საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა ქვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

11

გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები

ნათუნა მშვიდობაძე

ექსპერტის აზრი

2013

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

ექსპერტის აზრი

ხათუნა მშვიდობაძე

გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები

11

2013

პუბლიკაცია დაიბეჭდა ამერიკის შეერთებული შტატების საელჩოს ფინანსური მხარდაჭერით.

რედაქტორი: რუსუდან მარგიშვილი

ტექნიკური რედაქტორი: არტემ მელიქ-ნუბაროვი

ISSN 1512-4835
ISBN 978-9941-0-2681-2

შესავალი

ინფორმაციული ტექნოლოგიების მზარდმა განვითარებამ და მასზე დამოკიდებულების სწრაფმა ზრდამ წარმოშვა გლობალური მნიშვნელობის სისტემათა სისტემა. ინფორმაციულ სივრცეში, ინტერნეტტექნოლოგიების ინფრასტრუქტურის ურთიერთდამოკიდებული საკომუნიკაციო ქსელებისაგან, კომპიუტერული სისტემებისა და მათი მონაცემთა ბაზისაგან შეიქმნა ახალი გლობალური მნიშვნელობის კიბერდომეინი, რომელმაც ბევრ სარგებელთან ერთად ახალი საფრთხეებიც გააჩინა.

რთულია ინტერნეტის წარმოშობის ზუსტი თარიღის განსაზღვრა, თუმცა პაკეტური დაკავშირების იდეა *(ქსელთაშორისი ციფრული კომუნიკაციის მეთოდი, რომელიც აჯგუფებს ყველა გადასაცემ მონაცემს, მათი შინაარსის, სტრუქტურისა და ტიპის მიუხედავად)* გაჩნდა XX საუკუნის სამოციანი წლების დასაწყისიდან, როდესაც მაშინდელმა შეერთებული შტატების მოწინავე კვლევითი პროექტების სააგენტომ (ARPA), ამჟამად კი თავდაცვის მოწინავე კვლევითი პროექტების სააგენტომ (DARPA), მნიშვნელოვანი ნაბიჯები გადადგა ტექნოლოგიური განვითარების მიმართულებით, რათა კომპიუტერული ქსელების ერთმანეთთან დაკავშირება ინტერნეტის საშუალებით გამხდარიყო შესაძლებელი. ამ იდეის განხორციელების დემონსტრირება თარიღდება 1969 წლის 29 ოქტომბრით, როდესაც კალიფორნიის უნივერსიტეტის (UCLA) მაგისტრატურის სტუდენტმა ჩარლზ კლაინმა გაგზავნა პირველი ინტერნეტშეტყობინება – „ჩატვირთვა.“ არპანეტმა (ARPANET) მაშინ ლოს-ანჯელესში კალიფორნიის უნივერსიტეტის (UCLA) და სტენფორდის უნივერსიტეტის მხოლოდ ორი კომპიუტერი დააკავშირა, დღეს კი ინტერნეტის მომხმარებელი დაახლოებით ორმილიარდ-ნახევარი ადამიანია.[1]

იმ დროისათვის, ცხადია, ძნელად წარმოსადგენი იყო, რომ ეს პაკეტური გადაცემის გლობალური ქსელი სულ რაღაც ოთხი ათეული წლის შემდეგ უსაფრთხოების მნიშვნელოვან გამოწვევად გადაიქცეოდა.

არპანეტის შექმნის იდეის ისტორიული კვალი ჯერ კიდევ 1951 წელს მასაჩუსეტსის ტექნოლოგიების ინსტიტუტში ლინკოლნის ლაბორატორიის შექმნასა და ამერიკელი მეცნიერის ჯოზეფ კარლ რობნეტ ლიკლაიდერის მიერ გაჟღერებული გალაქტიკური კომპიუტერული ქსელის კონცეფციაზე გადის.[2] ლიკლაიდერის

„გალაქტიკური ქსელის“ კონცეფცია განსაზღვრავდა სოციალური ინტერაქციის ახალ ტიპს, რომლის მიღწევაც შესაძლებელია გლობალური კომპიუტერული საკუმუნიკაციო სისტემების საშუალებით, სადაც წვდომა მონაცემზე, ინფორმაციაზე ფართო მასებისათვის იქნება შესაძლებელი. მისი კონცეფცია ჯერ კიდევ მაშინ წარმოადგენდა დღევანდელი ინტერნეტის კონცეფციას.

თავად ინტერნეტისა და ამ ტერმინის შემოღება შესაძლოა ასევე 1974 წლით დათარიღდეს, როდესაც ვინტონ ცერფის, იოგენ დალალისა და კარლ სანშაინის მიერ წარმოდგენილ ინტერნეტდაკავშირების კონტროლის პროგრამის სპეციფიკაციის შესახებ კვლევაში *(Specification of Internet Transmission Control Program)* ტერმინი „ინტერნეტი“ იქნა გამოიყენებული. ამერიკელი მეცნიერების ვინტონ ცერფისა და რობერტ ხანის სახელს უკავშირდება ქსელთაშორისი ოქმების/მონაცემთა გადაცემის უმთავრესი საკომუნიკაციო ***TCP/IP*** *პროტოკოლებისა* და პირველი კომერციული ელექტრონული ფოსტის სისტემის შექმნა.

რთულია შედარების გაკეთება ახალ აღმოჩენებსა და იმ ტექნოლიურ მიღწევებს შორის, რასაც ადამიანი ათასწლეულების მანძილზე ახერხებდა. თუმცა, არც ერთ სხვა ტექნოლოგიურ მიღწევას არ მოუხდენია იმგვარი გავლენა ადამიანზე ასე სწრაფად და ასე მასშტაბურად, როგორიც ამ ტექნოლოგიურმა მიღწევამ შეძლო.

ინტერნეტტექნოლოგიებმა მსოფლიოში სხვადასხვა მიმართულებით მოახდინა დიდი გავლენა ფართო მასებზე. ინტერნეტის შექმნის თავდაპირველი მიზანი სამეცნიერო-კვლევითი საქმიანობისთვის უფრო ხელსაყრელი პირობების შექმნა იყო. ამ უდიდესი სისტემათა სისტემის უსაფრთხოება კი მხოლოდ შემდგომ იქცა მნიშვნელოვან გამოწვევად. ახალი ინფორმაციული სივრცის წარმოშობამ ასევე მსოფლიოს ერთიან აღქმას შეუწყო ერთგავრად ხელი. ეს არის სივრცე, სადაც პოლიტიკური საზღვრები არ არსებობს.

ახალი გამოწვევები

ახალი ვირტუალური განზომილების შექმნიდან სულ რაღაც რამდენიმე ათეული წლის შემდეგ, 2010 წელს, ჩრდილოატლანტიკური ალიანსის (ნატო) ახალი სტრატეგიული კონცეფციის რეკომენდაციების ავტორები წერენ, რომ „შემდეგი მნიშვნელოვანი შეტევა ალიანსზე შესაძლოა ოპტიკურ-ბოჭკოვანი კაბელის მეშვეობით

განხორციელდეს“, ანუ ინტერნეტის საშუალებით.[3] ნატოს ახალი სტრატეგიული კონცეფცია ასევე ხაზს უსვამს შემდეგ გარემოებას, „კიბერშეტევები გახდა უფრო ხშირი, უფრო ორგანიზებული და უფრო მეტი ზიანის მომტანი მთავრობების, ბიზნესის, ეკონომიკისთვის, აგრეთვე ტრანსპორტირებისა და მიწოდების ქსელებისთვის და სხვა კრიტიკული ინფრასტრუქტურისთვის; ამგვარი შეტევები საფრთხეს უქმნის ეროვნულ და ევროატლანტიკურ კეთილდღეობას, უსაფრთხოებას და სტაბილურობას“.[4] არსებული რეალობიდან გამომდინარე ისმის კითხვა: შეგვიყვანა თუ არა ჩიხში უსაფრთხოების თვალსაზრისით ჩვენმა საკუთარმა ტექნოლოგიებმა?!

დღეს სახელმწიფოებს და, განსაკუთრებით, განვითარებულ ქვეყნებს უწევთ ახალ, უფრო რთულ საფრთხეებთან გამკლავება. კიბერმზვერავებმა, კიბერჯარისკაცებმა, კიბერტერორისტებმა, ერთი ან რომელიმე ძალის, იდეოლოგიის მხარდამჭერმა ჯგუფებმა ვირტუალურ სამყაროში დაიდეს ბინა.

კიბერსაფრთხეები არა მარტო ტექნოლოგიურად განვითარებულ ქვეყნებს, არამედ ნაკლებად განვითარებულ ქვეყნებსაც ემუქრება. პოტენციური სამიზნე ქვეყნები კიბერუსაფრთხოებას სერიოზულად უდგებიან. ქვეყნები, თავისი კულტურული, სოციალური, ეკონომიკური, გეოგრაფიული და პოლიტიკური მდგომარეობის შესაბამისად აყალიბებენ კიბერპოლიტიკას. ეძებენ ეფექტურ გზებს, ქმნიან და ცვლიან სტრატეგიულ დოკუმენტებს, ტაქტიკას და მიდგომის მეთოდებს.

ყოველდღიურად ხდება კიბერდანაშაული ინდივიდების, სხვადასხვა ბიზნესისა თუ მთავრობის წინააღმდეგ. კიბერომი უკვე წარმოადგენს საფრთხეს, რომლის წინააღმდეგაც ეროვნული უსაფრთხოების ექსპერტები ეძიებენ უფრო ეფექტურ, თანმიმდევრულ სტარტეგიებსა და საერთაშორისო შეთანხმებებს.

კიბერთავდასხმები შესაძლოა იყოს სპეცოპერაციებისა და საჰაერო თავდასხმების ეკვივალენტური. სპეციალური დანიშნულების რაზმების ან საჰაერო ძალების გაწვრთნისა და აღჭურვისათვის საჭირო ფინანსურ და ადამიანურ რესურსებთან შედარებით ჰაკერები, კომპიუტერები და ბოტნეტები თუ სხვა სახის კიბერ და ინფორმაციული იარაღის შექმნა გაცილებით მცირე დროსა და სახსრებს მოითხოვს. ამან შესაძლოა საფრთხე შეუქმნას ქვეყნის კრიტიკულ ინფრასტრუქტურას, ეკონომიკას და მოსახლეობის ფსიქოლოგიურ მდგომარეობას. კიბერიარაღის გამოყენება მეტო-

ქის წინააღმდეგ გაცილებით იაფია, ვიდრე სამხედრო-პოლიტიკური ინტერვენცია. „თქვენ შეგიძლიათ დააფინანსოთ მთლიანი კიბერომის კამპანია იმავე თანხად, რაც ტანკის მუხლუხოს გამოცვლა დაგიჯდებათ, ასე რომ, უგუნური იქნებით, ასე რომ არ მოიქცეთ“, განაცხადა ბილ ვუდკოკმა, არასამთავრობო ორგანიზაცია *Packet Clearing House*-ის კვლევების დირექტორმა.[5] კიბერკრიმინალურმა დაჯგუფებებმა და კიბერდამნაშავე ქვეყნებმა შესაძლოა მცირედი დანახარჯებით განახორციელონ სამიზნე ქვეყნის ეკონომიკისა და მისი მნიშვნელოვანი ინფრასტრუქტურის დესტაბილიზაცია. ექსპერტები დღემდე დაობენ იმასათან დაკავშირებით, თუ როგორი განსაზღვრება უნდა მიეცეს კიბერშეტევებს – როგორც კრიმინალური ქმედება თუ როგორც საომარი ქმედება?

მსოფლიოში ისეთი ბერკეტის არსებობისას, როგორიც ინტერნეტია, კომპიუტერული უნარებით აღჭურვილი აქტიური ადამიანებისგან ხშირად ყალიბდებიან კარგად გაწვრთნილი ჰაკტივისტები, ჰაკერ-ტერორისტები და ჰაკერ-მებრძოლები და ისინი მთელ მსოფლიოში არიან გაბნეული.

აქვე უნდა აღინიშნოს, რომ კიბერ საფრთხეები ემუქრება არა მხოლოდ ღია სისტემას, არამედ ასევე საშიშროებას ქმნის დახურული სისტემისთვისაც. არც დახურული სისტემები – ქსელები, რომლებიც პირდაპირ არ არიან დაკავშირებული ინტერნეტთან – არიან სრულად დაცული. ამას სტაქსნეტის და ვიკილიქსის მაგალითებიც ცხადყოფს: ერთმა – ჭია ვირუსმა, რომელმაც გაანადგურა ათასი ცენტრიფუგა ნათანზის ბირთვულ ელექტროსადგურზე, და მეორემ – აშშ-ის არმიის ყოფილი რიგითი ჯარისკაცის ბრედლი მენინგის მიერ ვებგვერდ „ვიკილიქსისათვის“ ათიათასობით აშშ-ის სახელმწიფო საიდუმლო დოკუმენტის გადაცემით – უდიდესი საფრთხის წინაშე დააყენა ამერიკის სახელმწიფო უსაფრთხოება. ინტერნეტი არ არის ერთადერთი გზა კომპიუტერულ სისტემებში შესაღწევად, თუმცა ეს არის ფართო და გახსნილი გზა.

ინფორმაციულმა სივრცემ ასევე ხელი შეუწყო აქტიური და მეამბოხე ინტერნეტთაობის შექმნას. სწორედ ამ სივრცის აქტიური გამოყენების შედეგად მოხდა შესაძლებელი სახალხო მობილიზაცია სხვადასხვა ქვეყანაში. პოლიტიკურმა აქტივობებმა, დებატებმა კიბერსივრცეში, სოციალურ მედიაში გადაინაცვლა. სწორედ სოციალურმა მედიამ მისცა ბიძგი მასობრივ გამოსვლებს არაბულ ქვეყნებში. ამ სივრცის აქტიური გამოყენების შედეგად მოხდა

შესაძლებელი 10 დეკემბრის სახალხო მობილიზაციაც რუსეთში, როდესაც ათიათასობით ადამიანმა გააპროტესტა 2011 წლის საპარლამენტო არჩევნების შედეგები.

ინტერნეტის ფართოდ გამოყენება კონფლიქტურ სიტუაციაში პირველად 90-იანი წლების ჩეჩნეთის ომის დროს განხორციელდა. ჩეჩნებმა იმდენად ეფექტურად მოახერხეს ამ სივრცის გამოყენება, რომ მოგვიანებით რუსეთის პრეზიდენტმა ვლადიმერ პუტინმა ასეთი რამ განაცხადა: „ჩვენ მივატოვეთ და უგულებელვყავით ეს სივრცე... მაგრამ ახლა ამ თამაშში დაუყოვნებლივ უნდა ჩავერთოთ“.[6] ჩეჩნები კარგად ახერხებდნენ გავლენიან დასავლელ ჟურნალისტებთან დაკავშირებას და მათთვის ინფორმაციის მიწოდებას. ისინი ინფორმაციას მანამდე აწვდიდნენ, სანამ რუსული პროპაგანდისტული მანქანა თავის ვერსიას გაავრცელებდა. ჩეჩნები განსაკუთრებით კარგად გაიწაფნენ რუსების მიერ ჩადენილი ძალადობრივი მოქმედებების ამსახველი სურათების გავრცელებაში. რუსული მხარე, ცხადია, ამ ფაქტების არსებობას საჯაროდ უარყოფდა. ჩეჩენი სეპარატისტების წარმატებად ითვლება ისიც, რომ მათ მხარდამჭერებისგან თავიანთ კალიფორნიის საბანკო ანგარიშზე ფულის მოზიდვაც კი შესძლეს.[7] მას შემდეგ ინტერნეტის გამოყენება ე.წ. „წესად“ იქცა თითქმის ყველა სახის კონფლიქტში. არატრადიციული ძალების კონფლიქტებში ჩართვამ მსოფლიო მასშტაბით არაერთგვაროვანი რეაქცია და გამოძახილი ჰპოვა. დამკვიდრდა ინტერნეტის ფართოდ გამოყენებისა და ჩართულობის ახალი ტრენდი. თუმცა საზოგადოებას ამ სივრცის კონფლიქტურ სიტუაციებში გამოყენების მაქსიმუმი ჯერ არ უნახავს.

ინტერნეტის საომარ მოქმედებებში გამოყენება თანამედროვე მეთოდია და მასში ხშირად არიან ჩართული რიგითი მოქალაქეები თუ კიბერსაომარი საშუალებებით შეიარაღებული ან ნაწილობრივ შეიარაღებული მებრძოლები. ასეთ განვითარებას სამი სახის შედეგი აქვს: პირველი – სხვადასხვა ჯგუფი, რომლებიც სახელმწიფოს სახელით არ მოქმედებენ. მეორე – სახელმწიფო ძალები გადადიან მოქმედების ახალ სტრატეგიებზე და ქმნიან ან იყენებენ კიბერმებრძოლთა ჯგუფებს და მესამე – ინტერნეტის მეშვეობით იწყება ახალი სახის მებრძოლთა ტიპის ჩამოყალიბება, რასაც ინდივიდუალური კიბერმებრძოლები ეწოდება. ზოგიერთი ქვეყნის მთავრობას არა მხოლოდ შემწყნარებლური დამოკიდებულება აქვს კიბერკრიმინალური დაჯგუფებების მიმართ, არამედ ქირაობს

კიდეც მიზანში ამოღებული ქვეყნების წინააღმდეგ. მაგალითად, 2008 წელს საქართველოზე განხორციელებულ კიბერთავდასხმებში ერთ-ერთ მთავარ აქტორად მიიჩნევა რუსული ბიზნესქსელი (RBN). რუსული ბიზნესქსელი იყო და შესაძლოა, კვლავაც არის კიბერ-კრიმინალების ჯგუფი, რომელთაც მჭიდრო კავშირები აქვთ რუსეთის მთავრობასთან, – განუცხადა „გლობალური სტრატეგიული პარტნიორობის“ წარმომადგენელმა შტეფან სპონამორმა *Internet news.Com*-ს.[8]

რევიზიონისტული ქვეყნებისთვის, მაგალითად, როგორიცაა რუსეთი და ჩინეთი, კიბერშპიონაჟი წარმოადგენს სტატუს-კვო სახელმწიფოზე (აშშ) ეკონომიკური და სამხედრო-ტექნოლოგიური უპირატესობის მოპოვების მთავარ საშუალებას, ხოლო ქვეყნის შიგნით ინფორმაციული კონტროლი, კიბერრეპრესიები, არადემოკრატიული საკანონმდებლო ინიციატივები – სოციალური და პოლიტიკური წესრიგის დაცვის მნიშვნელოვან ბერკეტს. სუბნაციონალური ძალები, როგორიცაა ალ-ქაიდა და ანონიმუსი, ასევე წარმოადგენენ რევიზიონისტულ ძალებს. თუმცა, მიუხედავად რადიკალური განსხვავებისა, ზემოთ მოყვანილ ქვეყნებთან შედარებით, მათ აქვთ ერთი საერთო შეხედულება აშშ-ისა და მისი მოკავშირეების დომინანტური პოზიციების შერყევის თაობაზე. თანამედროვე ეპოქაში საერთაშორისო პოლიტიკურ ასპარეზზე კიბერნეტიკული სიძლიერე იქნება ამ დომინანტური როლის ერთ-ერთი განმსაზღვრელი წინაპირობა. კიბერტექნოლოგიები რუსეთისა და ჩინეთისთვის წარმოადგენს რევიზიონისტული მიზნების განხორციელებისათვის უმნიშვნელოვანეს საშუალებას. ალ-ქაედა ამ ტექნოლოგიებს კველივისთვის, ინფორმაციის შენახვისა და კომუნიკაციის საშუალებად იყენებს. ანონიმუსი კი იდეოლოგიურ-წინააღმდეგობრივი დამოკიდებულების გამოსახატავად პირდაპირ კიბერთავდასხმებს მიმართავს.

ყოველდღიურად იქმნება უამრავი სხვადასხვა ტიპის კიბერ- და ინფორმაციული იარაღი, რომელიც მიმართულია ინდივიდების, მთავრობების და ორგანიზაციების წინააღმდეგ. ამჟამად საერთაშორისო საზოგადოება, ან მისი ნაწილი მაინც, ეძებს ეფექტურ გზებს კიბერშეტევებთან საბრძოლველად, თუ რომელია ყველაზე ეფექტური ტექნიკური, იურიდიული და პოლიტიკური სტრატეგია ამ საფრთხის წინააღმდეგ და სად გაავლონ ზღვარი დანაშაულსა და ომს შორის.

საქართველო კიბერსივრცეში

ზოგიერთ ქვეყანაში თითქმის ყველაფერი ინტერნეტთანაა დაკავშირებული, მაგრამ საქართველო ისე არ არის ინტერნეტიზირებული, როგორც, მაგალითად, გერმანია, საფრანგეთი, ამერიკის შეერთებული შტატები და სხვა განვითარებული ქვეყნები. ასეთ გარემოში კომფორტი მცირეა, თუმცა საქართველო ამ გლობალურ სისტემათა სისტემის ნაწილია და მისი კრიტიკული ინფრასტრუქტურაც მეტწილად ინტერნეტზეა დამოკიდებული. ინფორმაციული სივრცე სინათლის სიჩქარით სცდება დაწესებულ ეროვნულ საზღვრებს, სტანდარტებს კი ტექნოლოგიური ლიდერები აწესებენ. მაგალითად, უსაფრთხოების სტანდარტებს, რომელსაც საქართველოს ბანკები უნდა აკმაყოფილებდნენ, რა თქმა უნდა, ადგენენ არა თავად ეს ბანკები, არამედ განსაზღვრულია მსხვილი ბანკების მიერ ფრანკფურტში, ლონდონსა და ნიუ-იორკში. აქვე მნიშვნელოვანია აღინიშნოს იმ საერთაშორისო ბანკების გადაწყვეტილებების შესახებ, რაც ქართულ ბანკებთან დაკავშირებით მიიღეს 2008 წელს, საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევების დროს. *InternetNews.com*-ზე კენეტ კორბინი ამ ფაქტთან დაკავშირებით წერს: „თავდამსხმელებმა საქართველოს საბანკო სისტემაზე ისეთი მასშტაბური შეტევები განახორციელეს, რომ შეუძლებელი გახდა სისტემის უსაფრთხოების უზრუნველყოფა. გააცნობიერეს რა, რომ სისტემა შეტევის ქვეშ იმყოფებოდა, საერთაშორისო ბანკებმა შეწყვიტეს მომსახურება. ყოველივე ამის შედეგად საქართველოს ბანკებმა რამდენიმე დღით შეაჩერეს ქვეყნის მასშტაბით ტრანზაქციების შესრულება“.[9] ამავე პრინციპით თბილისის საერთაშორისო აეროპორტიც უნდა აკმაყოფილებდეს საჰაერო ტრანსპორტის საერთაშორისო ასოციაციის მიერ (IATA) დადგენილ სტანდარტებს.

გლობალური სისტემების გათვალისწინებით და ამ თვალსაზრისით დაწესებული საერთაშორისო სტანდარტების მიხედვით, მაგალითად, საბანკო და საჰაერო სისტემების უსაფრთხოების მიზნით, ქვეყნები ვალდებული არიან, დადგენილი ნორმების შესაბამისად, მიიღონ კიბერუსაფრთხოებისათვის სათანადო ზომები.

ბევრი სხვა უფრო მნიშვნელოვანი პროცესი კონტროლდება ინდუსტრიული კონტროლის სისტემების მეშვეობით, რომელთა უმრავლესობა ინტერნეტის ქსელშია ჩართული. ინდუსტრიული კონ-

ტროლის სისტემის ექსპერტი ჯოზეფ ვაისი წერს: „ინდუსტრიული კონტროლის სისტემები მართავს ინდუსტრიულ ინფრასტრუქტურას მსოფლიოში, მათ შორის ელექტროსადგურებს, გაზის, წყლის, ნავთობის მიწოდებისა და გადამუშავების პროცესებს, ტრანსპორტირების და სხვა მრავალ სისტემას".[10] იმის გათვალისწინებით, რომ ნებისმიერი სასიცოცხლოდ მნიშვნელოვანი პროცესი, რომელიც აღნიშნული სისტემით კონტროლდება და ინტერნეტქსელშია ჩართული, მოწყვლადია კიბერშეტევების მიმართ.

2010 წლის სექტემბერში გამოქვეყნებული საქართველოს საფრთხეების შეფასების დოკუმენტის მესამე ნაწილში, რომელიც ტრანსნაციონალურ საფრთხეებს ეხება, კიბერთავდასხმებისგან მომდინარე საფრთხეებიცაა მიმოხილული. დოკუმენტში წერია, რომ „2008 წლის აგვისტოს ომის დროს რუსეთის ფედერაციამ, სახმელეთო, საჰაერო და საზღვაო თავდასხმების პარალელურად, განახორციელა მიზანმიმართული, მასობრივი კიბერშეტევები საქართველოზე", რომელმაც გვიჩვენა, რომ „ინფორმაციული ტექნოლოგიების გამოყენება კიბერშეტევების განსახორციელებლად წარმოადგენს რეალურ საფრთხეს გლობალიზებულ სამყაროში".[11] სწორედ 2008 წლის რუსეთის კიბერშეტევამ, რომელიც კინეტიკური ომის პარალელურად განხორციელდა, ერთგვარი ბიძგი მისცა საქართველოს მთავრობას გარკვეული ნაბიჯები გადაედგა ამ მიმართულებით. 2008 წელს რუსეთმა თავდასხმები როგორც საბჭოთა პერიოდის ტანკებით, ისე 21-ე საუკუნის ოპტიკურ-ბოჭკოვანი კაბელის მეშვეობით განახორციელა. კიბერშეტევებმა რამდენიმე დღით საქართველოში გათიშა მთავრობის საინფორმაციო და საკომუნიკაციო საშუალებები, ახალი ამბების პორტალები, ფინანსური ტრანსაქციები და ინტერნეტკავშირი. კიბერსივრცეში განხორციელებულმა შეტევებმა შეასრულა ის მისია, რომელსაც მანამდე ავიაცია და არტილერია ასრულებდა. 2008 წლის მწარე გამოცდილების შემდგომ საქართველოს მთავრობამ რიგი თანმიმდევრული ნაბიჯები გადადგა საქართველოს კიბერსივრცის უსაფრთხოების თვალსაზრისით. ძალაში შევიდა „კანონი ინფორმაციული უსაფრთხოების შესახებ", რომელიც განსაზღვრავს ინფორმაციული უსაფრთხოების სტანდარტებს კერძო და საჯარო ორგანიზაციებისათვის. 2010 წელს შეიქმნა იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტო, რომლის მთავარ მიზანს წარმოადგენს საქართველოში ელექტრონული მმართველობის განვი-

თარება, მონაცემთა გაცვლის ინფრასტრუქტურის შექმნა და ერთიანი სამთავრობო ქსელის ჩამოყალიბება. სააგენტო ასევე უფლებამოსილია საჯარო სექტორში ინფორმაციულ და საკომუნიკაციო სფეროსთან დაკავშირებული სტანდარტების შემუშავების, ინფორმაციული უსაფრთხოების პოლიტიკის ჩამოყალიბებისა და მისი გატარების თვალსაზრისით".[12] ამავე სააგენტოს დაქვემდებარებაში შეიქმნა კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფი (CERT). კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი მუშაობს კვირაში შვიდი დღე, 24 საათის განმავლობაში. როგორც ჯგუფის ოფიციალურ ვებგვერდზეა მითითებული, ის უფლებამოსილია განახორციელოს საქართველოს კიბერსივრცის მონიტორინგი და რეაგირება მოახდინოს საქართველოს სამთავრობო ქსელსა და კრიტიკულ ინფრასტრუქტურაში დაფიქსირებულ კომპიუტერულ ინციდენტებზე.[13] ქვეყნის ინტერნეტტრაფიკის დიდი ნაწილი 2008 წლის აგვისტოს ომის დროს რუსეთის გავლით გადიოდა, აგვისტოს მოვლენების შემდგომ კი ფოთი-ვარნას ახალი დამაკავშირებელი მაგისტრალი ოპტიკურ-ბოჭკოვანი კაბელი „კავკასია" ინტერნეტტრაფიკის დაახლოებით 90%-ს ფარავს.

2013 წლის 17 მაისს საქართველოს პრეზიდენტმა ხელი მოაწერა საქართველოს კიბერუსაფრთხოების სტრატეგიას და კიბერუსაფრთხოების სტრატეგიის სამოქმედო გეგმას. დოკუმენტი მოუწოდებს სახელმწიფო უწყებებს გამართული, კოორდინირებული მუშაობისაკენ და სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის მექანიზმების შემუშავებისაკენ. დოკუმენტი ასევე ხაზს უსვამს საერთაშორისო თანამშრომლობის აუცილებლობას და საგანმანათლებლო ბაზის ჩამოყალიბებას. სამოქმედო გეგმა განსაზღვრულია 2015 წლის ჩათვლით.[14]

ცოტა ხნის წინ ქართულმა CERT-მა საერთაშორისო აღიარება მოიპოვა საქართველოს წინააღმდეგ მიმართული კიბერშპიონაჟისათვის შექმნილ Win32/Georbot ვირუსის აღმოჩენისა და რეაგირებისათვის. ვირუსი გამოირჩეოდა კომპიუტერულ სისტემებში მაღალი შეღწევადობის უნარით და შეეძლო ნებისმიერი სახის დოკუმენტზე მართლსაწინააღმდეგო წვდომა, მფლობელისგან დამოუკიდებლად პერსონალური კომპიუტერის მეშვეობით აუდიო- და ვიდეოჩანაწერების გაკეთება, ასევე, მომხმარებლის კომპიუტერის სამუშაო დაფის გადაღება და ყველა ამ ინფორმაციის გადაგზავნა ვირუსის მმართველ კომპიუტერზე. ვირუსის სამიზნეები იყო

სახელმწიფო და კრიტიკული ინფრასტრუქტურის კომპიუტერული ქსელები. ასევე რამდენიმე შემთხვევაში დაინფიცირდა საბანკო სექტორის, არასამთავრობო ორგანიზაციებისა და კერძო კომპანიების კომპიუტერები.[15] Georbot-ის მიზანი იყო აღმოეჩინა და მოეპარა ის დოკუმენტები, რომლებშიც გამოყენებული იყო უსაფრთხოებასთან ასოცირებული სიტყვები და შემდგომ ამ მონაცემების გაგზავნა საკონტროლო სერვერთან. საქართველოს CERT-მა შექმნა და დააინფიცირა ყალბი დოკუმენტი თავდამსხმელის შეცდომაში შეყვანის მიზნით და შედეგად შესაძლებელი გახადა შემტევის იდენტიფიცირება. ქართულმა CERT-მა უკუსვლითი ინჟინერული პროცესის გამოყენებით მოიპოვა სრული წვდომა მართვისა და კონტროლის სერვერებზე, გაშიფრა კომუნიკაციების მექანიზმები და გაანალიზა ვირუსული ფაილები. მიღებული ინფორმაციის საფუძველზე მოხერხდა პირების, ორგანიზაციების იდენტიფიცირება. საგამოძიებო მოქმედებების ჩატარების შემდგომ გამოიკვეთა რუსი ჰაკერებისა და სახელმწიფო ორგანიზაციების კვალი.[16]

2012 წლის 6 ივნისს საქართველომ მოახდინა ევროპის საბჭოს „კიბერდანაშაულის შესახებ კონვენციის“ რატიფიცირება. ამ კონვენციას საქართველომ 2008 წელს მოაწერა ხელი, თუმცა კონვენცია მოითხოვს არა მარტო საერთაშორისო თანამშრომლობას კიბერსაგამოძიებო მოქმედებების ჩატარების მიზნით, არამედ საქართველოს კანონმდებლობის ჰარმონიზაციას კონვენციით დადგენილ ნორმებთან. კონვენციის რატიფიცირების დაჩქარებას ხელი შეუწყო „ინფორმაციული უსაფრთხოების შესახებ კანონის“ მიღებამ. აღნიშნული კონვენცია ძალაში შევიდა 2012 წლის 1 ოქტომბერს.[17] ცხადია, 2008 წლის შემდგომ დღემდე საქართველომ მნიშვნელოვანი ნაბიჯები გადადგა კიბერუსაფრთხოების თვალსაზრისით, თუმცა ამ უდიდესი პრობლემის წინააღმდეგ ბრძოლა მოითხოვს მიზანმიმართული, თანმიმდევრული კიბერპოლიტიკის განხორციელებას, რომლის პრიორიტეტულობა სახელმწიფო დონეზე იქნება აყვანილი. ამ პრობლემასთან ეფექტური ბრძოლა იმავდროულად მოითხოვს ქვეყნის შიგნით სათანადო ზომების მიღებას – არის თუ არა სამთავრობო კომპიუტერული ქსელი შესაბამისი პროგრამული უზრუნველყოფით აღჭურვილი, აქვს თუ არა სამთავრობო კომპიუტერებს სათანადო უსაფრთხოების სისტემა და გააცნეს თუ არა სამთავრობო უწყების წარმომადგენლებს ელემენტარული, საბაზისო წესები კიბერუსაფრთხოების თაობაზე. აუცილე-

ბელია როგორც სამთავრობო, ასევე ბიზნესორგანიზაციებს შორის თანამშრომლობის გაღრმავება, საგანმანათლებლო პროგრამების ფართოდ განხორციელება და საზოგადოებრივი ცნობიერების ამაღლება. მნიშვნელოვანია მაღალი სტანდარტების შეტევების პრევენციის სენსორული სისტემების დანერგვა, ფართო მასშტაბის კიბერკონტრდაზვერვის გეგმისა და თავდაცვითი სტრატეგიების შემუშავება. ამ თვალსაზრისით პრიორიტეტულია უწყებათაშორისი კოორდინაცია და კომუნიკაცია. მნიშვნელოვანია ქვეყნის შიგნით საკანონმდებლო ბაზის არა მარტო შემუშავება, არამედ აღსრულება. ამ პრობლემასთან გამკლავება ასევე საჭიროებს მჭიდრო საერთაშორისო თანამშრომლობას.

დასკვნა

ინტერნეტის შექმნის თავდაპირველი მისია არ მოიაზრებდა უსაფრთხოების ზომების შემუშავებას. ინტერნეტის შექმნა განპირობებული იყო სამეცნიერო საქმიანობისათვის უფრო ხელსაყრელი გარემოს შესაქმნელად. დღეს კომპიუტერული ქსელების დაცულობა მუდმივად მოითხოვს ახალი უსაფრთხოების ზომების გატარებასა და უზრუნველყოფას.

ინტერნეტის შემქმნელები ვერასოდეს წარმოიდგენდნენ, რომ ინტერნეტტექნოლოგიების მზარდი განვითარება წარმოშობდა ისეთ მასშტაბურ სისტემათა სისტემას, რომლის უსაფრთხოება ესოდენ მნიშვნელოვან გამოწვევად იქცეოდა. ამ ძნელად კონტროლირებად სივრცეში, ბევრ სარგებელთან ერთად, გაჩნდა ახალი საფრთხეები, ახალი გამოწვევები. ხალხმა და ფულმა გადაინაცვლა კიბერსამყაროში. შესაბამისად, კრიმინალმა, შპიონაჟმა, ტერორმა და ომმა ადგილი ახალ სივრცეში იპოვა.

ამ უდიდესმა ტექნოლოგიამ გაზარდა მთავრობების, ბიზნესისა და ინდივიდების დამოკიდებულება ინტერნეტზე და თითქმის ყველაფრის კომპიუტერიზაცია მოითხოვა. კიბერრეალობამ შექმნა ახალი გამოწვევები, ამასთან, არა მხოლოდ ტექნიკური, არამედ პოლიტიკური და სამართლებრივი თვალსაზრისითაც.

მსოფლიო სულ უფრო მეტად ხდება ინტერნეტზე დამოკიდებული, ქვეყნები მისგან სარგებელსაც იღებენ, მაგრამ შეიძლება ასევე აღმოჩნდნენ მისი ბოროტად გამოყენების მსხვერპლიც. ვერც ერთი ქვეყანა, მიუხედავად მისი სიდიდისა თუ რესურსებისა, ვერ შეძლებს ინფორმაციული ტექნოლოგიების უგულებელყოფას.

მაგალითად, 2008 წელთან შედარებით, საქართველოს დამოკიდებულება ინტერნეტტექნოლოგიებზე მნიშვნელოვნად გაიზარდა, რამაც გაზარდა არა მარტო მისი კიბერსივრცის უსაფრთხოების მნიშვნელობა, არამედ მისი ხვედრითი წილი და პასუხისმგებლობა გლობალური კიბერსივრცის უსაფრთხოების თვალსაზრისითაც.

გამოყენებული წყაროები

1 *Internet World Stats*, "Usage and Population Statistics." Undated. Retrieved from www.internetworldstats.com/stats.htm on August 10, 2013

2 Leiner, Barry, Vincent Cerf, et.al., *A Brief History of the Internet,* The Internet Society, undated.Retrieved from www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet on August 8, 2013

3 North Atlantic Treaty Organization, *NATO 2020: Assured Security; Dynamic Engagement, Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO,* Brussels, 17 May 2010, p. 45. Retrieved from www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf on August 7, 2013

4 NATO, *Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon,* November 19, 2010. Retrieved from www.nato.int/cps/en/natolive/official_texts_68580.htm on August 10, 2013

5 Markoff, John, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008. Retrieved from www.nytimes.com/2008/08/13/technology/13cyber.html, on August 4, 2013.

6 Geers, Kenneth, "Cyberspace and the Changing Nature of Warfare," *SC Magazine,* August 27, 2008. Retreived from www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/ on August 5, 2013

7 Geers, Kenneth, "Cyberspace and the Changing Nature of Warfare," *SC Magazine,* August 27, 2008. Retrieved from www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/ on August 8, 2013

8 Corbin, Kenneth, "Lessons From the Russia-Georgia Cyberwar," Internetnews.com, March 12, 2009. Retrieved from www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm on August 10, 2013

9 Corbin, Kenneth, "Lessons from the Russia-Georgia Cyberwar," *InternetNews.com,* March 12, 2009.Retrieved from www.internetnews.com/government/article.php/3810011/Lessons+From+the+RussiaGeorgia+Cyberwar.htm on August 4, 2013

10 Weiss, Joseph, *Protecting Industrial Control Systems from Electronic Threats*. New York: Momentum Press, 2010.

11 Melikishvili, Alexander, "Georgia's New Threat Assessment Document identifies Russia as a Main Threat," *Eurasia Daily Monitor,* October 25, 2010. Retrieved from www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=37077&tx_ttnews%5BbackPid%5D=27&cHash=3ebccbc084, on August 10, 2013.

12 მონაცემთა გაცვლის სააგენტო. იხ. შემდეგი ბმული: www.dea.gov.ge/?action=page&p_id=5&lang=geo. მოძიებულია 2013 წლის 5 აგვისტოს.

13 მონაცემთა გაცვლის სააგენტო, *CERT.GOV.GE*. იხ. ბმული: www.dea.gov.ge/?action=page&p_id=120&lang=eng მოძიებულია 2013 წლის 5 აგვისტოს.

14 საქართველოს პრეზიდენტის ბრძანებულება საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013-2015 წწ. სამოქმედო გეგმის დამტკიცების შესახებ. 17 მაისი, 2013. იხ. ბმული: www.nsc.gov.ge/files/files/legislations/kanonqvemdebare%20normatiuli%20aqtebi/cyber%20security%2017%20may.pdf მოძიებულია 2013 წლის 10 აგვისტოს.

15 მონაცემთა გაცვლის სააგენტო, *„კიბერშპიონაჟი საქართველოს წინააღმდეგ“*, 24 ოქტომბერი, 2012. იხ. შემდეგი ბმული და მასზე მბმული PDF ფაილი: http://dea.gov.ge/uploads/CERT%20DOCS/CERT.GOV.GE.pdf მოძიებულია 2013 წლის 5 აგვისტოს.

16 იგივე წყარო.

17 Council of Europe, Treaty Office, *Convention on Cybercrime,* undated. Retrieved from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG on August 10, 2013