ჯეოქეისი
კ. ხეთაგუროვის ქ. 36, 0102 თბილისი, საქართველო
T: +995 32 2555755 | E: info@geocase.ge
www.geocase.ge

კიბერშეტევები, როგორც ომის წარმოების თანამედროვე ფორმა

ავტორი: პროფ. ხათუნა ბურკაძე, „ჯეოქეისი“-ს მკვლევარი

9 ივნისი, 2020 წ.

ფოტო: https://imedinews.ge

ტექნოლოგიური მიღწევები არის გასაღები საზოგადოების განვითარებისთვის. თუმცა კომპიუტერული ქსელების გამოყენებით შესაძლებელია ომის თანამედროვე ფორმით წარმოებაც. მეტიც, მომავალში სახელმწიფოები ალბათ კიბეროპერაციებს სპეციალური რობოტების მეშვეობითაც განახორციელებენ.

როგორც პროფესორი მაიკლ შმიტი აღნიშნავს, კიბერსივრციდან მომდინარე საფრთხე ტრადიციული საფრთხეებისგან განსხვავებით არ არის შეზღუდული კონკრეტული პოლიტიკური და გეოგრაფიული საზღვრებით. კიბერშეტევები, ჩვეულებრივი თავდასხმებისგან 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.

მზარდი ტექნოლოგიური მიღწევების გამო კიბერშეტევები უფრო იხვეწება და იკარგება კონტროლი ინფორმაციული ტექნოლოგიების ინფრასტრუქტურაზე.

2007 წელს ესტონეთისა და 2008 წელს საქართველოს წინააღმდეგ განხორციელებულმა კიბერშეტევებმა თვალსაჩინო გახადა კიბერთავდაცვითი შესაძლებლობების განვითარების აუცილებლობა. ესტონეთისგან განსხვავებით 2008 წლის აგვისტოში საქართველოს წინააღმდეგ კიბერშეტევები ტრადიციული საომარი მოქმედებების პარალელურად განხორციელდა. აღნიშნული ჰიბრიდული გამოწვევის წინაშე საქართველო დგას დღემდე, განსაკუთრებით უნდა გამოვყოთ 2019 წლის 28 ოქტომბერს საქართველოს წინააღმდეგ განხორციელებული ფართომასშტაბიანი კიბერშეტევა, რომელიც გულისხმობდა საქართველოს პრეზიდენტის ადმინისტრაციის, სასამართლო სისტემის, სხვადასხვა მუნიციპალიტეტის საკრებულოების, სახელმწიფო, კომერციული და მედია ორგანიზაციების ვებ-გვერდებისა და სერვერების ფუნქციონირების შეფერხებას. საბოლოო ჯამში, კიბერშეტევის შედეგად ხსენებული ორგანიზაციების სერვერები და მართვითი სისტემები დაზიანდა.

აღნიშნული კიბერშეტევის მიზანი იყო საქართველოს ეროვნული უსაფრთხოების ხელყოფა, საქართველოს მოსახლეობისთვის ზიანის მიყენება და საზოგადოებაში მღელვარების დათესვა სხვადასხვა ორგანიზაციის, მათ შორის სახელისუფლებო სტრუქტურების ფუნქციონირების შეფერხებით.

შეიძლება ითქვას, რომ საინფორმაციო ტექნოლოგიების ერაში ეროვნული უსაფრთხოება მოიცავს არა მხოლოდ საჰაერო, სახმელეთო, საზღვაო კომპონენტებს, არამედ კიბერსივრცესაც. რადგან კიბერსივრცე არ არის შემოფარგლული კონკრეტული საზღვრებით, ეს კიბერსივრცის თანმდევ გამოწვევებს მასშტაბურ ხასიათს სძენს. ამდენად, მშვიდობიანი, თავისუფალი, ღია და უსაფრთხო კიბერსივრცის განვითარების აუცილებელი წინაპირობაა საერთაშორისო პარტნიორებთან მჭიდრო თანამშრომლობა. საქართველო აგრძელებს პარტნიორებთან როფორც ორმხრივ, ისე მრავალმხრიფ ფორმატებში თანამშრომლობას, რაც აუცილებელია კიბერსივრცეში დესტრუქციული მოქმედებების თავიდან ასაცილებლად.

არაერთმა პარტნიორმა გამოხატა მხარდაჭერა საქართველოს კიბერუსაფრთხოების გასაძლიერებლად. საქართველოში ამერიკის შეერთებული შტატების საელჩოს მიერ გავრცელებულ განცხადებაში აღინიშნა: „ამერიკის შეერთებული შტატები მოუწოდებს რუსეთს, შეწყვიტოს მსგავსი ქმედებები საქართველოში და სხვაგან. კიბერსივრცის სტაბილურობა დამოკიდებულია სახელმწიფოების პასუხისმგებლიან ქცევაზე. ჩვენ საერთაშორისო საზოგადოებასთან ერთად გავაგრძელებთ მუშაობას, რომ დავიცვათ სახელმწიფოს პასუხისმგებლიანი ქცევის საერთაშორისო სისტემა კიბერსივრცეში“. ამასთანავე, განცხადებაში განსაკუთრებული ყურადღებაა გამახვილებული ამერიკის შეერთებული შტატების მზაობაზე მხარი დაუჭიროს საქართველოს მავნე კიბერ აქტორებთან ბრძოლაში,

საჯარო ინსტიტუტების განმტკიცებაში, შესთავაზოს დამატებითი შესაძლებლობების განვითარება და ტექნიკური დახმარება მსგავსი ქმედებებისგან თავდასაცავად.

გაერთიანებულმა სამეფომაც დაგმო რუსეთის მიერ საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევა და ხაზი გაუსვა იმ ფაქტს, რომ აღნიშნული მოქმედება არის მცდელობა შეარყიოს საქართველოს სუვერენიტეტი, დათესოს გაურკვევლობა და ზიანი მიაყენოს ქართველი ხალხის ყოველდღიურ ცხოვრებას. გაერთიანებული სამეფო რჩება საქართველოს სუვერენიტეტისა და ტერიტორიული მთლიანობის მტკიცე მხარდამჭერად.

ამერიკის შეერთებულ შტატებთან და გაერთიანებულ სამეფოსთან ერთად საქართველოს მიმართ მხარდაჭერა გამოხატეს დანიის, ესტონეთის, ლატვიის, ლიეტუვის, პოლონეთის, ნორვეგიის, ჩეხეთის, შვედეთის, მონტენეგროს, ისლანდიის, კანადის, ნიდერლანდების სამეფოს, რუმინეთის, უკრაინისა და ავსტრალიის საგარეო უწყებებმა.

ამა წლის 5 მარტს კი გაერთიანებული ერების ორგანიზაციის უშიშროების საბჭოს სხდომაზე ცალკე თემად განიხილეს საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევა. ამასთანავე, საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიურო ჩრდილოატლანტიკური ალიანსის გონივრული თავდაცვის პროექტის მავნე კოდებზე ინფორმაციის მიმოცვლის მრავალეროვნული პლატფორმის (MISP) სრულუფლებიანი წევრი გახდა. პლატფორმა უზრუნველყოფს კიბერშეტევების შესახებ ინფორმაციის გაზიარებას. ყოველივე ეს ცხადყოფს, რომ ჩვენ გვაქვს საერთაშორისო მხარდაჭერა როგორც ორმხრივი, ისევე მრავალმხრივი ფორმატების ფარგლებში.

რაც შეეხება კიბერშეტევების საერთაშორისო სამართლებრივ ასპექტებს, არ არსებობს საერთაშორისო ხელშეკრულება, რომელიც უშუალოდ დაარეგულირებს კიბერშეტევებისა და კიბერომის საერთაშორისო სამართლებრივ საკითხებს. ერთადერთი საერთაშორისო სამართლებრივი დოკუმენტია ევროსაბჭოს ფარგლებში მიღებული კონვენცია „კიბერდანაშაულის შესახებ“. თუმცა, ეს კონვენცია კიბერსივრცეში მომხდარ დარღვევებს განიხილავს სისხლის სამართლის კონტექსტში და იგი არ ეხება კიბერშეტევებს, როგორც ომის წარმოების ერთ-ერთ ფორმას.

მიმაჩნია, რომ აუცილებელია არსებული საერთაშორისო სამართლებრივი ნორმების ხელახალი ინტერპრეტაცია, რათა სახელმწიფოებმა შეძლონ შესაბამისი რეაგირება კიბერშეტევებზე. გაერთიანებული ერების ორგანიზაციის წესდება და ჩრდილოატლანტიკური ხელშეკრულება მიიღეს იმ პერიოდში, როდესაც კიბერსივრცის შექმნის განჭვრეტა რთული იყო. იმის გათვალისწინებით, რომ 21-ე საუკუნეში კიბერინციდენტები ყოველდღიური რეალობაა, მნიშვნელოვანია იმის ხაზგასმა, რომ გაეროს წესდება და ჩრდილოატლანტიკური ხელშეკრულების მე-5 მუხლი -კოლექტიური თავდაცვის უფლება, ვრცელდება კიბერსივრცეზე. მით

უფრო, რომ ამ საერთაშორისო ხელშეკრულებებში არ არის განმარტებული შეიარაღებული თავდასხმის ცნება. საერთაშორისო პრაქტიკის ანალიზის საფუძველზე შეიძლება ითქვას, რომ კიბერშეტევების შემთხვევებში გასათვალისწინებელია თავდასხმის ინტენსივობა, მასშტაბი და ხანგრძლივობა. ასევე იმისათვის, რომ კიბერშეტევამ მიაღწიოს შეიარაღებული თავდასხმის ზღურბლს და სახელმწიფოს ჰქონდეს ინდივიდუალური ან კოლექტიური თავდაცვის უფლების გამოყენების შესაძლებლობა, ის უნდა იწვევდეს არსებით ზიანს.

ამასთანავე, ეს მოქმედება უნდა ხორციელდებოდეს ერთი სახელმწიფოს მიერ მეორე სახელმწიფოს წინააღმდეგ ან არასახელმწიფოებრივი აქტორის მეშვეობით, როდესაც კიბერთავდასხმები ხორციელდება უცხო ქვეყნის ტერიტორიიდან, მაგალითად, ჰაკერთა ჯგუფის მიერ სხვა სახელმწიფოს მხარდაჭერით, დაფინანსებით.

ამ კონტექსტში საინტერესოა ნატო-ს გამოცდილების ანალიზი, კერძოდ, ჩრდილო-ატლანტიკური ალიანსის მხარდაჭერით განხორციელდა კვლევითი პროექტი, რომლის ფარგლებში 2013 და 2017 წლებში გამოიცა ტალინის სახელმძღვანელოები. ამ სახელმძღვანელოების ავტორები, ცნობილი საერთაშორისო ექსპერტები, განმარტავენ, რომ კიბერშეტევამ შეიძლება მიაღწიოს შეიარაღებული თავდასხმის ზღურბლს, რაც გაეროს წესდების 51-ე და ნატოს მე-5 მუხლების საფუძველზე სახელმწიფოს აძლევს უფლებას განახორციელოს როგორც ინდივიდუალური, ისე კოლექტიური თავდაცვითი ოპერაციები.

2016 წლის ვარშავის სამიტზე კი ალიანსმა კიბერსივრცე აღიარა ოპერაციების წარმოების დომეინად, რაც ნიშნავს ნატო-ს კოლექტიური თავდაცვის პრინციპის მოდერნიზებას. ისტორიულად ჩრდილოატლანტიკური ალიანსი ორიენტირებული იყო სახმელეთო, საჰაერო და საზღვაო თავდაცვითი შესაძლებლობების გაძლიერებაზე. დღეს კოლექტიური თავდაცვის აღნიშნულ კომპონენტებს დაემატა კიბერთავდაცვითი შესაძლებლობების გაძლიერება.

მზარდი ჰიბრიდული გამოწვევები განაპირობებენ სახელმწიფო დონეზე ერთიანი სტრატეგიის შემუშავების აუცილებლობას. კერძოდ, აუცილებელია ჰიბრიდულ საფრთხეებთან ბრძოლის სტრატეგიის მიღება.

ჰიბრიდულ საფრთხეებთან ბრძოლის სტრატეგიამ უნდა განსაზღვროს თანამედროვე ჰიბრიდული საფრთხეების ტიპები და მკაფიოდ წარმოაჩინოს ჰიბრიდული გამოწვევების არასამხედრო მახასიათებლები, ტაქტიკა, გაანალიზოს მათი შესაძლო გავლენა ქვეყნის პოლიტიკურ, ეკონომიკურ პროცესებზე, ასევე განიხილოს მათთან ბრძოლის გზები.

ჰიბრიდულ საფრთხეებთან ბრძოლის სტრატეგია უნდა ასახავდეს აღნიშნულ გამოწვევებთან ბრძოლის სამკომპონენტიან მექანიზმს (რაც ეფუძნება ჩრდილოატლანტიკური ალიანსის გამოცდილებას):

1) მზადება ჰიბრიდული საფრთხეებისთვის, რაც გულისხმობს შესაძლო ჰიბრიდული აქტივობების შესახებ ინფორმაციის შეგროვებასა და ანალიზსს, ასევე, გადაწყვეტილებების მიმღებთა აღჭურვას შესაბამისი მონაცემებითა და ცოდნით;

2) შეკავება ჰიბრიდული საფრთხეების, რაც ნიშნავს შესაბამისი სამთავრობო უწყებების ინსტიტუციურ გაძლიერებას, რათა მათ შეძლონ დროულად და ეფექტიანად ჰიბრიდული გამოწვევის შესაძლო ნეგატიური, დესტრუქციული შედეგის თავიდან აცილება;

3) თავდაცვა - თუ შეკავების პოლიტიკამ ვერ მიაღწია სასურველ სტრატეგიულ მიზანს, აუცილებელია, ჰიბრიდულ საფრთხეებთან სწრაფი რეაგირების შესაძლებლობების განვითარება.

ჰიბრიდულ საფრთხეებთან ბრძოლის სტრატეგია შესაძლოა ითვალისწინებდეს ჰიბრიდულ საფრთხეებთან ბრძოლის უწყებათაშორისი ჯგუფის შექმნას, რაც აუცილებელია გრძელვადიანი სტრატეგიული რეაგირების ინსტიტუციური მექანიზმის უზრუნველსაყოფად.

საბოლოო ჯამში, ჰიბრიდულ საფრთხეებთან ბრძოლის სტრატეგიის მიღება მნიშვნელოვანია კიბერუსაფრთხოების გაძლიერების თვალსაზრისითაც, რადგან იგი ხელს შეუწყობს კიბერინციდენტების, როგორც ჰიბრიდული გამოწვევების პრევენციას ან მათზე მყისიერ რეაგირებას.

ასევე, კიბერუსაფრთხოების გასაძლიერებლად მნიშვნელოვანია შემდეგი ნაბიჯების გადადგმა: 1) კრიტიკული ინფრასტრუქტურის დაცვის მიზნით შესაბამისი სტანდარტების განვითარება; 2) კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის დონეზე კვლევების განხორციელება; 3) კიბერთავდაცვითი შესაძლებლობების გაძლიერების მიზნით პარტნიორებთან ერთად უფრო მეტი სიხშირით ერთობლივი წვრთნების ჩატარება, მათ შორის ამერიკელ და ესტონელ ექსპერტებთან ურთიერთობების გაღრმავება; 4) საჯარო და კერძო სექტორის აქტორების ჩართულობით სახელმწიფო დონეზე კიბერუსაფრთხოების მუდმივმოქმედი პლატფორმის საბოლოოდ ჩამოყალიბება; 5) უნივერსიტეტების ჩართულობით კიბერუსაფრთხოების სპეციალისტების მოსამზადებლად მეტი პროგრამის შექმნა; 6) საზოგადოების ცნობიერების ასამაღლებლად საინფორმაციო-საგანმანათლებლო პროექტების მეტი სიხშირით განხორციელება.

დაბოლოს, საქართველოს აქტიური ჩართულობა ინფორმაციული სისტემების დაცვის მექანიზმების განვითარების მიმართულებით უზრუნველყოფს დაცული საინფორმაციო ტექნოლოგიების შექმნას და გაზრდის ჩვენს სტრატეგიულ როლს, მეტიც გვაქცევს ციფრულ ჰაბად რეგიონში.

9 ივნისი, 2020 წ.