**საქართველოს კიბერსივრცეში არსებული საფრთხეები**

ქვეყნის წინაშე არსებული კიბერსაფრთხეების მასშტაბი მზარდია, როგორც სირთულის, ისე მრავალფეროვნების თვალსაზრისით. ანტიტერორისტული კოალიციის აქტიური წევრობისა და ქვეყნის მკაფიოდ გამოხატული ევროატლანტიკური ვექტორის გათვალისწინებით, ეროვნული მნიშვნელობის კრიტიკული ინფრასტრუქტურის გარდა, კიბერთავდასხმების სამიზნეს წარმოადგენს საქართველოში არსებული სხვა ქვეყნების, საერთაშორისო ორგანიზაციების თუ საზღვარგარეთული კომერციული სტრუქტურების საინფორმაციო ქსელები და ინფრასტრუქტურა.

ზოგადად, სახელმწიფოსათვის კიბერსაფრთხე შესაძლოა მომდინარეობდეს ისეთი აქტორებისაგან, როგორებიცაა:

* მაღალგანვითარებული კიბერშეტევითი პოტენციალის მქონე ქვეყნები (რუსეთი, ჩინეთი, ირანი, ჩრდ. კორეა);
* ტერორისტული ორგანიზაციების კიბერდანაყოფები და იდეოლოგიურად მოტივირებული ან ექსტრემისტულად განწყობილი ჰაკერები;
* ფინანსურად მოტივირებული კიბერდამნაშავეები.

საქართველოსათვის ყველაზე რეალური საფრთხის შემცველი არის რუსეთის კიბერაქტივობები, საინფორმაციო-ტექნიკური, ასევე საინფორმაციო-ფსიქოლოგიური ეფექტით. რუსეთის მიერ განხორციელებულმა ან მხარდაჭერილმა საინფორმაციო-ტექნიკურ შედეგზე ორიენტირებულმა კიბერშეტევამ საქართველოში შესაძლოა გამოიწვიოს მნიშვნელოვანი ზარალი და მსხვერპლიც კი, ხოლო კიბერარხებით გავრცელებულმა პროპაგანდისტულმა კონტენტმა, შესაძლოა გამოიწვიოს საინფორმაციო-ფსიქოლოგიური ეფექტი: კრემლის სასარგებლოდ ცნობიერების შეცვლა, პროდასავლური განწყობების შემცირება და პრორუსული ელიტის ფორმირება-გაძლიერება, რაც კონვენციური მოქმედებების წინაპირობა შეიძლება გახდეს. სუსტად დაცული ინფრასტრუქტურის პირობებში დაბალტექნოლოგიური კიბერშეტევაც კი შესაძლოა არაპროპორციულად მაღალი ზარალის მიზეზი გახდეს.

საქართველოსთან მეგობრული ურთიერთობის გამო, ირანისა და ჩინეთის მხრიდან მომდინარე კიბერსაფრთხეები მინიმალურია. რეალურია ჩინური არასახელმწიფო აქტორების მიერ განხორციელებული კიბერშპიონაჟის ალბათობა, სენსიტიური ეკონომიკური მონაცემების, ინტელექტუალური საკუთრების და ტექნოლოგიური სიახლეების მოპოვების მიზნით. ირანის ექსტრემისტულად განწყობილ ჰაკერების ინტერესს შესაძლოა წარმოადგენდეს საქართველოში განთავსებული ჩვენი სტრატეგიული პარტნიორების ინფრასტრუქტურა და მონაცემთა ბაზები, რომელთაც ისინი საკუთარ იდეოლოგიურ მოწინააღმდეგედ განიხილავენ.

ტერორისტული ორგანიზაციები, (Hizballah, HAMAS, al Qa’ida, ISIS, თალიბანი) აგძელებენ კიბერსივრცის გამოყენებას სადაზვერვო ინფორმაციის მოსაპოვებლად, ფონდების მოსაძიებლად, რეკრუტირებისათვის, პროპაგანდის გასავრცელებლად. ისინი გამუდმებით ცდილობენ შემდგომი ტერაქტების განსახორციელებლად მოიპოვონ სენსიტიური ინფორმაცია ანტიტერორისტული კოალიციის წევრი სახელმწიფოების მოქალაქეებზე, განსაკუთრებით კი სამხედრო პერსონალზე, რათა მათზე თავდასხმის შედეგად გამოწვეულმა მღელვარებამ და შიშმა აიძულოს მთავრობა, დატოვოს კოალიციის რიგები ან შეწყვიტოს სამხედრო ოპერაციები ტერორისტული ორგანიზაციების წინააღმდეგ. ტერორისტული დაჯგუფებები დღესდღეობით არ ფლობენ მნიშვნელოვანი ზიანის მისაყენებლად საკმარის კიბერსაშუალებებს. ამიტომ, ისინი, არსებული ტენდენციით, კონვენციურ შეტევებს მიანიჭებენ უპირატესობას, როგორც ამ ეტაპზე მნიშვნელოვანი ზიანისა თუ შიშის გამომწვევ მათ ხელთ არსებული ერთადერთ მექანიზმს. ტერორისტული ორგანიზაციების მხრიდან დიდია ალბათობა ისეთი კიბერშეტევის განხორციელებისა, რომელიც გამოიწვევს ელექტრონული სერვისების და ვებ-გვერდების დროებით, ლოკალურ დაზიანებას. მასობრივი ზიანის ან მსხვერპლის გამომწვევი კიბერშეტევის ორგანიზება და განხორციელება ამ ეტაპზე ნაკლებად სავარაუდოა.

რთულად პროგნოზირებადია მოგებაზე ორიენტირებულ კიბერდამნაშავეთაგან მომდინარე საფრთხეების ინტენსივობა. უკანასკნელ პერიოდში, განსაკუთრებით კი რუსეთის შემთხვევაში, ზღვარი სახელმწიფოსა და კრიმინალურ აქტორებს შორის წაშლილია, რადგან კიბერკრიმინალი დესტრუქციული კიბეროპერაციების განხორციელების იაფი და ატრიბუციის თვალსაზრისით საიმედო იარაღია. კიბერდამნაშავეები წარმატებით ახორციელებენ ბიზნესისა და ფინანასური ინსტიტუტების ქსელებში შეღწევას, რათა მოიპოვონ ფინანსური ინფორმაცია, პერსონალური მონაცემები, საცხოვრებელი თუ ელექტრონული ფოსტის მისამართები და სამედიცინო ჩანაწერები. კრიტიკული ინფრასტრუქტურის დიდი ნაწილი კერძო სექტორშია კონცენტრირებული. ბიზნეს სექტორის საინფორმაციო სისტემები, ხშირ შემთხვევაში სახელმწიფო მნიშვნელობის ინფორმაციულ მასივებს შეიცავს. სახელმწიფო უსაფრთხოებისათვის მნიშვნელოვანია კრიტიკული სერვისების პროვაიდერებში არსებული მონაცემთა ბაზები, სადაც, გარდა პერსონალურისა, კონცენტრირებულია ინფორმაცია ქვეყნის თავდაცვისუნარიანობის შესახებ.