კავკასიის საერთაშორისო უნივერსიტეტი

სოციალურ მეცნიერებათა ფაკულტეტი

ანა დანელიანი

კიბერუსაფრთხოების უზრუნველყოფა ეროვნულ და რეგიონულ დონეზე საქართველოს, სომხეთისა და აზერბაიჯანის მაგალითზე

საერთაშორისო ურთიერთობების და საერთაშორისო უსაფრთხოების სამაგისტრო საგანმანათლებლო პროგრამა

სამაგისტრო ნაშრომი შესრულებულია საერთაშორისო ურთიერთობების მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: პოლიტიკურ მეცნიერებათა დოქტორი,

პროფესორი - ვახტანგ მაისაია

თბილისი 2019

ანოტაცია

ნაშრომი ეხება გლობალური კიბერუსაფრთხოების უზრუნველყოფის საკითხებს და მისი ეროვნული და რეგიონული სტრატეგიის განვითარების მნიშვნელობას საქართველოს, სომხეთისა და აზერბაიჯანის მაგალითზე.

თანამედროვე მსოფლიოში გლობალიზაციასა და ვირტუალურმა სივრცემ დაიმკვიდრა მოწინავე ადგილი, როგორც ტექნოლოგიური განვითარების ხელშეწყობაში და მასობრივ კომუნიკაციებში, ასევე საერთაშორისო ურთიერთობებსა და საერთაშორისო უსაფრთხოების უზრუნველყოფის საკითხებში. ინფორმაციის გაცვლა ინტერნეტ-რესურსის მეშვეობით წარმოადგენს ერთგვარ განზომილებას, რომელიც გამოირჩევა სისწრაფით და მარტივი გამოყენებით, სწრაფად განვითარებადი ტექნოლოგიების მეშვეობით და გახდა დღევანდელობის განუყოფელი ნაწილი, როგორც ცალკეული ადამიანებისათვის, ასევე მსოფლიოს მოწინავე სახელმწიფოებისათვის და მმართველებისათვის.

ისტორია გვიჩვენებს, რომ სახელმწიფოთაშორისო ურთიერთობები, უძველესი დროიდან წარმოადგენდა რთულ პროცესს და გამომდინარეობდა აქტორების სასიცოცხლო ეროვნული და გეოპოლიტიკური ინტერესებიდან. სახელმწიფოს პოლიტიკა ყოველთვის მიმართულია თვითგადარჩენისაკენ. მსგავს საერთაშორისო ტენდენციას ადგილი XXI საუკუნეშიც აქვს, თუმცა პოლიტიკური სტრატეგიის განხორციელება დღეს ნაწილობრივ ტრანსფორებულია ვირტუალურ სივრცეში.

ზემოაღნიშნულიდან გამომდინარე, ცხადია, რომ სახელმწიფოები, ისევე როგორც ცალკეული ადამინეაბი ქმნიან საერთაშორისო ურთიერთობების ახალ სისტემას, რომელსაც გააჩნია საკუთარი ტემპი, წესები და გამოწვევები. მოწინავე პოზიციას დღეს, ნეოკლასიკური რეალიზმის მოდელი იკავებს, რომლის თანახმად სახელმწიფოებრივ აქტორებთან ერთად საერთაშორისო სისტემას არასახელმწიფოებრივი აქტრებიც აფორმებენ.

ვირტუალური სამყაროს საკითხები საერთაშორისო უსაფრთხოების გადმოსახედიდან გასცდა სამი განზომილების პარამეტრებს. გლობალური, რეგიონული და ლოკალური

დონის კიბერუსაფრთხოების უზრუნველყოფა დღეს წარმოადგენს ამ სამი დონის კოლაბორაციული პროცესების ერთობლიობას. ხოლო თვით უზრუნველყოფის პროცესი რთულდება ვირტუალური სივრცის სპეციფიკიდან და განვითარების ტემპიდან გამომდინარე.

ნაშრომში განხილულია კიბერუსაფრთხოების უზრუნველყოფის ფორმა კოლექტიური უსაფრთხოების მოდელის მიხედვით. გარდა ამისა, აღნიშნულია რომ სახელმწიფოების როლი ამ დარგში მეტად ანარქიულ ხასიათს ატარებენ, რაც გამომდინარეობს საერთაშორისო სამართლებრივი ბაზისა და ნორმების სისუსტედან.

Annotation

National and Regional Cybersecurity Provision on the Example of Georgia, Armenia and Azerbaijan

Key point of the Thesis consists the strategy of global cybersecurity and cybersecurity provision on regional and local security levels, considering an example of Georgia, Armenia and Azerbaijan.

Modern society is fully depended on globalization and virtual reality aspects. The development of cyberspace brought the circumstances of full integrity to the technological, communicative, international relations and security forms. Internet resource provided humanity with the ability to exchange information and communicate without any horizons or frames of time. The changes affected both, individuals and governments.

World History shows international relations as a complicated process of state life interest, geopolitical circumstances and cooperation. We can observe the states have always act according to its own interest and the trend is still actual in XXI century. However today, the system of international relations have been partially transform to the virtual reality. Transformation process created slightly new platform for international and individual security aspects. New Worlds' Order matches the theory of neo classic realism. Theory claims, the world's international relations system is being formed by non-governmental actors, such as corporations, NGOs, groups of interests and media. The question of Cybersecurity has left previously formed model of international security. Global, regional and local security aspects in case of virtual space are now collaborated together and create one system with depended processes to each other. However, the specifics and development speed of the virtual reality is constantly affecting the security procuring worldwide.

Master's Thesis consists positive and negative feedback on collective security perspectives of Cybersecurity. Besides, the elements of international relations in Cybersecurity frames are

underlined as anarchic, since the global virtual space is not supported by the center and due to the lack of international laws, regulations and widely spread standards.

Ana Daneliani

სარჩევი

შესავალი

თანამედროვე საერთაშორისო უსაფრთხოება მოიცავს მრავალ გლობალურ, რეგიონულ, ლოკალურსა და ინდივიდუალური უსაფრთხოების უზრუნველყოფის ასპექტებს. მათ შორის არის, საერთაშორისო ტერორიზმი, ეკონომიკური სტაბილურობის შენარჩუნება, ცალკეული ქვეყნების ინტერესების დაბალანსება, ენერგეტიკული უსაფრთხოება, ეკოლოგია და მრავალი სხვა. XXI საუკუნეში, მსოფლიოს განსაკუთრებული ყურადღების ქვეშ საინფორმაციო უსაფრთხოების ელემენტებიც ჩამოყალიბდა, რომელიც წარმოადგენს როგორც ცალკეული უსაფრთხოების უზრუნველყოფის არეალს, ასევე სხვა დარგების შემადგენელ ელემენტს. ვირტუალური სივრცე დიდი დოზით ინტეგრირებულია ენერგეტიკული ინფრასტრუქტურის საკონტროლო სისტემებში, რაც საციცოცხლო მნიშვნელობას ატარებს გლობალური მასშტაბით და ისაჭიროებს უსაფრთხოების უზრუნველყოფას. ინტერნეტის ქსელის მეშვეობით ფუნქციონირებს სხვადასხვა ქვეყნის სამხედრო ბაზები, სამედიცინო დაწესებულებები, ეკონომიკური სისტემები, აგრარული ინფრასტრუქტურა და მრავალი სხვა. ადამიანების ამგვარი სწრაფვა განპირობებულია ტექნოლოგიების მეშვეობით ხელმისაწვდომი კომფორტით, სისწრაფით და სიმარტივით. ამის გათვალისწინებით, აუცილებელია სათანადო ზედამხედველობა რისკებისა და საფრთხეების აცილებასა და სისტემების ნორმალური მუშაობის უზრუნველსაყოფად.

<u>თემის აქტუალობა</u>

21-ე საუკუნის კაცობრიობის საარსებო პირობები მხოლოდ ფიზიკური ხასიათის უკვე აღარ არის. ტექნოლოგიური პროგრესი თანაბრად გლობალიზაციასთან ჩვენი ისტორია ვირტუალურ რეალობაში გადაიტანა, რომელიც ადამიანის ჩვეულებრივი ცხოვრების განუყოფილი ნაწილი არის და დღეს გლობალური კიბერ-კომუნიკაციის

მოდელი მოიცავს როგორც მსოფლიოს სამხედრო-პოლიტიკურ და ეკონომიკურ პროცესებს, ასევე ცალკეული ადამიანის ყოველდღიური მოღვაწეობის ასპექტებს.

შედეგად კი, კაცობრიობას გააჩნია არსებობის კიდევ ერთი - ვირტუალური განზომილება, საკუთარი საფრთხითა და უსაფრთხოების პარამეტრებით, მოვლენათა დინამიკით და აქტორებით. ამის მიუხედავად, გასათვალისწინებელია ის, რომ ვიტუალური სივრცე მჭიდროდ არის დაკავშირებული ფიზიკურთან და მასში განხორციელებული ნებისმიერი ქმედების შედეგი გავლენას ახდენს ადამიანის ყოველდღიურ ნორმალურ არსებობაზე. ამის დასამტკიცებლად არსებობს არაერთი ცნობილი მაგალითი. ისეთი როგორც: ირანის ბირთვული პროგრამის შეჩერება კომპიუტერული ვირუსი „Stuxnet“-ის გამოყენებით 2010 წელს ; 2014 წლის ამერიკული სავაჭრო საიტის „Home Depot”-ის გატეხვა, რომლის შედეგად მოტაცებული იყო 56 მილიონზე მეტი მომხარებლების საკრედიტო ბარათების მონაცემები ; 2008 წლის DDOS შეტევები საქართველოს სამთავრობო ვებ - საიტებზე და მრავალი სხვა.

ვირტუალური განზომილება სწრაფი კომუნიკაციის საშუალებების არსებობით მსოფლიოს უფრო სწრაფ გეოპოლიტიკურ ცვლილებას უწყობს ხელს და მისი აქტორები არიან როგორც ცალკე ადამიანები და ჯგუფები, ასევე ქვეყნები და საერთაშორისო ორგანიზაციები. ამ უსასრულო რესურსის სამართლებრივი გაკონტროლების მექანიზმები ჯერ კიდევ განვითარების პროცესშია, ხოლო არსებული და პოტენციური საფრთხეები უკვე აქტუალურია.

<u>საკვლევი კითხვები:</u>

- როგორ ხორციელდება კიბერუსაფრთხოების სტრატეგია რეგიონული უსაფრთხოების დონეზე - სამი ლოკალური აქტორის მაგალითზე?
- რას წარმოადგენს კიბერუსაფრთხოება და რამდენად შესაძლებელია მისი პრაქტიკული გამოყენება?
- რაში გამოიხატება ვირტუალურ სივრცეში კიბერსაშიშროების პარამეტრები და როგორი სახით არიან ისინი წარმოდგენილები?

ჰიპოთეზა

კიბერუსაფრთხოების სტრატეგიის რეგიონული უსაფრთხოების განხორციელების დონეები მოითხოვს თანამედროვე უსაფრთხოების გარემოში არსებული და მოსალოდნელი რისკების, საფრთხეების და გამოწვევების განსაზღვარას. თანამედროვე საერთაშორისო უსაფრთხოების სისტემის ფარგლებში კიბერუსაფრთხოებამ გარკვეული ადგილი დაიმკვიდრა და აისახა, როგორც მისი შემადგენელი და აუცილებელი კომპონენტი. თუმცა, კიბერუსაფრთხოება, როგორც სამეცნიერო-პრაქტიკული დარგი ჩამოყალიბების პროცესშია და მისი რეგულირება ხორციელდება როგორც სამართლებრივი, ასევე პოლიტიკური და კონტექსტური ფორმატების მეშვეობით.

თემის მიზნები და ამოცანები:

- ემპირიული მიზანი - კიბერუსაფრთხოების სტრატეგიის გაძლიერების აუცილებლობის წარმოჩენა პრაქტიკული და ისტორიული მაგალითების გათვალისწინებით
- კოლექტიური უსაფრთხოების თეორიის გამოყენებით საქართველოს, სომხეთისა და აზერბაიჯანის თანამშრომლობითი მექანიზმების მიმოხილვა
- ძალთა ბალანსის თეორია გათვალისწინებით არსებული ვითარების ობიექტური მიმოხილვა
- არსებული ისტორიული მაგალითების განხილვის შედეგად შემუშავებული პრევენციის პარამეტრების მიმოხილვა
- კავკასიის რეგიონში კიბერუსაფრთხოების მნიშვნელობის განსაზღვრა

მეთოდოლოგიის ჩარჩო:

- პოლიტიკური რეალიზმის სკოლის ანარქიზმის თეორია. ამ თეორიის თანახმად, ყველა საერთაშორისო აქტორის ქმედება და მამოძრავებელი ძალა გამომდინარეობს მხოლოდ თვითგადარჩენისა და საკუთარი საცხოვრებლო ინტერესის მიღწევის პერსპექტივიდან და გლობალურ დონეზე არ არსებობს

ერთიანი ძალა, რომელიც შეუწყობდა ხელს საერთაშორისო თანამშრომლობის კონსტრუქტივიზმს;

  - ანარქიზმის თეორია გამოყენებულია კიბერუსაფრთხოების გლობალური აქტორების ინტერესებისა და მიზნების გასაანალიზებლად

- ნეოკლასიკური რეალიზმის თეორია, რომლის თანახმად საერთაშორისო ურთიერთობებში დომინანტური ძალა არასახელწიფოებრივ სუბიექტებს გააჩნია
  - ნეოკლასიკური რეალიზმის თეორიას ემთხვევა ნაშრომში გამოკვეთილი არასახელმწიფოებრივი სუბიექტების გაზრდილ როლს კიბერუსაფრთხოების დარგში
- ნაშრომში გამოყენებული იქნება პოლიტიკური რეალიზმის სკოლის „ძალთა ბალანსის“ თეორია, რომელიც გამომდინარეობს საერთაშორისო ურთიერთობების ანარქიული სტრუქტურისგან;
  - თეორიას ეთანხმება ვირტუალური ტექნოლოგიების არათანაბარი ინტეგრაციის ფაქტი სხვადასხვა სახელმწიფოს მაგალითზე. გარდა ამისა, გამოკვეთილია თვალსაჩინო სხვაობა სამართლებრივი დარეგულირების მექანიზმებისა და კომპიუტერული ტექნოლოგიების განვითარების ტემპებს შორის
- „კოლექტიური უსაფრთხოების“ რიჩარდ კოენის თეორია, რომელიც გულისხმობს სახელმწიფოების თანამშრომლობას მშვიდობის შესანარჩუნებლად და საერთაშორისო უსაფრთხოების უზრუნველსაყოფად;
  - თეორიის მიხედვით განხილულია კიბერუსფართხოების უზრუნველყოფის ეფექტიანობა კოლექტიური უსაფრთხოების სტრატეგიის შესაბამისად.

<u>კვლევის მეთოდები:</u>

- თემისთვის შერჩეული სავარაუდო მეთოდოლოგიის თეორიული მასალის განხილვა და ანალიზი, რომელიც ასევე დაეფუძნება ემპირიული კვლევის საფუძვლებს
- Case Study (შემთხვევის გარჩევა / ანალიზი), რომელიც ემსახურება არსებული გამოცდილების და ისტორიული მაგალითების განხილვას და გაანალიზებას

- თვისობრივი კვლევის მეთოდები:
    - ისტორიულ-აღწერილობითი მეთოდი
    - მონაცემთა ანალიზის მეთოდი
- რაოდენობრივი კვლევის მეთოდის მიხედვით გამოყენებული იქნება კონტენტ-ანალიზი

<u>გამოყენებული ლიტერატურის მიმოხილვა</u>

- *Cyber Security Policy Guidebook – Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss; John Willey & Sons Publication, Hoboken, New Jersey, 2012.* ნაშრომი შემუშავებულია სპეციალურად დაკომპლექტებული ინჟინერების და საინფორმაციო ტექნოლოგიების სპეციალისტების მიერ. შეერთებული შტატების მიერ ბუდაპეშტის 2001 წლის კონვენციის რატიფიცირების შემდგომ. წიგნში ფართოდ არის გაშლილი კიბერუსაფრთხოების ტექნიკური განხორციელების შესაძლებლობა პოლიტიკური და სამართლებრივი პარამეტრების გათვალისწინებით. ნაშრომის მთავარ იდეას წარმოადგენს ტექნოლოგიური სირთულეების ადაპტირება ფართო აუდიტორიაზე.
- ***კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები - კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები. <u>ვლადიმერ სვანიძე, ანდრია გოცირიძე</u> / ნაშრომების და სტატიების კრებული ; სსიპ კიბერუსაფრთხოების ბიურო, საქართველოს თავდაცვის სამინისტრო, თბილისი, 2015.*** პირველი ქართულენოვანი კრებული, რომელშიც სრულყოფილადაა განხილული კიბერსივრცის თავისებურებები, საფრთხეები და გამოწვევები. ნაშრომში განხილულია საერთაშორისო კიბერუსართხოების სტრატეგიები ამერიკისა და ევროპის წამყვანი ქვეყნების მაგალითზე და წარმოჩენილია საქართველოსა და პოსტ-საბჭოთა ქვეყნების ეროვნული უსაფრთხოების ასპექტები კიბერუსაფრთხოების საკითხებში.

- ***საქართველოს საგარეო პოლიტიკის პრიორიტეტები და დეტერმინანტები „ცივი ომის“ შემდეგ (1991 – 2004 წ.წ.) (სახელმძღვანელო) - <u>ვახტანგ მაისაია</u>, სუხიშვილის სასწავლო უნივერსიტეტი, თბილისი, 2013*** - ნაშრომში განხილულია საქართველოს გეოპოლიტიკური მდგომარეობა და საგარეო-პოლიტიკური კურსი, რომელიც გამოიკვეთა ქვეყნის დამოუკიდებლობის გამოცხადების შედგომ. წიგნში ასევე აღწერილია სამხრეთ-კავკასიისა და კასპიის რეგიონი და ამ რეგიონში არსებული სახელმწიფოების თანამშრომლობის მექანიზმები.
- ***ჰიბრიდული ომი და ევრო-ატლანტიკური სივრცის უსაფრთხოების ლანდშაფტის ცვლილება, პოლიტიკური და ეკონომიკური შედეგები - <u>გრიგოლ მგალობლიშვილი, ბათუ ქუთელია, ირინა გურული, ნინო ევგენიძე;</u> ეკონომიკური პოლიტიკის კვლევის ცენტრი, „ღია საზოგადოება - საქართველო“-ს ფონდი, თბილისი, 2016*** - ნაშრომი ეხება რუსეთის ფედერაციის პოლიტიკას ევრო-ატლანტიკურ ალიანსში გაწევრიანების სურვილის მქონე სახელმწიფოების მიმართ, საქართველოს მაგალითზე. განხილულია რუსეთის ამგვარი პოლიტიკური კურსის საინფორმაციო და ეკონომიკური შედეგები, როგორც ნატო-ს, ასევე საქართველოს შემთხვევაში.
- ***XXI საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების თეორია: მითი და რეალობა - რეგიონული და გლობალური ასპექტები - ვ. მაისაია, გ. მაღრაძე, გამომცემლობა „უნივერსალი“, თბილისი, 2017*** – ნაშრომში განხილულია გლობალური უსაფრთხოების XXI საუკუნის პარამეტრები სხვადასხვა სახელმწიფოებრივი და არასახელმწიფოებრივი აქტორის მაგალითზე. მოყვანილია ჰიბრიდული საფრთხეების ჩამონათვალი და დეფინიცია და ხაზგასმულია ასიმეტრიული საფრთხეების მნიშვნელობა გლობალური უსაფრთხოების თვალსაზრისით. წიგნში აღწერილია კოლექტიური უსაფრთხოების თეორია და გაანალიზებულია თეორიის პრაქტიკული მაგალითები
- ***ეკონომიკური უსაფრთხოება. თეორია, მეთოდოლოგია, მრაქტიკა - ბ. ალადაშვილი, თბილისი, 2011*** – წიგნში ფართოდ არის გაშლილი

გლობალიზაციის კონცეფცია, მისი დადებითი და უარყოფითი გავლენა ეროვნული ეკონომიკური უსაფრთხოებისათვის. მოყვანილია მსოფლიოს მოწინავე ქვეყნების ეკონომიკური უსაფრთხოების უზრუნველყოფის მექანიზმების მაგალითები და განხილულია საქართველოს ეკონომიკური უსაფრთხოების პარამეტრები.

თავი I

კიბერუსაფრთხოება და მისი მნიშვნელობა XXI საუკუნეში

XXI საუკუნეში კიბერსუფართხოება წარმოადგენს კომპლექსურ ტექნოლოგიურ სისტემას, რომელიც გამოიყენება ინტერნეტის მომხმარებლების პერსონალური მონაცემების ხელშეუხებლობისა და უსაფრთხოების უზრუნველსაყოფად. ინდივიდუალურ და გლობალურ დონეზე, კიბერუსაფრთხოების არარსებობამ დღეს შეიძლება გამოიწვიოს როგორც ფინანსური, ასევე ინფრასტრუქტურული კრიტიკული დანაკარგი.[1] ინფორმაციული ტექნოლოგიების განვითარება და მათი ინტეგრაცია საყოფაცხოვრებო პროცესებში გამოირჩევა სისწრაფით, ხელმისაწვდომობით და გამარტივებული მოხმარების შესაძლებლობით, რაც უწყობს ხელს ტექნოლოგიებსა და ინტერნეტს უფრო მეტ სფეროში ინტეგრირებას. მონაცემთა გაცვლა, კომუკაცია, ვაჭრობა, თანამედროვე მედია, საბანკო და ფინანსური მექანიზმები, ტრანსპორტირება, განათლება და სამედიცინო ტექნოლოგიები არის იმ სფეროების მცირე ჩამონათვალი, რომლის ნორმალური სამუშაო პროცესები ნაწილობრივ ან სრულად ტრანსფორმირებულია ვირტუალურ განზომილებაში და აგებულია ინტერნეტ-ტექნოლოგიებზე. დღევანდელ დღეს ჩვენ გაგვიჭირდება რაიმე კომპანიის ან დაწესებულების მოძებნა, რომლის ოფისში ან სამუშაო სივრცეში არ იქნება

[1] CISCO deffinition of cyber security - https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html

კომპიუტერი, ისევე როგორც სტუდენტის, რომელიც თავის საკურსო ნაშრომს ინტერნეტის გამოყენების გარეშე დაწერდა. ყოველივე ეს გვითითებს, რომ ინტერნეტი და ტექნოლოგიები ქმნის შესაძლებლობებს, რომელიც ეხმარება კაცობრიობას ყოველდღიურ რეჟიმში და ამარტივებს უფრო მეტი შედეგების მიღწევას.

აღნიშნული პროგრესის პარალელურ დინამიკაში იზრდება საფრთხე, რომელიც მოიაზრებს არალეგალურ ჩარევას სხვადასხვა სისტემის მუშაობაში და მის ბოროტმოქმედ გამოყენებაში. პირველ რიგში, ვირტულური საფრთხეები უკავშირდება პერსონალური სამომხმარებლო ინფორმაციის ქურდობას, ხოლო მსგავსი საფრთხის ქვეშ შეიძლება იყოს როგორც პერსონალური და ფინანსური მონაცემების, ასევე მსხვილი კომპანიის ან სახელმწიფო უწყების ინფორმაცია, რომელიც ტრანსფორმირებულია ელექტრონულ ფორმატში. არაკომერციულმა ორგანიზაციამ „ინტერნეტის განვითარების ინიციატივის“ პროექტის ფარგლებში გამოაქვეყნა ბროშურა, სადაც ჩამოყალიბებულია კიბერუსაფრთხოების ხუთი განზომილება ტექნოლოგიური ინტეგრაციის დონეების მიხედვით. ესენია:

- პოლიტიკური დონე;
- სამხედრო დონე;
- ეკონომიკური დონე;
- ტექნიკური დონე;
- სამოქალაქო საზოგადოება - სამომხმარებლო დონე;

თითოეული დონე ადასტურებს განსაზღვრებას, რომ ყოველი სექტორის ფარგლებში ინფორმაციული ტექნოლოგიების ინტეგრაციამ სამუშაო პროცესების უდიდესი ნაწილი დაიკავა და ნორმალური რეჟიმის მწყობრიდან გამოყვანის მცდელობამ შეიძლება მიაყენოს კრიტიკული ზიანი.[2]

ცხადია, რომ კომპიუტერული ტექნოლოგიები და ინტერნეტი არის ღია რესურსი, რომელიც ხელმისაწვდომია ნებისმიერი ადამიანისათვის მსოფლიოში. ამის

[2] კიბერუსაფრთხოების ახალი გამოწვევები და საქართველო, ინტერნეტის განვითარების ინიციატივა, გვ. 5, 2015 წ.

გათვალისწინებით, საკმაოდ რთულია იმის განსაზღვრა, თუ რა მიზნებისთვის შეიძლება იყოს გამოყენებული ეს რესურსი ამა თუ იმ ადამიანის მიერ. კიბერ-შეტევების უმეტესობა ხორციელდება ე.წ. კომპიუტერული ვირუსების გამოყენებით. პარადოქსულია, რომ ერთსა და იმავე ტექნოლოგიით შესაძლებელია ვირუსული პროგრამის აწყობა და ამავე დროს, უსაფრთხოების პროტოკოლის გამოყენება. აქედან გამომდინარეობს დასკვნა, რომ ნებისმიერი კიბერ-დანაშაულის უკან დგას ადამიანი ან ადამიანთა ჯგუფი, რომლის ინსტრუმენტი არის ინტერნეტ რესურსი და მისი არალეგალური გამოყენება.

1.1 კიბერუსაფრთხოების მნიშვნელობა 21-ე საუკუნეში

დრევანდელ დღეს, ადამიანის ყოველდღიური საქმიანობის უდიდესი ნაწილი დამოკიდებულია ინფორმირებულობაზე და ინფორმაციის სწორ გამოყენებაზე. თანამედროვე ინფორმაციული ტექნოლოგიები მუშაობის პროცესი მოიცავს მონაცემთა მიღებას, დამუშავებას და გაცვლას ინტერნეტ-ტექნოლოგიებისა და კომპიუტერული ოპერაციების რეგლამენტირებული წესების მეშვეობით.

გლობალური ქსელის ფართო გავრცელების ფონზე არსებობს ბევრი შეკითხვა, რომელიც უკავშირდება მის ეფექტიანობას, ინფორმაციაზე თავისუფალ წვდომასა და უსაფრთხოებას. მომხდარი პრეცედენტები გვიჩვენებს, რომ ინფორმაციული ტექნოლოგიების უსაფრთხოების ზომები იშვიათად არის ეფექტიანი სხვადასხვა საფრთხის წინააღმდეგ და გამოწვევები მნიშვნელოვნად უსწრებს წინ პრევენციისა და დაცვის მექანიზმებს. ჩამოშორების ერთ-ერთ მიზეზად თვლიან იმ ფაქტს, რომ თავდაპირველად გლობალური ქსელი შექმნილი იყო მხოლოდ სამეცნიერო მონაცემთა გაცვლისა და საფოსტო ტექნოლოგიების განვითარების მიზნით.[3] თუმცა დღეს, ქსელურ ტექნოლოგიაზე სრულიად აგებულია როგორც მსოფლიო ეკონომიკა,

[3] Демократическое Управление и Вызовы Кибербезопасности, Б.С. Бакленд, Ф. Шрайер, Т.Х.Винклер, Вступление, стр. 1 - https://www.dcaf.ch/sites/default/files/publications/documents/Horizon_1_Good_Governance_CyberSecurity_RUS.pdf

ასევე ყველა სასიცოცხლო საქმიანობა და საქმიანობის სფერო, ხოლო გამოყენებისა და ფუნქციონირების მასშტაბი და გავცელების ტემპი ბერვად უფრო სწრაფია, ვიდრე ინფრასტრუქტურული და იურიდიული რეფორმებისა და უსაფრთხოების უზრუნველყოფის ზომების შემუშავების მცდელობები. მაგალითად, პირველი მასშტაბური კიბერ-შეტევა დაფიქსირებულია 1988 წელს ამერიკის შეერთებულ შტატებში. მიუხედავად იმისა, რომ კორნელის უნივერსიტეტის ასპირანტი რობერტ მორისის ქმედება არ იყო მიზანმიმართული ზიანის მიყენებაზე, მის მიერ შექმნილი პროგრამა გავრცელდა აშშ-ს 6000-ზე მეტ კომპიუტერზე და გადმოიწერა მომხმარებლების პერსონალური მონაცემები. ახლად დამტკიცებული კანონის მიხედვით, მორისს წაუყენეს ბრალდება „კომპიუტერული თაღლითობის“ სტატიის შესაბამისად.[4] თავად მორისი უწოდებდა ამ ქმედებას „შემთხვევითს“ და ამტკიცებდა, რომ მას არ ჰქონდა გათვლილი თუ რამდენად მავნე აღმოჩნდებოდა მის მიერ შექმნილი პროგრამა. ეს შემთხვევა ფართოდ გავრცელდა ამერიკის საზოგადოებაში და ამასთან ერთად, წამოაყენა კომპიუტერული უსაფრთხოების საკითხი ქვეყნის მასშტაბით. „მორისის ჭია“-მ გამოიწვია ინტერესი მაშინდელი ჰაკერების წრეებშიც და მისი გამეორების მცდელობები აშშ-ში ყოველ წილს ფიქსირდებოდა. იმის და მიუხედავად, რომ აშშ კომპიუტერული ტექნოლოგიების განვითარების მაჩვენებლით XX საუკუნის მიწურულს მოწინავე პოზიციებს იკავებდა და მორისის პრეცედენტის გათვალისწინებით, აშშ-მ ეროვნული კიბერუსაფრთხოების სამმართველო ჩამოაყალიბა მხოლოდ 2003 წელს. ეს მაგალითი ნათლად აჩვენებს იმას, რომ საუკუნეების განმავლობაში ჩამოყალიბებული სახელმწიფო სტრუქტურები ნაკლებად უწევენ კონკურენციას ტექნოლოგიური განვითარების ტემპებს.

დღევანდელ დღეს, ფაქტობრივად ყველა მონაცემი და ინფორმაცია ინახება ელექტრონულ ფორმატში. ადამიანების აბსოლიტური უმრავლესობა ანდობს პირად მონაცემებს კომპიუტერებს, სმარტფონებს და ვირტუალურ არქივებს (ე.წ. “Cloud”) და ავრცელებს ინფორმაციას სხვადასხვა საკომუნიკაციო რესურსის დახმარებით. მსგავსი

[4] «Первая в истории кибератака», 2018 - https://futurist.ru/news/6624-pervaya-kiberataka-proizoshla-sluchayno-iz-za-lyubopitnogo-programmista

გახსნილობა აძლევს საკმაოდ ფართო მოედანს კომპიუტერული ვირუსებისათვის და მათი შემქმნელებისათვის. „მორისის ჭია“ აღიარებულია, როგორც პირველი DDos-შეტევა ისტორიაში, რომელიც განხორციელდა მაშინ, როდესაც ინფრასტრუქტურული სისტემების ტრანსფორმაცია ვირტუალურ განზომილებაში და ინტერნეტ-ტექნოლოგიების ინტეგრირება ჯერ კიდევ საწყის ეტაზე იყო, თუმცა ვირუსით გამოწვეული ფინანსური ზიანი შეფასებული იყო 96.5 მილიონი აშშ-ს დოლარის ოდენობით. ინტერნეტ-ტექნოლოიების ფართო ინტეგრაციასთან პარალელურად ტრანსოფრმაცია კომპიუტერულ ვირუსებზეც გავრცელდა. 2017 წლის კასპერსკის ლაბორატორიის მონაცემების მიხედვით, ბოლო 10 წლის განმავლობაში მსოფლიოში დაფიქსირებულია 300 000-ზე მეტი მავნედმოქმედი კომპიუტერული პროგრამა და ეს მაჩვენებელი პროგრესულად მატულობს.[5]

ბოროტმოქმედება კომპიუტერული ვირუსების გამოყენებით ხშირად მიმართულია არა მხოლოდ ცალკეული ადამიანების, არამედ კომპანიების, კორპორაციების, ორგანიზაციებისა და სახელმწიფოების წინააღმდეგაც. ვირუსული პროგრამა დღეს წარმოადგენს ძლიერ ინსტრუმენტს, რომელიც გამოიყენება როგორც ფულადი თაღლითობასა და თანხების არალეგალური მისაკუთრებისათვის, ასევე მნიშვნელოვანი ინფორმაციის მოსაპოვებლად სტრატეგიული ან კომერციული ინტერესის მისაღწევად. აქვე უნდა აღინიშნოს, რომ კიბერ-საშიშროებები არ მოიცავს მხოლოდ კომპიუტერულ ვირუსებს.

კომპიუტერული ვირუსის გამოყენების გარეშე ყველაზე მასშტაბური მონაცემთა გატაცება ისტორიაში მოხდა აშშ-ში 2013 წელს. მაშინ ცრუ-ს სპეცაგენტმა და ტექნიკოსმა ედვარდ სნოუდენმა მოახერხა 1.7 მილიონი საიდუმლო საბუთის მოპოვება და ჟურნალისტებისთვის გადაცემა. ამ ქმედებამ გამოიწვია აშშ-ს სახელმწიფოს დისკრედიტაცია საერთაშორისო დონეზე და იქამდე საიდუმლო ეროვნული პროგრამის გასაჯაროვება. უკვე რუსეთის ფედერაციის მობინადრე სნოუდენმა, 2013 წელს გამოაქვეყნა ინფორმაცია სხვადასხვა სახელმწიფო პროექტის შესახებ, რომლის

[5] Отчёт Лаборатории Касперского, 2017 - https://rns.online/it-and-media/Kolichestvo-viyavlyaemih-kompyuternih-virusov-v-mire-za-10-let-viroslo-v-200-raz--2017-04-18/

მიხედვით აშშ აწარმოებდა ადამიანების პერსონალური მონაცემების, მიმოწერების და ზარების მონიტორინგს მთელს მსოფლიოში. ამ შემთხვევამ გამოიწვია უპრეცედენტო რეზონანსი და ედვარდ სნოუდენის ინტერპოლით ძებნილად გამოცხადება. გაერო-მ მოითხოვა ოფიციალური განცხადება აშშ-ს მთავრობისაგან, გაერო-ს ნიუ იორკის შტაბ-ბინის არალეგალური მოსმენის შესახებ, გერმანიამ გააუქმა აშშ-სთან და დიდ ბრიტანეთთან 1968 წელს დადებული ხელშეკრულება, რომლის თანახმად ამერიკის სპეც. დანიშნულების აგენტებს შეეძლოთ ელექტრონული დაზვერვა გერმანიის ტერიტორიაზე, ხოლო აშშ-ს ეროვნული უსაფრთხოების სააგენტომ საკუთარი თანამშრომლების და ტექნიკოსების 90% ჩაანაცვლა სარობოტო ავტომატიზირებული ტექნიკით. ტექნიკური თვალსაზრისით, ედვარდ სნოუდენი მუშაობდა ცრუ-ს ისეთ პოზიციაზე, რომელის გულისხმობდა წვდომას საიდუმლო არქივებზე და მონაცემების გატაცება მოახერხა მხოლოდ USB Flash-ის გამოყენებით.[6] ედვარდ სნოუდენის რეზონანსული მოქმედება იყო არასკამრისი ინფორმაციული დაცულობის მაგალითი. როდესაც რიგითმა თანამშრომელმა მოახერხა მონაცემების გადმოწერა და გატანა ერთ-ერთი ყველაზე დაცული სახელმწიფო ობიექტიდან და ამ მონაცემების გადაცემა მესამე პირებისათვის. აშშ-ში აღიარებული კიბერ-დანაშაულის მაგალითი, მიმართული სახელმწიფოს წინააღმდეგ.

კიბერ-საშიშროების კომპიუტერული ვირუსის გარეშე კიდევ ორი მაგალითი არის კიბერ-ბულინგი და კიბერ-ტერორიზმი. ორივე მათგანი მიმართულია ადამიანების ფსიქოლოგიური დაშინების და ზეწოლის მოხდენაზე. კიბერ-ტერორიზმის გამოვლინებად ასევე ითვლება ონლაინ რეკრუტინგი, რომელსაც აქტიურად იყენებდა ტერორისტული ორგანიზაცია „ისლამური სახელმწიფო“ სოციალური ქსელების მეშვეობით. საერთაშორისო ორგანიზაციებისა და სახელმწიფოების უმთავრესი გამოწვევა კიბერ-უსაფრთხოების ფარგლებში არის დანაშაულისა და დამნაშავეების დადგენა და დამტკიცება. რადგან მაღალი კვალიფიკაციის მქონე ჰაკერებისთვის ვირტუალური სივრცე აძლევს საკუთარი ვინაობის დამალვისა და კვალის დაფარვის

---

[6] Wikipedia, The Free Encyclopedia, Edward Snowden - https://en.wikipedia.org/wiki/Edward_Snowden

საშუალებას, რაც სერიოზულად ართულებს როგორც საგამოძიებო, ასევე შემდგომ სამართლებრივ პროცესებს.

1.2 ვირტუალური სივრცის განზომილება და ჰიბრიდული ომი

როგორც უკვე ავღნიშნეთ, ვირტუალური სივრცის განზომილებაში შეიძლება გამოიყოს რამდენიმე სექტორი. ამ ჩამონათვალის და სხვადასხვა საერთაშორისო გამოკვლევის შესაბამისად, შესაძლებელია კიბერ-შეტევების ძირითადი ობიექტების განსაზღვრაც. პერსონალური მონაცემების გატაცებისა და სხვადასხვა არალეგალურ ქმედებასთან პარალელურად, კიბერ-საშიშროების ობიექტი ხშირად არის მთლიანი ქვეყანა და მისი სახელმწიფო უწყებები და სტრუქტურები. ზოგიერთი უკვე მომხდარი კიბერ-შეტევა შეიძლება ჩაითვალოს თანამედროვე დროის აგრესიის გამოხატვის ფორმად. მსგავსი შეტევის შედეგად შესაზლებელია ისეთი მონაცემების გატაცება, რომელიც სახელმწიფო საიდუმლოს წარმოადგენს და გამოიწვიოს სახელმწიფოს სასიცოცხლო

სისტემების დარღვევა, რაც თავის დროს წარმოადგენს საერთაშორისო სამართლის ნორმების დარღვევას.[7]

კიბერ-შეტევებს სახელმწიფოს წინააღმდეგ აქვს რამდენიმე ძირითადი ფორმა:

- **კიბერ-შპიონაჟი** - კომპიუტერული ჯაშუშობა ან კიბერ-დაზვერვა. ინფორმაციის მიღების არასანქციონირებული საშუალება, რის შედეგადაც შესაძლებელია სახელმწიფოს შიდა ეკონომიკური, სამხედრო, სტრატეგიული და ტაქტიკური მონაცემების მისაკუთრება პოლიტიკური ან სტრატეგიული მიზნების მისაღწევად
- **ინფრასტრუქტურული შეტევები** - კიბერ-შეტევა ქვეყნების ან ქალაქების ინფრასტრუქტურულ ან ენერგეტიკულ სისტემებზე, მათი მწყობრიდან გამოყვანის მიზნით
- **სამხედრო-ინფრასტრუქტურული შეტევები** - კიბერ-შეტევები სამხედრო სისტემებზე, რომლის ფუნქციონირებაზე დამოკიდებულია სამხედრო ტექნიკის და მოწყობილობების მუშაობა. ასევე, სამხედრო-სანავიგაციო სისტემებზე
- **„სერვისის უარი“** (Access Denial) - მსგავსი ტიპის შეტევის მიზანი არის სახელწიფო სტრუქტურებისა და უწყებების ვებ-პორტალები და მონაცემთა ბაზები, რომლის მწყობრიდან გამოყვანამ შეიძლება გამოიწვიოს სერიოზული დანაკარგი სახელმწიფოს ეკონომიკაში და მოსახლეობის პანიკა გამოიწვიოს
- **პროპაგანდა და ვანდალიზმი** - შეტევა ვებ-გვერდებზე, პროპაგანდისტული და სახელმწიფო რელიგიურ-კულტურული შინაარსობრივი ვანდალიზმის მქონე კონტენტის განთავსების მიზნით.

2018 წელს ბლუმბერგის გამომცემლობამ გამოაქვეყნა სტატია, რომელშიც აღწერილი იყო ჩინეთის სახალხო რესპუბლიკის ქმედებები ამერიკის შეერთებული შტატების წინააღმდეგ და რომლის შედეგად ამერიკამ და დიდმა ბრიტანეთმა ჩინეთს კიბერ-შპიონაჟის ბრალდება წაუყენა. ჩატარებული გამოძიების შედეგად გაირკვა, რომ რამდენიმე წლის მანძილზე ჩინეთში არსებული ტექნიკის საწარმო მსხვილი

[7] Кибератака как современная форма совершения агрессии, С.Г. Тимошков, стр. 128, 2018 г.

ამერიკული კომპანიებისათვის და სახელმწიფო სტრუქტურებისთვის განკუთვნილი კომპიუტერული ტექნიკის მიკროსქემებსა და დედა-პლატებზე ამონტაჟებდა სპეციალურ მიკრო-ჩიპებს, რომლის გამოყენებით შესაძლებელი ხდებოდა შემდგომი სადაზვერვო ქმედებების განხორციელება. ამავე გამომცემლობის მონაცემების მიხედვით, ამ შეტევის მსხვერპლთა რიცხვში შესული იყო ისეთი კომერციული გიგანტები როგორც კომპანია Apple და Amazon და რამდენიმე სახელმწიფო და სამხედრო დაწესებულება.[8] კომპიუტერული ტექნიკა დამზადებული იყო კომპანია Supermicro-ს საწარმოზე, თუმცა ამერიკელი ექსპერტების უმეტესობამ ჩათვალა, რომ მსგავსი ქმედების დამკვეთი უშუალოდ ჩინეთის მთავრობა იყო.

კიდევ ერთი ცნობილი კიბერ-შეტევის მაგალითი სახელმწიფოს წინააღმდეგ არის 2010 წლის "Stuxnet"-ის ტიპის კომპიუტერული ვირუსის გავრცელება ირანის ბირთვულ ინფრასტრუქტურაზე. იმავე წლის სექტემბრის თვეში გახდა ცნობილი, რომ კომპიუტერულმა ვირუსმა შეაღწია 10 000-ზე მეტ ქალაქ ნატანზეს ბირთვული საწარმოს კომპიუტერში და 5000 ბირთვული დანადგარიდან, 1400-ის მუშაობა სრულად შეაჩერა და მნიშვნელოვნად გადაავადა ირანის პირველი ატომური ელექტრო სადგურის ექსპლუატაციაში შესვლის თარიღი. კომპიუტერების „დაინფიცირების" მიზეზი გახდა კომპანია Siemens-ის რიგითი თანამშრომელი, რომელმაც ვირუსი USB Flash-ის საშუალებით გაავრცელა.

სრულად ნათელი მიზნების გამო, "Stuxnet"-ის ტიპის ვირუსის შემქმნელის შესახებ არ არის ცნობილი, ხოლო ასეთი ტიპის ვირუსი თავისი დროის უპრეცედენტო მასშტაბისა და ძალის აღმოჩნდა. მსგავსი პროექტის შესაქმნელად საჭიროა მსხვილი ფინანსური და ინტელექტუალური რესურსი. ამის გათვალისწინებით, ბევრი საერთაშორისო ექსპერტი მიიჩნევს, რომ ასეთი პოტენციალი არ გააჩნია არც ერთ იატაკქვეშა ჰაკერს ან „საინიციატივო" ჰაკერულ ჯგუფს და ასეთი მასშტაბური ვირუსი მხოლოდ სახელმწიფოსთვის ხელმისაწვდომი რესურსებით გახდა შესაძლებელი. კომპანია

---

[8] The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, Bloomberg Businessweek, 2018 - https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

GSMK-ს ტექნიკურმა დირექტორმა ფრანკ რუგერმა ივარაუდა, რომ მსგავსი ვირუსული პროგრამის შესაქმნელად საჭირო იყო 8-10 პროფესიონალური ტექნიკოსი, ნახევარწლიანი სამუშაო პროცესი და დაახლოვებით, 3 მილიონი აშშ დოლარი.[9] ირანელმა ექსპერტთა ჯგუფმა განაცხადა, რომ ვირუსი შემუშავებული იყო აშშ-სა და ისრაელის სადაზვერვო ჯგუფების მიერ. იმავე 2010 წლის აშშ-ს თავდაცვის მინისტრის მაშინდელმა მოადგილემ უილიამ ლინმა, სიტყვით გამოსვლის დროს ჩამოაყალიბა აშშ-ს კიბერუსაფრთხოების ახალი სტრატეგიის ხუთი პრინციპი, რომლებმაც შემდგომში მოიპოვა ფართო მხარდაჭერა ჩრდილო-ატლანტიკური ალიანსის სხვა წევრებისგანაც. ამ პრინციპების თანახმად, აშშ-ს კიბერუსაფრთხოების სტრატეგია უნდა გადასულიყო სრულიად ახალ ფაზაში. უილიამ ლინის თქმით, სასიცოცხლოდ მნიშვნელოვანი გახდა ვირტუალური განზომილების შესაძლებლობების სწორი შეფასება და აღიარება, რომ კიბერ-სივრცე გახდა ახალი ტიპის სამხედრო ქმედებების მოედანი.

დღევანდელ დღეს, კიბერ-შეტევები უმეტეს წილად მიჩნეულია საინფორმაციო ომის ინსტრუმენტად, სამხედრო-სტრატეგიული და პოლიტიკური მიზნების მისაღწევად. ტერმინი „საინფორმაციო ომი“ კაცობრიობისათვის ცნობილია ჯერ კიდევ ძველი ბერძნული წყაროებიდან. მაშინდელი საინფორმაციო ომის გამოვლინებად ჩათვლილია დეზინფორმაციის გავრცელება ერთი მხარეს სამხედრო საბრძოლო რიგებში მეტოქეს სიძლიერისა და მრავალრიცხოვნობის შესახებ მეომრების მორალური და ფსიქოლოგიური სულისკვეთების დისტრუქციის მიზნით. დღეს კი, ინფორმაციული ომის წარმოებამ განიცადა სრული ტრანსოფმრაცია, ჩამოყალიბდა ცალკეულ საბრძოლო იარაღად და მიჩნეულია ჰიბრიდული ომის წარმოების კომპონენტად. ფრენკ ჰოფმანის თანამედროვე კონფლიქტების ანალიზში ჩამოყალიბებულია ჰიბრიდული ომის კონკრეტული დეფინიცია. ის წერს, რომ ჰიბრუდული ომი არის სხვადასხვა არასაომარი ტაქტიკის, კრიმინალური ქცევის, პროპაგანდისა და ინფორმაციული ომის ელემენტების კოლაბორაცია.[10] ჰიბრიდული ომის მთავარი არსი მდგომარეობს მის არატრადიციულობაში და ექსპერტის თქმით,

---

9 Stuxnet, Война 2.0, 2010 - https://habr.com/ru/post/105964/

10 F. Hoffman, F.G. Hybrid Warfare and Challenges, JFQ / issue 52, p. 34, 2009

მსგავსი სტრატეგია მოწინავე პოზიციაზე აყენებს საბრძოლო ქმედებების წარმოებას არასამხედრო გზით. ვ. მაისაია და გ. მაღრაძის 21-ე საუკუნის საერთაშორისო პოლიტიკაში ჰიბრიდულ ომს ასიმეტრიული საფრთხეების რიცხვში მოიხსენიებენ. ამ ფორმატში, ავტორები აღნიშნავენ, რომ ისევე როგორც სხვა ასიმეტრიული საფრთხეები, ჰიბრიდული ომის ელემენტები მიმართულია სახელმწიფოს ყველაზე დაუცველ ობიექტებზე და ამ ობიექტების შემადგენლობაში დიდ წილად ქვეყნის კიბერ-სივრცე იგულისხმება.[11]საერთაშორისო უსაფრთხოების ექსპერტთა უმრავლესობა თანხმდება, რომ ჰიბრიდული ომის მწარმოებელი აქტორები შეიძლება შედგებოდეს როგორც რამდენიმე სახელმწიფოსგან, კერძო სექტორისა და კორპორაციებისგან, ასევე მათი კოლაბორაციისგან.

ჰიბრიდული ტიპის ომის მაგალითის აღწერა საკმაოდ რთული პროცესია, რადგან რაიმე აქტორის უშუალო ჩართულობისა და აგრესიული ხასიათის ქმედების მხოლოდ ირიბი მტკიცებულებები არსებობს. გარდა ამისა უნდა ითქვას, რომ ჰიბრიდული ომის წარმოება არის გრძელვადიანი პროცესი, რომლის მთავარი მიზანი არის მეტოქის შინაგანი დესტრუქცია და ხელის შეშლა სტრატეგიული მიზნების მიღწევაში. მიუხედავად ამისა, თანამედროვე ჰიბრიდული ომის გამოვლინებად მიჩნეულია რუსეთის ფედერაციის მიერ დივერსიული ხასიათის ქმედებები უკრაინის წინააღმდეგ. რუსეთ-უკრაინის კონფლიქტში ჰიბრიდული ომის პირველი თვალსაჩინო ეტაპი გახდა 2014 წლის ნახევარკუნძულ ყირიმის ანექსია. შემდომ პერიოდში რუსეთმა ჩაატარა საკმაოდ ბევრი ქმედება, მიმართული უკრაინის ეკონომიკური დისტაბილიზაციისაკენ. ისეთი როგორც, სავაჭრო გზების ჩაკეტვა ცენტრალურ აზიასა და მოსკოვთან, ენერგო-ექსპორტის შემცირება ზამთრის პერიოდში, კერჩის ხიდის მშენებლობა და აზოვის საზღვაო-სატრანზიტო ხაზების მონოპოლიზაცია და უკრაინა-ევროკავშირის თავისუფალი ვაჭრომის შესახებ ხელმშეკრულების დადებაში ხელის შეშლა სხვადასხვა ბერკეტის გამოყენებით. თუმცა, როგორც მიიჩენევენ თავად უკრაინული ექსპერტები,

[11] ვ. მაისაია, გ.მაღრაძე, 21-ე საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების“ თეორია: მითი და რეალობა - რეგიონული და გლობალური ასპექტები, გვ. 25-26. 2017 წ.

უმთავრესი და ურთულესი გამოწვევა უკრაინის სახელმწიფოსთვის აღმოჩნდა საინფორმაციო ომი და კიბერ-შეტევები. შეტევების მთავარი მიზანი იყო უკრაინის სამრეწველო და სახელმწიფო ინსტიტუტების სისტემები და მონაცემთა ბაზები, რომელზეც აქტიური კიბერ-თავდასხმები 2017 წელს ხორციელდებოდა ვირუსი "Petya.A"-ს გამოყენებით. გარდა ამისა, რუსეთის მხრიდან მიმდინარეობდა ფარული სოციალური კამპანიები მიმართული უკრაინული მთავრობის მხარდაჭერების კიბერ-ბულინგზე და პოლიტიკური ლიდერების დისკრედიტაციაზე სოციალურ ქსელებში. უკრაინის ფინანსთა ყოფილი მინისტრის ა. დანილიუკი თავის სტატიაში წერს:

„ჩვენ უნდა გავიაზროთ, რომ ამგვარი კონფლიქტის დასაძლევად ძლიერი არმია და სამხედრო ტექნიკა საკმარისი აღარ არის. მოსაგებად საჭიროა სტრუქტურული და ეკონომიკური ცვლილებები, რომელიც მიუღწეველია სისტემური რეფორმების ჩატარების გარეშე. ჩვენ გვესმის, რომ ეს არ არის მხოლოდ ჩვენი ომი. უბრალოდ, ჩვენ ავღმოჩნდით ფრონტის ყველაზე ცხელ წერტილში. ეს არ არის ლოკალური კონფლიქტი - ეს არის მსოფლიოს წესრიგის რეფორმირების მცდელობა და ამავე დროს, რუსეთის ფედერაცია ჰიბრიდულ ომში მთელს მსოფლიოს ჩართავს" – [ა. დანილიუკი, 2018[12]]

რუსეთ-უკრაინის კონფლიქტის მაგალითიდან ჩანს, რომ ჰიბრიდული ომის წარმოება არ იფარგლება საბრძოლო ან სამხედრო დაპირისპირებით. ეს არის კომპლექსური ქმედება, რომლის ფარგლებში ობიექტის მრავალი სასიცოცხლოდ მნიშვნელოვანი ინფრასტრუქტურის და სტრატეგიის ჩამოშლაა შესაძლებელი. ხოლო, ვირტუალური კომპონენტის დაცულობა სწორედ სათანადო კიბერუსაფრთხოების სტრატეგიაზეა დამოკიდებული.

1.3 ეკონომიკური უსაფრთხოების ვირტუალური პარამეტრები

ნებისმიერი სახელმწიფოს ეროვნული უსაფრთხოების განუყოფელი შემადგენელი კომპონენტი არის ქვეყნის ეკონომიკური უსაფრთხოება. ეკონომიკური უსაფრთხოება

[12] Александр Данилюк, Гибридная война России. Что пережила Украина, 2018 - https://nv.ua/opinion/hibridnaja-vojna-rossii-chto-perezhila-ukraina-2468342.html

განაპირობებს სახელმწიფოს მეურნეობის, სოციალურ-ეკონომიკური სტაბილურობის, მოსახლეობის კეთილდღეობისა და ფინანსური სტრუქტურების ნორმალური ფუნქციონირების ასპექტებს, სხვადასხვა შიდა და გარე ფაქტორებისა და გამოწვევების პირობებში. ამ დროს, გლობალიზაციის პროცესი და ტექნოლოგიური ინტეგრაცია, ადამიანების ცხოვრებისა და მოღვაწეობის სხვადასხვა სფეროებთან ერთად, დიდ წილად ეკონომიკურ სფეროებშიც აღინიშნება. შეიძლება ითქვას, რომ ეკონომიკური და ფინანსური პროცესების უმეტესობა, როგორც ლოკალურ, ასევე გლობალურ დონეზე ტრანსოფრმირებულია ვირტუალურ განზომილებაში. ინტერნეტი წარმოადგენს ამ პროცესების ოპტიმიზაციის ახალ შესაძლებლობას, რომლის გამოყენებით მარტივდება როგორც ინფორმაციული გაცვლა, ასევე ვაჭრობის წარმოება, საბანკო-საკრედიტო და საკომუნიკაციო სისტემა, ფულადი ტრანზაქციების პროცესები, სისტემური გარდაქმნა ავტომატიზირებულ მმართვაზე სამრეწველო სფეროში და მრავალი სხვა. გლობალიზაცია გახდა თანამედროვე ეკონომიკის ერთ-ერთი უმთავრესი ტენდენცია, რომელმაც მოახდინა საკვანძო ტრანსფორმაცია მსოფლიოს ეკონომიკურ სისტემაში.

ვირტუალური სივრცის სტრუქტურის ძირითადი დამახასიათებელი ნიშანი არის ანარქიულობა. ამავე დროს, ეკონომიკა, ისევე როგორც მსოფლიოს საზოგადოების არსებობის სხვა კომპონენტები, წარმოადგენს სისტემას, რომლის ნორმალური ფუნქციონირება მრავალ შემადგენელ ფაქტორზეა დამოკიდებული. ამ ფაქტორების მაგალითი თვალსაჩინოა ეროვნული ეკონომიკური უსაფრთხოების ინდიკატორების ჩამონათვალში, რომლის მიხედვით გამოიყოფა ქვეყნის ეკონომიკური სტაბილურობისა და ნორმალური განვითარების რამდენიმე აუცილებელი ელემენტი[13]:

- წარმოების სფერო
- უცხოური ინვერსტიციები
- სტრატეგიული განვითარების პარამეტრები
- მოსახლეობის ცხოვრების დონე

[13] ეკონომიკური უსაფრთხოება: თეორია, მეთოდოლოგია, პრაქტიკა. ბ. ალადაშვილი, 2011, გვ. 84-93

- მაკროეკონომიკა და ფინანსური სტაბილურობა
- ფულად-საკედიტო სფერო
- სასურსათო უსაფრთხოება
- ენერგეტიკული უსაფრთხოება
- ერთიანი ეკონომიკური სივრცის უსაფრთხოება
- ეკონომიკის კრიმინალიზაციის დონე

ამ ჩამონათვალში არსებული ელემენტების ფუნქციონირება და სამუშაო პროცესის უდიდესი ნაწილი დღეს ვირტუალურ განზომილებაში მიმდინარეობს, რაც ოპტიმიზაციასთან ერთად, მთელი რიგი საფრთხეების მომტანია ეროვნული და გლობალური ეკონომიკისათვის. აქედან გამომდინარე, 21-ე საუკუნის ეკონომიკური უსაფრთხოების უზრინველყოფის აუცილებელი ნაწილი საინფორმაციო და კიბერ უსაფრთხოებაც გახდა.

ძირითადი ვირტუალური საფრთხეების ჩამონათვალიდან, ეკონომიკური უსაფრთხოების პირობებში უმთავრესი გამოწვევაა კიბერ-შპიონაჟი და კიბერ-შეტევები სახელმწიფო ინფრასტრუქტურის ვირტუალურ ელემენტებზე, რისი დამადასტურებელი მაგალითი იყო 2010 წლის „Stuxnet"-ის შეტევა ირანში და 2018 წლის ჩინური მიკროჩიპების საქმე. ორივე შემთხვევამ აშშ-სთვის, ჩინეთისა და ირანისთვის საკმაოდ მაღალი ეკონომიკური ზიანი მიაყენა. ამასთან ერთად, თანამედროვე ეკონომიკის კიდევ ერთ გამოწვევას წარმოადგენს კრიპტოვალუტა და მისი მზარდი როლი მსოფლიოს სავაჭრო და საბანკო-ფინანსურ პროცესებში.

მსოფლიო ისტორიის ბოლო ასი წლის მანძილზე, სწრაფი ტექნოლოგიური პროგრესის პირობებში მნიშვნელოვანი განვითარება საბანკო-საფინანსო სისტემაშიც აღინიშნება, რამაც დღეს განაპირობა ე.წ. ელექტრონული ვალუტის გამოჩენაც. სხვადასხვა თეორიის თანახმად, ელექტრონული ვალუტის კომფორტულობამ და პოპულარობამ შეიძლება გამოიწვიოს ფიზიკური ფულის სრული ჩანაცვლება მომავალში და დღევანდელ დღეს ამისთვის უკვე არსებობს ყველა საჭირო პირობა და

რესურსი.[14] ელექტრონული ვალუტის რიცხვი დღეს მოიცავს 1000-მდე სხვადასხვა ერთეულს, რომლის სტაბილურობა ვირტუალურ სავაჭრო პლატფორმებზე საკმაოდ ცვალებადია. მათ შორის ერთ-ერთი ყველაზე მყარი და გავრცელებულია ე.წ. ბიტკოინი (Bitcoin – BTC) არის, რომლის საბაზრო ფასი დღეს 8 000 აშშ დოლარს შეადგენს. ბიტკოინი წარმოადგენს მათემატიკურ ალგორითმს ან ელექტრონულ საგადასახადო პლატფორმას, რომელიც არ არის მიბმული არც ერთ საბანკო სისტემაზე ან რომელიმე სახელმწიფოს ეროვნულ ვალუტაზე. ბიტკოინის საგადასახადო პლატფორმას არ გააჩნია რაიმე კონტროლის მექანიზმი. ამ ვალუტის ერთეული სრულიად არის დამოკიდებული ვირტუალური მომხმარებლების მოთხოვნაზე და გამომუშავებაზე სპეციალიზებული კომპიუტერების მეშვეობით. ბიტკოინის შექმნის იდეა ჯერ კიდევ გასული საუკუნის 80-იან წლებში ჩაისახა, თუმცა მსგავსი ელექტრონული პლატფორმის შესაქმნელი საჭირო ტექნოლოგიები ჯერ კიდევ არ არსებობდა. განსაკუთრებული პოპულარობა ბიტკოინმა 2009-2010 წლებში მოიპოვა და მისი მთავარი ფუნქცია აგებულია პირდაპირ ელექტრონულ გადახდებზე მესამე პირის გარეშე, ისეთი როგორც ბანკი საკრედიტო ან სადებიტო ბარათების გამოყენების შემთხვევაში ან სახელმწიფო ვალუტა ფიზიკური ფულის შემთხვევაში. ტექნიკურად, ელექტრონული ვალუტა აგებულია ე.წ. „peer-to-peer" ტექნოლოგიაზე, რომელიც წარმოადგენს დეცენტრალიზებულ ქსელს. ამ ქსელის მეშვეობით ნებისმიერ მომხმარებელს შეუძლია ვალუტის პირდაპირი გადაცემა ან გადახდა, ხოლო ამ „ტრანზაქციას" ადასტურებენ ქსელის სხვა მომხმარებლები (ე.წ. მაინერები - Miners) თანაბარ პირობებში, რაც თავის დროს უარყოფითად მოქმედებს გაცვლის სისწრაფეზე. ტრანზაქციის (ბლოკების) დასტური ხერხდება სპეციალიზებული კრიპტოგრაფიული ხელმოწერის მეშვეობით და ყოველი ბლოკის დახურვის, ანუ დადასტურების შემდეგ, მომხმარებელი იღებს გარკვეულ საკომისიოს - ბიტკოინებს. ამრიგად, ყოველი მომხმარებელი და მისი კომპიუტერი წარმოადგენს დეცენტრალიზებულ ქსელს, რომელიც წააგავს ჩვეულებრივ საბანკო-სავალურო სისტემას, თუმცა ერთი საბანკო

[14] Роль криптовалю в современном мире. О.С. Зиниша, 2016 - https://iupr.ru/domains_data/files/zurnal_30/Zinisha%20O.S.,%20Syutkina%20E.%20S..pdf

სერვერის მაგივრად, ბიტკოინის ალგორითმი მიმაგრებულია ყველა მის მომხმარებელზე.[15] ამგვარი ელექტრონული ვალუტის ბუმს უარყოფითი თვისებებიც გააჩნია:

- არასტაბილურობა - ამ ვალუტის გამოყენებით შეუძლებელია რაიმე დაგროვებითი აქტივების შენარჩუნება. მისი საბაზრო ღირებულება სრულიად დამოკიდებულია მოთხოვნაზე, რომელიც საკმაოდ ფართო დიაპაზონის ფარგლებში მერყეობს.

- სახელმწიფო შეზღუდვა - რადგან ეს ვალუტა არ არის გამაგრებული არც ერთი ეკონომიკური სისტემით ან ფიზიკური ღირებულებებით, მოსალოდნელია მისი გამოყენების აკრძალვა სახელმწიფო ინსტიტურების მხრიდან. იმ სიტუაციაში, თუ ბლოქჩეინის მომხმარებლების უმრავლესობის კომპიუტერული ტექნიკა ასეთი სახელმწიფოს ტერიტორიაზეა განთავსებული, ვალუტაზე მოთხოვნა მნიშვნელოვნად შემცირდება და მის საბაზრო გაუფასურებას გამოიწვევს.

ბოლო წლებში, კრიპტოვალუტის გავრცელებამ მოიპოვა არაერთგვარი საზოგადოებრივი რეზონანსი. ამავე დროს, მსოფლიოს წამყვანი სახელმწიფოები ცდილობენ ამ ფენომენის სამართლებრივ ჩარჩოებში მოქცევას. ავსტრალიასა და აშშ-ში ბიტკოინი ოფიციალურ ღირებულებადაა აღიარებული და ნებისმიერი კომპანიის ინტერესიბან გამომდინარე დაშვებულია სავაჭრო საქმიანობის წარმოება მისი გამოყენებით. სინგაპურსა და ვირგინის კუნძილებზე საქონლის შესყიდვა ბიტკოინის ვალუტით იბეგრება ფიზიკურ ვალუტასთან იგივე პროცენტით და პირობებით. ევროპის 10 ქვეყნის სხვადასხვა ქალაქში დამონტაჟებულია ბიტკოინის ბანკომატი, ხოლო 2015 წელს, ევროპის უმაღლესი სასამართლოს დადგენილებით ბიტკოინის ყიდვა ფიზიკური ფულით შესაძლებელი იქნება დღგ-ს დაკისრების გარეშე.[16]

---

[15] Криптовалюта биткоин и её роль в экономике, П.В. Сухина, 2018 - https://alley-science.ru/domains_data/files/Janu18/KRIPTOVALYuTA%20BITKOIN%20I%20EYo%20ROL%20V%20EKONOMIKE.pdf

[16] Криптовалюта: роль в современном мире, И.М. Кравченко, 2015 - http://xn--90aeteg4bd.xn--p1ai/wp-content/uploads/2015/11/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%B

ბიტკოინის რამდენიმე სახელმწიფოს დონეზე აღიარების მიუხედავად, საერთაშორისო ეკონომიკის ექსპერტების საკმაოდ დიდი რიცხვი ელექტრონულ ვალუტაში თანამედროვე ეკონომიკის უდიდეს გამოწვევას ხედავს. პირველ არგუმენტად მიჩნეულია სახელმწიფოს ეროვნული ვალუტისა და ეროვნული ბანკების როლის დაკნინება და ეროვნული ვალუტის გაუფასურების წინაპირობის შექმნა. კრიპტოვალუტის საფრთხე სახელმწიფოსთვის მდგომარეობს მის ხელმისაწვდომობაში და რაც უფრო მეტი კომერციული ორგანიზანია დაუშვებს მისი საქონლის შესყიდვას ამ ვალუტის გამოყენებით, მით უფრო მცირდება სარგებელი სახელმწიფო ეკონომიკისათვის. გარდა ამისა, ბიტკოინის მზარდი პოპულარობა და მოთხოვნა ქმნის დამოკიდებულებას და ამ ვალუტის არასტაბილურობის გამო, მასზე დამოკიდებული კომერციული სტრუქტურები ან ინდივიდუალური პირები მუდმივად იმყოფებიან სრული გაკონტრების მაღალი რისკის ქვეშ. ისევე როგორც სხვა საფინანსო სისტემა, ბიტკოინის ბლოქჩეინები იმყოფებიან მუდმივი ჰაკერული თავდასხმების ქვეშ და კიბერ-შეტევების პრობლემა იკავებს მეორე ადგილს კრიპტოვალუტის განვითარების პროცესში. ჰაკერების მთავარი მიზანი წარმოადგენს სამომხმარებლო სისტემებში ჩარევას, წვდომის არალეგალური მოპოვება მომხმარებლების ე.წ. „ვირტუალურ საფულეებზე“ და ტრანზაქციების გადამისამართებას საკუთარ ანონიმურ ანგარიშებზე. ფასიანი ქაღალდების საერთაშორისო კომისიის განცხადებით, კიბერ-შეტევები განხორციელდა ბიტკოინის პლატფორმების 60%-ზე. მაგალითად, 2016 წელს DAO-ს ჰეჯ-ფონდის სისტემაში არსებული ხარვეზის გამო, ჰაკერებმა მოიპოვეს არასანქციონირებული წვდომა ფონდის წევრების ელექტორნულ საფულეებზე და მოახერხეს 150 მილიონი აშშ დოლარის გატაცება. კიდევ ერთი ცნობილი შემთხვევა ეხება ვირტუალური ბირჟის Bitfinex-ის შეტევას და ჰაკერების მიერ 70 მილიონი დოლარის გატაცებას.

B%D1%8E%D1%82%D0%B0-
%D0%9A%D1%80%D0%B0%D0%B2%D1%87%D0%B5%D0%BD%D0%BA%D0%BE-
%D0%98%D0%BB%D1%8C%D1%8F-
%D0%9F%D0%BE%D1%81%D1%82%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2-
%D0%BC%D0%B8%D1%85%D0%B0%D0%B8%D0%BB.pdf

იმის გათვალისწინებით, რომ კრიპტოვალუტა მიმაგრებულია მომხმარებლების პერსონალურ ტექნიკაზე, მისი უსაფრთხოების უზრუნველყოფა განსაკუთრებულად რთულდება. კრიპტოვალუტის მომავალი საკმაოდ ბუნდოვანია, თუმცა დაზუსტებით შეიძლება ითქვას, რომ ის მიმზიდველ წყაროს წარმოადგენს, როგორც ცალკეული ადამიანებისათვის, ასევე მსხვილი კომპანიებისათვის და ზოგ შემთხვევაში, ეს რესურსი შეიძლება ქვეყნის ეკონომიკური უსაფრთხოების გამოწვევად ჩამოყალიბდეს.

თავი II

კიბერუსაფრთხოების როლი საერთაშორისო უსაფრთხოებაში; გლობალურ, რეგიონულ და ლოკალურ დონეებზე

საერთაშორისო უსაფრთხოების ცნება მოიცავს საერთაშორისო ურთიერთობების უმნიშვნელოვანეს ინდიკატორებს, მათ შორის: განვითარების სტაბილურობას, გარე საფრთხეების დაძლევას, სუვერენიტეტისა და დამოუკიდებლობის უზრუნველყოფას და ყველა იმ ასპექტს, რომელიც სახელწიფოს სასიცოცხლო ინტერესს წარმოადგენს საერთაშორისო დონეზე. საერთაშორისო უსაფრთხოების მასშტაბი იყოფა რამდენიმე დონეებად:

- *ეროვნული დონე* - უსაფრთხოების უზრუნველყოფა ცალკე აღებული სახელმწიფოს შემთხვევაში, რომელიც მოიცავს სახელმწიფოს სუვერენიტეტის, დამოუკიდებლობისა და ტერიტორიული მთლიანობის წინააღმდეგ მიმართული აგრესიული ან საომარი ქმედებების მცდელობას. უსაფრთხოება ეროვნულ დონეზე ნიშნავს სახელმწიფოს საგარეო ან შინაგანი პოლიტიკის გატარების და ქვეყნის მოსახლეობის ნორმალური ცხოვრების ხელშეუხებლობის უზრუნველყოფას
- *რეგიონული დონე* - საერთაშორისო უსაფრთხოების დონე, რომელიც მოიცავს კონკრეტულ გეოპოლიტიკურ რეგიონს და რეგიონში შემავალ

სახელმწიფოების უსაფრთხოებას. ეროვნული უსაფრთხოების ინდიკატორების ერთობლიობას რეგიონულ დონეზე

- *გლობალური დონე* - გლობალური უსაფრთხოების უზრუნველყოფა მოიცავს ისეთი საკითხების დაძლევას, რომელიც შეიცავს საფრთხეს დედამიწის მოსახლეობისათის. გლობალური უსაფრთხოების უზრუნველყოფის საკითხებში შეიძლება ჩაითვალოს: საერთაშორისო ტერორიზმი, ნარკოტრაფიკი, მსოფლიოს ეკონომიკური სტაბილურობის შენარჩუნება, შეიარაღების კონტროლი, ეთნო-პოლიტიკური კონფლიქტები, რელიგიური და კულტურული მემკვიდრეობის შეუხებლობა და ეკოლოგიური საკითხები.

თანამედროვე მსოფლიოს განვითარების ფაქტორები დიდ წილად დამოკიდებულია გლობალიზაციის პროცესზე. ამ შემთხვევაში, გლობალიზაციის პროცესი მოიცავს ერთიანი მჭიდრო ფინანსურ-ინფორმაციული სივრცის არსებობას, რომლის პირობებში არის მოქცეული როგორც საზოგადოება, ასევე საერთაშორისო და ეკონომიკური ურთიერთობებიც. ამის გათვალისწინებით შეიქმნა პირობა, რომელშიც განსაკუთრებულ მნიშვნელობას იძენს ინფორმაციულ-ტექნოლოგიური კომპონენტი. გლობალიზაციის სხვა პროცესებთან ერთად, გაზრდილი როლი ეკუთვნის საერთშორისო ურთიერთობების არაინსტიტუციონალურ დემოკრატიზაციასაც.[17] სახელმწიფოებისა და საერთაშორისო ორგანიზაციებთან ერთად გლობალურ დონეზე გამოჩნდა მრავალი „არატრადიციული“ აქტორები, ისეთი როგორც: არასამთავრობო ორგანიზაციები, აქტივისტთა ჯგუფები, მოძრაობები, მასობრივი ინფორმაციის საშუალებების დივერსიფიციური წყაროები. ამ ჩამონათვალის ბოლო ელემენტი ახდენს განსაკუთრებულ გავლენას როგორც საზოგადოებრივი, ასევე პოლიტიკური ტენდენციების განვითარებაზე გლობალურ დონეზე.

კიბერუსაფრთხოების ელემენტები საერთაშორისო უსაფრთხოებაში შედარებით ახალი კომპონენტია. სხვა გლობალურ გამოწვევებთან პარალელურად, გასული

---

[17] Международная безопасность в условиях глобальной информационной революции. А.Е. Белянцев, стр. 311-312 - http://www.unn.ru/pages/e-library/vestnik/9999-0200_West_MO_2003_1/30.pdf

საუკუნის 1980-იანი წლებში ნეორეალიზმის ფარგლებში ჩამოყალიბდა „რბილი ძალის“ იდეა, რომელიც დღეს უკვე ცალკეულ და შემდგარ კონცეფციას წარმოადგენს.[18] საფრთხეს, რომლის წყაროდ ვირტუალური სივრცე ითვლება ხშირად ზუსტად „რბილი ძალის“ კონცეფციის ფარგლებში მოიაზრებენ. იმ დროს როცა პოლიტიკური რეალიზმის გადმოსახედიდან, საერთაშორისო ურთიერთობების მთავარი აქტორები სახელმწიფოები არიან, არასახელმწიფოებრივი ძალები და მათი როლი დღეს სცილდება კლასიკურ პოლიტიკურ თეორიებს და წარმოადგენს კვლევისა და დაკვირვების ცალკეულ ობიექტს.[19] საერთაშორისო უსაფრთხოების უმთავრეს გამოწვევას ამ ძალების მრავალფეროვნებაც წარმოადგენს. მრავალპოლარული მსოფლიო წესრიგისა და საინფორმაციო-ტექნოლოგიური მიღწევების პირობებში რაიმე აქტორის ინტერესების ამოცნობა ან პროგნოზირება რთულდება. განსაკუთრებით იმ პირობებში, როდესაც აქტორებად ითვლება ცალკეული ჯგუფები, გავლენიანი პირები ან კორპორაციები. აქედან გამომდინარე შეიძლება ითქვას, რომ ისევე როგორც საერთაშორისო ურთიერთობების აქტორები და ინტერესთა პოლუსები, ტრანსოფმრაციის პირობებში საერთაშორისო უსაფრთხოების დონეებიც იმყოფებიან.

---

[18] Концепция «мягкой силы» в современной теории международных отношений – Н. Минасян, 2017 - https://cyberleninka.ru/article/v/kontseptsiya-myagkoy-sily-v-kontekste-teoriy-mezhdunarodnyh-otnosheniy

[19] Кибербезопасность как основной фактор национальной и международной
безопасности XXI века – Е.Г. Коновалова, стр. 13-16.

2.1 - გლობალური, რეგიონული და ლოკალური დონეების ტრანსფორმაცია და გლობალიზაციის კონცეფცია

მსოფლიოს ისტორიისათვის გლობალიზაცია არ წარმოადგენს სიახლეს. რომაული იმპერიის ჰეგემონია ხმელთაშუა ზღვაზე და ალექსანდრე მაკედონელის კამპანია მიჩნეულია გლობალიზაციის პირველ გამოვლინებად ანტიკურ ეპოქაში. ხოლო შემდგომ, გლობალიზაციის ელემენტები შეიმჩნეოდა შუა საუკუნეების დასავლეთ ევროპული საბაზრო ურთიერთობების განვითარებაში და უფრო გვიან, პირველი ტრანსნაციონალური ჰოლანდიური ოსტინდოეთის სავაჭრო კომპანიის გამოჩენის დროს. გლობალიზაცია წარმოადგენს ურთიერთკავშირების შემჭიდროვებას ცხოვრების სხვადასხვა ფრაგმენტებისა და სოციუმებს შორის. პირველ რიგში ეს ეხება ეკონომიკას, ფინანსური კავშირებს, საერთაშორისო პოლიტიკას, სოციალურ-კულტურულ ურთიერთობებს, საინფორმაციო-გაცვლით პროცესებსა და სხვას. გლობალიზაცია უწყობს ხელს დედამიწის ცივილიზაციისა და კულტურის

უნივერსალიზაციას და სხვადასხვა სისტემის ტრანსნაციონალიზაციას.[20] გლობალიზაციის პროცესმა დღეს, ისევე როგორც საინფორმაციო ტექნოლოგიების ინტეგრაციამ, შეეხო ადამიანის მოღვაწეობისა და ცხოვრების ყველა სფეროს. ზუსტად ამიტომ, ინტერნეტ-ტექნოლოგიების ინტეგრაცია და უნივერსიფიკაცია მსოფლიოში ითვლება გლობალიზაციის პროცესის ერთ-ერთ ყველაზე მნიშვნელოვან თვალსაჩინო კომპონენტად.

გლობალიზაციის პროცესის გავლენა სხვადასხვა სფეროზე გამოკვლეულია ბევრი თეორეტიკოსა და მეცნიერის მიერ. სხვადასხვა ვკლევის შედეგი და მეცნიერული ხედვა ორიენტირებულია იმის დასადგენად, თუ რამდენად დიდია გლობალიზაციის პროცესების გავლენა როგორც საზოგადოებაზე, ასევე ეკონომიკურ და პოლიტიკურ ინსტიტუტებზე და ამ გავლენების უარყოფითი და დადებითი თვისებები. გლობალიზაციის პროცესების ბრიტანელი მკვლევარი როლანდ რობერტსი აქვეყნებს შეხედულებას, რომლის თანახმად გლობალიზაციის ეკონომიკურ და პოლიტიკურ ასპექტებთან პარალელურად, გლობალური შემჭიდროვების პროცესმა ადამიანების სოციალურ-ფსიქოლოგიური ტენდენციების ტრანსფორმაციაც მოახდინა, რამაც განაპირობა მსოფლიოს გარდაქმნა „ერთიან სოციალურ-კულტურულ განზომილებად“. რობერტსონი წერს, რომ ერთიანი განზომილების ფარგლებში, მსოფლიოს სხვადასხვა წერტილებში მომხდარი ესა თუ ის მოვლენა დღეს წარმოადგენს ერთიანი ურთიერთდამოკიდებული პროცესის ელემენტების ერთობლიობას.[21] შემუშავებული თეორიის თანახმად, მკვლევარი ახარისხებს გლობალიზაციის თანამედროვე ტენდენციის 2 კომპონენტს, ესენია: გლობალური საზოგადოების ინსტიტუციონალიზაცია და უსაფრთხოებისა და საერთაშორისო ურთიერთობების ლოკალური დონის გლობალურ დონესთან გაიგივება. ბოლო პუნქტის თანახმად, რობერტსონი უსვამს ხაზს თანამედროვე გლობალური აქტორების გავლენას ლოკალურ აქტორებზე. პრაქტიკულად, ეს გულისხმობს დასავლური

---

[20] Глобализация и национальная безопасность, А.Д. Урсул, Т.А. Урсул, 2012 - http://www.nbpublish.com/library_get_pdf.php?id=18450

[21] Globalization: Social Theory and Global Culture, R. Robertson, 1992 - https://sk.sagepub.com/books/globalization

ღირებულებების მასობრივ გავრცელებას, მსოფლიო პროცესების სტანდარტიზაციას, ტრანს-ნაციონალური კორპორაციების როლს ლოკალურ ეკონომიკებში, ასიმეტრიულ ურთიერთდამოკიდებულებას სხვადასხვა სახელმწიფოს შორის და საზოგადოებრივი ფსიქოლოგიის იდენტურობის ელემენტებს მსოფლიოს შორეულ წერტილებში. საერთაშორისო ურთიერთობებისა და უსაფრთხოების დონეების ტრანსფორმაციის კიდევ ერთი თეორია გამოქვეყნებული იყო ჯერ კიდევ 1999 წელს ბრიტანელი მკვლევარი მალკოლმ უოტერსის მიერ. მან გამოთქვა მოსაზრება, რომ გლობალიზაციის ერთ-ერთი შედეგი არის ფიზიკურ-ტერიტორიული საზღვრების ფაქტობრივი წაშლა, რომელიც კარგად იგრძნობა სავაჭრო-ეკონომიკურ და საინფორმაციო ურთიერთობებში. მკვლევართა ნაწილი, უოტერსა და რობერტსთან ერთად თანხმდება, რომ გლობალიზაციის პროცესის ელემენტები გავლენას ახდენს როგორც საზოგადოების სოციალურ-კულტურულ ცხოვრებაზე, ასევე საერთაშორისო ურთიერთობებზე და სახელმწიფოთა ურთიერთდამოკიდებულებაზე, ხოლო ტექნოლოგიური პროგრესი ამ ურთიერთდამოკიდებულების ასიმეტრიულობას უწყობს ხელმს. ამ იდეების შედეგად, საერთაშორისო ურთიერთობების ანალიზში ჩამოყალიბდა ტრანსფორმატიზაციის თეორია. ტრანსფორმისტები ამტკიცებენ, რომ კლასიკური ეროვნული სახელმწიფოს მოდელი გლობალიზაციის პირობებში სისტემურად იცვლება, რასაც ამტკიცებს კავშირების ხასიათის ტრანსფორმაცია სახელმწიფოს სუვერენინეტის, ტერიტორიულობისა და მმართველობის ინსტიტუტებს შორის. მიუხედავად იმისა, რომ სახელმწიფოს გააჩნია დომინანტური როლი საკუთარი ტერიტორიის ფარგლებში, სახელმწიფოში მიმდინარე პროცესები უფრო მეტად არის დამოკიდებული ტრანსნაციონალურ პროცესებზე და ნებისმიერი სახელმწიფოს ამ ტენდეციების შესაბამისი ადაპტირება უწევს.[22]

ტრანსოფორმატიზაციის თეორიის სასარგებლოდ შეიძლება ჩაითვალოს არგუმენტი, რომ გლობალიზაციამ საკვანძო ცვლილება მოახდინა სახელმწიფოს ინტიტუტებზე და ამ ინტიტუტების სისტემურ მუშაობაზე. გლობალიზაციის პროცესების გავლენა ნათლად

[22] Теории глобализации в контексте постклассической парадигмы, Л.Г. Кирьянова, О.А. Мазурина, 2007 - https://core.ac.uk/download/pdf/53066059.pdf

ჩანს სახელმწიფოს როგორც შინაგან, ასევე საგარეო პოლიტიკაზე. სახელმწიფოს შინაგანი ინსტიტუტები იმყოფებიან ინტერნაციონალიზაციის პირობებში, რასაც შეუწყო ხელი სახელმწიფოთაშორისო ურთიერთობების შემჭიდროვებამ. შედეგად, სახელმწიფო ინტიტუტების გავლენის სფეროებისა და სისტემების მუშაობა უკვე არ ეფუძნება მხოლოდ ამ სახელმწიფოს შიდა პროცესებზე და მოთხოვნებზე, არამედ ფუნქციონირებს საერთაშორისო საზოგადოების ჩამოყალიბებულ ინტერესებზე. მაგალითად, სახელმწიფოს ეკონომიკა და მისი ფუნქციები დღეს უფრო მეტად არის დამოკიდებული ტრანსნაციონალური კორპორაციების (ტნკ) მიერ ნაკარნახევი საერთაშორისო საბაზრო სტანდარტებზე. ფაქტია, რომ ტრანსნაციონალური კორპორაციებს უკავია საკვანძო როლი გლობალური ეკონომიკური სისტემის ფორმირებაში.[23] გაერო-ს მიერ შემუშავებული დეფინიციის თანახმად, ტნკ-ს სტრუქტურა შედგება კომპანიის ცენტრის მიერ დეცენტრალიზებული ფილიალების ქსელისგან სხვადასხვა რეციპიენტ-სახელმწიფოებში. უნდა აღინიშნოს, რომ მსოფლიოში ჯერ კიდევ არ არსებობს ტნკ-ს ზუსტი განსაზღვრა. სხვადასხვა მონაცემების მიხედვით, კომპანია ტრანსნაციონალურია თუ მისი აქტივების 25-30% არ იმყოფება უშუალო ცენტრის სახელმწიფოში და თუ მას გააჩნია 2 ან მეტი საერთაშორისო ფილიალი. სწორედ ამიტომ სხვადასხვა წყაროში განსხვავდება ტნკ-ს ჯამური რიცხვი მსოფლიოში, ისევე როგორც მათი წილი და როლი სხვადასხვა სახელმწიფოს ეკონომიკაში. ეკონომიკური ინტერესის თვალსაზრისით, ტნკ-ს მთავარი ფუნქცია არის კომერციული მოგება და რაც უფრო მსხვილია ესა თუ ის კორპორაცია, მით უფრო დიდ როლს ასრულებს მისი ინსტიტუტი სახელმწიფოს ეკონომიკურ სისტემაში.[24] მეორეს მხრივ, ტნკ-ს მოღვაწეობის უკან ყოველთვის დგას კონკრეტული ადამიანთა ჯგუფი, რომელსაც ხშირად გააჩნია როგორც იდეოლოგიური, ასევე პოლიტიკური ინტერესები. ასეთი ორგანიზაციის მაგალითი არის რუსული ენერგეტიკული კორპორაცია გაზპრომი, რომელიც წარმოადგენს ტნკ-ს ერთგვარ

---

[23] The impact of Globalization on the State Functions, V. Portugimov, 2011, p. 86-87

[24] Multinational Corporations, Wikipedia – The Free Encyclopedia - https://en.wikipedia.org/wiki/Multinational_corporation

კოლაბორაციულ ფორმას სახელმწიფო სტრუქტურასთან ერთად. 1990-იანი წლებიდან, გაზპრომის აქციების 40% ეკუთვნის სახელმწიფოს და ვლადიმერ პუტინის მმართველობის პირველი წლებიდან გაზპრომი არის საკვანძო ბერკეტი რუსეთის ფედერაციის დასავლური საგარეო პოლიტიკის გატარებისა და ინტერესების მიღწევაში. ეს გახდა შესაძლებელი 2001 წლის შედგომ, როდესაც ევროპაში შეიცვალა დამოკიდებულება ახლო აღმოსავლეთის ქვეყნების მიმართ და გაზისა და ნავთობ-პროდუქტების ალტერნატიული მსხვილი იმპორტიორის მოძებნის საჭიროება ჩამოყალიბდა. ამის შედეგან ევროპულ ენერგეტიკულ რუკაზე გამოჩნდა რუსეთის ფედერაციის მიერ შემოთავაზებული კომპანია გაზპრომი. სამართლიანია იმის აღნიშვნა, რომ ტნკ გაზპრომი წარმოადგენს ცალკე კორპორაციას საკუთარი მონოპოლიით რუსეთის გაზისა და ნავთობის მრეწველობაში და ამავე დროს, ამ მონოპოლიას უწყობს ხელმს უშუალოდ სახელმწიფო საკუთარი რიტორიკის გასატარებლად საერთაშორისო დონეზე. თუმცა, ასეთი მაგალითი მსოფლიოში იშვიათია. ტნკ-ს რიცხობრივი კუთხით, ყველა რეიტინგის პირველი ადგილი უკავია ამერიკის შეერთებულ შტატებს და მის ტერიოტორიაზე დაბინავებულ კორპორაციების ცენტრებს. Global Fortune 500 - ის რეიტინგის თანახმად, ყოველწლიური სალიდერო პოზიცია ტნკ-ს რაოდენობით ზუსტად აშშ-ს ეკუთვნის. ასეთი უპირატესობის საფუძველი გამომდინარეობს თვით აშშ-ს შიდა პოლიტიკური სტრუქტურისაგან, ისევე როგორც ამ სახელმწიფოს წამყვანი პოზიციიდან მსოფლიო არენაზე. ლიბერალური სავაჭრო პოლიტიკისა და სხვა წამყვან ქვეყნებთან შემუშავებული სტაბილური ეკონომიკური და პოლიტიკური ურთიერთობების ფონზე, ამერიკულმა პროდუქტმა მსოფლიოში უზარმაზარი პოპულარობა მოიპოვა და შეუწყო ხელი ამერიკული კორპორაციების ექსპანსიას, როგორც სავაჭრო, ასევე ადამინური რესურსებისა და ინტელექტუალური პოტენციალის თვალსაზრისით. ტნკ-ს რიცხობრივი ლიდერები აშშ-სთან ერთად არის დიდი ბრიტანეთი, ჩინეთი, იაპონია, გერმანია, საფრანგეთი, რუსეთი და სხვა მსოფლიოს წამყვანი სახელმწიფოები. გასათვალისწინებელია ისიც, რომ ტნკ-ს ცენტრი სახელმწიფოების რიცხვი ემთხვევა მსოფლიო არენაზე ჩამოყალიბებული ეკონომიკური ლიდერი სახელმწიფოების ჩამონათვლს, რაც კიდევ ერთხელ უსვამს

ხაზს ტრანსნაციონალური კორპორაციების როლს ამა თუ იმ სახელმწიფოს ეკონომიკაში.

დღევანდელ დღეს, ტრანსნაციონალიზმი გახდა გლობალიზაციის პროცესის ყველაზე მნიშვნელოვანი დამახასიათებელი ნიშანი. კომერციულ კომპანიებთან ერთად, საერთაშორისო დონის მოთამაშეების რიცხვს დაემატა რელიგიური, სამართლებრივი, ეკოლოგიური, საქველმოქმედო და სხვა ორგანიზაციები, რომლებიც მონაწილეობას იღებენ საერთაშორისო საზოგადოების აზრების, ტენდენციებისა და ხასიათის ფორმირებაში. ტექნოლოგიურმა განვითარებამ და ინტერნეტმა საინფორმაციო დინების სახელმწიფო-სამართლებრივ კონტროლს პრაქტიკულად შეუძლებელს ხდის. ამასთან ერთად, აღსანიშნავია, რომ გლობალიზაციის პროცესის გავლენა სხვადასხვა სახელმწიფოზე განსხვავდება.

გაეროს ყოფილი გენერალური მდივანი კოფი ანანის თქმით, გლობალიზაციის უპირატესობების დანახვა მარტივია, თუმცა მისი „ჩამალული“ უარყოფითი მხარე ზუსტად მის არათანაბარ გადანაწილებაში მდგომარეობს. გლობალიზაციის ორი მთავარი ინდიკატორი არის მისი პროცესებით გამოწვეული გავლენის მაჩვენებელი სახელმწიფოზე და ამ გავლენის კონტროლის მექანიზმები. პარამეტრების მხრივ, გლობალიზაციის მაჩვენებელი განსხვავდება გავლენის სფეროების მიხედვით. ზოგ ქვეყანაში ეს შეიძლება იყოს ეკონომიკური სისტემის ოპტიმიზაცია ან მაღალი ტექნოლოგიების ინტეგრაცია, ხოლო სხვაში, გამოიწვიოს სახელმწიფო-საზოგადოებრივი კრიზისი. მაგალითად სამხრეთ აფრიკა, სადაც 90-იანი წლების მიწურულს გადაწყვეტილი იყო სხვადასხვა ქალაქში ბანკომატების ქსელის დამონტაჟება და ერთ-ერთი ტნკ-ს პროდუქციის გავრცელება მობილური ტელეფონების სახით. ამ გადაწყვეტილებას არ მოჰყოლია დადებითი შედეგი, რადგან ქვეყნის მოსახლეობის ცხოვრების დონის მაჩვენებელი დარჩენილი იყო საკმაოდ დაბალ საფეხურზე და მოთხოვნა პროდუქციაზე არ გაიზარდა, ხოლო ჩადებულმა ინვესტიციებმა როგორც კორპორაციის, ასევე სახელმწიფოს მხრიდან გამოიწვია არსებითი ეკონომიკური პრობლემები სრული ქვეყნის მასშტაბით. საპირისპირო შემთხვევები ხშირია გარდამავალი ეკონომიკის მქონე ქვეყნების რიგში. როდესაც

ინფორმაციული გლობალიზაციის პროცესები ახდენს გავლენას მოსახლეობის მენტალობაზე და ხასიათზე, საზოგადოების დიდი ნაწილის მიზანი ხდება საკუთარი ცხოვრების აწყობა დასავლური ღირებულებების მიხედვით: უკეთესი განათლების მიღება, შრომის უფრო მაღალი ანაზღაურება, ინფრასტრუქტურულად და ტექნოლოგიურად უფრო განვითარებულ ქვეყანაში ცხოვრება. ამგვარი საზოგადოებრივი მოთხოვნების დაკმაყოფილების სახელმწიფო უუნარობა ქმნის საბაბს ქვეყნის ინტელექტუალური პოტენციალის გადინებას რაც წარმოადგენს გამოწვევას ქვეყნის ეროვნული უსაფრთხოებისათვის. საერთაშორისო ეკონომიკისა და ურთიერთობების თანამედროვე მდგომარეობა დიდ წილად დამოკიდებულია ზუსტად სავაჭრო-საფინანსო და კომერციულ სახელმწიფოთაშორისო ურთიერთობებზე. გლობალური ეკონომიკა დღეს წარმოადგენს ერთიან საბაზრო სისტემას, სადაც სისტემის მუშაობას განაპირობებს კაპიტალი. სახელმწიფოს ეროვნულ მეორნეობის ინსტიტუტი უფრო მეტად ხვდება გლობალიზაციის უნიფიკაციის პროცესის ფარგლებში, რომელსაც განაპირობებს სხვადასხვა საერთაშორისო შეთანხმება, ხელშეკრულება, კონვენცია და ა.შ. შედარებით სუსტი პოტენციალის მქონე სახელმწიფოებს უფრო ხშირად უწევს ადაპტირება მაღალ განვითარებული ქვეყნების მიერ შექმნილ რიტორიკასა და წესრიგზე, რასაც შედეგან მოჰყვება ქვეყნებს შორის ასიმეტრიულ ურთიერთდამოკიდებულებას.[25]

გლობალიზაციის ერთ-ერთ დადებით მხარედ ითვლება თანამედროვე ტექნოლოგიების გავრცელება. ინფორმაციულ-ტექნოლოგიურმა ინტენსიფიკაციამ შეუწყო ხელი მსოფლიოს გლობალურ დემოკრატიზაციასა და სისტემების დეცენტრალიზაციას. გარდა ამისა, გლობალური ვირტუალური ქსელის მეშვეობით ფაქტობრივად წაშლილია ტერიტორიული შეზღუდვები კომუნიკაციისათვის, როგორც საზოგადოებისათვის, ასევე კორპორაციებისათვისაც. ზუსტად ეს ფაქტორი იდეალური საბაბია ტნკ-ს უფრო ინტენსიური ექსპანსიისათვის და ახალი საზოგადოებრივი ჯგუფებების ჩამოყალიბებისათვის და მათი იდენტურობის ფორმა სცილდება

[25] Неравномерность развития мирового хозяйства в условиях глобализации, Н.Н. Думная, 2013 - http://www.mirkin.ru/_docs/_dumnaya/neravnomer.pdf

ეროვნულ-ტერიტორიულ დამახასიათებლებს. მსგავსი ორგანიზაციები დღევანდელ დღეს წარმოადგენენ საერთაშორისო ურთიერთობების ახალ სუბიექტებს. საერთაშორისო ურთიერთობების ასეთი ფორმა ბევრი ასპექტით ემთხვევა ნეოკლასიკური რეალიზმის თეორიას, რომლის თანახმად სახელმწიფოთაშორისო ურთიერთობები დიდ წილად აგებულია სავაჭრო კომუნიკაციებზე და ამ ურთიერთობების მამოძრავებელი მექანიზმები სახელმწიფოებთან ერთად ლოკალური არასახელმწიფოებრივი სუბიექტები აყალიბებენ.

ამრიგად, საერთაშორისო ურთიერთობებისა და მსოფლიო წესრიგის ტრანსფორმაციამ და ინტერნაციონალიზაციამ მოიტანა ახალი გამოწვევების რიგი საერთაშორისო უსაფრთხოებისათის. ფიზიკურად და გეოპოლიტიკურად დაყოფილი საერთაშორისო უსაფრთხოების უზრუნველყოფა სამი დონის მიხედვით ბევრ თანამედროვე ასპექტში კარგავს თავის ეფექტიანობას და უფრო ხშირად, ლოკალური და რეგიონული დონეები უნდა გამოიკვლიოს გლობალური საფრთხეებისა და გამოწვევების პერსპექტივიდან. აღნიშნულზე მეტყველებს ისეთი ფაქტორები როგორც:

- ლოკალური აქტორის საგარეო და შინაგანი პოლიტიკის ურთიერთდამოკიდებულება. კაპიტალის ფინანსური ნაკადი, ინფორმაცია, მიგრაცია, ტერორიზმი და ეკოლოგიური პრობლემები აიძულებს სახელმწიფოს ჩამოაყალიბოს ლოკალური უსაფრთხოების სტრატეგია გლობალური საფრთხეების გათვალისწინებით
- ეროვნული და გლობალური უსაფრთხოების უზრუნველყოფის კოლაბორაცია. ზუსტად გლობალური დონის საფრთხეებიდან გამომდინარე ცალკე აღებული სახელმწიფოს შინაგანი პოლიტიკა უფრო ხშირად მოქცეულია გლობალური უსაფრთხოების სტანდარტიზაციის ფარგლებში, რაც გლობალურ ინტერესებს სახელმწიფოს ეროვნულ ინტერესებთან თანაბარ დონეზე აყენებს
- საერთაშორისო ურთიერთობების ახალ სუბიექტებთან პარალელურად იზრდება საერთაშორისო არასამხედრო (ასიმეტრიული) საფრთხეების პოტენციალიც. უმეტეს წილად, ეს ეხება ტერორისტულ ორგანიზაციებს და მათი

გავლენის არეალს, რომელსაც გააჩნია თანაბარი პარამეტრი საერთაშორისო უსაფრთხოების უზრუნველყოფის ყველა დონეზე

- კოლექტიური უსაფრთხოების კონცეფციის მზარდი როლი გლობალური გამოწვევების წინააღმდეგ. ეს ფაქტორი გამოწვეულია არათანაბარი ინფორმაციულ-ტექნოლოგიური და ეკონომიკური განვითარებით და საერთაშორისო მჭიდრო ურთიერთდამოკიდებულების ასიმეტრიზმით
- საინფორმაციო-ტექნოლოგიური გახსნილობა და მასიური ხელმისაწვდომობა წარმოადგენს გამოწვევას როგორც ეროვნული, ასევე გლობალური სამართლებრივი მექანიზმებისათვის. ადამიანის უფლებების ხელშეუხებლობისა და პირად ცხოვრებაში ჩაურევლობის პოლიტიკა ართულებს საინფორმაციო ტექნოლოგიების გამოყენების სახელმწიფოებრივ კონტროლს. გლობალური ქსელისა და ვირტუალური ტერიტორიების არარსებობის ფონზე არასათანადო კონტროლი იწვევს თანაბარ საფრთხეს როგორც ლოკალურ, ასევე რეგიონულ და გლობალურ დონეზე

2.2 - კიბერუსაფრთხოების პრაქტიკა ევროპული კოლექტიური უსაფრთხოების სტრატეგიის ფარგლებში

თანამშრომლობითი (კოლექტიური) უსაფრთხოების თეორია უკავშირდება საერთაშორისო უსაფრთხოების ამერიკელ მკვლევარს რიჩარდ კოენს. მისი თეორიის ფაგლებში კოლექტიური უსაფრთხოებისა და კოლექტიური თავდაცვის გარდა, თანამშრომლობითი უსაფრთხოება მოიცავს კიდევ ორ კომპონენტს - სტაბილურობის შენარჩუნებასა და ინდივიდუალურ უსაფრთხოებას. ყოველი კომპონენტი აუცილებლად გასათვალისწინებელია სწორედ ახალი გლობალური გამოწვევების გამოჩენის ფონზე, ისეთი როგორც ტერორიზმი, კიბერ-დანაშაული, მიგრაცია, ეკოლოგია და მრავალი სხვა.[26]

კაცობრიობის ისტორიაში, კოლექტიური უსაფრთხოების მოდელი შემოთავაზებული იყო ჯერ კიდევ XVII საუკუნეში, კარდინალ რიშელიეს მიერ. სწორედ მის მიერ გამოთქმული მოსაზებების ნაწილი ჩადებული იყო 1648 წლის ვესტფალიის ზავში და კოლექტიური უსაფრთხოების თეორია ყველაზე ხშირად ზუსტად ევროპული ქვეყნების პოლიტიკაში შეიმჩნეოდა უფრო გვიანდელ პერიოდშიც. „მშვიდობიანი თანამშრომლობითი საზოგადოების“ იდეა ასევე გაჟღერებული იყო იმანუილ კანტის ნაშრომებშიც. თუმცა, მისი იდეის განსხვავება და ინოვაცია მდგომარეობდა იმაში, რომ უსაფრთხოება და სტაბილურობის შენარჩუნება ევროპაში უნდა შემდგარიყო ცალკე აღებული ქვეყნების სტრატეგიის შედეგად და არა კოალიციურად, სადაც ყალიბდება კონკრეტული სამმართველო ძალების ინტერესები. კანტი ამტკიცებდა, რომ თითოეული სახელმწიფო პასუხისმგებელია საზოგადოებრივ ქცევასა და ხასიათზე და მან უნდა უზრუნველყოს საზოგადოებრივი ტენდენციების ფორმიერება საკუთარი და კოლექტიური უსაფრთხოების ინტერესების გათვალისწინებით.[27]

---

[26] 21-ე საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების“ თეორია: მითი და რეალობა - რეგიონული და გლობალური ასპექტები, ვ. მაისაია, გ.მაღრაძე, გვ. 85-86. 2017 წ.

[27] Collective Security, Wikipedia the Free Encyclopedia - https://en.wikipedia.org/wiki/Collective_security#Theory

კოლექტიური უსაფრთხოების სტრატეგიის პრაქტიკურ-ისტორიული მაგალითი არის XX საუკუნის დასაწყისში შექმნილი ორგანიზაცია - ერთა ლიგა. ერთა ლიგის შექმნის მთავარი იდეა მდგომარეობდა დიპლომატიისა და დემოკრატიის პრინციპების გავრცელებაში, კონფლიქტების მშვიდობიანი გზით მოგვარებაში, გლობალური განიარაღებისა და მშვიდობის შენარჩუნების აიცილებლობაში პირველი მსოფლიო ომის შემდგომ პერიოდში. ორგანიზაციის 26 წლიანი არსებობის განმავლობაში, მან გააერთიანა ჯამში 63 ქვეყანა გლობალური მასშტაბით. ამავდროულად, ერთა ლიგის მოღვაწეობა არაერთხელ მოქცეულა კრიტიკის ქვეშ და საწინააღმდეგო არგუმენტების მთავარი მიზეზი გახდა მასში შემავალი ანტანტა-ს ყოფილი წევრი ქვეყნების პოლიტიკური ინტერესების დომინანტობა, რომელიც ორგანიზაციის სტრატეგიაში შეიმჩნეოდა. ერთა ლიგამ არსებობა 1946 წელს შეწყვიტა და მისი მუშაობის იდეები და ფუნქციები გაერთიანებული ერების ორგანიზაციას გადაეცა, რომელიც ისტორიიდან გამომდინარე მეტად წარმატებული აღმოჩნდა საერთაშორისო ურთიერთობების მშვიდობიანი მოგვარების თვალსაზრისით.

XX საუკუნის 90-იან წლებში საბჭოთა კავშირთან ერთად დაიშალა მსოფლიოს ბიპოლარული წესრიგიც. ამ მოვლენების შედეგან, საერთაშორისო ურთიერთობებში გააქტიურდა საუბარი კოლექტიური უსაფრთხოების იდეის ირგვლივ, რაც გამოწვეული იყო შეცვლილი გეოპოლიტიკური მდგომარეობის მიერ „ცივი ომის“ შედგომ პერიოდში. კაპიტალიზმის გამარჯვებამ შეუწყო ხელი გლობალიზაციის პროცესების ექსპანსიასა და პოსტ-საბჭოთა ქვეყნების დემოკრატიზაციას. ამასთან ერთად, შეიცვალა უსაფრთხოების უზრუნველყოფის მოდელიც კოლექტიური უსაფრთხოების სტრატეგიის ფარგლებში. ნეოკლასიკური რეალიზმის თეორიიდან გამომდინარე, საერთაშორისო ურთიერთობების არასახლმწიფოებრივ სუბიექტებთან ერთად, გლობალური პოლიტიკური პროცესების კოლექტივიზაციის ტენდენცია შეიმჩნევა. ამ ტენდენციის ფარგლებში გლობალური საფრთხეების დაძლევა კოლექტიური უსაფრთხოების სტრატეგიით ხორციელდება.

დღევანდელ დღეს, მსოფლიოს ყველაზე მსხვილი კოლექტიური უსაფრთხოების ორგანიზაცია არის ჩრდილოატლანტიკური ალიანსი - ნატო. ალიანსი შეიქმნა 1949

წლის 4 აპრილს 1948 წლის ბრუსელის შეთანხმების ხუთი ქვეყნის ხელმოწერის საფუძველზე, ესენია: ბელგია, ნიდერლანდები, ლუქსემბურგი, დიდი ბრიტანეთი და საფრანგეთი. უფრო გვიან, 1949 წლის ვაშინგტონის შეთანხმებამ ალიანსის წევრთა რიცხვი აშშ-სა და კანადის მონაწილეობით გაიზარდა, რამაც განაპირობა ორგანიზაციის გაფართოვება ევრო-ატლანტიკურ გეოპოლიტიკურ რეგიონზე. ორგანიზაციის შექმნის თავდაპირველი მიზანი ემსახურებოდა ევროპისა და ჩრდილოეთ ამერიკის წევრების უსაფრთხოებისა და სტაბილური განვითარების გარანტიას და ორგანიზაციის სტრატეგიის განხორციელება სრულიად ეყრდნობოდა გაერთიანებული ერების ორგანიზაციის მიერ შემუშავებულ პრინციპებს. ალიანსის კონცეფციის სამი ძირითადი მიმართულება არის კოლექტიური თავდაცვა, კრიზისების დარეგულირება და თანამშრომლობითი მექანიზმების შემუშავება უსაფრთხოების უზრუნველსაყოფად. ორგანიზაციის მიერ ოფიციალურად აღიარებული საფრთხეების რიგში მნიშვნელოვანი ყურადღება თანამედროვე გლობალურ საფრთხეებსაც ენიჭერბა.

„ცივი ომის“ დასასრულმა ევრო-ატლანტიკური ალიანსის სტრატეგიული ორიენტაციის ცვლილება გამოიწვია. კონკრეტულად ერთი გამოწვევა საბჭოთა კავშირის სახით შეწყვიტა არსებობა და „დღის წესრიგში“ გამოჩნდა სხვა, გლობალური საფრთხეების ჩამონათვალი. ეს საფრთხეები შედგებოდა რამდენიმე კომპონენტისგან:

- ლოკალური კონფლიქტები, რომლის კერა ნატო-ს წევრი-ქვეყნების გეოგრაფიულ სიახლოვეში იმყოფებოდა
- საერთაშორისო ტერორიზმი - რომელიც არსებობდა ბიპოლარულ ეპოქაში, თუმცა სსრკ - დასავლეთის კონფრონტაციის პერიოდში მეორეხარისხოვან მნიშვნელობას ატარებდა
- ასიმეტრიული საფრთხეები - იარაღით არალეგალური ვაჭრობა, ტრეფიკინგი, ნარკოტრაფიკი, ორგანოებით ვაჭრობა და სხვა

- საინფორმაციო უსაფრთხოება - ასიმეტრიული საფრთხეების კიდევ ერთი კომპოტენტი, რომლსაც განსაკუთრებული ყურადღება ბოლო 15 წლის მანძილზე მიენიჭა[28]

ჩამონათვალის ბოლო საფრთხის „პრობლემურობა“ არის მისი ბუნებისა და დესტრუქციული პოტენციალის დადგენა. ლონდონის საგარეო საქმეთა სამეფო ინსტიტუტის მიხედვით, ინფორმაციული საფრთხეების კლასიფიკაცია შედგება ისეთი გამოწვევებისაგან როგორც: 1) ინდივიდუალური პირების (ჰაკერების) ქმედება 2) ორგანიზებული დანაშაული, ჰაკერთა ჯგუფები 3) იდეოლოგიური და პოლიტიკური ექსტრიმიზმი ვირტუალურ სივრცეში 4) ინფორმაციული აგრესია სახელმწიფოების მხრიდან. ნატო-ს კიბერუსაფრთხოების ცენტრის ექსპერტები ხაზს უსვამენ ინტერნეტის მილიტარიზაციის ტენდენციას და აღნიშნავენ, რომ ვირტუალური სამყაროს ასეთი განვითარების ტრენდი სერიოზულ გამოწვევას წარმოადგენს როგორც გლობალური წესრიგის, ასევე ნატო-ს კოლექტიური უსაფრთხოების პრინციპებისათვის.[29] ნატო-ს ყურადღებამ კიბერ-საფრთხეების საკითხების მიმართ ოფიციალური სახე 2010 წლის ლისაბონის სამიტის სტრატეგიული კონცეფციის შედგენის დროს მიიღო. ამ კონცეფციის მიხედვით, ინფორმაციული შეტევები იდენტიფიცირებულია როგორც უმსხვილესი გამოწვევა ალიანსის წევრი-ქვეყნების განვითარებისა და უსაფრთხოების მიმართებაში. პოტენციური საფრთხე ვირტუალურ სოვცეში გაიგივებული იყო მასობრივი განადგურების იარაღის არალეგალურ გავრცელებასთან და საერთაშორისო ტერორიზმთან და ამის შემდგომ, კიბერუსაფრთხოება ტექნიკური დისციპლინიდან სტრატეგიულ კონცეპტად გარდაიქმნა.

ზოგადი თვალსაზრისით, კიბერუსაფრთხოების უზრუნველყოფა შეიცავს კომპლექსური სახის პრობლემებს, რომლებიც განსხვავდება საკუთარი წყაროებისა და მოტივით. უმთავრესი გამოწვევა დღეს არის საერთაშორისო კონსენსუსის არარსებობა. მსოფლიო ჯერ კიდევ არ შეთანხმებულა თუ რას წარმოადგენს „კიბერ-ომი“, „კიბერ-

---

[28] NATO and contemporary challenges and threats to euro-atlantic security, M. Volkov, p. 44-47

[29] НАТО и кибербезопасность, А.В. Казаковцев, стр. 110

შეტევა“, „კიბერ-ტერორიზმი“ ან „კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურა“. ამ ეტაპზე, არსებობს მხოლოდ ერთი მრავალმხრივი საერთაშორისო დოკუმენტი - კიბერ-დანაშაულის ბუდაპეშტის კონვენცია, რომელიც მიღებული იყო ევროპის საბჭოს მიერ 2001 წელს. კონვენცია მოიცავს კიბერ-დანაშაულის კლასიფიკაციასა და რეკომენდაციებს ლოკალური აღმასრულებელი და საკანონმდებლო მმართველობების მიმართ ამ ტიპის დანაშაულის იდენტიფიცირებისა და პრევენციისათვის.[30] 2019 წლისთვის კონვენცია რატიფიცირებულია 63 ქვეყნის, მათ შორის საქართველოს, სომხეთისა და აზერბაიჯანის მიერ. ჩრდილო-ატლანტიკური ალიანსის სტრატეგიაში კიბეუსაფრთხიების საკითხის გადასვლა უფრო მაღალი გადაწყვეტილების მიღების საფეხურზე 2002 წლის ქალაქ პრაღის სამიტის დროს გადაწყდა. ამ პერიოდიდან, ნატო-ს შვილობილ ორგანიზაციათა რიცხვს საკომუნიკაციო და საინფორმაციო სისტემის მომსახურების სააგენტო დაემატა, რომლის მიზანი გახდა კიბერ-დანაშაულის ხარისხობრივი ანალიზი, რეკომენდაციათა შემუშავება, რისკების პროგნოზირება და პრევენცია ნატო-ს კომპეტენციის ფარგლებში. კიბერუსაფრთხოების მეტად გაფართოვებული სტრატეგიის შექმნა საჭირო გახდა 2007 წლის ესტონეთის კიბერ-შეტევების სერიის შემდგომ. 2008 წლის ბუქარესტის სამიტის დროს, ნატო-ს წევრი ქვეყნების თავდაცვის მინისტრების დონეზე შედგა ოფიციალური სტრატეგიული კურსი (NATO Cyber Defence Policy), რომლის მიხედვით კიბერ-საფრთხე ნატო-ს წევრი ქვეყნის მიმართ ჩაითლებოდა აგრესიის გამოხატვის აქტად მთლიანი ალიანსის წინააღმდეგ და მსგავს ქმედებას მოჰყვებოდა ადრე შემუშავებული საპასუხო მექანიზმების ამოქმედება. უნდა აღინიშნოს, რომ ესტონეთის შემთხვევამ ევროპულ საზოგადოებაში საკმაოდ მაღალი რეზონანსი გამოიწვია. 2008 წელს ნატო-ს მიერ გაცემული აკრედიტაციით ესტონეთის ქალაქ ტალინში ამოქმედდა კიბერ-თავდაცვის კვლევის ცენტრი, რომელმაც შემდგომ საერთაშორისო სამხედრო ორგანიზაციის სტატუსი მიენიჭა. ამ ორგანიზაციის ძირითადი ფუნქცია არის თეორიული ბაზის შექმნა, კვლევითი ღონისძიებები ვირტუალური საფრთხეების დარგში და ზოგადი

[30] Conention on Cybercrime. Council of Europe, Europian Threaty Series – No. 185, Budapest, 23.11.2001, Chapter II – Measures to be taken at the national levels.

კონცეპტუალური რეგულაციების შემუშავება ნატო-ს წევრი ქვეყნებისა და პარტნიორი სახელმწიფოებისათვის. დღეს, ესტონეთი წარმოადგენს ნატო-ს ერთგვარ კიბერუსაფრთხოების ცენტრს, რომლის მონაწილეობა ალიანსის კიბერუსაფრთხოების სტრატეგიაში, ხშირ შემთხვევაში გადამწყვეტია. აღსანიშნავია ისიც, რომ 2008 წლის შემდგომ, ესტონეთი ითვლება ევროპის ლიდერად ვირტუალური ტექნოლოგიების ინტეგრაციისა და სისტემური დაცულობის თვალსაზრისით.[31]

ჩრდილო-ატლანტიკურ ალიანსთან პარალელურად, კიბერუსაფრთხოების პრობლემის დაყენება დღის წესრიგში ევროკავშირის სამმართველო ორგანოების შემთხვევაშიც გახშირდა. ევროკავშირის ორგანიზაციის მთავარი მიზანი არის ევროპული ქვეყნების სავაჭრო-ეკონომიკური, პოლიტიკური, იდეოლოგიური და თავდაცვითი პროცესების სტაბილური განვითარება. იმის გათვალისწინებით, რომ ამ პროცესების ინფრასტრუქტურული ბაზა მთლიანად ან ნაწილობრივ ვირტუალურ სივცეშია ტრანსფორმირებული, ევროკავშირი დიდ ყურადღებას ამ სივცის დაცულობას ანიჭებს. 2004 წლის მარტში შეიქმნა ევროკავშირის ინფორმაციული და ქსელური უსაფრთხოების სააგენტო - ENISA (European Union Agency for Network and Information Security). ორგანიზაციის უნიკალური სტრუქტურა შედგება როგორც ევროკავშირის მანდატის მქონე დიპლომატიური კორპუსისგან, ასევე კერძო სექტორისა და აკადემიური წრეების ექსპერთთა წარმომადგენლებისგან. როგორც აღინიშნება სააგენტოს ოფიციალურ ვებ-გვერძე, მისი მთავარი ფუნქცია არის კიბერ-საფთხეების წყაროს იდენტიფიცირება, შესაძლო რისკების განსაზღვრა კონკრეტული ქვეყნის და სრული ევროკავშირის მასშტაბით.[32] ორგანიზაცია მონაწილეობას იღებს ევროკავშირის სტრატეგიულ დაგეგმვაში და ევროპული საზოგადოების შემეცნებით პროცესში სტატიებისა და სახელმძღვანელოების გამოყენებით. ასევე, ENISA აქტიურად თანამშრომლობს ევროპის ბიზნეს-სექტორთან, სადაც სააგენტოს საექსპერტო

---

31 НАТО и кибербезопасность, А.В. Казаковцев, стр. 111-112

32 European Union Agency for Network and Information Security, About ENISA - https://www.enisa.europa.eu/about-enisa

გამოკვლევების საფუძველზე ხორციელდება კორპორატიული სისტემებისა და სამეწარმეო კრიტიკული ინფრასტრუქტურის უსაფრთხოების უზრუნველყოფა.

ევროპული კიბერუსაფრთხოების იზრუნველყოფის დარგში კიდევ ერთი საკვანძო მოთამაშე არის ევროპის თანამშრომლობისა და უშიშროების ორგანიზაცია - ეუთო, რომლის სრული საქმიანობის სპექტრში თანაბარ პოზიციას ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების უსაფრთხოებაც შედის. ეუთო-ს კიბერუსაფრთხოების სტრატეგია მიმართულია შემდეგ კომპონენტებზე:

- სახელმწიფოთაშორისო კომუნიკაციის გაღრმავება. ერთობლივი ღონისძიებებისა და საკონსულტაციო მექანიზმების შემუშავება პრობლემის დეესკალაციის მიზნით
- სახელმწიფოთაშორისო პლატფორმის შექმნა გამოცდილების გაზიარების მიზნით
- კონკრეტული მიზანმიმართული ქმედებები, რომელიც ავტორიზებული იქნება ეუთო-ს ყველა წევრი სახელმწიფოს მიერ და რომლის მიზანი იქნება კოლექტიური კიბერუსაფრთხოების სისტემის შემუშავება ადამიანის უფლებებისა და საერთაშორისო სამართლის პრინციპების გათვალისწინებით[33]

საერთაშორისო ორგანიზაციებისა და მათი შვილობილი სააგენტოების გარდა, ევროპულ საზოგადოებაში შექმნილია სხვადასხვა კომერციული და არაკომერციული ინსტიტუტების რიგი, რომლის უშუალო ფუნქცია ინტერნეტ-სივრცის დაცული გამოყენების უზრუნველყოფაში მდგომარეობს. ამ ტიპის ორგანიზაციები უწევენ ქსელურ მხარდაჭერას როგორც სახელმწიფოებრივ ინსტიტუტებს, ასევე კორპორაციებსა და ინდივიდუალურ მომხმარებლებს. ვირტუალური უსაფრთხოების უზრუნველყოფის დარგი გარკვეულ წილად მომგებიანი ბიზნესიც გახდა. მსოფლიოს უმსხვილესი კიბერუსაფრთხოების სერვისის კომპანიების უმეტესობა დაფუძნებულია ამერიკის შეერთებულ შტატებში, თუმცა მათი მომსახურება მსოფლიოს ყველა

[33] Cyber / ICT Security. OSCE, What we do - https://www.osce.org/cyber-ict-security

წერტილზე ვრცელდება. მაგალითად, კომპანია Symantec-ი, რომლის წლიური ბრუნვა 6 მილიარდ აშშ დოლარს შეადგენს. კომპანიის მიერ შემუშავებული პროგრამული იზრუნველყოფა და ე.წ. ანტი-ვირუსული პროტოკოლები საკმაოდ ცნობილია მთელს მსოფლიოში: ანტი-ვირუსული პროგრამები - Norton 360, Ghost, Norton Internet Security Protocol, Think C და მრავალი სხვა.[34]

[34] Топ-25 Компаний по кибербезопасности 2018-ого года, Рейтинг BlackBerry, 2019 - https://blackberryrussia.ru/top-25-kompaniy-po-kiberbezopasnosti-2018-goda/

2.3 კიბერუსაფრთხოება და მისი როლი საერთაშორისო უსაფრთხოებაში

ნებისმიერი სისტემის ნორმალური ფუნქციონირებისათვის საჭიროა მისი სამუშაო პროცესის კონტროლი და სათანადო ზედამხედველობა. კიბერუსაფრთხოების პრობლემა შედარებით ახალია მსოფლიოს უსაფრთხოების პარამეტრებში. იგი წარმოიშვა პირველი გამომთვლელი ტექნიკის, კომპიუტერული და საკომუნიკაციო ქსელების ექსპლუატაციაში შესვლის დროიდან. მაშინ, ბოროტმოქმედების მოტივი იყო მარტივი ადამიანური ფაქტორი, საკუთარი ცოდნის და შესაძლებლობების განმტკიცების მიზნით. ტექნოლოგიური განვითარების და ინტენსიური ინტეგრაციის შედეგად საფრთხეებმა ბევრად მასშტაბური სახე მიიღეს და ტექნოლოგიების გამოყენება შესაძლებელი გახდა როგორც ფინანსური მაქინაციების, ასევე ტერორისტული აქტების დაგეგმვისა და სახელმწიფო ინფრასტრუქტურის საწინააღმდეგო შეტევების განხორციელების დროს.

საერთაშორისო უსაფრთხოების ერთ-ერთი უმთავრესი გამოწვევა არის საერთაშორისო ტერორიზმი. აგრესიის გამოხატვის ყველაზე მწვავე ფორმა, მიმართული როგორც ადამიანის, ასევე საზოგადოებისა და სახელმწიფოების წინააღმდეგ. გლობალიზაციის პროცესებიდან გამომდინარე, ტერორიზმი წარმოადგენს წერტილოვანი ლოკალური ძალის ტრანსფორმირებულ საერთაშორისო ქსელს, რომელსაც გააჩნია ნებისმიერი საერთაშორისო ორგანიზაციის მსგავსი დამახინჯებული ფორმა. XXI საუკუნეში, საერთაშორისო ექსტრიმისტული დაჯგუფებების საბრძოლო მექანიზმებს დაემატა კიბერსაშიშროების ელემენტიც. ტერმინი „კიბერ-ტერორიზმი“ საერთაშორისო უსაფრთხოებაში 1980-იან წლებში ამერიკის შეერთებულ შტაბებში გაუღერდა. მაშინ, ისევე როგორც დღეს, ტერმინის გამოყენებით აღიწერებოდა ტერორისტული ქმედებები ვირტუალურ განზომილებაში. მთავარი პრობლემა მდგომარეობს იმაში, რომ კომპიუტერული ტერორიზმის ზუსტი ცნების ახსნა საკმაოდ რთულია, გამომდინარე იქიდან, რომ მსოფლიოში არ არსებობს კიბერ-დანაშაულის ზუსტი დეფინიცია და დახასიათება. ამის მიუხედავად, არსებობს რამდენიმე ინდიკატორი, რომელიც ქმედებას ვირტუალურ განზომილებაში ახასიათებს როგორც ექსტიმისტულ-ტერორისტული მიზნებით ჩადენილ აგრესიულ აქტს. მსგავსი

ქმედება მოიაზრებს ინფორმაციულ შეტევას პოლიტიკური დისტრუქციის მოტივით და მოიცავს ფსიქოლოგიურ ზეგავლენას, დაშინებას, ძალადობრივ მუქარას შიშსა და პანიკის გამოსაწვევად სოციალურ ქსელებში. გარდა ამისა, ცნობილია ვირტულური რეკრუტინგის ხერხი, რომელსაც განსაკუთრებულად ხშირად მიმართავდა ტერორისტული ორგანიზაცია „ისლამური სახელმწიფო“. ახალი რეკრუტების ასაყვანად ტერორისტულ ორგანიზაციებში ცალკე სპეციალისტები არსებობენ, რომლის მთავარი მოვალეობა არის ექსტიმისტული იდეოლოგიის გავრცელება და ფსიქოლოგიური ზეწოლა სოციალური ქსელებისა და სოციალური მედიის მეშვეობით. ტერორისტული პროპაგანდას მაგალითად შეიძლება ჩაითვალოს 2014 წლის სექტემბრის დასაწყისში ბრიტანული მედიის ვებ-გვერდზე გამოქვეყნებული მასალის შინაარსიც. სტატიაში საუბარი იყო იმაზე, რომ „ისლამური სახელმწიფოს“-ა და „ალ-ქაიდას“ წარმოამდგენლები ღიად აცხადებენ ჰაკერებისა და კომპიუტერული სპეციალისტების შეკრების ინიციატივებს. ჰაკერები დაიწყებდნენ „კიბერ-ხალიფატის“ მშენებლობას საკუთარი კრიფტოგრაფიული კოდებით და პროგრამული უზრუნველყოფით და ისინი მონაწილეობას დასავლეთის წინააღმდეგ წარმოებულ კიბერშეტევებში მიიღებდნენ[35]. ვირტუალური ტერორიზმის კიდევ ერთი ცნობილი შემთხვევა მოხდა 2008 წელს ინდოეთის ქალაქ მუმბაიში. მაშინ, ტერორისტული აქტის განხორციელების დაგეგმვის ეტაპზე ესტრიმისტულმა დაჯგუფებამ გამოიყენა ყველასთვის ხელმისაწვდომი კარტოგრაფიული ვებ-საშუალება „Google Maps”. Google რუკების სიზუსტემ მისცა მათ აფეთქების დიაპაზონის, ეპიცენტრისა და სავარაუდო ზარალის არეალის ზუსტი გამოთვლის საშუალება, რის შედეგად აფეთქებამ 164-კაციანი მსხვერპლი გამოიწვია.[36]

კიბერგანზომილების გამოყენების ეფექტიანობა ტერორისტული ორგანიზაციებისათვის გამომდინარეობს რამდენიმე ფაქტორისგან. პირველ რიგში, ეს რესურსი არ

---

[35] Corey Charlton for Mail Online UK. 11 September 2014 http://www.dailymail.co.uk/news/article-2751896/Islamic-State-jihadists-planning-encryption-protected-cyber-caliphate-carry-hacking-attacks-West.html

[36] Серия экспертных онлайн-форумов ОБСЕ по использованию Интернета террористами; угрозы, ответы и возможные будущие шаги. Отчёт. Action against terrorist unit, Transnational Threats Department. OSCE, Vienna, 2013

ისაჭიროებს მსხვილ ფინანსურ ინვესტიციას. ნებისმიერი ქმედების განსახორციელებლად საკმარისია ერთი პერსონალური ან პორტატული კომპიუტერი, წვდომა ინტერნეტზე და ერთი პროგრამისტი, რომელსაც შეეძლება მულტი-ფუნქციური ვირუსული პროგრამის დაწერა, ექნება ანონიმური გვერდები სოციალურ ქსელებში და ელექტრონული ფოსტის მისამართი. მეორეს მხრივ, თვით ინტერნეტი აძლევს გლობალური წვდომის საშუალებას, რომლის გამოყენებით მარტივია პროპაგანდისტული ბერკეტების ამოქმედება მსოფლიოს ნებისმიერ წერტილში და ინფორმაციის სწრაფი გავრცელება ე.წ. ტერორისტულ ფილიალებს შორის. კიბერტერორიზმით გამოწვეული საფრთხე ძალიან მასშტაბურია. ექსტრიმისტული მოტივით შესრულებული უკანონო ქმედებების კლასიფიკაციიდან გამომდინარე შესაძლებელია განსაზღვრა თუ რამდენად მნიშვნელოვან როლს ასრულებს ვირტუალური საშუალება ტერორისტული ორგანიზაციის საბრძოლო მეთოდებში.

- ფსიქოლოგიური ზეგავლენა და პროპაგანდა
- ახალი ბოევიკების რეკრუტიზაცია
- ეკონომიკური ზარალის მიყენება და კიბერ შეტევები კრიტიკულად მნიშვნელოვან ინფრასტრუქტურაზე
- დეზინფორმირების, პანიკასა და შიშის ჩანერგვა საზოგადოებაში
- ექსტიმისტული იდეოლოგიის აგიტაცია
- ზეწოლა სახელმწიფოს სამართალდამცავ ორგანოებზე და მმართველობაზე ტერორისტული აქტის ჩადენის მუქარით
- უკანონოდ მიღებული ინფორმაციის გავრცელების მუქარა და შანტაჟი

ჩამონათვალიდან ყველა პუნქტის შესრულება მარტივია ვირტუალური სივრცის გამოყენებით.

საერთაშორისო ურთიერთობების არასახელმწიფოებრივ აქტორებთან ერთად, ყურადღება ენიჭება სახელმწიფო სუბიექტებს და მათ როლს კიბერუსაფრთხოების გლობალურ პოლიტიკაში. კიდევ ერთი ტერმინი, რომელიც გულისხმობს კიბერსივრცის გამოყენების აგრესიული ქმედებებისათვის არის „კიბერომი“. ამერიკის

შეერთებული შტატების ეროვნული უსაფრთხოების ექსპერტი, რიჩარდ კლარკი თავის წიგნში წერს:

„კიბერომი - ერთი სახელმწიფოს მიერ დესტრუქციული ხასიათის ქმედება მეორე სახელმწიფოს ვირტუალურ ინფრასტრუქტურასა და ქსელურ სისტემაზე საკუთარი პოლიტიკური და სტრატეგიული ინტერესების მისაღწევად“ [R. Clark, 2010: 6]

კიბერომი არის ინფორმაციული ომის ერთ-ერთი კომპონენტი და წარმოადგენს კომპლექსურ დაპირისპირებას ვირტუალურ სივრცეში რამდენიმე აქტორს შორის. ინფორმაციული ომის უმთავრეს პრიორიტეტს წარმოადგენს არამხოლოდ თავდასხმა, არამედ საკუთარი კრიტიკული ინფრასტრუქტურისა და ინფორმაციის ხელშეუხებლობის უზრუნველყოფა და სწორედ ამიტომ კიბერუსაფრთხოების საკითხი დომინანტურია კიბერომის სუბიექტი სახელმწიფოს სტრატეგიისათვის. ისევე როგორც ნებისმიერი სხვა კიბერშეტევის მიზანი, კიბერომის ობიექტი არის სახელმწიფოს საკვანძო სამმართველო სტრუქტურები და სისტემები, რომლის ფუნქციონირებაზე აგებულია ქვეყნის ფინანსური, ენერგეტიკული და სატრანსპორტო ინფრასტრუქტურა. დღევანდელ დღეს, მსოფლიოში არსებობს რამდენიმე დე-ფაქტო კიბერ-მოთამაშე სახელმწიფო, რომელიც ამავე დროს ვირტუალური საბრძოლო პროცესების პოლუსებს წარმოადგენს. ესენია: აშშ, რუსეთი, ირანი, ჩინეთი, ისრაელი და ჩრდილოეთ კორეა. ყოველი ჩამოთვლილი ქვეყნის პოლიტიკურ-ისტორიული სპეციფიკიდან გამომდინარე მთავარი მეტოქის დადგენა მარტივია, თუმცა განსაკუთრებულ ყურადღებას ამ სახელმწიფოებს შორის ბოლო პერიოდში ჩრდილოეთ კორეის ფაქტორი იმსახურებს.

მიუხედავად იმისა, რომ ამ სახელმწიფოს პირდაპირი კავშირი რაიმე კიბერშეტევასთან დამტკიცებული არ არის, მისი როლი კიბერუსაფრთხოების საკითხებში ფართოდ განიხილება ინტერნეტ საზოგადოებასა და მას მედიაში. 2017 წელს ამერიკულმა გამომცემლობამ The New York Times გამოაყვეყნა სტატია, სადაც აღწერილი იყო ამერიკული და ბრიტანული სადაზვერვო მონაცემები ჩრდილოეთ კორეის ჰაკერული პოტენციალის შესახებ. ამ მონაცემებით, ჩრდილოეთ კორეის სახელმწიფოს

დაფინანსებით ქვეყნის ტერიტორიაზე ოპერირებს 6000-ზე მეტი გამოცდილი ჰაკერი, რომლებიც მუშაობენ ფულის არალეგალურ მისაკუთრებასა და ქაოსის ჩანერგვაზე გლობალური მასშტაბით. 2017 წლისთვის, სხვადასხვა ანალიტიკოსის ყურადღებას იპყრობდა ჩრდილოეთ კორეის ბირთვული პროგრამა, რის შესახებ ძალიან მცირე იყო ცნობილი საერთაშორისო დონეზე. მათი აზრით, ბირთვული ინფრასტრუქტურის საკონტროლო სისტემები ჩრდილოეთ კორეაში უნდა იყოს ციფრული, რაც ნიშნავს იმას, რომ კიბერსაფრთხის ქვეშ თავად ჩრდილოეთ კორეაც არის. თუმცა ამ სახელმწიფო კიბერუსაფრთხოების სტრატეგია ეროვნული უსაფრთხოების ელემენტებს შორის ერთ-ერთ უმნიშვნელოვანეს პოზიციას იკავებს.[37]

მეორეს მხრივ, ჩრდილოეთ კორეას კიბერთავდასხმების მოტივაცია მდგომარეობს ფინანსური მოგების გაზრდაში. ბირთვულ-სარაკეტო პროგრამის არსებობის გამო, ჩრდილოეთ კორეის წინააღმდეგ ამოქმედებულია მთელი რიგი საერთაშორისო სანქციების, დაწესებული გაეროს უსაფრთხოების საბჭოს, ევროკავშირის, ამერიკის შეერთებული შტატების, იაპონიის, სამხრეთ კორეის და მრავალი სხვა სახელმწიფოს მიერ. საერთაშორისო სანქციებმა და ქვეყნის ჩაკეტილობის პოლიტიკამ ჩრდილოეთ კორეის ეკონომიკურ მდგომარეობაზე იმოქმედა და სწორედ ამიტომ, სახელმწიფო დონეზე გადაწყვეტილი იყო სხვა გზის მონახვა სახსრების მოსაპოვებლად. ვირტუალური სივცე კი ამისთვის იდეალური მოედანია, რადგან ის არ ისაჭიროებს მაღალ ფინანსურ ინვესტიციებს. არაოფიციალური მონაცემების თანახმად, ჩრდილოეთ კორეაში შექმნილია სპეციალიზებული დანაყოფი გენერალური შტაბის სადაზვერვო სამმართველოს განკარგულების ქვეშ, ცნობილი როგორც „ბიურო 121“. დანაყოფის ფუნქცია მდგომარეობს სამხედრო-კიბერნეტიკული ოპერაციების ჩატარებაში და მისი შტატი მოიცავს დაახლოვებით 2000 ადამიანს. საინტერესო ფაქტია, რომ ბიუროს თანამშრომელების უმრავლესობა არ იმყოფება ჩრდილოეთ კორეის ტერიტორიაზე და საკუთარ საქმიანოს მსოფლიოს სხვადასხვა წერტილიდან ეწევა.[38]

---

[37] The World Once Laughed at North Korean Cyberpower. No More. The New York Times, 2017 - https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

[38] Wikipedia, The Free Encyclopedia - https://en.wikipedia.org/wiki/Bureau_121

ბიუროს არსებობის შესახებ მსოფლიო საზოგადოება ყოფილმა თანამშრომელმა ჩან ჰეკმა გააცნო, ჯერ კიდევ 2007 წელს (სახელი შეცვლილია). ჩანი და სხვა ჰაკერები მუშაობდნენ ჩინეთის ქალაქ პეკინში და იყვნენ „ბიურო 121“-ის ჩინური ფილიალის თანამშრომლები. სამხრეთ კორეაში გაქცევის შემდეგ, ჩან ჰეკმა გაასაჯაროვა ბიუროს სამუშაო სპეციფიკა, სტრუქტურა და მოტივი. სწორედ მისი განცხადების შემდგომ მსოფლიოს სხვადასხვა ანალიტიკოსმა გამოთქვა ვარაუდი, რომ დაწესებულმა სანქციებმა „ფუთკრის სკა“ გააღიზიანა და გამოიწვია უკურეაქცია, რომელსაც ვერც ერთი სანქცია ვერ შეაჩერებს.

2017 წელს, დონალდ ტრამპის ადმინისტრაციამ ჩრდილოეთ კორეა ვირუსული პროგრამის “Wanna Cry”-ს გავცელებაში დაადანაშაულა. „Wanna Cry”-ს ვირუსი მსოფლიოში იმავე წელს გავრცელდა და 500 000-ზე მეტი კომპიუტერი დააავადა. ვირუსის მსხვერპლი გახდა როგორც კერძო პირები, ასევე კორპორაციული და სახელმწიფო უწყებების კომპიუტერები და სხვადასხვა მონაცემებით, უმსხვილესი დარტყმა მიიღო რუსეთმა, უკრაინამ და ინდოეთმა. პროგრამა შიფრავდა წვდომას Windows-ის ოპერაციულ სისტემაზე მომუშავე კომპიუტერში არსებულ მონაცემებზე და ამ მონაცემების წაშლის ან გასაჯაროვების შანტაჟით ითხოვდა კომპენსაციას ბიტკოინების სახით. შეტევის ყველაზე მნიშვნელოვანი ობიექტი გახდა სამედიცინო დაწესებულებების კომპიუტერული ტექნიკა, რის შედეგადაც ჩაიშალა მრავალი გადაუდებელი ოპერაცია და სამედიცინო პროცედურა. აშშ-ს პრეზიდენტის შინაგანი უშიშროების მრჩეველებმა განაცხადეს, რომ ჰაკერულ თავდასხმაზე პასუხისმგებელია ჩრდილოეთ კორეის განკარგულების ქვეყ მყოფი ჰაკერული დაჯგუფება „ლაზარუს“-ის (Lazarus Group).[39] ეს ბრალდება სრულიად უარყოფილი იყო ჩრდილოეთ კორეას საგარეო საქმეთა სამინისტროს მიერ. მათი თქმით, ამერიკის შეერთებულ შტატებს

[39] U.S. blames North Korea for 'WannaCry' cyber attack, D. Voltz, The Reuters, 2017 - https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q

აწყობთ ხელოვნურად შექმნილი კონფრონტაცია ჩრდილოეთ კორეას საწინააღდეგო სანქციების გამკაცრებისა და უფრო მეტი სახელმწიფოს ჩართულობისათვის.[40]

“Wanna Cry”-ს ვირუსი და მრავალი სხვა შემთხვევა საერთაშორისო საზოგადოება ჩრდილოეთ კორეის მიერ კიბერომის წარმოების ფაქტში დაარწმუნა. მიუხედავად იმისა, რომ არც ერთი პრეცედენტი ბოლომდე არ არის გამოვკლეული და ყოველი ბრალდება ან ეჭვი დაფუძნებულია რამდენიმე სახელმწიფოს სადაზვერვო მონაცემებზე. საერთაშორისო საზოგადოებაში ჯერ-ჯერობის არ არსებობს ბერკეტი, რომელიც ამ საფრთხეს შეაჩერებდა, ხოლო ჩრდილოეთ კორეასთვის ეს არის ძვირადღირებული დროის მოგება საკუთარი მიზნების მისაღწევად.

ჩრდილოეთ კორეის კიბერომი და კიბერ-ტერორიზმი წარმოადგენს გამოწვევას როგორც გლობალური, ასევე რეგიონული და ეროვნული უსაფრთხოებისათვის. უკანონო ქმედებაში ჩარეული ადამიანებისათვის ვირტუალური სამყარო აძლევს თავისუფალი, ანონიმური და სწრაფი ქმედების მოედანს.

[40] КНДР отвергла обвинения США в распространении вируса WannaCry, 2017 - https://www.rbc.ru/politics/21/12/2017/5a3b60fa9a79474f03c542ca

თავი III

კიბერუსაფრთხოება კავკასიის რეგიონული უსაფრთხოების სტრატეგიის ფარგლებში, საქართველოს, სომხეთისა და აზერბაიჯანის მაგალითზე

მიუხედავად მრავალი რეგიონული კონფლიქტებისა, სამხრეთ კავკასიის რეგიონი იმყოფება ტრადიციულად მნიშვნელოვან პოზიციაზე გლობალურ ეკონომიკასა და პოლიტიკაში. კავკასიის სატრანზიტო ფუნქციიდან და საკვანძო სასაზღვრო ტერიტორიებიდან გამომდინარე, რეგიონი წარმოადგენს ჩრდილოეთ-სამხრეთისა და დასავლეთ-აღმოსავლეთის სატრანსპორტო დერეფანს და აერთიანებს კასპიასა და შავ ზღვას. უნდა აღინიშნოს, რომ კავკასიის გეოპოლიტიკური რეგიონი მოიცავს ასევე რუსეთის ფედერაციის ჩდრილოეთ კავკასიის ტერიტორიას და ნაწილობრივ თურქეთსაც, ხოლო საქართველო, სომხეთი და აზერბაიჯანი რეგიონის ცენტრალურ ნაწილს წარმოადგენენ. რეგიონული უსაფრთხოების თვალსაზრისით და გეოგრაფიული მნიშვნელობიდან გამომდინარე, კავკასია აღმოჩნდა ერთ-ერთი მნიშვნელოვანი კომპონენტი რუსეთსა და დასავლური ქვეყნების შორის არსებულ დაძაბულ საერთაშორისო პოლიტიკაში. უნდა აღინიშნოს ისიც, რომ ისტოირულად, რუსეთი ახდენდა საკმაოდ მაღალ გავლენას კავკასიის რეგიონში არსებულ ქვეყნებზე. ხოლო დღევანდელი ვითარებით, ამერიკა - ირანის ბირთვული პროგრამით

გამოწვეულ პრობლემებსა და ვაშინგტონი - მოსკოვის ურთიერთობებმა საკუთარი კვალი კავკასიის რეგიონზეც დატოვა. კავკასიის რეგიონული უსაფრთხოება 1990-ანი წლების შემდგომ მოიცავს რამდენიმე მნიშვნელოვან კომპონენტს, რამდენიმე მათგანი:

- შიდაპოლიტიკური დაძაბულობა
- ტერიტორიული კონფლიქტები
- პოსტ-საბჭოური ტრანზიციის ეტაპები
- ეკონომიკური და საზოგადოებრივი ტრანსოფორმაცია

სსრკ-ს სისტემის დაშლამ სხვა ყოფილ წევრ ქვეყნებთან პარალელურად გამოიწვია სამხრეთ კავკასიის ქვეყნების დემოკრატიზაცია, რასაც ხელი შეუწყო გლობალიზაციის პროცესების ექსპანსიამაც. მიუხედავად იმისა, რომ კავკასიას მსოფლიო ტერიტორიების საკმაოდ მცირე ნაწილი უკავია, რეგიონის მნიშვნელობა სწორედ რუსეთ-დასავლეთის ურთიერთობებში ვლინდება. ეს განსაკუთრებით თვალსაჩინოა რეგიონის პრო-დასავლური ხასიათის პოლიტიკაში და რუსეთის ფედერაციის სამხედრო ჩართულობაში რეგიონული დონის კონფლიქტებში.

კავკასიის რეგიონის სამი ცენტრალური ქვეყნის კიბერუსაფრთხოების სტრატეგიის გასარკვევად საჭიროა ყოველივე მათგანის ეროვნული უსაფრთხოების კონცეფციის მიმოხილვა. გარდა ამისა, რეგიონული კოლექტიური თანამშრომლობის პერსპექტივების დადგენა კიბერუსაფრთხოების საკითხებში. ისევე როგორც მრავალმა სახელმწიფომ, საქართველომ, სომხეთსა და აზერბაიჯანმა მოახდინა ბუდაპეშტის 2001 წლის კიბერუსაფრთხოების კონვენციის რატიფიცირება, 2012, 2007 და 2010 წლებში შესაბამისად. მიუხედავად იმისა, რომ კავკასიის რეგიონის ცენტრალური ქვეყნების სპეციფიკა და სახელმწიფო სტრატეგია განსხვავდება, სამივე ქვეყანაში ვირტუალურ-ტექნოლოგიური ინტეგრაცია სხვადასხვა სისტემის მუშაობაში საკმაოდ მაღალია. სახელმწიფოს ვირტუალური უსაფრთხოების პარამეტრების დასადგენად, საჭიროა იმის გარკვევა, თუ რამდენად მნიშვნელოვან როლს ასრულებს ტექნოლოგიური ელემენტი ამა თუ იმ სახელწმიფოს კრიტიკულად მნიშვნელოვან ინფრასტრუქტურაში.

3.1 - კიბერუსაფრთხოების სამართლებრივი რეგულირება სამი ქვეყნის ეროვნული უსაფრთხოების კონცეფციის მიხედვით

სომხეთი

დრევანდელ დღეს, სომხეთის რესპუბლიკის ეროვნულ სტრატეგიაში არსებობს მხოლოდ ორი დოკუმენტი, რომელშიც ირიბად არის აღწერილი კიბერუსაფრთხოების საკითხი. ორივე მათგანი კიბერუსაფრთხოების საკითხებს გლობალური გადმოსახედიდან განიხილავს და არ ეხება ეროვნული კიბერუსაფრთხოების უზრუნველყოფის მექანიზმის ან სამართლებრივი დარეგულირების მნიშვნელობას რესპუბლიკურ დონეზე. ერთის მხრივ, ეს გამოწვეულია იმით, რომ სომხეთის ტერიტორიაზე კიბერდანაშაულის ფაქტები არ ატარებდა სისტემატიურ ხასიათს და კიბერ-შეტევებს არ მიუყენებია ზარალი, რომელიც შექმნიდა საფრთხეს ეროვნული უშიშროებისათვის. როგორც კოლექტიური უსაფრთხოების ორგანიზაციის მუდმივი წევრი, სომხეთის რესპუბლიკის კიბერუსაფრთხოების პოლიტიკაზე ბოლო წლებში რუსეთის ფედერაციის გამოცდილებამ იმოქმედა. 2011 წელს სომხეთმა მიიღო ორგანიზებული დანაშაულის პრევენციის ეფექტიანობის გაზრდის ეროვნული პროგრამა, სადაც კიბერუსაფრთხოების საკითხი განიხილება თანამშრომლობითი უსაფრთხოების პერსპექტივიდან, კოლექტიური უსაფრთხოების ორგანიზაციის ფარგლებში. კიბერუსაფრთხოების ინსტიტუციონალური ხასიათი სომხეთში ჯერ კიდევ შემუშავების პროცესში იმყოფება, იმის მერე რაც სომხეთის თავდაცვის სამინისტრომ გამოთქვა კიბერ-დანაყოფის შექმნის ინიციატივა 2017 წელს. როგორც აცხადებენ

სომხური ექსპერტები, ეროვნული დამოკიდებულება კიბერუსაფრთხოების საკითხების მიმართ ფორმირებული არ არის, თუმცა სომხური ინფრასტრუქტურა უკვე ნაწილობრივ ტრანსფორმირებულია სატელეკომუნიკაციო ტექნოლოგიაზე. სახელმწიფოს ასეთი პოლიტიკის საწინააღმდეგო არგუმენტი სტატისტიკურ მონაცემებში მდგომარეობს. კომპიუტერული ტექნოლოგიების ინტეგრირება სომხეთის ტერიტორიაზე თანაბრად მაღალი ტემპით მიმდინარეობს, როგორც სომხეთის დედაქალაქში, ასევე რეგიონებშიც. მსოფლიო ბანკის მონაცემების მიხედვით, 2015 წლისთვის ინტერნეტ-მომხმარებლების რაოდენობა სომხეთის მოსახლეობის 58%-ს შეადგენდა, ხოლო 2016 წელს, ციფრი 70%-მდე გაიზარდა.[41] ისევე როგორც საქართველოში და აზერბაიჯანში, სამომხმარებლო პერსონალური კომპიუტერების უმეტესობა სომხეთის ტერიტორიაზე მუშაობს არალიცენზირებულ პროგრამულ უზრუნველყოფაზე, ძირითად შემთხვევაში ეს არის „გატეხილი“ ოპერაციული სისტემა - Microsoft Windows. ასეთი ოპერაციული სისტემის უსაფრთხოების პროტოკოლები ხშირ შემთხვევაში სათანადო რეჟიმში არ მუშაობს ან სრულად წაშლილია, ზუსტად იმისთვის, რომ Windows-ის ოპერაციული სისტემის გამოყენება და გავრცელება შესაძლებელი გახდეს უფასოდ. მომხმარებლების რიცხვის გაზრდასთან პარალელურად იზრდება კიბერდანაშაულის პროცენტიც. კასპერსკის ლაბორატორიის 2016 წლის მონაცემებით, ინტერნეტის ყოველი მესამე მომხმარებელი გახდა სხვადასხვა სიმძიმის ჰაკერული თავდასხმის მსხვერპლი.[42] CyberGates-ის მონაცემების თანახმად, 2017 წლისთვის დომენი .am-ის ზონაში მყოფი 100-ზე მეტი ვერ-საიტი კიბერშეტევის ქვეშ იმყოფებოდა.

აღსანიშნავი ფაქტია, რომ ფიზიკური საკაბელო უზრუნველყოფა, რომლის მეშვეობით გლობალური ქსელი სომხეთის ტერიტორიაზე მიეწოდება გადის აზერბაიჯანის და თურქეთის ტერიტორიაზე. ხაზი უნდა გაისვას იმასაც, რომ სომხეთის რესპუბლიკას

---

41 Armenian Internet: Social Networks & Users, B4B, 2016 - http://b4b.am/archives/our_authors/%D5%B0%D5%A1%D5%B5%D5%A1%D5%BD%D5%BF%D5%A1%D5%B6%D5%B5%D5%A1%D5%B6-%D5%AB%D5%B6%D5%BF%D5%A5%D6%80%D5%B6%D5%A5%D5%BF%D5%A8%E2%80%A4-%D5%BD%D5%B8%D6%81%D6%81%D5%A1%D5%B6%D6%81%D5%A5%D6%80%D5%B6-%D5%B8

42 Armenian Cyber Threat, Kaspersky Lab, 2016 - https://ittrend.am/2017/03/03/kaspersky-lab-every-3-th-armenian-user-meets-cyber-dangers/

შეწყვეტილი აქვს დიპლომატიური ურთიერთობები ორივე სახელმწიფოსთან და გააჩნია მიმდინარე ტერიტორიული კონფლიქტი აზერბაიჯანთან. ბოლო პუნქტი უთითებს, რომ ინტერნეტის საკაბელო უზრუნველყოფის გასვლა აზერბაიჯანის ტერიტორიაზე სომხეთისთვის კიბერსაშიშროებას წარმოადგენს და განსაკუთრებულად რთულდება ეროვნული უზრუნველყოფის მექანიზმების არარსებობის დროს. გლობალური კიბერუსაფრთხოების 2017 წლის ინდექსის თანახმად, 193 ქვეყნის შორის სომხეთის რესპუბლიკა სხვადასხვა მაჩვენებლით მხოლოდ 111-ე ადგილი დაიკავა.[43] მედიაექსპერტის, სამველ მარტიროსიანის თქმით, სახელმწიფოს ასეთი დამოკიდებულების ფონზე უფრო მსხვილი კიბერშეტევების თავიდან აცილება ხერხდება მხოლოდ მოტივის ნაკლებობით, როდესაც ჰაკერული ინტერესი უფრო მსხვილ ქვეყნებზეა მიმართული.[44]

2017 წლის დაბალი რეიტინგული მაჩვენებლების შემდგომ, სომხეთის რესპუბლიკაში დაიწყო მუშაობა კიბერუსაფრთხოების სტრატეგიის გასაუმჯობესებლად. ტელეკონიკაციებისა და ტრანსპორტის მინისტრის 2018 წლის ანგარიშით სომხეთმა მიიღო 70 მილიონი დოლარის კერძო ინვესტიცია, რომელიც სრულიად იყო მიმართული ეროვნული ინფორმაციული ტექნოლოგიების უსაფრთხოების სისტემების შემუშავებისათვის. გარდა ამისა, 2019 წლისთვის სომხეთში ამოქმედდება სომხეთის უშიშროების საბჭოს მიერ შემუშავებული კიბერდანაშაულის აღკვეთის სამართლებრივი რეფორმა, რომელიც ასევე მოიცავს კიბერუსაფრთხოების სააგენტოს შექმნას თავდაცვის სამინისტროს განკარგულების ქვეშ.

აზერბაიჯანი

2007 წლის 23 მაისს დამტკიცდა აზერბაიჯანის რესპუბლიკის ეროვნული უსაფრთხოების კონცეფცია. დოკუმენტის ბოლო, 4.3.11 პუნქტი სრულიად არის მიძღვნილი ქვეყნის

---

[43] Глобальный индекс кибербезопасности ITU, 2017 - https://digital.report/globalnyiy-indeks-kiberbezopasnosti-ot-itu-gruziya-i-rossiya-voshli-v-top-10/

[44] Эксперт: к кибербезопасности в Армении серьезно относятся только банки, 2017 - https://ru.armeniasputnik.am/society/20170712/7921970/ehkspert-k-kiberbezopasnosti-v-armenii-serezno-otnosyatsya-tolko-banki.html

ინფორმაციული უსაფრთხოების უზრუნველყოფის მნიშვნელობას და სტრატეგიას. მოიაზრებს ისეთ მექანიზმებს და ქმედებებს, როგორც:

- ეროვნული უსაფრთხოების სისტემების შექმნა, კონტროლი და მუდმივი განახლება
- საექსპერტო თანამშრომლობა გადაწყვეტილების მიღების პროცესში
- დაზვერვისა და კონტრდაზვერვის ეფექტიანობის გაუმჯობესება აღნიშნული დარგის ფარგლებში
- სახელმწიფო საიდუმლო ინფორმაციის ხელშეუხებლობის უზრუნველყოფა
- სამართლებრივი დარეგულირების მექანიზმების შემუშავება და ინფორმაციული უსაფრთხოების უზრუნველყოფა დემოკრატიის პრინციპების გათვალისწინებით[45]

გარდა ამისა, აზერბაიჯანის ეროვნული უსაფრთხოების კონცეფციის დიდი ნაწილი ენერგო-უსაფრთხოების საკითხებსაც ეხება, რაც ბოლო წლებში გარკვეული დოზით კიბერუსაფრთხოებასთანაც ასოცირდება.

2018 წლის Day Roadshows ყოველწლიური ფორუმის დროს, აზერბაიჯანის რესპუბლიკის ტრანსპორტისა და მაღალი ტექნოლოგიების მინისტრის პირველმა მოადგილემ ელმირ ველიზადემ გააჟღერა რესპუბლიკის დამოკიდებულება კიბერუსაფრთხოების საკითხებთან დაკავშირებით. მისი თქმით, აზერბაიჯანის საზოგადოების უდიდესი ნაწილი დამოკიდებულია ინტერნეტ ტექნოლოგიებზე და ტექნოლოგიური განვითარების ელემენტები დიდ როლს ასრულებენ როგორც ბიზნეს სექტორში, ასევე სახელისუფლებო ინსტიტუტებშიც. ველიზადემ გამოთქვა აზერბაიჯანის მზადყოფნა „ციფრული საზოგადოების“ ფორმირებისათვის და პირველი ეტაპი სახელმწიფო ეკონომიკური, ფინანსური და საბანკო სისტემებისა და

[45] National Security Doctrine of Republic of Azerbaijan, 23 May 2007. 4.3.11. Information Security Policy, p. 601-602

ინფრასტრუქტურის კონტროლი და უსაფრთხოების უზრუნველყოფის გაუმჯობესება იქნება.[46]

ერთი წლით ადრე, აზერბაიჯანის მთავრობამ მიიღო კანონი, რომლის 10-ე პუნქტის თანახმად საინფორმაციო უსაფრთხოების უზრუნველყოფა სრულად გადავიდოდა ქვეყნის სამართალდამცავი და სამხედრო სტრუქტურების განკარგულების ქვეშ. ოფიციალური პირების თქმით, ეს გადაწყვეტილება მიღებული იყო ევროპული მაგალითის გათვალისწინებით, სადაც კერძო სექტორთან თანამშრომლობისა და სპეციალიზებული ორგანოების არსებობის გარდა, საინფორმაციო უსაფრთხოების საკითხი შეიარაღებულ ძალებსაც ეხება. ამით აზერბაიჯანელმა ექსპერტებმა კიდევ ერთხელ გაუსვეს ხაზი იმ მტკიცებულებას, რომ XXI საუკუნის ვირტუალური საფრთხეები ატარებენ შეიარაღებული კონფლიქტის ხასიათს.[47]

აზერბაიჯანის რესპუბლიკისთვის განსაკუთრებულად მნიშვნელოვანია ქვეყნის ტერიტორიასა და კასპიის ზღვის აკვატორიაში არსებული კრიტიკული სანავთობო ინფრასტრუქტურის დაცვა. სახელმწიფოს უსაფრთხოების კონცეფციაში ენერგოუსაფრთხოების საკითხი ეროვნული უსაფრთხოების სხვა კომპონენტების პერსპექტივიდან ბევრჯერ მოიხსენიება. გარდა ამისა, ისევე როგორც სომხეთის შემთხვევაში, არალიცენზირებული პროგრამული უზრუნველყოფის გავცელების საკითხი ამ ქვეყანაშიც არსებობს. ბოლო 3 წლის განმავლობაში, აზერბაიჯანის დედაქალაქში ჩატარდა 10-ზე მეტი საერთაშორისო კონფერენცია და სემინარი კიბერუსაფრთხოების დარგში. აზერბაიჯანული მხარე დიდ ყურადღებას ანიჭებს თანამშრომლობას ჩრდილო-ატლანტიკურ ალიანსთან და გაეროს უსაფრთხოების საბჭოსთან და აცხადებს სრულ მზადყოფნას გადმოიღოს ევროპულ ქვეყნებში არსებული სტარდარტების რიგი კიბერუსაფრთხოების უზრუნველსაყოფად საკუთარ ქვეყანაში.

---

[46] В Азербайджане разрабатывается национальная стратегия по кибербезопасности, 2018 - http://www.biznesinfo.az/news/technonews/params/ln/ru/article/114466

[47] Новый закон о ВС Азербайджана заставит всех быть более осторожными, 2017 - https://az.sputniknews.ru/azerbaijan/20171215/413217097/ministerstvo-oborony-zakon-vooruzhennye-sily.html

საქართველო

საქართველოს ეროვნული უსაფრთხოების კონცეფციაში კიბერუსაფრთხოების პუნქტი აღნიშნულია როგორც ეროვნული ინტერესების, ასევე საქართველოს სახელმწიფოს წინაშე არსებული საფრთხეებისა და საქართველოს ძირითადი პოლიტიკური მიმართულებების ჩამონათვალშიც. გარდა ამისა, 2017-2018 წლებში საქართველოს მთავრობის დადგენილებით გამოაქვეყნეს საქართველოს კიბერუსაფრთხოების სტრატეგია და სამოქმედო გეგმა. დოკუმენტის ორივე დანართში ვრცლად არის ჩაშლილი ქვეყნის კიბერუსაფრთხოების დღევანდელი ვითარება, მთავარი გამოწვევები და რისკები. ასევე, აღნიშნულია საქართველოს კიბერუსფართხოების სუსტი წერტილები, განვითარების პერსპექტივები და სამართლებრივი ბაზის შექმნის აუცილებლობა. აღსანიშნავია ფაქტი, რომ უკვე ხსენებული გლობალური კიბერუსაფრთხოების ინდექსის მიხედვით, საქართველომ აღნიშნულ რეიტინგში 8-ე ადგილი დაიკავა. ელექტროკავშირების საერთაშორისო ბიურომ (ITU) საქართველოს ასეთ წარმატებას კიბერუსაფრთხოების სფეროში 2008 წლის კიბერშეტევების შემდგომი პრევენციული მექანიზმების განვითარებას და ეროვნული კიბერუსაფრთხოების ბიუროს შექმნას უკავშირებს. გარდა ამისა, არასამთავრობო საკონსულტაციო ორგანიზაციამ, ელექტრონული მმართველობის აკადემიამ (e-GA) თავის ყოველწლიურ რეპორტში საქართველოს კიბერუსაფრთხოების პოტენციალს აფასებს როგორც საშუალოზე მაღალს. აღნიშნული ორგანიზაციის შეფასება საქართველოსთან ერთად შეეხო სხვა პოსტ-საბჭოთა ქვეყნებსაც, მათ შორის აზერბაიჯანს, სომხეთს, ბელორუსიასა და უკრაინას. ორგანიზაციის ექსპერტებმა 100%-ით შეაფასეს საქართველოში არსებული კიბერუსაფრთხოების კონცეფცია, კიბერსაშიშროების ანალიტიკა, ელექტრონული იდენტიფიკაციის უსაფრთხოება, კრიტიკული საინფორმაციო ინფრასტრუქტურის დაცულობასა და კიბერდანაშაულის საწინააღმდეგო სამართლებრივი ბაზა.[48]

2014 წელს, საქართველოს თავდაცვის მინისტრის დადგენილებით შეიქმნა საქართველოს თავდაცვის სამინისტროს განკარგულების ქვეშ მყოფი

[48] The e-Governance Academy, 2017 - https://ega.ee/wp-content/uploads/2017/10/ega_e-demcyber_policy-rec_205x275_bleed5mm_RUS.pdf

კიბერუსაფრთხოების ბიურო. ბიუროს ვებ-გვერდზე გამოყვეყნებულია მისი საქმიანობის ძირითადი პუნქტები, ესენია:

- კიბერუსაფრთხოების ერთიანი პოლიტიკის განხორციელება
- თავდაცვის სფეროში ინფორმაციული და კომუნიკაციების ტექნოლოგიების სისტემის უსაფრთხოების უზრუნველყოფა
- კომპიუტერულ ინციდენტებზე დახმარების ჯგუფების 24/7 (CSIRT, CSIRT/CC, Call Center 24/7) მექანიზმების დანერგვა, ამოქმედება და განვითარება;
- საქართველოს თავდაცვის სფეროში ინფორმაციული და კომუნიკაციების ტექნოლოგიების ინფრასტრუქტურის დაცვა კიბერსაფრთხეებისა და კიბერრისკებისგან
- თავდაცვის სფეროში არსებული ინფრასტრუქტურის შესწავლა, მისი უსაფრთხოების განვითარება და გაძლიერება
- კონცეპტუალური ბაზის შექმნა ("კიბერუსაფრთხოების პოლიტიკის დოკუმენტი", "კიბერუსაფრთხოების განვითარების სამოქმედო გეგმა" და ა.შ.)
- საქართველოს კანონმდებლობის საერთაშორისო სამართლებრივ ნორმებთან ჰარმონიზაცია
- ცნობიერების ამაღლება კიბერუსაფრთხოების სფეროში
- საგანმანათლებლო პროგრამებსა და ტრეინინგებში მონაწილეობა
- მჭიდრო ურთიერთობის დამყარება ეროვნულ და საერთაშორისო დონეზე
- სამხედრო პერსონალის გადამზადებაში ხელშეწყობა კიბერუსაფრთხოების თანამედროვე სტანდარტების შესაბამისად[49]

ინსტიტუციონალური ბაზის გარდა, საქართველოში არსებობს მთელი რიგი არასამთავრობო ორგანიზაციებისა და სტუდენტური ინიციატივების, რომლის მთავარი მიზანი არის საზოგადოებრივი ცნობიერების ამაღლება კიბერუსაფრთხოების მიმართ.

[49] სსიპ კიბერუსაფრთხოების ბიურო. ჩვენს შესახებ, კიბერუსაფრთხოების ბიუროს ძირითადი ამოცანები, 2017 - http://csbd.gov.ge/bureau.php?lang=ge

ასეთი ორგანიზაციის მაგალითი არის უსაფრთხოების ექსპერტთა კავკასიის აკადემია[50], რომელიც კიბერუსაფრთხოებისა და ინფორმაციული დაცულობის კუთხით თანამშრომლობს საქართველოში არსებულ მსხვილ ბიზნეს-სექტორთან და აქტიურად ატარებს სატრეინინგო კურსებს, როგორც ძალოვანი სტრუქტურების წარმომადგენლებისა, ასევე ნებისმიერი მსურველისათვის.

სტატისტიკურად, ფინანსური სექტორი კიბერშეტევების უპირველესი მიზანია მთელს მსოფლიოში. აქედან გამომდინარე, კიბერუსაფრთხოების მიმართ განსაკუთრებულ ყურადღებას გლობალურად და ლოკალურად ანიჭებს საბანკო სექტორი. საქართველოს ბანკის და სხვა მსხვილი ბანკების სტრუქტურაში, ბოლო წლებში შექმნილია სპეციალური ჯგუფები, რომლებიც სამომხმარებლო საბანკო მონაცემების დაცვაზე აქტიურად მუშაობენ. 2019 წელს გაცემულია საქართველოს ეროვნული ბანკის ბრძანება კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ.[51] ბრძანების თანახმად, ეროვნულმა ბანკმა გაწერა კონკრეტული დადგენისა და ანალიზის, პრევენციისა და აღკვეთის მექანიზმები, რომელიც უნდა შეასრულოს საქართველოს ტერიტორიაზე არსებულმა კომერციულმა ბანკებმა. სამართლებრივად, საბანკო მონაცემებისა და ინფორმაციული უსაფრთხოების უზრუნველყოფის კუთხით, იუსტიციის სამინისტროს 2010 წლის დადგენილებით შეიქმნა მონაცემთა გაცვლის სააგენტო, რომლის მთავარი მისია არის ელექტრონული მმართველობის, მონაცემთა გაცვლის ინფრასტურქტურისა და ინფორმაციული უსაფრთხოების მონიტორინგი საქართველოში.[52]

ამრიგად, კავკასიის ცენტრში მდებარე სამი ქვეყნის კიბერუსაფრთხოების სტრატეგია და გამოცდილება საფუძვლიანად განსხვავდება. იმის და მიუხედავად, რომ სამივე ქვეყანა ერთმანეთთან გეოგრაფიულ სიახლოვეში იმყოფება და ქმნის ერთიან

---

[50] უსაფრთხოების ექსპერტთა კავკასიის აკადემია - CASE. ჩვენს შესახებ, 2019 - https://globalcase.org/page/about-case/

[51] კომერციული ბანკების კიბერუსაფრთხოების მართვის ჩარჩოს დამტკიცების შესახებ, საქართველოს ეროვნული ბანკის ბრძანება #№56/04, 22.03.2019 - https://matsne.gov.ge/ka/document/view/4515476?publication=0

[52] იუსტიციის სამინისტრო, მონაცემთა გაცვლის სააგენტო. მთავარი ფუნქციები, 2012 - http://www.dea.gov.ge/?action=page&p_id=5&lang=geo

რეგიონს, ვირტუალური უსაფრთხოების პარამეტრები, ისევე როგორც გამოწვევები და რისკები გამომდინარეობს კონკრეტული ქვეყნის ვირტუალური ინტეგრაციის პროცენტულობისგან. როგორც უკვე აღინიშნა აზერბაიჯანის შემთხვევაში, ქვეყნის უმთავრესი გამოწვევა არის კრიტიკულად მნიშვნელოვანი სანავთობო ინფრასტრუქტურის დაცვა, რომელიც გეოპოლიტიკურად წარმოადგენს რუსეთის, ცენტრალური აზიისა და აზერბაიჯანის ინტერესთა კოლაბორაციას. სომხეთის ეროვნული უსაფრთხოების სტრატეგიაში კიბერუსაფრთხოების საკითხი ბუნდოვნად მოიხსენიება. ინფორმაციული უსაფრთხოების თვალსაზრისით სომხეთის რესპუბლიკის უსაფრთხოების სტრატეგია ითვალისწინებს მხოლოდ თავისი სახელმწიფოს კულტურული, რელიგიური და სოციოლოგიური ინფორმაციის სიზუსტეს ინტერნეტ სივრცეში და სარისკო გამოწვევაში მხოლოდ დეზინფორმაციის გავცელებას გულისხმობს. თვალსაჩინო რეგიონული უპირატესობა კიბერუსაფრთხოების თვალსაზრისით საქართველოს გააჩნია. მნიშვნელოვანი ასპექტი ამ დარგში არის საქართველოსა და ესტონეთის თანამშრომლობა, რომელიც გამომდინარეობს 2007-2008 წლის რუსეთის მიერ ჩატარებული კიბერშეტევების სერიიდან ამ ორ ქვეყანაში. ევროკავშირისა და ჩრდილოატლანტიკური ალიანსის კიბერუსაფრთხოების კუთხით მოწინავე ესტონეთი აქტიურად აზიარებს საკუთარ გამოცდილებას და აცხადებს მზადყოფნას დარგის განვითარების შემუშავებაში საქართველოს ტერიტორიაზე. რეგიონული კოლექტიური თანამშრომლობის საკითხი სამხრეთ კავკასიაში პრაქტიკულად გამორიცხულია. ეს გამომდინარეობს სომხეთისა და აზერბაიჯანის შორის დაძაბული ურთიერთობებიდან და რუსეთის აქტიური ჩართულობიდან როგორც სომხეთის, ასევე მთლიანი რეგიონის პოლიტიკაში.

3.2 განხორციელებული კიბერშეტევები. გამოცდილება და შედეგები

საქართველოს, სომხეთისა და აზერბაიჯანის კიბერუსაფრთხოების პარამეტრები პირდაპირ პროპორციულია ამ სამ ქვეყანაში განხორციელებული კიბერშეტევების გამოცდილებასთან. რეგიონული თვალსაზრისით, დარგის განვითარების მესამე ადგილს სომხეთის რესპუბლიკა იკავებს და ეს დიდ წილად გამომდინარეობს იქედან, რომ სომხეთში არ მომხდარა მსხვილი ინფორმაციული თავდასხმები. თუმცა, შესაძლო კიბერშეტევებზე სომხური მედია ჯერ კიდებ 2016 წელს ალაპარაკდა. მაშინ, სომხურმა მხარემ სამთავრობო ვებ-საიტებზე DDos შეტევის განხორციელებაში თურქეთი

დააღანაშაულა და ეს ქმედება მთიან ყარაბახში გამწვავებულ სიტუაციას დაუკავშირა. ამ კიბერშეტევაზე პასუხისმგებლობა დააკისრეს თურქულ ჰაკერულ დაჯგუფებას Aslan Neferler Tim-ს, რომელსაც უკვე გააჩნდა გარკვეული გამოცდილება სომხეთის ცენტრალური ბანკის კიბერთავდასხმის ჩატარებაში.[53] კოლექტიური კიბერუსაფრთხოების შელახვის სომხეთისა და რუსეთის მიერ აღიარებული მცდელობა 2017 წელს დაფიქსირდა. საინტერესოა, რომ უკვე ხსენებული ვირუსული პროგრამა "Wanna Cry" სომხური და რუსული ექსპერტების თქმით გავრცელებული იყო ამერიკული სპეცსამსახურების მიერ, იმ დროს როცა დანარჩენი მსოფლიო ამ კიბერშეტევას ჩრდილოეთ კორეას აწერდა. ვირუსულმა პროგრამამ მნიშვნელოვანი ზიანი რუსეთის საბანკო და კომერციულ სექტორს მიაყენა და შეტევის შედეგების ლიკვიდაცია რუსეთში სომხური სპეციალისტების დახმარებით მოხერხდა. უფრო გვიან, 2018 წელს სომხეთის ეროვნული უსაფრთხოების სააგენტოს განცხადებით, ბოლო 2 წლის განმავლობაში რესპუბლიკაში გახშირდა კიბერშეტევების მცდელობები აზერბაიჯანის მხრიდან.

სომხეთის საპირისპირო მტკიცებულებებს აზერბაიჯანული მხარე ავრცელებს. 2017 წელს განხორციელებული კიბერშეტევა აზერბაიჯანული საბანკო ონლაინ სისტემაზე, აზერბაიჯანულმა მხარემ ზუსტად სომხეთს მიაწერა. მიუხედავად იმისა, რომ არც ერთი მხარე ბრალდებას არ აღიარებს, აზერბაიჯანული სპეცსამსახურების და ექსპერტის თქმით, სომხური კიბერშეტევები არ ხორციელდება უშუალო სომხეთის ტერიტორიიდან და ერთ-ერთი დაფიქსირებული შეტევა ავსტრალიასა და არგენტინის IP მისამართებიდანაა განხორციელებული. აზერბაიჯანული მხარე ხაზს უსმავს მსხვილი სომხური დიასპორის ჩართულობას დეზინფორმაციის და აზერბაიჯანის ეროვნული კულტურისა და პოლიტიკის დისკრედიტაციის მცდელობაში გლობალური მასშტაბით. თუმცა კიდევ ერთი აღსანიშნავი შემთხვევა აზერბაიჯანის რესპუბლიკაში შიდა პოლიტიკური სიტუაციიდან გამომდინარეობდა. 2018 წლის საპრეზიდენტო არჩევნების დროს ჰაკერული თავდასხმები აზერბაიჯანულ ოპოზიციური ორგანიზაციის

[53] Турецкие хакеры атаковали сайты министерств Армении – СМИ, Эхо Кавказа, 2016 - https://www.ekhokavkaza.com/a/27658129.html

სოციალური ქსელის გვერდსა და ვერ-საიტზე განხორციელდა. Maydan.TV-სა და სხვა ალტერნატიული აზრის მქონე მედია-საშუალების მონაცემები და საჯარო ინფორმაცია სრულიად დაიბლოკა.[54] საინტერესოა, რომ ამგვარი ზომის მიღება აზერბაიჯანში არ არის უკანონო. 2017 წელს ეროვნული უსაფრთხოების სააგენტოს მიერ მიღებულ იქნა კანონის შესწორება, რომლის თანახმად ასეთი ტიპის ინტერნეტ-წყაროს დაბლოკვა ეროვნული უსაფრთხოების უზრუნველყოფის საკითხად გადაიქცა და აზერბაიჯანის მთავრობას ვებ-კონტენტისა და ცენზურის კონტროლის ბერკეტი მისცა.

კავკასიის რეგიონის კიბერუსაფრთხოება მსოფლიო ექსპერტების დღის წესრიგში 2008 წელს რუსეთის მიერ განხორციელებული საქართველოს საწინააღმდეგო კიბერშეტევამ დააყენა. რუსეთ-საქართველოს 2008 წლის ომის დროს, რუსულმა მხარემ სამხედრო პოტენციალის ამოქმედებისა და სისხლიანი თავდასხმის გარდა ჰიბრიდული ომის ელემენტებიც გამოიყენა. ასიმეტრიული თავდასხმის მაგალითი იყო ფართომასშტაბიანი DDos შეტევა საქართველოს სამთავრობო, საბანკო და საინფორმაციო ვებ-გვერდებზე. საქართველოს კიბერუსაფრთხოების ექსპერტი ვლადიმერ სვანიძე თავის სტატიაში წერს:

„2008 წლის აგვისტოს ომის დროს რუსეთმა მასირებული შეტევა მიიტანა საქართველოს კიბერსივრცეზე, რის შედეგადაც დაზიანდა ქვეყნის კრიტიკული ინფრასტრუქტურის დიდი ნაწილი. რუსი ჰაკერების შეტევის მთავარ სამიზნეს სამთავრობო, საერთაშორისო ორგანიზაციების, კერძო და არასამთავრობო სექტორის დიდი ნაწილის ვებგვერდები წარმოადგენდა. შეიქმნა საფრთხე, რომ ქვეყანა აღმოჩნდებოდა ინფორმაციულ ვაკუუმში და საქართველოში რუსეთის მხრიდან განხორციელებული აგრესია და აქ მიმდინარე პროცესები არ გახდებოდა ცნობილი დანარჩენი მსოფლიოსთვის. ფაქტიურად, ქვეყნის ინფრასტრუქტურის დიდი ნაწილი პარალიზებული აღმოჩნდა.“[55][ვ. სვანიძე]

---

[54] В интернете за неделю: кибератаки на независимые СМИ в Азербайджане и Филиппинах, 2018 - https://globalvoices.org/2018/02/12/70072/

[55] ლადო სვანაძე: „საქართველოზე განხორციელებული კიბერშეტევები ჯაშუშურ ხასიათს ატარებდა“, 2016 - http://cyber.kvira.ge/9981/

კავკასიური ცენტრის ვერ-გვერდზე გამოქვეყნებული ინფორმაციის თანახმად, ჰაკერული თავდასხმები რუსეთის მხრიდან აგვისტოს ომამდე 1 თვით ადრე დაიწყო. ეს ინფორმაცია ცნობილი გახდა ამერიკელი ექსპერტების სამონიტორინგო ჯგუფის შეფასების შემდგომ, რომელიც ასევე გაზეთ The New York Times-ში იყო გამოქნეყნებული. The Arbor Network-ის თანამშრომელმა ხოსე ნაზარიომ შეამჩნია უცნაური პროტოკოლების მოქცევა ქართული IP მისამართების მიმართულების, რომელიც შეიცავდა საკვანძო სიტყვებს: *„победа+любовь+в+Россия“ (გამარჯვება+სიყვარული+ში+რუსეთი)*[56] [ხ. ნაზარიო]. აღსანიშნავია ისიც, რომ რუსული კიბერაგრესია 2008 წელს სამხედრო ქმედებასთან ერთად არ შეწყვეტილა. ამერიკული ორგანიზაცია FireEye-ის სტატისტიკური რეპორტის თანახმად, 2008-2014 წლებში კიბერშეტევები რუსეთის მხრიდან სისტემატიურ ხასიათს ატარებდა.[57] რეპორტის თანახმად, შეტევების 2 ძირითადი სამიზნე იყო საქართველოს თავდაცვისა და შინაგან საქმეთა სამინისტრო. თავდასხმა ასევე განხორციელდა ამერიკის შეერთებული შტატების დანაყოფზე, რომელიც ამ წლებში წვრთნებს ატარებდა საქართველოს სამხედრო კორპუსთან საქართველოს ტერიტორიაზე. გარდა ამისა, ჰაკერული შეტევების არეალი მოიცავდა კერძო ჟურნალისტების სოციალური ქსელებისა და ვებ-გვერდესაც, რომლის საჯაროდ ხელმისაწვდომი კონტენტი კავკასიის რეგიონის თემატიკას უკავშირდებოდა. 2008 წელს კი, საქართველოს ვირტულური სივრცე მოუმზადებელი აღმოჩნდა ასეთი მძიმე თავდასხმის განეიტრალებისათვის. სამთავრობო სისტემების უმეტესობა პროგრამულად გადამისამართებული იყო ევროპის სხვადასხვა ქვეყნების სასერვერო უზრუნველყოფაზე. ყოველი კიბერშეტევა საქართველოს წინააღმდეგ ატარებდა პროვოკაციულ ხასიათს. თავდასხმების მთავარი მოტივაცია იყო მოსახლეობაში პანიკის გამოწვევა, დეზინფორმაციის გავრცელება და სამხედრო-სტრატეგიული ჯაშუშობა.

---

[56] Кибератаки на Грузию из России начались задолго до начала военных действий, 2008 - https://www.kavkazcenter.com/russ/content/2008/08/13/60176/kiberataki-na-gruziyu-iz-rossii-nachalis-zadolgo-do-nachala-voennykh-dejstvij.shtml

[57] FireEye Special Report, APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? Interest in Caucasus, Particularly Georgia, p. 7-11

კიდევ ერთი გამოწვევა საქართველოს ინტერნეტ სივრცისთვის აღმოჩნდა ფრანგული გამომცემლობა Charlie Hebdo-ს სააგენტოში განხორციელებული 2015 წლის ტერაქტი. ეს შემთხვევა კიდევ ერთხელ უთითებს იმაზე, რომ ეროვნული უსაფრთხოების კიბერნეტიკული ელემენტები სცილდება კონკრეტული ქვეყნის საზღვრებს და გლობალური ხასიათის გამოწვევას წარმოადგენს. საქართველოსგან შორეულ საფრანგეთში მომხდარი ტერიტორისტული აქტის შედეგად კიბერშეტევის მსხვერპლი გახდა საქართველოში არსებული ფრანგული სასურსათო ქსელის - „კარფურის“ ვერ-პორტალი. 2 დღის განმავლობაში, გვერდზე არსებული პროდუქციის კატალოგის მაგივრად ჰაკერულმა ჯგუფმა განათავსა ისლამური ექსტრიმიზმის სააგიტაციო შინაარსის მქონე კონტენტი, სადაც არანორმატიული ლექსიკით აღწერილი იყო Charlie Hebdo-ს მიერ ჩადენილი „დანაშაული“ მუსლიმანური სამყაროს წინააღმდეგ. კავკასიის საკითხების ექსპერტის, ალეკო კვახაძის კომენტარში აღნიშნული იყო, რომ ქმედების განხორციელება საქართველოს .ge დომენზე გამოწვეული იყო „კარფურის“ ქსელის მთავარი ვებ-გვერდის გატეხვის წარუმატებელი მცდელობით, რამაც კიბერ-ტერორისტები საქართველოს ნაკლებად დაცულ კიბერსივრცეზე გადაამისამართა.[58]

ქართული სამხედრო პორტალის, მილიტარიუმის ვებ-გვერდზე გამოქვეყნებულია ექსპერტთა მოსაზრება შესაძლო კიბერსაფრთხესთან დაკავშირებით ტეროტისტული ორგანიზაციების მხრიდან. სტატიაში აღწერილია, რომ საქართველოს პრო-დასავლური პოლიტიკიდან გამომდინარე ქვეყანაში ხორციელდება მნიშვნელოვანი საერთაშორისო და ევროპული კომერციული და სამთავრობო ორგანიზაციების ფილიალების გახსნა. რაც თავის დროს გულისხმობს ევროპელი და ამერიკელი ექსპერტების ქვეყანაში ჩამოსვლას და მუშაობას საქართველოს ტერიტორიაზე. ყოველივე ეს გასათვალისწინებელია კიბერდაცულობის კუთხით, რადგან ეს

58 Кибер-армия добралась до Грузии. Эхо Кавказа, 2015 - https://www.ekhokavkaza.com/a/26790341.html

ადამიანები და ორგანიზაციები იმყოფებიან ტერორისტული თავდასხმის საფრთხის ქვეშ.[59]

ჩრდილო-ატლანტიკური ალიანსის კიბერუსაფრთხოების დე-ფაქტო სტრატეგიაში დიდ როლს ასრულებს ყოველი სახელმწიფოს თვით-დაცულობის უნარიანობა. კოლექტიური უსაფრთხოების კუთხით, მთავარი პრობლემა მდგომარეობს ზუსტი ხაზის არარსებობაში, თუ როდის შეიძლება კიბერშეტევის ჩათვლა კოლექტიური უსაფრთხოების შელახვის მცდელობად. საერთაშორისო სტანდარტებისა და ზუსტი ნორმების არარსებობა ქმნის ბუნდოვან ჩარჩოს, სადაც ყოველი შემთხვევა ცალკეულ პრეცედენტად განიხილება როგორც ეროვნულ, ასევე რეგიონულ და საერთაშორისო დონეზე. კავკასიის შემთხვევაში, კიბერუსაფრთხოების სტრატეგია ცალკეული სახელმწიფოს ეროვნული სტრატეგიის გადმოსახედიდან განიხილება. თუ განვიხილავთ რუსეთის სტრატეგიულ და გეოპოლიტიკურ ინტერესებს ამ რეგიონში, თვალსაჩინო ხდება, რომ სამივე ქვეყანა საფუძვლიანად სხვადასხვა ღირებულებისა და პოტენციალის მატარებელია რუსული მხარესათვის. ხოლო კიბერპოტენციალის კუთხით, რუსეთის ფედერაცია მსოფლიოს 5 უმსვილესი ქვეყნის შორის იმყოფება. ასეთი ძლიერი სასაზღვრო მეზობელი, რომელსაც ოკუპირებული აქვს საქართველოს ტერიტორიების 20% აუცილებლად გასათვალისწინებელია ეროვნულ და რეგიონულ კიბერუსაფრთხოების სტრატეგიის განვითარებაში.

[59] ახალი გამოწვევა საქართველოს ინტერნეტსივრცისათვის. პორტალი მილიტარიუმი, 2018 - https://militarium.org/kiberusafrtxoeba-da-saqartvelo/

დასკვნა

XXI საუკუნის საერთაშორისო უსაფრთხოებაში კიბერუსაფრთხოების კომპონენტი მნიშვნელოვან ადგილს იკავებს. თანამდროვე ვირტუალური ტექნოლოგიები ჩვენი ცხოვრების განუყოფელი ნაწილი გახდა და მასზე აგებულია კაცობრიობის საყოფაცხოვრებო სისტემების აბსოლიტური უმრავლესობა. კომუნიკაცია, ტრასნპორტირება, სამედიცინო ტექნოლოგიები, კოსმოსური მიღწევები და მრავალი სხვა დღესდღეობით წარმოუდგენელია ვირტუალური რეალობის გარეშე. ხოლო მთავარ გამოწვევას წარმოადგენს საერთაშორისო სამართლებრივი ნორმებისა და სტანდარტების სუსტი სისტემა, ვირტუალური სივრცის ანონიმურობის ხელშემყობი ფაქტორები და საზღვრების არარსებობა.

როგორ ხორციელდება კიბერუსაფრთხოების სტრატეგია რეგიონული უსაფრთხოების დონეზე - სამი ლოკალური აქტორის მაგალითზე?

კიბერუსაფრთხოების სტრატეგია საქართველოს, სომხეთისა და აზერბაიჯანის შემთხვევაში გამომდინარეობს თითოეული სახელმწიფოს ლოკალური პარამეტრებიდან. კოლექტიური უსაფრთხოების თვალსაზრისით აღსანიშნავია სომხეთის რესპუბლიკის აქტიური თანამშრომლობა რუსეთის ფედერაციასთან, კოლექტიური უსაფრთხოების ორგანიზაციის ფაგლებში, რაც წარმოადგენს ერთგვარ გარანტიას სომხეთის ვირტუალური უსაფრთხოებისათვისაც. კავკასიის რეგიონის არასტაბილურობა რუსეთის ფედერაციასა და სხვა აქტორების ინტერესების კვეთიდან გამომდინარეობს. პოსტ-საბჭოთა ტრანსფორმაციის ეტაპი სამივე ქვეყანაში ბოლომდე გასული ჯერ კიდევ არ არის და ეს ელემენტი იმყოფება გარკვეულ დისონანსში ტექნოლოგიურ წინსვლასთან. ვირტუალური სივრცე, როგორც გლობალიზაციის პროცესის მთავარი ელემენტი აერთიანებს მსოფლიოს შორეულ წერტილებს და კავკასიის ბუფერული რეგიონის ელემენტი აქაც იკვეთება. ცხადია, რომ კავკასიის

კიბერუსაფრთხოების პარამეტრების დადგენა სრული რეგიონის მასშტაბით, ისევე როგორც თანამშრომლობა ამ კუთხით რთულდება სომხეთსა და აზერბაიჯანის მუდმივი კონფლიქტის ფონზე. გლობალური სტატისტიკის თანახმად, რეგიონის უპირატესობა ინფორმაციული უსაფრთხოების თვალსაზრისით საქართველოს გააჩნია, რაც გამომდინარეობს ამ ქვეყნის გამოცდილებიდან. სამივე ქვეყანამ მოახდინა 2001 წლის ბუდაპეშტის კიბერუსაფრთხოების კონვენციის რატიფიცირება სხვადასხვა წლებში, თუმცა სამართლებრივი ნორმების თვალსაზრისით, კონტროლის მეტად დემოკრატიული ხასიათი საქართველოსა და სომხეთს გააჩნია. სამივე ქვეყანაში დიდი დოზით წარმოდგენილია არალეგალური „მეკობრული“ პროგრამული უზრუნველყოფა, რაც აუარესებს კიბერუსაფრთხოების უზრუნველყოფას ინდივიდუალური უსაფრთხოების თვალსაზრისითაც.

რას წარმოადგენს კიბერუსაფრთხოება და რამდენად შესაძლებელია მისი პრაქტიკული გამოყენება?

სხვადასხვა შემუშავებული დეფინიციებისა და კლასიფიკაციების თანახმად, კიბერუსაფრთხობა წარმოადგენს კომპლექსური ქმედებებისა და სტრატეგიების ერთობლიობას, რომელიც მიმართულია ვირტუალური ქსელების, პროცესების, კომპიუტერების, პროგრამებისა და მონაცემების ხელშეუხებლობის უზრუნველსაყოფად. დღეასდღეობით, კიბერუსაფრთხოების უზრუნველყოფა არის საერთაშორისო ორგანიზაციებისა და სხვადასხვა ქვეყნის უსაფრთხოების სტრატეგიების განუყოფელი ელემენტი. ყოველივე ეს გამოწვეულია ტექნოლოგიების ფართომასშტაბიანი ინტეგრაციიდან სხვადასხვა დონის სისტემაში. კიბერუსაფრთხოების პარამეტრები, ცალკეული მაგალითების გათვალისწინებით წარმოადგენს უსაფრთხოების სამი დონის კოლაბორაციულ ფორმას, რაც უფრო მეტად ართულებს საერთაშორისო და ეროვნული პრევენციული მექანიზმების შემუშავებას. საერთაშორისო პრაქტიკა ითვალისწინებს იმ გარემოებას, რომ ტექნოლოგიური წინსვლის, ისევე როგორც ჰაკერული თავდასხმებისა და ვირუსული პროგრამების განვითარების ტემპი ბევრად უფრო მაღალია, ვიდრე საერთაშორისო ნორმებისა და სტანდარტების შემუშავების პროცესი. აქედან გამომდინარე,

გახშირებულია სხვადასხვა სახელმწიფოს თანამშრომლობა კერძო სექტორებთან და კორპორაციებთან, რომლებიც სთავაზობენ კიბერუსაფრთხოების უზრუნველყოფის თანამედროვე მექანიზმებს.

კიბერუსაფრთხოების პრაქტიკული გამოყენება არ გულისხმობს მხოლოდ სამართლებრივი ბაზის შემუშავებას. საინფორმაციო ომის ვითარებაში ორ სახელმწიფოს შორის ერთი და იგივე მეთოდების გამოყენებას გულისხმობს. რაც თავის დროს ნიშნავს საკმარისი კვალიფიკაციის კადრების ყოლას, შესაბამისი ინფრასტრუქტურისა და პროგრამული უზრუნველყოფის მშენებლობას ეროვნულ დონეზე. ამ შემთხვევაში, ძირითადი გამოწვევა არის თავდაცვისა და თავდასმის შორის ზუსტი ზოლის გაყვანა.

რაში გამოიხატება ვირტუალურ სივრცეში კიბერსაშიშროების პარამეტრები და როგორი სახით არიან ისინი წარმოდგენილები?

კიბესაშიშროების პარამეტრები პირდაპირ პროპორციულია ვირტუალურ-ტექნოლოგიურ ინტეგრაციასთან. თავისთავად ცხადია, რომ რაც უფრო მეტი კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურა ქსელურ უზრუნველყოფაზეა დამოკიდებული, მით უფრო მატულობს ამ ობიექტის კიბერშეტევების სამიზნედ გადაქცევის პოტენციალი. კიბერსაშიშროების თავიდან აცილებისათვის საჭიროა რისკების ზუსტი პროგნოზირება და დროული რეაგირება, რაც ისაჭიროებს მუდმივ მონიტორინგსა და სიტუაციის კონტროლს. ტექნოლოგიურმა პროგრესმა უკვე მოგვცა იმის საშუალება, რომ მონაცემთა ხელშეუხებლობის 24-საათიანი მონიტორინგისათვის ავტომატიზირებული ტექნიკა გამოვიყენოთ. თუმცა ისიც უნდა გვახსოვდეს, რომ ყოველი კიბერშეტევის უკან დგას პროფესიონალური ჰაკერი, რომელიც მოქმედებს განსხვავებული მოტივით. კიბერსაშიშროების მთავარი გამოწვევა, ისევე როგორც ჰაკერების ფავორიტი ინსტრუმენტი, ჯერ ჯერობის კომპიუტერული ვირუსული პროგრამებია. მსოფლიოში უკვე არსებობს მთელი რიგი კომერციული გიგანტებისა, რომლებიც მუშაობენ ანტი-ვირუსული პროგრამული უზრუნველყოფის შემუშავებაზე, თუმცა მათი მუშაობა რთულდება „მეკობრული“ Soft-ისა და ოპერაციული სისტემების

ექსპლუატაციის დროს, რაც დღევადელ დღეს საკმაოდ ხშირია. გლობალური კიბერსაშიშროების უპირველეს სამიზნედ რჩება საბანკო-საფინანსო სექტორი. ბანკის გაძარცვა და სახსრების მოპოვება სახლიდან გაუსვლელად ჰაკერული ნიჭის მქონე ადამიანისთვის გარკვეულ „ჩართულობის რიტუალსაც“ წარმოადგენს. განსაკუთრებული ყურადღების ქვეშ იმყოფება სახელმწიფო საიდუმლო ინფორმაცია, რომელიც ელექტრონულ ფორმატში ინახება. ვირუსული პროგრამდების განვითარებამ გვიჩვენა, რომ არც სახელმწიფო ინსტიტუციონალური და არც კომერციული სექტორი არ არის საკმარისად დაცული მაღალი ენტუზიაზმისა და მოტივაციის მქონე ჰაკერული პროგრამისგან, თუნდაც “Wanna Cry”-ს ინციდენტის მაგალითზე. კიდევ ერთ პრობლემას წარმოადგენს სოციალური ცნობიერება. საზოგადოება, რომლის შემადგენელი ადამიანები ვირტუალური სივრცის აქტიური მომხმარებელნი არიან და ნაკლებად აქცევენ ყურადღებას პირადი ინფორმაციის დაცულობას. ინდივიდუალური უსაფრთხოების ელემენტებს შეიცავს ეროვნული უსაფრთხოებაც, ხოლო ვირტუალური უსაზღვრო განზომილების გათვალისწინებით, გლობალური უსაფრთხოების უზრუნველყოფაზეც მოქმედებს.

<u>კვლევის შედეგი:</u>

ნაშრომში დასმული ჰიპოთეზა ჩატარებული კვლევის შედეგად დადასტურებულია. კიბერუსაფრთხოების უზრუნველყოფა შედარებით ახალი დარგია თანამედროვე სამყაროში და სხვადასხვა სახელმწიფოს შემთხვევაში, არათანაბრადაა წარმოდგენილი ეროვნული და რეგიონული სტრატეგიის ფარგლებში. გლობალური თვალსაზრისით, მსოფლიოში არსებობს სამართლებრივი ბაზისა და საერთაშორისო სტანდარტების ნაკლებობის პრობლემა, რაც გლობალიზაციისა და თანამედროვე მსოფლიოს წესრიგის გათვალისწინებით ართულებს რეგიონული და ეროვნული კიბერუსაფრთხოების სტრატეგიის ჩამოყალიბების პროცესს. ამის და მიუხედავად, კიბერუსაფრთხოების უზრუნველყოფის მექანიზმები დიდ წილად დამოკიდებულია

ცალკეული ქვეყნის გამოცდილებაზე ამ საკითხის ირგვლივ, რასაც კავკასიის რეგიონული უსაფრთხოების შემთხვევაში, საქართველოს მაგალითი გვიჩვენებს.

XXI საუკუნეს სამყაროში ვირტუალურ-ტექნოლოგიური ინტეგრაციის მაღალი პროცენტი იკვეთება, რაც დადასტურებულია ტექნოლოგიების გამოყენებით სხვაგასხვა დარგში, სისტემურ მუშაობასა და ცალკეული ადამიანის ცხოვრებით. კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურის დაცულობა სახელწმიფოს საციცოცხლო ინტერესს წარმოადგენს, ხოლო კიბერუსაფრთხოების ელემენტი ამ შემთხვევაში უპირველესად გასათვალისწინებელია.

გამოყენებული ლიტერატურა

1 ბ. ალადაშვილი, ეკონონომიკური უსაფრთხოება: თეორია, მეთოდოლოგია, პრაქტიკა. თბილისი, 2011

2. ვ. მაისაია, ბ. ობოლაძე, ახალი გეოპოლიტიკური რეალობა და საერთაშორისო ტერორიზმი XXI საუკუნეში (გლობალური და რეგიონული ასპექტები), თბილისი, 2009;
3. ვ. მაისაია, საქართველოს საგარეო პოლიტიკის პრიორიტეტები და დეტერმინანტები „ცივი ომის“ შედეგ (1991 – 2004), სუხიშვილის სასწავლო უნივერსიტეტი, თბილისი, 2013;
4. ვლადიმერ სვანიძე, კიბერ სივრცე და კიბერუსაფრთხოების გამოწვევები, (კრებული), , თბილისი, 2015;
5. ვლადიმერ სვანიძე, ადრია გოცირიძე, კიბერ თავდაცვა: კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები. სსიპ კიბერუსაფრთხოების ბიურო, თბილისი, 2015;
6. გ. მგალობლიშვილი, ბ. ქუთელია, ი. გურული, ნ. ევგენიძე, ჰიბრიდული ომი და ევრო-ატლანტიკური სივრცის უსაფრთხოების ლანდშაფტის ცვლილება: პოლიტიკური და ეკონომიკური ასპექტები. ფონდი ღია საზოგადოება საქართველო, თბილისი, 2016;

7. მ. მელიქიშვილი, ქ. ქველაძე, ნ. ქისტაური, ეკონომიკური უსაფრთხოების ინფორმაციული ფაქტორები. ი. ჯავახიშვილის თბილისის სახელმწიფო უნივერსიტეტი, საკონფერენციო ნაშრომი, 2018;
8. საქართველოს ეროვნული უსაფრთხიების კონცეფცია;
9. საქართველოს კიბერუსაფრთხოების 2017-2018 სტრატეგია;
10. ე. ისმაილოვი, ვ. პაპავა, ცენტრალური კავკასია: გეოპოლიტიკური ეკონომიის ნარკვევები, პირველი ქართული გამოცემა, თბილისი, 2007;
11. ვ. მელიქიძე, მსოფლიო პოლიტიკის გლობალიზაცია, სალექციო კურსი სოციალური მეცნიერებების მაგისტრატურისათვის, სოციალურ მეცნიერებათა ცენტრი, თბილისი, 2006;
12. J. Cooper, Countering Terrorism, Protecting Human Rights, OSCE Office for Democratic Institutions and Human Rights (ODIHR) Warsaw, Poland, 2007;
13. The Role of Cyber Security in World Politics – V.T. Tsakanyan, RUDN University, Moscow, Russia, 2017;
14. Convention on Cyber Crime, Council of Europe, Budapest, Hungary, 2001;
15. M. Stamp, Information Security, Principles and Practice, San Jose State University, CA, United State of America, 2016;
16. B. Valeriano and Ryan C. Maness, Cyber War Versus Cyber Realities, Chapter 20 – International Relations Theory and Cyber Security - Threat, Conflict, and Ethics in an Emergent Domain, Oxford University Press, Oxford, United Kingdom, 2015;
17. V.V. Kikhtan, Z.N. Kachmazova, Information War: Concept and Main Forms of Manifestation. Volga State University, Volgograd, Russian Federation, 2018;
18. M. Dzhantaleeva, The Problems of International Security in International Relations Theory, Astrahan State University, Astrahan, Russian Federation, 2017;
19. M. Volkov, NATO and Contemporary Challenges and Threats to Euro-Atlantic Security, Kuban State University, Political Science Faculty Guidebook, Russian Federation, 2008;
20. V.T. Tskanyan, The Role of Cybersecurity in World Politics;

21. V. Portugimov, the Ipmact of Globalization on the States' Functions. The Politology Journal, Moscow, 2011;
22. А.В. Казаковцев, НАТО и Кибербезопасность. Центр Изучения Информационных Технологий, Санкт-Петербург, 2015;
23. Г.П. Григорян, Проблемы международной безопасности на Южном Кавказе. Ереванский Государственный Университет, Ереван, 2016;
24. Б. Бакленд, Ф. Шрайер, Т. Х. Винклер, Демократическое Управление и Вызовы Кибербезопасности. Женевский Центр Демократического Контроля над Вооруженными Силами, Женева, 2013;
25. Е.Г. Коновалова, Кибербезопасность как основной фактор национальной и международной безопасности XXI века. Квалификационная работа при поддержке Министерства Образования РФ, Москва, 2018;
26. А. Казарин, В. Тарасов, Современные Концепции Кибербезопасности Ведущих Зарубежных Стран, О. Москва, Российская Федерация, 2013;
27. А. С. Керобян, Н. А. Волгина, Роль Американских Транснациональных Корпораций в Мировой Экономике, РУДН, Москва, 2012;
28. А. Гасанов, Политика Национального Развития и Безопасности Азербайджанской Республики. Академия Государственного Управления и Развития при Президенте Республики Азербайджан, Баку, 2014;
29. Доктрина Национальной Безопасности Республики Армения;
30. Доктрина Национальной Безопасности Республики Азербайджан;
31. Д. К. Фамиль, Современные Аспекты Кибербезопасности в Мире, в Контексте Глобальных Угроз. Баку, 2017;
32. М. Котухов, А. Кубанков, А. Калашников, Информационная Безопасность, Московский Физико-Технический Институт, Москва, Российская Федерация, 2009;
33. Н. Минасян, Концепция «Мягкой Силы» в Контексте Теории Международных Отношений, газета «21-ый Век», Москва, 2017;

34. С. Г. Тимошков, Кибератака как Современная Форма Совершения Акта Агрессии. Москва, 2017;
35. Ю. В. Жилкина, Международная Безопасность в Эпоху Глобализации Мировой Экономики. ОаО «Федеральная сетевая компания единой энергетической системы», Москва, 2010;