Scientific and Practical Cyber Security Journal (SPCSJ) 8(4): 132 – 138 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

ინტერნეტ ფრაგმენტაცია როგორც ახალი გამოწვევა ინტერნეტის ერთიანობის, უსაფრთხოებისა და სტაბილურობისთვის

INTERNET FRAGMENTATION AS A NEW CHALLENGE FOR THE UNIFIED, SECURITY AND STABILITY OF INTERNET

ვლადიმერ სვანაძე
კავკასიის უნივერსიტეტის აფილირებული პროფესორი
საჯარო მმართველობის დოქტორი
Vladimer Svanadze
Affiliated Professor at the Caucasus University
Doctor in the Public Administration

აბსტრაქტი: გლობალური ინტერნეტის ერთიანობისთვის, უსაფრთხოებისა და სტაბილური განვითარებისთვის ახალ გამოწვევად იქცა ფრაგმენტაციის სულ უფრო ღრმა პროცესი, ანუ შეიძლება ითქვას, რომ ინტერნეტს ემუქრება დაშლის საფრთხე ერთმანეთთან სუსტად დაკავშირებულ ცალკეულ ფრაგმენტებად. ფრაგმენტაციის გამომწვევ მიზეზებად სახელდება მთელი რიგი შემაშფოთებელი ტენდენციები, რაც უკავშირდება ინტერნეტის ტექნოლოგიურ განვითარებას, ცალკეული ქვეყნების ინტერნეტ პოლიტიკებსა და კომერციულ საქმიანობას, ასევე არსებულ საერთაშორისო ვითარებას. ფაქტიურად, ფრაგმენტაციის პროცესმა გლობალური ინტერნეტ სივრცე დააყენა ახალი საფრთხის წინაშე, რაც გარდა აღნიშნულისა, ასევე უკავშირდება ცალკეული ავტოკრატული ხელისუფლებების მხრიდან მასზე ტოტალური კონტროლის დაწესებას, გლობალურად არსებულ ეთნოკონფლიქტებსა და საომარ მოქმედებებს, აგრეთვე გაზრდილ კიბერდანაშაულებებს. ყოველივე ეს კი არღვევს ინტერნეტის ერთიანობასა და მდგრადობას, საფრთხეს უქმნის მის სტაბილურ და უსაფრთხო განვითარების პროცესს. მოცემული პროცესი ასევე ეწინააღმდეგება გაერთიანებული ერების ორგანიზაციის ასამბლეის მიერ 2005 წელს მიღებულ ტუნისის დღის წესრიგს. ინტერნეტ ფრაგმენტაცია არის ახალი პროცესი და ის წარმოადგენს ფართო შესწავლის საკითხს. წინამდებარე ნაშრომი მოკლედ მიმოიხილავს ინტერნეტ ფრაგმენტაციის technical, commercial and governmental ფორმებს, და ამავდროულად, ყურადღებას ამახვილებს უფრო ფრაგმენტაციის political ასპექტზე. კერძოდ, მოცემული საკითხი განიხილება უკრაინის ომისა და რუსეთის ხელისუფლების ინტერნეტ პოლიტიკის კუთხით. სწორედ, ცალკეული ქვეყნების ინტერნეტ პოლიტიკები და მიდგომებია ის, რაც მიიჩნევა ფრაგმენტაციის პოლიტიკურ ნაწილად, და რაც ყველაზე მნიშვნელოვანია ხშირ შემთხვევაში პოლიტიკურ ფრაგმენტაციას გავლენა აქვს ფრაგმენტაციის დანარჩენ სამ ფორმაზე. აქვე ყურადღებას იმსახურებს ის გარემოებაც, რომ ისეთი გლობალური ორგანიზაციები, როგორებიც არის ICANN და RIPE NCC ჯერ - ჯეროვნად ახერხებენ შეინარჩუნონ დამოუკიდებელი პოზიცია და არ მოახდინონ საკითხის პოლიტიკურ ჭრილში გადაყვანა, რადგან ინტერნეტის ტექნიკური მართვის პოლიტიზირება წარმოადგენს იმ საფრთხეს, რასაც შეიძლება მოყვეს ინტერნეტ ფრაგმენტაციის შეუქცევადი პროცესი.

საკვანძო სიტყვები: ინტერნეტის ფრაგმენტაცია, ერთიანობა, მდგრადობა, გამძლეობა, უსაფრთხოება, სტაბილურობა, განვითარება, პოლიტიკური, ტექნიკური, კომერციული, სამთავრობო, პოლიტიკა.

ABSTRACT: The deepening process of fragmentation has become a new challenge for the unity, security and stable development of the global Internet. That is, it can be said that the Internet is in danger of disintegrating into separate fragments that are weakly connected to each other. A number of

disturbing trends related to the technological development of the Internet, the Internet policies and commercial activities of individual countries, as well as the current international situation are called the causes of fragmentation. In fact, the process of fragmentation has put the global Internet space in front of a new threat, which is also related to the establishment of total control over it by individual autocratic governments, the global ethno-conflicts and hostilities, as well as increased cybercrimes. All this violates the unity and stability of the Internet and threatens its stable and safe development process. This process also contradicts the Tunisian Agenda adopted by the United Nations Assembly in 2005. Internet fragmentation is a new process and it is a subject of extensive research. This paper briefly reviews the technical, commercial and governmental forms of Internet fragmentation, and at the same time, focuses on the political aspect of fragmentation. In particular, this issue is discussed in terms of the war in Ukraine and the Internet policy of the Russian government. It is the Internet policies and approaches of individual countries that are considered the political part of fragmentation, and in many cases political fragmentation has an impact on the other three forms of fragmentation. The fact that such global organizations as ICANN and RIPE NCC still manage to maintain an independent position and not to turn the issue into a political one deserves attention here, because the politicization of the technical management of the Internet represents the danger that may follow the irreversible process of Internet fragmentation.

KEYWORDS: Internet fragmentation, unity, sustainability, robustness, security, stability, development, political, technical, commercial, governmental, policy.

შესავალი

ინტერნეტისა და ინტერნეტ ტექნოლოგიების სწრაფი მიმართულებით განვითარების პოზიტიურ პროცესს თან ახლავს გარკვეული რისკები, რაც საფრთხეს უქმნის გლობალური ინტერნეტ ქსელის ერთიანობასა და უსაფრთხოებას, მის მდგრადობასა და სტაბილურ განვითარებას.

როცა ვსაუბრობთ გლობალური ინტერნეტ ქსელის ერთიანობაზე, უსაფრთხოებასა და სტაბილურობაზე, აუცილებლად უნდა აღვნიშნოთ გაერთიანებული ერების ორგანიზაციის გენერალური მდივნის მიერ მოწვეული ინტერნეტ მმართველობის ყოველწლიური ფორუმი, რომლის მუშაობაში ჩართული არის ყველა დაინტერესებული მხარე – საჯარო და კერძო სექტორები, სამოქალაქო საზოგადოება და აკადემიური წრეების წარმომადგენლები. ეს არის საუკეთესო პლატფორმა, სადაც ხდება ინტერნეტ სივრცეში მიმდინარე პროცესების შესახებ აზრთა გაცვლა, დისკუსია და გამოცდილებების გაზიარება დაინტერესებულ მხარეთა შორის, როგორც გლობალურ, ისე ეროვნულ და რეგიონულ დონეზე.

გაერთიანებული ერების ორგანიზაციის მხრიდან ინტერნეტ მმართველობის ფორუმის მოწვევას წინ უსწრებდა 2005 წელს საინფორმაციო საზოგადოებისთვის ტუნისის დღის წესრიგის მიღება. ეს მოიცავდა ტერმინის ინტერნეტის მმართველობის განმარტებასა და იმის აღიარებას, რომ ინტერნეტის მართვის პროცესი მოიცავს დაინტერესებულ მხარეთა ჩართულობას სხვადასხვა როლში. კერძოდ, საინფორმაციო საზოგადოებისთვის ტუნისის დღის წესრიგში ვკითხულობთ, რომ „ინტერნეტის მმართველობა არის მთავრობების, კერძო სექტორისა და სამოქალაქო საზოგადოების მიერ თავიანთი როლების შემუშავება და გამოყენება საერთო პრინციპების, ნორმების, წესების, გადაწყვეტილების მიღების პროცედურებისა და პროგრამების, რომლებიც აყალიბებენ ინტერნეტის ევოლუციას და გამოყენებას“. აქვე უნდა აღინიშნოს, რომ ტუნისის დღის წესრიგის 72 - ე პარაგრაფი ადგენს ინტერნეტ მმართველობის ფორუმის მანდატს, სადაც ვკითხულობთ, რომ ფორუმზე უნდა ხდებოდეს:

a. „.....ინტერნეტის მართვის ძირითად ელემენტებთან დაკავშირებული საჯარო პოლიტიკის საკითხების განხილვა, რათა ხელი შეუწყოს ინტერნეტის მდგრადობას, გამძლეობას, უსაფრთხოებას, სტაბილურობას და განვითარებას.....“

ფაქტიურად, გაერთიანებული ერების ორგანიზაციის ასამბლეა აღიარებს ფორუმის მნიშვნელობას ინტერნეტის მდგრადობის, გამძლეობის, უსაფრთხოების, სტაბილურობისა და განვითარების ხელშეწყობაში.

ინტერნეტ ფრაგმენტაციის ფორმები

სწორედ ინტერნეტ და ინტერნეტ ტექნოლოგიების სულ უფრო აქტიურმა გამოყენებამ კიდევ უფრო გაზარდა მისი მნიშვნელობა და მასზე დამოკიდებულება. გარდა ამისა, ინტერნეტი და ზოგადად, კიბერსივრცე დადგა ახალი საფრთხის წინაშე, რაც უკავშირდება ცალკეული ავტოკრატული ხელისუფლებების მხრიდან მასზე ტოტალური კონტროლის დაწესებას, გლობალურად არსებულ ეთნოკონფლიქტებსა და საომარ მოქმედებებს, გაზრდილ კიბერდანაშაულებს. ყოველივე ეს კი არღვევს ინტერნეტის ერთიანობასა და მდგრადობას, საფრთხეს უქმნის მის სტაბილურ და უსაფრთხო განვითარების პროცესს. მოცემული პროცესი ასევე ეწინააღმდეგება გაერთიანებული ერების ორგანიზაციის ასამბლეის მიერ თავის დროზე მიღებულ ტუნისის დღის წესრიგს [1-2].

ბოლო წლებში სულ უფრო ხშირად გამოითქმის შეშფოთება იმის თაობაზე, რომ ინტერნეტს ემუქრება დაშლის საფრთხე ერთმანეთთან სუსტად დაკავშირებულ ცალკეულ ფრაგმენტებად. მთელი რიგი შემაშფოთებელი ტენდენციები, რაც უკავშირდება ტექნოლოგიურ განვითარებას, სახელმწიფოების ინტერნეტ პოლიტიკასა და კომერციულ საქმიანობას, ასევე არსებულ საერთაშორისო ვითარებას, ვრცელდება ინტერნეტ ქსელში, მის ცალკეულ ფენებში, რაც გავლენას ახდენს პროცესზე, რასაც უწოდეს ინტერნეტ ფრაგმენტაცია. თუმცა, უნდა აღინიშნოს, რომ ჯერ კიდევ არ არსებობს ფართო გაგება იმისა თუ რა არის და რა არ არის „ფრაგმენტაცია“, ან რა რისკებს უქმნის ის ინტერნეტის, იგივე კიბერსივრცის ერთიანობას, სტაბილურობასა და უსაფრთხოებას.

აქ ჩნდება კითხვა რა არის „ინტერნეტ ფრაგმენტაცია“ და როგორ შეიძლება ეს ტერმინი თუ ქმედება განისაზღვროს? ინტერნეტ ფრაგმენტაცია, იგივე Splinternet, ეს არის ინტერნეტის საწინააღმდეგო მოვლენა, მისი საპირისპირო, რომლის მიხედვით ღია, უსაფრთხო და სტაბილური გლობალურად ერთიანი ინტერნეტი, რომლითაც ჩვენ ვსარგებლობთ, იყოფა ცალკეულ ერთმანეთისგან იზოლირებულ ქსელებად, რომლებიც კონტროლდება სახელმწიფოებისა და კორპორაციების მიერ. გარდა ამისა, „ინტერნეტ ფრაგმენტაციის“ მსგავს განსაზღვრებას, ბოლო დროს განვითარებული გლობალური მოვლენების გათვალისწინებით, შეიძლება დავუმატოთ ასევე საომარი მოქმედებები და ეთნოკონფლიქტები, რომლებიც უკვე ფიზიკურად აზიანებს კიბერსივრცის ერთიანობას [3-4].

არსებობს ინტერნეტ ფრაგმენტაციის ყველასთვის ნაცნობი სამი ფორმა:

1. **ტექნიკური ფრაგმენტაცია** – ეს არის საბაზისო ინფრასტრუქტურის პირობები, რომლებიც აფერხებენ სისტემების სრულყოფილ და თანხვედრილ ურთიერთობას, მონაცემთა პაკეტების გაცვლასა და ინტერნეტის ნორმალურ ფუნქციონირებას;
2. **სახელმწიფო ფრაგმენტაცია** – ცალკეული ქვეყნების მთავრობების ინტერნეტ პოლიტიკა და ქმედებები, რომლებიც ზღუდავს ან ხელს უშლის ინტერნეტის

გარკვეულ გამოყენებას საინფორმაციო რესურსების შესაქმნელად, მათი გავრცელების ან წვდომისათვის;

3. **კომერციული ფრაგმენტაცია** – ბიზნეს პრაქტიკა, რომელიც ზღუდავს ან ხელს უშლის ინტერნეტის გარკვეულ გამოყენებას საინფორმაციო რესურსების შესაქმნელად, მათი გავრცელების ან წვდომისათვის.

აქვე, ინტერნეტ ფრაგმენტაციის მეოთხე ტიპად შეიძლება დავამატოთ – ინტერნეტ ფრაგმენტაცია, რომელიც მივიღეთ ამა თუ იმ მთავრობების როგორც შიდა, ისე საგარეო ინტერნეტ პოლიტიკის, საომარი მოქმედებებისა და ზოგადად, გლობალურად თუ რეგიონულად არსებული არამდგრადი ვითარების შედეგად, რაც ზიანს აყენებს ინტერნეტის ერთიანობას, უსაფრთხოებასა და სტაბილურობას [5].

ამ მეოთხე ტიპს უწოდებენ პოლიტიკურ ფრაგმენტაციას, რომელსაც ზოგი მოიხსენიებს სახელმწიფო ფრაგმენტაციასთან ერთად. აუცილებელია აღინიშნოს ის გარემოება, რომ ინტერნეტ ფრაგმენტაციის თითოეული ტიპი შეიძლება ძალზედ განსხვავდებოდეს მთელი რიგი განზომილებების მიხედვით. ამ შემთხვევაში გამოვყოთ ოთხი ძირითადი მახასიათებელი, კერძოდ:

- **წარმოშობა** – ანუ არსებობს თუ არა ფრაგმენტაციის ესა თუ ის ფორმა და რა პოტენციური საფრთხის შემცველია ფრაგმენტაციის კონკრეტული ფორმა;
- **მიზანმიმართულობა** – ფრაგმენტაცია ეს არის მიზანმიმართული მოქმედების შედეგი თუ გაუთვალისწინებელი, სპონტანური შედეგი;
- **გავლენა** – არის ფრაგმენტაცია ღრმა, სტრუქტურული და კონფიგურაციული, თუ უფრო ზედაპირული, ვიწრო და შეზღუდული პროცესების ერთობლიობა;
- **ხასიათი** – ზოგადად, არის თუ არა ფრაგმენტაცია დადებითი, უარყოფითი ან ნეიტრალური.

პოლიტიკური გამოწვევები და ინტერნეტ ფრაგმენტაციის არსებული საფრთხეები

როცა პოლიტიკური ფორმის ფრაგმენტაციაზე ვსაუბრობთ, მსჯელობა იწყება უკრაინა - რუსეთის ომით, რაც დიდ გავლენას ახდენს სწორედ კიბერსივრცეზე. უკრაინაში რუსეთის შეჭრის შემდეგ გაჩნდა საფრთხე, რომ რუსეთი გამოეყოფოდა გლობალურ ინტერნეტს, რაც მართალია არ მოხდა, მაგრამ ჩვენ შეიძლება გავხდეთ გლობალური ინტერნეტის უფრო ფუნდამენტური ფრაგმენტაციის დაწყების პროცესის მოწმენი.

რუსეთის ფედერაციის მთავრობამ დაავალა რუსეთის ოპერატორებს, რომ 2022 წლის 11 მარტისთვის გამხდარიყვნენ დამოუკიდებელნი გლობალური ქსელისგან. თუმცა, მართალია, რომ გლობალური ქსელისგან გამოიყოფა მხოლოდ სახელმწიფო ვებგვერდი და სერვერები, მაგრამ რუსეთის გამოყოფა გლობალური ინტერნეტ ქსელისგან ისევ განიხილება და წარმოადგენს მსჯელობის საგანს.

უკრაინაში შეჭრის შემდეგ, რუსეთმა მართლაც გადადგა ქმედითი ნაბიჯები, კერძოდ, რუსეთის ხელისუფლებამ დაბლოკა მრავალი საინფორმაციო საიტი, აკრძალა მრავალი პოპულარული დასავლური ინტერნეტ სერვისი და სოციალური პლატფორმა, მათ შორის Facebook, Instagram და Twitter, შემოიღო ახალი კანონი ე. წ. „fake news“ და დეზინფორმაცია – პროპაგანდის გავრცელების შესახებ. მიუხედავად მსგავსი რეპრესიული ქმედებებისა, რუსეთმა არ გაწყვიტა კავშირი გლობალურ ინტერნეტთან. 2019 წელს მიღებული რუსეთის კანონი „ინტერნეტის სუვერენიტეტის“ შესახებ ინტერნეტის მომწოდებელი ოპერატორებისგან ითხოვს ტრაფიკის მარშრუტიზაცია განახორციელონ იმ გაცვლითი წერტილების საშუალებით, რომლებიც დამტკიცებულია Роскомнадзор - ის ფედერალური სააგენტოს მიერ. გარდა ამისა, კანონი Роскомнадзор - ს უფლებას აძლევს აიძულოს

ინტერნეტის მომსახურების მომწოდებელი კომპანიები განახორციელონ ტრაფიკის მარშრუტიზაცია ბლოკირების სპეციალური სისტემებით, რომელთა გამოყენება ხელისუფლებას შეუძლია ტრაფიკის ფილტრაციისა და მათთვის სასურველი მარშრუტიზაციისთვის. უფრო მეტიც, 2021 წლიდან რუსეთის ინტერნეტ მომწოდებელ კომპანიებს უნდა შეეძლოთ დაამუშაონ მოთხოვნები დომენური სახელების სისტემებზე, სერვერებზე, რომლებიც განლაგებულია ქვეყნის შიგნით და გლობალური ინტერნეტ ქსელიდან გათიშვის შემთხვევაში შესაძლებელი იქნება ინტერნეტ რესურსების მოძებნა. ძნელი სათქმელია თუ როგორ იმუშავებს ეს სისტემები რეალურ სიტუაციაში, თუმცა ფაქტია, რომ ავტონომიური სეგმენტი, რომელიც იმეორებს გლობალური ინტერნეტის ფუნქციების დიდ ნაწილს, უფრო რთულად რეალიზდება ტექნიკური კუთხით, ვიდრე პოლიტიკურად. ყოველ შემთხვევაში, რუსეთის შესაძლებლობა შეწყვიტოს მონაცემთა გადაცემა არ წარმოადგენს რაღაც შეუძლებელს და ეს არ გამოიწვევს მომსახურების ხარისხის გაუარესებას.

და მაინც, ომმა უკრაინაში შესაძლოა მისცეს უფრო დიდი ბიძგი გლობალური ციფრული კავშირის ფუნდამენტურ ფრაგმენტაციას. ერთ - ერთ ასპექტს წარმოადგენს ინტერნეტის ტექნიკური მართვის პოლიტიზება, და ამასთან ერთად, ინტერნეტის ფრაგმენტაციის გრძელვადიანი რისკი, რაც იძლევა გარანტიას, რომ მონაცემები შეიძლება გადაეცეს მრავალი ქსელის საშუალებით, რომლებიც ერთად შეადგენს ინტერნეტს, როგორც ერთიან მთლიანობას. რუსეთის აგრესიის საპასუხოდ, უკრაინა შეეცადა გაეწყვიტა რუსეთის კავშირები გლობალურ ინტერნეტთან და ამით შეეზღუდა მისი შესაძლებლობები გადაეჭრა მოთხოვნები ქვეყნის შიგნით. ამ მიზნით, უკრაინამ გააგზავნა წერილი ICANN - თან, რომელიც კოორდინაციას უწევს დომენური სახელების სისტემებს, და მიმართა თხოვნით, გააუქმოს რუსეთის ფედერაციაში გამოშვებული უმაღლესი დონის დომენები (მაგ., „.ru“, „.рф“ და „.su“) და გაეთიშა რუსეთში მდებარე DNS root სერვერები. უკრაინის ხელისუფლებამ ასევე სთხოვა RIPE - ს, რეგიონულ ინტერნეტ რეესტრს ევროპის, ახლო აღმოსავლეთისა და ცენტრალური აზიის ნაწილისთვის, გაეუქმებინა რუსული IP მისამართები. თუმცა, ორივე ორგანიზაციამ, ICANN - მა და RIPE - მა უარყვეს უკრაინის მოთხოვნა და ხაზი გაუსვეს მათი ნეიტრალიტეტის მნიშვნელობას ტექნიკური ინტერნეტის მართვაში, გლობალური და თავსებადი ინტერნეტის შენარჩუნების მიზნით [6-8].

ფაქტობრივად, უკრაინის მოთხოვნის დაკმაყოფილება იქნებოდა საგარეო პოლიტიკისა და ტექნიკური ადმინისტრაციის შერწყმის პრეცედენტი, რაც, თავის მხრივ, ძირს უთხრის ამ ინსტიტუტების, როგორც საყოველთაოდ ლეგიტიმური მმართველობის ორგანოების როლს. თუ ინტერნეტის ტექნიკური მართვის შესახებ გლობალური კონსენსუსი გაქრება, კონკურენტი ინსტიტუტების გაჩენა იქნება ახალი გამოწვევა და მწვავე რისკი ინტერნეტის ერთიანობისთვის. მიუხედავად იმისა, რომ მმართველობითი ინსტიტუტები ეწინააღმდეგებოდნენ პოლიტიკურ დაკვეთებს, ციფრულ ინფრასტრუქტურაზე კონტროლის გაძლიერება, თავის მხრივ, გამოიწვევს ინტერნეტ ფრაგმენტაციის პროცესის კიდევ უფრო მეტ გაძლიერებას.

ფაქტობრივად, რუსეთის უკრაინაში შეჭრის შემდეგ, რუსეთის გლობალური ინტერნეტიდან გათიშვა ჯერ კიდევ არ მომხდარა. თუმცა, უნდა აღინიშნოს ის გარემოება, რომ ომი ხაზს უსვამს სახელმწიფოების დიდ ცდუნებას, ინტერნეტზე ტექნიკური კონტროლი და ინტერნეტის მთლიანი ინფრასტრუქტურა გამოიყენონ როგორც იარაღი. მიუხედავად იმისა, რომ დროულად აღიკვეთა მცდელობები კიბერსივრცის სრული კონტროლი გამოყენებული ყოფილიყო როგორც იარაღი, ომის გარშემო ფართო

გეოპოლიტიკური დაპირისპირება ამძაფრებს გლობალური ციფრული კავშირის ღრმა ფრაგმენტაციას, ხდის მას უფრო ფუნდამენტურს.

როცა ვსაუბრობთ ინტერნეტის ინფრასტრუქტურაზე კონტროლის დაწესებაზე, აუცილებლად უნდა აღინიშნოს ირანისა და ჩინეთის ხელისუფლებების მიდგომები მოცემულ საკითხთან, რაც ძირითადად არის პოლიტიკური გადაწყვეტილებები და, რაც გარკვეულ ზიანს აყენებს გლობალური ინტერნეტის ერთიანობას, მდგრადობას, უსაფრთხოებასა და სტაბილურობას და ხელს უწყობს ინტერნეტ ფრაგმენტაციის პროცესს [9].

ირანის ისლამურ რესპუბლიკაში გამკაცრებულია კიბერსივრცის კონტროლი, რაზეც მეტყველებს არსებული ცენზურის წესები, დაბლოკილია მრავალი ვებგვერდი, ასევე ხელისუფლების მხრიდან არსებობს ბლოგერების მკაცრი კონტროლი და მათი საქმიანობის მუდმივი შევიწროება. ირანის ენერგოსისტემაზე განხორციელებულმა კიბერშეტევამ და ამით მიყენებულმა ზიანმა ირანის ხელისუფლება კიდევ ერთხელ მიიყვანა იმ დასკვნამდე, რომ საჭიროა ეროვნული ინტერნეტის შექმნა და საკუთარი კიბერსივრცის გაძლიერება. ხელისუფლებამ დაიწყო საერთაშორისო სოციალური ქსელების ალტერნატიული შიდა მოხმარების სოციალური ქსელების განვითარების პროცესის დაფინანსება, რაც ხელს უწყობს საკუთარ მოსახლეობაზე ვირტუალურ სივრცეში კონტროლის დაწესებას. შედეგად, ირანში დღეს არსებული სურათის მიხედვით, ქვეყანაში მაქსიმალურად არის შეზღუდული საერთაშორისო სოციალური ქსელები, რითაც გზა გაეხსნა მხოლოდ ქვეყნის ხელისუფლების ხელშეწყობით შექმნილ ეროვნულ ალტერნატიულ ონლაინ პლატფორმების ფუნქციონირებას. 2015 წელს ჩინეთის ხელისუფლებამ წარმოადგინა ახალი გეგმა ინტერნეტ პოლიტიკასთან დაკავშირებით, რომელიც ითვალისწინებს ქვეყნის ეკონომიკურ და ტექნოლოგიურ ზრდას კიბერსივრცის მეშვეობით. ფაქტობრივად, ჩინეთის ხელისუფლების ინტერნეტ პოლიტიკა მიმართულია გლობალური ინტერნეტ სივრციდან ნაწილობრივ გამოყოფაზე და მისი პოლიტიკა ცნობილია, როგორც "Great Firewall". იმავე წელს შემოღებულ იქნა ახალი კანონი, რომლის თანახმად, ყველა მომხმარებელი ვალდებული იყო ონლაინ პლატფორმაზე სარეგისტრაციო ფორმაში შეეყვანა თავისი მონაცემები. ამ კანონის თანახმად, კომპანიებს (საუბარია ISP კომპანიებზე), რომელთა გვერდზეც რეგისტრირდებოდნენ მომხმარებლები, ევალებოდათ მყისიერად გადაემოწმებინათ მიწოდებული ინფორმაცია და მხოლოდ ამის შემდეგ დაეშვათ მომხმარებლისთვის ვებგვერდზე წვდომა, მათ უნდა ეკონტროლებინათ ყველა საჯარო ანგარიში და დაეხარისხებინათ ისინი ინფორმაციის მიხედვით. გარდა ამისა, ჩინეთმა დაიწყო კონტროლის განხორციელება არა მარტო საკუთარ მოქალაქეებზე, არამედ მათ შეუზღუდეს ინტერნეტ პლატფორმებზე წვდომა უცხო ქვეყნის მოქალაქეებსაც. ამჟამად, მხოლოდ ჩინური ტელეფონის ნომრით არის შესაძლებელი ონლაინ აპლიკაციაზე წვდომა და ვებგვერდები გამოსაყენებლად მიუწვდომელია ჩინეთის ტერიტორიის ფარგლებს გარედან. უცხოელი მოქალაქეებისათვის საგრძნობლად გართულებულია ჩინურ ვებგვერდებზე და აპლიკაციებზე წვდომა. მათ უნდა გაიარონ საკმაოდ ხანგრძლივი და რთული პროცესი რეგისტრაციისთვის, რისთვისაც მოეთხოვებათ წარმოადგინონ თავისი პერსონალური ინფორმაცია. ქვეყანას გააჩნია დიდი ამბიციები და თუ გადავხედავთ მის აქტიურობას საერთაშორისო დონეზე, მაშინ ვნახავთ, რომ დღევანდელ მსოფლიოში არსებობს დიდი რაოდენობით ჩინური ინვესტიცია, რომელიც ინტერნეტ სივრცისკენ არის მიმართული. ფაქტია, რომ ჩინეთი აშენებს საკუთარ, ეროვნულ ინტერნეტს, რაც უკვე ნიშნავს ინტერნეტ ფრაგმენტაციას. ჩინეთის იდეოლოგიაში წარმოდგენილი ინტერნეტი სულაც არ არის ღია, თავსებადი და თავისუფალი. შეიძლება ითქვას, რომ ჩინეთს არ აქვს მიზანი მსოფლიო ინტერნეტი კიბერშეტევებისგან გახადოს

უფრო უსაფრთხო, არამედ ცდილობს შექმნას კიბერსივრცის სრულიად განსხვავებული არქიტექტურა, რომელიც მორგებული იქნება არა საერთაშორისო უსაფრთხოებაზე არამედ ჩინეთის ეროვნულ ინტერესებზე. ჩინეთი ქმნის ფრაგმენტულ კიბერლანდშაფტს და მისი მთავარი მიზანი გახლავთ გახდეს დომინანტი მსოფლიო საზოგადოებაზე ინტერნეტის გავლით.

დასკვნა

და ბოლოს, დასკვნის სახით შეიძლება ითქვას, რომ გლობალურ ციფრულ ხელშეკრულებაზე მუშაობის ფარგლებში, გრძელდება გლობალური და ინკლუზიური პროცესი ციფრული სივრცის ერთიანი პრინციპების შემუშავების კუთხით. ეს არის შესაძლებლობა, რომლის მიხედვით მოხდება გლობალური ინტერნეტის აღიარება, როგორც საერთო პრობლემების გადაწყვეტის მნიშვნელოვანი ინსტრუმენტის. ამაზე მეტყველებს გაერთიანებული ერების ორგანიზაციის ბოლო შეხვედრაზე მიღებული გადაწყვეტილებებიც.
ზოგადად, უნდა აღინიშნოს, რომ ინტერნეტის ფრაგმენტაციის პროცესის შეჩერება რთული ამოცანაა, მაგრამ ეს შესაძლებელია სახელმწიფოთა შორისი მაღალი დონის შეხვედრებით, ფოკუსირებული დიალოგებითა და ძალისხმევით იმ ძირითად ფრაგმენტულ ფაქტორებზე, როგორიცაა კიბერჯაშუშობა, ინტერნეტის ინფრასტრუქტურაზე კონტროლის დაწესების მცდელობა და ინტერნეტისა და ინტერნეტ ტექნოლოგიების გამოყენებაზე, როგორც იარაღის ქვეყნებისა და ადამიანთა წინააღმდეგ.
და მაინც ჯერ ისევ რჩება კითხვა გვაქვს თუ არა ფრაგმენტაცია, და რას შეიძლება ვუწოდოთ ფრაგმენტაცია? რამდენად წარმოადგენს ის საფრთხეს გლობალური ინტერნეტისთვის, მისი უსაფრთხოების, სტაბილურობისა და ერთიანობისთვის?

დადასტურება

აღნიშნული ნაშრომის შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის მხარდაჭერით - CG-24-220

ბიბლიოგრაფია

1. Vladimer Svanadze, Maksim Iavich, Impact of Internet Fragmentation on the Unity, Security, and Stability of Global Internet; CPITS 2024 Cybersecurity Providing in Information and Telecommunication Systems 2024; CEUR, Vol-3654, pp. 520–525. https://ceur-ws.org/Vol-3654/
2. Svanadze, Vladimer. 2023. “Challenges of Internet Fragmentation and Global Cyberspace.” Scientific and practical cyber security journal – SPCSJ № 4 vol. 07, December 2023;
3. Christopher Meinel, „Russia’s War Against Ukraine is Catalyzing Internet Fragmentation“, Council on Foreign Relations, 2023;
4. Kamaitis Konstantions, “Internet Fragmentation: Why It Matters for Europe”, 2023;
5. Stokel-Wallker Chris, “Russia Inches Toward Its Splinternet”, 2022;
6. Sullivan Andrew, “Misguided Policies the World over are slowly killing the Open Internet”, Internet society, 2023;
7. Drake J. drake, Cerf Vinton G., Kleinwachter Wolfgang, “Internet Fragmentation: An Overwiev” , 2016.
8. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019 https://journal.scsa.ge/papers/cyber-security-european-standards-in-business/.
9. Vladimer Svanadze, Maksim Iavich, and Sergiy Gnatyuk, Challenges and Solutions for Cybersecurity and Information Security Management in Organizations; CPITS 2024 Cybersecurity Providing in Information and Telecommunication Systems 2024; Vol-3654, pp. 497–504. https://ceur-ws.org/Vol-3654/