Student Journal of Social Sciences

სტუდენტთა ჟურნალი

სოციალურ მეცნიერებებში

№26, თებერვალი, 2024

კიბერუსაფრთხოება, როგორც მთავარი გამოწვევა საერთაშორისო ურთიერთობებში (საქართველოს, უკრაინის, ესტონეთის შემთხვევების ანალიზი)

თამარი ბიბიჩაძე

შოთა ოვაკიმიან

საერთაშორისო ურთიერთობების და კომპიუტერული მეცნიერებების საბაკალავრო პროგრამა

სოციალურ და პოლიტიკურ მეცნიერებათა ფაკულტეტი

ზუსტი და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

E-mail : tamari.bibichadze373@sps.tsu.ge

E-mail : shota.ovakimyan981@hum.tsu.edu.ge

აბსტრაქტი

ციფრული ტექნოლოგიებისა და საერთაშორისო ურთიერთობების ურთიერთდამოკიდებულებამ წარმოშვა უპრეცედენტო გამოწვევები, სადაც ქვეყნების სტაბილურობისა და უსაფრთხოების უზრუნველსაყოფად კიბერუსაფრთხოება კრიტიკულ სფეროდ არის ჩათვლილი. ნაშრომის მიზანია განისაზღვროს საერთაშორისო ურთიერთობებში კიბერუსაფრთხოების მრავალმხრივი განზომილებების მნიშვნელობა კონკრეტული ქვეყნებისა (უკრაინა, ესტონეთი, საქართველო) და ნატოს მაგალითზე.

ნაშრომის საკვლევ კითხვას წარმოადგენს, თუ რა როლს ასრულებს კიბერუსაფრთხოება სამხედრო ოპერაციებისა და სტრატეგიების ჩამოყალიბებაში. როგორ იმოქმედა კიბერ შესაძლებლობების ინტეგრაციამ ქვეყნების თავდაცვისუნარიანობაზე? საკვლევ კითხვაზე პასუხის გასაცემად დავისახეთ შემდეგი ამოცანები: შევისწავლოთ აკადემიური მასალა სამიზნე ქვეყნების ზოგადი კიბერუსაფრთხოების პოლიტიკისა და გამოწვევების შესახებ და გავაანალიზოთ კონკრეტული შემთხვევები.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, ჰიპოთეზა შემდეგნაირად ჩამოყალიბდა: კიბერ შესაძლებლობების ინტეგრაციამ ფუნდამენტურად შეცვალა სამხედრო ოპერაციები და სტრატეგიები ისეთი ქვეყნებისთვის, როგორიცაა უკრაინა, საქართველო, ესტონეთი და თავის მხრივ, ნატო, თუმცა უსაფრთხოების სისტემების დანერგვა თითოეულმა მათგანმა სხვადასხვაგვარად შეძლეს. რამდენადაც ციფრული ტექნოლოგიები სულ უფრო მეტად ერწყმის საერთაშორისო ურთიერთობებს, კიბერსივრცის მრავალმხრივი შესაძლებოლები გადამწყვეტ როლს თამაშობს არა მხოლოდ თავდაცვის პოლიტიკის, არამედ ამ ქვეყნების და ნატოს ალიანსის უფრო ფართო სამხედრო სტრატეგიების ჩამოყალიბებაში. კიბერ შესაძლებლობების სტრატეგიულმა ჩართვამ გამოიწვია პარადიგმის ცვლილება ტრადიციულ სამხედრო დოქტრინებში, რაც მოითხოვს თავდაცვის სტრატეგიების გადაფასებას განვითარებადი კიბერ საფრთხეების ფონზე.

კვლევის პრობლემის ძირითადი მახასიათებელია დიდი ხნის განმავლობაში გადაწყვეტილების მიმღები პირების მიერ ციფრული ტექნოლოგიების ტრანსფორმაციული ზემოქმედების უგულებელყოფა გლობალური უსაფრთხოების ლანდშაფტის გაგებისას, მაშინ როცა ციფრული ტექნოლოგიებისა და საერთაშორისო ურთიერთობების ურთიერთდამოკიდებულება მოიცავს უპრეცედენტო გამოწვევებს. უფრო მეტიც, კიბერუსაფრთხოების დინამიურ და რთულ დინამიკას.

საკვანძო სიტყვები: Distributed Denial-of-Service (DDoS) attack, კრიტიკული ინფრასტრუქტურა, კიბერსივრცე, კიბერშეტევა

შესავალი

საერთაშორისო დღის წესრიგში მომხდარმა გეოპოლიტიკურმა ცვლილებებმა აქტუალური გახადა თანამედროვე პირობებში არსებული კიბერუსაფრთხოების საკითხები, რომლებიც საინფორმაციო-სტრატეგიული-სამხედრო თვალსაზრისით უფრო და უფრო მეტად იძენს ჰიბრიდული ომის მახასიათებლებს. მისი კომპლექსური დინამიკის გაანალიზება, რომელიც პირდაპირკავშირშია სახელმწიფო უსაფრთხოების, სამხედრო ოპერაციების, ეკონომიკური ინტერესებისა და დიპლომატიური ურთიერთობების წარმოებასთან, განაპირობებს კიბერუსაფრთხოების ყოვლისმომცველ გაგებას თანამედროვე გლობალური ლანდშაფტის ჩამოყალიბებაში. მითუმეტეს, რომ ციფრული ტექნოლოგიების წინსვლის დაჩქარებული ტემპი გასცდა ტრადიციულ გეოპოლიტიკურ საზღვრებს, რაც საჭიროებს გლობალური უსაფრთხოების ლანდშაფტის გადაფასებას. კიბერუსაფრთხოების მნიშვნელობა საერთაშორისო ურთიერთობებში მდგომარეობს მის უნარში, შეამსუბუქოს ციფრულ სფეროსთან დაკავშირებული რისკები, სადაც სახელმწიფო აქტორებს, არასახელმწიფო ერთეულებს და ინდივიდებს შეუძლიათ გამოიყენონ სახელმწიფოს დაუცველობა პოლიტიკური, ეკონომიკური ან სტრატეგიული მიზნებისთვის, რაც განაპირობებს კიდეც მის აქტუალურობას და კიბერ საფრთხეების, ეროვნული და საერთაშორისო სტრატეგიების, გამოწვევებისა და თანამშრომლობის მექანიზმების მნიშვნელობას.

სამხედრო სტრატეგიების შექმნისას გადაწყვეტილების მიმღები პირები ყურადღებას ამახვილებენ საინფორმაციო ტექნოლოგიების პრაქტიკულ დანერგვაზე. ამავდროულად, საინფორმაციო და ფსიქოლოგიური ოპერაციები სულ უფრო და უფრო ხშირად გამოიყენება პოლიტიკური და სამხედრო მიზნების მისაღწევად (Sargana, 2020). რამდენადაც ერები სულ უფრო დამოკიდებულნი ხდებიან ურთიერთდაკავშირებულ ქსელებზე სტრატეგიული კომუნიკაციების, კომერციული შეთანხმებების და მმართველობის დროს, კიბერ უსაფრთხოების პოტენციური შედეგები ტექნიკურ შეფერხებებს სცილდება. კიბერუსაფრთხოება დღითიდღე უფრო და უფრო მნიშვნელოვანი ხდება საერთაშორისო ურთიერთობების დინამიკის ფორმირებაში, რამეთუ გავლენას ახდენს დიპლომატიურ ჩართულობებზე, სამხედრო სტრატეგიებზე და ეკონომიკურ ურთიერთქმედებებზე (Khoroshko, Hryshchuk, Brailovskyi & Kapustian,2023).

ტექნოლოგიების სწრაფმა წინსვლამ მრავალი სარგებელი მოიტანა, მაგრამ მან ასევე წინა პლანზე გადმოსწია სახელმწიფოების დაუცველობა და მოწყვლადობა კიბერშეტევების მიმართ. მაგალითისთვის, 2007 წელს ესტონეთი გახდა კიბერშეტევის მსხვერპლი, რომელიც მოიცავდა გამიზნულ თავდასხმებს მთავრობისა და კომერციული ვებსაიტების წინააღმდეგ (Ottis, Solvak, & Ress, 2009). მიღებულმა გაკვეთილმა ესტონეთის მთავრობა აიძულა გადაედგა მრავალი პროგრესული ნაბიჯი კიბერუსაფრთხოების გაუმჯობესებისა და ეროვნული მდგრადობის მიღწევის მიზნით. საინფორმაციო და საკომუნიკაციო ტექნოლოგიებზე მზარდი დამოკიდებულების გამო, ქვეყნებისთვის კიბერუსაფრთხოება გახდა კრიტიკული საზრუნავი მთელ მსოფლიოში.

დღესდღეობით, კიბერუსაფრთხოება ეროვნული უსაფრთხოების იმპერატიულ ასპექტად იქცა. კიბერუსაფრთხოება გულისხმობს ტექნოლოგიების, პროცესებისა და პრაქტიკის ერთობლიობას, რომელიც შექმნილია ქსელების, სისტემებისა და მონაცემების უნებართვო წვდომისგან, კიბერშეტევებისა და დაზიანებისგან დასაცავად. ის მოიცავს ზომების ფართო სპექტრს, მათ შორის პრევენციულ ქმედებებს, გამოვლენის მექანიზმებს და საპასუხო სტრატეგიებს, რომლებიც მიმართულია ციფრული ინფორმაციის მთლიანობის, კონფიდენციალურობისა და ხელმისაწვდომობის შენარჩუნებისკენ (Perwej, 2021).

როდესაც ვსაუბრობთ კიბერუსაფრთხოებაზე საერთაშორისო ურთიერთობებში მხედველობაში გვაქვს ეროვნული სუვერენიტეტის კონცეფცია, რამეთუ მთავრობების მიზანია დაიცვან თავიანთი ტერიტორიები, მოქალაქეები და კრიტიკული ინფრასტრუქტურა კიბერ საფრთხეებისგან. მიუხედავად ამისა, კიბერსივრცის უსაზღვრო ბუნებამ გაართულა გადაწყვეტილების მიმღები პირების მიერ სუვერენული საზღვრების ეფექტურად განსაზღვრისა და დაცვის პერსპექტივა. ამ კონტექსტში, ეროვნული ინტერესების დაცვასა და კიბერსივრცის გლობალური ურთიერთდაკავშირების პატივისცემას შორის დელიკატური ბალანსი რჩება მუდმივ გამოწვევად (Kramer, 2023). ამასთან გამომდინარე იქიდან, რომ ციფრულმა ეპოქამ გარდაქმნა ეკონომიკა, რაც გამოიხატა საინფორმაციო ქსელებზე, მონაცემებსა და ციფრულ ტრანზაქციებზე დამოკიდებულების გაზრდით კიბერშეტევების შედეგები გლობალურ ეკონომიკაზე გადამწყვეტი გახდა საერთაშორისო ვაჭრობის, ფინანსური სისტემებისა და ბიზნეს ოპერაციების გამართული ფუნქციონირების უზრუნველსაყოფად. ინტელექტუალური საკუთრების დაცვის, მონაცემთა გარღვევის თავიდან აცილებისა და კიბერ ჯაშუშობის წინააღმდეგობის გაწევის უნარი აუცილებელია ეკონომიკური სტაბილურობისა და ზრდის შესანარჩუნებლად.

საფრთხეებს შორის მნიშვნელოვან ადგილს იკავებს კიბერ ჯაშუშობა, რადგან სახელმწიფო და არასახელმწიფო აქტორები იყენებენ ციფრულ მოწყვლადობას სენსიტიური ინფორმაციის მოსაგროვებლად. მთავრობები, სადაზვერვო სააგენტოები და კიბერდანაშაულებრივი ქსელები ჩართულნი არიან კიბერ ოპერაციებში, რათა შეაგროვონ ინფორმაცია პოლიტიკურ, სამხედრო, ტექნოლოგიურ და ეკონომიკურ საკითხებზე. ამრიგად, კიბერუსაფრთხოება, როგორც ძირითადი თავდაცვითი მექანიზმი იცავს სუბიექტებს ასეთი შეჭრისგან და თავიდან აცილებს სამიზნე ჯგუფებს კრიტიკული ინფორმაციის დაკარგვას (Trope & Hantover, 2017).

კიბერუსაფრთხოების ზეგავლენა სახელმწიფოებზე იზრდება, რადგან იგი წარმოადგენს სტრატეგიულ იარაღს გეოპოლიტიკური ძალაუფლების მოსაპოვებლად. ფარულ კიბერ ოპერაციებს, მათ შორის კიბერთავდასხმებს და დეზინფორმაციულ კამპანიებს, აქვს პოტენციალი ჩაშალოს პოლიტიკური პროცესები, გავლენა მოახდინოს საზოგადოებრივ აზრზე და შეარყიოს ეროვნული უსაფრთხოება. 2016 წლის აშშ-ის საპრეზიდენტო არჩევნებში ჩარევა წარმოადგენს თვალსაჩინო მაგალითს თუ როგორ მოქმედებს კიბერშეტევა სახელმწიფოზე. კერძოდ, რუსეთის სახელმწიფოს მიერ დაფინანსებულ ჰაკერებს ბრალი დასდეს, რომ მათ მიიტანეს კიბერშეტევა აშშ-ის არჩევნებთან

დაკავშირებულ სხვადასხვა სუბიექტებზე, მათ შორის პოლიტიკურ პარტიებსა და ინდივიდებზე. აღსანიშნავია, რომ დემოკრატიული ეროვნული კომიტეტის (DNC) ელექტრონული ფოსტის სერვერების გატეხვამ მნიშვნელოვანი ყურადღება მიიპყრო. კიბერშეტევების შედეგად გავრცელდა სენსიტიური ინფორმაცია, რამაც გავლენა იქონია არჩევნების დინამიკაზე. აღნიშნულ ქმედებებს დაემატა კოორდინირებული დეზინფორმაციული კამპანიები. კერძოდ, სოციალური მედიის პლატფორმების საშუალებით ტროლების ჯგუფები და ყალბი ანგარიშები ავრცელებდნენ შეცდომაში შემყვან ინფორმაციას, რაც გავლენას ახდენდა საზოგადოებრივ აზრზე (Jamieson, 2018). რა თქმა უნდა, მსგავსი ოპერაციის მიზანი იყო უთანხმოების დათესვა, არსებული პოლიტიკური განხეთქილების გაძლიერება და დემოკრატიული პროცესისადმი ნდობის შელახვა. ეს მაგალითი გვიჩვენებს, თუ როგორ შეიძლება გამოყენებულ იქნას კიბერშეტევები და დეზინფორმაციული კამპანიები პოლიტიკური მიზნების მისაღწევად. ინციდენტმა გამოიწვია დისკუსიები დემოკრატიული პროცესების დაუცველობაზე უცხოური ჩარევის მიმართ, რამაც გააძლიერა გადაწყვეტილების მიმღები პირების მხრიდან ცნობიერების ამაღლების კამპანიები და ძალისხმევა კიბერუსაფრთხოების გასაძლიერებლად, რათა შემდგომ არჩევნებში საზოგადოება დაცული ყოფილიყო ინფორმაციული მანიპულაციისგან.

კიბერუსაფრთხოება მოითხოვს საერთაშორისო თანამშრომლობასა და ნორმების, სტანდარტებისა და სამართლებრივი ჩარჩოების ჩამოყალიბებას. საერთაშორისო ინსტიტუტები, როგორიცაა გაერო, ნატო და ევროკავშირი, მნიშვნელოვან როლს ასრულებენ დიალოგის ხელშეწყობაში, კონსენსუსის ჩამოყალიბებასა და ქვეყნებს შორის თანამშრომლობის გაღვივებაში. ერთობლივ ძალისხმევას შეუძლია გააძლიეროს სახელმწიფოების ღია პოლიტიკა ინფორმაციის გაზიარების, საუკეთესო პრაქტიკის დანერგვისა და კიბერ საფრთხეებზე რეაგირების კოორდინაციის მხრივ, რაც გააძლიერებს გლობალური კიბერუსაფრთხოების მდგრადობას. თუმცა საერთაშორისო კიბერუსაფრთხოების ერთ-ერთი მრავალწლიანი გამოწვევა არის კიბერშეტევების მიკუთვნება. კიბერსივრცის ანონიმური ბუნება და თავდასხმების წარმოშობის შენიღბვის შესაძლებლობა ართულებს იდენტიფიცირებას, რაც აფერხებს ეფექტურ საერთაშორისო რეაგირებას. მაგალითად, 2014 წლის ნოემბერში Sony Pictures Entertainment-ზე მოხდა კიბერშეტევა, რის შედეგადაც გავრცელდა სენსიტიური ინფორმაცია: შიდა ელფოსტის მონაცემები, პირადი მიმოწერები, გამოუქვეყნებელი ფილმები და სხვა. თავდამსხმელებმა, რომლებიც საკუთარ თავს "მშვიდობის მცველებს" უწოდებდნენ, სონისაგან მოითხოვეს წაეშალათ ფილმი "ინტერვიუ" ("The Interview“), სატირული კომედია, რომელიც ასახავს ჩრდილოეთ კორეის ლიდერის გამოგონილ მკვლელობას.

აშშ-ის მთავრობამ, კონკრეტულად კი გამოძიების ფედერალურმა ბიურომ (FBI), საჯაროდ მიაწერა კიბერშეტევა ჩრდილოეთ კორეას და ამტკიცებდა, რომ ეს იყო შურისძიება ფილმის გამო. FBI-იმ მოიყვანა ტექნიკური მტკიცებულებები, მათ შორის პროგრამების ანალიზი მისი ვარაუდის დასამტკიცებლად. თუმცა, გადაგმულმა ნაბიჯებმა გამოიწვია სკეპტიციზმი კიბერუსაფრთხოების ზოგიერთი ექსპერტისა და საგარეო პოლიტიკის ანალიტიკოსების მხრიდან. კრიტიკოსებმა აღნიშნეს, რომ კიბერთავდასხმების იდენტიფიცირება არსებითად რთულია თავდამსხმელების შესაძლებლობის

გამო (Peterson, 2014). ეს მაგალითი ასახავს საერთაშორისო კიბერუსაფრთხოებაში იდენტიფიცირების სირთულეს. თავდამსხმელების საბოლოო ამოცნობასთან დაკავშირებული გამოწვევები ხაზს უსვამს საერთაშორისო თანამშრომლობის გაგრძელებისა და კიბერსივრცეში ნორმებისა და სტანდარტების შემუშავების აუცილებლობას.

რამდენადაც ტექნოლოგიები ვითარდება, კიბერუსაფრთხოების მნიშვნელობა საერთაშორისო ურთიერთობებში არ შეიძლება გადაჭარბებული იყოს. მთავრობებმა, პოლიტიკის შემქმნელებმა და საერთაშორისო ინსტიტუტებმა უნდა მიიღონ ჰოლისტიკური მიდგომა კიბერუსაფრთხოების მიმართ, აღიარონ მისი მრავალმხრივი ზომები. სამართლებრივი ჩარჩოების ადაპტირება, თანამშრომლობის ხელშეწყობა და კიბერუსაფრთხოების შესაძლებლობების გაძლიერება გადამწყვეტი ნაბიჯია ეროვნული ინტერესების დაცვის, ეკონომიკური სტაბილურობის ხელშეწყობისა და ციფრულ ეპოქაში გლობალური უსაფრთხოების შესანარჩუნებლად.

ლიტერატურის მიმოხილვა

კიბერ ომის მნიშვნელოვანი შემთხვევები დაფიქსირდა ყოფილ საბჭოთა რესპუბლიკებში: საქართველოსა და ესტონეთში, რომელიც ინიცირებული იყო რუსეთის მიერ (Goel, 2020). ამ შემთხვევებში, კიბერშეტევები მიზნად ისახავდა სამთავრობო ვებგვერდების, საკომუნიკაციო სისტემებისა და კრიტიკული ინფრასტრუქტურის მწყობრიდან გამოყვანას, არღვევდა სამთავრობო თუ კერძო ოპერაციების სტაბილურობასა და ავრცელებდა დეზინფორმაციას (Vakulyk, 2020). მსგავსი შემთხვევები ცხადყოფს ომის ცვალებად ბუნებას ციფრულ ეპოქაში, სადაც ინფორმაცია და ტექნოლოგია გახდა ძლიერი იარაღი პოლიტიკური და სამხედრო მიზნების მისაღწევად. თანამედროვე საერთაშორისო ურთიერთობებში ინფორმაციული-სამხედრო უსაფრთხოება წარმოიშვა, როგორც სახელმწიფო უსაფრთხოების კრიტიკული კომპონენტი.

კიბერ უსაფრთხოებაზე ყურადღების გამახვილება დაიწყო ესტონეთზე მასშტაბური კიბერ თავდასხმის შემდეგ. 2007 წლის გაზაფხულზე, ესტონეთი, რომელიც ცნობილია თავისი მოწინავე ციფრული ინფრასტრუქტურით, გახდა ჰიბრიდული ომის ბრძოლის ასპარეზი. მასზე განხორციელებული კიბერშეტევა აღიარებულია, როგორც სუვერენულ სახელმწიფოზე ფართომასშტაბიანი კიბერშეტევის პირველი შემთხვევა, რომლის დროსაც სახელმწიფომ აჩვენა არა მხოლოდ თავისი კრიტიკული ინფრასტრუქტურის გამძლეობა, არამედ შექმნა პრეცედენტი გეოპოლიტიკურ კონფლიქტებში კიბერ შესაძლებლობების ინტეგრაციისთვის.

კიბერთავდასხმამდე დაძაბულობა ისტორიული და გეოპოლიტიკური თვალსაზრისით პიკს აღწევდა. ესტონეთმა 1991 წელს მოიპოვა დამოუკიდებლობა და სწრაფად აიტაცა ციფრული ტექნოლოგიები, რითაც მოიპოვა მეტსახელი "e-Estonia" ტექნოლოგიებისადმი მისი ინოვაციური მიდგომის გამო. თუმცა, ამ პროგრესმა გამოიწვია უთანხმოება რუსეთთან, განსაკუთრებით ისტორიულ და პოლიტიკურ ნარატივებთან დაკავშირებით (Jiri, & Valenta, 2018). კიბერშეტევის უშუალო გამომწვევი

მიზეზი იყო საბჭოთა ომის მემორიალის „ტალინის ბრინჯაოს ჯარისკაცის“ გადატანა ქალაქის ცენტრიდან სამხედრო სასაფლაოზე. ამ გადაწყვეტილებამ ესტონეთის რუსულენოვანი უმცირესობის პროტესტი გამოიწვია, რასაც მოჰყვა რუსეთის პასუხი. კიბერშეტევები დაიწყო 2007 წლის აპრილის ბოლოს, რაც დაემთხვა პროტესტის პიკს და აჩვენა ფიზიკური და კიბერ ელემენტების სტრატეგიული შერწყმა. თავდასხმები ძირითადად მოიცავდა Distributed Denial-of-Service (DDoS)-ს შეტევებს, რაც აჭარბებდა ესტონეთის ციფრული ინფრასტრუქტურის შესაძლებლობებს. სამიზნე ობიექტებს წარმოადგენდა სამთავრობო ინსტიტუტები, ფინანსური ორგანიზაციები, მედიასაშუალებები და ინტერნეტ სერვისის პროვაიდერები. თავდამსხმელებმა გამოიყენეს ესტონეთის სისტემების დაუცველობა, რამაც გამოიწვია კრიტიკული ინფრასტრუქტურის შეფერხება. მიუხედავად იმისა, რომ კიბერ სფეროს ატრიბუცია აშკარად რთულია, ესტონეთმა თითი რუსეთზე გაიშვირა, გეოპოლიტიკური კონტექსტისა და ტექნიკური მტკიცებულებების მოტივით. რუსეთმა უარყო მონაწილეობა და ხაზი გაუსვა ინტერნეტის დეცენტრალიზებულ ბუნებას. თუმცა, საერთაშორისო საზოგადოებამ დაგმო თავდასხმები. ინციდენტმა ხელი შეუწყო დისკუსიებს კიბერსივრცეში ნორმებისა და რეგულაციების აუცილებლობის შესახებ. კიბერშეტევებმა დიდი გავლენა მოახდინა ესტონელ საზოგადოებასა და მმართველობაზე. ძირითადი სერვისების შეფერხებამ ხაზი გაუსვა სისუსტეს ციფრულ ინფრასტრუქტურაზე ქვეყნის დამოკიდებულების მხრივ. ინციდენტმა ასევე გამოავლინა თანამედროვე სამყაროს ურთიერთდამოკიდებულება, სადაც ერის ვირტუალური უსაფრთხოება ისეთივე მნიშვნელოვანია, როგორც მისი ფიზიკური დაცვა. მითუმეტეს მაშინ, როცა თავდასხმები აერთიანებდა ფიზიკურ და კიბერ ელემენტებს, რაც ჰიბრიდული ომის სტრატეგიების ერთ-ერთი მთავარი მანიშნებელია. ტრადიციული და კიბერ ტაქტიკის ეს შერწყმა გახდა განმეორებადი თემა შემდგომ გეოპოლიტიკურ კონფლიქტებში. თუმცა ესტონეთი იყო გაკვეთილი მსოფლიოსთვის. მისმა გამოცდილებამ წინა პლანზე გადმოწია კიბერმდგრადობის გადამწყვეტი მნიშვნელობა. ქვეყნებს სჭირდებოდათ ციფრული ინფრასტრუქტურის გაძლიერება განვითარებადი კიბერ საფრთხეების წინააღმდეგ ეფექტური რეაგირებისთვის.

თავდასხმების შემდგომ ესტონეთმა მნიშვნელოვანი ნაბიჯები გადადგა თავისი კიბერთავდაცვისა და საერთაშორისო თანამშრომლობის გასაძლიერებლად. კერძოდ, დიდი ინვესტიცია ჩადო კიბერუსაფრთხოებაში, გააუმჯობესა კიბერ საფრთხეების აღმოჩენისა და პრევენციის სისტემები. კრიტიკული ინფრასტრუქტურის დივერსიფიკაციით ქვეყანამ შეამცირა თავდასხმების შესაძლებლობა. მან ასევე გადამწყვეტი როლი ითამაშა ტალინში ნატოს კოოპერატიული კიბერ თავდაცვის ცენტრის (CCDCOE) დაარსებაში. ეს ცენტრი ფოკუსირებულია კვლევებზე, ტრენინგებსა და კიბერუსაფრთხოების სისტემების გაუმჯობესებაზე. ესტონეთის მიღწევებს დაემატა ეროვნული კიბერ დიაპაზონის შექმნა, რაც გულისხმობს კიბერ საფრთხეების სიმულაციას, რითაც საშუალებას აძლევს სამთავრობო უწყებებს და კერძო პირებს გამოსცადონ თავიანთი მზადყოფნა (Ilves, 2016).

საბოლოოდ, თავდასხმებმა ერები აიძულა გადაეხედათ თავიანთი გეოპოლიტიკური სტრატეგიებისთვის, რამეთუ მათ გააცნობიერეს კიბერუსაფრთხოების მნიშვნელობა ეროვნული ინტერესების დაცვაში. ამასთან დაიწყო ძალისხმევა კიბერსივრცეში სახელმწიფოს პასუხისმგებელი

ქცევის ნორმებისა და წესების შემუშავების მიზნით. 2007 წლის კიბერშეტევები ესტონეთზე გადამწყვეტი ფაქტორი იყო კიბერ ომის ისტორიაში. მყისიერი შეფერხების გარდა, ინციდენტმა გამოიწვია გლობალური დისკუსიები კიბერუსაფრთხოების შესახებ. ციფრული ლანდშაფტის განვითარებასთან ერთად, ესტონეთის გამოცდილებიდან მიღებული გაკვეთილები რჩება გარდამტეხი ქვეყნებისთვის კიბერთავდაცვის სფეროში წარმატების მისაღწევად.

საინტერესოა სხვა პოსტსაბჭოთა ქვეყნების შემთხვევებიც. მაგალითისთვის საქართველოს დამოკიდებულება კიბერუსაფრთხოების სფეროსთან მიმართებით საკმაოდ საინტერესო შედეგების მატრიცას იძლევა. პირველ რიგში იმიტომ, რომ ქვეყნის კრიტიკული ინფრასტრუქტურის წინააღმდეგ გახშირებული კიბერშეტევები ასუსტებს თავდაცვისუნარიანობას და საზოგადოებაში აჩენს დაუცველობის შეგრძნებას. დღესდღეობით მთავარი გამოწვევაა კიბერშპიონაჟი და მასთან დაკავშირებული საფრთხეები, რასაც ემატება მიზანმიმართული შეტევები საბანკო და საფინანსო სექტორზე. საქართველოს წინააღმდეგ პირველი მასობრივი კიბერშეტევა ჯერ კიდევ რუსეთთან ომის დროს მოხდა, რამაც გამოიწვია სამთავრობო და კერძო სექტორების ვებ-გვერდების პარალიზება. მას შემდეგ, ქვეყანა მრავალჯერ გახდა კიბერშეტევის მსხვერპლი. (მაგალითად, 2019 წელს, 2020 წელს ლუგარის ლაბორატორიაზე და ა.შ.), თუმცა 2008 წლის კიბერშეტევამ საქართველოს აჩვენა, რომ ქვეყანაში ეროვნული უსაფრთხოების მიღწევა შეუძლებელია კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე და საზღვაო, საჰაერო თუ სახმელეთო სივრცეების დაცვის პარალელურად აუცილებელია ქვეყანას ჰქონდეს ეფექტური კიბერპოლიტიკა. 2008 წლის აგვისტოს ომის პერიოდში მიზანმიმართული ინფორმაციული ომის შედეგად საქართველო აღმოჩნდა საერთაშორისო ინფორმაციულ ვაკუუმში. სამართლიანობისთვის უნდა აღინიშნოს, რომ ესტონელი კოლეგების დახმარებით მოხდა კიბერშეტევის შეჩერება, რითაც მთლიანი სისტემა გადაურჩა განადგურებას (სვანაძე, 2015). ამასთან საქართველოს წინაშეა ისეთი პრობლემები, როგორიცაა მუდმივი როგორც კიბერჯაშუშური, ისე ფინანსური მოგებით მოტივირებული კიბერკრიმინალების შეტევები, რაც გამოიხატება სხვადასხვა საფრთხის აქტორების მცდელობით მიიღონ სენსიტიურ ინფორმაციაზე არაავტორიზებული წვდომა, ფინანსური სარგებელი და ა.შ. ეს ინციდენტები ხშირად ატარებენ სახელმწიფოს მიერ დაფინანსებული ოპერაციების ნიშნებს.

ქვეყნის მიერ გადადგმულ წარმატებულ ნაბიჯად შეიძლება ჩაითვალოს 2012 წლის ივნისში მიღებული კანონი ,,ინფორმაციული უსაფრთხოების შესახებ“, რომელშიც განსაზღვრულია პრიორიტეტული საფრთხეები. მაგალითად, კიბერშეტევა, რომელიც მიმართულია სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსური და საკუთრების უფლების წინააღმდეგ, საფრთხეს უქმნის ადამიანების სიცოცხლეს, სახელმწიფო ინტერესებს და კრიტიკულ ინფორმაციულ სისტემებს. ასევე მნიშვნელოვანია 2013-2015 და 2017-2018 წლებში მიღებული საქართველოს კიბერუსაფრთხოების სტრატეგია, რომელიც გახლავთ კონცეპტუალური და სტრატეგიული დოკუმენტების მნიშვნელოვანი ნაწილი. მსგავსი პოლიტიკის დოკუმენტების შემუშავებით მოხდა სისტემური უზრუნველყოფის განმტკიცება, მინიმალური სტანდარტების შემოღება და ა.შ. თუმცა მიუხედავად მიღებული კანონებისა პრობლემურია მათი ქმედითუნარიანობა, რეალობაში განხორციელების პერსპექტივები (ჯღარკავა,

2021). საქართველო აქტიურად თანამშრომლობს საერთაშორისო პარტნიორებთან და ორგანიზაციებთან კიბერუსაფრთხოების შესაძლებლობების გასაძლიერებლად. ინფორმაციის გაზიარების ინიციატივებში ჩართვა და ერთობლივ წვრთნებში მონაწილეობა ხელს უწყობს ქვეყნის უნარს მოახდინოს ეფექტური რეაგირება კიბერ საფრთხეებზე. საინტერესოა ის ფაქტიც, რომ კიბერუსაფრთხოების გამოწვევებს საქართველოში უფრო ფართო რეგიონალური გავლენა აქვს. მისი გამოცდილება კიბერ საფრთხეებთან და თავდასხმებთან დაკავშირებით ხაზს უსვამს კიბერუსაფრთხოებასა და გეოპოლიტიკას შორის არსებულ რთულ ურთიერთობას. საქართველო აგრძელებს განვითარებად კიბერ ლანდშაფტში ნავიგაციას, რის გამოც ბევრი გამოწვევაა მის წინაშე.

რაც შეეხება უკრაინას, იგი ხშირად იყო სახელმწიფოს მიერ დაფინანსებული კიბერშეტევების სამიზნე, განსაკუთრებით რუსეთის მხრიდან. ეს თავდასხმები ხშირად ემთხვევა ორ ქვეყანას შორის გამწვავებულ პოლიტიკურ დაძაბულობას. კიბერშეტევების მთავარი სამიზნე ქვეყნის კრიტიკული ინფრასტრუქტურაა, მათ შორის ელექტროენერგიის ქსელები. მაგალითისთვის, 2015 და 2016 წლებში, ქვეყნის მასშტაბით ორჯერ გაითიშა ელექტროენერგია, რაც გამოწვეული იყო კიბერ შეტევებით. ინციდენტის შედეგად ასობით ათასი ადამიანი დაზარალდა, რამაც ხაზი გაუსვა კრიტიკული ინფრასტრუქტურის დაუცველობას კიბერ საფრთხეების მიმართ. (Zetter.2016). კიბერშეტევები ხშირად გამოიყენება როგორც ჰიბრიდული ომის ტაქტიკის ნაწილი, ჩვეულებრივი სამხედრო მოქმედებების პარალელურად. ეს მოიცავს კიბერ, საინფორმაციო და კინეტიკური ზომების ერთობლიობას სტრატეგიული მიზნების მისაღწევად. უკრაინა იყო ერთ-ერთი მთავარი სამიზნე დეზინფორმაციული კამპანიებისა, რომლებიც გამოიყენება პროპაგანდის გასავრცელებლად და საზოგადოებრივ აზრზე ზემოქმედებისთვის. ეს მოიცავს ცრუ ინფორმაციის გავრცელებას პოლიტიკური არეულობისა და კონფლიქტის დროს. აღნიშნულთან დაკავშირებით მთავრობამ ქმედითი ნაბიჯები გადადგა, მაგალითად შეიმუშავა კიბერუსაფრთხოების ეროვნული სტრატეგია კიბერ საფრთხეების წინააღმდეგ რეაგირებისთვის. ეს სტრატეგია მოიცავს საერთაშორისო პარტნიორებთან თანამშრომლობას და მიზნად ისახავს ქვეყნის კიბერუსაფრთხოების შესაძლებლობების გაძლიერებას. უკრაინის მთავრობამ ასევე შემოიღო კანონმდებლობა კიბერუსაფრთხოების ზომების გასაძლიერებლად, კრიტიკული ინფრასტრუქტურის დაცვისა და ინციდენტებზე რეაგირების რეგულაციების ჩათვლით. ამასთან ქვეყანა აქტიურად თანამშრომლობს საერთაშორისო ორგანიზაციებთან და მოკავშირეებთან ციფრული უსაფრთხოების გასაძლიერებლად. ნატოსთან, ევროკავშირთან და სხვა პარტნიორებთან თანამშრომლობა გადამწყვეტია საფრთხის შესახებ ინფორმაციის გაზიარებისა და საუკეთესო პრაქტიკის დანერგვისას (Trope & Hantover, 2017). საინტერესოა ის ფაქტიც, რომ უკრაინა სულ უფრო და უფრო მეტ ინვესტიციებს ახორციელებს კიბერუსაფრთხოების სფეროში მდგრადობის მისაღწევად, რაც მოიცავს არა მხოლოდ ტექნოლოგიურ ზომებს, არამედ კიბერუსაფრთხოების გამოცდილი მუშახელის გადამზადებას და კიბერ ცნობიერების კულტურის ხელშეწყობას. რასაც ემატება ის ფაქტიც, რომ კიბერ საფრთხეების დინამიური ბუნების გათვალისწინებით, უკრაინა აგრძელებს კიბერუსაფრთხოების სტრატეგიის ადაპტირებას ახალი გამოწვევების მოსაგვარებლად. ეს მოიცავს

მოწინააღმდეგეების მიერ გამოყენებული ახალი ტაქტიკების იდენტიფიცირებას. გამომდინარე იქიდან, რომ უკრაინა კიბერუსაფრთხოების მუდმივი გამოწვევების წინაშე დგას, დაფინანსებული კიბერ თავდასხმები, კრიტიკული ინფრასტრუქტურის დაუცველობა და ჰიბრიდული ომის ტაქტიკა მნიშვნელოვან პრობლემას წარმოადგენს. ქვეყანა აქტიურად მუშაობს კიბერუსაფრთხოების შესაძლებლობების გაძლიერებაზე საკანონმდებლო ღონისძიებების, საერთაშორისო თანამშრომლობისა და ყოვლისმომცველი ეროვნული სტრატეგიის მეშვეობით. განვითარებადი საფრთხეებისადმი ადაპტაციის უნარი და საერთაშორისო თანამეგობრობის მხარდაჭერა არის უკრაინის მდგრადი კიბერუსაფრთხოების გარანტი.

თავის მხრივ საინტერესოა ნატოს ძალისხმევა კიბერუსაფრთხოების სფეროში. ნატოსთვის გაკვეთილი იყო 1999 წელს ბალკანებზე განხორციელებული ოპერაცია, რომლის დროსაც ადგილი ჰქონდა ქსელურ შეტევებს. ამ პერიოდიდან მოყოლებული ალიანსისთვის კიბერუსაფრთხოება გახდა ერთ-ერთი პრიორიტეტული საკითხი (Sevim, 2022). ამის მაგალითია, 2002 წელს ალიანსის მიერ შემუშავებული კიბერნეტიკული დაცვის პროგრამა. მათ ასევე შექმნეს ინფორმაციულ ქსელებში ინციდენტებზე რეაგირების ჯგუფი, რომლის ცენტრი ბრიუსელში, ნატო-ს შტაბ ბინაშია განთავსებული (სვანაძე,2015). მთავარ მიღწევად შეიძლება ჩაითვალოს არასანქცირებული შეღწევების აღმოჩენა, საფრთხის წარმოქმნის საწინააღმდეგო ტექნიკური ღონისძიებების დანერგვა და კრიპტოგრაფიული დაცვის ეფექტური მართვის უზრუნველყოფა. ალიანსი ახორციელებს მხარდამჭერ პროგრამებს პარტნიორი და წევრი ქვეყნებისთვის, რომელიც ემსახურება ეფექტური ეროვნული პოლიტიკის დანერგვას და რეაგირების ჯგუფების შექმნას. გამომდინარე იქიდან, რომ ჰიბრიდული ომის მეთოდები საკმაოდ მწვავე პრობლემაა, ალიანსისთვის მნიშვნელოვანია დაიცვას კრიტიკული ინფრასტრუქტურა.

თუმცა, 2007 წელს ესტონეთსა და 2008 წელს საქართველოზე რუსეთის კიბერშეტევების კვალდაკვალ, ნატო აღმოჩნდა ომის ახალი ეპოქის სათავეში. ამ ინციდენტების სიმძიმემ აიძულა ნატოს თავდაცვის მინისტრები ეღიარებინათ კიბერთავდაცვაში გაძლიერებული ძალისხმევის აუცილებლობა (Van Epps, 2013). შემდგომმა სტრატეგიულმა ცვლილებამ ნატოში ხაზი გაუსვა კიბერთავდაცვის ყოვლისმომცველი პოლიტიკის განმტკიცების მნიშვნელობას. 2008 წლის ბუქარესტის სამიტზე წევრმა ქვეყნებმა ერთობლივად აღიარეს ნატოსა და ეროვნულ მთავრობებს შორის თანამშრომლობის გაღრმავების აუცილებლობა კიბერ თავდაცვის სფეროში. ეს იყო გადამწყვეტი მომენტი, რადგან ის დაუპირისპირდა კიბერ საფრთხეების განვითარებად ლანდშაფტს.

2010 წლის ლისაბონის სამიტის დეკლარაციამ აღიარა კიბერშეტევებით გამოწვეული მზარდი საფრთხე და ხაზი გაუსვა ალიანსის საინფორმაციო და საკომუნიკაციო სისტემების ძლიერი დაცვის აუცილებლობას. იმავე წლის სტრატეგიულ კონცეფციაში გაანალიზებული იყო კიბერშეტევების სიხშირე და მათი პოტენციალი ზიანი მიაყენოს მთავრობას, ადმინისტრაციას, ბიზნესს და ეკონომიკას. მიჩნეული იყო, რომ ამ კიბერ საფრთხეებს შეეძლოთ მიეღწიათ იმ დონეებისთვის, რაც საფრთხის შემცველი იქნებოდა ეროვნული და ევროატლანტიკური კეთილდღეობის, უსაფრთხოებისა და

სტაბილურობის უზრუნველყოფისთვის (Lété, & Dege,2017). ამ გამოწვევებზე საპასუხოდ, ნატოს თავდაცვის მინისტრებმა 2011 წელს მხარი დაუჭირეს განახლებულ პოლიტიკას, რომელშიც ასახულია კიბერთავდაცვის ზომები ალიანსის მასშტაბით. შემდგომი ნაბიჯი იყო გაძლიერებული კიბერთავდაცვის პოლიტიკა, რომელიც მიიღეს 2014 წელს, მისი მიზანი იყო ალიანსის კოლექტიური თავდაცვის განუყოფელ კომპონენტად ექცია კიბერთავდაცვა. ეს პოლიტიკა ნატოს ქვეყნებს ანიჭებდა შესაძლებლობას გამოეყენებინათ ჩრდილო ატლანტიკური ხელშეკრულების მე-5 მუხლი კიბერშეტევის საპასუხოდ, რაც მიანიშნებს იმაზე, თუ რა სიმძიმით უყურებდა ნატო საფრთხეებს კიბერ დომენში (Hitchens & Goren, 2017) 2016 წლის ვარშავის სამიტზე ოფიციალურად იქნა აღიარებული კიბერსივრცე, როგორც ოპერაციების მეხუთე სფერო, რითაც მისი სტატუსი გაუთანაბრდა ოპერაციებს ხმელეთზე, ზღვაში, ჰაერსა და კოსმოსში. თუმცა ამ ყველაფერს თავისი გამოწვევებიც აქვს, მაგალითად თუ რა მასშტაბით უნდა განხორციელდეს კოლექტიური თავდაცვა კიბერსივრცეში, შემტევი აქტორების გამოვლენისა და იდენტიფიცირების სირთულე კიდევ უფრო ამძაფრებს პრობლემას. თუმცა ჯეი ში, რომელიც არის ნატოს გენერალური მდივნის თანაშემწე უსაფრთხოების ახალ გამოწვევებში, მხარს უჭერს ინფორმაციის გამჟღავნების გაურკვევლობას პოტენციური აგრესორების შეკავების მიზნით (ILVES, EVANS, CILLUFFO & NADEAU, 2016).

ამასთან ნატოს გენერალური მდივანი იენს სტოლტენბერგი მნიშვნელოვან აქცენტს აკეთებს ტექნოლოგიურ განვითარებაზე, სადაც კიბერსივრცეს მიიჩნევს, როგორც ბრძოლის ახალ ველს. ეს გულისხმობს რესურსებისა და აღჭურვილობის პრიორიტეტიზაციას. ბოლო პერიოდში კი განსაკუთრებით აქტუალური გახდა ხელოვნური ინტელექტის (AI) მნიშვნელობა კიბერთავდაცვაში. სტოლტენბერგი ელის განახლებულ სტრატეგიულ კონცეფციას და აღიარებს, რომ კიბერ საფრთხეები გაიზრდება ახალი ტექნოლოგიების წინსვლასთან ერთად, რაც ფუნდამენტურად შეცვლის ომის ბუნებას (Stoltenberg,2023). ნატო აქტიურად ადაპტირდება ამ რეალობასთან და ემზადება გლობალურ აქტორებთან, როგორიცაა ჩინეთი და რუსეთი წინააღმდეგობის გასაწევად. არსებითად, ნატოს მოქმედებები კიბერ თავდაცვის სფეროში ასახავს დინამიურ პასუხს განვითარებად საფრთხეებზე, ხაზს უსვამს თანამშრომლობას, ტექნოლოგიურ ინოვაციებს და კიბერ დომენის მიერ წარმოდგენილ გამოწვევებს.

მეთოდოლოგია

ნაშრომში ემპირიული დასკვნების გამოსატანად გამოყენებულია თვისებრივი კვლევის მეთოდები. საკითხის სიღრმისეული შესწავლისთვის გამოვიყენეთ ლიტერატურული წყაროების დამუშავების, კოგნიტიური კარტირებისა და კონტენტ-ანალიზის მეთოდი, კერძოდ შემთხვევის ანალიზი. ამასთან პირველადი წყაროები მოვიპოვეთ კიბერუსაფრთხოების დარგის ექსპერტთან ჩაწერილი სიღრმისეული ინტერვიუების საფუძველზე.

წყაროები შეგროვდება შესაბამისი ლიტერატურის, მათ შორის აკადემიური სტატიების, პოლიტიკის ანგარიშებისა და მედია წყაროების სისტემური მიმოხილვით. მიმოხილვა ფოკუსირებული იქნება

ძირითადი თემებისა და ტენდენციების იდენტიფიცირებაზე, რომლებიც დაკავშირებულია კიბერუსაფრთხოების როლზე საერთაშორისო ურთიერთობებში.

შედეგები/ დისკუსია

2007 წელს რუსეთის მიერ ესტონეთის წინააღმდეგ ჩატარებული კიბერთავდასხმების კამპანია იყო გეოპოლიტიკურად ანგაჟირებული ,,სპეცოპერაცია“. თუმცა სხვა სახელმწიფოებისთვის ესტონეთი გახდა ე.წ. გაკვეთილი. დიდწილად სწორედ ესტონეთზე მასობრივი კიბერშეტევის შემდეგ დაიწყო ნატომ ეფექტური ნაბიჯების გადადგმა კიბერთავდაცვის სფეროში. რაც შეეხება, რუსი ჰაკერების მიერ ესტონეთის, საქართველოსა და უკრაინის წინააღმდეგ განხორციელებულ თანმიმდევრულ კიბერშეტევებს, ვფიქრობთ, რომ 2007-2020 წლებში რუსეთმა ისწავლა წინა გამოცდილებებიდან თუ როგორ განევითარებინა კიბერშეტევა და გამოეყენებინა იგი, როგორც პოლიტიკური, ასევე ჩვეულებრივი ომის მხარდასაჭერად. რუსმა სამხედროებმა სამხედრო ოპერაციებთან ინტეგრირებული კიბერ და საინფორმაციო კამპანიები წამოიწყეს, რამაც უარყოფითად იმოქმედა პოსტსაბჭოთა სახელმწიფოებზე. განსაკუთრებით უკრაინაზე, რომელიც ახალი მიდგომების/ სტრატეგიების საცდელი ადგილი გახდა. რუსეთმა უკრაინაში ესკალაცია გაუწია კიბერ კონფლიქტს დესტრუქციული კიბერშეტევების განხორციელებით „ზეკრიტიკულ“ ინფრასტრუქტურაზე (კერძოდ ენერგეტიკისა და ფინანსური სექტორების), რამაც გამოიწვია ფართომასშტაბიანი ეკონომიკური ზიანი და საზოგადოების შეცდომაში შეყვანა/ საზოგადოებრივ აზრზე ზემოქმედება.

რუსეთის კიბეროპერაციული შესაძლებლობები განვითარდა ბოლო ათწლეულის განმავლობაში და ახლა თამაშობს მთავარ როლს სამხედრო სტრატეგიებში, რაც ხელს უწყობს მისი ასიმეტრიული შესაძლებლობების გაზრდას. რუსეთის მთავრობის კიბერ აქტორებმა შეარყიეს დემოკრატიული ინსტიტუტები, მიაყენეს დიდი ეკონომიკური ზარალი და დააზიანეს კრიტიკული ინფრასტრუქტურა მეზობელ ქვეყნებში, დასავლეთ ევროპასა და ჩრდილოეთ ამერიკაში. რუსული APT-ების მიერ გამოყენებული დესტრუქციული მავნე პროგრამები აღმოჩენილია აშშ-ს ენერგეტიკული ქსელის ადმინისტრაციულ და ბიზნეს ქსელებში.

თუმცა საპასუხოდ, ნატომ განავითარა კიბერთავდაცვის სისტემები და მექანიზმები, შექმნა მუდმივმოქმედი საკოორდინაციო ჯგუფი, რაც უზრუნველყოფს მსგავსი შემთხვევების პრევენციას. ყოფილი პოსტსაბჭოთა სახელმწიფოები, მათი განვითარების დონიდან გამომდინარე, მოწყვლადები არიან მსგავსი შეტევების მიმართ რის გამოც აუცილებელია საერთაშორისო თანამშრომლობა და მასში დიდ როლს თამაშობს ნატოს ჩართულობა.

ბიბლიოგრაფია:

1. Hitchens, T., & Goren, N. (2017). International Cybersecurity Information Sharing Agreements. Center for International & Security Studies, U. Maryland. http://www.jstor.org/stable/resrep20426
2. https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
3. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/ (Last seen: 19/01/2024)
4. ILVES, L. K., EVANS, T. J., CILLUFFO, F. J., & NADEAU, A. A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. PRISM, 6(2), 126–141. http://www.jstor.org/stable/26470452
5. Ilves, T. H. (2016). The Consequences of Cyber Attacks. Journal of International Affairs, 70(1), 175–181. https://www.jstor.org/stable/90012601
6. Jamieson, K. H. (2018). The 2016 U.S. Election: Can Democracy Survive the Internet? American Behavioral Scientist, 62(3), March 2018.
7. Jiri, & Valenta, L. F. (2018). 2007: Russia's Cyber War in Estonia. In Russia's Strategic Advantage in the Baltics: A Challenge to NATO? (pp. 24–27). Begin-Sadat Center for Strategic Studies. http://www.jstor.org/stable/resrep16828.19
8. Khoroshko, V., Hryshchuk, R., Brailovskyi, N., Kapustian, M. (2023) Information-Military Security is a Component of State Security. Scientific and Practical Cyber Security Journal (SPCSJ), 7(1), 1-10. ISSN 2587-4667. https://journal.scsa.ge/wp-content/uploads/2023/04/1information-military-security-is-a-component-of-state-security.pdf
9. Kramer, L, (2023), United States: Cybersecurity In The Boardroom: 'Caremark' Liability For Boards' Failure To Oversee Cybersecurity, Mondac https://www.kramerlevin.com/en/perspectives-search/cybersecurity-in-the-boardroom-caremark-liability-for-boards-failure-to-oversee-cybersecurity.html?utm_source=mondaq&utm_medium=syndication&utm_term=Technology&utm_content=articleoriginal&utm_campaign=article
10. Lété, B., & Dege, D. (2017). NATO Cybersecurity: A Roadmap to Resilience. German Marshall Fund of the United States. http://www.jstor.org/stable/resrep18857
11. Ottis, R., Solvak, M., & Ress, K. (2009). The Cyber Attacks on Estonia in 2007: Lessons Learned and Future Prospects. International Journal of Critical Infrastructure Protection, 2(3–4),
12. Pernik, P., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Limnell, J., Pawlak, P., Reinhold, T., Reshetnikov, A., Soldatov, A., & Vilmer, J.-B. J. (2018). The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. In N. Popescu & S. Secrieru (Eds.), HACKS, LEAKS AND DISRUPTIONS: RUSSIAN CYBER STRATEGIES (pp. 53–64). European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21140.9

13. Perwej et al., December 2021, International Journal of Scientific Research and Management (IJSRM) Volume 9(Issue 12): Pages 669 – 710, DOI:10.18535/ijsrm/v9i12.ec04
14. Peterson, A. (2014, December 18). The Sony Pictures hack, explained. The Washington Post. Retrieved from
15. Sevim, H. O, (2022, October 20), A Political Perspective on the Increasing Cyber Attacks in the Balkan Countries, https://www.ankasam.org/a-political-perspective-on-the-increasing-cyber-attacks-in-the-balkan-countries/?lang=en
16. Trope, R. L., & Hantover, L. L. (2017). Reckoning with the Hacker Age: Cybersecurity Developments. The Business Lawyer, 73(1), 227–238. https://www.jstor.org/stable/26419201
17. Vakulyk, Olga & Petrenko, Pavlo & Kuzmenko, Iulia & Pochtovyi, Maksym & Orlovskyi, Ruslan. (2020). CYBERSECURITY AS A COMPONENT OF THE NATIONAL SECURITY OF THE STATE. Journal of Security and Sustainability Issues. 9. 775-784. 10.9770/jssi.2020.9.3(4)
18. Van Epps, G. (2013). Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain. *Connections*, *12*(4), 15–50. http://www.jstor.org/stable/26326340
19. Zetter, K. (2016, March 3), Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, WIRED, retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
20. გოცირიძე, ა. (2019) რუსული დესტრუქციული კიბეროპერაციებისგან თავდაცვის ძირითადი სტრატეგიული მიმართულებები, საქართველოს სტატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
21. კირკიტაძე, მ.(2020) სამხედრო კიბეროპერაციები, როგორც რუსეთის იარაღი ევროპის ქვეყნებში პოლიტიკური დღის წესრიგის შესაცვლელად, საქართველოს სტატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
22. სვანაძე, ვ. (2015), კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები, GIPA, https://gipa.ge/uploads/files/Cyber_Protection.pdf
23. საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ" ხელმისაწვდომია https://matsne.gov.ge/ka/document/view/1679424?publication=7