

# საინფორმაციო ომები და თანამდროვეობა

ეკა თხილავა  
კავკასიის საერთაშორისო უნივერსიტეტი;  
სოციალურ მეცნიერებათა დოქტორი

მაია ეკალაძე  
კავკასიის საერთაშორისო უნივერსიტეტის დოქტორანტი

<https://doi.org/10.52340/gbsab.2026.57.03>

**საკვანძო სიტყვები:** საინფორმაციო ომი, მედია მანიპულირება, ელექტრონული ომი, ფსიქოლოგიური ოპერაციები, დეზინფორმაცია, პროპაგანდა, კიბერთავდასხმები, უსაფრთხოება.

## შესავალი

ჩვენ ვცხოვრობთ ეპოქაში, სადაც ყველაფერი ურთიერთდაკავშირებულია. სიახლეები და ინფორმაცია მილიონობით ადამიანამდე ერთ წამზე ნაკლებ დროში აღწევს. თუმცა ინტერნეტში არსებული ყველა ინფორმაცია 100%-ით ნამდვილი არ არის - ხშირად ინფორმაცია გამოიყენება მრავალი ფორმით. წინამდებარე კვლევის მიზანია, წარმოაჩინოს, რა საფრთხეებკონკრეტული საკითხის ნაწილობრივი ან სრული გაყალბების მიზნით (García, 2020). საინფორმაციო ომი ფარავს ჩვენი საზოგადოების ყველასფეროსდა ის შეიძლება გამოვლინდეს სშეიცავს საინფორმაციო ომები და რამდენად მართლდება ჯიმ მორისონის ცნობილი მოსაზრება: „ვინც მართავს ინფორმაციის საშუალებებს, ის მართავს ადამიანთა გონს.“

## თეორიული ჩარჩო

საკითხის კვლევისთვის თეორიულ ჩარჩოდ გამოვიყენეთ კომუნიკაციის

ტექნოლოგიური დეტერმინიზმის თეორია, რომელიც რეღევანტურად მივიჩნიეთ მოცემული საკითხის შესასწავლად. აღნიშნული თეორია არის მედიასაზოგადოების თეორიის ერთ-ერთი ყველაზე აქტუალური და ყოველდღიურად განვითარებადი (მედიური ტექნოლოგიების განვითარების კვალდაკვალ) ნაირსახეობა. თეორიის ეს ტიპი ეძიებს, ავლენს და იკვლევს ურთიერთკავშირებს ეპოქის დომინანტურ საკომუნიკაციო ტექნოლოგიასა და საზოგადოების ძირითად მახასიათებლებს შორის. ჩვენი კვლევისთვის მნიშვნელოვანი იყო ამ თეორიის არქიტექტონიკაში მედიატექნოლოგიის ცენტრალური როლი და მისი გავლენა საზოგადოების სხვადასხვა სფეროზე.

## შინაარსი

ტერმინი „საინფორმაციო ომი“ ამერიკული კონცეფციაა; იგი მოიცავს მოწინააღმდეგეზე უპირატესობის მოსაპოვებლად საინფორმაციო ტექნოლოგიების (სატელეკომუნიკაციო და კომპიუტერული მოწყობილობები) გამოყენებასა და მენეჯმენტს. საინფორმაციო ომი შესაძლოა, მოიცავდეს მიღებული ინფორმაციის ვალიდურობის დადასტურებას, ტაქტიკური ინფორმაციის მოპოვებას, დეზინფორმაციისა და პროპაგანდის გავრცელებას - მოწინააღმდეგისა და

საზოგადოების მანიპულაციისთვის ან დემორალიზებისთვის; მოწინააღმდეგისთვის ხელის შეშლას სარწმუნო ინფორმაციის მოპოვებაში.

ინფორმაცია და დეზინფორმაცია საუკუნეების განმავლობაში გამოიყენებოდა ადამიანთა გონების, ნებისა და ცნობიერების დასაპყრობად. ე.წ. ექსპლუატატორებსა და ექსპლუატირებულთა შორის საუკუნოვანი ბრძოლის განუყოფელ ნაწილს იღებდა ბრძოლა წარმოადგენს. საინფორმაციო ომის სამიზნე აუდიტორიად შეიძლება მოიაზრებოდეს საკუთარი, მოწინააღმდეგე თუ ნეიტრალური ქვეყნების სამოქალაქო მოსახლეობა. საინფორმაციო ომი (GI) შედარებით ახალი კონცეფციაა, რომელსაც, გარკვეული თვალსაზრისით, ემყარება თანამედროვე ომი; პარადოქსულია, მაგრამ ეს ელემენტი - ინფორმაცია - უძველესი დროიდანვე იყო ჩართული ადამიანთა ომებში. მეტიც, ის მუდამ იყო ნებისმიერი სადაზვერვო პროცესის ნედლეული და ყველა სამხედრო საქმიანობაც მასთანაა დაკავშირებული.

## **ისტორიული ველი**

ცხადია, საინფორმაციო ომი ახალ მოვლენად ვერ ჩაითვლება; მის შემადგენელი ელემენტების უმეტესობა საბრძოლო ხელოვნების ისტორიაშია ფესვებგადგმული. ამასთან, საინფორმაციო ომები ფსიქოლოგიური ოპერაციების ფარგლებშიც გამოიყენებოდა; ის განსაზღვრავდა მოწინააღმდეგის შესაძლებლობებისა და განზრახვების შესახებ ინფორმაციის მოპოვებას, საკუთარი შესაძლებლობებისა და განზრახვების შესახებ ინფორმაციის უარყოფას, დეზინფორმაციას, შეცდომაში შეყვანასა და ინფორმაციასთან პირდაპირ დაკავშირებულ სხვა მრავალ ქმედებას (Riquelme, 2012).

## **ინფორმაცია, როგორც „რესურსი, იარაღი, სამიზნე“**

თანამედროვე ტექნოლოგიურმა პროგრესმა მარტივი გახადა ინფორმაციაზე წვდომა. სამხედრო და სამოქალაქო სისტემებზე ინფორმაციის მართვის ტექნოლოგიების დამოკიდებულებაც სულ უფრო იზრდება; ამ დამოკიდებულებამ შესაძლებელი გახადა ახალი მოწყვლადობებისა და სუსტი წერტილების იდენტიფიცირება, რამაც განაპირობა ახალი ტექნოლოგიებისა და მათი კონტროლის განვითარება.

საინტერესოა, რომ პოლიტიკური ლიდერები დაინტერესებულნი არიან იმ ომებით, რომლებიც მოკლე, ნაკლებხარჯიანი და ადამიანური მსხვერპლის მხრივ მინიმალური იქნება.

შედეგად, ინფორმაციის როლი ომის პროცესების წარმართვაში უმნიშვნელოვანესია; ის გარდაიქმნა „რესურსად, იარაღად და სამიზნედ“; მეტიც, ინფორმაციას შეუძლია კონფლიქტის ბედის განსაზღვრა საბრძოლო მოქმედებების დაწყებამდეც.

ახალი ტექნოლოგიების გამოყენება „ინფორმაციული უპირატესობის მისაღწევად, მოწინააღმდეგის საინფორმაციო სისტემებზე ზემოქმედებისა და საკუთარი სისტემების დაცვის“ მიზნით - ეს არის ის, რასაც საინფორმაციო ომი ეწოდება (Badillo, 2019).

საინფორმაციო ომის კონცეფციად შეიძლება განიხილებოდეს ინფორმაციის გამოყენება და მართვა მოწინააღმდეგეზე კონკურენტული უპირატესობის მოპოვების მიზნით.

## საინფორმაციო ომების საფრთხეები

საინფორმაციო ომი ჰიბრიდული ომების ერთგვარი შემადგენელი ნაწილია; მეტიც, ითვლება, რომ ის სამხედრო ოპერაციების თანადროული მოქმედებაცაა. რასაკვირველია, საინფორმაციო ომები ტარდება გარკვეულ მასებზე აზრის შესაცვლელად, მაგრამ სახესა და ფორმას იცვლის დროისა და იმ რეჟიმების მიხედვით, რომელშიც ის მიმდინარეობს.

ავტორიტარულსა და ტოტალიტარულ გარემოში მთავრობები საინფორმაციო ომებს იყენებენ საკუთარი მოსახლეობის საწინააღმდეგოდ; ესელოგიკურიცაა, ვინაიდან ასეთი რეჟიმები, უპირველესად, დგას სწორედ დეზინფორმაციასა და პროპაგანდაზე. ამ საფრთხეებთან გამკლავება უმთავრესი გამოწვევაა დღევანდელი დროის. მით უფრო, რომ საინფორმაციო ომები გავლენას ახდენს ქვეყანათა როგორც პოლიტიკურ, ასევე ეკონომიკურსა და სოციალურ სტაბილურობაზე; შედეგად ვიღებთ ხალხის ნდობის შემცირებასა და საზოგადოების პოლარიზებას.

ციფრული ტექნოლოგიების ეპოქაში დეზინფორმაცია და პროპაგანდა კიდევ უფრო სახიფათო გახდა, რადგან ურთულესია საინფორმაციო სივრცის დაცვა სიყალბეებისაგან.

თუმცა, არსებობს კონტრ-საინფორმაციო ომის ქვედანაყოფები, რომელთა მიზანია, ხელი შეუშალოს მოწინააღმდეგეს ყალბი ინფორმაციის გავრცელებაში.

ასეთი საშუალებების გამოყენება პირველად მოხდა სპარსეთის ყურის ომში, ერაყის საკომუნიკაციო ქსელების წინააღმდეგ. სხვათა შორის, ამავე ომში ჰოლანდიელმა ჰაკერებმა ინფორმაცია მოიპარეს თავდაცვის დეპარტამენტის კომპიუტერებიდან შეერთებული შტატების ჯარების გადაადგილების შესახებ და სცადეს, ისინი ერაყელებისთვის მიეყიდათ; მაგრამ ამ უკანასკნელებმა ჩათვალეს, რომ ამერიკელები ხაფანგს უგებდნენ და მათ დეზინფორმირებას ცდილობდნენ.

## საინფორმაციო ომების მიზნები

საინფორმაციო ომების მიზანია სამშვიდობო და სამხედრო პერიოდში სამოქალაქო და სამხედრო სარგებლობის საინფორმაციო სისტემებზე ზემოქმედება; კონკრეტულად:

- მოწინააღმდეგის შესახებ ინფორმაციის ფარულად მოპოვება;
- მოწინააღმდეგის მიერ მოპოვებული და შენახული ინფორმაციის ცვლილება ან გაყალბება მისი შეცდომაში შეყვანის მიზნით;
- კონკრეტული მიზნების მისაღწევად, მოწინააღმდეგის მიერ მოპოვებული სრულიად მცდარი ან ნაწილობრივ სიმართლის შემცველი, გულდასმით შერჩეული ინფორმაციით დეზინფორმირება;
- მოწინააღმდეგის ინფორმაციის, ინფორმაციაზე დაფუძნებული პროცესების ან/და საინფორმაციო სისტემების ფიზიკური განადგურება;
- მოწინააღმდეგის საინფორმაციო სისტემებისათვის საჭირო ელემენტების ან სერვისების ხელმიუწვდომლობა.

## დეზინფორმაცია

დეზინფორმაციაში იგულისხმება გარკვეული მოქმედებები ან უმოქმედობა, რომელთა საშუალებითაც ფაქტები (სიმართლე) იმალება; ის კონტექსტიდან ამოგდებულია ან განზრახ გაყალბებულია არასათანადო მიზნებისათვის.

დეზინფორმაცია ორი ძირითადი მეთოდით ხორციელდება:

1. ფაქტების (სიმართლის) უარყოფა და დამალვა;
2. ფსევდოინფორმაცია - მცდარი, კონტექსტიდან ამოგდებული ან შეუსაბამო მონაცემებისა და ფაქტების გავრცელება.

მასობრივი დეზინფორმაცია, როგორც ძალაუფლების ინსტრუმენტი, რომელიც ხორციელდება მასობრივი ინფორმაციის საშუალებათა ბოროტად გამოყენებით, საფრთხეს წარმოადგენს მშვიდობისათვის და წარმოქმნის საერთაშორისო და ეროვნული უსაფრთხოების პრობლემებს.

დეზინფორმაციის ფლაგრანტული გამოყენების ძირითადი მიმართულებებია:

1. აგრესიული ომების, ეთნიკური გენოციდისა და სხვა ფორმის მასობრივი ძალადობის გამართლება და ხელშეწყობა;
2. მოსახლეობის შეშინება არარსებული ან გაზვიადებული საფრთხეებითა და რისკებით - ტერორიზმის ფორმით;
3. პროგრესული ლიდერების, პარტიების, ორგანიზაციებისა და მთავრობების დიფამაცია, დემონიზაცია, შეტევა და დესტაბილიზაცია;
4. რევოლუციური ან პროგრესული პროცესებისა და მათზე განხორციელებული თავდასხმების შესახებ სიმართლის დამალვა;
5. კონსტიტუციური მთავრობების წინააღმდეგ სახელმწიფო გადატრიალებების ხელშეწყობა, გამართლება და მხარდაჭერა;
6. სოციალური, ეკონომიკური და პოლიტიკური სისტემებისათვის საფრთხეების შექმნა.

## **ციფრული ინსტრუმენტები და ფსიქოლოგიური ზეგავლენები**

ციფრული ინსტრუმენტებით შესაძლებელი ხდება ყალბი სიტუაციების შექმნა; ამ გზით ფსიქოლოგიურ ზეგავლენას ახდენენ სამიზნე ჯგუფებზე და იწვევენ მოსახლეობის სუბვერსიასა და ინსურგენციას.

ინტერნეტი, მაგალითად, საშუალებას იძლევა, ინფორმაცია მიეწოდოს ერთდროულად მილიონობით ადამიანს; და თუ ინფორმაცია ყალბია, მაშინ დეზინფორმაციით „ვირუსდება“ უამრავი პირი.

თანამედროვე საინფორმაციო ომში უფრო მნიშვნელოვანია ვიცოდეთ, რას მალავს ესა თუ ის ინფორმაცია, ვიდრე მისი პირდაპირი შინაარსი. შინაარსი ყველასათვის ხელმისაწვდომია, ის კი, რასაც ინფორმაცია მალავს - არა. ომში უპირატესობას იძლევა არა საიდუმლო ინფორმაცია, არამედ არამატერიალური რესურსების ათვისება.

## **ყალბი ინფორმაციების ამოცნობის კრიტერიუმები**

ინტერნეტში ყალბი ინფორმაციების ამოცნობისათვის შეიძლება, გამოვიყენოთ შემდეგი კრიტერიუმები:

- ანონიმურობა: ყალბი ინფორმაციების უმეტესობა უსახელოა, არ ციტირებს წყაროებს (ვინაიდან ისინი არ არსებობს) და ხელმოუწერელია სამართლებრივი შედეგების თავიდან ასაცილებლად;
- თარიღი: არ არის მითითებული თარიღი; ტემპორალური ფორმით არის დაწერილი, რათა ინტერნეტში შეძლებისდაგვარად დიდხანს ცირკულირებდეს;
- „ხაფანგი“: ყალბი ინფორმაცია შეიცავს „ხაფანგს“ - რაც მეტია მასში საცდური, ფულის მომტანი ან შიშის გამომწვევი ელემენტი, მით მეტია მისი გავრცელების ალბათობა.

ყალბი ინფორმაცია (Fake News ან Hoax) წარმოადგენს ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების გამოყენებით გადაცემულ ცრუ ან შეცდომაში შემყვანი შინაარსის შეტყობინებებს. ჩვეულებრივ, ისინი ჯაჭვური რეაქციით ვრცელდება შოკისმომგვრელი შინაარსის ან იმის გამო, რომ შეტყობინება მოითხოვს გადაგზავნას (Pennycook & Rand, 2021).

საინფორმაციო ომი, ასევე, შეიძლება მოიცავდეს:

- ტაქტიკური ინფორმაციის შეგროვებას;
- ინფორმაციის სიზუსტის დადასტურებას;
- პროპაგანდის ან დეზინფორმაციის გავრცელებას მოწინააღმდეგის მორალის შესარყევად;
- მოწინააღმდეგის საინფორმაციო სისტემების ხარისხის შემცირებას;
- მოწინააღმდეგისათვის ინფორმაციის შეგროვების შესაძლებლობის აღკვეთას.

## დასკვნა

საინფორმაციო ომი ყოვლისმომცველი და დეზინტეგრაციული ფენომენი გახდა თანამედროვე საზოგადოებაში. ციფრულ პლატფორმებზე ინფორმაციის მანიპულაციის გზით ღრმა ზეგავლენა ხდება საზოგადოებრივ აზრსა და სოციალურ ქცევაზე, რაც პოლიტიკურ პოლარიზაციას აძლიერებს და ინსტიტუტებისადმი ნდობასაც ძირს უთხრის. ყოველივე ეს მნიშვნელოვან საფრთხეს უქმნის გამჭვირვალობას, ეროვნულ უსაფრთხოებას და გამოიყენება საერთაშორისო კონფლიქტებისა და ჰიბრიდული ომების იარაღად.

ციფრულ ტექნოლოგიებზე მზარდი დამოკიდებულება ზრდის მანიპულაციისა და კიბერშეტევებისადმი მოწყვლადობას, რაც ადასტურებს, რომ აუცილებელია ციფრული წიგნიერების გაუმჯობესება, კიბერუსაფრთხოების განმტკიცება და ციფრული პლატფორმების რეგულირება. ამ საფრთხეებთან გამკლავება მოითხოვს გლობალური მასშტაბის ჩართულობას კიბერსივრცეში ინფორმაციის დაცვისათვის.

## ბიბლიოგრაფია

1. Badillo, A. (2019). The society of disinformation: Propaganda, “fake news” and the new geopolitics of information. Working Paper, 8, 2019–14.
2. García, J. (2020). The grand manipulation: How disinformation turned Spain into a coronavirus paradise. The Sphere of Books.
3. Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. Trends in Cognitive Sciences, 25(5), 388–402.
4. Riquelme, E. J. (2012). The influence of the information war in a theater of operations

## აბსტრაქტი

საინფორმაციო ომი მრავალმხრივი ფენომენია და ის განსაკუთრებულ პრომინენტულობას იძენს ციფრულ ეპოქაში.

საინფორმაციო ომი, უპირველესად, გამოიყენება საზოგადოებრივი აზრის მანიპულირების მიზნით.

ჩვენი ნაშრომი განიხილავს საინფორმაციო ომს, მის წანამძღვრებსა და

მახასიათებლებს, ასევე, მის ზეგავლენას საზოგადოებაზე; შესწავლილია, როგორ ზემოქმედებს ყალბი ინფორმაციები (Fake News) საომარ პროცესებზე; განხილულია პროპაგანდისა და დეზინფორმაციის მავნე გავლენებიც.

## **INFORMATION WARS AND MODERNITY**

**Eka Tkhilava**  
**Caucasus International University;**  
**PHD**

**Maia Ekaladze**  
**PHD, Caucasus International University**

### **Abstract**

Information warfare is a complex phenomenon that is gaining particular prominence in the digital age.

Information warfare is primarily used to manipulate public opinion. Our paper examines information warfare, its origins and characteristics, and its impact on society; examines how fake news affects war processes; and discusses the harmful effects of propaganda and disinformation.

**Keywords:** information warfare, media manipulation, electronic warfare, psychological operations, disinformation, propaganda, cyberattacks, security.