Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 105 – 110 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ინტერნეტ ფარგმენტაციის გამოწვევები და გლობალური კიბერსივრცე

ვლადიმერ სვანაძე[1]

[1]საჯარო მმართველობის დოქტორი, ბიზნესისა და ტექნოლოგიების უნივერსიტეტის აფილირებული პროფესორი

რეზუმე: „ინფორმაციული აფეთქება“ ასე უწოდეს თავის დროს ინფორმაციული ტექნოლოგიების გლობალური განვითარებისა და მომხმარებლის სწრაფი ტემპებით ზრდის პროცესს. მოცემული პროცესი კიდევ უფრო დააჩქარა პანდემიის არსებობამ, რომლის დროსაც ინტერნეტისა და ინტერნეტ ტექნოლოგიების გამოყენებამ როგორც საყოფაცხოვრებო, ისე პროფესიულ დონეზე არნახულ ზღვარს მიაღწია. სამწუხაროდ, 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 ავღნიშნოთ გაერთიანებული ერების ორგანიზაციის გენერალური მდივნის მიერ მოწვეული ინტერნეტ მმართველობის ფორუმი[1], 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 რეგიონალურ დონეზე.

საკვანძო სიტყვები: ინტერნეტი, ინტერნეტ ტექნოლოგიები, ინტერნეტ ფრაგმენტაცია, კიბერსივრცე, კიბერუსაფრთხოება, კიბერდანაშაული, ინტერნეტ პროტოკოლები, კონფლიქტები, ინტერნეტ მმართველობის ფორუმი, ტუნისის დღის წესრიგი

ABSTRACT: "Information explosion" was the name given to the process of global development of information technologies and rapid growth of users. This process was further accelerated by the existence of the pandemic, during which the use of the Internet and Internet technologies at both the household and professional levels reached an unprecedented limit. Unfortunately, the positive process of rapid development of the Internet and Internet technologies is accompanied by certain risks, which threaten the unity and security of the global Internet network, its stability and stable development. When we talk about the unity, security and stability of the global Internet network, we must mention the Internet Governance Forum convened by the Secretary General of the United Nations, whose work involves all interested parties - public and private sectors, civil society and representatives of academic circles. It is the best platform where the exchange of ideas, discussion and sharing of experiences about the processes taking place in the Internet space takes place among the interested parties at the global, national and regional levels.

KEYWORDS: Internet, Internet Technology, Internet Fragmentation, Cyberspace, Cybersecurity, Cybercrime, Internet Protocols, Conflicts, Internet Governance Forum, Tunis Agenda

[1] https://www.intgovforum.org/en/about#about-us

1. შესავალი

2005 წელს გაერთიანებული ერების ორგანიზაციის მიერ მიღებულ იქნა საინფორმაციო საზოგადოებისთვის ტუნისის დღის წესრიგის მიღება[2], რაც წინ უსწრებდა ინტერნეტ მმართველობის ფორუმის მოწვევას. ეს მოიცავდა ტერმინის ინტერნეტის მმართველობის განმარტებასა და იმის აღიარებას, რომ ინტერნეტის მართვის პროცესი მოიცავს დაინტერესებულ მხარეთა ჩართულობას სხვადასხვა როლებში. 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“ (Tunis Agenda for the Information Society) [1].

აქვე უნდა აღინიშნოს, რომ ტუნისის დღის წესრიგის 72 - ე პარაგრაფი ადგენს ინტერნეტ მმართველობის ფორუმის მანდატს[3], სადაც ვკითხულობთ, რომ:

- **a)** ინტერნეტის მართვის ძირითად ელემენტებთან დაკავშირებული საჯარო პოლიტიკის საკითხების განხილვა, რათა ხელი შეუწყოს ინტერნეტის მდგრადობას, გამძლეობას, უსაფრთხოებას, სტაბილურობას და განვითარებას;
- **b)** ხელი შეუწყოს დისკუსიას იმ ორგანოებს შორის, რაც ეხება ინტერნეტთან დაკავშირებით სხვადასხვა საერთაშორისო თუ საჯარო პოლიტიკას და განიხილავს ისეთ საკითხებს, რომლებიც არ განეკუთვნება არცერთ არსებულ ორგანოს სფეროს;
- **c)** მათ დაქვემდებარებაში მყოფ საკითხებზე შესაბამის სამთავრობათაშორისო ორგანიზაციებთან და სხვა ინსტიტუტებთან ურთიერთობა;
- **d)** ინფორმაციისა და საუკეთესო პრაქტიკის გაცვლის ხელშეწყობა და ამ კუთხით აკადემიური, სამეცნიერო და ტექნიკური საზოგადოებების ექსპერტიზის სრულად გამოყენება;
- **e)** ურჩიეთ ყველა დაინტერესებულ მხარეს განვითარებად სამყაროში ინტერნეტის ხელმისაწვდომობისა და მისი დაჩქარების გზებისა და საშუალებების შეთავაზებაში;
- **f)** გააძლიეროს დაინტერესებული მხარეების ჩართულობა ინტერნეტის მართვის არსებულ და/ან მომავალ მექანიზმებში, განსაკუთრებით განვითარებადი ქვეყნებიდან;
- **g)** აღმოაჩინოს წამოჭრილი საკითხები, მიაწოდოს ისინი შესაბამის ორგანოებსა და ფართო საზოგადოებას. საჭიროების შემთხვევაში, რეკომენდაციების გაცემა;
- **h)** წვლილის შეტანა განვითარებად ქვეყნებში ინტერნეტის მართვის შესაძლებლობების განვითარებაში, ცოდნისა და ექსპერტიზის ადგილობრივი წყაროების სრულად გამოყენებით;
- **i)** ინტერნეტის მართვის პროცესებში WSIS[4] პრინციპების ხელშეწყობა და შეფასება;
- **j)** კრიტიკულ ინტერნეტ რესურსებთან დაკავშირებული საკითხების განხილვა;
- **k)** დახმარება ინტერნეტის ბოროტად გამოყენების შედეგად წარმოქმნილი საკითხების გადაწყვეტაში, რაც განსაკუთრებით აწუხებს ყოველდღიურ მომხმარებლებს;
- **l)** საქმიანობის ღიაობა.

[2] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[3] https://www.iisd.org/system/files/publications/igf_mandate_review.pdf
[4] World Summit on the Internet Society

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

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 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 თავის დროზე მიღებულ ტუნისის დღის წესრიგს [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 სამიანობას, 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, მისი საპირისპირო. Splinternet არის იდეა, 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].

2. ინტერნეტის ფრაგმენტაციის ფორმები

განსაზღვრებიდან გამომდინარე, 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 ინფორმაციის რესურსების შესაქმნელად, მათი გავრცელების ან წვდომისათვის.

აქვე, ინტერნეტ ფრაგმენტაციის მეოთხე ტიპად შეიძლება დავამატოთ - **საერთაშორისო, გლობალური თუ რეგიონალური ინტერნეტ ფრაგმენტაცია,** რომელიც მივიღეთ ამა თუ იმ მთავრობების როგორც შიდა, ისე საგარეო ინტერნეტ პოლიტიკების, საომარი მოქმედებებისა და ზოგადად, გლობალურად თუ რეგიონალურად არსებული არამდგრადი ვითარების შედეგად, რაც ზიანს აყენებს ინტერნეტის ერთიანობას, უსაფრთხოებასა და სტაბილურობას [4-5].

სანამ თითოეული ფორმის განხილვას დავიწყებთ აუცილებელია ასევე აღინიშნოს ის გარემოება, რომ ინტერნეტ ფრაგმენტაციის თითოეული ტიპი შეიძლება ძალზედ განსხვავდებოდეს მთელი რიგი განზომილებების მიხედვით. ამ შემთხვევაში გამოვყოთ ოთხი ძირითადი მახასიათებელი, კერძოდ:

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

3. პრობლემური კატეგორიები

ინტერნეტ ფრაგმენტაციის თითოეულ ფორმის განხილვისას განიხილება სხვადასხვა სახის პრობლემური კატეგორიები და მათგან გამომდინარე ფრაგმენტაციის სახეობები, კერძოდ [6]:

1. ტექნიკური ფრაგმენტაციის დროს განიხილება ოთხი პრობლემური კატეგორია - ინტერნეტ მისამართები, ინტერნეტ დაერთებები, ინტერნეტის დასახელება და მისი უსაფრთხოება. მოცემული კატეგორიების ფარგლებში იდენტიფიცირებულია სხვადასხვა ხარისხისა და მნიშვნელობის ფრაგმენტაციის შემდეგი 12 სახეობა:
   - ქსელური მისამართების ტრანსლაცია (Network Address Translation);
   - IPv6 - ს შეუთავსებლობა და ორმაგი დასტის მოთხოვნა (IPv6 შეუთავსებლობა და ორმაგი წყობის მოთხოვნა);
   - კორუფციის მარშრუტირება;
   - Firewall-ის დაცვა;
   - ვირტუალური კერძო ქსელის იზოლაცია და დაბლოკვა;
   - TOR “onion space” და “dark web”;
   - ინტერნაციონალიზებული დომენური სახელების (IDN) ტექნიკური შეცდომები;
   - ახალი ზოგადი ტოპ დონის დომენების ბლოკირება;
   - პერსონალური სახელების სერვერები და დანაწევრებული ჰორიზონტის DNS;
   - სეგმენტირებული Wi-Fi სერვისები სასტუმროებში, რესტორნებში და ა.შ.;
   - ალტერნატიული DNS წყაროების შესაძლებლობა;
   - სერტიფიცირების ორგანოების მიერ ყალბი სერთიფიკატების წარმოება.
2. სახელმწიფო ფრაგმენტაციის შემთხვევაში განიხილება შემდეგი ექვსი კატეგორია:
   - შინაარსი და ცენზურა;
   - ელექტრონული კომერცია და ვაჭრობა;
   - ეროვნული უსაფრთხოება;

- კონფიდენციალურობა და მონაცემთა დაცვა;
- მონაცემთა ლოკალიზაცია;
- ფრაგმენტაცია, როგორც ყოვლისმომცველი ეროვნული სტრატეგია.

მოცემული კატეგორიების ფარგლებში იდენტიფიცირებულია სხვადასხვა ხარისხის ფრაგმენტაციის შემდეგი 10 სახეობა:

- იმ ვებსაიტების, სოციალური ქსელების ან სხვა რესურსების გაფილტვრა და დაბლოკვა, რომლებიც არასასურველ კონტენტს გვთავაზობენ;
- იმ საინფორმაციო რესურსებზე თავდასხმები, რომლებიც არასასურველ კონტენტს გვთავაზობენ;
- ციფრული პროტექციონიზმი ელექტრონული კომერციის ძირითადი პლატფორმებისა და ინსტრუმენტების გამოყენებაზე ბლოკავს მომხმარებლების წვდომას;
- საერთაშორისო ურთიერთკავშირის ცენტრალიზაცია;
- თავდასხმები ეროვნულ ქსელებსა და ძირითად აქტივებზე;
- ადგილობრივი მონაცემთა დამუშავების ან/და შენახვის მოთხოვნები;
- მონაცემთა ნაკადის შესანარჩუნებლად, ტერიტორიის ფარგლებში არქიტექტურული ან მარშრუტის ცვლილებები;
- გარკვეული კატეგორიის მონაცემების ტრანსსასაზღვრო გადაადგილების აკრძალვები;
- „ეროვნული ინტერნეტ სეგმენტების“ ან „კიბერსუვერენიტეტის“ შექმნის სტრატეგიები;
- საერთაშორისო ჩარჩოები, რომლებიც შემზღუდავი პრაქტიკის ლეგიტიმაციას ისახავს მიზნად.

3. კომერციული ფრაგმენტაცია განიხილავს ხუთ კატეგორიას. კერძოდ, ესენია - თანასწორობა და სტანდარტიზაცია; ქსელის ნეიტრალიტეტი; ე.წ. “walled gardens”; გეო-ლოკალიზაცია და გეობლოკირება; ინფრასტრუქტურასთან დაკავშირებული ინტელექტუალური საკუთრების დაცვა [7]. მოცემულ შემთხვევაში იდენტიფიცირებულია სხვადასხვა ხარისხის ფრაგმენტაციის შემდეგი 6 სახეობა:

- პოტენციური ცვლილებები ურთიერთკავშირის ხელშეკრულებებში;
- პოტენციური საკუთრების ტექნიკური სტანდარტები, რომლებიც IoT-ში თავსებადობას აფერხებენ;
- ქსელის ნეიტრალიტეტიდან ბლოკირება, ჩახშობა ან სხვა დისკრიმინაციული გადახრები;
- ე.წ. “Walled gardens”
- კონტენტის გეობლოკირება;
- დასახელებისა და ნუმერაციის პოტენციური გამოყენება ინტელექტუალური საკუთრების დაცვის მიზნით შინაარსის დასაბლოკად.

ინტერნეტ ფრაგმენტაციის თითოეული ფორმის განხილვისას გვაქვს სხვადასხვა სახის პრობლემური კატეგორიები და მათგან გამომდინარე ფრაგმენტაციის სახეობები, თუმცა ფართოდ განიხილება ასევე ინტერნეტ ფრაგმენტაციის სწორედ ის მეოთხე სავარაუდო ფორმა, რაც უკავშირდება ეროვნულ თუ გლობალურ უსაფრთხოებას და, რომელიც აჩვენებს ცალკეული მთავრობების მიერ გატარებული შიდა და საგარეო ინტერნეტ პოლიტიკების გავლენის შედეგს თავად ინტერნეტის, იგივე კიბერსივრცის ერთიანობაზე, მდგრადობაზე, უსაფრთხოებასა და სტაბილურობაზე.

როცა ვსაუბრობთ ინტერნეტ ფრაგმენტაციის მეოთხე სავარაუდო ფორმაზე, აუცილებლად უნდა ვახსენოთ ის ქვეყნები, რომელთა ხელისუფლებები ზღუდავენ ინტერნეტის მიწოდების პროცესს, ახდენენ კონტროლს ინტერნეტში კონტენტის გავრცელებას, ცდილობენ შექმნან თავიანთი

ეროვნული ინტერნეტ ქსელი, ონლაინ პლატფორმები და სოციალური ქსელები თავიანთი მოქალაქეებისთვის, შეზღუდონ საერთაშორისო სოციალური ქსელები, რითაც საშუალება ეძლევათ ადვილად მოახდინონ კონტროლი ინტერნეტ სივრცეზე, და რითაც ხელს უწყობენ გლობალური ინტერნეტ სივრცის ფარგმენტაციის პროცესს. ასეთ ქვეყნებს მიეკუთვნება ისეთი დიდი ქვეყნები, როგორებიც არის ირანი, რუსეთი და ჩინეთი. თითოეული მათგანი თავიანთი კიბერსივრცის შეტევებისგან თავდაცვის მომიზეზებით ცდილობენ მაქსიმალურად შეამცირონ წვდომა უცხოეთიდან მათ ინტერნეტ სივრცეზე და ქვეყნის შიგნით შექმნან ისეთი სახის ინსტრუმენტები, რაც ხელს შეუწყობს კონტროლსა და მათთვის არასასურველი კონტენტის გავრცელების პროცესს, მოახდინონ მაქსიმალური დაბლოკვა.

4. დასკვნა

ბოლოში დასკვნის სახით შეიძლება ითქვას, რომ დროა სახელმწიფოებმა გააძლიერონ თავიანთი ძალისხმევა მიმართული ინტერნეტის როგორც გლობალური საზოგადოებრივი კეთილდღეობის, ინტერნეტის ერთიანობის, უსაფრთხოებისა და სტაბილურობის შესანარჩუნებლად. გლობალურ ციფრულ ხელშეკრულებაზე მუშაობის ფარგლებში, რომელიც შეთანხმებული უნდა იყოს 2024 წლის სექტემბერში, 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 ისნტრუმენტი. 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 იარაღი ქვეყნებისა და ადამიანთა წინააღმდეგ.

გამოყენებული ლიტერატურა

1. სვანაძე ვ. „კიბერუსაფრთხოების ახალი გამოწვევები და საქართველო“, 2022;
2. Carnap Kai Von, “Fragmentation the Internet-Beyond and Within the Great Firewall”, MERICS-Mercator Institute for Chinese Studies, 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.