კიბერშეტევის საერთაშორისო სამართლებრივი განსაზღვრება

ხათუნა ბურკაძე
ბიზნესისა და ტექნოლოგიების უნივერსიტეტი, პროფესორი

რეფერატი. საინფორმაციო და საკომუნიკაციო ტექნოლოგიების ერაში კომპიუტერული ქსელების გამოყენებით შესაძლებელია ომის თანამედროვე ფორმით წარმოება. მზარდი ტექნოლოგიური მიღწევების შედეგად კიბერთავდასხმის სახეები უფრო იხვეწება და იკარგება კონტროლი ინფორმაციული ტექნოლოგიების ინფრასტრუქტურაზე. სახელმწიფოებს ციფრული ინსტრუმენტების მეშვეობითა და ჰაკერთა ჯგუფების დახმარებით შეუძლიათ სხვა სახელმწიფოების წინააღმდეგ განახორციელონ კიბერშეტევები. აღნიშნული დესტრუქციული მოქმედებები ზიანს აყენებენ ქვეყნის თავდაცვისუნარიანობას, უსაფრთხოებას, სტაბილურობას, ეკონომიკურ მდგრადობას და აფერხებენ როგორც საჯარო, ასევე კერძო ორგანიზაციების ფუნქციონირებას. ამ მოცემულობას კიდევ უფრო მეტად ართულებს საერთაშორისო აქტორებს შორის შეუთანხმებლობა კიბერშეტევის განმარტებასთან დაკავშირებით. მით უფრო იმ ფონზე, რომ დღეს მოქმედი საერთაშორისო სამართლებრივი ნორმები უშუალოდ არ ეხება კიბერთავდასხმების საკითხების რეგულირებას. გაერთიანებული ერების ორგანიზაციის წესდება გასულ საუკუნეში მიიღეს, როდესაც დოკუმენტის ავტორები ვერ განჭვრეტდნენ კიბერსივრცის შექმნის პროცესს. შესაბამისად, სტატიის მიზანია კიბერშეტევის სამართლებრივი დეფინიციის კვლევა მოქმედი საერთაშორისო ნორმების ხელახალი განმარტების საფუძველზე. ეს კი მნიშვნელოვანია იმისათვის, რომ განისაზღვროს კიბერსივრცეში ახალი ნორმების განვითარებისა და მიღების შესაძლებლობები და განიმარტოს სახელმწიფოს პასუხისმგებლიანი კიბერქცევა.

საკვანძო სიტყვები: კიბერშეტევა, ძალის გამოყენება, შეიარაღებული თავდასხმა

შესავალი

კიბერშეტევა, როგორც თავდასხმის ახალი კატეგორია განსხვავდება ტრადიციული საომარი მოქმედებებისგან. კიბერშეტევები, მათგან განსხვავებით, შეიძლება განხორციელდეს მშვიდობიან პერიოდშიც. ამასთანავე, კიბერშეტევების მეშვეობით მიზანი მიიღწევა არა იარაღის, არამედ კომპიუტერული ქსელების გამოყენებითა და სისტემაში უნებართვოდ შეღწევით, მონაცემების დაზიანებით, განადგურებით ან მანიპულირებით. ასევე, კიბერსივრციდან მომდინარე საფრთხე არ არის შეზღუდული კონკრეტული პოლიტიკური და

გეოგრაფიული საზღვრებით[1]. ეს კი კიბერთავდასხმის ინიციატორსა და შემსრულებელს აძლევს შესაძლებლობას ანონიმურად დარჩეს. მოწინააღმდეგის იდენტიფიცირების სირთულე თავდამსხმელ სახელმწიფოს მსხვერპლი სახელმწიფოს წინააღმდეგ მეტი დამაზიანებელი მოქმედებების განხორციელებისათვის სივრცეს უტოვებს, რაც ართულებს დროულად აგრესორის გამოვლენასა და სათანადო რეაგირებას.

2007 წელს ესტონეთისა და 2008 წელს საქართველოს წინააღმდეგ განხორციელებულმა კიბერშეტევებმა თვალსაჩინო გახადა კიბერთავდაცვითი შესაძლებლობების განვითარების აუცილებლობა. ესტონეთისგან განსხვავებით 2008 წლის აგვისტოში რუსეთის ფედერაციამ საქართველოს წინააღმდეგ კიბერშეტევები ტრადიციული საომარი მოქმედებების პარალელურად განახორციელა. კიბერგამოწვევების წინაშე საქართველო დგას დღემდე, განსაკუთრებით უნდა გამოვყოთ 2019 წლის 28 ოქტომბერს რუსეთის მიერ საქართველოს წინააღმდეგ განხორციელებული ფართომასშტაბიანი კიბერშეტევა, რომელიც გულისხმობდა საქართველოს კრიტიკული ინფრასტრუქტურისათვის ზიანის მიყენებას კვლავ. საბოლოო ჯამში, აღნიშნული კიბერშეტევის მიზანი იყო საქართველოს ეროვნული უსაფრთხოების ხელყოფა, საზოგადოებაში მღელვარების დათესვა და საქართველოს მოსახლეობისთვის ზიანის მიყენება სხვადასხვა ორგანიზაციის, მათ შორის სახელისუფლებო სტრუქტურების ფუნქციონირების შეფერხებით.

შეიძლება ითქვას, რომ საინფორმაციო ტექნოლოგიების ერაში სახელმწიფოთა ეროვნული უსაფრთხოების პოლიტიკა ფოკუსირებულია კიბერსივრცეში საკუთარი ინტერესების დაცვაზე. რადგან კიბერსივრცე არ არის შემოფარგლული კონკრეტული საზღვრებით, ეს მის თანმდევ გამოწვევებს მასშტაბურ ხასიათს სძენს. კიბერშეტევების ბუნება მოითხოვს, მოქმედი საერთაშორისო სამართლებრივი ჩარჩოს ანალიზის შედეგად, იმ ტენდენციების გამოკვეთას, რომელთა გათვალისწინებით სახელმწიფოები შეძლებენ აღნიშნულ თავდასხმებზე ეფექტიან რეაგირებას და სახელმწიფო ინტერესების დაცვას. ამ ტიპის პრეცედენტებს პრევენციული მნიშვნელობაც ექნებათ კიბერშეტევების შესამცირებლად. საკითხის აქტუალობას განაპირობებს ისიც, რომ არ არსებობს საერთაშორისო ხელშეკრულება, რომელიც უშუალოდ დაარეგულირებს კიბერშეტევებისა და კიბერომის საერთაშორისო სამართლებრივ საკითხებს. ერთადერთი საერთაშორისო სამართლებრივი დოკუმენტია ევროსაბჭოს ფარგლებში მიღებული კონვენცია „კიბერდანაშაულის შესახებ“[2]. თუმცა ეს კონვენცია კიბერსივრცეში მომხდარ დარღვევებს განიხილავს სისხლის სამართლის კონტექსტში და იგი არ ეხება კიბერშეტევებს, როგორც ომის წარმოების ერთ-ერთ ფორმას.

1. *Michael Schmitt,* „Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework“, 37 Columbia Journal of Transnational Law, (1998-1999), 888.

2. Convention on Cybercrime, Budapest, 23.XI.2001, Council of Europe, https://rm.coe.int/1680081561 (Accessed April 23, 2022).

კიბერშეტევების კონტექსტში საერთაშორისო სამართალში ძალის გამოყენების დეფინიცია

ციფრულ ეპოქაში იმის საკვლევად, თუ რამდენად შეიძლება კიბერშეტევა ძალის გამოყენებას უტოლდებოდეს, მნიშვნელოვანია ძალის გამოყენების ცნების ძირითად ელემენტებში გარკვევა. საერთაშორისო მშვიდობისა და უსაფრთხოების უზრუნველსაყოფად სახელმწიფოები შეთანხმდნენ უარი ეთქვათ ძალის გამოყენების მონოპოლიზაციისგან და მისი გამოყენება დაეშვათ მხოლოდ გამონაკლის შემთხვევებში.

ძალის გამოყენების თანამედროვე საერთაშორისო სამართლებრივი განმარტება ეფუძნება გაერთიანებული ერების ორგანიზაციის წესდებას. დოკუმენტის ავტორებს სურდათ აეკრძალათ ძალის გამოყენება, თუმცა, იმავდროულად, გაითვალისწინეს გარკვეული გამონაკლისი შემთხვევები.

გაეროს შექმნის ერთ-ერთი მიზანი იყო მე-20 საუკუნეში საერთაშორისო სამართლის მოდერნიზება. ლიდერებმა გადაწყვიტეს შეექმნათ ისეთი სისტემა, რომელიც დაეფუძნებოდა საერთაშორისო ხელშეკრულებებით ნაკისრი ვალდებულებების პატივისცემას და საერთაშორისო ნორმების დაცვას[3]. მათი თვალთახედვით, ეს აუცილებელი იყო მომავალი თაობების ახალი მსოფლიო ომისგან დასაცავად.

ძალის გამოყენებისა და კონფლიქტის თანამედროვე სამართლებრივი რეგულირება იწყება გაეროს წესდებით და განსაკუთრებით ამ წესდების მე-2 მუხლის მე-4 პუნქტით[4], რომლის თანახმად, გაერთიანებული ერების ორგანიზაციის ყველა წევრი სახელმწიფო თავს იკავებს საერთაშორისო ურთიერთობებში მუქარის ან ძალის გამოყენებისაგან ნებისმიერი სახელმწიფოს ტერიტორიული მთლიანობის და პოლიტიკური დამოუკიდებლობის წინააღმდეგ, ან ნებისმიერი სხვა ფორმით, რომელიც ეწინააღმდეგება გაეროს მიზნებს[5].

გაეროს წესდების მე-2 მუხლის მე-4 პუნქტის ფორმულირებიდან ჩანს, რომ დოკუმენტის ავტორებმა ომის ნაცვლად უფრო ფართო ტერმინი ძალის გამოყენება აირჩიეს. ომი კონკრეტულ ვითარებაზე მიუთითებს, რომელიც, როგორც წესი, ომის გამოცხადებით იწყება და ზავის დადებით მთავრდება. ომის ზოგადად აკრძალვის პირობებში სახელმწიფოები ამ ტერმინის ნაცვლად იყენებდნენ სხვა ტერმინებს, მათ შორის სამხედრო ოპერაციას, რათა შეექმნათ აღქმა იმისა, რომ ომის ამკრძალავ ნორმებს არ არღვევდნენ. შესაბამისად, საერთაშორისო პრაქტიკის გათვალისწინებით აუცილებელი იყო განზოგადებუ-

3. Charter of the United Nations, http://wwwupdate.un.org/en/documents/charter/intro.shtml (Accessed April 23, 2022).

4. *Matthew C. Waxman,* „Cyber Attacks as Force under UN Charter Article 2(4)“, 87 International Law Studies Series, US Naval War College, 44 (2011).

5. See supra note 3.

ლი ცნების დამკვიდრება. ამდენად, ძალის გამოყენების ტერმინი აერთიანებს ყველა ძალისმიერ მოქმედებას, დაწყებული ტრადიციული ომით და დამთავრებული სასაზღვრო ინციდენტით. დღეს ძალის გამოყენების აკრძალვის წესი არ არის დამოკიდებული იმაზე, თუ სახელმწიფო რა ტიპის სახელწოდებას მიანიჭებს უპირატესობას სამხედრო კონფლიქტის დროს მის მიერ განხორციელებული დესტრუქციული მოქმედებების გამოსახატად[6]. მეტიც, გაეროს მართლმსაჯულების საერთაშორისო სასამართლომ „ნიკარაგუას საქმეში“ უარი თქვა ძალის გამოყენების ვიწრო ინტერპრეტაციაზე. კერძოდ, მართლმსაჯულების საერთაშორისო სასამართლომ დაადგინა, რომ სახელმწიფოს მიერ პარტიზანული ძალების შეიარაღება და გაწვრთნა სხვა სახელმწიფოს წინააღმდეგ ძალისმიერ მოქმედებებში ჩასართავად ნიშნავს ძალის გამოყენებას[7].

ამასთანავე, უნდა აღინიშნოს, რომ ნებისმიერი არამეგობრული მოქმედება არ აღწევს ძალის გამოყენების ზღურბლს. მეორე მხრივ, „ნიკარაგუას საქმეში“ გაეროს მართლმსაჯულების სასამართლომ მიუთითა, რომ პარტიზანული ძალების დაფინანსება არ წარმოადგენს იმ ტიპის მოქმედებას, რომელიც უთანაბრდება ძალის გამოყენებას. ეს კი იმას ნიშნავს, რომ კიბეროპერაციების განმახორციელებელი ჯგუფების დაფინანსება არ შეიძლება ჩაითვალოს ძალის გამოყენებად[8]. ასევე, აღსანიშნავია, რომ გაეროს წესდების ავტორებმა უარი თქვეს ძალის გამოყენების ცნებაში ეკონომიკური იძულების ზომების მოაზრებაზე. შესაბამისად, კიბეროპერაცია, რომელიც მიზნად ისახავს სხვა სახელმწიფოზე ეკონომიკურ ზემოქმედებას, ვერ აღწევს ძალის გამოყენების ზღურბლს[9].

როგორც კიბერსივრცეში, ასევე მის ფარგლებს გარეთ ამა თუ იმ მოქმედების ძალის გამოყენებად მიჩნევისათვის საჭიროა ისეთი ფაქტორების გათვალისწინება, როგორებიცაა: ღონისძიების კონტექსტი; სუბიექტი, რომელმაც დაგეგმა მოქმედება; სამიზნე; მდებარეობა; განზრახვა და შედეგი[10]. ამ ფაქტობრივი გარემოებების მხედველობაში მიღების საფუძველზე, თუ კიბერშეტევამ მიაღწია ძალისმიერი მოქმედების იმ დონეს, რომელიც უთანაბრდება ძალის გამოყენებას, შესაძლოა ითქვას, რომ გაეროს წესდების მე-2 მუხლის მე-4 პუნქტი ვრცელდება კიბერსივრცეზე. მით უფრო, რომ აღნიშნული დოკუმენტი არ გვთავაზობს ძალის გამოყენების დეფინიციას. საერთაშორისო პრაქტიკის ანალიზი კი მიანიშნებს, რომ ძალის გამოყენება არ შემოიფარგლება მხოლოდ ერთი ტიპის ძალისმიერი მეთოდებით და აერთიანებს კინეტიკურ, არაკინეტიკურ, რეგულარულ, არარეგულარულ საშუალებებს. კიბერძალის გა-

6. *René Värk,* „The Use of Force in the Modern World: Recent Developments and Legal Regulation of the Use of Force“, 2 Baltic Defense Review, 29-30 (2003).

7. *Michael N. Schmitt,* „The Law of Cyber Warfare: Quo Vadis?“, 25 Stanford Law & Policy Review, (Spring, 2014), 279, 280.

8. Id., 280.

9. Id.

10. *Antonia Chayes,* „Rethinking Warfare: The Ambiguity of Cyber Attacks“, 6 Harvard National Security Journal, (2015), 507.

მოყენება კი რა შემთხვევაში ჩაითვლება კანონიერად ან კანონგარეშედ ეს დამოკიდებულია იმაზე, თუ როგორ განვმარტავთ მოქმედ საერთაშორისო ნორმებს, რომლებიც ძალის გამოყენების გამონაკლისი შემთხვევების ფარგლებს ადგენენ.

ძალის გამოყენების საერთაშორისო სამართლებრივი რეგულირება გაეროს წესდებისა და ჩრდილოატლანტიკური ხელშეკრულების მიხედვით

გაეროს წესდება, რომელიც განსაზღვრავს სახელმწიფოთა ურთიერთობების მთავარ წესებს, და ჩრდილოატლანტიკური ხელშეკრულება, ნატოს სადამფუძნებლო დოკუმენტი, მიიღეს 1945 და 1949 წლებში. იმ პერიოდში გლობალური და რეგიონალური სისტემების მიერ კიბერსივრცის საკითხების გათვალისწინება, ბუნებრივია, ვერ მოხდებოდა, რადგან ის მომავლის საკითხს წარმოადგენდა. მიუხედავად ამისა, მზარდი კიბერშეტევების ფონზე, მოქმედი საერთაშორისო სამართლებრივი ნორმების განმარტების აუცილებლობა დადგა დღის წესრიგში, რათა სახელმწიფოებმა სათანადოდ შეძლონ ციფრულ რეალობასთან ადაპტირება. ამ თვალსაზრისით 2013 წელს გაეროს სამთავრობო ექსპერტთა ჯგუფმა გამოაქვეყნა მისი მესამე ანგარიში, რომლის თანახმად გაეროს წესდება ციფრულ სივრცეზე ვრცელდება[11].

რაც შეეხება ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის პოზიციას საერთაშორისო სამართლისა და კიბერსივრცის ურთიერთმიმართების შესახებ, 2014 წლის 4-5 სექტემბერს გამართულ უელსის სამიტზე მიღებული დეკლარაციის მიხედვით, ალიანსის წევრი ქვეყნები შეთანხმდნენ, რომ მოქმედი საერთაშორისო სამართალი, მათ შორის გაეროს წესდება და საერთაშორისო ჰუმანიტარული სამართალი, გამოიყენება კიბერსივრცეში. მათი თვალთახედვით, კიბერშეტევას შეუძლია მიაღწიოს ისეთ ზღურბლს, რომლითაც საფრთხეს შეუქმნის ეროვნულ და ევროატლანტიკურ უსაფრთხოებას. ის იწვევს ისეთივე დესტრუქციულ შედეგებს თანამედროვე საზოგადოებებისათვის, როგორც კონვენციური შეტევები. შესაბამისად, ნატოს ლიდერები თანხმდებიან, რომ კიბერთავდაცვა წარმოადგენს მათი კოლექტიური თავდაცვის მნიშვნელოვან კომპონენტს[12]. მეტიც, უელსის სამიტის დეკლარაციის მიღებამდე ნატოს კიბერთავდაცვის ცენტრმა ესტონეთში 2009 წელს დაიწყო საერთაშორისო კვლევითი პროექტის განხორციელება. პროექტის მიზანი იყო მოქმედი საერთაშორისო ნორმების საფუძველზე კიბერშეტევებთან და კიბე-

11. Back to Square One? The NATO Cooperative Cyber Defense Center of Excellence, https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html (Accessed April 26, 2022).

12. The Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 4-5, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (Accessed April 26, 2022).

როპერაციებთან დაკავშირებული საკითხების ანალიზი. 2013 და 2017 წლებში გამოცემული ტალინის სახელმძღვანელოები[13] ეხება საერთაშორისო ექსპერტების ხედვას იმის თაობაზე, თუ როგორ უნდა გამოიყენონ სახელმწიფოებმა მოქმედი ნორმები კიბერსივრცეში.

გაეროს წესდების თანახმად, უშიშროების საბჭო პასუხისმგებელია საერთაშორისო მშვიდობისა და უსაფრთხოების დაცვაზე. ეს მანდატი მას აძლევს დისკრეციულ უფლებამოსილებას, განსაზღვროს რა ტიპის მოქმედებები უქმნიან საფრთხეს საერთაშორისო მშვიდობას. საერთაშორისო მშვიდობისათვის საფრთხის შექმნის ან მისი ხელყოფის შემთხვევებში უშიშროების საბჭო, როგორც წესი, იღებს გადაწყვეტილებებს იმ ზომების მიღების შესახებ, რომლებიც აუცილებელია მშვიდობის უზრუნველსაყოფად. ამ ღონისძიებებს შორის მოიაზრება საფრთხის შემქმნელ, აგრესორ სახელმწიფოსთან ეკონომიკური ურთიერთობების სრულად ან ნაწილობრივ გაწყვეტა, სარკინიგზო, საზღვაო, საჰაერო, საფოსტო და სხვა სახის კომუნიკაციისა და დიპლომატიური ურთიერთობების შეწყვეტა[14]. თუ უშიშროების საბჭო მიიჩნევს, რომ აღნიშნული ზომები არ არის საკმარისი მშვიდობის დასაცავად, გაეროს წესდების 42-ე მუხლის თანახმად, მას შეუძლია გაეროს წევრ სახელმწიფოებს მიუთითოს საჰაერო, საზღვაო და სახმელეთო ძალების გამოყენებისაკენ[15]. საერთაშორისო ექსპერტთა ჯგუფის აზრით, ნებისმიერი მოქმედება, რომელიც აღნიშნული წესის გათვალისწინებით ხორციელდება, შეიძლება გულისხმობდეს კიბერშესაძლებლობების გამოყენებას, ან მათ წინააღმდეგ იყოს მიმართული[16]. კოლექტიური უსაფრთხოების ოპერაციაში შეიძლება ჩაერთოს გაეროს ყველა წევრი ან გარკვეული ნაწილი უშიშროების საბჭოს მიერ მიღებული გადაწყვეტილების შესაბამისად. ამდენად, საერთაშორისო მშვიდობისათვის საფრთხის შექმნა ან მისი ხელყოფა წარმოადგენს იმ გამონაკლის შემთხვევებს, რომელთა დროსაც, აუცილებლობიდან გამომდინარე, უშიშროების საბჭოს გადაწყვეტილების საფუძველზე, სახელმწიფოებს შეუძლიათ გამოიყენონ ძალა მშვიდობისა და უსაფრთხოების უზრუნველსაყოფად.

გაეროს წესდების 51-ე მუხლი კი ძალის გამოყენების მეორე გამონაკლის შემთხვევას ეხება. აღნიშნული მუხლის მიხედვით, გაეროს წევრ სახელმწიფოს აქვს ინდივიდუალური ან კოლექტიური თავდაცვის უფლება მის წინააღმდეგ განხორციელებული შეიარაღებული თავდასხმის შემთხვევაში, ვიდრე უშიშროების საბჭო არ მიიღებს ზომებს საერთაშორისო მშვიდობისა

13. The Tallinn Manual, The NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/research/tallinn-manual/(Accessed April 26, 2022).

14. See supra note 3, 5.

15. Id.

16. *Tallinn Manual* 1.0 on the International Law Applicable to Cyber Warfare, (Michael N. Schmitt, ed.), Cambridge University Press, (2013), 71.

და უსაფრთხოების დასაცავად[17]. საერთაშორისო ჩვეულებითი სამართლის თანახმად, შეიარაღებულ თავდასხმაზე პასუხი უნდა იყოს აუცილებელი და პროპორციული[18]. ამასთანავე, არსებობს მესამე კრიტერიუმიც, რაც გულისხმობს რეაგირების დროულობას, ანუ ისეთი ვითარების არსებობას, როდესაც მყისიერი მოქმედება გარდაუვალია[19]. პროპორციულობა კი ნიშნავს თანაბარზომირიების პრინციპის დაცვით შეტევის მოგერიებას, ანუ სახელმწიფომ არ უნდა გამოიყენოს იმაზე მეტი ძალა, რაც სჭირდება მიზნის მისაღწევად[20]. რაც შეეხება აუცილებლობის კრიტერიუმის დაცვას, ის სახელმწიფოსგან მოითხოვს იმის დემონსტრირებას, რომ მან თავდასხმის, მათ შორის კიბერშეტევის შესაკავებლად მიმართა ყველა მშვიდობიან ფორმას პოლიტიკური, დიპლომატიური, ეკონომიკური და სხვა ინსტრუმენტების გამოყენებით, თუმცა ვერ მიაღწია მიზანს და ძალის გამოყენება რჩება ერთადერთ საშუალებად თავდასხმის შესაჩერებლად. ამდენად, კიბერშეტევის წინააღმდეგ განხორციელებული თავდაცვითი ოპერაცია აუცილებლობის, პროპორციულობისა და დროულობის კრიტერიუმებთან შესაბამისობაში უნდა იყოს.

რაც შეეხება კოლექტიურ თავდაცვას, ამ თვალსაზრისით მნიშვნელოვანია ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის მე-5 მუხლის განხილვა. მე-5 მუხლის მიხედვით, ნატოს წევრი ქვეყნები თანხმდებიან, რომ თავდასხმა ალიანსის ერთი ან მეტი წევრი სახელმწიფოს წინააღმდეგ განიხილება თავდასხმად ყველა მათგანზე[21]. ნატოს უელსის სამიტის დეკლარაციის თანახმად, ჩრდილოატლანტიკური საბჭო კიბერშეტევების განხორციელებისას მე-5 მუხლის გამოყენების შესახებ გადაწყვეტილებას მიიღებს ცალკეული შემთხვევის ანალიზის საფუძველზე[22]. ერთი მხრივ, ეს ნიშნავს იმას, რომ ძალის გამოყენების გამონაკლის შემთხვევებთან დაკავშირებული საერთაშორისო სამართლებრივი ნორმები ვრცელდება კიბერშეტევებზე. მეორე მხრივ კი, არ არის მკაფიოდ განსაზღვრული, თუ რა შემთხვევებში შეიძლება მე-5 მუხლის ამოქმედება კიბერშეტევების შესაჩერებლად და ეს დამოკიდებულია ცალკეული ფაქტობრივი გარემოებების იმ ერთობლიობაზე, რომლებიც ლიდერებს დაარწმუნებენ კოლექტიური თავდაცვითი ოპერაციის განხორციელების საჭიროებაში. ამავდროულად, უნდა იყოს გათვალისწინებული გაეროს წესდების 51-ე მუხლითა და საერთაშორისო ჩვეულებითი სამართლით დადგენილი ფარგლები ძალის გამოყენებისას.

ძალის გამოყენების საერთაშორისო სამართლებრივი რეგულირების ანალი-

17. See supra note 3, 5, 14.

18. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. the United States of America), 1986, http://www.icj-cij.org/docket/ index.php (Accessed April 28, 2022).

19. *Michael N. Schmitt*, Preemptive Strategies in International Law, Michigan Journal of International Law, (2003), 55.

20. Id.

21. Founding Treaty – the North Atlantic Treaty, April 4, 1949, https://www.nato.int/cps/en/natohq/topics_67656.htm (Accessed April 29, 2022).

22. See supra note 12.

ზის შედეგად, შეიძლება ითქვას, რომ კიბერძალის გამოყენება ჩაითვლება უკანონოდ, თუ მისი გამოყენება არ შეესაბამება მოქმედი საერთაშორისო სამართლით დადგენილ გამონაკლის შემთხვევებსა და კრიტერიუმებს. კერძოდ, კიბეროპერაციის განხორციელება შესაძლებელია ინდივიდუალური და კოლექტიური თავდაცვის ფარგლებში და უშიშროების საბჭოს მიერ მშვიდობისათვის საფრთხის შექმნის ან ხელყოფის დროს მიღებული გადაწყვეტილებების საფუძველზე, კოლექტიური უსაფრთხოების უზრუნველყოფის ზომების განხორციელებისას.

კიბერშეტევის, როგორც თავდასხმის ახალი სახის განმარტება

ძალის გამოყენების გამონაკლისი შემთხვევების საერთაშორისო სამართლებრივი ფარგლების ანალიზის შედეგად უნდა ითქვას, რომ ინდივიდუალური ან კოლექტიური თავდაცვის უფლების გამოყენების საერთაშორისო სამართლებრივი საფუძველია შეიარაღებული თავდასხმა. მკვლევრები თანხმდებიან, რომ ამ კონტექსტში შეიარაღებული თავდასხმა გულისხმობს აქტიურ მოქმედებას, ვიდრე ასეთი მოქმედების განხორციელების საფრთხეს[23].

მიუხედავად იმისა, რომ გაეროს წესდების 51-ე მუხლი განსაზღვრავს თავდაცვითი უფლების განხორციელების საფუძველს, ის არ განმარტავს შეიარაღებულ თავდასხმას. დოკუმენტი არ ეხება იმ კრიტერიუმების დადგენას, რომლის დროსაც მოქმედება თავდასხმის ზღურბლს აღწევს. 2013 წლის ტალინის სახელმძღვანელოს ავტორების – საერთაშორისო ექსპერტთა ჯგუფის ინტერპრეტაციით შეტევის შეიარაღებულ თავდასხმად მიჩნევის კრიტიკული ელემენტია აღნიშნული მოქმედების გავლენის მასშტაბი. ტალინის სახელმძღვანელოს მე-13 წესი სახელწოდებით: „თავდაცვა შეიარაღებული თავდასხმის წინააღმდეგ“ მიუთითებს, რომ სახელმწიფო, რომელიც გახდა სამიზნე შეიარაღებული თავდასხმის ტოლფასი კიბეროპერაციისა, აქვს თავდაცვის უფლება. პრაქტიკაში შეტევის მასშტაბი და შედეგი განსაზღვრავს რამდენად მიაღწია ოპერაციამ შეიარაღებული თავდასხმის ნიშნულს[24]. ამ თვალსაზრისით საყურადღებოა, რომ გაეროს მართლმსაჯულების საერთაშორისო სასამართლო „ნიკარაგუას საქმეში“ განმარტავს, რომ მასშტაბისა და შედეგის კრიტერიუმები თვისებრივი, რაოდენობრივი ელემენტებია, რომლებიც ხელს უწყობენ შეიარაღებული თავდასხმის დიფერენცირებას უბრალო სასაზღვრო ინციდენტებისგან[25].

23. Yoram Dinstein, War, Aggression and Self-Defense, Fourth Edition, Cambridge University Press, (2005), 165-169.

24. *Kosmas Pipyros, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis*, Theodoros Apostolopoulos, “A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual”, 74 Computers and Security, (2018), 375.

25. Id., at 376.

შეიარაღებული თავდასხმის შედეგების გათვალისწინებით ნიშანდობლივია ტალინის სახელმძღვანელოს ავტორების მიერ კიბერშეტევასთან დაკავშირებით შემუშავებული განმარტება. აღნიშნული დოკუმენტის 30-ე წესის მიხედვით, კიბერთავდასხმა არის კიბეროპერაცია, რომელიც აერთიანებს როგორც შეტევით, ასევე თავდაცვით ოპერაციებს და იწვევს პიროვნებების სხეულის დაზიანებას, გარდაცვალებას ან საგნების გაფუჭებას, განადგურებას[26]. აღნიშნული დეფინიცია მიანიშნებს იმაზე, რომ კიბეროპერაციის შედეგად მიყენებული ზიანი უნდა იყოს ისეთი, როგორსაც მიიღებდნენ ტრადიციული საზღვაო, სახმელეთო და საჰაერო ძალების გამოყენების დროს. სერიოზული დანაკარგების გამოწვევის გარეშე კიბერშეტევა ვერ ჩაითვლება თავდასხმის ახალ სახედ, რომელიც წარმოშობს გაეროს წესდების 51-ე ან ჩრდილოატლანტიკური ხელშეკრულების მე-5 მუხლების ამოქმედების საფუძვლებს[27].

კიბერსივრცის საზღვრებს გარეშე ფუნქციონირება კიბერშეტევების განმახორციელებელ აქტორთა რაოდენობას ზრდის. საერთაშორისო სამართლებრივი თვალსაზრისითაც გაეროს წესდების 51-ე მუხლი არ აკონკრეტებს სახელმწიფოს წინააღმდეგ მიმართული თავდასხმის განმახორციელებელი სუბიექტი ვინ შეიძლება იყოს, რაც არ გამორიცხავს არასახელმწიფოებრივი აქტორის მიერაც ამა თუ იმ ქვეყნის წინააღმდეგ შეტევის შესაძლებლობას სხვა სახელმწიფოს ტერიტორიიდან. ამ კონტექსტში პროფესორი მაიკლ შმიტი აღნიშნავს, რომ მომავალი კიბეროპერაციები შეცვლიან გაეროს მართლმსაჯულების საერთაშორისო სასამართლოს ვიწრო ინტერპრეტაციას შეტევის განმახორციელებელ აქტორთან დაკავშირებით. არასახელმწიფოებრივი სუბიექტებისათვის კიბერსივრცე წარმოადგენს იმ დომეინს, სადაც უფრო ადვილადაა შესაძლებელი შეტევითი ოპერაციების წარმოებისათვის შესაბამისი საშუალებების მოპოვება[28].

შეიძლება ითქვას, რომ კიბერშეტევა წარმოადგენს ისეთ თავდასხმას, რომელიც კომპიუტერული ქსელების შესაძლებლობების გამოყენებით უკანონოდ კრიტიკულ ინფორმაციულ სისტემებში აღწევს და მათი ფუნქციონირების შეფერხებით, სხვაგვარი მანიპულაციებით ქვეყნის თავდაცვისათვის, უსაფრთხოებისათვის, განვითარების პროცესისათვის, საზოგადოებისათვის ისეთი არსებითი ზიანის მიყენება შეუძლია, რომლითაც კონვენციურ ოპერაციას უტოლდება. მეტიც, კიბერსივრცის ბუნებიდან გამომდინარე, ერთ სახელმწიფოს მეორე სახელმწიფოს წინააღმდეგ აღნიშნული შეტევის განხორციელებისას აქვს შესაძლებლობა, დარჩეს ანონიმურ მოწინააღმდეგედ და ჰაკერთა ჯგუფის მეშვეობით ტრადიციული საომარი მოქმედებების დაწყების გარეშე მიაყენოს ზიანი.

26. See supra note 16, 106.

27. See supra note 10, 482.

28. See supra note 7, 287.

დასკვნა

საინფორმაციო და საკომუნიკაციო ტექნოლოგიებმა შეცვალეს არა მხოლოდ ომის წარმოების ფორმები, არამედ ხელი შეუწყვეს შეიარაღებული თავდასხმის ხელახალ ინტერპრეტაციას. მოქმედი საერთაშორისო სამართლის ნორმები, მათ შორის გაეროს წესდება და ჩრდილოატლანტიკური ხელშეკრულება გამოიყენება კიბერშეტევებთან მიმართებით, რადგან მათ შეუძლიათ შეუქმნან საფრთხე სახელმწიფოთა ეროვნულ უსაფრთხოებას და ისეთივე ზიანი მოუტანონ ქვეყნებს, მათ საზოგადოებებს, როგორც კონვენციურმა შეტევებმა.

კიბერშეტევის საერთაშორისო სამართლებრივ განსაზღვრებაზე საუბრისას, გაეროს წესდების 51-ე და ჩრდილოატლანტიკური ხელშეკრულების მე-5 მუხლების საფუძველზე, რამდენიმე პარამეტრის გამოყოფა მიზანშეწონილია. პირველ რიგში, აღნიშნული მუხლების თანახმად, შეიარაღებული თავდასხმა არის საფუძველი დაზარალებული სახელმწიფოს მიერ ინდივიდუალური და კოლექტიური თავდაცვითი მექანიზმების ასამოქმედებლად. მეორე რიგში, კიბერშეტევის დესტრუქციული ბუნება იძლევა იმის თქმის შესაძლებლობას, რომ ამ ტიპის ქმედებას შეუძლია მიაღწიოს შეიარაღებული თავდასხმის ზღურბლს. სწორედ ამ კონტექსტში ტალინის სახელმძღვანელოს ინტერპრეტაციის შედეგად აღსანიშნავია, რომ თუ კიბერთავდასხმა იწვევს ადამიანების ჯანმრთელობისათვის არსებითი ზიანის მიყენებას, მათ გარდაცვალებას ან საგნების ისე გაფუჭებას, განადგურებას, რომლითაც ფერხდება სახელმწიფოს ნორმალური ფუნქციონირება, წარმოადგენს შეიარაღებულ თავდასხმას, ანუ ძალის გამოყენების ყველაზე მძიმე ფორმას უთანაბრდება. მესამე რიგში, კიბერშეტევა არ შეიძლება იყოს შემოფარგლული მხოლოდ სახელმწიფო აქტორით. კიბერთავდასხმის განმახორციელებელია როგორც სახელმწიფო, ასევე არასახელმწიფოებრივი აქტორი. მით უფრო, რომ გაეროს წესდების 51-ე მუხლი არ აწესებს შეზღუდვას იმასთან დაკავშირებით, რომ შეტევა ხორციელდება მხოლოდ ერთი სახელმწიფოს მიერ სხვა სახელმწიფოს წინააღმდეგ. ციფრული ტექნოლოგიების მიღწევები არასახელმწიფოებრივ წარმონაქმნებს აძლევს შესაძლებლობას შექმნან შეტევითი კიბერინსტრუმენტები. ამ საშუალებების გამოყენებით სახელმწიფოებს ან არასახელმწიფოებრივ აქტორებს უცხო ქვეყნის ტერიტორიიდან შეუძლიათ გამოიწვიონ კონვენციურ ოპერაციებზე არანაკლები ზიანი ფიზიკურად საზღვრების გადაკვეთის გარეშე.

საყურადღებოა, რომ ტალინის სახელმძღვანელოები არ წარმოადგენს სავალდებულო ძალის მქონე დოკუმენტებს. ისინი მხოლოდ უზრუნველყოფს მოქმედი საერთაშორისო სამართლებრივი ნორმების ხელახალ ინტერპრეტაციას. შესაბამისად, როგორც გლობალურ, ასევე რეგიონალურ ფორმატებში აუცილებელია სახელმწიფოებს შორის აქტიური დისკუსიების წარმართვა კიბერსივრცის საერთაშორისო სამართლებრივი ასპექტების ორაზროვნების აღმოსაფხვრელად. რეალისტური თვალთახედვით ბუნდოვანება შესაძლოა სტრატეგიულად ხელსაყრელი იყოს გარკვეული სახელმწიფოებისათვის შეტევითი

ახალი ოპერაციების განსახორციელებლად და ციფრულ სივრცეში ანონიმურ მოთაშედ დასარჩენად. ამ ტიპის ქმედებების თავიდან ასაცილებლად აუცილებელია ახალი საერთაშორისო რეჟიმის – საერთაშორისო კიბერრეჟიმის შექმნა, რომელიც განსაზღვრავს სახელმწიფოთა პასუხისმგებლიან ქცევასთან დაკავშირებულ წესებს კიბერსივრცეში და ახალი ნორმების ხელმყოფთათვის დაადგენს შესაბამის საერთაშორისო სამართლებრივი პასუხისმგებლობის სახეებს. ეს პროცესი ხელს შეუწყობს კიბერსივრცის უსაფრთხოების უზრუნველყოფას და სახელმწიფოთა კრიტიკული ინფორმაციული სისტემების დაცვას.

გამოყენებული ლიტერატურა

1. Antonia Chayes. „Rethinking Warfare: The Ambiguity of Cyber Attacks“. Harvard National Security Journal, (2015).
2. Back to Square One? The NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusivereport-un-general-assembly.html.
3. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. the United States of America), 1986, http://www.icjcij.org/docket/ index.php.
4. Charter of the United Nations, http://wwwupdate.un.org/en/documents/charter/intro.shtml.
5. Founding Treaty – the North Atlantic Treaty, April 4, 1949, https://www.nato.int/cps/en/natohq/topics_67656.htm.
6. Kosmas Pipyros. Christos Thraskias. Lilian Mitrou. Dimitris Gritzalis. Theodoros Apostolopoulos. „A New Strategy for Improving Cyber Attacks Evaluation in the Context of Tallinn Manual.“ 74 Computers and Security, (2018).
7. Matthew C. Waxman. “Cyber Attacks as Force under the U.N. Charter Article 2(4).“ 87 International Law Studies Series, the U.S. Naval War College, (2011).
8. Michael Schmitt. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.” Columbia Journal of Transnational Law, Volume 37, (1998-1999).
9. Michael N. Schmitt. “Preemptive Strategies in International Law.” Michigan Journal of International Law, (2003).
10. Michael N. Schmitt. “The Law of Cyber Warfare: Quo Vadis?” 25 Stanford Law & Policy Review, (Spring, 2014).
11. René Värk. “The Use of Force in the Modern World: Recent Developments and Legal Regulation of the Use of Force.” Baltic Defence Review No. 10, Volume 2, (2003).
12. Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, (Michael N. Schmitt, ed.), Cambridge University Press, (2013).
13. The Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 4-5, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.
14. Yoram Dinstein. War, Aggression, and Self-Defence. The Fourth Edition, Cambridge University Press, (2005).