Georgian Scientists

ქართველი მეცნიერები

Vol. 4 Issue 3, 2022

https://doi.org/10.52340/gs.2022.04.03.15

კიბერუსაფრთხოების გამოწვევები საქართველოში

ნინო ლომიძე

დოქტორანტი, კავკასიის უნივერსიტეტი, სახელმწიფო მართვის სკოლა, საერთაშორისო ურთიერთობების სადოქტორო პროგრამა, საქართველო, თბილისი

აბსტრაქტი

XXI საუკუნე ტექნოლოგიური განვითარების თვალსაზრისით გარდამტეხი აღმოჩნდა. სწრაფმა ტექნიკურმა პროგრესმა ბევრ სიკეთესთან ერთად მნიშვნელოვანი გამოწვევების წინაშეც დააყენა მსოფლიო. თითქმის ყველა სფეროში ციფრულ ტექნოლოგიებზე მზარდმა დამოკიდებულებამ გაზარდა კიბერდანაშაულის რისკები და საფრთხეები. კიბერსივრცეს საკმაოდ აქტიურად იყენებენ როგორც სახელმწიფო, ასევე, არასახელმწიფო აქტორები-ტერორისტული ორგანიზაციები, რომ არაფერი ვთქვათ ცალკეული ინდივიდების მიერ განხორციელებულ კიბერშეტევებზე. ამ გლობალურ საფრთხეს რა თქმა უნდა საქართველოც ვერ აუვლიდა გვერდს.

მოცემული ნაშრომი ეხება კიბერუსაფრთხოების გამოწვევებს საქართველოში. ნაშრომში განხილულია კიბერდანაშაულის მეთოდები და მისი გავლენა ეროვნული უსაფრთხოების კონცეფციაზე. ნაშრომი ეფუძვნება რეალიზმის თეორიას და განიხილავს იმ ძირითად მახასიათებლებს რისი მეშვეობითაც სახელმწიფოები და არასახელმწიფოებრივი აქტორები ატარებენ საკუთარ ინტერესებს და ახდენენ ძალის დემონსტრირებას ან გამოყენებას.

კვლევაში ასახულია ის ძირითადი საფრთხეები და გამოწვევები, რაც არსებობს კიბერ და საინფორმაციო მიმართულებით საქართველოში, გამოტანილია შესაბამისი დასკვნები და კვლევის ბოლოს მოცემულია გარკვეული სახის რეკომენდაციები.

საკვანძო სიტყვები: კიბერუსაფრთხობა, კიბერდანაშაული, ჰიბრიდული ომი, ეროვნული უსაფრთხოება.

შესავალი

XXI საუკუნე ტექნოლოგიური განვითარების თვალსაზრისით გარდამტეხი აღმოჩნდა. სწრაფმა ტექნიკურმა პროგრესმა ბევრ სიკეთესთან ერთად მნიშვნელოვანი გამოწვევების წინაშეც დააყენა მსოფლიო. თითქმის ყველა სფეროში ციფრულ ტექნოლოგიებზე მზარდმა დამოკიდებულებამ გაზარდა კიბერდანაშაულის რისკები და საფრთხეები. კიბერსივრცეს საკმაოდ აქტიურად იყენებენ როგორც სახელმწიფო, ასევე, არასახელმწიფო აქტორები-ტერორისტული ორგანიზაციები, რომ არაფერი ვთქვათ ცალკეული ინდივიდების მიერ განხორციელებულ კიბერ შეტევებზე. ამ გლობალურ საფრთხეს რა თქმა უნდა საქართველოც ვერ აუვლიდა გვერდს.

წინამდებარე **ნაშრომის მიზანია** საქართველოში არსებული კიბერსაფრთხეების იდენტიფიცირება ეროვნული უსაფრთხოების კონტექსტში, განსაკუთრებით კოვიდ პანდემიის პირობებში, როცა კიდევ უფრო მეტად გახდა დამოკიდებული მთელი მსოფლიო ციფრულ ტექნოლოგიებზე და გაზარდა მისი როლი ყველა სფეროში. უკრაინაში რუსეთის მიერ განხორციელებულმა აგრესიამ კიდევ უფრო ცხადად დაგვანახა კიბერ ომის მნიშვნელობა. ჰიბრიდული ომის მეთოდებმა და მძლავრმა პროპაგანდისტურმა ქსელმა გვაჩვენა თუ როგორ შეიძლება შეიცვალოს ომის მიმდინარეობა ყოველწამიერად. ამასთანავე, საბრძოლო ასპარეზზე ახალი ძალის- „ანონიმუსის“ გამოჩენამ საკმაოდ დიდი გავლენა იქონია ომის მიმდინარეობის პროცესზე, რაც ჯერ კიდევ დასრულებული არ არის. ყოველივე ამან კი გარკვეულწილად კიბერდანაშაულის რომანტიზებაც მოახდინა. ამ ეტაპზე მართალია ეს დაჯგუფება სწორ მხარეს იბრძვის, მაგრამ მომავალში მსგავსი ტიპის ორგანიზაციები რომელ მხარეს აღმოჩნდებიან და რა საფრთხეს შეუქმნიან მსოფლიო წესრიგს, არავინ უწყის. სწორედ ამიტომ, კიბერ დანაშაულის მნიშვნელობას და მის მასშტაბურობას აღნიშნული ქეისი კიდევ უფრო მეტად უსვამს ხაზს, რადაგან ცხადად ვხედავთ თუ რამხელა გავლენა აქვს ციფრულ სამყაროს ყოველდღიურ ცხოვრებაზე და ქვეყნის ეროვნულ უსართხოებაზე. მით იმეტეს, იმ ფონზე, როცა კიბერ დანაშაული არც ისე უცხო მცნებაა ჩვენი ქვეყნისთვის. საქართველოში არა ერთი კიბერშეტევა დაფიქსირებულა, არ მხოლოდ ლოკალური მასშტაბის, არამედ ეროვნული უსაფრთხოების კუთხითაც. იქნება ეს 2008 წლის აგვისტოს ომი და რუსული აგრესიის პარალელურად ჰაკერული შეტევები ქართულ სამთავრობო ქსელებსა თუ უწყებებზე, თუ უფრო მოგვიანებით-2019 წელს არანაკლებ მასშტაბური კიბერთავდასხმა ქართულ სახელმწიფო თუ საბანკო სექტორზე.

სწორედ 2008 წლის კიბერ შეტევის შედეგად მკვეთრად გამოჩნდა კიბერუსაფრთხოების მიმართულებით ეროვნული სტრატეგიის და სამოქმედო გეგმის შემუშავების აუცილებლობა (სვანაძე 9, 2015) და ამ მიმართულებით მნიშვნელოვანი ნაბიჯების გადადგმა.

ყოველივე ზემოთ აღნიშნულიდან გამომდინარე, აღნიშნული რისკებისა და საფრთხეების შეფასების მიზნით საკვლევი კითხვა ჩამოყალიბდა შემდეგი სახით: ***რა საფრთხეების და***

გამოწვევების წინაშე დგას საქართველო კიბერუსაფრთხოების კუთხით და როგორია მისი გავლენა ეროვნული უსაფრთხოების კონცეფციაზე?

მაშინ როდესაც ქვეყანა მუდმივი კუნფლიქტის საფრთხის რეჟიმშია მეზობელი რუსეთის მხრიდან მოსალოდნელი რისკების და საფრთხეების შეფასება აუცილებელი წინაპირობაა ქვეყნის ეროვნული უსაფრთხოებისათვის, სწორად დაგეგმილი კიბერ პოლიტიკა კი ერთ-ერთი უმთავრესი ბერკეტია ქვეყნის უსაფრთხოების თვალსაზრისით.

1. **კვლევის მეთოდოლოგია, ლიტერატურის მიმოხილვა და თეორიული ჩარჩო**

წინამდებარე კვლევა ეყრდნობა კიბერუსაფრთხოების საკითხთან დაკავშირებული აკადემიური და ნორმატიული მასალების დამუშავების შედეგად მიღებულ ინფორმაციას.

კვლევის პროცესში გავეცანი კიბერუსაფრთხოების, კიბერდანაშაულის, კიბერშპიონაჟის და ზოგადად კიბერსივრცის შესახებ არსებულ სხვადასხვა წყაროებს და ნორმატიულ მასალას.

კიბერდანაშაულის კუთხით მთავარ დოკუმენტს წარმოადგენს „კონვენცია კომპიუტერული დანაშაულის შესახებ“, რომელიც 2001 წლის 23 ნოემბერს იქნა მიღებული ქ. ბუდაპეშტში. აღნიშნული დოკუმენტი მიმართულია კომპიუტერული დანაშაულისგან საზოგადოების დაცვისკენ. კონვენციაში დეტალურად არის გაწერილი მონაცემების ბაზებთან უნებართოდ დაშვება, მონაცემების ხელყოფა, სისტემაში ჩარევა, მათ შორს იმ ტიპის კომპიუტერული მოწყობილობის გამოყენება, რომელიც შექმნილი და ადაპტირებულია კომპიუტერული თავდასხმებისთვის.

რაც შეეხება საქართველოში კიბერუსაფრთხოების კუთხით მთავარ დოკუმენტს წარმოადგენს „საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ“ (2012 წლის 1 ივლისი) და „საქართველოს კიბერუსაფრთხოების 2021-2024 წლების ეროვნული სტრატეგია და მისი სამოქმედო გეგმა“, რომელიც 2021 წლის 30 სექტემბერს იქნა მიღებული.

„საქართველოს კანონის ინფორმაციული უსაფრთხოების შესახებ“ ინფორმაციულ უსაფრთხოებას განმარტავს შემდეგნაირად: „საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიცენციალურობისა და განგრძობადი მუშაობის დაცვას“ (საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ 2012, მუხლი 2).

„კიბერსივრცე-სივრცე, რომელის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და

დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვისათვის, შეცვლისათვის ან გაცვლისათვის;

კიბერშეტევა-ქმედება, როდესაც ელექტრონული მოწყობილობა ან/და მასთან დაკავშირებული ქსელი ან სისტემა გამოიყენება კრიტიკულ ინფორმაციულ სისტემაში შემავალი სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით“ (საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ 2012, მუხლი 2).

კიბერშეტევა, რომელიც საფრთხეს უქმნის ადამიანის სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას, კანონის შესაბამისად კიბერუსაფრთხოების პრიორიტეტულ საფრთხეებს მიეკუთვნება (საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ 2012, მუხლი 8).

ზოგადად, „კიბერუსაფრთხოება გულისხმობს კომპიუტერული ქსელების და მათში შემავალი ინფორმაციის დაცვას შეღწევისგან და მავნე დაზიანებისგან ან შეფერხებისგან“ (ლუისი 2006, 1).

საერთაშორისო სატელეკომუნიკაციო გაერთიანება (ITU) კიბერუსაფრთხოებას შემდეგნაირად განმარტავს: „კიბერუსაფრთხოება ეს არის ინსტრუმენტების, პოლიტიკის, უსაფრთხოების კონცეფციების, უსაფრთხოების გარანტიების, რისკის მართვის და ტექნოლოგიების ერთობლიობა, რომელიც შეიძლება გამოყენებულ იქნას კიბერგარემოსა და ორგანიზაციის და მომხმარებლის დასაცავად“ (Cremer, Frank, et al. 2014, 14).

„საქართველოს კიბერუსაფრთხოების 2021-2024 წლების ეროვნული სტრატეგია“ მის სამოქმედო გეგმასთან ერთად წარმოადგენს კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ ძირითად დოკუმენტს. დოკუმენტში დეტალურად არის გაწერილი კიბერუსაფრთხოების სტრატეგიული მიზნები და ამოცანები, დასახულია კონკრეტული აქტივობები და განსაზღვრულია ამ აქტივობებზე პასუხისმგებელი უწყებები (საქართველოს კიბერუსაფრთხოების 2021-2024 წლების ეროვნული სტრატეგია).

კვლევის პროცესში გავეცანი სხვადასხვა სტატიებსა თუ მნიშვნელოვან წყაროებს. „კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები“ ინფორმაციის თავისუფლების განვითარების ინსტიტუტის (IDFI) მიერ Counterpart International-ის და ამერიკის შეერთებული შტატების საერთაშორისო განვითარების სააგენტოს (USAID) ფინანსური მხარდაჭერით ამ მიმართულებით განხორციელებული საკმაოდ საინტერესო კვლევაა, რომელშიც იკვეთება სწორი აქცენტები საქართველოს კიბერ გამოწვევების მიმართულებით.

საკმაოდ მნიშვნელოვან წყაროს წარმოადგენს კიბერუსაფრთხოების მიმართულებით ვლადიმერ სვანაძის კრებული „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები.“ კრებული წარმოადგენს სხვადასხვა დროს გამოცემულ სტატიების ერთობლიობას, რომელიც ავტორის მიერ გამოქვეყნებულ იყო კიბერუსაფრთხოების კუთხით. მნიშვნელოვანი ქართულენოვანი წყაროა ვლადიმერ სვანაძის და ანდრია გოცირიძის ნაშრომების კრებული „კიბერ თავდაცვა- კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები.“

რაც შეეხება კვლევის თეორიულ ნაწილს საკვლევი დოკუმენტი დაფუძვნებულია რეალიზმის თეორიაზე და ძალის პრიმატზე. ძალთა ბალანსის სისტემა XXI საუკუნეში თითქოს/და არარელევანტურია და თავისი თავი ამოწურა, რეალიზმის თეორის კრიტიკოსებიც აღნიშნულ თეორიას არასიცოცხლისუანარიანად თვლიან, მაგრამ მიუხედავად ყველაფრისა რეალიზმი ჯერ კიდევ ინარჩუნებს თავის მნიშვნელობას მსოფლიო პოლიტიკაში და ქვეყნებს შორის ურთიერთობები ჯერ კიდევ დამოკიდებულია ძალთა გადანაწილებაზე. თუმცა, რა თქმა უნდა, რეალიზმის თეორიამ სახე იცვალა და გარემოსთან ადაპტირება მოახერხა. დღეს ქვეყნის სიძლიერე არა მხოლოდ სამხედრო ძალაზე, არამედ სხვა ბევრ ფაქტორზეც არის დამოკიდებული. მათ შორის ერთ-ერთი უმთავრესი სწორედ ტექნოლოგიური სიძლიერეა. კიბერ სივრცე კი ამ მხრივ მოქმედების ფართო არეალს იძლევა.

კლასიკური რეალიზმის ფუძემდებლის თუკიდიდეს „ისტორიის“ მიხედვით, სადაც აღწერილია ომი საბერძნეთის პოლისებს შორის (ე.წ. „პელოპონესის ომები“), ყველა სახელმწიფომ დიდმა თუ პატარამ უნდა მოახერხოს მოცემულ რეალობაში ადაპტაცია, რათა გადარჩეს (აკობია 2006, 17). ნეორეალიზმის თეორიის მიხედვით კი სახელმწიფოები აწესებენ მოქმედების იმ კურსს, რომელიც უკეთ ემსახურება მათი ქვეყნის ეროვნულ ინტერესებს (აკობია 2006, 27). ქვეყნის ეროვნული ინტერესებიდან გამომდინარე სახელმწიფოები ხშირად მიმართავენ ძალადობას. ბოლო პერიოდში კი კიბერ თავდასხმები საკმაოდ გახშირებული მეთოდია სახელმწიფოების მხრიდან თავისი ძალის დემონსტრირებისთვის თუ სხვა სახელმწიფოს შიდა საქმეებზე გავლენის მოხდენისთვის. დეზინფორმაციის გავრცელებით თუ პირდაპირი ჰაკერული შეტევებით ზოგჯერ სახელმწიფოს შიდა პოლიტიკურ მდგომარეობაზე იმხელა გავლენას ახდენენ, რომ პოლიტიკური ცვლილებების შედეგიც კი დგება. ამის მაგალითად შეგვიძლია მოვიყვანოთ რუსეთის მიერ აშშ-ს 2016 წლის საპრეზიდენტო არჩევნებში ჩარევა დონალდ ტრამპის სასარგებლოდ, რომელიც მართალია ოფიციალურად დადასტურებული არ არის, თუმცა ფაქტია, რომ საკმაოდ დიდი გავლენა იქონია ტრამპის გამარჯვებაზე და გამოიწვია შიდა პოლიტიკური ცვლილებები. მსგავს ჩარევას რუსეთის მხრიდან ადგილი ჰქონდა ცოტა მოგვიანებით საფრანგეთის არჩევნების დროსაც. არაერთი მსგავში შეტევა თუ დეზინფორმაციული კამპანიას რუსეთის მხრიდან საქართველოშიც არაერთხელ დაფიქსირებულა.

მიუხედავად იმისა, რომ რეალიზმის თეორიის მიხედვით სახელმწიფოები არიან მთავარი აქტორები, ბოლო პერიოდში არასახელმწიფოებრივი აქტორებიც საკმაოდ მნიშნელოვან როლს თამაშობენ მსოფლიო წესრიგსა და ძალთა გადანაწილებაზე. აქ ერთი მთავარი კომპონენტია აღსანიშნავი, რომ არასახელმწიფოებრივმა აქტორებმა გარკვეულწილად სახელმწიფოებრივი აქტორის როლი მოირგეს (სირბილაძე 2013). მაგალითად შეგვიძლია დავასახელოთ ტერორისტული ორგანიზაციები, რომლებსაც სახელმწიფო წარმონაქმნის პრეტენზია გააჩნიათ, იქნება ეს „ალ-ქაიდა“ თუ „დაეში.“ აღნიშნული ტერორისტული ორგანიზაციები კარგად იყენებენ კიბერსივრცეს და სწორად ახდენენ საკუთარი თავის პოზიციონირებას. ამასთანავე, როგორც უკვე აღვნიშნე, არა მხოლოდ ტერორისტული ორგანიზაციები, არამედ ხშირად თავად სახელმწიფოები იყენებენ კიბერთავდასხმებს ძალის დემონსტრირების თუ სხვა სახელმწიფოზე თავდასხმის მიზნით.

2. ინფორმაციულ უსაფრთხოებაზე პასუხისმგებელი უწყებები

სანამ უშუალოდ კიბერუსაფრთხოების მიმართულებით არსებულ საფრთხეებსა და გამოწვევაზე გადავალ, მოკლედ მიმოვიხილავ იმ სახელმწიფო უწყებებს, რომლის კომპეტენციასაც წარმოადგენს ინფორმაციული და კიბერ უსაფრთხოების დაცვა საქართველოში.

ინფორმაციული უსაფრთხოების წესების შესრულების უზრუნველყოფა და კოორდინაცია წარმოადგენს ციფრული მართველობის სააგენტოს (ყოფილი მონაცემთა გაცვლის სააგენტო) კომპეტენციას, თავდაცვის სისტემაში კი ინფორმაციული უსაფრთხოების დაცვასა და კოორდინაციაზე თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროა პასუხისმგებელი (კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები 2020, 10). ციფრული მართველობის სააგენტოს დაქვემდებარებაში ფუნქციონირებს კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი, რომელიც საკუთარი კომპეტენციის ფარგლებში, ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების და კიბერუსაფრთხოების მიმართულებით არსებული რისკების და საფრთხეების აღმოფხვრაზეა პასუხისმგებელი (კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები 2020, 11).

2012 წლიდან შსს-ში ფუნქციონირებს კიბერდანაშაულთან ბრძოლის სამმართველო, რომელიც პასუხისმგებელია კიბერსივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენასა, აღკვეთასა და პრევენციაზე (კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები 2020, 11).

რაც შეეხება ფინანსური მიმართულებით კომერციული ბანკების დარგობრივ მარეგულირებელს საქართველოს ეროვნული ბანკი წარმოადგენს, რომელიც კომერციულ ბანკებს უწევს ზედამხედველობას რათა დააკმაყოფილონ ინფორმაციული უსაფრთხოების მინიმალური სტანდარტები (კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები 2020, 12).

2019 წელს შეიქმნა ეროვნული უსაფრთხოების საბჭო, რომლის მთავარი ფუნქცია ეროვნული უსაფრთხოების საკითხებზე პოლიტიკის დაგეგმვისა და კოორდინაციის მიზნით გადაწყვეტილებების მომზადებაა. საბჭოს ფუნქციებში შედის ინფორმაციული უსაფრთხოების პოლიტიკის იმპლემენტაციის კოორდინაციაც (კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები 2020, 13).

3. კიბერუსაფრთხოების გამოწვევები

❖ სოციალური მედია

ინტერნეტის მომხმარებელთა რაოდენობა წლიდან წლამდე იზრდება. გაეროს საერთაშორისო სატელეკომუნიკაციო გაერთიანების (ITU) სტატისტიკის თანახმად საქართველოს მოსახლეობის 70% მოიხმარს ინტერნეტს, თუმცა რეალური რიცხვი შეიძლება გაცილებით უფრო მაღალიც იყოს (საქართველოს კიბერუსაფრთხოების 2021-2024 წლების ეროვნული სტრატეგია). ტექნოლოგიებზე მზარდმა დამოკიდებულებამ შესაბამისად რისკების გაზრდაც გამოიწვია. კოვიდპანდემიის პირობებში კი სახელმწიფო თუ კერძო სექტორის მასიურად დისტანციურ რეჟიმზე გადასვლამ კიბერთავდასხმების კუთხით მოწყვლადობა კიდევ უფრო გაზარდა.

ინტერნეტ რესურსებზე ადამიანების დამოკიდებულება დღითიდღე თვალში საცემია. ყველაზე მეტად კი ადამიანები სოციალურ მედიას და სხვადასხვა სოციალურ პლატფორმებს მოიხმარენ.

XX საუკუნის დასაწყისში ალბათ ვერავინ წარმოიდგენდა თუ რამდენად შეიძლებოდა გამხდარიყო ადამიანი დამოკიდებული სოციალურ მედიაზე. მისი გავლენა დღითიდღე იზრდება და გარდა ბევრი სიკეთისა ხშირად საფრთხის შემცველიც ხდება. სოციალურ მედიაში ბევრ სხვადასხვა ქსელს მოვიაზრებთ, მაგრამ მათ შორის განსაკუთრებით პოპულარულია Facebook, Twitter, YouTube, Linkedin, Instagram და სხვა.

სოციალური მედია მომხმარებლების რაოდენობა მსოფლიოში დღითიდღე მატულობს, რადგან იაფ საკომუნიკაციო საშუალებასთან ერთად მისი მოხმარება საკმაოდ მარტივია და

გამოყენებაც მრავალი მიმართულებით არის შესაძლებელი. თუმცა, სამწუხაროდ, სოციალურ მედიას სხვადასხვა ორგანიზაციები თუ ჯგუფები თავისი ინტერესების შესაბამისად იყენებენ. ტერორისტული ორგანიზაციების რეკრუტირების საკმაოდ დიდი წილი სწორედ სოციალურ მედიაზე მოდის. ზოგიერთი რადიკალური ექსტრემისტული ორგანიზაციები კარგად იყენებენ სოც. მედიას არა მხოლოდ რეკრუტირების კუთხით, არამედ ინფორმაციის გასავრცელებლად და შიშის დანერგვის მიზნითაც.

სოციალური მედიის ზუსტი განმარტება არ გვაქვს, მას ზოგადად ახასიათებენ. The US Congressional Research Service (CRS) ანალიტიკოსის ბრუს ლინდსის გამნარტებით: „ტერმინი სოციალური მედიის შესახებ განეკუთვნება ინტერნეტ-ბმულებს, რომლებიც იძლევა ადამიანთა შორის ურთიერთობის საშუალებას, რესურსებისა და ინფორმაციის ერთობლივ გამოყენებას“ (სვანაძე 2015, 14).

ტრადიციული მედიისგან განსხვავებით სოციალური მედია გაცილებით უფრო ხელმისაწვდომია და ინფორმაციაც უფრო სწრაფად ვრცელდება. შესაბამისად, რისკებიც კიდევ უფრო მაღალია. სოციალური მედიის საშუალებით ძალიან ხშირია დეზინფორმაციული ნარატივის გავრცელება და ძალიან კარგი საშუალებაა მასებზე ზემოქმედების კუთხით. ამიტომ, ხშირად დგება ხოლმე საკითხი სოციალური მედიის შეზღუდვის საჭიროების მიმართულებით. აქ კი ზღვარის გავლება საკმაოდ რთულია, რადგან ერთის მხრივ სიტყვის და გამოხატვის თავისუფლების დილება დგას, მეორეს მხრივ კი უსაფრთხოება, ამიტომ ამ ზღვარზე გავლა არც ისე ადვილია, რათა სხვადასხვა უწყებებმა თუ სახელმწიფოებმა პირადი ინტერესების მიზნით არ გამოიყენონ სოციალურ მედიაზე დაწესებული რეგუალიცები (სვანაძე 2014, 6).

❖ კიბერ ომი და კიბერ დანაშაული

თუ საუკუნეების განმავლობაში ომი ფიზიკური ძალადობის ფორმას წარმოადგენდა და დამოკიდებული იყო ჯარის და სამხედრო ტექნიკის ძლიერებაზე, ბოლო წლებია ომმა ფორმა შეიცვალა და ტექნოლოგიებზე სულ უფრო და უფრო დამოკიდებული გახდა. კიბერომი და კიბერდანაშაული ამის ერთ-ერთი მთავარი მაგალითია. კიბერომმა შეიძლება გაცილებით უფრო დიდი ზიანი მიაყენოს მოწინააღმდეგეს, ვიდრე ღია საბრძოლო მოქმედებებმა. კრიტიკული ინფრასტრუქტურის ძირითადი ობიექტები თითქმის სრულად დამოკიდებულია ინტერნეტზე და მასზე შეტევამ შეიძლება სრული პარალიზება გამოიწვიოს ქვეყნის როგორც თავდაცვის, აგრეთვე, ფინანსურ, ეკონომიკურ და ჯანდაცვის სისტემებზე.

სხვადასხვა სახელმწიფოები განსაკუთრებით აქტიურად იყენებენ კიბერშეტევებს. ასეთები არიან რუსეთი, აშშ, ისრაელი, ჩინეთი, ჩრ. კორეა. ამ სახელმწიფოებს მძლავრი

კიბერშესაძლებლობები გააჩნიათ. თუმცა უკვე ყველა სახელმწიფო ცდილობს გაზარდოს თავისი კიბერშესაძლებლობები.

რუსეთის მძლავრი კიბერ დანაშაული პირდაპირ აისახება საქართველოს ეროვნულ უსაფრთხოებაზე. ქვეყანა არა მხოლოდ სამხედრო ძალადობას ახორციელებს საქართველოს მიმართულებით, არამედ წლებია კიბერშეტევებსაც იყენებს. 2008 წელს საბრძოლო მოქმედებების პარალელურად რუსეთის ფედერაციამ არაერთი კიბეერშეტევა განახორციელა სასიცოცხლო ინფრასტრუქტურაზე და გათიშა სახელმწიფოს მნიშვნელოვანი ობიექტები. მოგვიანებით, 2019 წელს, აგრეთვე დიდი შეტევა განახორციელა საქართველოს სამთავრობო და საფინანსო უწყებებზე. მცირე სახის შეტევებს ეტაპობრივად სულ აქვს ადგილი. განსაკუთრებით ხშირია კიბერ შეტევები ოკუპირებული აფხაზეთის ტერიტორიიდან (სვანაძე და გოცირიძე 2015, 100). კიბერსივრცეში განხორციელებული შეტევების დროული და ეფექტიანი გამოძიებისთვის განსაკუთრებული მნიშვნელობა ენიჭება საერთაშორისო გამოცდილებას და თანამშრომლობას. სწორედ ამ თანამშრომლობის პირობებში განხორციელდა „დაეშის“ მიერ 2015 წლის 23 ნოემბერს საქართველოს მიმართ მუქარის შემცველი ვიდეოს დაბლოკვა (საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში-01.08.2015-31.12.2015, 16).

წლიდან წლამდე ჰიბრიდული ომის საფრთხეები უფრო აქტუალური ხდება და უცხო ქვეყნის სპეცსამსახურები თუ მათთან დაკავშირებული ჰაკერული ჯგუფები საკუთარი ინტერესებიდან გამომდინარე სულ უფრო და უფრო აქტიურად იყენებენ კიბერსაშუალებებს სამთავრობო და კრიტიკული ინფრასტრუქტურის ობიექტებზე კიბერშეტევებისა და კიბერსადაზვერვო ოპერაციების განხორციელების მიზნით (საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში-01.01.2018-31.12.2018, 13). ტერორისტული ორგანიზაციებისთვის საკუთარი იდეოლოგიის გავრცელების და შემდგომში პოტენციური რეკრუტების გადაბირების ძირითადი საშუალება სწორედ ინტერნეტ სივრცეა. სახელმწიფო უსაფრთხოების სამსახური აღნიშნული მიმართულებით ახორციელებს სისტემატიურ მონიტორინგს რათა ხელი შეუშალოს ტერორისტული თუ ექსტრემისტული ნარატივების გავრცელებას ინტერნეტსივრცეში (საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 2019 წელი, 26).

როგორც საქართველოს სახელმწიფო უსაფრთხოების სამსახურის 2020 წლის ანგარიშშია ასახული, კიბერშეტევებმა განსაკუთრებით აქტიური ხასიათი მიიღო 2020 წლიდან კორონავირუსის პანდემიის დაწყების პარალელურად და არაერთი შეტევა განხორციელდა ქვეყნის ჯანდაცვის სისტემაზე. ზოგადად პანდემიის პერიოდში მსოფლიო ჯანდაცვის სისტემები კიბერ შეტევის მსხვერპლი არაერთხელ გახდნენ და ამ მხრივ არც საქართველო ყოფილა გამონაკლისი. 2020 წლის სექტემბერში ოკუპირებული აფხაზეთის ტერიტორიიდან საქართველოს დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს კომპიუტერულ სისტემაზე განხორციელდა კიბერთავდასხმა, რომლის დროსაც ადგილი ქონდა მნიშვნელოვანი დოკუმენტაციის, მათ შორის რ. ლუგარის სახელობის ლაბორატორიიდან

ინფორმაციის მოპოვებას და ერთ-ერთ უცხოურ ვებგვერდზე ატვირთვას. ამასთანავე, იგივე ვებ გვერდზე აიტვირთა გაყალბებული ინფორმაციაც, რაც მიზნად ისახავდა ლუგარის ლაბორატორიის საქმიანობისასთან დაკავშირებით საზოგადოების შეცდომაში შეყვანას და ქვეყნის დისკრედიტაციას და იმიჯის შელახვას საერთაშორისო მასშტაბით. აღსანიშნავია, რომ აღნიშნულ ფაქტს წინ უსწრებდა რუსული დეზინფორმაციის მძლავრი კამპანია ლუგარის ლაბორატორიასთან დაკავშირებით (საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 2020 წელი, 24). კიბერაქტორები კარგად იყენებენ ე.წ. ფიშინგის, კიბერშპიონაჟის მეთოდებს, იპარავენ პირად ინფორმაციას და ხშირად აღნიშნულ ინფორმაციას შავ ბაზარზე ყიდიან. კიბერრისკების სწრაფად ცვალებადი ბუნების გამო, ხშირად შეუძლებელია მის შესახებ სრული ინფორმაციის მოპოვება და განსაზღვრა (Cremer, Frank, et al 2022, 710). კიბერსივრცის დაცვა განსაკუთრებით რთულია მთელი რიგი ფაქტორების გამო: კიბერაქტორების უნარი მოქმედებნენ მსოფლიოს ნებისმიერი ადგილიდან, კიბერსივრცისა და ფიზიკურ სისტემებს შორის კავშირები და რთულ კიბერ ქსელებში დაუცველობისა და შედეგების შემცირების სირთულე (Cybersecurity& Infrastructure Security Agency).

ამასთანავე, სოციალური მედიით სისტემატიურად ვრცელდება სიძულვილის ენის ფაქტები და არაერთი ჯგუფი თუ გვერდი არსებობს, რომელიც ძალადობისკენ არის მიდრეკილი (მაგ: „ალტ-ინფო“ და მასთან დაკავშირებული სატელიტი ჯგუფები და ორგანიზაციები). მსგავსი ჯგუფები პერიოდულად მოუწოდებენ მოსახლეობას ძალადობისაკენ, ავრცელებენ ცრუ ინფორმაციას და რელიგიურ სენტმენტებზე ზემოქმედების გზით მოსახლეობაში ნერგავენ დასავლური ღირებულებების სიძულვილს და არ ერიდებიან პირდაპირ აგრესიას.

დასკვნები

როგორც ვხედავთ, კიბერსივრცე საკმაოდ ფართო შესაძლებლობებს იძლევა სხვადასხვა მიმართულებით და დადებითის გარდა ძალიან დიდი საფრთხის შემცველიცაა. ჰიბრიდული ომი და ასიმეტრიული ომის მეთოდები თანამედროვე კონფლიქტების მძლავრი იარაღია.

ყველა სახელმწიფო საკუთარი ინტერესებიდან გამომდინარე იყენებს ყველა რესურსს პოლიტიკის გატარების და ძალის დემონსტრირების მიზნით და ინტერნეტ სივრცე ამის კარგი საშუალებაა. რეალისტური იდეოლოგიის ჭრილში თუ განვიხილავთ, როგორც თუკიდიდე აღნიშნავს, ყველა სახელმწიფო ცდილობს მოცემულ რეალობაში ადაპტაცია მოახერხოს, რათა გადარჩეს (აკობია 2006, 17). ნეორიალიზმის თეორიიდან გამომდინარეც სახელმწიფოები სწორედ იმ კურსს ირჩევენ, რომელიც მათ ეროვნულ ინტერესებს უკეთ ემსახურება (აკობია 2006, 27). ამიტომ, რეალიზმის თეორიის მიხედვით, სახელმწიფოს არჩევანი განახორციელოს ძალადობა

სხვადასხვა მიმართულებით დასაშვებია, თუ ეს ქვეყნის ინტერესებს ემსახურება. კიბერშეტევები ამის კარგი მაგალითია. სახელმწიფოები ღიად თუ ფარულად ახორციელებენ ჰაკერულ თავდასხმებს, აზიანებენ კრიტიკულ ინფრასტრუქტურას, მოიპოვებენ ინფორმაციას და ა.შ. არასახელმწიფო აქტორები კიდევ უფრო კარგად იყენებენ ინფორმაციულ ქსელს საკუთარი ინტერესების გატარების მიზნით. მაგალითად, უკრაინის ომის ერთ-ერთი მთავარი განმსაზღვრელი სწორედ კიბერთავდასხმებიც იყო, „ანონიმუსმა“ არაერთხელ განახორციელა რუსული სამხედრო ტექნიკის მწყობრიდან გამოყვანა და არაერთი მნიშვნელოვანი დოკუმენტი მოიპოვა და გაასაჯაროვა. ზოგიერთი მკვლევარი კიბერსუბიექტების მნიშვნელობას დადებით ჭრილში განიხილავს ძალთა ბალანსის შენარჩუნებაზე, რადგან აქ არ არსებობს ერთიანი დომინანტური ძალა (Chitadze 2018, 75). ფაქტი ერთია, რომ ომმა ფორმა იცვალა და ინტერნეტ სივრცეში გადაინაცვლა, ვინც მძლავრ ტექნოლოგიურ რესურს ფლობს ძალაც და გამარჯვებაც მის მხარესაა. ამიტომ ყველა სახელმწიფო თუ არასახელმწიფოებრივი აქტორი ისწრაფვის ტექნოლოგიური გაძლიერებისათვის.

რეკომენდაციები

კვლევიდან იკვეთება, რომ კიბერუსაფრთხოება თანამედროვე მსოფლიოს დიდი გამოწვევაა. სახელმწიფოს ინტერესებიდან გამომდინარე ძალისმიერი მეთოდები გამართლებულია თუ ყოველივე ამას რეალიზმის ჭრილში განვიხილავთ. ამიტომ საჭიროა, რომ სახელმწიფო უწყებებმა გააძლიერონ დაცვის სისტემები, რათა თავიდან იქნას აცილებული კიბერშეტევები სახელმწიფო უწყებებზე და ჰაკერული თავდასხმები კრიტიკულ ინფრასტრუქტურაზე. ამასთანავე, სხვადასხვა ტიპის დეზინფორმაციისა და ტერორიზმის ან რადიკალური ექსტერმიზმის კუთხით არსებული ინფორმაცია სოციალურ სივრცეში და სხვადასხვა სოციალურ პლატფორმებში მკაცრად უნდა კონტროლდებოდეს და შესაბამისი რეაგირებაც მოხდეს. ოღონდ აქ მთავარია არ დაირღვეს ზღვარი სიტყვის გამოხატვის თავისუფლებასა და უსაფრთხოებას შორის.

ამასთანავე, ძალზედ მნიშვნელოვანია საერთაშორისო გამოცდილების გაზიარება და პრაქტიკაში დანერგვა. სახელმწიფო უწყებებმა უნდა ითანამშრომლონ სხვადასხვა სახელმწიფოებთან და საერთაშორისო ორგანიზაციებთან. განსაკუთებით აქტიური თანამშრომლობაა საჭირო ნატოსთან, რადგან ნატოს ყველა კონცეფცია და დოქტრინა ხაზს უსვამს იმას, რომ ალიანსი თითოეულ წევრ სახელმწიფოს საშუალებას აძლევს კოლექტიური გზით მიაღწიოს ეროვნული უსაფრთხოების მიზნებს (Chitadze 2018, 71). ნატო ერთადერთი ორგანიზაციაა, რომელსაც აქვს ტექნიკური, ფინანსური და ადამიანური რესურსი, რათა

გაუძლოს კიბერ საფრთხეებს (Chitadze 2018, 71), ამიტომ მნიშვნელოვანია ორგანიზაციასთან თანამშრომლობა და საერთაშორისო პრაქტიკის გაზიარება.

ჰიბრიდული და ასიმეტრიული ომები XXI საუკუნის მოვლენაა და ამ კუთხით კიბერომს, კიბერდანაშაული და დეზინფორმაციას განსაკუთრებული მნიშვნელობა ენიჭება, ამიტომ აუცილებელია რომ გავაძლიეროთ ამ კუთხით მუშაობა რათა თავიდან იქნას აცილებული ის საფრთხეები და გამოწვევები რის წინაშეც დგას საქართველო მეზობელი რუსეთის თუ სხვა არასახელმწიფოებრივი აქტორების მხრიდან. რადგან ჩვენნაირი ტიპის მცირე სახელმწიფო გაცილებით უფრო მოწყვლადია კიბერდანაშაულის მიმართულებით, რადგან არ გაგვაჩნია შესაბამისი დაცვის სისმტემები.

გამოყენებული ლიტერატურა:

აკობია, ეკა. 2006. *საერთაშორისო ურთიერთობების თეორია.* თბილისი: სოციალურ მეცნიერებათა ცენტრი.

„კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები.“ 2020. თბილისი: ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI), Counterpart International და ამერიკის შეერთებული შტატების საერთაშორისო განვითარების სააგენტო (USAID).

„კონვენცია კომპიუტერული დანაშაულის შესახებ.“ 23.11.2001, ბუდაპეშტი.

„საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ.“ 2012.

„საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია“ (2021-2024 წლები). 2021.

„საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 2019 წელი." თბილისი. https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/%E1%83%A1%E1%83%A3%E1%83%A1%202019%20%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%98.pdf - (21.06.2022).

„საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში 2020 წელი.“ თბილისი. https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/%E1%83%A1%E1%83%90%E1%83%AE%E1%83%94%E1%83%9A%E1%83%9B%E1%83%AC%E1%83%98%E1%83%A4%E1%83%9D%20%E1%83%A3%E1%83%A1%E1%83%90%E1%83%A4%E1%83%A0%E1%83%97%E1%83%AE%E1%83%9D%E1%83%94%E1%83%91%E1%83%98%E1%83%A1%20%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%98%202020--.pdf - (21.06.2022).

„საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში-01.01.2018-31.12.2018.“

თბილისი.
https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%98%202018.pdf - (21.06.2022).

„საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში-01.08.2015-31.12.2015.“ თბილისი.
https://ssg.gov.ge/uploads/%E1%83%90%E1%83%9C%E1%83%92%E1%83%90%E1%83%A0%E1%83%98%E1%83%A8%E1%83%94%E1%83%91%E1%83%98/SSSG%20REPORT.pdf - (21.06.2022).

სვანაძე, ვლადიმერ. 2015. „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები.“

სვანაძე, ვლადიმერ. 2014. „სოციალური ქსელები, დემოკრატია თუ უსაფრთხოება?.“

სვანაძე ვლადიმერ, გოცირიძე ანდრია. 2015. „კიბერ თავდაცვა-კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები (ნაშრომების და სტატიების კრებული). თბილისი: საქართველოს თავდაცვის სამინისტრო, სსიპ-კიბერუსაფრთხოების ბიურო,

სირბილაძე, ირაკლი. 2013. http://www.socium.ge/index.php/articles/student-articles/45-terorizmis-gavlena-vestfaliur-saertashoriso-wesrigze - (21.06.2022).

Chitadze, Nika, 2018. Cyber warfare – New threat for national and international security and transformation of the conflicts under the conditions of the new geopolitical order. Journal of Social Sciences; ISSN: 2233-3878; e-ISSN: 2346-8262; Volume 7, Issue 2.

Craigen, Dan, et al. “Defining Cybersecurity.” *Technology Innovation Management Review*, vol. 4, no. 10, 2014, www.timreview.ca/article/835.

Cremer, Frank, et al. “Cyber Risk and Cybersecurity: A Systematic Review of Data Availability.” *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. volume 47, pages698–736 (2022), no. volume 47, 17 Feb. 2022, 10.1057/s41288-022-00266-6.

Cybersecurity & Infrastructure Security Agency. “CYBERSECURITY | CISA.” *Cisa.gov*, 2019, www.cisa.gov/cybersecurity.

Lewis, James. *Cybersecurity and Critical Infrastructure Protection*. 2006.

Cyber Security Challenges in Georgia

Nino Lomidze

PhD student, Caucasus University, School of Governance, PHD program in International Relations,

Abstract

The XXI century turned out to be a turning point in terms of technological development. Rapid technical progress along with many other benefits has posed significant challenges to the world. The growing reliance on digital technology in almost every field has increased the risks and dangers of cybercrime. Cyberspace is widely used by both state and non-state actors -terrorist organizations not to mention cyberattacks carried out by individual individuals. Georgia could not avoid this global threat either.

This paper addresses the challenges of cyber security in Georgia. The paper discusses the methods of cybercrime and its impact on the concept of national security. The paper is based on the theory of realism and discusses the key characteristics through which states and non-state actors pursue their own interests and demonstrate or use force.

The study reflects the main threats and challenges that exist in cyber and information in Georgia, relevant conclusions are drawn and some kind of recommendations are given at the end of the study.

Keywords: Cyber Security, Cybercrime, Hybrid War, National Security.