Scientific and Practical Cyber Security Journal (SPCSJ) 2(1):37-47
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

THE ROLE OF CYBERSECURITY IS NATIONAL SECURITY ENHANCEMENT

L.Saraidarov
Georgian Technical University, Tbilisi, Georgia

ABSTRACT. I think that the present article discusses the issues that cyber security is currently facing, which in its turn remains as one of the main components of the national security system of our country; the mitigation of those issues, their avoidance in the future and also the question of strengthening of the security system. Because cyber danger represents a relatively new and dangerous challenge both for us and for the world, it is still hard for most of the people to imagine or believe in the scale of the unfortunate results and damage caused by the cyber danger. It is obvious that cyber security should be one of the main concerns of our country due to the fact that Georgia is often a victim of cyber-attacks. The mere resources that our country possesses in the area of cyber security, used against fighting the mentioned challenges are often resulting in almost nothing, as cyber area as well as the persons operating in it, their evil goals and interests are only evolving and widening, thereby increasing the level of damage and endangering the security system of our country at its most. In my opinion, the threats that technological and informational security system of Georgia faces, lay a fundamental basis for the inevitability of the unfortunate results. Having said this, it is unfailingly necessary to strengthen the role of the jobs related to fighting the challenges and threats of cyber security as well as increase the number of those jobs and enhance the quality of professionalism, which finally will have a positive impact on the prevention of the expected threat and the evolvement and strengthening of cyber security system.

რეზიუმე. ვფიქრობ, წინამდებარე სტატიაში განხილულ იქნა ჩვენი ქვეყნის ეროვნული უსაფრთხოების სისტემის შემადგენელი ერთ-ერთი მთავარი კომპონენტის-კიბერუსაფრთხოების წინაშე მდგარი პრობლემები და მათი განეიტრალების, მომავალში თავიდან აცილებისა და თავდაცვითი სისიტემის განმტკიცების საკითხები. ვინაიდან, კიბერსაფრთხე ჩვენი ქვეყნისთვის და მსოფლიოსთვის შედარებით თანამედროვე, დიდი საშიშროების შემცველ გამოწვევას წარმოადგენს, ხალხთა უმეტესი ნაწილისთვის ჯერ კიდევ წარმოუდგენელია და დაუჯერებელი მისი მეშვებოთ გამოწვეული დაზიანებისა და სავალალო შედეგების მასშტაბები. თვალნათელია, რომ კიბერუსაფრთხოება ჩვენი ქვეყნის ერთ-ერთ უმთავრეს საზრუნავს უნდა წარმოადგენდეს, ვინაიდან, საქართველო ხშირად ხდება უცხო ქვეყნების მხრიდან კებერთავდასხმის სამიზნე. კიბერუსაფრთხოების სფეროში არსებული ჩვენი სახელმწიფოს მწირი რესურსი, რომლითაც ვცდილობთ გამკლავებას ხსენებული გამოწვევების წინაშე, არის დაბალი შედეგიანობის მომცემი, ვინაიდან კიბერსივრცე და მასში ოპერირებადი სუბიექტები, მათი ბოროტი განზრახვები და ინტერესები, სულ უფრო ვითარდება და ფართოვდება, შესაბამისად

დამაზიანებელი შედეგის ხარისხი მატულობს და უდიდესი საფრთხის წინაშე აყენებს ჩვენი ქვეყნის უსაფრთხოების სისტემას.

მიმაჩნია, რომ საქართველოს ტექნოლოგიური და ინფორმაციული უსაფრთხოების სისტემის წინაშე მდგარი საფრთხეები, ქმნიან რეალურ საფუძველს სავალალო შედეგის გარდაუვალობის, რის გამოც აუცილებელია გაძლიერდეს კიბერსივრციდან მომავალი საფრთხეებისა და გამოწვევების წინააღმდეგ მებრძოლი სამსახურების როლი და გაიზარდოს მათი რიცხოვნობა და ამაღლდეს პროფესიონალიზმის ხარისხი, რაც საბოლოოდ პოზიტიურ გავლენას იქონიებს მოსალოდნელი საშიშროების პრევენციაზე და კიბერუსაფრთხოების სისტემის განვითარება-გაძლიერებაზე.

KEYWORDS: cyber-attacks, cyber security, cyber danger, national security;

არსებული მდგომარეობის ზოგადი მიმოხილვა

შესავალი

დღვანდელ რეალობაში კიბერშეტევების მრავალფეროვნება და სიმძლავრე დღითიდღე მატულობს, რასაც ძირითად შემთხვევაში ტექნოლოგიების მოხმარებაში გათვითცნობიერება განაპირობებს.
უდაოა, რომ ყოველდღიურად სულ უფრო მეტი ადამიანი ინტერესდება ტექნოლოგიური საშუალებების სიახლეებითა და შესაძლებლობებით, მათი გამოყენებითა და მანიპულირებით, ზოგიერთი მათგანი კი მიდის იმ დასკვნამდეც, რომ ამ მეთოდებით შესაძლებელია სერიოზული ზიანის მიყენება და ზოგჯერ მნიშვნელოვანი სარგებლის მიღებაც კი.
კიბერშეტევები ძირითადად ცალკეული დაჯგუფებების მიერ ხორციელდება და მიზნად, ზიანის მიყენებას ან ჩვეულებრივი მოხმარებლისათვის მიუწვდომელი ინფორმაციის მიღებას ისახავს. ამ მთავარი ასპექტებიდან გამომდინარე, მრავალმა დომინანტმა სახელმწიფომ გადაწყვიტა კიბერუსაფრთხოებისა და კიბერშეტევების აყვანა სახელმწიფო და სამხედრო დონეზე, შესაბამისად კონკრეტულმა სახელმწიფო სტრუქტურებმა საკუთარ რიგებში ჩართეს მაღალი დონის სპეციალისტები, რომელთაც შესწევთ ძალა, განახორციელონ მასობრივი კიბერშეტევები, აწარმოონ კიბერშპიონაჟი და მოაწყონ დივერსიები.
ტერმინი-კიბერშეტევა ნიშნავს კომპიუტერული ქსელებისა და ელექტრონული სერვისების კონფიდენციალურობაზე, ერთიანობასა და ხელმისაწვდომობაზე თავდასხმას ან ასეთის მცდელობას. მსგავსი ქმედება შესაძლოა, გამიზნული იყოს როგორც სერვისის დასაზიანებლად ან

შესაფერხებლად, ასევე კომპიუტერული ქსელის პირადი მიზნებისთვის გამოსაყენებლად.

მთავარი გამოწვევები კიბერუსაფრთხოების სფეროში

უკანასკნელ პერიოდში კიბერშეტევების ხასიათი, გეოგრაფიული ველი, განვითარების სისწრაფე და სიმძლავრე საგრძნობლად შეიცვალა. ზოგადად, გამოიყოფა კიბერშეტევების ორი ძირითადი სახე: კიბერსაბოტაჟი და კიბერშპიონაჟი.

კიბერსაბოტაჟის მეშვეობით შესაძლებელია მნიშვნელოვანი, სტრატეგიული ობიექტების მწყობრიდან გამოყვანა, საზოგადოებაში შიშის დათესვა, ქაოსის შექმნა, მოწინააღმდეგის თავდაცვისუნარიანობის შესუსტება და მომზადება ძირითადი სამხედრო დარტყმის განსახორციელებლად, ხოლო კიბერშპიონაჟის უმთავრესი მიზანია, მოწინააღმდეგე ქვეყნის მნიშვნელოვანი, დიპლომატიური საიდუმლოებებისა და ინფორმაციის მოპარვა. გარდა ამისა, ცალკეული ჰაკერული დაჯგუფებები არა პოლიტიკური, არამედ პირადი სარგებლის მიღების განზრახვით, ესხმიან თავს მნიშვნელოვან კიბერსისტემებს და ეუფლებიან მასში დაცულ აქტივებს.

საქართველოსთვის მეტად მნიშვნელოვანია ინფორმაციული სივრცის უსაფრთხოება და ელექტრონული ინფორმაციის დაცულობა. ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად პირდაპირპროპორციულად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება და ურთიერთკავშირი. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერდანაშაულთან ბრძოლას და კიბერსივრცეში მოსალოდნელი დივერსიული აქტებისგან თავდაცვას.

ინფორმაციულ ტექნოლოგიებზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულებასთან ერთად იზრდება ის გამოწვევები, რომლებიც საქართველოს ინფორმაციული სივრცის დაცვასთანაა დაკავშირებული. 2008 წლის რუსეთ-საქართველოს ომის დროს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ, სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, მიზანმიმართული და მასობრივი კიბერთავდასხმები განახორციელა. ამ კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა.

თუმცა, თამამად შეიძლება ითქვას, რომ დღევანდელ მსოფლიოში კიბერშეტევების პოლიტიკური ბრძოლის, ხოლო ინტერნეტის ჰიბრიდული-არაკონვენციური მეთოდებით ომის წარმოების იარაღად გამოყენება, დომინანტი ტენდენცია გახდა და არა მხოლოდ ინტერნეტინდუსტრიის, არამედ მსოფლიო პოლიტიკის ერთ-ერთ მთავარ თავსატეხად იქცა.

საქართველოს ეროვნული უსაფრთხოების ახალი კონცეფცია და სხვა სამართლებრივი აქტები

საქართველოს პარლამენტმა 2011 წლის 23 დეკემბერს დაამტკიცა საქართველოს ეროვნული უსაფრთხოების ახალი კონცეფცია, რომელმაც 2005 წლის ივლისში მიღებული იგივე სახის დოკუმენტი ჩაანაცვლა. უნდა აღინიშნოს, რომ ახალ კონცეფციაში, წინა ვარიანტისაგან განსხვავებით, სხვა სახის ეროვნულ ინტერესებთან ერთად განსაზღვრულია კიბერუსაფრთხოების განმტკიცება, სწორედ იგი წარმოადგენს ეროვნული უსაფრთხოების პოლიტიკის ერთ-ერთ ძირითად მიმართულებას. იმავე დოკუმენტში ქვეყნის წინაშე არსებულ ერთ-ერთ უმნიშვნელოვანეს საფრთხეებად და გამოწვევებად, საერთაშორისო ტერორიზმთან და ტრანსნაციონალურ ორგანიზებულ დანაშაულთან ერთად სრულიად საფუძვლიანად და არგუმენტირებულად დასახელებულია-კიბერსაფრთხეები.
2012 წელს, საქართველოს პარლამენტის მიერ მიღებულ იქნა კანონი ინფორმაციული უსაფრთხოების შესახებ, სადაც დეტალურად გაიწერა ინფორმაციულ სფეროში უსაფრთხოების დაცვასთან დაკავშირებული ტერმინებისა და ნორმების განმარტებები, კანონის მოქმედების სფერო, ინფორმაციული აქტივების მართვისა და უსაფრთხოების დაცვის წესები. ამ კანონშივე ცალკე თავი დაეთმო კიბერუსაფრთხოების უზრუნველყოფას და მასზე პასუხისმგებელ სამსახურებს, მათ სტატუსსა და ფუნქციებს. იმავე წელს საქართველოს პრეზიდენტის ბრძანებულებით, ძალაში შესვლის მიზნით დამტკიცებულ იქნა „კიბერდანაშაულის შესახებ“ ევროსაბჭოს კონვენცია (ე.წ. ბუდაპეშტის კონვენცია), რომელიც აღნიშნულ საკითხთან დაკავშირებით შესასრულებლად სავალებულო დოკუმენტს წარმოადგენს. ხსენებულ დოკუმენტში მკაფიოდაა განსაზღვრული კიბერდანაშაულის ტიპები, კომპიუტერული მონაცემებისა და სისტემების კონფიდენციალობისა და მთლიანობის წინააღმდეგ მიმართული კონკრეტული დანაშაულები.

კიბერდაზვერვა-არაეთიკური საქმიანობა

კიბერშპიონაჟი ანუ კომპიუტერული შპიონაჟი (კიბერდაზვერვა), გულისხმობს სხვისი ინფორმაციის წყაროებზე (პირადი, პოლიტიკური, სამხედრო, კომერციული, ტექნოლოგიური და სხვა) არასანქცირებული წვდომისა და მართვის საშუალების მოპოვებას, რაც ხორციელდება კომპიუტერული დაცვითი სისტემების გვერდის ავლით, ზიანის მომტანი პროგრამული უზრუნველყოფის, მათ შორის ტროიანებისა და ჯაშუშური პროგრამების გამოყენებით. კიბერშპიონაჟი ხორციელდება, როგორც

დისტანციურად ინტერნეტის გამოყენებით, ასევე კომპიუტერში შეღწევით ლოკალური ქსელის გამოყენებით. დიდი ხანი არ არის, რაც კიბერდაზვერვის ერთ-ერთ საშუალებად სპეცსამსახურები აქტიურად იყენებენ სოციალური ქსელებში არსებულ პირად ინფორმაციას, რაც აშკარად უხვი ინფორმაციის მატარებელია. ხშირია შემთხვევები, როდესაც სოციალურ ქსელში თავს იყრის განსხვავებული შინაარსისა და მნიშვნელობის მქონე ინფორმაცია, კერძოდ, ექსტრემისტული, ტერორისტული ან კიდევ ანტისახელმწიფოებრივი საქმიანობისაკენ მოწოდების კონტექსტით, რაც თავისთავად რეაგირებას და ზოგ შემთხვევაში პრევენციული ღონისძიებების შემუშავებას გულისხმობს და ითვალისწინებს.

კიბერდაზვერვის ინტერესს და მიზანს წარმოადგენს სადაზვერვო ობიექტთან დაცული და თავმოყრილი მნიშვნელოვანი და კონფიდენციალური ინფორმაციის, მიუხედავად მისი ფორმატისა და დაცულობის ხარისხისა, მოპოვება, მართვა, დამახინჯება და სხვადასხვა სახის კონფიგურაცია, რაც საბოლოო ჯამში ითვალისწინებს, ინფორმაციის დაკარგვა-განადგურებას, დამახინჯებას, სასურველი სახით გამოყენების შეზღუდვას ან შეუძლებლობას, რეპუტაციის შელახვას და ასე შემდეგ, ყველაფერი ეს კი, ჯამში არის უდიდესი ზიანის გამომწვევი და გამოუსწორებელ შედეგამდე მიყვანის საფუძველი.

თვალნათელია, რომ კიბერდაზვერვის გარკვეული ანუ ანალიტიკური მუშაობის ნაწილი შესაძლოა ლეგალური იყოს, ანუ ღია წყაროებზე დაყრდნობით განხორციელებული საქმიანობა, ხოლო, რაც შეეხება არასანქცირებული გზით კომპიუტერული სისტემებიდან ინფორმაციის მოპოვებას, მათ განადგურებას, მათზე წვდომის სრულად მოპოვებას, სხვა პირებისათვის მათზე წვდომისა და გამოყენების შეზღუდვას და კონფიგურაციას, უდავოა, რომ ეს დანაშაულთან კავშირშია და მისი ლეგიტიმურობა ყოველთვის ეჭვქვეშ იდგება. მსგავსი არხებით ინფორმაციაზე წვდომის მოპოვების ლეგალური საფუძველი არ არსებობს, შესაბამისად, ინფორმაციის მოპოვება-შეგროვებაზე და ეროვნული სტრატეგიების და კონცეფციების განსაზღვრაზე პასუხისმგებელი და უფლებამოსილი, ასევე დაინტერესებული სახელმწიფო უწყებები მკაცრად ერიდებიან მსგავს საქმიანობაში ღიად, შენიღბვის გარეშე მონაწილეობის მიღებას. საიდუმლოდ აღარ მიიჩნევა, რომ ქვეყანაში არსებული საინფორმაციო-ტექნოლოგიურ სფეროში თავმოყრილი ინტელექტუალური პოტენციალი და რესურსი, წარმოადგენს სპეცსამსახურების უდიდეს ინტერესს. კიბერსადაზვერვო საქმიანობის წარმატებით განსახორციელებლად სპეცსამსახურები იყენებენ კომპანიებს, კერძო პირებს-ხაკერებს, რომლებიც აქტიურად არიან დაკავებული მსგავსი საქმიანობით. შესაბამისად, კონსპირაციულობის პრინციპიდან გამომდინარე, მათი არალეგალური მოქმედება იღებს შენიღბულ სახეს და შედეგის მისაღწევად იყენებენ ყველა საჭირო საშუალებას, რომელიც ხელმისაწვდომს გახდის ინფორმაციის მოპოვებასა და მართვას. მოცემულ შემთხვევაში რეალური დამკვეთი

და დაინტერესებული სუბიექტი, ის სახელმწიფოა, რომლისათვისაც მნიშვნელოვანია ინფორმაციის ფლობა სხვა ქვეყნებზე, გავლენის სფეროებისა და მასშტაბების გათვალისწინებით. თუმცა უნდა აღინიშნოს, რომ მსგავსი საქმიანობით არამარტო სახელმწიფო სპეცსამსახურები არიან დაინტერესებულნი და დაკავებულნი, რამდენადაც გასაკვირი არ უნდა იყოს, კიბერსფეროსა და კიბერსივრცეს აქტიურად და წარმატებით იყენებენ ტერორისტული ორგანიზაციები და დაჯგუფებები. ხსენებული სუბიექტები ტერორისტული მიზნებისთვის, ახორციელებენ საინფორმაციო პროპაგანდას, საზოგადოების დაშინებისა და გადაბირების მიზნით იყენებენ სოციალურ ქსელებს, ასევე ტელე-საკომუნიკაციო საშუალებებს, გარდა ხსენებულისა, თანამოაზრეების და მხარდამჭერების გამოვლენის მიზნით ავრცელებენ მოწოდებებს, როგორც ფიზიკური, ასევე ფინანსური მხარდაჭერის მისაღებად, საკუთარი საქმიანობის შენიღბვისა და შემოსავლების მიღების მიზნით, ახდენენ სხვა, შირმად ქცეული საქმიანობის აფიშირებას, რაც საბოლოოდ ხელს უწყობს მათ მიზანმიმართულ და საუბედუროდ, წარმატებულ საქმიანობას.

კიბერკონტრდაზვერვა (threat intelligence) საფრთხეების დაზვერვა

კიბერთავდასხმა ნებისმიერი ქვეყნის უსაფრთხოების სერიოზული პრობლემაა. ნებისმიერი სახელმწიფო ისეთივე პრობლემების წინაშეა კიბერსივრცეში, როგორც კლასიკურ, ტრადიციულ სივრცეში. უსაფრთხოების ღონისძიებების ძირითად ბერკეტს წარმოადგენს კიბერმზადყოფნა: კიბერარმია, კიბერპატრული, სამართლებრივი გარემო, ინფრასტრუქტურა, მომზადებული საზოგადოება და კიბერპოლიტიკა.

ყურადსაღებია, რომ საქართველოს ძირითადი საფრთხე ემუქრება რუსეთის სპეციალური სამსახურებისგან, რომლებიც რეგულარულად ახორციელებენ კიბერსადაზვერო საქმიანობას, როგორც სახელმწიფო საიდუმლოების შემცველი, ასევე სხვა სახის დახურული ინფორმაციის მოპოვების მიზნით. 2011 წელს საქართველოს შესაბამისი სამსახურების მიერ გამოვლენილ იქნა საკმაოდ დიდი მასშტაბის კიბერსადაზვერვო ოპერაცია – GEORBOT, რომელიც მიზნად ისახავდა სამხედრო სფეროს და, ასევე საქართველოს ხელისუფლებასა და ნატო-ს შორის არსებული ურთიერთობების თაობაზე ინფორმაციის მოპოვებას. სადაზვერვო ოპერაციის მთავარ სამიზნე ობიექტებს წარმოადგენდნენ საქართველოს მაღალი თანამდებობის პირების სამსახურებრივი გამოყენების ელექტრონული რესურსები, სადაც დისტანციურად განხორციელდა ჯაშუშური პროგრამული უზრუნველყოფის საშუალებათა ინსტალაცია, რომლის მეშვეობითაც მუდმივად ხორციელდებოდა სხვადასხვა კატეგორიის ინფორმაციის გადინება. 2008-2011 წლებში საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევების თავდაცვის საჭიროებამ და

კიბერსაფრთხეების ზრდამ, ბიზნესისა და სახელმწიფოსთვის უსაფრთხო კიბერგარემოს ფორმირების აუცილებლობამ, კიბერინციდენტებზე დროული რეაგირების საჭიროებამ, რეგიონული კიბერკონფლიქტების აღმოცენების საშიშროებამ, ჯამში გლობალურმა და ლოკალურმა საფრთხეებმა დაგვანახა კიბერარმიის ჩამოყალიბების აუცილებლობა, რასაც საფუძველი ჩაეყარა 2015 წელს.

კიბერკონტრდაზვერვა-ეთიკური საქმიანობა უსაფრთხოების განმტკიცებისა და თავდაცვის მიზნით გასატარებელი ღონისძიებები

რეალური პრაქტიკიდან გამომდინარე რომ შევაფასოთ არსებული მდგომარეობა და გავავლოთ პარალელები, უნდა განვიხილოთ მარტივი მაგალითი, კერძოდ: უცხო ქვეყნის სპეციალური და სადაზვერვო სამსახურების, ორგანიზაციების და დაჯგუფებების, ჩვენი ქვეყნის სახელმწიფო ინტერესების წინააღმდეგ მიმართული სადაზვერვო ან/და ტერორისტული საქმიანობის და მასთან დაკავშირებული საფრთხეების გამოვლენა და თავიდან აცილება ხორციელდება კონტრდაზვერვითი საქმიანობისა და სპეციალური რესურსების გამოყენების საფუძველზე. ჩვენს შემთხვევაში კიბერკონტრდაზვერვით საქმიანობად შესაძლოა ჩაითვალოს ყველა საშუალებისა და რესურსის გამოყენება, რათა გამოვლინდეს და თავიდან იქნას აცილებული კიბერთავდასხმის, ანუ კიბერდაზვერვისა და კიბერტერორიზმის საფრთხეები. ხსენებულ საფრთხეებთან გასამკლავებლად, როგორც აღვნიშნეთ, სხვადასხვა ქვეყანაში შეიქმნა კიბერსაფრთხეებთან მებრძოლი რაზმები, საქართველოში კი 2015 წელს, პირველად კავკასიის რეგიონში, საფუძველი ჩაეყარა „კიბერრეზერვის შექმნას“, საქართველოს თავდაცვის სამინისტროს შემადგენლობაში სსიპ-ის სახით შეიქმნა „კიბერუსაფრთხოების ბიურო“, რომლის საქმიანობის მიზანად განისაზღვრა კიბერუსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა, ასევე კიბერდანაშაულთან ბრძოლის ერთიანი სახელმწიფო პოლიტიკის განხორციელება. ბიუროს ფუნქციებად განისაზღვრა ინფორმაციული სისტემების უსაფრთხოების აუდიტი, ტექნოლოგიების განვითარების მონიტორინგი, კომპიუტერული უსაფრთხოების ინციდენტების, სისუსტეებისა და მტკიცებულებების დამუშავება და სხვა მრავალი. ბუნებრივია, რომ კიბერრეზერვის მობილიზება და საქმიანობა, თავის წილად უზრუნველყოფს ქვეყნის კიბერსივრცისა და ეროვნული უსაფრთხოების შეუვალობასა და სიმტკიცეს.

თვალნათელია, რომ მსგავსი სამსახურების ჩამოყალიბება და საქმიანობა ხორციელდება რეალური საფრთხეების წარმოშობისა და შეფასების და მათთან ბრძოლისა და თავდაცვის სტრატეგიის განსაზღვრის შემდეგ, თუმცა განსხვავებით კიბერდაზვერვისაგან, კიბერთავდაცვას და კიბერკონტრდაზვერვას გააჩნია ლეგიტიმური საფუძველი, რომელიც მომართულია არალეგალური და ზიანის

მომტანი კიბერთავდასხმის გამოსავლენად და მასთან საბრძოლველად. კიბერრეზერვში მსახური დამოკიდებულია კიბერჯარის კაცის, მაღალ ინტელექტზე და სპეციალურ განათლებაზე, და არა მისი ფიზიკური და ტაქტიკური მომზადების მაღალ დონეზე, ის სწორედ ინტელექტით უნდა გაუმკლავდეს კრიტიკულ სიტუაციაში ინტელექტუალურ, არასანქცირებულ, ვირტუალურ შემოტევას. თვალნათელია, რომ ფრონტის ხაზმა სახელწიფო საზღვრებიდან და გეოლოკაციებიდან, გადამოინაცვლა კლავიატურაზე და სამხედრო ოპერაციების ნაცვლად, სადაც გამოიყენება ფიზიკური ძალა და საბრძოლო ტექნიკა, კიბერ თავდაცვის გასახორციელებლად აუცილებელია ინტელექტუალური რესურსის გამოყენება. მაგალითად, აშშ-ში პენტაგონმა კიბეროპერაციების მიზნით კიბერჯარის რაოდენობა 2016 წლისათვის 6000 კაცით განსაზღვრა, ასევე დიდმა ბრიტანეთმა შექმნა „კიბერმებრძოლი რაზმი“ და განსაზღვრა მათი რიცხოვნობა და საქმიანობის მიმართულებები, ნიდერლანდებში, კიბერთავდაცვის მიზნით შექმნილია ერთობლივი თავდაცვის კიბერსარდლობა, ჩრდილოეთ კორეა ფლობს 3000-კაციან კიბერჯარს, ირანში, ისლამური რევოლუციის დამცველების მიერ ფორმირებული იქნა „ელექტრონული იარაღის“ რევოლუციური გვარდია.

აქვე არ უნდა დაგვავიწყდეს, რომ, გარდა სხვა უფრო დიდი მნიშვნელობისა და მასშტაბის მქონე თავდაცვითი საშუალებებისა, არსებობს კიბერთავდაცვის ყოველდღიური მოხმარების აქტიური და გავრცელებული საშუალებები, ჩვენს კომპიუტერულ სისტემებში გააქტიურებული ანტივირუსული პროგრამები და ფაირვოლები, რომლებიც ახერხებენ საზიანო პროგრამების აღმოჩენას და მისგან მოსალოდნელი არასახარბიელო შედეგისაგან და არასანქცირებული წვდომისგან დაცვას.

კიბერუსაფრთხოების ეროვნული სტრატეგია

კიბერუსაფრთხოება ეროვნული უსაფრთხოების განუყოფელი ნაწილია. მინდა მოგახსენოთ, რომ ხაზგასმის ღირსია ჩვენი ხელისუფლების მნიშვნელოვანი გადაწყვეტილება კიბერუსაფრთხოების ეროვნული სტრატეგიის შემუშავების თაობაზე.

მიუხედავად იმისა, რომ აღნიშნულთან დაკავშირებული საფრთხე წარმოიშვა 2008 წელს, რუსეთის მხრიდან საქართველოს წინააღმდეგ გონხორციელებული კიბერთავდასხმის შემდეგ, უკეთესი იქნებოდა, მსგავსი სახის დოკუმენტი შემუშევებული ყოფილიყო რეალური საფრთხის წარმოშობამდე და შესაბამისად გატარებული ყოფილიყო პრევენციული და თავდაცვისთვის აუცილებელი ღონისძიებები. სწორედ, პირველად ამ ქართულ დოკუმენტში გაიჟღერა ტერმინმა-კიბერომი, რაც უკავშირდებოდა 2008 წელს რუსეთის ფედერაციის მიერ

საქართველოს წინააღმდეგ გამოვლენილ აგრესიას, განხორციელებულს სამხედრო და კიბერსთავდასხმის სახით.

საქართველოს ხელისუფლებამ, 2013 წლის შემდეგ, 2017 წელს კვლავ, უკვე მეორედ გამოქვეყნა საქართველოს კიბერუსაფრთხოების ეროვნულ სტრატეგია, პირველად კი ეს განხორციელდა 2013 წელს. 2008 წლის აგვისტოში, რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ კიბერსივრცეში განხორციელებულმა აგრესიამ და, ასევე საქართველოს მზარდმა დამოკიდებულებამ ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე, ნათლად წარმოაჩინა, რომ საქართველოს ეროვნული უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე. ამრიგად, კიბერუსაფრთხოების განვითარება წარმოადგენს ეროვნული უსაფრთხოების განუყოფელ ნაწილსა და მნიშვნელოვან კომპონენტს.

საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს ამოცანებს და მათ შესასრულებლად განსაზღვრავს შესაბამის აქტივობებს. ამასთან, მოცემული სტრატეგია მიზნად ისახავს ხსენებულ დოკუმენტებში არსებული საფრთხეების აღკვეთასა და შემცირებას, ასევე ემსახურება ქვეყნის თავდაცვისუნარიანობის განმტკიცებასა და გაძლიერებას. ამასთან, ინფორმაციული სისტემის კრიტიკულობისა და კიბერუსაფრთხოებისადმი მდგრადობა განისაზღვრება ისეთი კრიტერიუმებით, როგორიცაა მოსალოდნელი ზიანის სიმძიმე და მასშტაბი, ინფორმაციული სისტემის აუცილებლობა სახელმწიფოსა და საზოგადოების ნორმალური ფუნქციონირებისათვის, სისტემის მომხმარებელთა რაოდენობა და კიბერუსაფრთხოების სათანადო დონის უზრუნველსაყოფად საჭირო რესურსები. ინფორმაციული და კიბერტექნოლოგიური ომი არის შეუქცევადი და მუდმივად პროგრესირებადი პროცესი, შესაბამისად მასთან ბრძოლა მოითხოვს უდიდეს იტელექტუალურ ძალისხმევასა და რესურსს.

დასკვნა

ზემოთქმულიდან გამომდინარე, საქართველოს წინაშე არსებული კიბერსაფრთხეების მასშტაბი მზარდია, როგორც სირთულის, ისე მრავალფეროვნების თვალსაზრისით. საჭიროა განსაკუთრებული ყურადღება დაეთმოს კიბერაქტორების განზრახვების, შესაძლებლობებისა თუ ღონისძიებების შესახებ ინფორმაციის მოპოვებისა და ანალიზის მექანიზმის ჩამოყალიბებას და ამ მხრივ აქტიური მუშაობის წარმართვას.

ყველაზე რეალური საფრთხის შემცველი საქართველოს კიბერსივრიცისათვის არის რუსეთის კიბერაქტივობები, რომელიც მიმართულია როგორც კრიტიკული ინფრასტრუქტურის მოშლის, ასევე საკუთარი მიზნებისათვის გამოყენებისაკენ.

რაც შეეხება ირანისა და ჩინეთის მხრიდან მომდინარე კიბერსაფრთხეებს, აქ, უპირველეს ყოვლისა, არ უნდა გამოგვრჩეს საქართველოში განთავსებული იმ სახელმწიფოების ინფრასტრუქტურა და მონაცემთა ბაზები, რომელთაც ეს ქვეყნები საკუთარ მოწინააღმდეგედ განიხილავენ. ასეთებს განეკუთვნება საქართველოს სტრატეგიული პარტნიორი აშშ, ჩრდილოატლანტიკური ალიანსისა და ევროკავშირის წევრი ქვეყნები და თავად ამ საერთაშორისო ორგანიზაციების სისტემები.

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.

უდავოა, რომ საქართველომ თვალი გაუსწორა გლობალურ და საფრთხისშემცველ ყოველდღიურ გამოწვევებს და წარმატებულადაც გაართვა თავი. კიბერომში მიწინავეა ის მხარე, რომელმაც დროულად შექმნა ორგანიზებული კიბერსივრცე, შეიმუშავა კიბერუსაფრთხოების სტრატეგია და პოლიტიკა, მომზადა IT-სპეციალისტები, უზრუნველყო საზოგადოებისა და სახელმწიფოს კოორდინირებული კიბერმზადყოფნა, სახელმწიფოში შეძლო თანამედროვე ინფრასტრუქტურის ფორმირება, გააჩნია მართვის ერთიანი კიბერცენტრი და მუდმივი მონიტორინგის კიბერჯგუფი. დღევანდელი რეალობიდან გამომდინარე ვრწმუნდებით, რომ განხილული ტექნოლოგიური ომის გეოგრაფიული საზღვრები აღარ არსებობს. ხშირად ვისმენთ, რომ ვირტუალურ სივრცეში უკვე მიმდინარეობს მესამე მსოფლიო ომი, ფრონტის ხაზი კი თითოეული ადამიანის გონებაში გადის.

REFERENCES

1. http://georgianreview.ge/2015/10/kibersivrceshi-safrtxeebi/?lang=ge; საქართველოს კიბერსივრცეში არსებული საფრთხეები;

2. http://dspace.nplg.gov.ge/bitstream/1234/144787/1/Kibertavdacva.pdf; კიბერთავდაცვა კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ვლადიმერ სვანაძე, ანდრია გოცირიძე. თბილისი 2015;

3. *„ღია წყაროების ანალიზი“,* სახელმძღვანელო, პატარაია ლ., დავიდოვი მ., გახოკიძე ბ.;

4. https://gipa.ge/uploads/files/Cyber_Protection.pdf; კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები 2015 ვლადიმერ სვანაძე;

5. http://acge.ge/2015/11/, საქართველოს კიბერსივრცეში არსებული საფრთხეები

6. https://risspa.podster.fm/26/embed/13?link=1&ap=0; Кибербразведка — что это и для чего?;

7. http://www.securitylab.ru/analytics/479451.php; На что способна кибербразведка; Автор: Виктор Ивановский;

8. http://www.civil.ge/geo/article.php?id=24953; ეროვნული უსაფრთხოების ახალი კონცეფცია, სივილ ჯორჯია, თბილისი , 23/12/2011;

9. http://yata.ge/ge/?p=907; კიბერუსაფრთხოება – კოლექტიური თავდაცვის ახალი გამოწვევა
ავტორი: კონსტანტინე კევლიშვილი, 16/11/2016;

10. https://matsne.gov.ge/ka/document/view/1923932; საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013–2015 წწ. სამოქმედო გეგმის დამტკიცების შესახებ, საქართველოს პარლამენტი 2013 წ;

11. https://matsne.gov.ge/ka/document/view/1555410; საქართველოს ეროვნული უსაფრთხოების კონცეფცია საქართველოს პარლამენტი 2011 წ;

12. https://matsne.gov.ge/ka/document/view/1665167; „კიბერდანაშაულის შესახებ“ კონვენციის დამტკიცების თაობაზე, საქართველოს პრეზიდენტის ბრძანებულება 2012წ;

13. https://matsne.gov.ge/ka/document/view/1679424; საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, საქართველოს პარლამენტი 2012 წ;

14. https://matsne.gov.ge/ka/document/view/3548407; საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია, საქართველოს მთავრობის დადგენილება 2017 წ;

15. https://matsne.gov.ge/ka/document/view/27364; საქართველოს კანონი „კონტრდაზვერვითი საქმიანობის შესახებ“, საქართველოს პარლამენტი 2005 წ;

16. https://www.youtube.com/watch?v=ko4jnL5A7rQ&t=13s, კიბერრეზერვი, ტელე-კომპანია „მაესტროს“ სიუჟეტი, ანდრო გოცირიძე,ლაშა პატარაია;

17. https://www.youtube.com/watch?v=xqM12S68Ilo კიბერრეზერვი, ტელე-კომპანია „საზოგადოებრივი მაუწყებლის“ სიუჟეტი, ანდრო გოცირიძე, ლაშა პატარაია;