საქართველო და კიბერუსაფრთხოება

ზურაბ გორგოძე

წინასიტყვაობა

კიბერსივრცის ტერმინის განსაზღვრების ბევრი ვარიანტი არსებობს, თითოეული მათგანი იძლევა თავისებურ განმარტებას, თუმცა ყველა განმარტებაში მოცემულია, რომ კიბერსივრცე - ეს არის ინფორმაციული და ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირში არსებული კომპლექსი, სადაც შედის გლობალური ინტერნეტისა და ტელეკომუნიკაციის ქსელები, კომპიუტერული სისტემები, ასევე ჩართული პროცესორები, სერვერები და მაკონტროლირებელი მოწყობილობები, რომლებიც გამოიენება მრეწველობის სხვადასხვა დარგში.

უკანასკნელი ათწლეულების განმავლობაში განხორციელებული კონფლიქტების ანალიზი ცხადყოფს, რომ კიბერუსაფრთხოება ყველა კონფლიქტისა და ომის განუყოფელი ნაწილია. იმის გათვალისწინებით,რომ ნატოსთვის კიბერუსაფრთხოება ერთ-ერთი მნიშვნელოვანი პრიორიტეტია და შესაბამისად განსაკუთრებულ აქცენტირებას ახდენს კიბერუსაფრთხოების განვითარებაზე, ალიანსის წევრობის მსურველი ყველა ქვეყანა, და მათ შორის საქართველოც, უნდა აცნობიერებდეს, რომ ერთობლივი საიმედო კიბერუსაფრთხოების საწყისი სწორედ საკუთარი ქვეყნის კიბერთავდაცვაა. ამ მხრივ მნიშვნელოვანია 2014 წლის ნატოს უელსის სამიტი, სადაც ნატომ კიბერთავდაცვა 16 პრიორიტეტში დაასახელა და განაცხადა, რომ მზად არის გამოცდილების გაზიარების მეტი შესაძლებლობები შესთავაზოს პარტნიორ ქვეყნებს და გააძლიეროს მათთან თანამშრომლობა მსოფლიო უსაფრთხოების სფეროში არსებული გამოწვევების ერთობლივად დასაძლევად, ვინაიდან ინტეგრაციის შემდეგ მათ მოუწევთ ერთიან სისტემაში მუშაობა და შესაბამისად უნდა ჰქონდეთ მზაობა მოცემულ საკითხში ბარიერების მარტივად გადასალახად.

შ ე ს ა ვ ა ლ ი

2008 წლის აგვისტოში რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ინტერნეტ სივრცეზე, გარკვეული პერიოდი დააპარალიზა სამთავრობო და კერძო სექტორის ვებ-გვერდები, რის შედეგადაც შეუძლებელი გახდა გარე სამყაროსთან კავშირი. ამ ყველაფერმა კი ცხადყო რომ ,,საქართველოს უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე''(პრეზიდენტის ბრძანებულება N321).

აღნიშნულმა კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა, ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სამხედრო თავდაცვა. შეიძლება ითქვას, რმ კიბერთავდასხმის საფრთხე გაუთანაბრდა სამხედრო თავდასხმისას და მეტიც, კიბერთავდასხმამ უფრო დიდი ზიანი შეიძლება მიაყენოს სახელმწიფოს ვიდრე კონფენსიური იარაღით თავდასხმამ.

2008 წლის აგვისტოს ომისა და მისი შედეგების გათვალისწინებით, რაც უკავშირდებოდა ქვეყნის დაუცველ კიბერსივრცეს, საქართველოს ხელისუფლება, დაიწყო სამართლებრივ-ნორმატიულ ბაზაზე მუშაობა მოცემული მიმართულებით, რის შედეგადაც 2013 წლის მაისში გამოქვეყნდა ,,საქართველოს კიბერუსაფრთხოების სტრატეგია'', რომელიც წარმოადგენს ეროვნული უსაფრთხოების მიმოხილვის პროცესის ფარგლებში შექმნილ კონცეპტუალური და სტრატეგიული დოკუმენტების პაკეტის ნაწილს. ახალი კიბერუსაფრთხოების სტრატეგია გამოქყვეყნებულ იქნა 2017 წლის იანვარში.

ეროვნული უსაფრთხოების კონცეფციის მიხედვით, საქართველო დიდ მნიშვნელობას ანიჭებს საიდუმლო ინფორმაციის უსაფრთხოების უზრუნველყოფას და სახელმწიფოს საინფორმაციო სისტემების დაცვას. დიდი მნიშვნელობა ენიჭება ასევე საქართველოს მეგობარ ქვეყნებთან თანამშრომბლობასა და მათი გამოცდილების გაზიარებას, მაგრამ უნდა გავითვალისწინოთ ისიც, რომ მეგობარიც შეიძლება ფარული მტერი აღმოჩნდეს.

1. კიბერუსაფრთხოების სტრატეგია და საქართველო

კიბერუსაფრთხოების პირველი სტრატეგია შემუშავდა ამერიკის შეერთებულ შტატებში, რომელმაც დაიწყო კიბერუსაფრთხოების აღქმა, როგორც სახელმწიფო მნიშვნელობის საკითხი. 2003 წლის აშშ-ის კიბერუსაფრთხოების ეროვნული სტრატეგია წარმოადგენს, უფრო ფართო ეროვნული უსაფრთხოების უზრუნველყოფის სტრატეგიის ნაწილს, რომელიც შეიქმნა 2001 წლის 11 სექტემბრის ტერორისტული თავდასხმის პასუხად. შემდეგ დაიწყო მისი აქტიური შემუშავება ევროპულმა ქვეყნებმაც.

2005 წელს გერმანია იღებს ინფორმაციული ინფრატსტრუქტურის დაცვის სახელმწიფო გეგმის შემუშავებას. 2006 წელს შვედეთი ამუშავებს ინტერნეტის უსაფრთხოების გაძლიერების სტრატეგიას, ესტონეთმა მისი კიბერუსაფრთხოების სტრატეგიის შემუშავება დაიწყო 2007 წელს, რუსეთის მხრიდან ქვეყანაზე განხორციელებული მასობრივი კიბერშეტევის შემდეგ და 2008 წელს, ევროკავშირის წევრ ქვეყნებს შორის, გახდა პირველი, რომელმაც გამოაქყეყნა კიბერუსაფრთხოების სახელმწიფო სტრატეგია. რაც შეეხება საქართველოს, 2008 წლის აგვისტოს ომის შემდეგ, რუსეთმა საქართველოზე მოახდინა მასობრივი კიბერშეტევა, რის შედეგადაც სახელმწიფო და კერძო სექტორები რამდენიმე დღე უმოქმედოდ იყვნენ, ამ დროს საჭირო იყო ისეთი პრეცედენტის ძიება, რომლის მეშვეობითაც მარტივი გახდებოდა პრობლემის აღმოფხვრა, ასეთი კი გახლდათ ესტონეთი, ვინაიდან მათ ჰქონდათ გამოცდილება რუსეთის მხრიდან კიბერთავდასხმისა და შესაბამისად საუკეთესო ვარიანტსად ისინი წარმოადგენდნენ. მათი ჩარევის შემდეგ პრობლემა გადაიჭრა, რის შედეგადაც შეჩერებულ და თავიდან აცილებულ იქნა მთლიანი ინფრასტრუქტურის განადგურება.

ზემოთ აღნიშნული თავდასხმა იყო მიზეზი ბიძგისა, რომლის შედეგიც გახლდათ 2013 წლის მაისში გამოქვეყნებული ,,საქართველოს კიბერუსაფრთხოების სტრატეგია''. ეს სტრატეგია ეფუძნება ,,საქართველოს საფრთხეების შეფასების დოკუმენტს'' და ,,საქართველოს ეროვნული უსაფრთხოების კონცეფციას''. დღეისათვის ეს სტრატეგია მოძველებულ დოკუმენტს წარმოადგენს, სწორედ ამიტომ საქართველოს მთავრობამ, 2017 წლის 13 იანვარს გამოსცა დადგენილება, სადაც შედის ინფორმაცია, საქართველოს კიბერუსაფრთხოების 2017-18 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ.

საქართველოს კიბერუსაფრთხოების 2017-18 წლების ეროვნული სტრატეგია წარმოადგენს ,,ეროვნული უსაფრთხოების'' მიმოხილვის პროცესის ფარგლებში შექმნილი კონცეპტუალური და სტრატეგიული დოკუმენტების პაკეტის ნაწილს, შესაბამისად, აღნიშნული სტრატეგია ეფუძნება ,,საქართველოს საფრთხეების შეფასების 2015-18 წლების დოკუმენტს'' და საქართველოს ეროვნული უსაფრთხოების კონცეფციას.

საქართველოს სახელმწიფოსა და მისი ინფორმაციული საზოგადოების განვითარება, თითოეული მოქალაქის სოციალური და ეკონომიკური კეთილდღეობა, მნიშვნელოვნად დამოკიდებულია ინფორმაციული სისტემებისა და ელექტრონული მომსახურებების უსაფრთხოების უზრუნველყოფაზე, კიბერშეტევები დიდ გავლენას ახდენს, ეკონომიკის ყველა სექტორზე, აფერხებს ეკონომიკური სფეროს გამართულ ფუნქციონირებას, ამცირებს ელექტრონული სერვისების მიმართ საზოგადოებრივ ნდობას და საფრთხეს უქმნის ინფორმაციული და საკომუნიკაციო ტექნოლოგიების გამოყენებით, ქვეყნის მდგრადი ეკომონიკური განვითარების მომავალს.

სტრატეგიის მიზანშეწონილად მოქმედების პროცესში, საქართველო ხელმძღვანელობს სხვადასხვა პრინციპებით, რომელთა შორის უმნიშვნელოვანესია :

- ადამიანის უფლებათა და ძირითად თავისუფლებათა განუხრელი დაცვა და პატივისცემა - საქართველოს ხელისუფლება ითვალისწინებს ადამიანის უფლებათა განუხრელი დაცვის პრინციპებს, ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და განხორციელების პროცესში.
- თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის - კიბერუსაფრთხოების უზრუნველსაყოფად, არანაკლებ მნიშვნელოვანია თანამშრომლობის მექანიზმის განვითარება, როგორც სახელმწიფო უწყებებს, ასევე კერძო სექტორებს შორის. დღეს-დღეობით სახელმწიფოსა და კერძო სექტორებს შორის მუშაობა დიდ პრობლემას წარმოადგენს არა მარტო ჩვენთან, არამედ ბევრ წამყვან ქვეყანაში. სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობა, აუცილებელი წინაპირობაა კიბერსივრცის უსაფრთხოებისთვის.
- აქტიური საერთაშორისო თანამშრომლობა - საქართველოს მთავრობა აცნობიერებს, რომ შეუძლებელია მხოლოდ საკუთარი რესურსებით უზრუნველყოს კიბერუსაფრთხოების სფეროში არსებულ გამოწვევებთან და საფრთხეებთან გამკლავება. საქართველო წარმოადგენს მსოფლიოს დემოკრატიული საზოგადოების ნაწილს და შესაბამისად მოწყვლადია იმ საფრთხეებისა და გამოწვევების მიმართ, რომლის წინაშეც ეს საზოგადოება დგას.

საქართველო დგას დემოკრატიზაციის გზაზე, რომლის მიზანიც გახლავთ ევროპულ და ევროატლანტიკურ სივრცეში ინტეგრაცია როგორიცაა NATO. ნატოს წესდების მე-10 მუხლის თანახმად ნებისმიერი ევროპული სახელმწიფო, რომელიც იზიარებს წესდების პრინციპებსა და მზადაა ხელი შეუწყოს ჩრდილოატლანტიკური სივრცის უსაფრთხოებას, ალიანსის წევრთა კონსესუსის შემთხვევაში შეიძლება გახდეს მისი წევრი. აქიდან გამომდინარე, საქართველომ აუცილებლად უნდა გაატაროს კონკრეტულ საკითხში, ისეთი ღონისძიებები, რომლებიც ხელს შეუწყობს მის ევროპეიზაციას, მაგრამ ეს დიდი ხნის პერსპექტივაა, ვინაიდან ჩვენს წინაშე დგას ისეთი პრობლემები და გამოწვევები, რომელთა არსებობაც ბინდს ფენს საქართველოს დემოკრატიული განვითარების პროცესს.

2. საქართველოს კიბერსივრცის წინაშე მდგარი პრობლემები და გამოწვევები

საქართველოს კიბერ უსაფრთხოების სტრატეგიის მიზანშეწონილად მუშაობის პროცესის პრინციპებს შორის წინამდებარე თავში დასახელებულ იქნა ისეთი პრინციპი, როგორიცაა : თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის, სადაც ვაწყდებით რიგ გამოწვევებს.

სახელმწიფო ეროვნული უსაფრთხოების უზრუნველყოფიდან გამომდინარე, ვალდებულია დაიცვას ქვეყნის მთლიანი ინფრასტრუქტურა არასანქცირებული შეღწევისაგან, მაგრამ ამისთვის არ ფლობს ყველა საჭირო რესურსს, ვინაიდან რესურსების დიდი ნაწილი კერძო სექტორის ხელშია. კერძო სექტორს არ გააჩნია არავითარი სამართლებრივი ვალდებულებები ითანამშრომლოს სახელმწიფოსთან და გამოაყენებინოს მის ხელთ არსებული რესურსი. ამ შემთხვევაში ჩვენ მივდივართ საჭირო საკანონმდებლო ბაზის არ არსებობის პრობლემასთან, რომელიც დაარეგულირებდა უკვე არსებული, თითოეული სუბიექტის, მონაცემთა გაცვლის სააგენტოს, კიბერუსაფრთხოების ბიუროსა და შსს კიბერდანაშაულთან ბრძოლის სამმართველოს ურთიერთკოორდინირებულ საქმიანობას.

კვლევის შედეგად, რომელიც სოხუმის სახელმწიფო უნივერსიტეტის ინფორმაციული ტექნლოგიების დეპარტამენტში 2017 წლის 23 მაისს ჩავატარე, მივიღე ინფორმაცია, რომლითაც ნათელი გახდა, რომ სოხუმის სახელმწიფო უნივერსიტეტი არ თანამშრომლობს სახელმწიფო სექტორთან, მიუხედავად ამისა სოხუმის სახელმწიფო უნივერსიტეტზე კიბერშეტევა დღემდე არ განხორციელებულა, მაგრამ ჩვენ არ ვართ დაზღვეულები, ვინაიდან რიკსი თანამედრივე ტექნოლოგიების სამყაროში დღითიდღე იზრდება, ასევე გასათვალისწინებელია ისიც, რომ სოხუმის სახელმწიფო უნივერსიტეტი ეროვნულ მიზნებს ემსახურება და რისკიც უფრო მაღალია.

საქართველოს კიბერსივრცეში არსებულ გამოწვევებს შორის უმნიშვნელოვანესია საზოგადოების ცნობიერების დაბალი დონე მოცემულ საკითხში. საზოგადოების ძალიან მცირე ნაწილმა იცის, თუ რა საფრთხე შეიძლება ახლდეს ინტერნეტში მუშაობის პროცესს, რაც კიდევ უფრო ზრდის კიბერსივრცესთან დაკავშირებულ რისკებს. აქვე აუცილებელია გამოვყოთ პერსონალური მონაცემების დაცვის საკითხი, რადგან დღეს ამ მიმართულებას ნაკლები ყურადღება ეთმობა, რაც ყოვლად დაუშვებელია, მაგრამ აქვე უნდა აღინიშნოს, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორის ოფისი იწყებს მუშაობას ახალ სტრატეგიაზე,სადაც, სავარაუდოდ, აისახება ყველა ის პრობლემური ასპექტი, რაც კიბერსივრცეში პიროვნების დაცვის საკითხს უკავშირდება. მე მსურს, რომ მიზერული წვლილი შევიტანო საზოგადოების კიბერსივრცეში დაცვასა და მათი ცნობიერების ამაღლებაში. კერძოდ, კიბერუსაფრთხოების ბიურო აფრთხილებს ანდროიდის სისტემაზე მომუშავე ელექტრონული მოწყობილობებს მფლობელებს, რომ შემდეგი აპლიკაციები :

- Quickpic - მობილური ტელეფონების ფოტოგალერეის მარტივად გამოსაყენებლი აპლიკაცია, რომელიც ჩინურმა კომპანია Cheetahs Mobile-მა შეიძინა, რომელმაც მომხმარებლის პერსონალური ინფორმაცია ფარულად, საკუთარ DNS, დომენურ სერვერებზე ატვირთა. დომენური სახელი, მარტივი ტექნიკური გაგებით, არის ინტერნეტ უნიკალური დასახელება, მისამართი, რომელიც მიუთითებს, ინდივიდის საიტზე ან ელ.ფოსტაზე, მისი მეშვეობით, ყველას შეუძლია ამა თუ იმ ადამიანის საიტისა და ელ.ფოსტის მოძებნა ინტერნეტში.

- ES File Explorer - ფაილების უფასო მენეჯერი, რომელიც განკუთვნილია მედია ფაილების მენეჯმენტისათვის, პროგრამა შეიცავს მავნე ტიპის რეკლამებს და მომხმარებლისგან ფარულად ითხოვს სხვადასხვა აპლიკაციების გამოყენებას.
- UC Browser – Google მარკეტის ერთ-ერთი ყველაზე პოპულარული აპლიკაცია, რომელიც მომხმარებელს სთავაზობს სწრაფ რეჟიმში მუშაობას. აპლიკაცია მონაცემებს დაუცველი სტანდარტით გზავნის, ის აგზავნის ცუფრულ კოდს, ანდროიდის ID-ს ჩინეთში განთავსებულ სხვადასხვა სერვერებზე.

საქართველოს კიბერსივრცეში არსებულ პრობლემებს შორის საკვანძო მომენტი გახლავთ ის, რომ ქვეყანას არ ჰყავს საკმარისი რაოდენობის საჭირო პროფესიული კადრები და სპეციალისტები, მაგ: ქვეყანაში არ არიან კიბერანალიტიკოსები, რომლებიც შეისწავლიდნენ მავნე ვირუსების ბუნებასა და ხასიათს, გააკეთებდნენ შესაბამის ანალიზს და მოამზადებდნენ სათანადო რეკომენდაციებს. ასევე არ არიან კიბერსამართლის დარგის სპეციალისტები, ქვეყანას არ ჰყავს კრიპტოგრაფები, რაც აუცილებელია კიბერთავდაცვითი საქმიანობის განვითარებისათვის, რადგან სწორედ სპეციალური კრიპტების დახმარებით იზრდება კრიტიკული ინფრასტრუქტურის დაცულობა.

არსებული პრობლემებისა და გამოწვევების საფუძველზე იქმნება ნიადაგი შემდეგი რეკომენდაციებისა :

1. პირველ ეტაპზე აუცილებელია შემუშავდეს ინტერნეტის განვითარების ერთიანი სტრატეგია და სამოქმედო გეგმა, განისაზღვროს სახელმწიფოს მიდგომა ინტერნეტ/კიბერსივრცის მიმართ. პროცესში აუცილებელია საკანონმდებლო და აღმასრულებელი ხელისუფლების კერძო და სამოქალაქო სექტორებს შორის ჩართულობა.
2. დაიწყოს აქტიური მუშაობა კიბერსივრცისა და მასთან დაკავშირებული საფრთხეების, ასევე სოცალური ქსელების სწორად გამოყენებასთან დაკავშირებით საზოგადოებაში ცნობიერების ამაღლების მიმართულებით.
3. განსაკუთრებული ყურადღება მიექცეს მოქალაქეთა პერსონალურ მონაცემთა დაცვის მიმართულებით საზოგადოების ცნობიერების ამაღლების პროცესს.
4. უნდა დაიწყოს აქტიური მუშაობა კადრების გადასამზადებლად, რათა ქვეყანაში საერთაშორისო სტანდარტების დანერგვის შემდეგ, გვყავდეს შესაბამისი სპეციალისტები, რომლებიც უზრუნველყოფენ საქართველოს კიბერსივრცეში არსებული საფრთხეების დროულად აღმოფხვრას.
5. სკოლის ასაკის მოსწავლეებისთვის, უნდა შეიქმნას სპეციალური საგანმანათლებლო პროგრამა, რითიც მოხდება არსებული საუკეთესო გამოცდილების შესწავლა და გაანალიზება, ასევე მომავალი თაობების ცნობიერების ამაღლება, რაც ხელს შეუწყობს ქვეყნის კიბერსივრცეში არსებული რისკებისა და გამოწვევების შემცირების პროცესს.

ეს რეკომენდაციები ძირითადად შეეხება სახელმწიფო სექტორს, რომელიც წარმატებას იმ შემთხვევაში მიაღწევს თუ იგი იმუშავებს კოორდინირებულად კერძო და სამოქალაქო სექტორებთან. რაც შეეხება კერძო სექტორს, რომელიც არის ინტერნეტის მომხმარებელი და სარგებლობს კიბერსივრცეში შეიძლება მიეცეს შემდეგი რეკომენდაციები :

1. უნდა გაანალიზოს, რომ ინტერნეტ/კიბერსივრცე არის ქვეყნის ეროვნული ინფრასტრუქტურის შემადგენელი და უმთავრესი ნაწილი, და მიმართოს ისეთ ღონისძიებებს, როგორიცა, IT კადრების გადამზადება და მათი პროფესიონალიზმის ამაღლება.
2. უნდა ითანამშრომლოს სახელმწიფო სექტორთან, რადგან ეს აუცილებელი პირობაა, კერძო და სახელმწიფო სექტორების კიბერსივრცეში დაცულობის თვალსაზრისით.

პროცესი რა თქმა უნდა მარტივი არ არის და მოითხოვს დიდ დროსა და რესურსს, მათ შორის უმთავრესს, ფინანსურსაც, მაგრამ არსებული ვითარება გვაიძულებს იზომების მიღებას, რომლებიც იქნებიან გარანტი ჩვენი და ჩვენი ქვეყნის კიბერსივრცის უსაფრთხოებისა.

შეჯამება

საქართველოს ეროვნული უსაფრთხოების კონცეფციის მიხედვით, რუსეთი და მისი ქმედებები ისევ საფრთხის შემცველნი არიან, ჩვენი ქვეყნის ეროვნული უსაფრთხოებისათვის, მათ შორის კიბერსივცის სფეროში. ასევე მომავალში საფრთხის შემცველი შეიძლება გახდნენ სომხეთი და ირანი, რომლებიც რუსეთის სტრატეგიულ მოკავშირეებად მოიაზრებიან და გააჩნიათ თავიანთი მუდმივი ინტერესები სამხრეთ კავკასიაში. ამავე ეროვნული უსაფრთხოების სტრატეგიიდან გამომდინარე საქართველოს სწორ პარტნიორებად ითვლებიან აშშ, უკრაინა და თურქეთი, ასევე ევროკავშირი და მისი ზოგიერთი წევრი ქვეყანა და ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაცი.

მე ვფიქრობ, რომ მოცემულ საკითხში, თამშრომლობა აუცილებელია ესტონეთთან, რადგანაც ამ ქვეყანამ მოკლე დროში შეძლო განევითარებინა კიბერუსაფრთხოების სფერო და გახდა ერთ-ერთი მოწინავე ევროკავშირსა და ალიანსის ქვეყნებს შორის, მისი გამოცდილება კი ჩვენი კიბერთავდაცვისათვის დიდ მნიშვნელობას იძენს.

საერთაშორისო დონეზე თანამშომლობა არის ერთ-ერთი ძირითადი პირობა და საწინდარი კიბერუსაფრთხოების დარგის განვითარებისათვის, მაგრამ პირველ რიგში აუცილებელია ქვეყნის შიგნით კიბერსივრცეში არსებული ხარვეზების გამოსწორება, ისეთივე როგორიცაა კერძო და სახელმწიფო სექტორებს შორის უთანამშრომლობა, რადგან შიგნით მოწესრიგებული ვითარება, საგარეო ასპარეზზე მოსაწესრიგებელი ვითარების წინაპირობა გახდება.

გამოყენებული ლიტერატურა

1. ,,კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები'' - ანდრია სვანაძე, ვასილ გოცირიძე. 2015 - თბილისი
2. ,,კიბერსივრცე და კიბერუსაფრთხოების გამოწვევებ'' - ვასილ სვანაძე. 2015 - თბილისი
3. ,,კიბერუსაფრთხოების პოლიტიკა''- საქართველოს თავდაცვის სამინისტრო(2014-2016)
4. საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობადა კვლევის ფონდი. ექსპერტი აზრი. ,,რეკომენდაციები საქართველოს კიბერსივრცის განვითარებისათვის''- ვასილ სვანაძე
5. საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობადა კვლევის ფონდი. ექსპერტის აზრი. ,,სუსტი რგოლის დილემა''- შოთა უტიაშვილი
6. ,,საქართველოს ეროვნული უსაფრთხოების კონცეფცია''.