ინტერვიუ

ხათუნა ბურკაძე
9 მარტი, 2020 წ.

ხათუნა ბურკაძე - საქართველოსთვის უმნიშვნელოვანესია ჰიბრიდულ საფრთხეებთან ბრძოლის სტრატეგიის მიღება

კიბერუსაფრთხოების საკითხებზე „ინტერპრესნიუსი“ „ჯეოქეისის“ მკვლევარს **ხათუნა ბურკაძეს** ესაუბრა.

- ქალბატონო ხათუნა, 2008 წლიდან საქართველო არაერთხელ აღმოჩნდა კიბერშეტევების სამიზნე, მათ შორის 2019 წლის 28 ოქტომბერს საქართველოს წინააღმდეგ განხორციელდა კიბერშეტევა.

ახლახან გაირკვა, რომ 2019 წლის 28 ოქტომბერს საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევაც რუსეთიდან მომდინარეობდა. გასულ კვირას გაერო-ს უშიშროების საბჭოს სხდომაზე ამერიკის შეერთებულმა შტატებმა, ესტონეთმა და დიდმა ბრიტანეთმა დაადგეს 2019 წლის ოქტომბერში რუსეთის მიერ საქართველოზე განხორციელებული კიბერთავდასხმა.

იქნებ უფრო დეტალურად მოგვითხროთ, რას გულისხმობს ფართომასშტაბიანი კიბერშეტევების განხორციელება?

- 2008 წლის აგვისტოში საქართველო ტრადიციული საომარი მოქმედებების პარალელურად კიბერშეტევების სამიზნე აღმოჩნდა. სამწუხაროდ, აღნიშნული პერიოდიდან დღემდე კიბერსივრცის სტაბილურობის უზრუნველყოფა გამოწვევად რჩება. თუმცა კიბერუსაფრთხოების გაძლიერება აქტუალურია არაერთი სახელმწიფოსთვის. მით უფრო, რომ კიბერსივრცე უსაფრთხოების პოლიტიკის უახლესი, ფართომასშტაბიანი და რთული კომპონენტია.

2019 წლის 28 ოქტომბერს რუსეთის მიერ საქართველოს წინააღმდეგ განხორციელებული ფართომასშტაბიანი კიბერშეტევა 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.

მსგავსი დესტრუქციული მოქმედებები მიზნად ისახავენ ეროვნული უსაფრთხოების ხელყოფას, მოსახლეობისთვის ზიანის მიყენებას და საზოგადოებაში მღელვარების დათესვას სხვადასხვა ორგანიზაციის, მათ შორის სახელისუფლებო სტრუქტურების

ფუნქციონირების შეფერხებით.საქართველოს წინააღმდეგ რუსეთის მიერგანხორციელებული კიბერშეტევები საერთაშორისო სამართლის ფუნდამენტურ პრინციპებს ეწინააღმდეგება, რადგან ისინი ხელყოფენ ქვეყნის სუვერენიტეტს, ტერიტორიული მთლიანობის ხელშეუხებლობის პრინციპსა და საქართველოს განვითარებას აფერხებენ.

- როგორ შეაფასებდით საერთაშორისო პარტნიორების მხრიდან გაკეთებულ საქართველოს მხარდამჭერ განცხადებებს. თქვენი აზრით, რამდენად შეუძლიათ ამ განცხადებებს ხელი შეუწყონ საქართველოს კიბერუსაფრთხოების გაძლიერებას?

- ნიშანდობლივია, რომ საქართველოზე განხორციელებულ კიბერშეტევის ფაქტს საერთაშორისო პარტნიორების მხრიდან სათანადო რეაგირება მოჰყვა.

ჩვენმა არაერთმა პარტნიორმა ქვეყანამ დაგმო საქართველოში რუსეთის მიერ განხორციელებული კიბერშეტევა, რაც ხელს შეუწყობს საქართველოს კიბერუსაფრთხოების გაძლიერებას.

გასათვალისწინებელია ის ფაქტი, რომ კიბერსივრცე არ არის შემოფარგლული კონკრეტული საზღვრებით, რაც გამოწვევას მასშტაბურ ხასიათს სძენს. შესაბამისად, მშვიდობიანი, თავისუფალი, ღია და უსაფრთხო კიბერსივრცის განვითარების აუცილებელი წინაპირობაა საერთაშორისო პარტნიორებთან მჭიდრო თანამშრომლობა.

საქართველოს მხარდამჭერი განცხადებები იმაზე მეტყველებს, რომ გაგრძელდება პარტნიორებთან თანამშრომლობა, რაც აუცილებელია კიბერსივრცეში დესტრუქციული მოქმედებების თავიდან ასაცილებლად.

მეტიც, ახლახან, საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიურო ჩრდილოატლანტიკური ალიანსის გონივრული თავდაცვის პროექტის მავნე კოდებზე ინფორმაციის მიმოცვლის მრავალეროვნული პლატფორმის (MISP) სრულუფლებიანი წევრი გახდა. აღნიშნული გადაწყვეტილება ხელს შეუწყობს კიბერუსაფრთხოების გაძლიერებას, რადგან ხსენებული პლატფორმა უზრუნველყოფს კიბერშეტევების შესახებ ინფორმაციის გაზიარებას.

ამ თვალსაზრისით უნდა აღინიშნოს, რომ საქართველოში ამერიკის შეერთებული შტატების საელჩოს მიერ გავრცელებულ 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 იმას, 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, უკრაინის, ავსტრალიის საგარეო უწყებებმა.

ამა წლის 5 მარტს კი გაერთიანებული ერების ორგანიზაციის უშიშროების საბჭოს სხდომაზე ცალკე თემად განიხილეს საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევა. ყოველივე ეს ცხადჰყოფს, რომ ჩვენ გვაქვს საერთაშორისო მხარდაჭერა როგორც ორმხრივი, ისევე მრავალმხრივი ფორმატების ფარგლებში.

- საინფორმაციო ტექნოლოგიების განვითარების შედეგად კიბერინციდენტებთან ერთად რა სახის გამოწვევების წინაშეა საქართველო და როგორ უნდა მოხდეს მათი დაძლევა?

- საინფორმაციო ტექნოლოგიების განვითარების პირობებში კიბერინციდენტებთან ერთად მზარდი ჰიბრიდული გამოწვევებია დეზინფორმაცია, პროპაგანდა, რაც განაპირობებს სახელმწიფო დონეზე ერთიანი სტრატეგიის შემუშავების აუცილებლობას.

საქართველოში კიბერშეტევებისა და დეზინფორმაციული კამპანიების განხორციელების ფონზე უმნიშვნელოვანესია ერთიანი სამთავრობო ხედვის შემუშავება. 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.

- ფაქტია, რომ დრამატულად შეიცვალა ომის წარმოების მეთოდები. შესაბამისად, საინტერესოა იმის გარკვევა, თუ როგორია საერთაშორისო აქტორების ხედვა ომის წარმოების უახლეს ფორმებზე?

- გლობალურ დონეზე ჯერ კიდევ არ არის ერთიანი ხედვა ჩამოყალიბებული კიბერშეტევებისა და კიბერომის განმარტებებთან მიმართებით. მიუხედავად ამისა, რეგიონალურ დონეზე ნატო-ს წევრმა ქვეყნებმა შეიმუშავეს მკაფიო ხედვა კიბეროპერაციებთან დაკავშირებით.

ჩრდილოატლანტიკური ალიანსისთვის 2007 წელს ესტონეთის წინააღმდეგ განხორციელებული კიბერშეტევა კიბერთავდაცვითი პოლიტიკის შემუშავების საფუძვლად იქცა.

ნატო-ს წევრი ქვეყნები შეთანხმდნენ, რომ არსებული საერთაშორისო სამართლებრივი ნორმები, მათ შორის გაერო-ს წესდება და ჩრდილოატლანტიკური ხელშეკრულება შეიძლება გამოიყენონ კიბერსივრცეში.

თუმცა, გასათვალისწინებელია ხსენებულ სივრცეში განხორციელებული თავდასხმის ინტენსივობა, მასშტაბი და ხანგრძლივობა. საბოლოო ჯამში, შეიძლება ითქვას, რომ საინფორმაციო ტექნოლოგიების ერაში უსაფრთხოების პოლიტიკა მოიცავს არა მხოლოდ საჰაერო, სახმელეთო, საზღვაო კომპონენტებს, არამედ კიბერსივრცესაც.

-კიბერუსაფრთხოების გაძლიერების კონტექსტში სტრატეგიის, საერთაშორისო პარტნიორებთან მჭიდრო თანამშრომლობის გარდა, საქართველომ განსაკუთრებული ყურადღება რაზე უნდა გაამახვილოს?

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

ტექნოლოგიური მიღწევები ხელს უწყობენ საბრძოლო ტაქტიკის სწრაფად განვითარებას კიბერსივრცეში. ამდენად, სახელმწიფოებისთვის, მათ შორის საქართველოსთვის, მნიშვნელოვანია კრიტიკული ინფორმაციული სისტემების დაცვა.

საქართველოს მიერ ინფორმაციული სისტემების დაცვის მექანიზმების განვითარება უზრუნველყოფს დაცული საინფორმაციო ტექნოლოგიების შექმნას და რეგიონში ჩვენს სტრატეგიულ როლს გაზრდის.

- რადგან კიბერშეტევების საფრთხე საკმაოდ სერიოზულია, ვიდრე ჰიბრიდულ საფრთხეებთან ბრძოლის სტრატეგიის მიღება შესაძლებელი იქნება, ამ ეტაპზე რა კონკრეტული ნაბიჯების გადადგმა იქნებოდა ეფექტური და აუცილებელი?

ვფიქრობ, რომ კიბერუსაფრთხოების გასაძლიერებლად მნიშვნელოვანია:

კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის დონეზე კვლევების განხორციელება; კიბერთავდაცვითი შესაძლებლობების გაძლიერების მიზნით პარტნიორებთან ერთად უფრო მეტი ინტესივობით ერთობლივი წვრთნების ჩატარება; პარტნიორი ქვეყნების ექსპერტებთან, მათ შორის ამერიკელ და ესტონელ ექსპერტებთან ურთიერთობების გაღრმავება; საჯარო და კერძო სექტორის აქტორების ჩართულობით სახელმწიფო დონეზე კიბერუსაფრთხოების მუდმივმოქმედი პლატფორმის საბოლოოდ ჩამოყალიბება; კრიტიკული ინფრასტრუქტურის დაცვის მიზნით შესაბამისი ზომების გატარება; უნივერსიტეტების ჩართულობით კიბერუსაფრთხოების სპეციალისტების მოსამზადებლად მეტი პროგრამის შექმნა; საზოგადოების ცნობიერების ასამაღლებლად საინფორმაციო-საგანმანათლებლო პროექტების მეტი ინტენსივობით განხორციელება.

„ინტერპრესნიუსი“, კობა ბენდელიანი