როგორ მოვახდინოთ ტერორიზმის პრევენცია

წინათქმა

კიბერ ეპოქაში, საზოგადოება ინტერნეტსა და სოციალურ ქსელებს განიხილავდა კეთილდღეობისა და სტაბილურობის ხელშემწყობი ტექნოლოგიების სახით.

ბოლო პერიოდში ტერორისტულ კამპანიებში მნიშვნელოვნად წარმოჩინდა სოციალური ქსელის როლი და „ფასეულობა“.

ნიშანდობლივია, რომ არსებული კიბერსაფრთხეების პირობებში, გამოვლინდა საქართველოს კიბერარმიის ფორმირების აუცილებლობა. შესაბამისად, საკითხი ტერორისტული საფრთხეების ზრდასთან ერთად განსაკუთრებით აქტუალურია.

მოცემული სტატიით წარმოჩენილია, კიბერგარემო, კიბერტერორიზმის საფრთხეები და კიბერარმიის ფორმირების აუცილებლობა საქართველოში.

კიბერგარემოს გლობალური საფრთხეები

კიბერსივრცეში, ინტერნეტ-ტექნოლოგიები გახდა ტერორისტული საქმიანობის განუყოფელი ნაწილი. კიბერსაფრთხეებმა Facebook-ის, Twitter-ის, YouTube-ის, ბლოგისა თუ სხვა საიტების ძალა და გავლენა წარმოაჩინა. ტერორისტული ორგანიზაციები web-ტექნოლოგიებს იყენებს ტერორისტული ჯგუფების ფორმირების, ტერორისტული ქსელის მართვის, ტერორისტულ კამპანიაში ჩართვის, თავდასხმებისა და სხვა პროცესების განხორციელების მიზნით.

რეალობა ცხადყოფს, რომ **Facebook-ი გამოიყენება უკანონო პროცესების დაგეგმვისთვის, Twitter-ი ტერორიზმის კოორდინაციისთვის, მრავალფეროვანი დიალოგისა და ინსტრუქციის წარმოდგენისთვის, YouTube-ი იმისათვის, რომ მსოფლიო გაეცნოს მოვლენებსა და პროცესებს, ხოლო ბლოგი - ონლაინ აქტივობისა და მოვლენების აღწერის მიზნით, ტერორისტული ორგანიზაციის მიზნების უფრო ფართოდ წარმოჩენისთვის.**

მიმდინარე საუკუნის დასაწყისში არაბულ ქვეყნებში, ინტერნეტისა და სოციალური ქსელის ტექნოლოგია იყო ავტორიტარული გარემოს წინააღმდეგ ბრძოლის პლატფორმა და ინსტრუმენტი, ე.წ. სუსტებისა და უუფლებოების იარაღი, საზოგადოების განთავისუფლების საფუძველი. თუმცა განვითარებული მოვლენების ფონზე, იგი იქცა უკანონო ჯგუფების შექმნის საშუალებად, ტერორიზმის წყაროდ და რესურსად.

დღეს, კიბერტერორიზმის ფორმირების საფუძვლად, განიხილება ისეთი ინფორმაციული და საკომუნიკაციო ტექნოლოგიები, როგორიცაა:

• **სოციალური მედია** (ბლოგები და მიკრობლოგინგი, მაგ.:Twitter. ასევე, აუდიო/ვიდეო სტრიმინგი, ჰიბრიდული დანართები) - ტერორისტულ ორგანიზაციებში ჩართულ პირებს უადვილებს კონტენტის

(ტექსტი, ვიდეო, ფოტო) გადმოტვირთვას, პოვნას, განხილვას, შექმნასა და სხვა მიზნების შესაძლებლობას; ე.წ. ისლამური სახელმწიფო ISIS -ს, მხოლოდ Twitter-ზე ჰყავს 90 ათასი მხარდამჭერი მიმდევარი (ინტერნეტ-ექაუნთი). ISIS-ს ონლაინ აქტივობისა და სოციალური მედიის მეშვეობით 100 მლნ ადამიანთან აქვს წვდომა, მათი წარმომადგენლები ყოველდღე Twitter-ზე 100 000 ტვიტს პოსტავს. მხარდამჭერების ლოკაცია მოიცავს: ე.წ. ისლამურ სახელმწიფოს, სირიას, ერაყს, საუდის არაბეთს;

• **სოციალური ქსელები** ((Facebook, LinkedIn)- მას იყენებენ ტერორისტულ დაჯგუფებათა ქსელის გაზრდა/გაფართოებისთვის, ინფორმაციულობისა და ინფორმაციის ნაკადის გავრცელებისთვის. ე.წ. ისლამური სახელმწიფო ISIS -ის წარმომადგენლები ყოველდღე 90 ათას მედია მესიჯს ავრცელებს;

მობილური კომუნიკაცია - ინტერნეტ-დაშვების გაფართოება ახალი თაობის მობილური ტელეფონებითა და ჯიბის კომპიუტერებით; ასევე, დეცენტრალიზებული ჯგუფების მართვის საშუალება. ISIS - იყენებს სმარტფონებს, მათ შორის: ანდროიდი (69%), Apple -ის ტელეფონები (30%) და Blackberry (1%).

ტერორისტული ორგანიზაციების მიერ ინტერნეტ-ტექნოლოგიების გამოყენების მიზნები:

• ინტერნეტში ადვილია ფართო აუდიტორიის მოზიდვა, მიზნობრივი ჯგუფების შექმნა (ტერორისტული, საბრძოლო);

• კლაუდსორსინგის იდეალური საშუალება. მოხალისე ჯგუფების (მათ შორის ტერორისტული, მებრძოლი) მოძიებისა და შექმნის ყველაზე ეფექტიანი და ადვილი შესაძლებლობა;

• ინტერნეტ-მომხმარებლებს ძირითადად წარმოადგენენ ახალგაზრდები (18-34 წლის), რომლებიც ისწრაფვიან გაცნობის, საკუთარი თავის წარმოდგენის, საზოგადოებაში ადგილის დამკვიდრებისთვის;

• ინტერნეტ-ტექნოლოგიებით, მილიონობით ადამიანთან შესაძლებელია ინტენსიური და ხანგრძლივადიანი ურთიერთქმედება, ასევე შესაძლებელია ადამიანების შთაგონება (ინსპირირება გამოწვიო), ერთნაირად აზროვნებისა და მხარდაჭერის მოპოვება;

• ინტერნეტი უზრუნველყოფს მაღალ ინტერაქტიულობას, მიზნობრივ ჯგუფებთან კომუნიკაციის შესაძლებლობით. „სოციალური ქსელის“ საიტებს გააჩნიათ ინტერაქტიული მხარდაჭერა; მიზნობრივ ჯგუფებზე ზემოქმედების ფართო შესაძლებლობა, შთაგონებისა და ემოციური ზეგავლენის პოტენციალი;

• ტექნოლოგიები წარმოადგენს მასობრივი ინფორმაციის ფორმას. იგი სოციალური ურთიერთობების (ამ შემთხვევაში ტერორისტული მიზნებით) ორგანიზაციის ინსტრუმენტია;

• ინტერნეტი წარმოადგენს სოციალურ სტრუქტურას, რომელიც ზეგავლენას ახდენს ტერორისტული ჯგუფების ფორმირებაზე, ტერორიზმის ევოლუციასა და მის სტრუქტურაზე;

• ინტერნეტი შესაფერისი პლატფორმაა ინფორმირებული და ინტერაქტიული კიბერპოლი-ტიკის, ტერორიზმში მონაწილეობის სტიმულირებისათვის;

• სოციალური ტექნოლოგიების შედეგად ყალიბდება ერთგვარი კიბერტერორიზმი, რომელიც ძლიერდება იდეოლოგიური ორიენტაციით, „ტერორიზმის მართვის ავტომატიზაციით“, კიბერტერორიზმის კამპანიის ეფექტიანი წარმოებით;

• ინტერნეტის ინსტრუმენტები და ფორმები, გლობალურ თუ ლოკალურ პირობებში ტერორისტული ძალების ფორმირების შესაძლებლობას იძლევა;

ᲥᲐᲠᲗᲣᲚᲘ ᲙᲘᲑᲔᲠᲐᲠᲛᲘᲘᲡ ᲨᲔᲥᲛᲜᲘᲡ ᲡᲐᲭᲘᲠᲝᲔᲑᲐ

გლობალური კიბერსაფრთხეების ფონზე, საქართველოს ერთ-ერთ მნიშვნელოვან გამოწვევას წარმოადგენს ქვეყნის **კიბერუსაფრთხოება** და **კიბერარმიის ფორმირება.**აღნიშნული საკითხი კიდევ უფრო აქტუალური გახდა საქართველოსთვის ე.წ. „ისლამური სახელმწიფოს“ საფრთხეების ზრდასთან მიმართებაში.

ბოლო პერიოდში, მედიაში გავრცელებულ ინფორმაციაზე დაყრდნობით, შეიძლება აღინიშნოს, **რომ საქართველო (უკვე) განიხილება ჩრდილო კავკასიასთან სატრანზიტო კომუნიკაციის უზრუნველყოფისა და საკომუნიკაციო კიბერსივრცედ. თუ, ქართულ მედიაში გავრცელებულ ინფორმაციას დავეყრდნობით, „ალ-ქაიდას“ დაჯგუფებას კიბერარმია უკვე ჰყავს კავკასიაში, რაც საქართველოსთვის რეალურ საფრთხეს წარმოადგენს. შესაბამისად, სასწრაფოდ უნდა ჩამოყალიბდეს ქართული კიბერარმია.**

აღსანიშნავია სახელმწიფოს მიერ გატარებული ქმედითი ღონისძიებები (საიტების დაბლოკვა, ოპერატიული ღონისძიებები და სხვა), რაც ქვეყნის კიბერსივრცის უსაფრთხოებას ემსახურება.

ზემოაღნიშნული გამოწვევების ფონზე, ძირთად პრობლემად რჩება ის, რომ ქვეყანას არ ჰყავს კიბერარმია. ქვეყნის სტრატეგიულ დოკუმენტშიც (ელექტრონული საქართველოს სტრატეგია და სამოქმედო გეგმა 2014-2018) არ არის ჩადებული კიბერარმიის შექმნის სტარტეგიული პრიორიტეტულობა.

რატომ გვჭირდება კიბერარმია?

• სახელმწიფო უსაფრთხოებისთვის;

• ინტერნეტ-ბიზნესის უსაფრთხოებისთვის;

• ინფორმაციული საზოგადოების უსაფრთხოებისთვის;

• ახალი საფრთხეების პრევენციისთვის.

ზემოაღნიშნულის გარდა, ქვეყანაში კიბერარმიის შექნა ხელს შეუწყობს:

• ტერორისტებისა და ორგანიზებული კრიმინალური ქსელების გამოვლენას;

• თავდაცვისუნარიანობის ზრდასა და სამხედრო ძლიერებას;

• ლოკალური და გლობალური კიბერთავდახსმების პრევენციას;

• კიბერშეტევის წყაროს გაშიფვრას;

• სისტემების კრიტიკული ავარიის თავიდან აცილებას;

• ჰაკერების ქმედებების ლოკალიზებას;

• სამრეწველო შპიონაჟის წინააღმდეგ ბრძოლას;

• მავნე კონტენტისგან არასრულწლოვანთა დაცვას;

კიბერარმიის დაკომპლექტება

ასაკობრივი ცენზის მიუხედავად, იგი უნდა მოიცავდეს ყველა თაობის წარმომადგენელს, ვისაც კომპიუტერის ეფექტიანად გამოყენება შეუძლია. ვინც ფლობს ტექნოლოგიებს და საჭიროების შემთხვევაში ქვეყნის კიბერუსაფრთხოებაზე ზრუნვა შეუძლია. კიბერარმია შეძლება დაკომპლექტდეს:

• სავალდებულო სამხედრო სამსახურს დაქვემდებარებული თუ სავალდებულო სამხედრო სამსახურისგან განთავისუფლებული პირებით;

• შრომისუნარიანი და აქტიური მოქალაქეებით;

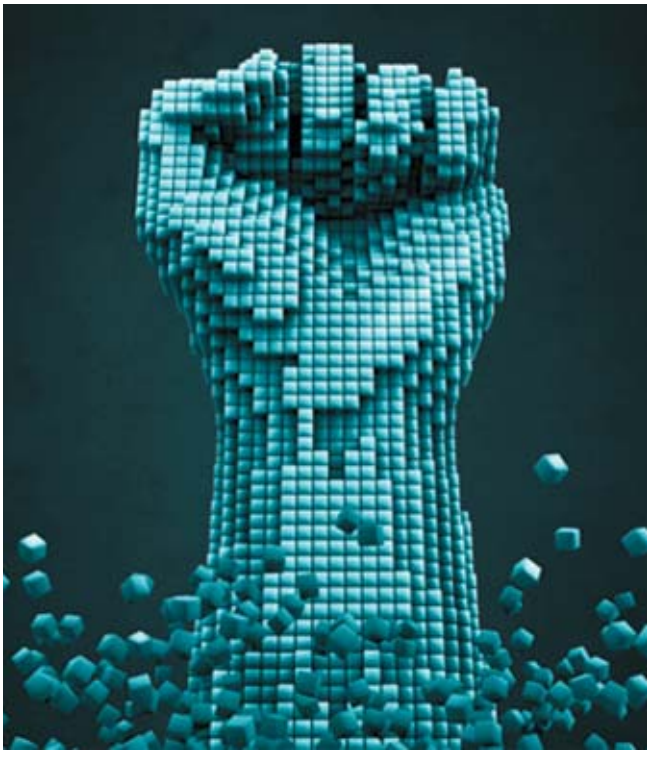
• სპეციალური საჭიროებების მქონე პირებით;

• ხანდაზმული და საპენსიო ასაკს გადაცილებული პირებით;

• ჯამში, სახელმწიფო, კერძო და სამოქალაქო სექტორის ყველა წარმომადგენელებით, ვინც ფლობს კომპიუტერულ ტექნოლოგიებს და ქმედუნარიანია კიბერსაფრთხეების პრევენციისთვის.

რეზიუმე

დესტრუქციული ძალების, ინფორმაციული აგრესიის, ინფორმაციული ოკუპაციის, ინფორმაციული



გენოციდის ლოკალიზაციისთვის, ასევე, გლობალურ კიბერგარემოსთან ლოკალურ ინტერესთა თავსებადობის მიზნით საჭიროა კიბერარმიის შექმნა.

კიბერარმიის შექმნისთვის აუცილებელია:

• კიბერ ჯგუფების მომზადება, მონაცემთა ბაზების ფორმირება, კიბერარმიის ორგანიზებაში სპეციალური საჭიროებების მქონე პირების დასაქმება და ეფექტიანად გამოყენება;

• კიბერარმიის დაკომპლექტებისთვის, საქართველოში მცხოვრები მოქალაქეების გარდა, საჭიროა უცხოეთში არსებულ ქართული „კიბერსათვისტომოების“ შექმნა და ფორმირება. აღნიშნული, საქართველოს საელჩოების ხელშეწყობით უნდა განხორციელდეს;

• სათვისტომოების კოორდინირებით, უცხოეთში მყოფი ასეულათასობით თანამემამულეებისგან უნდა შეიქმნას საინიციატივო ჯგუფები, დაკომპლექდეს მობილური ჯგუფები, რომელიც საქართველოს კიბერსაფრთხეებიდან გამომდინარე , ოპერატიულ კიბერმხარდაჭერას აღმოუჩენენ ქვეყანას (ქვეყანაში ჩამოსვლის გარეშე);

• ქვეყანაში უნდა გაიზარდოს ინტერნეტ-მომხმარებლების საქმიანობის მონიტორინგი, განხორციელდეს განსაზღვრულ web-საიტებთან მომხმარებლის დაშვების უარყოფა (ბლოკირება),საიტის ოპერატორებისთვის მონაცემთა ნაკადის ფილტრაცია, გამკაცრდეს ცენზურის წესების დაცვა, ინტერნეტ-ბლოკირება და ჩახშობა. აღნიშნულ ფონზე, მიზანშეწონილი და აუცილებელია, პროცესი განხორციელდეს საზოგადოების სამივე სექტორის (კერძო, სახელმწიფო და სამოქალაქო სექტორის) თანაბარუფლებიანი მონიტორინგით.

• ქვეყნისთვის საფრთხის შემცველი ინტერნეტ-ინფორმაციის ფილტრაცია უნდა განხორციელდეს დიფამაციის კანონის საფუძველზე - უნდა შეიქმნას ინტერნეტის რეგულირების კანონპროექტები და მოხდეს მისი საერთაშორისო ექსპერტიზა. უზრუნველყოფილი იქნას კიბერ-ბრძოლის პრევენციის საერთაშორისო მიდგომების უნიფიცირება;

• ქვეყანაში სასწრაფოდ უნდა შეიქმნას კომისია (რომელიც საზოგადოების სამივე სექტორის მიერ უნდა დაკომპლექტდეს) ინტერნეტ-რეგულირების კრიტერიუმების შემუშავების მიზნით;

• ქართული საზოგადოების სიფხიზლის, კიბერტერორიზმის, კიბერსაფრთხეების, აგრესიული ინტერნეტ-კონტენტის პრობლემის გათვიცნობიერების დონის ამაღლებისათვის უნდა გატარდეს საგანმანათლებლო და სოციალური აქტივობა. მოცემულ ლპროცესში ფართოდ უნდა ჩაერთოს მეცნიერები;

• დასასრულს, კავკასიის რეგიონში, უნდა შეიქმნას ინკლუზიური ელექტრონული მთავრობა, რომელიც კიბერსაფრთხეებისა და კიბერტერორიზმის წინააღმდეგ ბრძოლის ეფექტიანი სისტემა იქმნება და მისი უზრუნველყოფის გარანტიებს შექმნის.

რატი აბულაძე,
ეკონომიკის დოქტორი, პროფესორი