RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

ჩინეთი — დემოკრატიული სამყაროს მთავარი გამოწვევა კიბერსივრცეში

გვანცა ჩაჩანიძე

174

ექსპერტის აზრი

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

ექსპერტის აზრი

გვანცა ჩაჩანიძე

ჩინეთი – დემოკრატიული სამყაროს მთავარი გამოწვევა კიბერსივრცეში

174

2021

პუბლიკაცია დაიბეჭდა ამერიკის შეერთებული შტატების საელჩოს ფინანსური მხარდაჭერით. გამოცემაში გამოთქმული მოსაზრებები ეკუთვნის ავტორებს და შეიძლება არ ასახავდეს საელჩოს თვალსაზრისს.

ტექნიკური რედაქტორი: არტემ მელიქ-ნუბაროვი

ISSN 1512-4835
ISBN

კიბერსივრცის დაცვა საერთაშორისო და ეროვნული უსაფრთხოების ერთ-ერთ მთავარ გამოწვევად იქცა. ქართული საზოგადოება რუსულ კიბერაქტივობებს, სტრატეგიასა და მიზნებს უკვე კარგად იცნობს. სამთავრობო საიტებს რუსულმა სპეცსამსახურებმა პირველად 2008 წლის ომისას შეუტიეს. ეს იყო მსოფლიო ისტორიაში პირველი შემთხვევა, როდესაც საომარი მოქმედებების პარალელურად ერთი სახელმწიფო მეორეს კიბერსივრცეშიც უტევდა (Hollis 2011, 2). გარდა კიბერშეტევებისა, ქვეყნის უსაფრთხოებაზე გავლენას რუსული დეზინფორმაციაც ახდენს, რომელიც მოსახლეობის რადიკალიზაციისა და პოლარიზაციისკენ, ასევე დემოკრატიული და დასავლური ფასეულობების გაუფასურებისკენაა მიმართული.

საერთაშორისო უსაფრთხოებაში კიბერსივრცის მნიშვნელობა ნათელი გახდა 2007 წელს, როდესაც რუსეთმა ესტონეთის კიბერსივრცეს შეუტია. ესტონეთი რამდენიმე დღის განმავლობაში პარალიზებული იყო, ვინაიდან კიბერშეტევა შეეხო როგორც სამთავრობო საიტებს, ისე ბანკებს, სატელეკომუნიკაციო კომპანიებს, საავადმყოფოებსა და მედიას (Tamkin 2017). 2007 წლამდე მსგავსი მასშტაბის შეტევა არ მომხდარა. წერტილოვანი კიბერშეტევები ძირითადად ერთ კომპანიას ან ინსტიტუტს აზიანებდა.

თანამედროვე სამყაროში მეტად აქტუალურია მონაცემთა ციფრულ ფორმატში გადატანა, ელექტრონული ვაჭრობა, სოციალური მედია, საჯარო სერვისების ონლაინპლატფორმებით მიღება. სახელმწიფოები რაც უფრო დამოკიდებული ხდებიან კიბერსივრცეზე, მით მეტი მიზეზი და საშუალება უჩნდებათ მტრულად განწყობილ აქტორებს კიბერშეტევისთვის, ინფორმაციის მოპარვისა და დამახინჯებისთვის, სისტემების პარალიზებისთვის.

უნდა გავითვალისწინოთ, რომ კიბერუსაფრთხოება მხოლოდ კომპიუტერულ პროგრამირებასა და საინფორმაციო ტექნოლოგიებს არ ეხება. კიბერუსაფრთხოება ეროვნული უსაფრთხოების უმნიშვნელოვანესი ნაწილია, რადგან კიბერშეტევების სამიზნე ადამიანები, საზოგადო აზრი, საჯარო და ბიზნეს სექტორია.

მართალია, რუსეთი საკმაოდ აგრესიული კიბერაქტორია, თუმცა არსებობს სხვა, არადემოკრატიული სახელმწიფოც, რომელსაც გაცილებით დიდი ეკონომიკურ-ტექნოლოგიური რესურსი, ამბიცია და კიბერექსპანსიონიზმისკენ მისწრაფება აქვს.

შეიძლება ითქვას, რომ კიბერსივრცეში შეერთებული შტატებისა და მისი მოკავშირეების მთავარი გამოწვევა ჩინეთია. ჩინეთი, რუსეთის მსგავსად, რეგულარულად ახორციელებს კიბერშეტევებს აშშ-ისა და ევროკავშირის წინააღმდეგ. ასეთი შეტევების მიზანი ეკონომიკური საქმიანობისთვის ხელის შეშლა, უსაფრთხოებისა და თავდაცვის სექტორისთვის ზიანის მიყენება და საზოგადო აზრის შექმნა თუ შეცვლაა. გარდა ამისა, „ციფრული აბრეშუმის გზა“ და „კოსმოსის საინფორმაციო კორიდორი“ არა მარტო ხელს უწყობენ ჩინურ კიბერშპიონაჟს, არამედ მიზნად ისახავენ ავტორიტარული სტანდარტებით ინტერნეტსივრცის სრულად გარდაქმნასა და კიბერსივრცეში ჩინეთის დომინაციას.

ჩინეთის აქტივობები კიბერსივრცეში

ჩინეთიდან მომავალი კიბერსაფრთხეებით პირველად ამერიკული მედია დაინტერესდა. 2011 წლიდან ბევრი იწერებოდა ჩინურ კიბერშპიონაჟსა და ფიშინგით განხორციელებულ კიბერშეტევებზე, რომელთა საშუალებითაც ამერიკულ კომპანიებს ინტელექტუალურ საკუთრებას ჰპარავდნენ (Perlroth 2021).

გასათვალისწინებელია, რომ აშშ-ის წარმომადგენელთა პალატის დაზვერვის კომიტეტის კვლევის მიხედვით, ყოველწლიურად მხოლოდ ამერიკულ კომპანიებს ინტელექტუალური საკუთრების მოპარვით 540 მილიარდი დოლარის ზარალი ადგებათ. აქედან 400 მილიარდის ზარალი კიბერსივრცეში მოპარული იდეებზე მოდის. თავდასხმების 73% კი ჩინურ კიბერშპიონაჟს უკავშირდება (Hosenball 2020). ინტელექტუალური საკუთრების ქურდობაში ჩინეთი არაერთხელ დაადანაშაულეს. დღეს ეს თემა დღის წესრიგში ისე დგას, როგორც არასდროს. პეკინმა ეროვნული გეგმა „დამზადებულია ჩინეთში 2025“ შეიმუშავა, რომლის მიზანია დაბალფასიანი პროდუქციის მწარმოებლიდან ჩინეთი მაღალტექნოლოგიურ მწარმოებლად გარდაქმნას (Insikt Group 2021, 2).

კიბერშეტევების თავიდან აცილება, ისევე როგორც მიყენებული ზიანის წინასწარ განსაზღვრა ძალიან რთულია. მით უმეტეს, იმის გათვალისწინებით, რომ დღესდღეობით ჩინეთის მთავრობა და მასთან დაკავშირებული ჰაკერული დაჯგუფებები სამთავრობო თუ ბიზნეს სექტორების მონაცემთა ბაზებში შესასვლელად ბევრად მაღალი დონის ტექნოლოგიასა და ტაქტიკებს იყენებენ, ვიდრე ოდესმე. ჰაკერები თვეების განმავლობაში ცდილობენ შეისწავლონ პროგრამებისა და სერვერების სისუსტეები, ღირებული ინფორმაცია მოიპოვონ და, რაც მთავარია, ამ პროცესში შეუმჩნეველი იყვნენ. ეს კარგადაც გამოსდით. ჩინეთის სახელმწიფო უსაფრთხოების სამინისტროს ჰაკერები Marriott Group-ის სისტემაში 4 წლის განმავლობაში იყვნენ და ამ დროის მანძილზე 500 მილიონზე მეტი მომხმარებლის პირადი ინფორმაცია მოიპარეს (Venard 2019).

ჩინეთი კიბერშეტევებს ძირითადად სახალხო-განმათავისუფლებელი არმიის მე-3 დეპარტამენტის, შიდა ჰაკერული დაჯგუფებებისა და ტექნოლოგიური კომპანიების, მაგალითად Huawei-ს დახმარებით ახორციელებს. ჩინეთმა მოიპარა ამერიკული სამხედრო თვითმფრინავის F 35-ის მოდელი, შემდეგ კი ანალოგიური Shenyang FC-31 გამოუშვა (Gady 2015). შეიძლება ითქვას, რომ მიმდინარეობს მეორე ცივი ომი, ამჟამად –კიბერსივრცეში. ჩინეთის კიბერშეტევები და ინტელექტუალური საკუთრების ქურდობა ყველაზე უკეთ FBI-ის ყოფილმა ხელმძღვანელმა რობერტ მიულერმა შეაფასა. მისი თქმით, არსებობს ორი სახის ამერიკული კომპანიები: „ისინი, რომლებიც უკვე იყვნენ ჰაკერული თავდასხმების მსხვერპლი, და ისინი, რომლებიც მომავალში იქნებიან” (Mueller 2012) .

ჩინეთის ხელისუფლება კიბერსივრცეს ევროპელ პოლიტიკოსებსა და დიპლომატებზე თვალთვალისთვისაც იყენებს. 2018 წელს სახალხო-

განმათავისუფლებელ არმიასთან დაკავშირებულმა ჰაკერებმა ევროკავშირის დიპლომატიური საკომუნიკაციო ქსელი გატეხეს და სენსიტიური ინფორმაცია მოიპოვეს (Sanger et al 2018). ბევრი სპეკულირებდა, რომ ჩინეთი მოპოვებული მასალით მაღალჩინოსნების შანტაჟს შეეცდებოდა და აიძულებდა ჩინეთის სტრატეგიისა და გეოპოლიტიკური მიზნებისთვის მხარი დაეჭირათ. გამორიცხული არაა მსგავს შემთხვევას შედეგი გამოეღო. მით უმეტეს, გასათვალისწინებელია, რომ შეერთებული შტატებისგან განსხვავებით, ევროკავშირი ჩინეთს საფრთხედ ნაკლებად აღიქვამს და ღიად იშვიათად აკრიტიკებს.

ჩინეთი ცდილობს Huawei-მ ევროპული კომუნიკაციების სისტემაში მნიშვნელოვანი ადგილი დაიკავოს. ევროკავშირის უსაფრთხოებისთვის ეს მეტად სარისკოა, რადგან კომპანია კომუნისტურ პარტიასთანაა დაახლოებული და ჩინეთის დაზვერვასთან თანამშრომლობს. რაც მეტი წილი ექნება Huawei-ს ევროპულ ბაზარზე, მით ნაკლებად დაცული იქნება ევროკავშირის კიბერუსაფრთხოება. იგივე შეიძლება ითქვას საქართველოზეც. ქვეყნის საკომუნიკაციო ქსელის 75% Huawei-ს შექმნილია, რაც ეროვნული უსაფრთხოებისა და კიბერუსაფრთხოებისთვის წამგებიანია.

გარდა შპიონაჟისა, ჩინეთის ხელისუფლება კიბერსივრცეს დეზინფორმაციის გასავრცელებლადაც აქტიურად იყენებს. ამ მხრივ, შესამჩნევად პანდემიის დასაწყისიდან აქტიურობენ. ჩინური მედია, განსაკუთრებით კი, კომუნისტური პარტიის „სინხუას საინფორმაციო სააგენტო“ თავდაპირველად ვირუსის წარმოშობის კონსპირაციულ თეორიებს ავრცელებდა. ამას მოჰყვა ჩინური სამედიცინო დახმარების პროპაგანდა, პარალელურად კი აშშ-ისა და ევროკავშირის დადანაშაულება პანდემიის არაეფექტიანად მართვაში. „ფეიკ ნიუსის“ ბოლო ტალღა დასავლური ვაქცინებისკენ იყო მიმართული. კიბერსივრცეში რუსული და ჩინური ნარატივები ერთმანეთს ძალიან ჰგავს. ორივეს მიზანი დემოკრატიული სამყაროს დისკრედიტაცია და ნებისმიერ დარგში საკუთარი უპირატესობის წარმოჩენაა.

ჩინეთის კიბერექსპანსიონიზმი და „ციფრული აბრეშუმის გზისგან“ მომავალი საფრთხეები

ჩინეთის ხელისუფლება გამუდმებით ცდილობს ახალი ბაზრის ათვისებას. კომუნისტური პარტიის ინტერესი, ერთი მხრივ, ეკონომიკური სარგებლისა და პოლიტიკური გავლენის არეალის გაზრდაა. მეორე მხრივ კი, ჩინეთი ტექნოლოგიური ექსპორტით „კიბერექსპანსიონიზმს“ ეწევა, რაც კიბერსივრცეში ჩინური მართვის სტილის დამკვიდრებას, განვითარებადი ქვეყნების ჩინურ ტექნოლოგიაზე დამოკიდებულებასა და ჩინური დაზვერვისთვის მეტი შესაძლებლობების გაჩენას გულისხმობს.

„ერთი სარტყელი, ერთი გზის“ ინიციატივაზე მუშაობის დაწყებიდან 2 წლის შემდეგ პრეზიდენტმა სი ძინპინმა საფუძველი ჩაუყარა „ციფრულ აბრეშუმის გზას“.

ოფიციალურად პროექტის მიზანი ინტერნეტის ინფრასტრუქტურის, კომუნიკაციების, კიბერუსაფრთხოებისა და ელექტრონული კომერციის გაუმჯობესებაა. ციფრული აბრეშუმის გზის ფარგლებში ჩინეთი სადაზვერვო ტექნიკის (ქსელური კამერები, ლოკაციის სერვისი, სენსორები) ექსპორტს ახორციელებს. ეს კიდევ ერთი ეფექტური მექანიზმია, რომელიც პარტიასთან დაახლოებულ გიგანტებს – Huawei-ს, Alibaba-ს, Tencent-ს ახალ ბაზრებს უხსნის (Ghiasy et al 2021). პროექტის წყალობით ჩინეთი ექსპორტზე მილიონობით სადაზვერვო და საყოფაცხოვრებო ტექნიკას გაიტანს. აღსანიშნავია, რომ თითოეულ ჩინურ ელექტრომოწყობილობაზე, სერვერსა და პროგრამაზე ჩინურ დაზვერვას წვდომა აქვს. მათ შეუძლიათ თვალი ადევნონ ადამიანების გადაადგილებას, საბანკო ოპერაციებს, ყოველდღიურ აქტივობებს.

განვითარებადი ქვეყნების დამოკიდებულება ჩინურ ნაწარმზე, მომსახურებასა და ტექნოლოგიებზე ჩინეთის მთავრობას ადგილობრივ პოლიტიკურ ელიტებზე გავლენის მოხდენის საშუალებას აძლევს.

International Telecommunication Union-ის ინფორმაციით, დღესდღეობით ინტერნეტი მსოფლიოს მოსახლეობის 55%-ს აქვს. ეს მაჩვენებელი განვითარებულ ქვეყნებში 87%-ს აღწევს, განვითარებადში – 47%-ს, ყველაზე დაბალგანვითარებულში კი – მხოლოდ 19%-ს (ITU 2019). ჩინური პროდუქცია ძირითადად განვითარებადი და დაბალგანვითარებული ქვეყნებისთვისაა გათვლილი. ასეთი სახელმწიფოები კიბერსივრცეში გამოუცდელები არიან და ტექნოლოგიურ პროგრესშიც ისეთ ქვეყნებს, როგორიც ჩინეთია, ფეხს ვერ უბამენ. შესაბამისად, ჩინეთის მთავრობას მარტივად შეეძლება წვდომა ჰქონდეს სუსტი ქვეყნების სამთავრობო ფაილებზე, ღირებულ ინფორმაციაზე, პირად მონაცემებზე და ა.შ. ზემოთქმულიდან გამომდინარე, საუბარია „კიბერკოლონიალიზმზე“, ანუ ციფრული აბრეშუმის გზის გამოყენებაზე „ეკონომიკური, სოციალური და პოლიტიკური დომინაციისთვის სხვა ქვეყნის ტერიტორიაზე“ (Insikt Group 2021, 2). მართალია, სწრაფი ინტერნეტი და უახლესი ტექნოლოგიები განვითარებად ქვეყნებს ახალ შესაძლებლობებს, სამუშაო ადგილებს, უკეთეს განათლებასა და ჯანდაცვას მოუტანს, თუმცა – არა ჩინური დაზვერვის გარეშე.

ჩნდება ახალი დემოკრატიების მიერ ჩინური ნორმების ათვისების რისკიც. ჩინეთი ტექნოლოგიას მოსახლეობის მასობრივი დაზვერვისთვის იყენებს. იცავს კომუნისტური პარტიის ინტერესებს, დევნის საპროტესტოდ განწყობილ და პროდემოკრატიულ ჯგუფებს, ზღუდავს მედიას, ახშობს პროტესტს, სისტემურად ჩაგრავს რელიგიურ და ეთნიკურ უმცირესობებს. Freedom House-ის ანგარიშის მიხედვით, 2018 წელს ჩინური დაზვერვის ტექნოლოგია 18-მა ქვეყანამ შეიძინა. სადღეისოდ მსგავსი ქვეყნების რიცხვი 80-მდე ავიდა, მათ შორისაა აზიის, სამხრეთ ამერიკისა და აფრიკის სახელმწიფოების უდიდესი ნაწილი (Shahbaz 2018).

ამერიკული კიბერუსაფრთხოების კომპანიის Recorded Future-ის ანგარიშის მიხედვით, ზოგჯერ ქვეყნები ჩინური ტექნოლოგიის დაბალ ფასად მიღების

სანაცვლოდ, სახალხო-განმათავისუფლებელ არმიას თავად აწვდიან საიდუმლო მონაცემებს და მეტიც, უფლებას აძლევენ ცდები ჩაატარონ სახის ამომცნობ მასობრივი დაზვერვის კამერებზე. ზემოთქმული განსაკუთრებით აფრიკის ქვეყნებისთვისაა რელევანტური. ჩინეთი ცდილობს სათვალთვალო, ჭკვიანი კამერები განავითაროს და კანის ფერისა და რასის ამოცნობის ფუნქცია დაუმატოს (Insikt Group 2021, 8).

ზემოთ უკვე აღვნიშნეთ, რომ ქვეყნის საზღვრებში კომუნისტური პარტია სოციალურ ქსელებს ეფექტურად აკონტროლებს. მოქალაქეებს არ აქვთ დასავლური სოციალური პლატფორმების გამოყენების უფლება, რადგან პარტია ისეთ საიტებს, როგორებიცაა Facebook, Instagram, Google, Yahoo და სხვა, ბლოკავს. ამას ჩინეთის მთავრობა ადგილობრივი აპლიკაციების პოპულარიზაციითა და ჩინური ბიზნესის წახალისებით ხსნის, თუმცა რეალობა ერთია – ხელისუფლებას არ სურს მოსახლეობამ დასავლურ მედიას უყუროს, მოწყდეს პარტიულ ნარატივს, თავისუფლად დააფიქსიროს აზრი და პარტიის კონტროლისა და შიშის გარეშე თანამოაზრეები მარტივად იპოვოს.

კომუნისტური პარტია ინტერნეტში თავისუფალ სიტყვას ებრძვის. ამის ნათელი მაგალითი 2020 წლის დასაწყისში გამოვლინდა. კერძოდ, ჩინეთის მთავრობა ყველა იმ ადამიანს დევნიდა, რომელიც სოციალურ ქსელში ახლობლების გაფრთხილების მიზნით ახალი ვირუსის შესახებ ინფორმაციას ავრცელებდა. მათ შორის იყო ექიმი ლი ვენლიანი, რომელსაც მოგვიანებით დეზინფორმაციის გავრცელებაში დასდეს ბრალი და საჯაროდ ხელი მოაწერინეს დოკუმენტზე, რომელიც აცხადებდა, რომ ვენლიანი ფაქტების ნაცვლად ჭორებს ავრცელებდა და არანაირი სასიკვდილო ვირუსი არ არსებობდა. სამწუხაროდ, მოგვიანებით ექიმი კორონავირუსმა იმსხვერპლა (Hegarty 2020).

საინტერესოა ჟენ ჭიციენის შემთხვევაც, რომელიც 2020 წლის 14 მარტს, მას შემდეგ გაუჩინარდა, რაც თავის ბლოგში კორონავირუსის გავრცელებაზე პასუხისმგებლობა მთავრობას დააკისრა, სი ძინპინს კი „შეშლილი კლოუნი“ უწოდა. მოგვიანებით გაირკვა, რომ ჟენ ჭიციენი დააკავეს, ბრალად კორუფციულ გარიგებებში მონაწილეობა დასდეს და 18 წელი მიუსაჯეს (McDonell 2020).

„ინტერნეტის პროტოკოლის გეგმა“ და 5G

2019 წელს Huawei-ს ინჟინრებმა 40 პარტნიორი ქვეყნის დელეგატებს ახალი „ინტერნეტის პროტოკოლის გეგმა“ წარუდგინეს. მათი განცხადებით, ამჟამინდელი კიბერსივრცე მეტად ლიმიტირებული და მოძველებულია. Huawei-მ შეიმუშავა ახალი დიზაინი, რომელიც მთავრობებს საშუალებას მისცემს უფრო მარტივად და ეფექტიანად გააკონტროლონ ციფრული საკუთრება, მოსახლეობა და წესრიგი კიბერსივრცეში (Murgia et al 2020). ჩინეთის სახალხო რესპუბლიკა ე.წ.

„კიბერსუვერენიტეტის“ პრინციპს ემხრობა, რომლის მიხედვითაც მთავრობას კიბერსივრცეში შეუზღუდავი ძალაუფლება აქვს. ის აკონტროლებს ნებისმიერ კიბეროპერაციას, ინფრასტრუქტურასა და მოწყობილობას ქვეყნის შიგნით.

განვითარებად, არადემოკრატიულ ქვეყნებში ინტერნეტის ჩინური მართვის სტილი და სადაზვერვო ქსელები ავტორიტარულ მთავრობებს არამარტო სოციალურ მედიაში თავისუფალი სიტყვის შეზღუდვის, არამედ ოპოზიციურად განწყობილი ადამიანების რეპრესირების შესაძლებლობასაც მისცემს. Huawei და ჩინეთის მთავრობა დიქტატორებს აქამდეც დასდგომიან გვერდით. Wall Street Journal-ის საგამოძიებო სტატიის თანახმად, 2018 წელს უგანდის პრეზიდენტმა იოვერი მუსევენმა, ოპოზიციის ლიდერის, ბობი ვაინის, WhatsApp-ის პროგრამა Huawei-ს ინჟინრების დახმარებით გატეხა. მუსევენმა ოპონენტზე კომპრომატების შეგროვება დაიწყო. ვაინს ჯერ აშანტაჟებდნენ, შემდეგ კი ასობით მხარდამჭერთან ერთად სახელმწიფოს ღალატის ბრალდებით დააკავეს (Parkirson et al 2019).

Huawei კიბერსივრცეში მოპოვებულ ინფორმაციას უცხო ქვეყნების ავტორიტარული რეჟიმების წარმომადგენლების გარდა, ჩინეთის ხელისუფლებასაც აწვდის. მიუხედავად იმისა, რომ Huawei-ს მენეჯმენტი ამას კატეგორიულად უარყოფს, უნდა გავითვალისწინოთ, რომ 2017 წელს მიღებული საკანონმდებლო აქტის თანახმად, ნებისმიერი ჩინური კერძო კომპანია ვალდებულია ჩინეთის დაზვერვასთან ითანამშრომლოს (Girard 2019).

ჯერ კიდევ კანონის მიღებამდე, 2012 წელს, აშშ-ის წარმომადგენელთა პალატის დაზვერვის კომიტეტმა Huawei ეროვნულ საფრთხედ დაასახელა. Huawei-ს მაშინაც ინტელექტუალური საკუთრების მოპარვასა და მონაცემთა ბაზების ბოროტად გამოყენებაში ედავებოდნენ (Schmidt et al 2012). მიუხედავად იმისა, რომ შეერთებული შტატები მოკავშირეებს Huawei-სგან მომავალი კიბერსაფრთხეების შესახებ აფრთხილებს, კომპანია 5G-ის გაყიდვებში მსოფლიოს მასშტაბით ლიდერობას არ თმობს.

გასათვალისწინებელია, რომ აშშ-ის შემდეგ ჩინურ 5G ტექნოლოგიას ბოიკოტი ავსტრალიამ და დიდმა ბრიტანეთმაც გამოუცხადეს. თუმცა 2020 წელს ბრიტანეთმა შეზღუდვა მოხსნა და ჩინეთს ქვეყნის ტერიტორიაზე 5G ქსელის გაყვანის საშუალება მისცა (Reichert 2020). ჩინური 5G ქსელი ევროკავშირმაც მიიღო, მაგრამ განაცხადა, რომ ბაზარზე Huawei-ს სისტემის გარდა, სხვა 5G-ს მიმწოდებლებიც ეყოლება, რათა მხოლოდ ერთ მიმწოდებელზე დამოკიდებული არ გახდეს და კონკურენცია და მრავალფეროვნება უზრუნველყოს (Nietsche et al 2020).

ჩინური 5G სისტემით სარგებლობს ბრაზილიაც, რომელმაც თავდაპირველად შეერთებულ შტატებთან ერთად ხელი მოაწერა მემორანდუმს, რომელიც 5G-ის, ტელეკომუნიკაციებისა და ენერგიის სფეროში თანამშრომლობის გაღრმავებას მოიცავდა. ამ მემორანდუმით ბრაზილია შეუერთდა „სუფთა ქსელის ინიციატივას“ (Clean Network Initiative) რაც 5G ქსელის უსაფრთხოებისთვის საჭირო აპარატურის შეძენას, მოქალაქეთა პირადი ინფორმაციის კონფიდენციალურობას,

სატელეკომუნიკაციო ინფრასტრუქტურაზე არასანქცირებული წვდომისგან დაცვას და ეროვნული უსაფრთხოების უზრუნველყოფას გულისხმობდა (U.S Embassy and Consulates in Brazil 2020). მიუხედავად ამისა, პრეზიდენტმა ჟაირ ბოლსონარუმ შეთანხმება დაარღვია და Huawei-ს უფლება მისცა ქვეყნის მასშტაბით 5G ქსელი დაემონტაჟებინა. ბოლსონარუს ეს გადაწყვეტილება დიდწილად Huawei-ს სერვისის ხელმისაწვდომობით იყო განპირობებული. აქვე უნდა ითქვას, რომ კომპანია ბრაზილიის ბაზარზე 22 წლის წინ შევიდა და საკომუნიკაციო ქსელის დიდი უმეტესობა სწორედ მისი გაყვანილია (Chu 2021).

2021 წლის 14 იანვარს „სუფთა ქსელის ინიციატივას“ საქართველოც შეუერთდა (U.S Embassy in Georgia). 2 წლით ადრე ქვეყანაში „ციფრული აბრეშუმის გზის“ ფარგლებში 5G-ის ოპტიკურ-ბოჭკოვანი კაბელების დამონტაჟება იგეგმებოდა. ოფიციალური პირები ხშირად საუბრობდნენ ჩინურ ინვესტიციებსა და საქართველოს 5G ქსელის ჰაბად ქცევაზე. მას შემდეგ, რაც „კავკასუს ონლაინის“ აქციების 100%-იანი პაკეტი „ნექსონ ჰოლდინგის“ ხელში გადავიდა, კაბელების დამონტაჟება აზერბაიჯანის ტერიტორიაზე გადაწყდა. ქართველ ექსპერტთა დიდი ნაწილი ამ შემთხვევას უდიდესი შესაძლებლობის ხელიდან გაშვებად მიიჩნევს, თუმცა, როგორც ზემოთ აღვნიშნეთ, ჩინურ ტექნოლოგიებს ჩინური დაზვერვაც თან ახლავს. გარდა ამისა, საქართველოს მთავარი სტრატეგიული პარტნიორისთვის – ამერიკის შეერთებული შტატებისთვის – 5G ინტერნეტზე ჩინურ კომპანიებთან თანამშრომლობა პოლიტიკური გზავნილია და ქვეყნის აღმოსავლურ ორიენტაციაზე მიუთითებს. აქედან გამომდინარე, ეროვნული უსაფრთხოებისა და საერთაშორისო ურთიერთობების თვალსაზრისით, ჩაშლილი გეგმა სწორედაც რომ მომგებიანია.

სოციალური კრედიტის სისტემა

ტექნოლოგიების განვითარების პარალელურად, ჩინეთის კომუნისტურმა პარტიამ უკვე დაიწყო სოციალური კრედიტის სისტემის გამოყენება, რაც ადამიანის მორალურ შეფასებას გულისხმობს. ეს სისტემა South China Morning Post-ის თანახმად, ეროვნული განვითარებისა და რეფორმების კომისიამ, ჩინეთის სახალხო ბანკმა და ჩინურმა სასამართლომ შეიმუშავეს. სისტემის საშუალებით კიბერსივრცესა და რეალურ ცხოვრებაში ინდივიდებსა და კომპანიებს ყოველდღიურად აკონტროლებენ. საბანკო ოპერაციების წყალობით ადგენენ თუ რას ყიდულობენ ადამიანები, ქსელური კამერებით ნებისმიერი პიროვნების გადაადგილებასა და ქცევას აფიქსირებენ, სოციალურ მედიაში კი ინფორმაციის ნაკადი და თავისუფალი სიტყვა კიდევ უფრო შეიზღუდა (Lee 2020).

სოციალური კრედიტის ქულა კონკრეტული პიროვნების ქცევის შესაბამისად იზრდება ან იკლებს. ზუსტი მეთოდოლოგია გასაიდუმლოებულია, თუმცა „ფეიკ ნიუსის“ გავრცელება, ზედმეტად ბევრი ალკოჰოლის ყიდვა, ისეთ ადგილას მოწევა, სადაც ეს ნებადართული არაა, ხმაური, მოძრაობის წესების

დარღვევა და სხვა მსგავსი აქტივობა სოციალურ ქულას დაბლა წევს. რაც შეეხება დაბალი ქულის შედეგებს, ჩინეთმა უკვე დაიწყო ადამიანების დასჯა, რაც თვითმფრინავით სარგებლობის, მატარებელში ბიზნეს კლასით მგზავრობისა და სასტუმროს ძვირადღირებული ნომრის დაკავების შეზღუდვით გამოიხატება (Ma et al 2021). Foreign Policy-ის მიხედვით, სოციალურ კრედიტებზე აისახება გადასახადების დაგვიანებით გადახდა, კრედიტების დაგვიანებით დაფარვა და ა.შ. დაბალი სოციალური კრედიტის მქონე ადამიანებს უკვე შეეზღუდათ წვდომა უმაღლეს განათლებაზე (Minstreanu 2018).

მიუხედავად იმისა, რომ ეს სისტემა Black Mirror-ის ეპიზოდს ან რომელიმე სამეცნიერო ფანტასტიკის სცენარს გვაგონებს, უნდა გვახსოვდეს, რომ ყველაფერი რეალურია. და რაოდენ წარმოუდგენელიც არ უნდა იყოს, არსებობს იმის რისკი, რომ სოციალური კრედიტის სისტემა ჩინეთის საზღვრებს გასცდება. ჩინეთის მთავრობა სოციალური კრედიტების მეშვეობით საზოგადოებას უფრო მორჩილს ხდის, რათა რეჟიმი უფრო მარტივად შეინარჩუნოს. არაა გამორიცხული სხვა ავტორიტარულმა, არადემოკრატიულმა სახელმწიფოებმაც ამავე მიზნით გამოიყენონ თანამედროვე ტექნოლოგიები.

განვითარებად ქვეყნებში ჩინური ტექნოლოგიებით სოციალური კრედიტის სისტემის დანერგვა ადამიანის უფლებებისა და თავისუფლების შეზღუდვის გარდა, ჩინეთის სადაზვერვო სამსახურს ინფორმაციას მიაწვდის სხვა სახელმწიფოში მიმდინარე მოვლენებზე, ტენდენციებსა და მოქალაქეების ქცევებზე. ამ მონაცემებზე დაყრდნობით ჩინეთი ჰიბრიდული ომის ფარგლებში უფრო ეფექტიანად მოახდენს გავლენას საინფორმაციო გარემოსა და ადამიანთა შეხედულებებზე, გააძლიერებს ანტიამერიკულ და ანტიდასავლურ განწყობილებებს.

* * *

შესავალში უკვე აღვნიშნეთ, რომ ჩინეთი კიბერსივრცეში შეერთებული შტატებისა და მისი მოკავშირეების მთავარ გამოწვევად იქცა. მართალია, რუსეთი საკმაოდ აგრესიული და გამოცდილი მოთამაშეა, თუმცა ჩინეთს გაცილებით დიდი ეკონომიკურ-ტექნოლოგიური რესურსი, შესაძლებლობები და ამბიციები აქვს. მსოფლიოს მასშტაბით მილიონობით ჩინური სმარტფონი, კომპიუტერული ტექნიკა, პროგრამა, სენსორი, ჭკვიანი კამერა და სადაზვერვო მოწყობილობა იყიდება. ჩინურ დაზვერვას თითოეულ მათგანზე წვდომა აქვს. აქედან გამომდინარე, კიბერსივრცეში ჩინეთის სახალხო რესპუბლიკას სხვა სახელმწიფოებისთვის ყველაზე დიდი ზიანის მიყენება შეუძლია. ამას ემატება როგორც ჩინური 5G ტექნოლოგია, ისე ინტერნეტისა და კიბერსივრცის სრულად გარდაქმნის გეგმა, რომლის სისრულეში მოსაყვანად უკვე არაერთი სტრატეგიული ნაბიჯი გადაიდგა.

ჩინეთის მიზანია ციფრულ სამყაროში მმართველობის ავტორიტარული სტილი დაამკვიდროს და დემოკრატიული პრინციპები ჩაანაცვლოს. კომუნისტური პარტიის იდეები არადემოკრატიული ან ჰიბრიდული რეჟიმებისთვის შესაძლოა

მიმზიდველი იყოს. საკუთარი მოქალაქეების თვალთვალი, მოწინააღმდეგეებისა და თავისუფალი აზრის დევნა, ცენზურა – ამის საშუალებასა და ლეგიტიმაციას სახელმწიფოებს ჩინური „ინტერნეტის პროტოკოლის გეგმა“ მისცემს.

რაც შეეხება საქართველოს, ქვეყანაში უკვე გვქონდა მოქალაქეების თვალთვალისა და პირადი ცხოვრების ამსახველი კადრებით შანტაჟის არაერთი პრეცედენტი. არაა გამორიცხული, მთავრობისთვის „ინტერნეტის პროტოკოლის გეგმა“, როგორც ოპონენტების დევნის ახალი და ეფექტიანი გზა, მისაღები იყოს. მით უმეტეს, რომ ახალ დემოკრატიებში, რომლებშიც დასავლურ ფასეულობებსა და კანონის უზენაესობის იდეას ფესვები გადგმული არ აქვს, ავტორიტარული ტენდენციები ფეხს ადვილად იკიდებს. მიუხედავად ამისა, ვიმედოვნებთ, რომ ხელისუფლება მსგავს ნაბიჯებს არ გადადგამს და ქვეყნის განვითარების ევროატლანტიკურ გზას არ გადაუხვევს.

ამასთანავე, საქართველომ არ უნდა მიჰბაძოს ბრაზილიას, „სუფთა ქსელის ინიციატივიდან“ არ უნდა გამოვიდეს, პრინციპული უარი უნდა თქვას ჩინურ 5G ტექნოლოგიაზე. გარდა იმისა, რომ ზემოთქმული ეროვნული უსაფრთხოების დაცვისთვის მნიშვნელოვანია, ეს იქნება მკაფიო პოლიტიკური გზავნილი და იმის ხაზგასმა, რომ საქართველოსთვის შეერთებულ შტატებთან სტრატეგიული პარტნიორობა პრიორიტეტულია. ასევე აუცილებელია, დასავლური და დემოკრატიული ფასეულობების ერთგულნი დავრჩეთ, მათ შორის – კიბერსივრცეშიც.

საპირწონედ, საჭიროა შეერთებული შტატები განვითარებად ქვეყნებს 5G ინტერნეტის, თანამედროვე ტექნოლოგიებისა და საკომუნიკაციო ქსელების უსაფრთხო წყაროებისგან შეძენაში დაეხმაროს. აშშ-მ უნდა შეიმუშაოს ერთგვარი „მარშალის ციფრული გეგმა“ (Frenkel et al 2021), რომელიც კონკურენციას გაუწევს „ციფრულ აბრეშუმის გზას“, განვითარებად ქვეყნებს ახალ, ხარჯეფექტიან ალტერნატივას შესთავაზებს და, რაც მთავარია, ჩინეთის კიბერექსპანსიონიზმს წინ აღუდგება.

გამოყენებული ლიტერატურა

1. Chu, Daye. 2021. “Brazil ditches US drive to strangle Huawei.” Global Times, January 17, 2021. https://www.globaltimes.cn/page/202101/1213075.html.

2. Frenkel, Orit, Kent Hughes, Jennifer A. Hillman. 2021. “The U.S Needs a “Digital Marshal Plan” to counter China’s Digital Silk Road.” The Hill, July 12, 2021. https://thehill.com/opinion/technology/562435-the-us-needs-a-digital-marshall-plan-to-counter-chinas-digital-silk-road.

3. Ghiasy, Richard, Rajeshwari Krishnamurthy. 2021. “China’s Digital Silk Road and the Global Digital Order.” The Diplomat, April 13, 2021. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

4. Girard, Bonnie. 2019. “The Real Danger of China’s National Intelligence Law.” The Diplomat, February 23, 2019. https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/.

5. Hegarty, Stephanie. 2020. “The Chinese doctor who tried to warn others about coronavirus.” BBC, February 6, 2020. https://www.bbc.com/news/world-asia-china-51364382.
Mcdonell, Stephen. 2020. “Ren Zhiqiang: Outspoken ex-real estate tycoon gets 18 years jail.” BBC, September 22, 2020. https://www.bbc.com/news/world-asia-china-54245327.

6. Hollis, David. 2011. “Cyberwar Case Study: Georgia 2008.” Small Wars Journal, January 6, 2011. https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

7. Hosenball, Mark. 2020. “Top U.S. officials to spotlight Chinese spy operations, pursuit of American secrets.” Reuters, February 6, 2020. https://www.reuters.com/article/usa-china-espionage/top-u-s-officials-to-spotlight-chinese-spy-operations-pursuit-of-american-secrets-idUSL1N28S1B3.

8. Insikt Group. 2021. “China’s Digital Colonialism: Espionage and Repression Along the Digital Silk Road.” Recorded Future, July 27, 2021. https://go.recordedfuture.com/hubfs/reports/cta-2021-0727.pdf.

9. International Telecommunication Union. 2019. “Measuring digital development Facts and figures.” ITU Publications, November 5, 2019.
https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

10. Lee, Amanda. 2020. “What is China’s social credit system and why is it controversial?” South China Morning Post, August 9, 2020. https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial.

11. Ma, Alexandra, Katie Canales. 2021. “China’s ‘social credit’ system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy.” Business Insider, May 9, 2021. https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

12. Minstreanu, Samina. 2018. “Life Inside China’s Social Credit Laboratory.” Foreign Policy, April 3, 2018. https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/.

13. Mueller, Robert S. “Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies.” RSA Cyber Security Conference San Francisco, CA, March 01, 2012. The Federal Bureau of Investigation. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

14. Murgia, Madhumita, Anna Gross. 2020. “Inside China’s controversial mission to reinvent the internet.” Financial Times, March 28, 2020. Inside China’s controversial mission to reinvent the internet | Financial Times (ft.com).

15. Nietsche, Carisa, Martjin Rasser. 2020. “Washington’s Anti-Huawei Tactics Need a Reboot In Europe Efforts to convince allies of the Chinese threat in 5G have floundered.” Foreign Policy, April 30, 2020. https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/.

16. Parkirson, Joe, Nicholas Bariyo, Josh Chin. 2019. “Huawei Technicians Helped African Governments Spy on Political Opponents.” The Wall Street Journal, August 15, 2019. Huawei Technicians Helped African Governments Spy on Political Opponents - WSJ.

17. Perlroth, Nicole. 2021. “How China transformed Into a Prime Cyber Threat to the U.S.” The New York Times, July 19, 2021. https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html.

18. Reichert, Corinne. 2020. “Europe allows Huawei for 5G through security guidelines.” CNET, January 29, 2020. https://www.cnet.com/tech/mobile/europe-allows-huawei-for-5g-through-security-guidelines/.

19. Sanger, David E., Steven Erlanger. 2018. “Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran.” The New York Times, December 18, 2018. https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html.

20. Schmidt, Michael S., Keith Bradsher, Christine Hauser. 2012. The New York Times, October 8, 2012. U.S. Panel Calls Huawei and ZTE ‘National Security Threat’ - The New York Times (nytimes.com).

21. Shahbaz, Adrian. 2018. “Freedom on the Net 2018: The Rise of Digital Authoritarianism.” The Freedom House, October 18, 2018. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

22. Tamkin, Emily. 2017. “10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?” Foreign Policy, April 27, 2017. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

23. U.S Embassy and Consulates in Brazil. 2020. “United States and Brazil Sign US $1 Billion Memorandum of Understanding.” October 20, 2020. https://br.usembassy.gov/united-states-and-brazil-sign-us-1-billion-memorandum-of-understanding/.

24. U.S Embassy in Georgia. 2021. “United States-Georgia Memorandum of Understanding on 5G Strategy.” January 14, 2021. https://ge.usembassy.gov/united-states-georgia-memorandum-of-understanding-on-5g-security/.

25. Venard, Bertrand. 2019. “The Cold War 2.0 between China and the US is already a virtual reality.” The Conversation, October 16, 2019. https://theconversation.com/the-cold-war-2-0-between-china-and-the-us-is-already-a-virtual-reality-125081.