarian challenges faced by displaced persons. Instead, it was accused of promoting anti-Azerbaijani narratives and aligning with pro-Armenian positions. Such claims reinforce the argument that infoimperialism manifests through the manipulation of international media narratives, with institutions like USAID serving as operational instruments in the ideological struggles of global power centers. Rather than supporting balanced journalism, the financial and logistical backing provided to selective media organizations often amplifies specific geopolitical narratives while marginalizing dissenting or localized perspectives.

These practices raise serious concerns about information sovereignty and the fairness of international media coverage, particularly for small and mid-sized states seeking to assert their

narratives on the global stage. In this context, media becomes not merely a platform for objective reporting but a strategic asset for shaping perceptions, legitimizing power structures, and advancing geopolitical influence under the guise of development or public diplomacy.

The modern international information system constitutes a dynamic field that significantly shapes both global geopolitical processes and interstate relations. Contemporary international relations have developed on foundations established by modern geopolitical transformations. Historical experience demonstrates that innovations in information transmission have consistently influenced developments within the global geopolitical system. As a result, the late 20th century marked the transition from an industrial phase to a post-industrial information society. Technological and innovative developments of the post-industrial era—particularly projects applying the outcomes of the information revolution to global geopolitical interests—suggest that the Republic of Azerbaijan must align its approach to information security with newly emerging international standards. Infoimperialism is a framework in which information technologies and cyber resources function as central instruments for shaping global power structures. As Kastels (2000) emphasized, understanding the nature of the information society requires consideration of both the causes of the information revolution and the opportunities it generates. In this regard, infoimperialism encompasses the strategies of powerful states and corporations that seek to dominate flows of information and knowledge.

A notable example is the rivalry between global powers such as the United States (U.S.) and China, particularly in artificial intelligence, data analytics, and cybersecurity. Control over information and knowledge has become a means of pursuing hegemony in the global information space, often at the expense of other nations' information sovereignty. According to U.S. officials, cyberattacks now target not only private companies but also critical state institutions, including the National Nuclear Agency. A report from the Federal Bureau of Investigation (FBI) indicated that cyberattacks against the U.S. in 2020 increased by 69% compared to previous years. Financial losses totaled $4.2 billion in 2020, compared to $3.5 billion in 2019 and $1.5 billion in 2015 (Cyber Warfare to Cyber Terrorism, 2021). These figures indicate that even major global actors experience a rising number of cyberattacks directed at both governmental bodies and critical private infrastructure. This underscores the increasing relevance of cybersecurity at state and corporate levels. The targeting of institutions such as government agencies and the National Nuclear Agency

illustrates that cyber threats extend beyond financial or commercial domains, posing risks to national security and the energy sector.

Within the broader context of cybersecurity and geopolitical competition, the U.S. and other Western states employ cyber tools to maintain economic and informational advantages. These measures frequently include sanctions, trade restrictions, and offensive cyber operations aimed at undermining the technological infrastructures of rival states. The U.S. government regularly accuses Russia, China, Iran, and North Korea of orchestrating such attacks. As a consequence, rival states and corporations engage in offensive cyber operations to steal industrial data, acquire strategic advantage, and perpetuate what some analysts describe as "informational colonialism." These dynamics highlight the close interconnection between cybersecurity and infoimperialism. Cyberattacks can simultaneously operate as economic and security threats as well as instruments of broader global information warfare.

If governments act unilaterally to secure their national interests without international standards or agreements, such actions risk weakening global cybersecurity and destabilizing internet and digital communication systems. While intergovernmental cooperation can help constrain the activities of non-state actors and cybercriminals, no state can unilaterally guarantee comprehensive cybersecurity (Abbasi, 2021). Because contemporary cyber threats are global in scope, unilateral measures remain insufficient. This imbalance between national security and international stability drives some governments toward unilateral cyber operations, which, in turn, intensify intergovernmental tensions and increase the risk of conflict escalation.

Cybersecurity is therefore no longer merely a technical issue but an integral component of international politics. Without coordinated rules and collaborative mechanisms, states will face serious difficulties in addressing these growing threats.

As Goodman, Kirk, and Kirk (2007) argue, *"in terms of understanding international politics, threats related to network security once again highlight the contradictions between classical neorealist perspectives and international or institutionalist neoliberal approaches. Cybersecurity is sometimes viewed as a unilateral foreign policy problem or a stable neorealist paradigm. Proponents and opponents of collective cybersecurity cannot be easily categorized into specific theoretical frameworks, as various schools of thought offer different arguments concerning both the desirability and practicality of such cooperation"* (p. 198).

This interpretation illustrates how cybersecurity is conceptualized in international politics and how it exposes theoretical contradictions across different schools of thought. From a neorealist perspective, cybersecurity is perceived as an essential dimension of national security, where states manage cyber threats in alignment with their own interests, often resorting to unilateral strategies. Within this framework, disinformation is likewise understood as a political and strategic weapon deployed by states against their adversaries.

**Conclusion**

In the evolving landscape of global power competition, information has become a strategic asset, and its weaponization through cyberattacks and disinformation marks a new era of geopolitical confrontation. Infoimperialism, as demonstrated by the systemic use of digital tools to influence narratives, destabilize institutions, and challenge state sovereignty, is no longer a theoretical concept but a lived geopolitical reality. The proliferation of cyber threats against both governmental and private infrastructures—alongside the manipulation of public opinion via disinformation—reveals a growing asymmetry in international relations, where power is increasingly exercised in virtual domains.

For mid-sized and vulnerable states like Azerbaijan, the intersection of cybersecurity and strategic communication underscores a critical national priority: safeguarding not only territorial integrity but also cognitive and informational sovereignty. Addressing this challenge demands more than defensive technical solutions; it requires a multidimensional strategy involving diplomatic coordination, institutional capacity-building, and international legal engagement. In this regard, cybersecurity cooperation and the establishment of binding global standards become not just desirable, but essential to maintaining a balanced and secure international order.

Ultimately, the battle for narrative dominance and digital sovereignty is not confined to the realm of technology—it is a contest over values, legitimacy, and the architecture of the emerging world order. States must act decisively to secure their information ecosystems while contributing to a fairer and more transparent global digital governance framework. Failure to do so risks entrenching structural inequalities and perpetuating new forms of digital colonialism under the guise of connectivity and develop

**References**

Abbasi, M. (2021). Security in cyberspace in the field of international relations. *Journal of Archives in Military Medicine*. https://www.researchgate.net/publ

Babaoğlu, H. (2013). İnfoimperializm və media [Infoimperialism and media]. MSA. (in Azerbaijani).

Bizim Media. (2021, August 2). Kibermüharibədən "kiberterrorizm"ə keçid – ABŞ nəyi anons edir? *Bizim Media*. https://bizim.media/az/siyaset/30861/kiber- (in Azerbaijani)

Cəbrayılov, M. (2019). Müasir geosiyasi proseslərdə informasiya amili [The information factor in modern geopolitical processes]. In *Müasir dünya və informasiya cəmiyyəti* [Modern world and information society] (Vol. 1, pp. 45–60). AFPoliqrAF. (in Azerbaijani).

Cyber Warfare to Cyber Terrorism. (2021, August 2). *Bizim Media*. https://bizim.media/az/siyaset/30861/kiber-muharibeden-kib

Goodman, S. E., Kirk, J. C., & Kirk, M. H. (2007). Cyberspace as a medium for terrorists. *Technological Forecasting and Social Change, 74*(2), 193–210.

Holms, M., & Bjola, K. (2015). Tsifrovaya diplomatiya: teoriya i praktika [Digital diplomacy: Theory and practice]. (in Russian).

Kastels, M. (2000). Informatsionnaya epokha: ekonomika, obshchestvo i kultura [The information age: Economy, society, and culture]. GU VShE. (in Russian).

Suxanov, A. P. (1988). Informatsiya i progress [Information and progress]. Nauka. (in Russian)

U.S. Agency for International Development, Office of Inspector General. (2025, January 28). *Memorandum: Challenges to accountability and transparency within USAID-funded programs*. https://oig.usaid.gov/node/7399

U.S. Department of State. (2010). *IT strategic plan: Fiscal years 2011–2013 – Digital diplomacy*. https://2009-2017.state.gov/m/irm/rls/148572.htm

USAID: A corruption hub for sinister plans. (2025, March 15). *Eurasia Review*. https://www.eurasiareview.com/example-link