

სოციალური ქსელები როგორც ინფორმაციული ომის იარაღი: ზეგავლენა, მეთოდები და პრევენცია

ლევან ჭოლიკიძე¹

ლაშა ნოზაძე²

<https://doi.org/10.61446/pa.3.2025.10286>

აბსტრაქტი

სოციალურმა ქსელებმა ფუნდამენტურად შეცვალეს ინდივიდების, ბიზნესებისა და სახელმწიფოების კომუნიკაციისა და ურთიერთქმედების ფორმა. ეს ციფრული პლატფორმები უზრუნველყოფენ გლობალურ, რეალურ დროში კავშირს, რაც საშუალებას აძლევს მომხმარებლებს გააზიარონ იდეები, ჩაერთონ დისკუსიებში და მიიღონ ინფორმაცია მყისიერად. თუმცა, სოციალური ქსელები დღეს აღარ წარმოადგენენ მხოლოდ კომუნიკაციის ინსტრუმენტებს - ისინი გადაიქცნენ მნიშვნელოვან აქტორებად ეკონომიკურ, პოლიტიკურ და უსაფრთხოების სფეროებში. ნაშრომი იკვლევს სოციალური ქსელების მრავალმხრივ როლს, მათ გავლენას საზოგადოებაზე, მათი გამოყენების შესაძლებლობებს საინფორმაციო ომებში და იმ საჭირო ზომებს, რომლებიც უნდა იქნას მიღებული არსებული რისკების შესამცირებლად. პირველი ნაწილი მიმოიხილავს უმსხვილეს სოციალურ ქსელებს, მათ შორის Facebook, Twitter (X), Instagram, Telegram, TikTok, WhatsApp, LinkedIn და Snapchat. თითოეული პლატფორმა სხვადასხვა დემოგრაფიულ ჯგუფს მოიცავს და უნიკალურ ფუნქციებს ასრულებს, დაწყებული მულტიმედიური კონტენტის გაზიარებით და დამთავრებული დამიჯნული მესიჯინგით. აღნიშნული პლატფორმები მნიშვნელოვან გავლენას ახდენენ ისეთ სფეროებზე, როგორებიცაა ბიზნესი, განათლება, პოლიტიკა, აქტივიზმი და უსაფრთხოება. სოციალური ქსელები აძლიერებენ ბიზნესს, რადგან კომპანიებს პირდაპირი მარკეტინგული არხებით მომხმარებელთან კავშირის შესაძლებლობას აძლევს, ცვლიან ტრადიციულ რეკლამირებას და ქმნიან ახალ ელექტრონული კომერციის შესაძლებლობებს. თუმცა, მათი გავლენა ვრცელდება პოლიტიკურ პროცესებზე, საზოგადოებრივ მოძრაობებზე და, გარკვეულ შემთხვევებში, მანიპულაციასა და კიბერ-მუქარებზეც. სოციალური ქსელების განვითარებამ საზოგადოებასთან ერთად, როგორც დადებითი, ასევე უარყოფითი შედეგები მოიტანა. ერთი მხრივ, სოციალური მედია ხელს უწყობს კომუნიკაციას, ციფრული განათლების განვითარებას და ინფორმაციის ხელმისაწვდომობას. მეორე მხრივ, ის აძლიერებს დეზინფორმაციის გავრცელებას, კიბერბულინგს, კონფიდენციალურობის პრობლემებს და პოლიტიკურ პოლარიზაციას. ალგორითმების უნარი, რომ მომხმარებელს მიაწოდოს სენსაციური და პოპულარული შინაარსი, კიდევ უფრო ამწვავებს ამ პრობლემებს, ქმნის ე.წ. "ექო კამერებს" და ხელს უწყობს პროპაგანდის გავრცელებას. კვლევის ერთ-ერთი ცენტრალური საკითხია სოციალური ქსელების ტრანსფორმაცია საინფორმაციო ომების ინსტრუმენტებად. სახელმწიფოები, ორგანიზაციები და არასახელმწიფოებრივი აქტორები სულ უფრო ხშირად იყენებენ სოციალურ მედიას ციფრული გავლენის ოპერაციებისთვის, პროპაგანდის გასავრცელებლად და სტრატეგიული დეზინფორმაციის კამპანიებისთვის. საინფორმაციო ომი მოიცავს პოლიტიკურ, ეკონომიკურ და სამხედრო დომენებს, სადაც მნიშვნელოვან როლს ასრულებენ ღრმა ყალბი (deepfake) ტექნოლოგიები, კიბერ-ჯაშუშობა და ფსიქოლოგიური ოპერაციები. სოციალური ქსელების საშუალებით ხორციელდება საზოგადოებრივი აზრის მანიპულირება, არჩევნებში ჩარევა და მმართველობის დესტაბილიზაცია კოორდინირებული ყალბი ქცევის (CIB) და ბოტ-ქსელების მეშვეობით. სოციალური ქსელებით მართული საინფორმაციო ომის გავლენა ვრცელდება პოლიტიკურ დესტაბილიზაციაზე, საზოგადოებრივ პოლარიზაციაზე, ეკონომიკურ შედეგებზე და ეროვნულ უსაფრთხოებაზე. დეზინ-

¹ სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიის ინფორმატიკის მიმართულების ასოცირებული პროფესორი, ინფორმატიკის მეცნიერებათა აკადემიური დოქტორი

² სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიის ინფორმატიკის მიმართულების ასისტენტ პროფესორი

ფორმაციის კამპანიები ხელს უწყობს დემოკრატიული ინსტიტუტების მიმართ ნდობის შენარჩუნებას, სამოქალაქო არეულობების აღფრთოვანებას და საზოგადოებრივი დაპირისპირების გაძლიერებას. სოციალურ ქსელებში პოლიტიკური და ეკონომიკური მანიპულაციები აზარალებს საზოგადოებრივ სტაბილურობას, ზიანს აყენებს ბიზნესის რეპუტაციას და იწვევს მომხმარებელთა პანიკას, რაც ფინანსური კრიზისების წინაპირობა ხდება. გარდა ამისა, ეროვნული უსაფრთხოების რისკები მოიცავს კიბერჯაშუშობას, სადაზვერვო ინფორმაციის გაჟონვასა და ფსიქოლოგიური ომის ტექნიკებს, რომლებიც არყევენ ნდობას სამხედრო და სახელმწიფო ინსტიტუტების მიმართ.

ამ გამოწვევების გადასაჭრელად, ნაშრომი განიხილავს სხვადასხვა პრევენციულ ზომებსა და თავდაცვით სტრატეგიებს. ძირითადი გადაწყვეტილებები მოიცავს ხელოვნური ინტელექტის (AI) გამოყენებას დეზინფორმაციის ამოსაცნობად, კონტენტის მოდერაციის პოლიტიკას, მთავრობის რეგულაციებს, საზოგადოებრივი ცნობიერების ამაღლების ინიციატივებსა და საერთაშორისო თანამშრომლობას. AI-ით მართული ფაქტჩეკინგის ინსტრუმენტები, დეზინფორმაციის რეალურ დროში მონიტორინგი და ეთიკური AI-ის მართვის მოდელები აუცილებელია ცრუ ინფორმაციის გავრცელების შესაჩერებლად. ასევე, უნდა გაძლიერდეს კიბერუსაფრთხოების პოლიტიკა, რათა დაიცვას პერსონალური მონაცემები, თავიდან აიცილოს კიბერთავდასხმები და დაარეგულიროს სოციალური მედიის როლი ეროვნულ უსაფრთხოებაში. ციფრული წიგნიერების პროგრამებიც გადამწყვეტია მოქალაქეების განათლებისთვის, რათა მათ შეძლონ დეზინფორმაციის ამოცნობა და მის წინააღმდეგ ბრძოლა. სოციალური ქსელების მომავალი, სავარაუდოდ, მოიცავს რეგულაციების გამკაცრებას, AI-ით მართული მოდერაციის გაუმჯობესებას და დეზინფორმაციის ტაქტიკების განვითარებას. მიუხედავად იმისა, რომ ტექნოლოგიური პროგრესი ახალ შესაძლებლობებს ქმნის გლობალური კომუნიკაციისა და ეკონომიკური ზრდისთვის, მას თან ახლავს რთული ეთიკური და უსაფრთხოების გამოწვევები. სოციალური ქსელების როლის გააზრება კრიტიკულად მნიშვნელოვანია იმისთვის, რომ სახელმწიფოებმა, ბიზნესებმა და ინდივიდებმა შეძლონ ციფრული სივრცის პასუხისმგებლიანად გამოყენება და განვითარებადი საფრთხეებისგან დაცვა. ეს ნაშრომი კომპლექსურ ანალიზს უტარებს სოციალური ქსელების როლს თანამედროვე საზოგადოებაში, ხაზგასმით აღნიშნავს მათ გავლენას, მოწყვლადობას და სტრატეგიულ მნიშვნელობას თანამედროვე საინფორმაციო ომების კონტექსტში. რეალურ მაგალითებზე, ისტორიულ ტენდენციებზე და ახალ კიბერუსაფრთხოების გადაწყვეტილებებზე დაყრდნობით, კვლევა ხელს უწყობს ციფრული მმართველობისა და სოციალური მედიის პასუხისმგებლიანი გამოყენების დისკურსის განვითარებას.

საკვანძო სიტყვები: სოციალური ქსელები, საინფორმაციო ომი, დეზინფორმაცია, კიბერშეტევა, ღრმა ყალბი (deepfake), ფსიქოლოგიური ოპერაციები, კიბერუსაფრთხოება

Social Networks as Weapons of Information Warfare: Impact, Methods, and Prevention

Levan Cholikidze³

Lasha Nozadze⁴

Abstract

Social networks have fundamentally reshaped the way individuals, businesses, and governments communicate, interact, and influence public discourse. These digital platforms facilitate real-time global connectivity, enabling users to share ideas, engage in discussions, and access information instantaneously. However, social networks have evolved beyond personal communication tools to become significant actors in economic, political, and security landscapes. This paper explores the multifaceted role of social networks, analyzing their impact on society, their potential as instruments of information warfare, and the necessary countermeasures required to mitigate associated risks. The first section provides an overview of major social networks, including Facebook, Twitter (X), Instagram, Telegram, TikTok, WhatsApp, LinkedIn, and Snapchat. Each platform caters to different demographics and serves unique functions, ranging from multimedia content sharing to encrypted messaging. These platforms influence various societal aspects, including business, education, politics, activism, and security. Social networks empower businesses by offering direct marketing channels, reshaping traditional advertising, and providing e-commerce opportunities. However, their influence extends beyond commerce into political engagement, social movements, and, in some cases, manipulation through misinformation and cyber threats. The rise of social networks has led to both positive advancements and significant challenges. On one hand, social media fosters enhanced connectivity, digital literacy, and open access to information. On the other hand, it contributes to misinformation, cyberbullying, privacy concerns, and political polarization. The ability of social media algorithms to prioritize sensational content exacerbates these challenges by reinforcing ideological echo chambers and enabling the spread of propaganda. A key theme explored in this research is the transformation of social networks into tools for information warfare. Governments, organizations, and non-state actors have increasingly leveraged social media for digital influence operations, propaganda dissemination, and strategic misinformation campaigns. Information warfare is categorized into political, economic, and military domains, with tactics such as deepfake technology, cyber espionage, and psychological operations playing a critical role. Social networks have been used to manipulate public opinion, interfere in elections, and disrupt governance through coordinated inauthentic behavior (CIB) and bot networks. The impact of information warfare extends to various societal dimensions, including political destabilization, social polarization, economic consequences, and national security threats. Disinformation campaigns have been utilized to undermine trust in democratic institutions, fuel civil unrest, and amplify societal divisions. Election interference, coordinated propaganda, and misinformation targeting specific communities have exacerbated political and social tensions globally. Economic ramifications of social media-based disinformation include market manipulation, corporate reputation damage, and consumer panic, leading to financial instability. National security risks include cyber espionage, intelligence leaks, and psychological warfare tactics that weaken public trust in military and governmental institutions. To address the challenges posed by social media-based information warfare, this paper explores various countermeasures and mitigation strategies. Key solutions include the implementation of artificial intelligence (AI) for misinformation detection, content moderation policies, government regulations, public awareness initiatives, and international collaboration. AI-driven fact-checking tools, real-time disinformation tracking systems, and ethical AI governance models are essential in mitigating the spread of false information. Additionally, cybersecurity policies must be strengthened to protect personal data, prevent cyberattacks, and regulate social media's role in national

³Associate Professor of Bachelor's program in Informatics of LEPL David Aghmashenebeli National Defence Academy of Georgia, Doctor of Computer Science

⁴Associate Professor of Bachelor's program in Informatics of LEPL David Aghmashenebeli National Defence Academy of Georgia, Doctor of Computer Science

security affairs. Digital literacy programs are also critical in equipping citizens with the skills to identify and combat misinformation. The future of social networks will likely involve increased regulatory oversight, AI-driven moderation, and evolving disinformation tactics. While technological advancements present new opportunities for global communication and economic growth, they also pose complex ethical and security challenges. Understanding the evolving role of social networks is essential for governments, businesses, and individuals to navigate the digital landscape responsibly and safeguard against emerging threats. This research provides a comprehensive analysis of the role of social networks in modern society, emphasizing their influence, vulnerabilities, and strategic significance in contemporary information warfare. By examining real-world case studies, historical trends, and emerging cybersecurity solutions, this study aims to contribute to the ongoing discourse on digital governance and the responsible use of social media platforms.

Keywords: Social networks, information warfare, disinformation, Cyber attack, Deepfake, psychological operations, Cybersecurity.

შესავალი

21-ე საუკუნეში სოციალური ქსელები თანამედროვე საზოგადოების ერთ-ერთ ყველაზე გავლენიან ძალად იქცა. თავდაპირველად, ისინი შეიქმნა როგორც პლატფორმები კომუნიკაციისა და კონტენტის გასაზიარებლად, თუმცა სწრაფადვე გადაიქცა ეკონომიკური განვითარების, პოლიტიკური ჩართულობისა და საინფორმაციო ომის ინსტრუმენტებად. სოციალური მედიის სწრაფმა გაფართოებამ ფუნდამენტურად შეცვალა ინდივიდთა ურთიერთქმედება, ბიზნესის ფუნქციონირება და სახელმწიფოთა კომუნიკაციის მეთოდები, რაც როგორც ახალ შესაძლებლობებს, ისე მნიშვნელოვან გამოწვევებს ქმნის. ამ პლატფორმებმა უზრუნველყოფს ინფორმაციის უპრეცედენტო ხელმისაწვდომობას და გლობალურ კავშირებს, მაგრამ ამავდროულად წარმოშობს ისეთ საფრთხეებს, როგორიცაა დეზინფორმაცია, კონფიდენციალურობის დარღვევა, სოციალური პოლარიზაცია და კიბერ-მუქარა.

სოციალური ქსელები, როგორიცაა Facebook, Twitter (X), Instagram, Telegram, TikTok, WhatsApp და LinkedIn, მილიარდობით მომხმარებელს აერთიანებს და კრიტიკულ როლს ასრულებს საზოგადოებრივი აზრის ფორმირებაში, არჩევნებზე ზემოქმედებაში და გლობალური ბაზრების ცვლილებაში. სოციალური ქსელების გავლენა სცილდება პირად კომუნიკაციას და მოიცავს კორპორატიულ ბრენდინგს, ციფრულ აქტივიზმს, ელექტრონულ კომერციასა და პოლიტიკურ მობილიზაციას. თუმცა, ამავე დროს, ეს პლატფორმები გამოყენებულა საზიანო მიზნებისთვის, მათ შორის პროპაგანდის გავრცელებისთვის, კიბერ-ჯაშუშობისთვის, საარჩევნო მანიპულაციებისთვისა და ფსიქოლოგიური ოპერაციებისთვის. სახელმწიფოები, სადაზვერვო სააგენტოები და არახელმწიფოებრივი აქტორები სულ უფრო მეტად იყენებენ სოციალურ ქსელებს სტრატეგიული გავლენის ოპერაციებისთვის, რაც ახალ საფრთხეებს ქმნის ეროვნული უსაფრთხოებისა და დემოკრატიული პროცესებისთვის.

ძირითადი ნაწილი

სოციალური ქსელების ევოლუციის ანალიზი

ფუნქციების ინტეგრაცია და მომხმარებლის ჩართულობა

სოციალური ქსელები თავდაპირველად შეიქმნა, როგორც კომუნიკაციის, კონტენტის გაზიარებისა და ადამიანების დაკავშირების პლატფორმები. თუმცა, დროთა განმავლობაში ისინი გადაიქცნენ ინფორმაციული მანიპულაციის, პროპაგანდის და გავლენის ოპერაციების მძლავრ იარაღად. სოციალური ქსელების საწყისი ეტაპი (2000-იანი წლები - ორგანული ზრდის ხანა) Facebook, Twitter და YouTube გაჩნდა, როგორც პლატფორმები პირადი ურთიერთობებისთვის და გასართობი კონტენტის გაზიარებისთვის. ძირითადი კონტენტი მომხმარებელთა მიერ გენერირდებოდა და მათზე გარე გავლენა ნაკლებად შეიმჩნეოდა. დეზინფორმაციის შემთხვევები მინიმალური იყო, ხოლო ფაქტების გადამოწმება არ წარმოადგენდა პრიორიტეტს.

სოციალური ქსელები მუდმივად ადაპტირდებიან მომხმარებლის ქცევასთან ახალი ფუნქციების დამატებით, რაც ზრდის ინტერაქტიულობას. ასეთი ფუნქციების მაგალითებია:

- პირდაპირი ეთერი.
- დროებითი კონტენტი (Stories).
- ალგორითმულად მართული სიახლეების ფიდი.
- ხელოვნური ინტელექტის რეკომენდაციები.
- ელექტრონული კომერციის ინტეგრაცია (მაგალითად, Facebook Marketplace ან Instagram Shopping).
- გაფართოებული რეალობის (AR) ფილტრები და ვირტუალური რეალობის სივრცეები;

ამ განვითარებამ გაზარდა მომხმარებლის ჩართულობა, რის შედეგადაც სოციალური ქსელები ყოველდღიური ცხოვრების განუყოფელ ნაწილად იქცა. ახალმა შესაძლებლობებმა უფრო მოქნილი გახადა კომუნიკაციის შესაძლებლობები. ქვემოთ მოცემულია ცხრილი, სადაც ნაჩვენებია ძირითადი სოციალური ქსელები, მათი შექმნის წელი და სხვადასხვა ფუნქციონალის დამატების თარიღები.

ცხრილი 1-სოციალური ქსელებში ფუნქციების დამატება წლების მიხედვით

სოციალური ქსელი	შექმნის წელი	ტექსტური ჩატი	აუდიო ზარები	ვიდეო ზარები	ფაილების გაზიარება	პირდაპირი ტრანსლაცია
Facebook	2004	2004	2013	2015	2011	2016
Twitter	2006	2006	-	-	2015	2015
LinkedIn	2003	2003	-	2017	2015	2019
Instagram	2010	2010	-	2018	2018	2016
TikTok	2016	2016	-	2018	2020	2016
WhatsApp	2009	2009	2015	2016	2017	2018
Telegram	2013	2013	2017	2020	2014	2021
Snapchat	2011	2011	2018	2018	2019	2015
WeChat	2011	2011	2012	2015	2013	2016
Discord	2015	2015	2015	2016	2017	2017

ცხრილი ასახავს როგორ გარდაიქმნენ სოციალური ქსელები დროის განმავლობაში, ძირითადად ახალი ფუნქციების ინტეგრაციის გზით, რაც აუმჯობესებს მომხმარებლის გამოცდილებას და ჩართულობას. ამ ფუნქციებმა შექმნა უფრო მდიდარი კომუნიკაცია, ჩართულობა და უფრო დინამიკური კონტენტის გაზიარება. თუმცა ამ ევოლუციამ ასევე გამოიწვია უსაფრთხოების მოწყვლადობები და ბოროტად გამოყენება, განსაკუთრებით დეზინფორმაციის და მცდარი ინფორმაციის გავრცელების კუთხით. სოციალური ქსელების ევოლუცია შეიძლება გავანალიზოთ შემდეგი ასპექტების მიხედვით, ფუნქციების ინტეგრაცია და მომხმარებლის ჩართულობა.

სოციალური ქსელები მუდმივად ადაპტირდებიან მომხმარებლის ქცევასთან ახალი ფუნქციების დამატებით, რაც ზრდის ინტერაქტიულობას ასეთი ფუნქციების მაგალითები და მომხმარებელთა ზრდის დინამიკა მოყვანილია შემდეგ ცხრილში.

ცხრილი 2-სოციალური ქსელების მომხმარებელთა რაოდენობის ზრდის დინამიკა.

სოციალური ქსელი	შექმნის წელი	მომხმარებელთა რაოდენობა (მლნ)	გაზიარების ფუნქციის დამატება	მოწონების ფუნქციის დამატება
Facebook	2004	2008: 100, 2012: 1000, 2017: 2000	2006	2009
Twitter	2006	2010: 54, 2012: 185, 2017: 330	2009	2015
Instagram	2010	2012: 30, 2014: 200, 2018: 1000	2013	2011
LinkedIn	2003	2010: 90, 2012: 175, 2017: 500	2008	2010
Snapchat	2011	2014: 50, 2016: 150, 2018: 186	2012	2015
TikTok	2016	2018: 500, 2019: 800, 2020: 1000	2016	2018
WhatsApp	2009	2013: 200, 2016: 1000, 2020: 2000	2011	•
Telegram	2013	2014: 35, 2016: 100, 2020: 400	2013	•
Viber	2010	2012: 50, 2014: 100, 2018: 260	2013	•
WeChat	2011	2013: 300, 2016: 846, 2020: 1200	2012	2014

აღნიშნული მონაცემები აჩვენებს, რომ სოციალური ქსელების ფუნქციების განვითარება და მომხმარებელთა რაოდენობის ზრდა მჭიდროდ არის დაკავშირებული. ფუნქციების დამატება, როგორცაა გაზიარება და მოწონება, ხელს უწყობს მომხმარებელთა ჩართულობის ზრდას, რაც თავის მხრივ აისახება პლატფორმების პოპულარობაზე.

პირდაპირი ეთერი, დროებითი კონტენტი, ალგორითმულად მართული სიახლეების ფიდი, ხელოვნური ინტელექტის რეკომენდაციები, ელექტრონული კომერციის ინტეგრაცია, როგორცაა facebook marketplace ან instagram shopping, გაფართოებული რეალობის ფილტრები და ვირტუალური რეალობის სივრცეები. ამ განვითარებამ გაზარდა მომხმარებლის ჩართულობა რაც სოციალურ ქსელებს აქცევს ყოველდღიური ცხოვრების აუცილებელ ნაწილად.

ცხრილი 3-მნიშვნელოვანი ფუნქციები, რომელმაც გავლენა იქონია მომხმარებელთა რაოდენობის გაზრდაზე.

სოციალური ქსელი	დაფუძნების წელი	მნიშვნელოვანი ფუნქციები
Facebook	2004	სიახლეების ფიდი (2006), პირდაპირი ვიდეო (2016), Marketplace (2016)
Twitter	2006	ჰეშთეგები (2007), გადატვიტვა (2009), სივრცეები (2021)

Instagram	2010	ისტორიები (2016), შოპინგი (2018), Reels (2020)
Snapchat	2011	ისტორიები (2013), Snap Map (2017)
TikTok	2016	ალგორითმული "For You" გვერდი (2018), პირდაპირი ეთერი (2020)
LinkedIn	2003	სტატიები (2014), ისტორიები (2020, წაშლილი 2021)

ყოველმა პლატფორმამ დროთა განმავლობაში გააფართოვა თავისი შესაძლებლობები, ხოლო ბევრი ფუნქცია გადმოღებულია კონკურენტებისგან. ვიდეო კონტენტი, მოკლე ფორმატის ისტორიები და ცოცხალი ურთიერთქმედება დღეს წამყვან ტენდენციებად მიიჩნევა.

ალგორითმული პერსონალიზაცია მნიშვნელოვან როლს ასრულებს მომხმარებლის ჩართულობისა და ინფორმაციის მოხმარების ფორმირებაში.

ინფორმაციული ომის მეთოდები სოციალური ქსელების გამოყენებით

ინფორმაციული ომი სოციალური ქსელების მეშვეობით მოიცავს სხვადასხვა ტაქტიკას და სტრატეგიას, რომლებიც გამოიყენება მოსახლეობაზე გავლენის მოსახდენად, მათი შეცდომაში შეყვანისა და დესტაბილიზაციისთვის. ძირითადი მეთოდები მოიცავს:

დეზინფორმაცია და ყალბი ახალი ამბები

დეზინფორმაცია გულისხმობს განზრახ გავრცელებულ მცდარ ან შეცდომაში შემყვან ინფორმაციას, რომელიც გამოიყენება არჩევნების მანიპულაციისთვის, საზოგადოებრივი არეულობის გამოწვევისთვის და რეპუტაციის დაზიანებისთვის. აღნიშნული პროცესი განსაკუთრებით ძლიერდება ბოტებისა და ტროლების ფერმების მიერ. ყალბი ახალი ამბების ვებსაიტები, სოციალურ ქსელებში გავრცელებული პოსტები, ღრმა ყალბი (deepfake) ვიდეოები და AI-ის მიერ გენერირებული სტატიები გამოიყენება საზოგადოების დაზნეულობისა და ინფორმაციული ქაოსის შესაქმნელად. დეზინფორმაციული კამპანიები ხშირად ორგანიზებულია სახელმწიფოებისა და გავლენიანი ჯგუფების მიერ, რათა ხელი შეუწყონ პოლიტიკურ პროპაგანდას და საზოგადოებრივი აზრის მანიპულაციას.

ფსიქოლოგიური ოპერაციები (PSYOPS)

ფსიქოლოგიური ოპერაციები მიზანმიმართული კამპანიებია, რომლებიც ემოციური, მსოფლმხედველობრივი და ქცევითი გავლენის მოხდენას ემსახურება. ისინი ფართოდ გამოიყენება სამხედრო ოპერაციებში მოწინააღმდეგის დემორალიზაციისა და საზოგადოებრივი აზრის ფორმირებისთვის. ეს მეთოდები ეყრდნობა შიშის, გაურკვევლობისა და ეჭვების გაღვივებას, რაც ხელს უწყობს საზოგადოების დაყოფასა და ინსტიტუტებისა და ლიდერების მიმართ უნდობლობის გაძლიერებას.

ღრმა ყალბი და ხელოვნური ინტელექტით (AI)⁵ გენერირებული კონტენტი

ხელოვნური ინტელექტით შექმნილი ვიდეოები და სურათები ცრუ ნარატივების გასავრცელებლად გამოიყენება. ღრმა ყალბი ტექნოლოგიები ქმნის ჰიპერრეალისტურ ვიდეოებსა და აუდიოჩანაწერებს, რომლებიც ადამიანებს იმ ქმედებებსა და განცხადებებს მიაწერენ, რაც რეალურად არასდროს გაუკეთებიათ ან უთქვამთ. ეს ტექნოლოგია გამოიყენება სკანდალების შექმნის, საზოგადოების შეცდომაში შეყვანისა და გეოპოლიტიკური დამაბულობის გასამწვავებლად.

კიბერ-შპიონაჟი და თვალთვალი

სოციალური ქსელები მნიშვნელოვან ინსტრუმენტს წარმოადგენს სადაზვერვო ინფორმაციის შესაგროვებლად. კიბერთავდამსხმელები იყენებენ სოციალურ ინჟინერიას მგრძნობიარე მონაცემების მოპოვებისთვის. სადაზვერვო სააგენტოები და კიბერდამნაშავეები სოციალურ ქსელებში არსებულ საჯარო მონაცემებს ინდივიდებისა და ორგანიზაციების ფსიქოლოგიური პროფილების შესაქმნელად იყენებენ. ფიშინგ-კამპანიები და მავნე ბმულები ვრცელდება სოციალური ქსელების საშუალებით, რაც კიბერთაღლითებს შესაძლებლობას აძლევს მოიპოვონ მომხმარებელთა პირადი მონაცემები, მათ შორის – შესასვლელი კოდები და ფინანსური ინფორმაცია.

კოორდინირებული არაავთენტური ქცევა (CIB)⁶

⁵ Benkler, Yochai, Robert Faris, and Hal Roberts. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press, 2018.

⁶ Bradshaw, Samantha, and Philip N. Howard. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute, 2017.

ეს მოიცავს ყალბი ანგარიშების ქსელებს, რომლებიც მიზანმიმართულად გამოიყენება გარკვეული ნარატივების გასაძლიერებლად. სახელმწიფო აქტორები ხშირად იყენებენ ამ ტექნიკას საერთაშორისო ურთიერთობების მანიპულაციისთვის. ტროლების ფერმები, ბოტნეტები და ყალბი პროფილები კოორდინირებულად მართავენ მასშტაბურ საინფორმაციო ოპერაციებს, რათა ხელოვნურად გაზარდონ ჩართულობა სოციალურ მედიაში და ყალბი ნარატივები უფრო სანდოდ წარმოაჩინონ.

ჰეშთეგების მანიპულაცია და ტრენდების ხელყოფა⁷

ბოტების გამოყენებით შესაძლებელია სოციალურ ქსელებში ტრენდული თემების მანიპულაცია, რაც ხელს უწყობს ყალბი მოძრაობების შექმნას ან რეალური მოძრაობების დესტაბილიზაციას. სოციალური მედიის ტრენდების ხელოვნური წარმართვა შეიძლება გამოყენებულ იქნას პანიკის გასავრცელებლად, იდეოლოგიური დაპირისპირების გასამძაფრებლად და პოლიტიკური გარემოს დესტაბილიზაციისთვის.

ამ მეთოდების კომბინირებული გამოყენება სოციალური ქსელების მეშვეობით ინფორმაციულ ომს ახალი მასშტაბით აძლიერებს, რაც საზოგადოებას კიდევ უფრო მეტად მოწყვლადს ხდის დეზინფორმაციის, ფსიქოლოგიური ზემოქმედებისა და კიბერ-შეტევების მიმართ.

სოციალური ქსელებით ინფორმაციული ომის შედეგები

პოლიტიკური დესტაბილიზაცია

- დემოკრატიული ინსტიტუტებისადმი ნდობის შემცირება.
- არჩევნებისა და რეფერენდუმების მანიპულირება.

სოციალური პოლარიზაცია

- პოლიტიკურ, ეთნიკურ და იდეოლოგიურ ჯგუფებს შორის დაძაბულობის გაზრდა.
- საზოგადოებაში კონფლიქტებისა და დაპირისპირების გაძლიერება.

ეკონომიკური ზიანი

⁷ Chesney, Robert, and Danielle Citron. “Deepfakes: A Looming Challenge for Privacy, Democracy, and National Security.” *California Law Review* 107, no. 6 (2019): 1753-1819.

- ყალბი ინფორმაცია გავლენას ახდენს საფონდო ბაზრებზე.
- კომპანიებს შეიძლება მიაღდეს რეპუტაციული და ფინანსური ზიანი.

ეროვნული უსაფრთხოების საფრთხე

- კიბერ-ჯაშუშობა ამცირებს თავდაცვის შესაძლებლობებს.
- დეზინფორმაცია იწვევს პანიკას და საზოგადოებრივ არასტაბილურობას.

სოციალურ მედიაზე დაფუძნებული საინფორმაციო ომის ზეგავლენა ღრმა და ფართომასშტაბიანია, რომელიც სხვადასხვა სფეროს – საზოგადოებას, პოლიტიკას, ეკონომიკასა და ეროვნულ უსაფრთხოებას – მოიცავს. ერთ-ერთი მთავარი შედეგი არის პოლიტიკური დესტაბილიზაცია, რადგან სოციალური მედიის მანიპულირება არყევს დემოკრატიული ინსტიტუტებისადმი ნდობას და გამოიყენება არჩევნების და რეფერენდუმების მანიპულაციისთვის. დეზინფორმაციის გავრცელება და პოლიტიკური ოპონენტების დისკრედიტაცია ასუსტებს დემოკრატიულ პროცესს და იწვევს მმართველი სტრუქტურებისადმი ნდობის დაკარგვას.

კიდევ ერთი მნიშვნელოვანი გავლენა არის სოციალური პოლარიზაცია, რადგან სოციალური მედიის პლატფორმები აძლიერებენ დაყოფას პოლიტიკურ, ეთნიკურ და იდეოლოგიურ ჯგუფებს შორის. მიზანმიმართული პროპაგანდა, ყალბი ინფორმაცია და პროვოკაციული კონტენტი ზრდის მტრობას და ამძაფრებს საზოგადოებრივ კონფლიქტებს, რაც ხშირად ძალადობას და არეულობას იწვევს. შედეგად, ადამიანები მეტად უპირისპირდებიან ერთმანეთს და ნაკლებად მზად არიან კონსტრუქციული დიალოგისთვის. სოციალურ მედიაზე დაფუძნებული საინფორმაციო ომის ეკონომიკური შედეგებიც საგანგაშოა. დეზინფორმაციის კამპანიებმა შეიძლება გამოიწვიოს საფონდო ბირჟების მერყეობა, რაც ფინანსურ არასტაბილურობას და გაურკვევლობას ქმნის. კომპანიები და ბიზნესები განსაკუთრებით მოწყვლადები არიან, რადგან ცრუ ჭორები და დეზინფორმაცია მათი რეპუტაციის დაზიანებას და სერიოზულ ფინანსურ ზარალს იწვევს. ასევე, ინვესტორთა ნდობა შეიძლება შეირყეს, რაც კაპიტალის გადინებასა და ეკონომიკური ზრდის შეფერხებას იწვევს. გარდა ამისა, ეროვნული უსაფრთხოებისთვის რისკები იზრდება კიბერ შპიონაჟისა და ყალბი ინფორმაციის გავრცელების გამო. მტრული ძალები იყენებენ სოციალურ მედიას კიბერ შპიონაჟისთვის, რაც ასუსტებს თავდაცვის სტრატეგიებს და

საფრთხეს უქმნის კონფიდენციალურ ინფორმაციას. ასევე, ყალბი ინფორმაციის სწრაფი გავრცელება კრიზისულ ვითარებაში – იქნება ეს ჯანდაცვის კრიზისი თუ გეოპოლიტიკური კონფლიქტი – იწვევს საზოგადოებრივ პანიკას, დაზნეულობას და მასობრივ ისტერიკას, რაც ასუსტებს სახელმწიფო პასუხს და ზოგად სტაბილურობას.

ამრიგად, სოციალური მედიის საშუალებით ინფორმაციის მანიპულაციას მრავალმხრივი ნეგატიური შედეგები აქვს, რაც აყალიბებს არასტაბილურობას, უნდობლობას და ეკონომიკურ ზიანს. ამ გამოწვევების დაძლევა საჭიროებს მედია წიგნიერების განვითარებას, სტრატეგიული საპასუხო ზომების გატარებას და სოციალური მედიის საინფორმაციო ომის საფრთხეების შესახებ საზოგადოების ცნობიერების ამაღლებას.

პრევენცია და წინააღმდეგობის მექანიზმები

AI და ფაქტების გადამოწმების ტექნოლოგიები⁸

- ავტომატური ინსტრუმენტები დეზინფორმაციის გამოსავლენად.
- რეალურ დროში კონტენტის მოდერაცია.

კანონმდებლობა და მთავრობის ჩარევა

- სახელმწიფოებმა უნდა მიიღონ მკაცრი რეგულაციები დეზინფორმაციის წინააღმდეგ.
- სოციალური ქსელების კომპანიებთან თანამშრომლობა.

მოსახლეობის ინფორმირებულობა და ციფრული წიგნიერება

- საზოგადოებას უნდა შეეძლოს ყალბი ამბების ამოცნობა.
- კრიტიკული აზროვნების განვითარება.

კიბერუსაფრთხოების გაძლიერება

- მონაცემთა დაცვა და სოციალური ინჟინერიის პრევენცია.

პრევენცია და საპასუხო ღონისძიებები

⁸ Golovchenko, Yevgeniy, Courtney Buntain, Gregory Eady, Michael A. Brown, and Joshua A. Tucker. “Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube during the 2016 U.S. Presidential Election.” *The International Journal of Press/Politics* 25, no. 3 (2020): 357-389.

სოციალურ ქსელებში საინფორმაციო ომის რისკების შემცირების მიზნით, შესაძლებელია სხვადასხვა სტრატეგიის გამოყენება, რომლებიც ფოკუსირებულია ტექნოლოგიურ განვითარებაზე, რეგულაციურ ზომებზე, საზოგადოებრივი ცნობიერების ამაღლებაზე, კიბერუსაფრთხოებასა და ხელოვნური ინტელექტის ეთიკურ გამოყენებაზე. ერთ-ერთი ძირითადი მიდგომა არის ხელოვნური ინტელექტისა და ფაქტების გადამოწმების ტექნოლოგიების გამოყენება. ავტომატიზებული ინსტრუმენტები მნიშვნელოვან როლს ასრულებენ დეზინფორმაციის ამოცნობასა და აღმოფხვრაში, რაც ხელს უწყობს ცრუ ნარატივების გავრცელების შეჩერებას. რეალურ დროში კონტენტის მოდერაციის მექანიზმები, რომლებიც დაფუძნებულია მანქანურ სწავლაზე, კიდევ უფრო აძლიერებს ამ პროცესს, რაც საშუალებას იძლევა დეზინფორმაციის შეზღუდვა მოხდეს მისი გავრცელების დაწყებამდე. დეზინფორმაციის წინააღმდეგ ბრძოლის კიდევ ერთი მნიშვნელოვანი კომპონენტია რეგულაციური პოლიტიკა და სახელმწიფო ჩარევა. სახელმწიფოებმა უნდა შეიმუშაონ და განახორციელონ შესაბამისი კანონები, რომლებიც პასუხისმგებლობას მისცემს იმ პირებსა და ორგანიზაციებს, რომლებიც მიზანმიმართულად ავრცელებენ ცრუ ინფორმაციას, განსაკუთრებით მაშინ, როდესაც ეს საფრთხეს უქმნის ეროვნულ უსაფრთხოებას ან საზოგადოებრივ წესრიგს. ამასთანავე, აუცილებელია სახელმწიფოსა და სოციალური მედიის კომპანიებს შორის თანამშრომლობა, რათა მოხდეს მავნე კონტენტის ეფექტიანი მონიტორინგი და მისი დროული აღმოფხვრა. მკაფიო წესებისა და ერთობლივი მოქმედების მეშვეობით შესაძლებელია ციფრული სივრცის უსაფრთხოების გაძლიერება. საზოგადოების ცნობიერების ამაღლება და ციფრული წიგნიერების განვითარება ერთ-ერთი გადამწყვეტი ფაქტორია საინფორმაციო ომის წინააღმდეგ ბრძოლაში. მოსახლეობის განათლება ყალბი ამბების, პროპაგანდისა და მანიპულაციური კონტენტის ამოცნობის უნარების განვითარებაზე ხელს შეუწყობს საზოგადოებრივ მდგრადობას დეზინფორმაციის მიმართ. კრიტიკული აზროვნების წახალისება დაეხმარება ადამიანებს, რომ გადაამოწმონ წყაროები, შეაფასონ საექვო ნარატივები და გაარჩიონ სანდო ინფორმაცია მცდარისგან. ცნობიერების ამაღლების კამპანიები, მედია წიგნიერების პროგრამები და საგანმანათლებლო ინიციატივები საზოგადოების ციფრულ გარემოში პასუხისმგებლიან ნავიგაციას

შეუწყობს ხელს. კიბერუსაფრთხოების ზომებს დიდი მნიშვნელობა აქვს კიბერ-სპიონაჟის თავიდან ასაცილებლად და მგრძნობიარე ინფორმაციის დაცვისთვის. უსაფრთხოების პროტოკოლების გაძლიერება ხელს უშლის ბოროტმოქმედებს მონაცემების უკანონო წვდომასა და მანიპულირებაში. უსაფრთხოების გაუმჯობესებული პრაქტიკები, როგორცაა დაშიფვრა, უსაფრთხო ავთენტიკაცია და შედფე-ვადობის გამოვლენის სისტემები, უზრუნველყოფს მომხმარებლების დაცვას კი-ბერშეთევებისგან. მონაცემთა დაცვის პრიორიტეტიზებით შესაძლებელია მანიპუ-ლაციისა და დეზინფორმაციის გავრცელების რისკების შემცირება.

ბოლოს, აუცილებელია ეთიკური მიდგომების გათვალისწინება ხელოვნური ინ-ტელექტისა და სოციალური მედიის მართვაში, რათა უზრუნველყოფილ იქნას სა-მართლიანობა და გამჭვირვალობა კონტენტის მოდერაციის პროცესში. ეთიკური ხელოვნური ინტელექტის დანერგვა ხელს შეუწყობს ალგორითმული მიკერძოების თავიდან აცილებას, რაც შესაძლოა უნებლიეთ გააძლიერებდეს დეზინფორმაციას ან შეავიწროებდეს სანდო ინფორმაციას. კონტენტის რეკომენდაციის სისტემებისა და მოდერაციის პოლიტიკის გამჭვირვალობა შექმნის მომხმარებლებს შორის ნდო-ბას და სოციალური მედიის პლატფორმების პასუხისმგებლიანი ფუნქციონირების საფუძველს. მნიშვნელოვანია, რომ არსებობდეს ეთიკური ზედამხედველობისა და ანგარიშვალდებულების მექანიზმები, რათა თავიდან იქნეს აცილებული ხელოვნუ-რი ინტელექტის ბოროტად გამოყენება საზოგადოებრივი აზრის მანიპულირების მიზნით.

ამ სტრატეგიების ინტეგრირებით შესაძლებელია საზოგადოები თავდაცვისუნა-რიანობის გაძლიერება საინფორმაციო ომის საფრთხეების წინააღმდეგ, რაც ხელს შეუწყობს უსაფრთხო და ინფორმირებულ ციფრულ გარემოს.

დასკვნა

სოციალური ქსელები თანამედროვე ციფრულ ეპოქაში იქცა არა მხოლოდ კომუნიკაციისა და ინფორმაციის გაზიარების საშუალებად, არამედ საინფორმა-ციო ომის ერთ-ერთ მთავარ ინსტრუმენტად. მათი ალგორითმული მექანიზმები და ხელოვნური ინტელექტის მოდელები ქმნიან ახალ ტიპის გავლენას საზოგა-

დოებრივ ცნობიერებაზე, რაც პოლიტიკურ, ეკონომიკურ და უსაფრთხოების სფეროებშიც აისახება. აღნიშნული პლატფორმები ხელს უწყობენ როგორც დემოკრატიული პროცესების გამჭვირვალობას, ისე მათი მანიპულაციის შესაძლებლობას. სწორედ ამიტომ, სოციალური ქსელები დღეს უკვე განიხილება როგორც „ციფრული ბრძოლის ველი“, სადაც მიმდინარეობს ნარატივების, მოსაზრებებისა და სიმბოლური ძალაუფლების დაპირისპირება.

სოციალური მედიის ალგორითმები ხშირად აძლიერებენ ე.წ. ექოკამერებს, რაც საზოგადოებრივ პოლარიზაციას იწვევს. მომხმარებლები იღებენ მხოლოდ მათთვის სასურველ შინაარსს, შედეგად კი მცირდება კრიტიკული აზროვნების უნარი და იზრდება მანიპულაციის რისკი. ამგვარად, დეზინფორმაციის კამპანიები ხშირად წარმატებით იყენებენ ფსიქოლოგიურ და ტექნოლოგიურ ხარვეზებს საზოგადოებაზე ზემოქმედებისთვის. ერთდროულად ვითარდება ღრმა ყალბი (deepfake) ტექნოლოგიები, რომლებიც ქმნიან რეალისტურ, მაგრამ ყალბ ვიდეო-და აუდიომასალებს, რითაც იბნევა საზოგადოებრივი აღქმა და ირღვევა ნდობა სახელმწიფო ინსტიტუტებისა და მედიასაშუალებების მიმართ. სოციალური მედიის ალგორითმები ხშირად აძლიერებენ ე.წ. ექო-კამერებს, რაც საზოგადოებრივ პოლარიზაციას იწვევს. მომხმარებლები იღებენ მხოლოდ მათთვის სასურველ შინაარსს, შედეგად კი მცირდება კრიტიკული აზროვნების უნარი და იზრდება მანიპულაციის რისკი. ამგვარად, დეზინფორმაციის კამპანიები ხშირად წარმატებით იყენებენ ფსიქოლოგიურ და ტექნოლოგიურ ხარვეზებს საზოგადოებაზე ზემოქმედებისთვის. ერთდროულად ვითარდება ღრმა ყალბი (deepfake) ტექნოლოგიები, რომლებიც ქმნიან რეალისტურ, მაგრამ ყალბ ვიდეო და აუდიომასალებს, რითაც იბნევა საზოგადოებრივი აღქმა და ირღვევა ნდობა სახელმწიფო ინსტიტუტებისა და მედიასაშუალებების მიმართ. ამ გარემოებებიდან გამომდინარე, აუცილებელია პრევენციული მექანიზმების დანერგვა რამდენიმე მიმართულებით: ხელოვნური ინტელექტის საფუძველზე შექმნილი აქტრეკინგის სისტემები, მკაცრი სახელმწიფო რეგულაციები, ციფრული წიგნიერების პროგრამები და საერთაშორისო თანამშრომლობა ინფორმაციული უსაფრთხოების დაცვისთვის. საქართველოს უსაფრთხოების კონტექსტში

ეს საკითხი განსაკუთრებულ მნიშვნელობას იძენს, რადგან ქვეყნის გეოპოლიტიკური მდებარეობა და რეგიონში არსებული საინფორმაციო დაპირისპირებები აძლიერებს კიბერშეტევებისა და პროპაგანდის კამპანიების რისკებს. აუცილებელია ციფრული თავდაცვის სისტემების გამყარება და სახელმწიფო სტრუქტურებსა და კერძო სექტორს შორის კოორდინირებული კიბერუსაფრთხოების პოლიტიკის ჩამოყალიბება. მომავალი ტენდენციების ათვალისწინებით, კაცობრიობა შეიძლება შევიდეს „ალგორითმული ცივი ომის“ ეპოქაში, სადაც სახელმწიფოები და კერძო სტრუქტურები ერთმანეთს შეეჯიბრებიან ინფორმაციის, მონაცემებისა და ზეგავლენის კონტროლში.

ბიბლიოგრაფია

- Benkler, Y., Faris, R., & Roberts, H. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press. (2018).
- Bradshaw, S., & Howard, P. N. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute. (2017).
- Chesney, R., & Citron, D. *Deepfakes: A Looming Challenge for Privacy, Democracy, and National Security*. California Law Review, 107(6), (2019). 1753-1819.
- Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. *Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube during the 2016 U.S. Presidential Election*. The International Journal of Press/Politics, 25(3), (2020). 357-389.
- Marwick, A., & Lewis, R. *Media Manipulation and Disinformation Online*. Data & Society Research Institute. (2017).