განვითარებადი ციფრული ტექნოლოგიები და კიბერუსაფრთხოების გამოწვევები

ლიკა ლაგვილავა
კავკასიის საერთაშორისო უნივერსიტეტის
სოციალურ და ჰუმანიტარულ მეცნიერებათა ფაკულტეტის
პოლიტიკის მეცნიერების სადოქტორო
საგანმანათლებლო პროგრამის დოქტორანტი
lika.lagvilava@ciu.edu.ge
ORCID iD: https://orcid.org/ 0009-0000-0120-0408
DOI: 10.52340/splogos.2025.03.13

აბსტრაქტი

თანამედროვე ციფრული ტექნოლოგიების სწრაფმა განვითარებამ რადიკალურად შეცვალა გლობალური უსაფრთხოების პარადიგმა. ხელოვნური ინტელექტი, ბლოკჩეინი, ინტერნეტი ნივთების (IoT), 5G კავშირი და ღრუბლოვანი ინფრასტრუქტურა ქმნიან ახალ შესაძლებლობებს, თუმცა, ამავე დროს ზრდიან კიბერუსაფრთხოების სირთულეებსა და საფრთხეებს. აღნიშნულ ტექნოლოგიებთან ერთად იზრდება კიბერშეტევების მასშტაბი, სირთულე და ფარული ზემოქმედების შესაძლებლობა როგორც სახელმწიფო, ისე კერძო სექტორზე. განსაკუთრებით რისკის ქვეშ დგანან კრიტიკული ინფრასტრუქტურები, სახელმწიფო უწყებები და მონაცემთა ბაზები, რომელთა უსაფრთხოება პირდაპირ კავშირშია ეროვნულ და საერთაშორისო სტაბილურობასთან.

წარმოდგენილი ნაშრომი მიზნად ისახავს გააანალიზოს ის ძირითადი კიბერუსაფრთხოების გამოწვევები, რომლებიც დაკავშირებულია განვითარებად ციფრულ ტექნოლოგიებთან. კვლევა ეფუძნება შემთხვევების ანალიზს, საერთაშორისო პრაქტიკასა და თანამედროვე სტრატეგიულ მიდგომებს. განსაკუთრებული ყურადღება ეთმობა კიბერმდგრადობის კონცეფციას, ინციდენტებზე რეაგირების მექანიზმებსა და მრავალდონიან კოორდინაციას. ნაშრომში გამოკვეთილია საჭიროება ინტეგრირებული პოლიტიკის, ციფრული სოლიდარობისა და ტექნოლოგიური სუვერენიტეტის გასაძლიერებლად.

აბსტრაქტი ასახავს კიბერუსაფრთხოების ინტერდისციპლინურ ბუნებას და ხაზს უსვამს პრევენციული, რეაგირებისა და აღდგენის პროცესების მუდმივ დახვეწის აუცილებლობას ტექნოლოგიური პროგრესის ფონზე.

საკვანძო სიტყვები: განვითარებადი ციფრული ტექნოლოგიები; კიბერუსაფრთხოება, კიბერშეტევები, კრიტიკული ინფრასტრუქტურა, გლობალური თანამშრომლობა

Emerging Digital Technologies and Cybersecurity Challenges

Lika Lagvilava
Ph.D. Student, Doctoral Educational Program in Political Science
Faculty of Social and Humanitarian Sciences
Caucasus International University
lika.lagvilava@ciu.edu.ge
ORCID iD: https://orcid.org/ 0009-0000-0120-0408

Abstract

The rapid development of modern digital technologies has radically changed the global security paradigm. Artificial intelligence, blockchain, the Internet of Things (IoT), 5G connectivity, and cloud infrastructure create new opportunities, but at the same time increase the complexity and threats of cybersecurity. Along with these technologies, the scale, complexity, and potential for covert impact of cyberattacks on both the public and private sectors are increasing. Critical infrastructures, government agencies, and databases, whose security is directly related to national and international stability, are particularly at risk. The presented paper aims to analyze the main cybersecurity challenges associated with emerging digital technologies. The study is based on case studies, international practice, and modern strategic approaches. Special attention is paid to the concept of cyber resilience, incident response mechanisms, and multi-level coordination. The paper highlights the need for integrated policies, digital solidarity, and technological sovereignty. The abstract reflects the interdisciplinary nature of cybersecurity and emphasizes the need for continuous improvement of prevention, response, and recovery processes in the context of technological progress.

Keywords: emerging digital technologies; cybersecurity, cyberattacks, critical infrastructure, global cooperation

კვლევის მეთოდოლოგია: მოცემული ნაშრომი ეფუძნება კომბინირებულ კვლევით მიდგომას, რომელიც მოიცავს ხარისხობრივ ანალიზს. გამოყენებული იქნება შედარებითი მეთოდი სხვადასხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციის (მაგ., ნატო, ევროკავშირი, გაერო) კიბერუსაფრთხოების სტრატეგიების შესაფასებლად. შემთხვევის ანალიზის (case study) მეთოდით განიხილება რამდენიმე მნიშვნელოვანი პრეცედენტი – მათ შორის, ესტონეთის 2007 წლის კიბერშეტევა, SolarWinds-ის ინციდენტი და რუსეთის მიერ გამოყენებული კიბეროპერაციები სამხედრო კონფლიქტებში. ნაშრომში გამოყენებული იქნება

დოკუმენტური ანალიზი (policy papers, სტრატეგიული დოკუმენტები, აკადემიური პუბლიკაციები) და ექსპერტებთან ჩაღრმავებული ინტერვიუები, რაც გააძლიერებს კვლევის ემპირიულ საფუძველს.

კვლევის თეორიული ჩარჩო: კვლევა დაფუძნებულია კიბერუსაფრთხოების კვლევის ინტერდისციპლინარულ თეორიებზე, რომლებიც აერთიანებს საერთაშორისო უსაფრთხოების, cyber resilience და კომპლექსური ურთიერთდამოკიდებულების კონცეფციებს. განსაკუთრებული მნიშვნელობა ენიჭება უსაფრთხოების სეკიურიტიზაციის თეორიას, რომელიც ხსნის, თუ როგორ იქცევა კიბერუსაფრთხოება სახელმწიფოთა პოლიტიკური დღის წესრიგის ერთ-ერთ ცენტრალურ საკითხად. ასევე გამოყენებული იქნება სისტემური მიდგომა, რომელიც ხაზს უსვამს კიბერსივრცის, ეკონომიკისა და სამხედრო სფეროს ურთიერთგადაჯაჭვულობას. კვლევის ჩარჩო მოიცავს ციფრული სოლიდარობის კონცეფციას, რომელიც განიხილება როგორც შესაძლო ახალი მექანიზმი საერთაშორისო კოოპერაციის გასაღრმავებლად.

სამეცნიერო სიახლე: ნაშრომის მთავარი სამეცნიერო სიახლე მდგომარეობს იმაში, რომ იგი ავითარებს ციფრული სოლიდარობის კონცეფციას, როგორც კიბერუსაფრთხოების კოლექტიური დაცვის ახალი ინსტრუმენტს. ამგვარი მიდგომისას ჩამოყალიბებულია მოდელი, რომელიც აერთიანებს პრევენციის, რეაგირებისა და აღდგენის ეტაპებს ერთიან სტრუქტურაში და ამყარებს კიბერსივრცეში თანამშრომლობის პრინციპებს არა მხოლოდ ნატოს წევრ, არამედ პარტნიორ ქვეყნებს შორისაც. კვლევა ასევე განიხილავს ინოვაციურ პრაქტიკას – მაგალითად, ხელოვნური ინტელექტის გამოყენებას რეალურ დროში საფრთხეების პროგნოზირებისთვის და ბლოკჩეინის ინტეგრაციას მონაცემთა სანდოობის გასაუმჯობესებლად.

შესავალი

ციფრული ტექნოლოგიების დინამიკურმა განვითარებამ ფუნდამენტურად გარდაქმნა თანამედროვე მსოფლიო – კომუნიკაცია, მმართველობა, ბიზნესი, სამხედრო სტრატეგია და ყოველდღიური ცხოვრება სულ უფრო მეტად ეყრდნობა ციფრულ სივრცეს. ინტერნეტ- და ინფრასტრუქტურების გაძლიერება, ხელოვნური ინტელექტის ინტეგრაცია, დიდი მონაცემების (Big Data) გამოყენება, ბლოკჩეინის სისტემები და ღრუბლოვანი ქსელები არა მხოლოდ აჩქარებს ინოვაციას, არამედ მნიშვნელოვნად ცვლის გლობალური უსაფრთხოების არქიტექტურას.

თუმცა, ციფრული პროგრესის პარალელურად გაიზარდა უსაფრთხოების რისკებიც – კიბერდანაშაულის სიხშირე, კიბერშეტევების სირთულე და მათი

გეოპოლიტიკური გავლენა ახალ საფრთხეებს უქმნის როგორც სახელმწიფოებს, ისე კერძო სექტორსა და ინდივიდებს. თანამედროვე სახელმწიფოების კრიტიკული ინფრასტრუქტურა – ენერგეტიკა, ჯანდაცვა, ტრანსპორტი, ბანკები და თავდაცვითი სისტემები – დიდწილად დამოკიდებულია ტექნოლოგიურ სტაბილურობაზე, რაც მათ პოტენციურად მოწყვლადს ხდის კიბერშეტევებისადმი.

გლობალურ დონეზე, კიბერუსაფრთხოება გარდაიქმნა ერთ-ერთ მთავარ სტრატეგიულ გამოწვევად. არაერთი საერთაშორისო კვლევა მიუთითებს, რომ სახელმწიფოთა ტექნოლოგიური განვითარება ვერ სდევს საკმარისად სწრაფად უსაფრთხოების პრევენციულ სტრატეგიებს. კიბერშეტევები ხშირად აღწევს მაღალი სენსიტიურობის სისტემებამდე, ზოგ შემთხვევაში კი, სახელმწიფოთაშორისი დაპირისპირების ინსტრუმენტადაც ყალიბდება, რასაც მეცნიერები „კიბერომად“ განიხილავენ.

განვითარებადი ციფრული ტექნოლოგიები ქმნიან ახალი ტიპის კიბერუსაფრთხოების გამოწვევებს, განვიხილავთ, თუ როგორ რეაგირებენ სახელმწიფოები და საერთაშორისო ორგანიზაციები ამ გამოწვევებზე და როგორ შეიძლება განვითარდეს ეფექტიანი მექანიზმები კიბერუსაფრთხოების უზრუნველსაყოფად. განსაკუთრებული ყურადღება დაეთმობა პრევენციის, რეაგირებისა და აღდგენის მექანიზმებს, ასევე, ციფრული სოლიდარობის მნიშვნელობას საერთაშორისო დონეზე.

პრობლემის აქტუალობა: ციფრული ტექნოლოგიების დინამიკურმა განვითარებამ არა მხოლოდ შეცვალა გლობალური ურთიერთობების არქიტექტურა, არამედ წარმოშვა სრულიად ახალი ტიპის რისკები, რომლებიც უშუალოდ ეხება სახელმწიფოების, კერძო სექტორისა და ინდივიდების უსაფრთხოებას. თანამედროვე მსოფლიოში კრიტიკული ინფრასტრუქტურის ციფრულ სისტემებზე დამოკიდებულებამ მნიშვნელოვნად გაზარდა კიბერმუქარის მასშტაბი. კიბერდანაშაული, ჰაკერული ჯგუფების მიერ განხორციელებული მასშტაბური შეტევები და სახელმწიფოთაშორისი კიბეროპერაციები ხშირად იწვევს ეკონომიკურ დანაკარგებს, დემოკრატიული ინსტიტუტების დესტაბილიზაციასა და ზოგიერთ შემთხვევაში – გეოპოლიტიკურ კრიზისს. ამ ფონზე, კიბერუსაფრთხოება იქცა არა მხოლოდ ტექნოლოგიურ, არამედ პოლიტიკურ და სტრატეგიულ გამოწვევად, რომელიც მოითხოვს სისტემურ, ინტერდისციპლინარულ მიდგომას. სწორედ ამიტომ, აღნიშნული თემის კვლევა წარმოადგენს აქტუალურ და პრიორიტეტულ საკითხს თანამედროვე პოლიტოლოგიისა და საერთაშორისო ურთიერთობების მეცნიერებაში.

სწრაფად განვითარებადი ციფრული ტექნოლოგიები

ციფრული ტექნოლოგიების სწრაფი განვითარება არა მხოლოდ აჩქარებს სოციალურ, ეკონომიკურ და სახელმწიფოებრივ პროგრესს, არამედ კიბერსივრცეს გარდაქმნის ახალი ტიპის არაერთი საფრთხის არენად. სწორედ ამ ცვლილების ფონზე, მთავარი სათქმელია ის, რომ ციფრული პროგრესი აუცილებლად უნდა ახლდეს კიბერუსაფრთხოების პარალელურ განვითარებას, რადგან ტექნოლოგიური ინოვაცია, თავის თავში, არ წარმოადგენს უსაფრთხოების გარანტს[160].

თანამედროვე მსოფლიოში კიბერუსაფრთხოება უნდა აღიქმებოდეს როგორც საერთაშორისო, მრავალდონიანი და ინტერდისციპლინური ამოცანა, რომლის წარმატებული შესრულება დამოკიდებულია არა მხოლოდ ინდივიდუალურ სახელმწიფოებზე, არამედ გლობალურ თანამშრომლობაზე, ციფრულ სოლიდარობასა და ერთიანი სტრატეგიული ხედვის ჩამოყალიბებაზე.

ციფრული ტექნოლოგიების განვითარება ვერ ჩაითვლება წარმატებულად, თუ მას არ აქვს საიმედო და მდგრადი კიბერუსაფრთხოების ჩარჩო. სწორედ ამიტომ, საჭიროა პოლიტიკის, ტექნოლოგიისა და საზოგადოების ერთიანი ძალისხმევა, რათა პროგრესი არ გადაიქცეს მოწყვლადობად, ხოლო ინოვაცია – საფრთხედ.[161]

ციფრული ტექნოლოგიები ყოველდღიურად ცვლიან ჩვენს ცხოვრებას, მაგრამ მათთან ერთად იზრდება კიბერუსაფრთხოების სერიოზული გამოწვევებიც. ქვემოთ წარმოდგენილია რამდენიმე კონკრეტული მაგალითი, რომლებიც ასახავს ამ პრობლემების რეალურ მასშტაბს:

1. სტაქსნეტი (Stuxnet) – ინდუსტრიული სისტემის წინააღმდეგ პირველი კიბერიარაღი;

2010 წელს აღმოჩენილი მავნე პროგრამა სტაქსნეტი (Stuxnet) მიზანმიმართულად შეიჭრა ირანის ბირთვულ ობიექტებში და გაანადგურა ურანის გამამდიდრებელი ცენტრიფუგები.[162] ეს იყო პირველი შემთხვევა, როდესაც კიბერშეტევა ფიზიკური დაზიანების გამოწვევით აისახა ეროვნულ ინფრასტრუქტურაზე. იგი ასახავს იმას, თუ როგორ შეიძლება ტექნოლოგიური

[160] Svitlyk Y., ,,OpenAIახალი სუპერძალა: რა არის ChatGPT აგენტი?", Root Nation, p. 1, 2023. https://ka.root-nation.com/en/articles-en/services-en/en-chatgpt-new-super-power/ (ბ.ნ. 25.07.2025).

[161] Singh, S., Hosen, A. S. M., Yoon, B., ''Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network". IEEE Access, 8, pp. 13938-13959. 2021. https://scispace.com/pdf/blockchain-security-attacks-challenges-and-solutions-for-the-47ml7a9t5w.pdf (ბ.ნ. 23.07.2025)

[162] სიდამონიძე, ნ., „STUXNET – გლობალური მნიშვნელობის კიბერ იარაღი, რომელმაც ბირთვული საფრთხე შეაჩერა". ანალიტიკური ცენტრი, გვ.1. 2023. https://shorturl.at/ZFTbI (ბ.ნ. 23.07.2025)

ცოდნის გამოყენება პოლიტიკური მიზნებისთვის და ხაზს უსვამს კიბერშეტევების სამხედრო პოტენციალს.

სტაქსნეტმა გააფუჭა დაახლოებით 1,000 ურანის გამამდიდრებელი ცენტრიფუგა, რაც იყო ირანის კონკრეტული ობიექტის კაპიტალის დაახლოებით 20-დან 30 პროცენტამდე. დაზიანება ფიზიკური ხასიათისა იყო, რამაც სერიოზულად შეაფერხა ირანის ბირთვული პროგრამის განვითარება. თავდასხმის შედეგად ირანის ბირთვული პროგრამა მნიშვნელოვნად შეფერხდა. ზუსტი ფინანსური ზარალის ოდენობა საჯაროდ არ არის ცნობილი, მაგრამ ცნობილია, რომ ტექნიკური აღდგენისა და შეცდომების გამოსწორების ხარჯები ძალიან დიდი იყო. სტაქსნეტის გამოჩენამ ახალი ეტაპი ჩაუყარა კიბერუსაფრთხოების პოლიტიკას მსოფლიოს სხვადასხვა სახელმწიფოში, მნიშვნელოვნად გაზარდა ტექნოლოგიური თავდაცვისა და კიბერუსაფრთხოების სტრატეგიების საჭიროება.

სტაქსნეტის ზარალი იყო არა მხოლოდ ტექნიკური და ფინანსური, არამედ სტრატეგიული ხასიათისა, რაც ცხადყოფს, რომ კიბერშეტევებმა შესაძლოა შეუქცევადი და მასშტაბური შედეგები გამოიწვიონ კრიტიკული ინფრასტრუქტურისთვის.[163]

2. კოლონიური მილსადენი (Colonial Pipeline) – 2021 წლის თავდასხმა ენერგეტიკულ სექტორზე

აშშ-ის ერთ-ერთი უმსხვილესი ნავთობის გადამამუშავებელი ქსელი გახდა რანსომვერის (გამოძალვის პროგრამის) მსხვერპლი. ჰაკერებმა დაბლოკეს სისტემების მუშაობა და კომპანიას მილიონობით დოლარის გამოსასყიდი მოსთხოვეს. კომპანიამ ჰაკერებს გადაუხადა დაახლოებით 4.4 მილიონი დოლარი გამოსასყიდის სახით, თუმცა, მოგვიანებით ფული აშშ-ის მთავრობამ დაუბრუნა.[164] მილსადენის სრულყოფილი მუშაობის აღდგენას რამდენიმე დღე დასჭირდა, რამაც გარდა პირდაპირი ზარალისა, გამოიწვია დიდი ხარჯები უსაფრთხოების გაძლიერებაზე, დაზიანებული სისტემების აღდგენასა და დამატებით ტექნიკურ სამუშაოებზე. ეს შემთხვევა ცხადყოფს, რამდენად მოწყვლადია კრიტიკული ინფრასტრუქტურა ტექნოლოგიურ სივრცეში და როგორ შეიძლება კიბერშეტევებმა გავლენა მოახდინოს რეალურ ეკონომიკასა და მოსახლეობის ყოველდღიურ ცხოვრებაზე.

[163] სიდამონიძე ნ., „STUXNET – გლობალური მნიშვნელობის კიბერ იარაღი, რომელმაც ბირთვული საფრთხე შეაჩერა“, ანალიტიკური ცენტრი, გვ.1. 2023. https://shorturl.at/ZFTbl (ბ.ნ. 23.07.2025)

[164] Svitlyk Y., ,,ყველაზე ცნობილი ჰაკერული თავდასხმები, რომლებიც მთელ მსოფლიოში მოხდა”, Root Nation, p.1. 2023. https://ka.root-nation.com/en/articles-en/tech-en/en-most-famous-hacker-attacks/ (ბ. ნ. 25.07.2025).

3. ესტონეთის 2007 წლის კიბერშეტევები – სახელმწიფოს პარალიზება ციფრულად

ესტონეთი, მსოფლიოში ერთ-ერთი ყველაზე ციფრულად განვითარებული სახელმწიფო, 2007 წელს მასშტაბური კიბერშეტევის მსხვერპლი გახდა. ჰაკერებმა თავდასხმა დაიწყეს სახელმწიფო უწყებების, ბანკებისა და მედიაპლატფორმების წინააღმდეგ. შედეგი იყო ინფორმაციული და ეკონომიკური პარალიზება რამდენიმე დღით. შემთხვევამ დააჩქარა ნატოს კიბერუსაფრთხოების სტრატეგიის გაძლიერება და კიბერშეტევების აღიარება როგორც პოტენციური სამხედრო თავდასხმის ფორმა.

მიუხედავად იმისა, რომ ზუსტ ფინანსურ ზარალზე ოფიციალური მონაცემები არ არსებობს, სხვადასხვა წყაროები მიუთითებენ რამდენიმე მნიშვნელოვან ასპექტზე:

სერვისების შეფერხება: მთავარი ბანკების, მთავრობის უწყებების და მედიაორგანიზაციების ვებსაიტები რამდენიმე დღით გადახურდა, რამაც შეაფერხა ქვეყნის ყოველდღიური ფუნქციონირება.

ეკონომიკური ზარალი: ბევრი კომპანია, განსაკუთრებით მცირე და საშუალო ზომის, განიცდიდა შემოსავლის დაკარგვას, რადგან მათი ონლაინსერვისები შეჩერებული იყო.

ამ ინციდენტმა გამოავლინა ციფრული თავდაცვის აუცილებლობა და ხელი შეუწყო შემდეგი ნაბიჯების გადადგმას: ატლანტიკური ალიანსი აღიარებდა კიბერშეტევების სერიოზულობას და გამოთქვა მზადყოფნა დაეხმარებოდა წევრ ქვეყნებს კიბერუსაფრთხოების სფეროში. 2008 წელს, ესტონეთში დაარსდა NATO-ს კოოპერატიული კიბერდაცვის ცენტრი, რომელიც გახდა საერთაშორისო თანამშრომლობის პლატფორმა კიბერუსაფრთხოების სფეროში. ესპანეთის მთავრობამ დაიწყო ციფრული ინფრასტრუქტურის გამაგრება, ახალი პოლიტიკის შემუშავება და საერთაშორისო პარტნიორებთან თანამშრომლობის გაძლიერება.

4. „ChatGPT“-ს (AI) ფიქტიური ინფორმაციების შექმნის საფრთხე

ხელოვნური ინტელექტის მოდელების (როგორიცაა ChatGPT) განვითარებამ წარმოშვა ახალი მრავალი ტიპის საფრთხეი: დეზინფორმაცია, ღრმა ფეიკები (deepfakes), ავტომატური ფიშინგი და სოციალური მანიპულაცია[165]. მაგალითად, კიბერჰაკერებმა შეძლეს GPT-4 მსგავსი მოდელების გამოყენება, რათა შეექმნათ სარწმუნო თაღლითური ტექსტები და მოეპარათ მომხმარებელთა პირადი

[165] Svitlyk Y., ,,OpenAIახალი სუპერძალა: რა არის ChatGPT აგენტი?”, Root Nation, p.1, 2023, https://ka.root-nation.com/en/articles-en/services-en/en-chatgpt-new-super-power/ (ბ.წ. 25.07.2025).

მონაცემები. ეს აჩვენებს, რომ AI შეიძლება გახდეს როგორც ინოვაციის, ისე კიბერსაფრთხის წყარო.

5. Pegasus – მობილური თვალთვალის პროგრამა

ისრაელის NSO Group-ის მიერ შექმნილი პროგრამა „პეგასუსი“ გამოიყენებოდა ჟურნალისტების, აქტივისტებისა და პოლიტიკური ოპონენტების მობილური ტელეფონების გასატეხად. პროგრამა ერთ-ერთ ყველაზე დახვეწილ მეთოდს იყენებს მობილური მოწყობილობების ფარული კონტროლისთვის და აჩვენებს, რომ ციფრული ტექნოლოგიები შეიძლება გამოიყენონ სახელმწიფოებმა პოლიტიკური კონტროლის იარაღადაც.[166]

6. Smart City – ტექნოლოგიური კომფორტი და დაცულობის დილემა

„ჭკვიანი ქალაქების“ კონცეფცია გულისხმობს სენსორებზე, IoT-ტექნოლოგიებსა და ხელოვნურ ინტელექტზე დაფუძნებულ ინფრასტრუქტურას. თუმცა, თუ კიბერუსაფრთხოების საკმარისი ზომები არ არის მიღებული, ამ სისტემებში შეღწევა საშუალებას აძლევს ჰაკერებს აკონტროლონ ტრანსპორტი, განათება, კამერები და სხვა სისტემები. ასეთი სცენარები რეალურ საფრთხეს უქმნის ურბანულ უსაფრთხოებას.

ზემოთ ჩამოთვლილი შემთხვევები აჩვენებს, რომ ტექნოლოგიური პროგრესი მხოლოდ იმ შემთხვევაში იქნება სტაბილური და სანდო, თუ მას თან ახლავს უსაფრთხოების ეფექტიანი ჩარჩო, გლობალური თანამშრომლობა და პრევენციული მექანიზმების მუდმივი განვითარება. განვითარებადი ციფრული ტექნოლოგიები გლობალურ საზოგადოებას უწყვეტი პროგრესის, კომუნიკაციისა და ინოვაციების საშუალებას აძლევს, მაგრამ ამასთანავე აჩენს კიბერუსაფრთხოების ახალ, კომპლექსურ გამოწვევებს. თანამედროვე ეპოქაში, სადაც ხელოვნური ინტელექტი, ინტერნეტი ნივთების, ბლოკჩეინი და ღრუბლოვანი ტექნოლოგიები ერთდროულად განავითარებს როგორც ეკონომიკასა და სოციალურ სივრცეს, ასევე უსაფრთხოების რისკს, აუცილებელია ამ გამოწვევებზე ეფექტიანი და კოორდინირებული რეაგირება[167].

მნიშვნელოვანია აღინიშნოს, რომ კიბერუსაფრთხოების უზრუნველყოფა შეიძლება მხოლოდ გლობალური თანამშრომლობის, მრავალდონიანი კოორდინაციისა და მუდმივი ტექნოლოგიური ინოვაციების გაერთიანებით.

[166] Svitlyk Y., ,,ყველაზე ცნობილი ჰაკერული თავდასხმები, რომლებიც მთელ მსოფლიოში მოხვდა”. Root Nation, p.1. 2023. https://ka.root-nation.com/en/articles-en/tech-en/en-most-famous-hacker-attacks/ (ბ.წ. 25.07.2025)

[167] Singh S., Hosen A. S. M., Yoon B., ‘’Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network”. IEEE Access, 8, pp. 13938-13959. 2021. https://scispace.com/pdf/blockchain-security-attacks-challenges-and-solutions-for-the-47ml7a9t5w.pdf (ბ.წ. 23.07.2025).

საზოგადოების ცნობიერების ამაღლება და სამართლებრივი ჩარჩოების გამკაცრება ასევე არანაკლებ მნიშვნელოვანია, რადგან კიბერსაფრთხე ეხება ყველას – ინდივიდებს, ორგანიზაციებსა და სახელმწიფოებს.

სწორად ჩამოყალიბებული კიბერუსაფრთხოების პოლიტიკა და მდგრადი ტექნოლოგიური ინფრასტრუქტურა საშუალებას მოგვცემს სრულად გამოვიყენოთ ციფრული ტექნოლოგიების შესაძლებლობები, განვავითაროთ ინოვაცია და ერთდროულად დავიცვათ ჩვენი კრიტიკული სისტემები და უფლებები თანამედროვე სამყაროში.

დასკვნა

ციფრული ტექნოლოგიების გამოყენების ზრდამ შექმნა ახალი ეპოქა, რომელშიც ციფრული სივრცე აღარ არის მხოლოდ ინფორმაციის გაცვლის პლატფორმა, არამედ გადამწყვეტი ფაქტორია გლობალური უსაფრთხოების, ეკონომიკური განვითარებისა და სოციალური სტაბილურობისთვის. ტექნოლოგიური პროგრესი – ხელოვნური ინტელექტი, ინტერნეტი ნივთების (IoT), ბლოკჩეინი, ღრუბლოვანი სერვისები, 5G ქსელები – უზრუნველყოფს უდიდეს შესაძლებლობებს საზოგადოებისთვის, თუმცა ამავე დროს ქმნის ახალ საფრთხეთა სპექტრს, რომელთა დასაძლევად საჭიროა კომპლექსური, ინტერდისციპლინური და გლობალურად კოორდინირებული მიდგომა.

წარმოდგენილმა კვლევამ ნათლად წარმოაჩინა, რომ კიბერსაფრთხეები ტექნოლოგიებთან ერთად ვითარდება და მორგებულია მათ არსებულ სისუსტეებზე. დღეს კიბერშეტევა აღარ არის მხოლოდ ტექნიკური დანაშაული – ის წარმოადგენს ჰიბრიდული ომის ერთ-ერთ მძლავრ ინსტრუმენტს, რომელსაც იყენებენ როგორც კრიმინალური ჯგუფები, ისე სახელმწიფო სტრუქტურები პოლიტიკური, ეკონომიკური ან სამხედრო მიზნების მისაღწევად. ეს ქმნის ახალ რეალობას, სადაც კიბერუსაფრთხოება უნდა აღიქმებოდეს არა როგორც ტექნიკური, არამედ როგორც სტრატეგიული ეროვნული და საერთაშორისო ამოცანა.

კვლევაში განხილულმა კონკრეტულმა ქეისებმა – სტაქსნეტის თავდასხმიდან კოლონიური მილსადენის ინციდენტამდე – ცხადყო, რომ კრიტიკული ინფრასტრუქტურები, შესაძლოა, მწყობრიდან გამოიყვანოს მხოლოდ კიბერშეტევით, ფიზიკური ინტერვენციის გარეშე. ეს ამძაფრებს ტექნოლოგიური მოწყვლადობის რისკს, მით უმეტეს, როცა სახელმწიფოები ტექნოლოგიური ინოვაციების დანერგვაში უსწრებენ უსაფრთხოების პოლიტიკების განვითარებას.

მნიშვნელოვანია აღინიშნოს, რომ ტექნოლოგიის უსაფრთხო განვითარება შეუძლებელია ციფრული სოლიდარობის, მრავალდონიანი კოორდინაციისა და განათლებაზე დაფუძნებული ცნობიერების ამაღლების გარეშე. კიბერუსაფრთხოება აღარ არის მხოლოდ სპეციალისტების საზრუნავი – იგი მოითხოვს საზოგადოების ფართო მონაწილეობას, რადგან ინდივიდუალური შეცდომები ხშირად იქცევა სისტემური რღვევის გამომწვევად.

გარდა ამისა, თანამედროვე რეალობაში აუცილებელია კიბერმდგრადობის კონცეფციის დანერგვა – უსაფრთხოების ის მოდელი, რომელიც ეფუძნება არა მხოლოდ თავდაცვას, არამედ ინციდენტის მართვას, სწრაფ რეაგირებასა და აღდგენას. ეს გულისხმობს ტექნიკური, სამართლებრივი და პოლიტიკურ-სტრატეგიული ინსტრუმენტების ინტეგრაციას როგორც ეროვნულ, ისე საერთაშორისო დონეზე.

ნაშრომის ფარგლებში წარმოდგენილი ანალიზი ხაზს უსვამს, რომ ციფრული ტექნოლოგიების განვითარება ვერ ჩაითვლება წარმატებულად, თუ მას არ ახლავს საიმედო კიბერუსაფრთხოების არქიტექტურა. სახელმწიფოსა და კერძო სექტორის ვალდებულებაა, არა მხოლოდ მოახდინონ ინოვაციების ინტეგრაცია, არამედ შექმნან გამართული უსაფრთხოების ჩარჩოები, რომლებიც მიმართულია რისკის მინიმალიზაციისკენ.

საბოლოოდ, დასკვნა შეიძლება შეჯამდეს სამი ძირითადი გზავნილით:

1. ტექნოლოგიური პროგრესი და კიბერუსაფრთხოება უნდა განვითარდეს თანაბრად, რადგან დაუცველი ინოვაცია საფრთხეს უქმნის მთლიანად სისტემას;

2. კიბერუსაფრთხოება გლობალური თანამშრომლობის სფეროა, რომელიც მოითხოვს საერთაშორისო სტანდარტების ჰარმონიზაციას და საერთო პოლიტიკური ნების ჩამოყალიბებას;

3. ინფორმაციული მდგრადობა და განათლება საზოგადოებრივი იმუნიტეტის საფუძველია – მხოლოდ ინფორმირებული და ტექნოლოგიურად პასუხისმგებელი საზოგადოება შეძლებს ტექნოლოგიურ რისკზე ადეკვატურად რეაგირებას.

ციფრულ ეპოქაში, სადაც ყოველი ნაბიჯი ტოვებს კიბერკვალს, კიბერუსაფრთხოება აღარ არის მომავლის ამოცანა – ის არის დღევანდელობის გადაუდებელი აუცილებლობა. მხოლოდ ინკლუზიური, სტრატეგიულად გააზრებული და მდგრადი მიდგომით შევძლებთ ტექნოლოგიური შესაძლებლობების სრულფასოვან გამოყენებას ისე, რომ მათ არ ახლდეს სხვადასხვა კატასტროფული საფრთხე.

გამოყენებული ლიტერატურა

1. სიდამონიძე ნ., „STUXNET – გლობალური მნიშვნელობის კიბერ იარაღი, რომელმაც ბირთვული საფრთხე შეაჩერა“, ანალიტიკური ცენტრი, გვ.1. 2023. https://shorturl.at/ZFTbI (ბ.ნ. 23.07.2025).
2. Anderson R. J., “Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.)“, Wiley, pp. 1-30. 2020, https://download.e-bookshelf.de/download/0015/3092/35/L-G-0015309235-0048729244.pdf (ბ.ნ. 23.07.2025).
3. Bada A., & Nurse J. R. C., “Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)”, Information & Computer Security, 27(3), pp. 393-410, 2019, https://scispace.com/pdf/developing-cybersecurity-education-and-awareness-programmes-2pyn2vv1gy.pdf (ბ.ნ. 25.07.2025.)
4. Böhme R., & Moore T., “The iterated weakest link–A model of adaptive security investment“, Workshop on the Economics of Information Security (WEIS), pp. 81-102, 2012, https://www.scirp.org/pdf/JIS_2016033115021747.pdf (ბ.ნ. 23.07.2025).
5. Clarke R., & Knake R. K., “Cyber War: The Next Threat to National Security and What to Do About It”, Ecco, 2010, https://georgetownsecuritystudiesreview.org/2013/12/10/richard-a-clarke-and-robert-k-knakes-cyber-war-the-next-threat-to-national-security-and-what-to-do-about-it-harper-collins-2010/ (ბ.ნ. 24.07.2025).
6. Conti M., Dehghantanha A., Franke K., & Watson S. ‘’Internet of Things security and forensics: Challenges and opportunities”, Future Generation Computer Systems, 78, pp. 544-546, 2018, https://arxiv.org/pdf/1807.10438 (ბ.ნ. 23.07.2025).
7. Greenberg A., “Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers”, Doubleday, pp. 1-371, 2020, https://dokumen.pub/sandworm-a-new-era-of-cyberwar-and-the-hunt-for-the-kremlins-most-dangerous-hackers-978-0385544405.html (ბ.ნ. 23.07.2025).
8. Mohammad N., Khatoon R., Nilima S. I., Akter J., Kamruzzaman M., Sozib H. M., “Ensuring Security and Privacy in the Internet of Things: Challenges and Solutions”, Scientific Research, pp. 257-277, 2024, https://www.scirp.org/journal/paperinformation?paperid=135664 (ბ.ნ. 23.07.2025).
9. Scmitt M. N., “Tallinn Manual on the International Law Applicable to Cyber Warfare NATO Cooperative Cyber Defence Centre of Excellence”, Cambridge University Press, pp. 1-215. 2013 https://csef.ru/media/articles/3990/3990.pdf (ბ.ნ. 24.07.2025).
10. Singer, P. W., & Friedman, A. “Cybersecurity and Cyberwar: What Everyone Needs to Know“. Oxford University Press, pp. 1-33, 2014, https://api.pageplace.de/preview/ DT0400.9780199918102_A23618218/preview-9780199918102_A23618218.pdf (ბ.ნ. 24.07.2025)
11. Singh S., Hosen A. S. M., Yoon B., ‘’Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network”, IEEE Access, 8, pp. 13938-

13959, 2021, https://scispace.com/pdf/blockchain-security-attacks-challenges-and-solutions-for-the-47ml7a9t5w.pdf (ბ.ნ. 23.07.2025).

12. Svitlyk Y., ,,ყველაზე ცნობილი ჰაკერული თავდასხმები, რომლებიც მთელ მსოფლიოში მოხვდა", Root Nation, pp.1. 2023, https://ka.root-nation.com/en/articles-en/tech-en/en-most-famous-hacker-attacks/ (ბ.ნ. 25.07.2025).
13. Svitlyk Y., ,,OpenAI ახალი სუპერძალა: რა არის ChatGPT აგენტი?", Root Nation, pp. 1. 2023, https://ka.root-nation.com/en/articles-en/services-en/en-chatgpt-new-super-power/ (ბ.ნ. 25.07.2025).