კავკასიის საერთაშორისო უნივერსიტეტი

ხელნაწერის უფლებით

თორნიკე ზედელაშვილი

კიბერომი - ეროვნული უსაფრთხოების თანამედროვე საფრთხე და პოლიტიკური კონფლიქტის ახალი განზომილება

სამეცნიერო ხელმძღვანელი:

პოლიტიკის მეცნიერების დოქტორი - ვახტანგ მაისაია

პოლიტიკის მეცნიერების დოქტორის აკადემიური ხარისხის

მოსაპოვებლად

წარმოდგენილი დისერტაციის

ავტორეფერატი

თბილისი, 0141, საქართველო

2020

სამეცნიერო ნაშრომი შესრულებულია კავკასიის საერთაშორისო უნივერსიტეტის სოციალურ მეცნიერებათა ფაკულტეტის პოლიტიკის მეცნიერების სადოქტორო პროგრამაზე

სამეცნიერო ხელმძღვანელი: **ვახტანგ მაისაია**
პოლიტიკის მეცნიერების დოქტორი,
კავკასიის საერთაშორისო უნივერსიტეტის
პროფესორი

ოფიციალური რეცენზენტები: **1. გუგული მაღრაძე**
ფსიქოლოგიის მეცნიერებათა დოქტორი,
ივანე ჯავახიშვილის თბილისის სახელმწიფო უნივერსიტეტის
პროფესორი

2. ზაზა ცოტნიაშვილი
ჟურნალისტიკის დოქტორი,
კავკასიის საერთაშორისო უნივერსიტეტის
პროფესორი

დისერტაციის დაცვა შედგება 2020 წლის ----------, ------- საათზე, კავკასიის საერთაშორისო უნივერსიტეტის სოციალურ მეცნიერებათა ფაკულტეტის პოლიტიკის მეცნიერების სადოქტორო პროგრამის სადისერტაციო საბჭოს სხდომაზე.
მისამართი: 0141, თბილისი, ჩარგლის ქუჩა N 73, კავკასიის საერთაშორისო უნივერსიტეტის პირველი კორპუსი, 305 აუდიტორია.
დისერტაციის გაცნობა შეიძლება კავკასიის საერთაშორისო უნივერსიტეტის ბიბლიოთეკაში. სადისერტაციო საბჭოს მდივანი: კავკასიის საერთაშორისო უნივერსიტეტის ასოცირებული პროფესორი პეტრე მამრაძე.

ნაშრომის ზოგადი დახასიათება

საკითხის წინაპირობა და თემის აქტუალობა

თითოეული მოქალაქის სოციალური და ეკონომიკური კეთილდღეობა, ჯანმრთელობა და სიცოცხლე მნიშვნელოვნად არის დამოკიდებული ინფორმაციული სისტემებისა და ელექტრონული მომსახურების უსაფრთხოების უზრუნველყოფაზე. კიბერშეტევები დიდ გავლენას ახდენს ეკონომიკის ყველა სექტორზე, აფერხებს ეკონომიკური სივრცის გამართულ ფუნქციონირებას, ამცირებს ელოქტრონული სერვისების მიმართ საზოგადოების ნდობას და საფრთხეს უქმნის ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების გამოყენებით ეკონომიკის განვითარებას. გლობალური მასშტაბით არსებული კიბერსაფრთხეების ფონზე, როდესაც ყოველდღიურ რეჟიმში ხორციელდება კიბერშეტევები, კიბერჯაშუშობა, კიბერტერორიზმი და ვრცელდება დეზინფორმაცია, ახალი თავდაცვითი მექანიზმების შემუშავება, დანერგვა და განვითარება მნიშვნელოვან საკითხს წარმოადგენს. აღსანიშნავია, რომ ნატოს ამ მიმართულებით მნიშვნელოვანი როლი ენიჭება და ევროკავშირთან ერთად წარმოადგენს უსაფრთხოების ერთგვარ ქოლგას, როგორც წევრი, ასევე პარტნიორი ქვეყნებისთვის.

ყოველ საუკუნეს თან სდევს თავისი პრობლემები. 21-ე საუკუნეში ყველაზე საშიშ მოვლენად იქცა კიბერსივრცეში მიმდინარე მოვლენები - ყოველდღიურად ზარალდება უამრავი ადამიანი, კერძო კომპანია და სახელმწიფო დაწესებულება. თავდაცვის მიზნით უკვე იხარჯება მილიარდობით დოლარი.

ნატოს ყველა კონცეფციასა თუ დოქტრინაში ხაზგასმითაა აღნიშნული, რომ ძირითადი პრინციპებიდან გამომდინარე, მისი წევრი არც ერთი ქვეყანა არ უნდა იყოს იძულებული, დაეყრდნოს მხოლოდ საკუთარ ძალებს. ალიანსის სტრატეგია საშუალებას აძლევს თითოეულ წევრ სახელმწიფოს, კოლექტიური მეთოდებით მოახდინონ ეროვნული უსაფრთხოების მიზნების რეალიზება.

მსოფლიოში ყველა წამყვან ქვეყანას გააჩნია **კიბერუსაფრთხოების ეროვნული სტრატეგია,** რაც არის სახელმწიფო პოლიტიკის განმსაზღვრელი ფაქტორი. **ეროვნული უსაფრთხოების სტრატეგია** მიზნად ისახავს არსებული საფრთხეების გამოვლენას, აღკვეთას, შემცირებას და მოსპობას. საქართველოსთვის დიდი მნიშვნელობა აქვს პარტნიორ სახელმწიფოებთან და ორგანიზაციებთან თანამშრომლობას.

მიუხედავად იმისა, რომ საქართველო ამ ეტაპზე არ იმყოფება მოწინავე პოზიციაზე (ამას ადასტურებს არაერთი კვლევა), არსებობს თავდაცვის ეფექტური სისტემა - ფუნქციონირებს კიბერუსაფრთხოების ბიურო და მონაცემთა გაცვლის სააგენტო. როგორც საქართველოს **ეროვნული უსაფრთხოების სტრატეგიაშია** აღნიშნული, საქართველოს მიზანია, გახდეს კიბერუსაფრთხოების სერვისების რეგიონული პროვაიდერი და განავითაროს საკუთარ ტერიტორიაზე განლაგებული სხვა ქვეყნების საკომუნიკაციო სისტემების მუშაობისთვის საჭირო ინფრასტრუქტურა. ამის გაკეთება შეუძლებელია პარტნიორების დახმარების გარეშე. საქართველოს **უსაფრთხოების სამსახურის ანგარიშებში** ნათქვამია, რომ ქვეყნის უსაფრთხოებისთვის მნიშვნელოვან რისკს წარმოადგენს უცხო ქვეყნების სპეცსამსახურების მიერ კონტროლირებადი ჰაკერული დაჯგუფებები, სამთავრობო ინფრასტრუქტურაზე კიბერშეტევებისა და კიბერსადაზვერვო ოპერაციების განხორციელება.

საფრთხეების თავიდან აცილება შეუძლებელია თანამედროვე ტექნოლოგიების, პროფესიონალი კადრებისა და წამყვან სახელმწიფოებთან თანამშრომლობის გარეშე შესაბამისად, ერთადერთ გზას წარმოადგენს საერთაშორისო თანამშრომლობა. საქართველოსთვის, უასფრთხოების თვალსაზრისით, გასაძლიერებელია ნატოსთან და წამყვანი სახელმწიფოების უსაფრთხოების სამსახურებთან თანამშრომლობა, რათა დროულად მოხერხდეს პრევენციული ზომების გატარება. ასევე საჭიროა უფრო მჭიდრო თანამშრომლობაა მეზობელი სახელმწიფოების უსაფრთხოების სამსახურებთან.

ნატო ერთადერთი ორგანიზაციაა, რომელსაც ტექნიკურად, ფინანსურად თუ ადამიანური რესურსების მხრივ შესწევს ძალა, წინააღმდეგობა გაუწიოს კიბერსივრციდან მომდინარე საფრთხეებს. ამიტომ მნიშვნელოვანია დღევანდელი მდგომარეობისა და სამომავლო გეგმების შესწავლა, გაანალიზება, კვლევა, პრაქტიკული კუთხით წარმოჩენა. მკვლევართა მტკიცებით, თუ იქნება სწორი მეცნიერული მიდგომა, კიბერომის შედეგები არ გახდება ისეთი დამაგრეველი, როგორც იყო წინა წლების განმავლობაში.

კვლევის მიზნები და ამოცანები

საკვლევი თემატიკის პირობებიდან გამომდინარე და ახალი ტიპის საფრთხეების უკეთ გამოვლენის მიზნით, რომელიც გამოიხატება იმით თუ როგორი ეფექტი გააჩნია კიბერომს მსოფლიო პოლიტიკაზე და ასევე ახალი პოლიტიკური კონფლიქტის გაანალიზება-შეფასების გათვალისწინებით, შეიძლება გამოიყოს კვლევის კონკრეტული მიზნები და ამოცანები.

კვლევის ძირითადი მიზნებია:

- კიბერომის, როგორც ახალი საფრთხის ფაქტორის წარმოჩენა და მისი განხილვა კონკრეტული პოლიტიკური კონფლიქტის კონტექსტში
- ქვეყნების უსაფრთხოების საკითხების შესწავლა და ანალიზი კიბერუსაფრთხოების ფორმატის ფარგლებში
- სამოქალაქო კიბერომის ავტორისეული განსაზღვრების დადგენა და მისი გავლენის ახსნა პოლიტიკურ პროცესებზე
- კიბერომისგან მომდინარე საფრთხეების საქართველოს ეროვნულ უსაფრთხოებაზე გავლენის კვლევა და ანალიზი

სადისერტაციო ნაშრომის ამოცანებია:

- კიბერომის განვითარების ისტორია და მისი კომპონენტების საშიშროების განსაზღვრა.

- კიბერომის თეორიის ადგილის განსაზღვრა თანამედროვე მსოფლიო პოლიტიკაში
- ჰიბდირული ომის თავიდან აცილება, ბრძოლის მექანიზმები და კიბერომის პოლიტიკის მნიშვნელოვანი ფაქტორის წარმოჩენა.
- კიბერომის, როგორც ასიმეტრიული საფრთხის ფენომენის წარმოჩენა
- კონფლიქტების ტრანსფორმაციის ძირითადი პარამეტრების დაფიქსირება ახალი გეოპოლიტიკური წესრიგის პირობებში.
- ახალი გეოსტრატეგიული ამოცანების აღწერა და ახალი საფრთხის შემცველი გამოწვევების ანალიზი
- ვირტუალური საფრთხის და ასიმეტრიული სამხედრო გამოწვევების კვლევა და ანალიზი

<u>ნაშრომის ძირითადი საკვლევი კითხვები:</u>

1. რამდენად შეიძლება კიბერომის აღქმა პოლიტიკური კონფლიქტის ახალ რეალობად?
2. რა გავლენა შეიძლება იქონიოს საერთაშორისო საზოგადოებაზე კიბერომმა?
3. როგორია სამოქმედო გეგმა და სამხედრო სტრატეგიის შემადგენელი ნაწილები კიბერ ომის პირობებში?
4. რა მნიშვნელობა ენიჭებათ კიბერუსაფრთხოების უზრუნველყოფის საკითხში საქართველოს სტრატეგიულ პარტნიორებს?

ჰიპოთეზა

გლობალურ უსაფრთხოებაში პოლიტიკური კონფლიქტების ახალი განზომილება ერთ-ერთი მნიშვნელოვანი და საკვანძო საკითხია. კიბერომი მნიშვნელოვან გავლენას ახდენს საერთაშორისო უსაფრთხოების პროცესების მიმდინარეობასა და შედეგებზე.

კვლევის საგანი და ობიექტი

კვლევის საგანი - კიბერომის და კიბერ საფრთხეების პირობებში ეროვნული უსაფრთხოების წინაშე მდგარი რისკები და საფრთხეები პოლიტიკური კონფლიქტის ახალი განზომილების პიროცესში თანამდეროვე მსოფლიო პოლიტიკაში.

კვლევის ობიექტი - ევროატლანტიკური ალიანსის როლი კიბერთავდაცვის საკითხში და საერთასორისო უსაფრთხოების უზრუნველყოფაში.

თემის მეცნიერული სიახლე

- ქართულ მეცნიერებაში პირველად მოხდა კიბერომთან და კიბერუსაფრთხოებასთან დაკავშირებით ასეთი კვლევის ჩატარება. ასევე ტექნოლოგიების, საფრთხეებისა და თავდაცვითი სისტემების კლასიფიკაციის გამოკვეთა. ტერმინების დეფინიციების განსაზღვრა. ვირუსებისა და ანტივირუსების მონაცემების დამუშავება-წარმოჩენა კომბინირებულ სისტემაში, კიბერშეტევის მიზნობრივი ჯგუფების ჩამოყალიბება.
- კიბერომი - ეს არის პოლიტიკური კონფლიქტის ახალი განზომილება, სივრცითი მოდელი, რომლის საშუალებითაც ხდება კიბეროპერაციების შეზავება სამხედრო თუ სხვა სახის მოქმედებებში. კიბერომამდე არსებობდა ომის სამი განზომილება - ხმელეთი, ცა და ზღვა. ამას დაემატა <u>ომის მეოთხე თაობა, ანუ ვირტუალური სივრცე</u> - ერთგვარი ალტერნატიული ომის ვარიანტი. ეს საკითხი პირველად არის ქართულ მეცნიერებაში გამოკვლეული მასშტაბური ფორმით, რომელიც ემყარება ავტორისეულ მოსაზრებებსა და კვლევებს.
- კიბერსივრცეში არსებული მდგომარეობიდან გამომდინარე, პოლიტიკურ ლექსიკონში გვინდა შემოვიტანოთ ახალი ტერმინი - <u>**სამოქალაქო კიბერომი,**</u> ეს გახლავთ ახალი გარემოების საფუძველზე ჩამოყალიბებული ტერმინი. სხვადასხვა **პოლიტიკური დაჯგუფებები** ეწევიან სამოქალაქო

დაპირისპირებას კიბერსივრცეში, ხშირია თავდასხმები, სადაც აშკარად ჩანს პოლიტიკური ინტერესები. მიმდინარეობს საინფორმაციო ომი, სადაც ჩართულნი არიან მედიასაშუალებები (მედიამფლობელები) და გამოხატავენ პოლიტიკური დაჯგუფებების პოზიციებს. მხარეები იყენებენ ახალ ტექნოლოგიებს, ბრძოლა მიდის აკრძალული ილეთებით - ავრცელებენ დეზინფორმაციას, იყენებენ სიძულვილის ენას, თესავენ ღვარძლს, აღვივებენ კონფლიქტებს ერებს შორის. ამ საშიშ კამპანიას უპირისპირდება მედიასაშუალებების გარკვეული ნაწილი, მაგრამ რამდენად ბალანსდება სიტუაცია, ეს საკამათო თემაა. მაგალითად, საქართველოში ერთ მხარეს არიან ტელევიზიები რომლებიც ეწევიან ავტორიტეტული ადამიანების მორალურ განადგურებას (**„მთავარი არხი“, „ტვ პირველი“ „ფორმულა“**) ხოლო მეორე მხარეს - (**„იმედი“, „პოსტვ“**) რომლებიც უპირისპირდებიან დეზინფორმაციას. საერთო ჯამში, ქართული მედიასაშუალებების სტილი არის უფერული, უიდეო, უინტერესო და რაც მთავარია, პოლიტიკურად ანგაჟირებული. რა თქმა უნდა, დემოკრატიული თვალსაზრისით ხელისუფლების კრიტიკა მისაღებია, მაგრამ საზოგადოების „დასახიჩრება“ ყალბი ახალი ამბებით დაუშვებელია. შესაცვლელია „კანონი სიტყვისა და გამოხატვის თავისუფლების შესახებ“, კონკრეტულად კი მე-4 მუხლი, სადაც ცილისწამებაზეა საუბარი. სისხლის სამართლის საპროცესო კოდექსში უნდა დაბრუნდეს მუხლი ცილისწამებისა და დეზინფორმაციის გავრცელების შესახებ. სიტყვისა და გამოხატვის თავისუფლება უნდა შეჩერდეს იქ, სადაც ილახება სხვისი თავისუფლება და უფლებები. აღნიშნული ფორმულირება დაფიქსირებულია საქართველოს კონსტიტუციაშიც. თუმცა „ცილისწამება“, როგორც ადამიანის მორალური განადგურების იარაღი, არ არის აკრძალული და არც ამ იარაღის გამომყენებელი ისჯება. გამკაცრებული კანონი ვერ დაანგრევს დემოკრატიულ წყობილებას, პირიქით, დაარეგულირებს საზოგადოების ინტერესებს. ამის საუკეთესო მაგალითია

საფრანგეთი, სადაც ცილისწამებასა და დეზინფორმაციის გავრცელებაზე საკმაოდ დიდი სასჯელია გათვალისწინებული.

- ახალი ტიპის ეროვნული სტრატეგიული დოკუმენტის შემოტანა ჩვენი ქვეყნის პოლიტიკურ რეალობაში წარმოადგენს მნიშვნელოვან საკითხს იმ ფონზე, როდესაც ხშირია საქართველოს კიბერსივრცეზე ჰაკერული შეტევები. ნაშრომში შემოთავაზებულია **კიბერუსაფრთხოების ეროვნული დოქტრინა,** რომელიც წარმოადგენს აუცილებელ გარემოებას ქვეყნის თავდაცვისა და უსაფრთხოების განმტკიცების საქმეში.

ნაშრომის თეორიული და პრაქტიკული მნიშვნელობა

თეორიული ღირებულება: ნაშრომის კვლევის შედეგები შესაძლებელია გამოადგეთ კიბერუსაფრთხოების სპეციალისტებს, ჰიბრიდული ომების ანალიტიკოსებს, კიბერტერორიზმის წინააღმდეგ მებრძოლ ორგანიზაციებს, დარგით დაინტერესებულ კერძო პირებს. მისი გამოყენება შესაძლებელია შემდგომი კვლევებისთვის. ასევე უმაღლესი სასწავლებლების საბაკალავრო და სამაგისტრო პროგრამებში.

პრაქტიკული ღირებულება: კვლევები და რეკომენდაციები გამოსადეგია საქართველოს მთავრობის მიერ ქვეყნის უსაფრთხოების სტრატეგიის ძირითადი მიმართულებების განსაზღვრის დროს. შესაძლოა, კვლევის შედეგები განზოგადდეს პოსტსაბჭოთა ქვეყნებისა და აღმოსავლეთ ევროპის სახელმწიფოებისთვის.

კვლევის მეთოდოლოგია

1. **ბიჰევიორიზმის თეორია** - ფსიქოლოგიური სკოლა, რომელსაც საფუძველი 1913 წელს **ჯონ უოტსონმა** (1878 -1958) ჩაუყარა. სკოლა ფსიქოლოგიის, როგორც მეცნიერების შესწავლის საგნად ქცევას ასახელებს, მიზნად ქცევის წინასწარმეტყველებასა და

კონტროლს ისახავს. **უოტსონის** კვლევებს ეხმიანებოდა **ი. პავლოვის** ნაშრომი, რამაც კიდევ უფრო გააძლიერა ბიჰევიორიზმი, როგორც მეცნიერული მიდგომა. თეორია გამოყენებულია კიბერბიჰევიორისტული მიდგომის თვალსაზრისით, რომელსაც ასევე აქტიურად იყენებს აშშ-ის არმია.

2. **პოლიტიკური რეალიზმის თეორია** - ამ თეორიის დებულება მდგომარეობს იმაში, რომ სახელმწიფოები **არ ცდილობენ თანამშრომლობას.** ადრეული რეალისტები **ედვარდ ქარი** და **ჰანს მორგენთაუ** მიიჩნევდნენ, რომ საკუთარი უსაფრთხოებაზე ზრუნვის გამო სახელმწიფოები არიან **ეგოისტური რაციონალური აქტორები,** რომლებიც ისწრაფვიან ძალაუფლებისკენ. მეთოდოლოგია გამოყენებულია რეალიზმის ფუძემდებლის, თუკიდიდეს და ამ თეორიის მიმდევრების, მორგენთაუს, სენეზის, ვასქეზის და ა.შ. მოსაზრებების საფუძველზე, ასევე კიბერტექნოლოგიების განვითარების თვალსაზრისით წარმოდგენილი მაგალითებით, განვიხილავთ კონფლიქტების ტრანსფორმაციას ახალი გეოპოლიტიკური წესრიგის პირობებში. პოლიტიკური რეალიზმის მეთოდოლოგიას დიდი ადგილი უკავია 21 საუკუნის კიბერპოლიტიკაში.
3. **ძალთა ბალანსი, ანუ ძალთა წონასწორობა** - იგი გამომდინარეობს საერთაშორისო სისტემის **ანარქიული სტრუქტურიდან.** ამ თეორიის თანახმად, დამოუკიდებლობისა და უსაფრთხოების შესანარჩუნებლად სახელმწიფოები ერთად მოქმედებენ, რათა დაუპირისპირდნენ იმ სახელმწიფოს (ან სახელმწიფოთა ჯგუფს), რომელიც საფრთხეს უქმნის მათ უსაფრთხოებასა და სუვერენიტეტს. ამგვარად, საერთაშორისო სისტემა დაყოფილია სახელმწიფოთა რამდენიმე ჯგუფად, რომლებიც დაახლოებით თანაბარი ძალისანი არიან და მათ შორის არსებული ძალთა ბალანსი (წონასწორობა) არის მშვიდობისა და წესრიგის მთავარი გარანტი საერთაშორისო სისტემაში, ამ სისტემის მდგრადობის ძირითადი პირობა.

ეს თეორია გამოვიყენეთ კიბერტექნოლოგიების განვითარების ფონზე, არსებული გეოპოლიტიკური ძალთა ბალანსის განსასაზღვრად და კიბერსივრცეში ძალთა ბალანსის, ანუ ძალთა წონასწორობის შეფასებისთვის. ტექნოლოგიების და ვირტუალური სივრცის განვითარებამ გარკვეულწილად შეცვალა ქვეყნების მიერ გადაწყვეტილებების მიღების, პოლიტიკის შექმნისა და ერთმანეთთან ურთიერთობის გზა, ამიტომ მნიშვნელოვანია ამ თეორიის მიხედვით გაანალიზებული გეოპოლიტიკური მდგომარეობა.

4. **რიჩარდ კოენის „კოლექტიური უსაფრთხოების“ თეორიის მიხედვით** წარმოდგენილია შემდეგი კონცეფცია - **ინდივიდუალური უსაფრთხოება, კოლექტიური უსაფრთხოება, კოლექტიური თავდაცვა და სტაბილურობის შენარჩუნება.** რიჩარდ კოენის თეორია, შეიძლება ითქვას, წარმოადგენს ნატოს უსაფრთხოების ქვაკუთხედს, რაც განსაზღვრულია ამ ორგანიზაციის წესდების მეხუთე მუხლში. იგი ვრცელდება კიბერსაფრთხეების თვალსაზრისითაც. აღნიშნული კოლექტიური თავდაცვის კონცეფცია ამ კუთხით გვაქვს გამოყენებული, რომლის მნიშვნელოვან გარანტს ნატო-ევროკავშირის ერთობლივი მუშაობა წარმოადგენს, როგორც წევრ, ისე არაწევრ ქვეყნებთან.

თემის დამუშავების დროს გამოყენებული კვლევის მეთოდები

არსებული თეორიული მასალის განხილვა, ანალიზი და დასკვნების გამოტანა, რომელიც ასევე დაეფუძნა ემპირული კვლევის საფუძვლებს.

თვისობრივი კვლევის მეთოდები:

- **ნარატიული და დესკრიფციული** - ითვალისწინებს თხრობით, მოთხრობით წყაროებს. მაგალითად: ისტორიის, დღიურების, ბიოგრაფიების, მემუარებისა და აღწერითს. აღნიშნული მეთოდი დაგვეხმარა ნაშრომში მასალების, წყაროების წარმოსადგენად.

ნაშრომში წარმოდგენილია ტექნოლოგიების, ინტერნეტის, კიბერშეტევების, ვირუსების, კიბერთაღლითობისა და კიბერომების ისტორიული მიმოხილვა, ასევე წარმოდგენილია კიბერშეტევების და მავნე კოდის შედევების აღწერა-კლასიფიკაცია. ნაშრომში აღწერილია რუსეთ-საქართველოს ომის ისტორია, ასევე ირანის ისლამური სახალიფოს შემთხვევის გარჩევა და ირანის ისლამური სახალიფოს კიბერშესაძლებლობები.

- **სიღრმისეული ინტერვიუ** - ინტერვიუს სახეობა, ნაწილობრივ სტრუქტურირებული ინტერვიუ, რომელიც აგებულია რესპონდენტთა მოსაზრებების საფუძველზე. მეთოდი გამოვიყენეთ ექსპერტებთან ინტერვიუების ჩაწერისას.
- **დისკურს-ანალიზი** - ეს მეთოდი გამოვიყენეთ სატელევიზიო გადაცემების გასაანალიზებლად.
- **შინაარსის ანალიზი** - Content-analyze მეთოდი, რომელიც დაკავშირებულია მედიის მიერ გავრცელებული ინფორმაციის შესწავლასთან. მეთოდი გამოვიყენეთ მედიასაშუალებების მიერ გავრცელებული ინფორმაციის გაანალიზება-განსაზღვრაში.
- **ივენტ-ანალიზის მეთოდი** - პოლიტიკური რეალობის შესწავლა. მეთოდი გამოიყენება პოლიტიკოსების ურთიერთქმედების დინამიკის გასაანალიზებლად. ნაშრომში გამოყენებულია სხვადასხვა ქვეყნის პოლიტიკოსების, მათ შორის საქართველოს პოლიტიკოსების ურთიერთობების დინამიკის ანალიზისთვის.
- **პოლიტიკის კვლევის ანალიზი** - გლობალურ, რეგიონულ და ლოკალურ დონეზე. ნაშრომში ეს საკითხი წარმოდგენილია როგორც გეოპოლიტიკური თვალსაზრისით, ისე კიბერპოლიტიკურ სივრცესთან მიმართებაში.

ლიტერატურის მიმოხილვა

სადისერტაციო ნაშრომში გამოყენებულია ყველა ის წყარო, რომელიც მნიშვნელოვნად და მიზანშეწონილად მივიჩნიეთ. გამოყენებულია მხოლოდ ის წყაროები, რომელსაც კავშირი აქვს

სადისერტაციო თემასთან. გამოყენებულია ბევრი უცხოენოვანი და ქართულენოვანი სახელმძღვანელოები, კრებულები, სტატიები, კვლევები, ოფიციალური დოკუმენტები და ა.შ.

მნიშვნელოვან წყაროებს შეადგენს, ნაშრომში გამოყენებული - **თუკიდიდეს, ედვარდ ქარის, ჰანს მორგენთაუს, ჯონ ვუტსონის, ი. პავლოვის, რიჩარდ კოენის, სენეზის, ვასქეზის** ნაშრომები და კონცეფციები, რომლებიც კლასიკურ თეორიებს თუ მოსაზრებებს გადმოგვცემენ უსაფრთხოების ჭრილში, რაც პირდაპირ უკავშირდება კიბერტექნოლოგიების და კიბერუსაფრთხოების ფუნდამენტურ საფუძვლებს. იქიდან გამომდინარე, რომ ნაშრომის ძირითადი თემატიკა კიბერომია, რომელიც მსოფლიო მასშტაბით შედარებით ახალ საკვლევ საგანს წარმოადგენს, ნაშრომში წარმოდგენილია შედარებით ახალი სახელმძღვანელოები და სხვადასხვა კვლევები. მაგალითად:

1. „Cyber Operations - Building, Defending, and Attacking Modern Computer Networks“. ავტორი გახლავთ მაიკ ოლილე (Mike O'Leary), გამოიცა აშშ-ის მათემატიკის დეპარტამენტის მხარდაჭერით, 2015 წელს.
2. სახელმძღვანელო - "Cyber Dragon - Inside China's Information Warfare and Cyber Operations", ავტორი გახლავთ მკვლევარი დეკანი ჩენგი (Dean Cheng). წიგნი გამოიცა 2017 წელს აშშ-ში.
3. კნაფ კენეტის (Kenneth J. Knapp) წიგნი - "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions“, რომელიც გამოქვეყნდა კოლორადოში, აშშ-ის საჰაერო ძალების აკადემიის მიერ, 2009 წელს.
4. „The NICE Cyber Security Framework - Cyber Security Intelligence and Analytics“, წიგნის ავტორი გახლავთ ტეხასის უნივერსიტეტის პროფესორი იზზატ ალსმადი. გამოიცა აშშ-ი, 2019 წელს.

ნაშრომში ასევე წარმოდგენილია წყაროები ქართველი პროფესორების, დოქტორებისა და მკვლევარების ნაშრომებიდან. **ვლადიმერ სვანაძის** და **ანდრია გოცირიძის** ნაშრომებისა და

სტატიების კრებული.- **„კიბერთავდაცვა, კიბერსივრცის მთავარი მოთამაშეები, კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები“**, რომელიც საქართველოს თავდაცვის სამინისტროს დაქვემდებარებაში მყოფმა კიბერუსაფრთხოების ბიურომ გამოსცა, 2015 წელს. ასევე სახელმძღვანელო, **XXI საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების თეორია: მითი და რეალობა - რეგიონული და გლობალური ასპექტები“ - ვახტანგ მაისაია, გუგული მაღრაძე, გამომცებლობა „უნივერსალი“. რომელიც გამოიცა თბილისში, 2017 წელს.** გასათვალისწინებელია, რომ წყაროები წარმოადგენს მნიშვნელოვან საინფორმაციო ბაზას გლობალურ პოლიტიკაში კიბერტექნოლოგიების განვითარების, კიბერომის, კიბერშეტევების, კიბერუსაფრთხოების მექანიზმების გაანალიზების, განსაზღვრისა და შეფასების კუთხით. ყველა წარმოდგენილი წყარო, რომელიც ეხება ნაშრომის თემატიკას, საინტერესო და გამოსადეგია.

სამეცნიერო ნაშრომის მოცულობა და სტრუქტურა:

სადოქტორო ნაშრომი კიბერომი - ეროვნული უსაფრთხოების თანამედროვე საფრთხე და პოლიტიკური კონფლიქტის ახალი განზომილება“ წარმოდგენილია A4 211 გვერდად. ნაშრომი შედგება შესავლის, სამი თავის, 9 ქვეთავის, სიღრმისეული ინტერვიუების, დისკურს-ანალიზის, დასკვნებისა და რეკომენდაციებისგან. ნაშრომს თან ერთვის გამოყენებული ლიტერატურის სია, რომელიც მოიცავს 139 დასახლებას.

ნაშრომის ძირითადი შინაარსი

თავი პირველი - კიბერომის არსი და ისტორიული მიმოხილვა

მოცემული თავი შედგება 3 ქვეთავისგან.

საერთაშრისო პოლიტიკაში ვითარდება ტექნოლოგიები და მათი გამოყენებით მავნე საქმიანობის საფრთხეც. ეპოქა, რომელშიც ვცხოვრობთ, ტექნოლოგიური რევოლუციების ყოველდღიურ რეჟიმს წარმოადგენს, ახალი ტექნოლოგიებით კი იბადება მძლავრი უფრო მოქნილი, როგორც თავდაცვითი, ასევე თავდასხმითი მექანიზმები. კიბერშეტევები ჩვენი ცხოვრების განუყოფელი ნაწილი გახდა, რომელიც ყველა სამხედრო ომის თანმდევია. დღეს ომები მიმდინარეობს ჰიბრიდული კომპონენტების გამოყენებით. კიბერომი, როგორც მოვლენა, დაიწყო კომპიუტერისა და ინტერნეტის გამოგონებით. აღნიშნული თავი ეთმობა კომპიუტერის შექმნას და განვითარებას, ინტერნეტის შექმნას, პირველ კავშირს, „ვების კონცეფციის“ ისტორიას, ვირუსის შექმნას, კიბერომის არსს, ისტორიულ მიმოხილვას, კიბერშეტევებისა და კიბერომების წარმოების პირველ ეტაპს.

1.1. კიბერომის თეორია და მისი ადგილი თანამედროვე მსოფლიო პოლიტიკაში

ყოველივე არსებულს გააჩნია როგორც თეორიული, ასევე პრაქტიკული მიმართულება, როდესაც ვსაუბრობთ კიბერომზე, პირველ რიგში უნდა ავხსნათ, თუ რა მოვლენასთან გვაქვს საქმე. ეს არის ერთი ქვეყნის მიერ მეორე ქვეყანაზე ციფრული შეტევების გამოყენება, (კომპიუტერული ვირუსები ან ჰაკერული კიბერშეტევები) კომპიუტერული ინფრასტრუქტურის დაზიანების, ლიკვიდაციისა და განადგურების მიზნით.

ტერმინ **„კიბერომთან“** დაკავშირებით ექსპერტებს შორის განსხვავებული მოსაზრებები არსებობს. ერთნი ამბობენ, რომ ტერმინი **„კიბერომი“** არასწორია, რადგან დღემდე არცერთი კიბერშეტევა არ შეიძლება შეფასდეს, როგორც **„ომი“**. ექსპერტების მეორე ნაწილი მიიჩნევს, რომ ეს შესაბამისი სახელწოდებაა, რადგან

კიბერშეტევა ფიზიკურ ზიანს აყენებს ადამიანებსა და საგნებს რეალურ სამყაროში. ამ ქვეთავში განხილულია კიბერომის თეორიული და პრაქტიკული ასპექტები, მისი ადგილი თანამედროვე მსოფლიო პოლიტიკაში. იმის საფუძველზე, რომ სხვადასხვა ექსპერტები კიბერომის განმარტებასთან დაკავშირებით დაობენ და მსოფლიო მასშტაბით ხშირია შემთხვევები, როდესაც კიბერომს და კიბერშეტევას ერთ ტერმინად განიხილავენ, ჩვენ განვსაზღვრეთ კიბერომისა და კიბერშეტევის განსხვავება. წარმოდგენილია კიბერომის წარმოების სამი ძირითადი მეთოდი და კიბერომის წარმოების მაგალითები.

1.2. კიბერომის ტრანსფორმაციის ისტორიული ასპექტები: სამხედრო კონფლიქტების სივრცული მახასიათებლები

ტექნოლოგიების განვითარებამ არ შეცვალა პრიორიტეტები სახელმწიფო დაცვის საკითხებში ისევე, როგორც მეორე მსოფლიო ომის დროს - ძირითადი ტაქტიკური დარტყმები ენერგეტიკული ობიექტებისკენ არის მიმართული. ამჟამად სერიოზული კიბერთავდასხმების უმეტესობა ხდება საწვავისა და ენერგეტიკულ კომპლექსებზე, შემდეგ მოდის ფინანსური სექტორი. ციფრულმა სამყარომ ახალი ტიპის საფრთხეების წარმოშობას შეუწყო ხელი. როგორც უკვე აღვნიშნეთ, ყველა სახის კიბერშეტევას ვერ განვიხილავთ კიბერომის ჭრილში. მიუხედავად იმისა, რომ ჩვენ განვსაზღვრეთ, რა არის კიბერომი და რა კიბერშეტევა, მაინც რთულია კიბერომის კვალიფიკაციის მინიჭება, რადგან უმეტესი ფაქტი მსოფლიო მასშტაბით ემყარება ვარაუდს. კვალს ხშირად მივყავართ რომელიმე აგრესორ სახემწიფომდე, მაგრამ ხშირად მტკიცებულებები არ არსებობს. კიბერომებსა თუ ტექნიკურ მახასიათებლებს განვიხილავთ სხვადასხვა კვლევებზე დაყრდნობით, ვაკეთებთ ანალიზს - როდიდან იწყება, როგორ ტრანსფორმირდა, რა როლი აქვს კონფლიქტების წარმოებისას და ასე შემდეგ. მნიშვნელოვანი ფაქტია, რომ მრავალი სახელმწიფო არა მხოლოდ ანხორციელებს კიბერჯაშუშურ საქმიანობას, დაზვერვას და გამოკვლევას, არამედ თვითონ ქმნიან კიბერომის

შესაძლებლობებს. მე-20 საუკუნის ბოლოს ვერავინ წარმოიდგენდა, რომ რეალური ომი იქცეოდა განყენებულ განზომილებაში შექმნილი ომის დანამატად, ან პირიქით, ირეალური სივრცე შეერწყმებოდა რეალურ სივრცეს. ალბათ, ვერც იმას წარმოიდგენდა ვინმე, რომ გაჩნდებოდა განზომილება, რომლის გაკონტროლება იქნებოდა თითქმის შეუძლებელი და უსაზღვრო, კაცობრიობა დადგებოდა უხილავი საფრთხის წინაშე.

აღნიშნულ ქვეთავში გაანალიზებულია კიბერომის ტრანსფორმაციის ისტორიული ასპექტები. იქიდან გამომდინარე, რომ კიბერომის წარმოების მეთოდების დახვეწა და განვითარება პირდაპირ არის დაკავშირებული ტექნოლოგიების განახლებასთან, ამ თავში ვაანალიზებთ კიბერშეტევებისა და კიბერომების ფორმებს - როგორი იყო და როგორი გახდა ტექნოლოგიები. განხილულია აქტიური და პასიური კიბერშეტევები. წარმოდგენილია ყველაზე აქტიური კიბერშეტევებისა და მავნე კოდის შეტევების ტიპები. კვლევის საფუძველზე გამოვყავით კიბერშეტევის სამი სამიზნე ჯგუფი. ამ თავში წარმოდგენილია საერთაშორისო კვლევითი კომპანია „Gartner"-ის სტატისტიკური მონაცემები კიბერტექნოლოგიების განვითარებაზე ფინანსური კუთხით. ასევე „Cybersecurity Ventures"-ის ანგარიში, სადაც დათვლილია 2021 წლისთვის კიბერთავდასხმებისგან მიყენებული ზარალი. ყურადღება გამახვილებულია რუსეთიდან მომდინარე საფრთხეებზე.

1.3. კიბერომის კონცეფცია და 21-ე საუკუნის საერთაშორისო უსაფრთხოების სისტემა

ჩვენ ვხედავთ ფიზიკურ ინსტრუმენტებს, როგორიცაა კომპიუტერები, კაბელები, მობილურები და ა.შ. ინსტრუმენტები ურთიერთქმედებენ ვირტუალურ და არარეალურ სფეროში. ეს ხელს უწყობს დედამიწის ერთი ნაწილიდან, ომის წარმოებას დედამიწის მეორე ნაწილში, დამნაშავის ამოცნობა კი ყოველთვის ვერ ხერხდება. კიბერომი ხშირად წარმოადგენს კონცეპტუალურ ჩარჩოს, რომელიც დაკავშირებულია ომის ტრადიციულ წარმოებასთან - მოიცავს

ძალის დემონსტრირებას, ფიზიკურ ზიანს და ძალადობას. რაც დრო გადის, მით უფრო მნიშვნელოვანი ხდება იმის დაზუსტება, თუ რა ტიპის კიბერშეტევას უნდა ეწოდოს კიბერომი. განხილულია კიბერომის კონცეფციის სხვადასხვა თეორიები. გაანალიზებულია ნატოს „კიბერთავდაცვის სფეროში თანამშრომლობის უნარების ცენტრის“ ხელმძღვანელობით შექმნილი **„ტალინის სახელმძღვანელო“**, სადაც საერთაშორისო სამართლის კანონების მიხედვით არის განხილული კიბერომებში გამოყენებული კანონდარღვევები. წარმოდგენილია ნატო-ევროკავშირის მოკლე ისტორიული მონაკვეთები კიბერუსაფრთხოებასთან დაკავშირებით. ყურადღება გამახვილებულია აშშ-ის დამოკიდებულებაზე, ფინანსურ ინვესტიციაზე კიბერტექნოლოგიების განვითარების კუთხით. გაანალიზებულია აშშ-ის სტრატეგია კიბერსივრცის დაცვასთან დაკავშირებით, ეროვნული უსაფრთხოების სტრატეგია, რუსეთის საინფორმაციო ომის დოქტრინა. ამ ქვეთავში წარმოდგენილია ციტირება მკვლევარ **დეკანი ჩენგის** წიგნიდან - **„კიბერ დრაკონი - ჩინეთის საინფორმაციო ომი და კიბერ ოპერაციები“**, სადაც აღწერილია ჩინეთის საინფორმაციო ომის წარმოება და კიბეროპერაციები.

თავი მეორე - კონფლიქტების ტრანსფორმაცია ახალი გეოპოლიტიკური წესრიგის პირობებში

<u>მოცემული თავი შედგება 3 ქვეთავისგან.</u>

თემას განვიხილავთ **პოლიტიკური რეალიზმის თეორიაზე** დაყრდნობით. რეალიზმი დიდი ხანია დომინირებს პარადიგმად საერთაშორისო ურთიერთობების სფეროში და ემყარება ზოგად ვარაუდებს საერთაშორისო პოლიტიკის შესახებ. მაგალითად, იმას, რომ სახელმწიფოები არიან ყველაზე მნიშვნელოვანი მოქმედი პირები, როგორც დამოუკიდებელი ერთეულები საერთაშორისო სისტემაში, არ გააჩნიათ ცენტრალიზებული ავტორიტეტი და აქვთ საკუთარი ინტერესები, რათა უზრუნველყონ ძალა და

უსაფრთხოება. ამ მეთოდოლოგიის არსი არის მნიშვნელოვანი კიბერუსაფრთხოების სფეროში. **პოლიტიკური რეალიზმის თეორიის** მნიშვნელობა დიდია **საერთაშორისო კიბერპოლიტიკაში.** ამ შემთხვევაში ის ცალსახად უკავშირდება კიბერუსაფრთხოებას. ისტორიულად, **პოლიტიკური რეალიზმის თეორიის** საფუძვლები შეიძლება მოვიძიოთ **თუკიდიდეს** მიერ **პელოპონესის ომის** აღწერილობაში (ძვ.წ. V საუკუნე), სადაც მან ხაზი გაუსვა საერთაშორისო პოლიტიკის ამორალურ ხასიათს და ძალაუფლების მნიშვნელობას გადარჩენისთვის. საერთაშორისო ურთიერთობებში ამ თეორიის ჩამოყალიბება შეიძლება ძირითადად **ჰანს მორგენთაუს** (1948) დამსახურება იყოს, რომელიც ყურადებას ამახვილებს ძალაუფლებისთვის ბრძოლაზე დამოუკიდებელ სახელმწიფოებს შორის.

ამ თავში პოლიტიკური რეალიზმის მეთოდოლოგიაზე დაყრდნობით განვიხილავთ კონფლიქტების ტრანსფორმაციას ახალი გეოპოლიტიკური წესრიგის პირობებში, თუ როგორი მნიშვნელოვანი ადგილი უკავია ამ მეთოდოლოგიას საერთაშორისო კიბერპოლიტიკაში.

2.1. ვირტუალური საფრთხე და ასიმეტრიული სამხედრო გამოწვევები

მსოფლიოში არსებობს ომის წაროების ხუთი სივრცე - **ჰაერი, ხმელეთი, ზღვა, კოსმოსური სივრცე და კიბერსივრცე.** ჩვენი საკვლევი თემაა **კიბერსივრცე.** ვირტუალურ საფრთხეებში მხოლოდ კიბერომები, ფქსიქოლოგიური ტერორი, ციფრული ვირუსები და ჰაკერული თავდასხმები არ შედის, ვირტუალური საფრთხე მოიცავს საინფორმაციო და დეზინოფორმაციულ მანიპულაციებსაც, ასევე გლობალურ ინტერნეტ ბაზარს, რომელიც შავი ბაზრის სახელით არის ცნობილი (Darknet). პირველ რიგში გამოვყოთ **საინფორმაციო ომი,** რომელიც მოიცავს საინფორმაციო ტექნოლოგიების გამოყენებას და მენეჯმენტს მოწინააღმდეგეზე უპირატესობის მოსაპოვებლად. იგი შეიძლება გამოყენებულ იქნას ტაქტიკური ინფორმაციის მოსაპოვებლად, დეზინფორმაციისა და პროპაგანდის

გავრცელებაში, რათა მოხდეს საზოგადოების ან მოწინააღმდეგის დემორალიზება. შეიძლება იქნას გამოყენებული მანიპულაციისთვის, ასევე შეუშალოს ხელი რეალური ინფორმაციის გავრცელებას.

განხილულია ვირტუალური საფრთხეები, სადაც მხოლოდ კიბერშეტევები და კიბერომები არ მოიაზრება. გაანალიზებულია კიბერსივრცეში საინფორმაციო, პროპაგანდისტული და დეზინფორმაციული მანიპულაციები, მოკლე ისტორია და განვითარება. ყურადღება გამახვილებულია ფეიკნიუსებზე, აღნიშნული საკითხები კი არის სხვადასხვა მაგალითებით გამყარებული. გაანალიზებულია, თუ როგორ მუშაობს ეს ყველაფერი საქართველოსთან მიმართებაში და მოყვანილია 2016 წლის NDI-ის კვლევა. ამ ქვეთავში ჩვენი კვლევის შედეგად არის წარმოდგენილი კიბერსივრცის კლასიფიკაცია და განხილულია **შავი ბაზარი,** რომელიც დიდ საფრთხეს წარმოადგენს მსოფლიო მასშტაბით. კიბერუსაფრთხოების სპეციალისტის, **კნაფ კენეტის** წიგნიდან მოცემულია ინფორმაცია - "**კიბერუსაფრთხოება და ინფორმაციის გლობალური უზრუნველყოფა - საფრთხეების ანალიზისა და რეაგირების გადაწყვეტილებების შესახებ**", რომელიც გამოიცა კოლორადოში, აშშ-ის საჰაერო ძალების აკადემიის მიერ და ეხება კიბერსივრცეში არსებულ **შავ ბაზარს.**

2.2. თანამედროვე მაღალი ტექნოლოგიების გავლენა საერთაშორისო უსაფრთხოების პროცესებზე

ტექნოლოგიების და ვირტუალური სივრცის განვითარებამ შეცვალა ქვეყნების მიერ გადაწყვეტილებების მიღების, პოლიტიკის შექმნისა და ერთმანეთთან ურთიერთობის გზა. ტექნოლოგიების განვითარებას მოაქვს ეფექტურობა და წარმატებები თითქმის ყველა სფეროში. თუმცა დღეს გაუგებარია, რამდენად შეცვალა თანამედროვე ტექნოლოგიებმა გლობალური **ძალთა ბალანსი, ანუ ძალთა წონასწორობა** კიბერსივრცეში. ამ მხრივ ცოტა განსხვავებული სურათი გვაქვს.

ძალთა ბალანსი, ანუ ძალთა წონასწორობა საერთაშორისო ურთიერთობათა თეორიაში ერთ-ერთი უძველესი და უმთავრესი საკითხია. ამ კონცეფციის თანახმად, სახელმწიფოების ძირითად ამოცანას თვითგადარჩენისა და თვითდამკვიდრებისთვის ბრძოლა წარმოადგენს, ისინი ზრუნავენ უსაფრთხოებასა და დამოუკიდებლობაზე. ხშირად სახელმწიფოები ერთიანდებიან, რათა დაუპირისპირდნენ იმ სახელმწიფოს, ან სახელმწიფოთა ჯგუფს, რომელიც საფრთხეს წარმოადგენს. გამოდის, საერთაშორისო სისტემა, ვუწოდოთ თანამშრომლობა, დაყოფილია სახელმწიფოთა რამდენიმე ჯგუფად, რაც განსაზღვრავს მათთვის მშვიდობას. თანამედროვე ეპოქაში კიბერშესაძლებლობების ასიმეტრიული გამოყენების მაღალმა შესაძლებლობამ დასაშვები გახადა პატარა ქვეყნების მიერ ზეგავლენის მოხდენა მსოფლიოში მიმდინარე პროლიტიკურ პროცესებზე. მიუხედავად ამისა, საერთო ტენდენცია აჩვენებს, რომ ძალაუფლება მაინც დიდი და ძლიერი ქვეყნების ხელთაა. მას შემდეგ, რაც კიბერომი საერთაშორისო პოლიტიკის სტანდარტულ იარაღად იქცა, შეგვიძლია ვთქვათ, თანამედროვე ტექნოლოგიებმა გარკვეულწილად შეცვალა გლობალური უსაფრთხოების მიდგომები. ამ საკითხთან დაკავშირებით მნიშველოვანია, **განვსაზღვროთ ძალთა ბალანსის კონცეფცია** და კიბერტექნოლოგიების გაძლიერების პირობები, რაც გულისხმობს სახელმწიფოთა კიბერშესაძლებლობებს, განვითარებას და დაბალანსებას. აქ იგულისხმება არა მხოლოდ ერთი სახელმწიფოს გაძლიერება თუ გაბატონება კიბერტექნოლოგიების თვალსაზრისით, არამედ თანამშრომლობის სხვადასხვა ეტაპები.

ჩვენ ამ ქვეთავს ვუთმობთ თანამედროვე მაღალი ტექნოლოგიების გავლენის ანალიზს, საერთაშორისო უსაფრთხოების პროცესებზე. აღნიშნულია, რომ ტექნოლოგიებისა და ინტერნეტის განვითარებამ ზეგავლენა მოახდინა საერთაშორისო უსაფრთხოების პროცესებზე. განხილულია კიბერსივრცეში ძალთა ბალანსის, ანუ ძალთა წონასწორობის მეთოდოლოგიის ფარგლებში. მოყვანილია

უამრავი მაგალითი, როგორც რუსეთის კიბერტექნოლოგიურ შესაძლებლობებზე, ასევე აშშ-ის, ჩინეთის, ირანის ისლამური სახალიფოს. განხილულია სხვადასხვა არჩევნებში, მათ შორის აშშ-ის 2016 წლის საპრეზიდენტო არჩევნებში რუსეთის ჰაკერების ჩარევის მცდელობა, ასევე ჩინეთის კიბერთავდასხმების მაგალითები, რასაც საერთაშორისო პოლიტიკურ დონეზე დიდი მნიშვნელობა ენიჭება და ძალთა ბალანსის საკითხში მნიშვნელოვან ელემენტს წარმოადგენს.

2.3. კიბერომის ფენომენის ასახვა ეროვნული უსაფრთხოების სტრატეგიებში: მითი და რეალობა

ეროვნული უსაფრთხოების სტრატეგია უმნიშვნელოვანეს დოკუმენტს წარმოადგენს სახელმწიფოს უსაფრთხო გარემოს შექმნისთვის. მსოფლიოში წამყვანი სახელმწიფოების უსაფრთხოების სტრატეგიებში კიბერომს მნიშვნელოვანი ადგილი უკავია - მაგალითად აშშ-ის, დიდი ბრიტანეთის, რუსეთის, ჩინეთის, ირანის, საფრანგეთის, ესპანეთის და ა.შ. საქართველოს ეროვნული უსაფრთხოების სტრატეგიაშიც აღნიშნული საკითხი მნიშვნელოვან ადგილს იკავებს. ასევე ყურადღება უნდა გავამახვილოთ **ნატო-ევროკავშირის** უსაფრთხოების სტრატეგიებზეც. თუმცა მნიშვნელოვანია, განვიხილოთ აგრესორი ქვეყნის უსაფრთხოების სტრატეგია. საინტერესოა, როგორია რუსეთის ხელისუფლების ხედვა გლობალური საფრთხეების კუთხით. ამ ქვეთავში საუბარია კიბერომის ფენომენის ასახვაზე ეროვნულ სტრატეგიებში, ნატო-ევროკავშირის კიბერუსაფრთხოების სტრატეგიებზე, რუსეთის სახელმწიფო უსაფრთხოების სტრატეგიაში განსაზღვრულ საფრთხეებზე, აშშ-ის უსაფრთხოების სტრატეგიასა და კიბერტექნოლოგიების მნიშვნელობაზე. გაანალიზებულია რიჩარდ კოენის „კოლექტიური თავდაცვის“ მეთოდოლოგიის მიხედვით წარმოებული კიბერპოლიტიკა. განხილულია სხვადასხვა ისტორიული ასპექტები, ასევე საქართველოსთან მიმართებაში. მოყვანილია კიბერუსაფრთხოების გლობალური ინდექსის მონაცემები, გაანალიზებულია კიბერომი ევროკავშირის სივრცეში -

მაგალითი რეკორდული სიძლიერის კიბერშეტევაზე და თავდაცვით კომპანიაზე, რომელიც გაუმკლავდა აღნიშნულ თავდასხმას. განხილულია ანტივირუსული კომპანიები, რომლებიც თავდაცვით მექანიზმს წარმოადგენენ კომპიუტერულ სისტემებთან და პროგრამებთან დაკავშირებით.

თავი მესამე - პოლიტიკური კონფლიქტის ახალი იდენტიფიკაცია და ასიმეტრიული საფრთხის ფენომენი კიბერომის მაგალითზე

<u>მოცემული თავი შედგება 3 ქვეთავისგან.</u>

ტექნოლოგიების განვითარება ყოველთვის აისახება და გავლენას ახდენს საზოგადოებაზე. ჩვენ ვერ გაუმკლავდებით ტექნოლოგიურ გამოწვევებს ადამიანის ბუნების გათვალისწინების გარეშე, ხოლო ადამიანის ბუნების ექსპერტები არიან ქცევითი მეცნიერები ანუ ბიჰევიორისტები. ბიჰევიორიზმის თეორიის გაჩენა უკავშირდება (1913 წ.) **ჯონ უოტსონის** დეკლარაციებს, რომელიც თავმოყრილი იყო მის სტატიაში - **"ფსიქოლოგია ბიჰევიორისტის თვალსაზრისით".**

ბიჰევიორისტები სწავლობენ ადამიანის ინდივიდუალურ და საზოგადოებრივ ქცევას. ჩვენ ამ თეორიას განვიხილავთ კიბერუსაფრთხოების ჭრილში. მეთოდოლოგია დამკვიდრებულია სხვადასხვა წამყვან ქვეყნებში. შეიძლება უცნაური იყოს, ასეთ ტექნიკურ მხარეს, როგორიც კიბერსამყაროა, როგორ უნდა უკავშირდებოდეს ბიჰევიორიზმი? კიბერუსაფრთხოების სპეციალისტი **ბრიუს შნაიერი** ამბობს, რომ მხოლოდ მოყვარულები უტევენ მანქანებს, პროფესიონალები მიზანში იღებენ ადამიანებს. მაგალითად, ჰაკერების ერთ-ერთი თავდასხმის ტექნიკა, რომელსაც **"ფიშინგი"** წარმოადგენს, ამ შეტევის დროს თავდამსხმელი ცდილობს, კომპიუტერულ სისტემაში შეაღწიოს, ამ დროს უპირველეს სამიზნეს წარმოადგენს მომხმარებელი და არა ავტომატიზებული დაცვის მექანიზმის გატეხვა.

ამ თავში ანალიზი ეყრდნობა ბიჰევიორიზმის მეთოდოლოგიას, რომელიც მნიშვნელოვან ადგილს იკავებს კიბერუსაფრთხოების თვალსაზრისით. მოცემულია არა მხოლოდ ჩვენს მიერ ბიჰევიორიზმის მეთოდოლოოგიით გაანალიზებული კიბერომი, კიბერშეტევა და კიბერუსაფრთხოება, არამედ ამ მეთოდოლოგიით მომუშავე აშშ-ის არმიის მაგალითი. გამოყოფილია კიბერსივრცის ოთხი ფენა. გაანალიზებულია Covid-19 -ით გამოწვეული საფრთხეები კიბერსივრცეში, ჰაკერების მაღალი აქტივობა და მანიპულაციები ვირუსთან დაკავშირებით. დაფიქსირებულია აქტიურად მომუშავე ჰაკერული ჯგუფის მონაცემები. გამოყენებულია კიბერუსაფრთხოების ექსპერტის, ლუკას ოლეჯინიკის მოსაზრებები. გაანალიზებულია, თუ რა გამოიწვია Covid-19-მა კიბეშეტევების, საინფორმაციო ომის, დეზინფორმაცია-პროპაგანდის მიმართულებებით, **Znet**-ის მიერ გამოქვეყნებული სტატია, რომელიც ეხება საქართველოს მოქალაქეების პერსონალური მონაცემების გასაჯაროვებას. შესწავლილია **ციფრული ვალუტის** მნიშვნელობა, მისი შექმნის მოკლე ისტორია და არსი. ირანის ისლამური რესპუბლიკის შემთხვევის გარჩევა - შესაძლებლობები და კიბერუსაფრთხოების სისტემები.

3.1. კიბერუსაფრთხოების პოლიტიკა და სამოქალაქო კიბერომის ფენომენი

სამოქალაქო კიბერომი - ეს არის ახალი ტერმინი, რომელიც შეიცავს საინფორმაციო ომის ელემენტებს და წარმოადგენს მეტად საშიშ მოვლენას არა მხოლოდ საქართველოში, არამედ მთელ მსოფლიოში. გადადის რა პოლიტიკური პროცესები და ელექტრონული მედია უახლეს ტექნოლოგიებზე, დღითიდღე ძლიერდება საფრთხეც. კიბერუსაფრთხოების პოლიტიკა, სამოქალაქო თვალსაზრისით, საჭიროებს მუდმივ განახლებას, დახვეწას და ეფექტური პროგრამების შემუშავებას. ასევე საზოგადოების სწორ, მიზანმიმართულ ინფორმირებას. საქართველოს მაგალითზე თუ ვიმსჯელებთ და მოვლენებს

გავაანალიზებთ, აშკარად დავინახავთ ფსიქოლოგიური ტერორის ნიშნებს სატელევიზიო მედიის მხრიდან.

ამ ქვეთავში წარმოდგენილია ჩვენს მიერ ჩატარებული კვლევა, დისკურს-ანალიზი - „მთავარი არხი“, „ფორმულა“, „ტვ პირველი“, რომლებიც წარმოადგენენ პოლიტიკურად მოტივირებულ ერთ მხარეს. გადაცემებში იგრძნობა სიძულვილის ენა, თითქმის უწყვეტად ვრცელდება დეზინფორმაცია. მეორე მხარეს არის **„იმედი“** და **„პოსტვ“.** ეს ტელევიზიები ცდილობენ განეიტრალებას, ანუ დაბალანსებას, მაგრამ ესენიც წარმოადგენენ მხარეს. მოცემული გვაქვს ამ ტელეკომპანიების გადაცემების განხილვა, დისკურს-ანალიზი და აქედან გამომდინარე, პოლიტიკურ ლექსიკონში შემოგვაქვს ახალი ტერმინი - **„სამოქალაქო კიბერომი“.**

3.2. ასიმეტრიული საფრთხეები და ჯიჰადისტების კიბერომი

ჩვენ ვსაუბრობთ კიბერომებზე, კიბერშეტევებზე, საინფორმაციო ომზე, პროპაგანდაზე, დეზინფორმაციაზე, ფეიკნიუსებზე და ზოგადად ჰიბრიდულ ომებზე, ტექნოლოგიების დადებით და უარყოფით მხარეებზე. რეალურად უნდა განვმარტოთ თუ ვის ხელში წარმოადგენს ტექნოლოგიური წინსვლა იარაღს და საფრთხეს. აქ მხოლოდ აგრესორ ქვეყნებზე კი არა, საუბარია არასახელმწიფოებრივ აქტორებზეც, რომლებიც კარგად ითვისებენ ახალ ტექნოლოგიებს. ტერორიზმს გააჩნია დიდი ისტორია და მისი უამრავი დეფინიცია არსებობს, ასევეა კიბერტერორიზმთან დაკავშირებით და ეს განმარტება უფრო სარწმუნოა: კიბერტერორიზმი ნიშნავს კომპიუტერული და სატელეკომუნიკაციო ტექნოლოგიების, მათ შორის ინტერნეტის გამოყენებას ძალადობრივი ქმედებების შესასრულებლად, რომელიც საფრთხეს უქმნის სიცოცხლეს ან იწვევს სიკვდილს. კიბერტერორისტული აქტები მიზნად ისახავს პოლიტიკური ან იდეოლოგიური უპირატესობების მიღწევას დაშინებისა და მუქარის საშუალებით. ტერმინი კიბერტერორიზმი პირველად გამოიყენეს 1980-იან წლებში. ზოგჯერ კიბერტერორიზმში მოიაზრებენ, როგორც კომპიუტერული ქსელების განძრახ დაზიანებას სხვადასხვა

საშუალებებით, მაგალითად, ვირუსების, ფიშინგის წარმოებით და სხვა მავნე პროგრამებით. ამ ქვეთავში გაანალიზებულია, თუ ვის ხელში იქცევა ტექნოლოგიური წინსვლა საშიშ აიარაღად. ტერორისტული ორგანიზაცია **„ისლამური სახალიფოს“** (**„დაეში“**) და მასთან დაკავშირებული დაჯგუფებების ტერორისტული მოქმედებები. მოყვანილია მაგალითები, თუ როგორ იყენებენ კიბერტექნოლოგიებს კიბერტერორიზმის წარმოებისთვის. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიშის საფუძველზე მოცემულია მაღალი ტერორისული საფრთხეები. უსაფრთხოების ექსპერტის, პროფესორ ვახტანგ მაისაიას კვლევებზე დაყრდნობით, ამ ქვეთავში კიბერტერორიზმთან დაკავშირებით მოყვანილია ინფორმაცია, რომელმაც მოგვცა ტერორიზმისა და კიბერტერორიზმის სიღრმისეული ანალიზის გაკეთების საშუალება.

3.3. პოლიტიკური კონფლიქტის ახალი მოდელი და 2008 წლის რუსეთ-საქართველოს კიბერომის ფაქტორი

2008 წლის აგვისტოში რუსეთმა საქართველოს წინააღმდეგ აგრესია ორ ფრონტზე განახორციელა - იყო რეალური სამხედრო თავდასხმა და იყო ირეალური, ანუ ვირტუალური თავდასხმა ინტერნეტსივრცეში. სანამ რეალური ომი დაიწყებოდა, რუსმა ჰაკერებმა ორკესტირებულად შეუტიეს სახელმწიფო უწყებების ვებ-გვერდებს. ოფიციალური ინფორმაციის თანახმად, კიბერთავდასხმა მოხდა 60-მდე ვებ-გვერდზე. უმეტეს მათგანზე გაჩნდა პროპაგანდისტული მოწოდებები, ფოტოები, სადაც ყოფილი პრეზიდენტი მიხეილ სააკაშვილი ადოლფ ჰიტლერთან იყო გაიგივებული. აღნიშნულ ქვეთავში გაანალიზებულია რუსეთ-საქართველოს 2008 წლის კიბერომი და რუსეთიდან მომდინარე კიბერსაფრთხეები.

სიღრმისეული ინტერვიუები ექსპერტებთან - წარმოდგენილია უსაფრთხოების ექსპერტებისა და სოციოლოგის სიღრმისეული ინტერვიუები, რომლებიც ეხება კიბერსივრცეს, კიბერტექნოლოგიებს, კიბერომს, კიბერშეტევებს,

კიბერუსაფრთხოებას. შერჩეული ექსპერტების ჩამონათვალი: **ამირან სალუქვაძე, ნიკა ჩიტაძე, ლევან ნიკოლეიშვილი, ანდრო გოცირიძე, ზურაბ ბიგვავა.**

ყველა ექსპერტი თანხმდება იმაზე, როგორც მსოფლიოსთვის, ისე საქართველოსთვის კიბერომი, კიბერთავდასხმები, საინფორმაციო ომი და ე.წ. ფეიკ-ნიუსი, როგორც მოვლენა, დიდი საფრთხეა. მათი აზრით, კიბერომის შეჩერება და ლიკვიდაცია ტექნოლოგიური მიღწევებით შეუძლებელია, მაგრამ თავდაცვა - აუცილებელი. საჭიროა, საქართველო მოერგოს საერთაშორისო სტანდარტებს, გაიზიაროს რეკომენდაციები და სამოქმედო გეგმა დასახოს ეროვნული უსაფრთხოების დონეზე. შესასწავლია, კონკრეტულად რის მიღწევა სურს რუსეთს პოსტსაბჭოთა ქვეყნებსა თუ ევროპაში. თუ არ იცი მტრის ენა, ვერ შეიმუშავებ ეფექტურ თავდაცვით პროგრამას, ამიტომ უნდა გაიაზრონ სახელმწიფო თუ არასახელმწიფო უწყებებმა 2008 წლის ომის პერიოდში განხორციელებული კიბერშეტევის დეტალები.

საქართველოს კიბერუსაფრთხოების თავდაცვის ეროვნული დოქტრინა

(ავტორისეული პროექტი)

ზოგადი სქემა

I ნაწილი

საქართველოს კიბერუსაფრთხოების თავდაცვის

ეროვნული დოქტრინის ძირითადი ფაქტორები

1) შესავალი;
2) კიბერუსაფრთხოების ძირითადი პრინციპები;
3) კიბერსივრცისგან მომდინარე, საფრთხეები და გამოწვევები;
4) კიბერომიდან მომდინარე საფრთხეების კლასიფიკაცია;
5) კიბერომი შიდა და გარე დონეზე საფრთხეების ფაქტორები;
6) კიბერუსაფრთხოების უზრუნველყოფა მსოფლიოსა და საქართველოს მასშტაბით;
7) ინტერნეტსივრცის დაცვა და კონტროლი;
8) ინტერნეტსივრცის უსაფრთხოება და კიბერდანაშაულის სამართლებრივი ასპექტები;
9) სოციალური ქსელები, სოციალური მედია და სახელმწიფო პოლიტიკა.

II ნაწილი

საქართველოს როლი გლობალური კიბერუსაფრთხოების სისტემაში

2.1. საქართველოს მიდგომები და მექანიზმები კიბერუსაფრთხოების საქმეში;

2.2. საქართველოს თანამშრომლობა სტრატეგიულ პარტნიორებთან კიბერუსაფრთხოების საკითხებში;

2.3. თანამშრომლობა საერთაშორისო ორგანიზაციებთან კიბერუსაფრთხოების საკითხებში;

2.4. თანამშრომლობა პოსტსაბჭოთა ქვეყნებთან კიბერუსაფრთხოების კუთხით;

III ნაწილი
კიბერსივრცისგან მომდინარე საფრთხეები და საქართველოს პოლიტიკა

3.1. საქართველოს სამხედრო თავდაცვითი მდგომარეობის ანალიზი კიბერუსაფრთხოების კონტექსტში;
3.2. შიდა სისტემური უსაფრთხოების მექანიზმები კიბერ სივრცისგან მომდინარე საფრთხეებზე რეაგირების კუთხით;
3.3. ბრძოლა კიბერ ტერორიზმის წინააღმდეგ და სტრატეგია;
3.4. სახლმწიფო დონეზე კიბერ საფრთხეებზე რეაგირების მექანიზმები;
3.5. კიბერ დაზვერვა და ეროვნული უსაფრთხოება;
3.6. სამოქალაქო კიბერუსაფრთხოება და ინფრასტრუქტურის დაცვა;
3.7. კიბერ საფრთხეებზე რეაგირების და კონტროლის ჯგუფების შექმნა.

დასკვნა

კიბერუსაფრთხოების უზრუნველყოფა შედარებით ახალი დარგია თანამედროვე სამყაროში. გლობალური თვალსაზრისით, მსოფლიოში არსებობს სამართლებრივი ბაზისა და საერთაშორისო სტანდარტების ნაკლებობის პრობლემა, რაც გლობალიზაციისა და თანამედროვე მსოფლიო წესრიგის გათვალისწინებით, ართულებს რეგიონული და ეროვნული კიბერუსაფრთხოების სტრატეგიის ჩამოყალიბების პროცესს. ამის მიუხედავად, კიბერუსაფრთხოების უზრუნველყოფის მექანიზმები დიდწილად დამოკიდებულია ცალკეული ქვეყნის გამოცდილებაზე, ყოველ შემთხვევაში, ამ საკითხთე კავკასიის რეგიონული უსაფრთხოების, პოსტსაბჭოთა სივრცისა და საქართველოს მაგალითები ასეთ სურათს გვიჩვენებს. რაც შეეხება ნატოსა და ევროკავშირში გაწევრიანებულ სახელმწიფოებს, ასევე ცალკეულ ქვეყნებს, რომელთაც გააჩნიათ და ხარჯავენ დიდ ფინანსებს ამ მიმართულებით, არაერთი ფაქტი ადასტურებს, რომ არც ეს ზონაა ბოლომდე დაცული.

<u>ნაშრომში დასმულ საკვლევ კითხვებზე გაცემულია შემდეგი პასუხები:</u>

1) **რამდენად შეიძლება კიბერომის აღქმა პოლიტიკური კონფლიქტების ახალ რეალობად?**

კიბერომი ნამდვილად არის პოლიტიკური კონფლიქტების ახალი რეალობა. ეს რომ ასეა, მსოფლიოში მიმდინარე პოლიტიკურმა მოვლენებმაც აჩვენა - უკვე არაერთი სახელმწიფოს საშინაო საქმეებში ჩაერივნენ დაინტერესებული სახელმწიფოები, მეტწილად საარჩევნო პროცესებში. რუსეთი კიბერსივრცეში გააქტიურებით ცდილობს, პოლიტიკური გავლენა მოიპოვოს როგორც აღმოსავლეთ ევროპის სახელმწიფოებზე, ისე პოსტსაბჭოთა ქვეყნებზე. ირანის ისლამური სახალიფოც კი, რომელიც არ არის მსოფლიოში მნიშვნელოვანი პოლიტიკური მოთამაშე, ცდილობს, ჩაერიოს ამერიკის შეერთებული შტატების საპრეზიტენტო არჩევნებში. ამის თაობაზე არაერთხელ განაცხადეს თეთრ სახლში.

2) **რა გავლენა შეიძლება იქონიოს საერთაშორისო საზოგადოებაზე კიბერომმა?**

შესაძლებელია, საერთაშორისო საზოგადოებაზე კიბერომმა იქონიოს დამანგრეველი გავლენა - ნუ გამოვრიცხავთ, მოიშალოს სახელმწიფოებისა და საზოგადოების ნორმალური ფუნქციონირება. კიბერდანაშაული კატასტროფულად აისახება ირეალურიდან რეალურ სივრცეში, დაზარალდება ბიზნესი, ეკონომიკა, თითქმის ყველა წამყვანი დარგი, გააქტიურდებიან ტერორისტული ორგანიზაციები, ჩაიშლება სადაზვერვო ოპერაციები, საფრთხე დაემუქრება უამრავი ადამიანის სიცოცხლესა და ჯანმრთელობას, ფინანსურ უსაფრთხოებას, კერძო საკუთრების უფლებას.

3) **როგორია სამოქმედო გეგმა და სამხედრო სტრატეგიის შემადგენელი ნაწილები კიბერომის პირობებში?**

კიბერომის პირობებში სამოქმედო გეგმა და სამხედრო სტრატეგიის შემადგენელი ნაწილები უნდა ხორციელდებოდეს წინასწარ გაწერილი დეტალების მიხედვით. სამოქმედო გეგმის შესრულებას ხელმძღვანელობენ სპეციალური უწყებები, ამ შემთხვევაში მთავარ უწყებას საერთაშორისო მასშტაბით წარმოადგენს ნატო, ხოლო საქართველოს მასშტაბით სახელმწიფო უსაფრთხოების სამსახური და თავდაცვის სამინისტროს დაქვემდებარებაში მყოფი კიბერუსაფრთხოების ბიურო.

4) **რა მნიშვნელობა ენიჭებათ კიბერუსაფრთხოების უზრუნველყოფის საკითხებში საქართველოს სტრატეგიულ პარტნიორებს?**

კიბერუსაფრთხოების უზრუნველყოფის საკითხებში საქართველოს სტრატეგიულ პარტნიორებს - ევროკავშირს, ნატოს, ამერიკის შეერთებულ შტატებს დიდი მნიშვნელობა ენიჭებათ. ვინაიდან, კიბერინციდენტები არის ტრანსნაციონალური ხასიათის, კიბერუსაფრთხოების დაცვა და უზრუნველყოფა შეუძლებელია მხოლოდ საკუთარი ძალებით. საფრთხეების აღკვეთა-შემცირების პროცესში აუცილებელია თანამშრომლობა საერთაშორისო

დონეზე. კიბერინციდენტებზე ეფექტური რეაგირების მიზნით, შესაძლოა, მონაცემები ინახებოდეს სხვადასხვა სახელმწიფოების ტერიტორიაზე, რაც წარმოადგენს მოწყვლად ინფორმაციას. ინფორმაციის დროული მოპოვება შეუძლებელია ეფექტიანი საერთაშორისო თანამშრომლობის გარეშე. მიუხედავად იმისა, რომ საქართველოს კიბერუსაფრთხოების სფეროში აქვს პროგრესი, მაინც დიდი მნიშვნელობა ენიჭება ნატოსა და ევროკავშირის კიბერუსაფრთხოების სტრატეგიას, ასევე გამოცდილებას. 2014 წლის შეთანხმების თანახმად, კიბერთავდაცვა იქცა კოლექტიური თანამშრომლობის განუყოფელ ნაწილად, საქართველოს მხრიდან კი ამ სისტებაში ჩართვა მიზნად ისახავს ალიანსის ოპერაციების მხარდაჭერას.

კიბერომი, კიბერშეტევა, ვირტუალური საფრთხეები, საინფორმაციო ომი, ინტერნეტჯაშუშობა, ასიმეტრიული საფრთხეები, კიბერტერორიზმი და კიბერუსაფრთხოება - ეს გახლავთ ნაშრომის ძირითადი კვლევის საგანი და შინაარსი. ასევე, კვლევის საგანია, თუ რა სერიოზული პრობლემებისა და საფრთხის წინაშე დგას ცივილიზებული სამყარო, რა სიკეთე მოაქვს ტექნოლოგიების განვითარებას და ამავე დროს, რა გამოწვევები ჩნდება ყოველდღიურად. სხვადასხვა ქვეყნების შესაძლებლობები კიბერტექნოლოგიების თვალსაზრისით, მაგალითად: აშშ-ის, რუსეთის, ირანის ისლამური სახალიფოს, ჩინეთის და ასე შემდეგ. ასევე, ნაშრომში დიდი ადგილი ეთმობა იმის გაანალიზებას, კიბერტექნოლოგიების თვალსაზრისით რა შესაძლებლობები აქვს საქართველოს და როგორ შეიძლება პატარა სახელმწიფოებმა თავი დაიცვან. აღსანიშნავია, რომ სტაბილურობის ერთადერთი გარანტი არის დასავლური კურსი, გაწევრიანება ნატოსა და ევროკავშირში. ამ ორგანიზაციებს გააჩნიათ ყველაზე დიდი და ეფექტური თავდაცვითი მექანიზმები თუ შესაძლებლობები. საქართველო ამ კუთხით სწორ გზას ადგას. თუმცა ჯერ კიდევ ბევრი მუშაობა და ფინანსებია საჭირო, რათა გახდეს დასავლური სამყაროს სრულფასოვანი წევრი.

ნაშრომში წარმოდგენილი ჰიპოთეზა დადასტურებულია ჩატარებული კვლევის შედეგად. ნაშრომში ჩამოყალიბებული ჰიპოთეზა ასე განისაზღვრა: გლობალურ უსაფრთხოებაში პოლიტიკური კონფლიქტების ახალი განზომილება ერთ-ერთი მნიშვნელოვანი და საკვანძო საკითხია. კიბერომი მნიშვნელოვან გავლენას ახდენს საერთაშორისო უსაფრთხოების პროცესების მიმდინარეობასა და შედეგებზე.

კვლევების შედეგად ვადასტურებთ, რომ ტექნოლოგიების განვითარებამ ისეთ მნიშვნელოვან სივრცეს, როგორიც არის ინტერნეტი, ხელი შეუწყო კიბერომებისა და კიბერშეტევების წარმოებას, რამაც საფრთხე შეუქმნა როგორც ეროვნულ, ასევე საერთაშორისო უსაფრთხოებას. ნაშრომში უამრავი მაგალითია, თუ რატომ და როგორ განსაზღვრავს კიბერტექნოლოგიები საერთაშორისო უსაფრთხოების პროცესების მიმდინარეობას, რა ზეგავლენას ახდენს ამ პროცესების შედეგებზე. საფუძველზე განვსაზღვრავთ, რომ რაც უფრო დიდი კიბერტექნოლოგიური შესაძლებლობები აქვს ამა თუ იმ ქვეყანას, მით უფრო მძლავრ მოთამაშეს წარმოადგენს საერთაშორისო პოლიტიკაში. სადისერტაციო ნაშრომში, ფაქტებზე დაყრდნობით, განვიხილეთ, გამოვიკვლიეთ და გავაანალიზეთ კიბერომის ფენომენი, რომელიც შესაძლოა, უფრო საშიში აღმოჩნდეს კაცობრიობისთვის, ვიდრე იყო მე-20 საუკუნის მეორე ნახევარში გაჩაღებული „ცივი ომი“ და დაპირისპირება ორ ბანაკს შორის. იქიდან გამომდინარე, რომ კიბერომი ყველა კონვენციური ომის თანმდევი პროცესია, რაც ნაშრომშია ასახული და გაანალიზებული, შეგვიძლია დავასკვნათ, რომ მსოფლიო დგას დიდი საშიშროების წინაშე.

ნაშრომის მიზანია, როგორც კიბერომისა და ვირტუალური საფრთხეების წარმოჩენა, ასევე იმ გზებისა თუ მექანიზმების შექმუშავება-განსაზღვრა, რაც გულისხმობს კიბეუსაფრთხოებას, რაც განისაზღვრა, წარმოჩინდა როგორც ნაშრომის თავებსა და ქვეთავებში, ასევე რეკომენდაციების სახით დანართებში.

<u>რეკომენდაციები:</u>

- უნდა მომზადდეს სათანადო კადრები და შესაბამის სახელმწიფო სტრუქტურებში დასაქმდნენ კერძო სექტორში მომუშავე პროფესიონალები.

  ხშირად სახელმწიფო სტრუქტურებში მომუშავე ადამიანთა მომზადების დონე ვერ უძლებს კრიტიკას.

- შესამუშავებელია ეროვნული უსაფრთხოების ახალი სტრატეგია, დასახვეწია კონცეფცია, რომლებიც ძირითადად გაჯერებულია ზოგადი, მაღალფარდოვანი ფრაზებით. გასაძლიერებელია საკანონმდებლო ბაზა.

- მსოფლიო მასშტაბით უნდა შეიქმნას კიბერსაწინააღმდეგო სპეციალური, გლობალური ორგანიზაცია, სადაც დაისახება სამომავლო გეგმები. შესაძლებელია, ეს ორგანიზაცია იყოს სრულიად გასაიდუმლოებული. მსგავსი სტრუქტურები უნდა ჩამოყალიბდეს ეროვნულ დონეებზეც, მათ შორის საქართველოშიც.

- სკოლებში დაწყებითი კლასებიდანვე უნდა ისწავლებოდეს კომპიუტერული სისტემები სხვადასხვა დონეებზე. შესადგენია სპეციალური სახელმძღვანელო, სადაც მარტივად იქნება ახსნილი ყველა საჭირო დეტალი - კიბერთავდასხმები, მოგერიება, ვირუსები, თავდაცვა, ისტორია, დღევანდელი მდგომარეობა, საინფორმაციო ომი და ასე შემდეგ. ასეთივე მიდგომაა საჭირო პროფესიულ და უმაღლეს სასწავლებლებში.

- გასაძლიერებელია ბრძოლა ე.წ. ბოტების, ფეიკ-ნიუსერებისა თუ სხვა პროპაგანდისტული თაღლითების წინააღმდეგ. ასევე უნდა გაძლიერდეს ტექნიკური მხარე, რათა რუსეთიდან თუ სხვა ქვეყნებიდან მომდინარე საფრთხეები თავიდან იქნას აცილებული.

დისერტანტის აკადემიური გამოცდილება სამეცნიერო ნაშრომები და პუბლიკაციები

სადისერტაციო ნაშრომის ძირითადი შედეგები წარმატებითაა დაცული კავკასიის საერთაშორისო უნივერსიტეტში თეორიულ-ემპირიული კვლევების და თემატური სემინარების ფარგლებში.

კავკასიის საერთაშორისო უნივერსიტეტის სოციალურ მეცნიერებათა ფაკულტეტის საგამოცდო კომისიაში, დაცულ იქნა სამი კოლოკვიუმი და ერთი სემინარი.

სამი კოლოკვიუმი (თითოეული არის სადისერტაციო ნაშრომის ნაწილი)

1) კოლოკვიუმი №1 – „კიბერომის არსი და ისტორიული მიმოხილვა“.
2) კოლოკვიუმი №2 – „კონფლიქტების ტრანსფორმაცია ახალი გეოპოლიტიკური წესრიგის პირობებში“
3) კოლოკვიუმი №3 – „პოლიტიკური კონფლიქტის ახალი იდენტიფიკაცია და ასიმეტრიული საფრთხის ფენომენი კიბერომის მაგალითზე“

თემატური სემინარი (ეძღვნება დარგის/ქვედარგის აქტუალურ საკითხს და არ წარმოადგენს სადისერტაციო თემის ნაწილს)

1) “ევროკავშირის გეოსტრატეგიული მიზნები სამხრეთ კავკასიაში”.

სადისერტაციო ნაშრომის ძირითადი შინაარსი გამოქვეყნებულია შემდეგ პუბლიკაციებში.

სტატიები:

1) „თანამედროვე საინფორმაციო ომის გეოპოლიტიკური კონტურები რუსეთ-აშშ-ის კონფრონტაციის ხაზი ბალტიის ზღვიდან შავ ზღვაში“, რეფერირებადი საერთაშორისო

სამეცნიერო ჟურნალი - ,,ANTE PORTAS Security Studies", № 13-ში. 2019 წ. (ინგლისურ ენაზე)

2) "კიბერომის ფენომენის ასახვა ეროვნული უსაფრთხოების სტრატეგიებში - მითი და რეალობა ამერიკის შეერთებული შტატების მაგალითზე", რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - ,,American Studies Periodical", შავი ზღვის საერთაშორისო უნივერსიტეტი, №12-ში. 2019 წ. (ინგლისურ ენაზე)
3) ,,კიბერ ომი, როგორც ასიმეტრიული საფრთხის ფენომენი და კიბერბირთვული უსაფრთხოების საფრთხეები", რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - ,,Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi", ჩერნოვეცის ეროვნული უნივერსიტეტი, N 40-ში. 2019 წ. (ინგლისურ ენაზე)
4) „კიბერომის კონცეფცია და 21-ე საუკუნის საერთაშორისო უსაფრთხოების სისტემა", კავკასიის საერთაშორისო უნივერსიტეტი. რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - „პოლიტო/ლოგოს". II გამოცემა. 2020 წ.

დოქტორანტი მონაწილეობდა სხვადასხვა სახის საერთაშორისო კონფერენციებში:

1) სახელმწიფო და კორპორაციული უსაფრთხოების სასწავლო-კვლევითი ცენტრი. სამეცნიერო პრაქტიკული კონფერენცია: „ეროვნული და კორპორაციული უსაფრთხოება". 2017 წ.
2) "ჰიბრიდული ომი და კიბერსაფრთხეები 21-ე საუკუნის ახალი კონფლიქტის ფორმა", მეექვსე საერთაშორისო სამეცნიერო კონფერენცია, კავკასიის საერთაშორისო უნივერსიტეტი, 2018 წ.
3) "21-ე საუკუნეში კიბერ და საინფორმაციო ომის საერთაშორისო უსაფრთხოება", მეშვიდე საერთაშორისო სამეცნიერო კონფერენცია, კავკასიის საერთაშორისო უნივერსიტეტი. 2019 წ.
4) "21-ე საუკუნის გამოწვევა - კიბერუსაფრთხოება და საინფორმაციო ომი", სტუდენტთა XI საერთაშორისო

სამეცნიერო კონფერენცია. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2019 წ.

5) სამეცნიერო კონფერენცია - „ეროვნული და კორპორაციული უსაფრთხოება“, ეროვნული და კორპორაციული უსაფრთხოების სასწავლო კვლევითი ცენტრი. 2019 წ.
6) "კიბერ ომი - როგორც ომის ახალი სახეობა და ევროკავშირის უსაფრთხოების სტრატეგია", სამეცნიერო კონფერენცია: „ევროკავშირის გაერთიანება - პრობლემები და პერსპექტივები“, საქართველოს საპატრიარქოს წმინდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტი. 2019წ.
7) “კიბერომის ფენომენის ასახვა ეროვნული უსაფრთხოების სტრატეგიებში - მითი და რეალობა ამერიკის შეერთებული შტატების მაგალითზე”, საერთაშორისო სამეცნიერო კონფერენცია - ,,American Studies International Conference“, შავი ზღვის საერთაშორისო უნივერსიტეტი, №12. 2019 წ.
8) "21-საუკუნის საერთაშორისო უსაფრთხოების სტრატეგიული თავდაცვითი მექანიზმები და კიბერშეტევების ტაქტიკა", მერვე საერთაშორისო კონფერენცია, კავკასიის საერთაშორისო უნივერსიტეტი. 2020 წ.

Caucasus International University
Faculty of Social Sciences
Doctoral Educational Program in Political Sciences

Right of Authorship

Thornike Zedelashvili

"Cyber War - A Modern Threat to National Security and a New Dimension of Political Conflict"

Abstract dissertation Presented for the degree of Doctor of Political Science

Tbilisi, 0142, Georgia
2020

Scientific work is done at the faculty of social sciences Doctoral Educational Program in Political Sciences.

Chief Supervisor: Vakhtang Maisaia
Doctor of political sciences
Caucasus International University Professor

Official reviewers: 1. Guguli Magradze
Doctor of Psychology,
Ivane Javakhishvili Tbilisi State University Professor

2. Zaza Tsotniashvili
Doctor of Journalism,
Professor at Caucasus International University

Defense of the thesis will take place on -------, 2020, ---- pm, in the Dissertation Council of the Caucasus International University Faculty of Social sciences

Address: 0141, Chargali Str. CIU, Building 1, Room 305
Read the thesis is possible in the library of the Caucasus international University

Secretary of the Dissertation Board
Petre Mamradze,
Associate Professor of the Caucasus international University

Annotation

The paper discusses the history of cyber warfare, its essence, basics and origins, the Internet and technological advances. As well as threats from cyber war, cyber-attacks, cyber defences of different countries, viruses, malware and hacker attacks, information warfare, propaganda, disinformation, fake news, security concepts and challenges. The main topic of the research is cyber war, as a process following the real conventional war, as well as an alternative version of the war. There are analysed global security, the role of the United States, Western Europe, Eastern Europe, the European Union and NATO, Georgia's geostrategic situation, security and cyber-attacks by Russia. Based on the research, the paper separates and explains different terms, focusing on the political term "civil cyber war" presented by discourse-analysis based on new circumstances. The article focuses on the hybrid wars, hacking attacks, information warfare waged by the Islamic Republic of Iran, China and Russia, as well as non-state actors, terrorists who rapidly master new technologies.

The paper presents its own opinions, recommendations (based on research), as well as analysis and recommendations developed by foreign or Georgian experts and specialists.

The dissertation contains three chapters (three subsections are given in each chapter), in-depth interviews with experts, discourse analysis, conclusion and recommendations.

Chapter One devotes to the creation and development of the computer, the creation of the Internet, the first connection, the history of the "web concept", the creation of the virus, the essence of cyber warfare, historical overview, the first stage of cyber-attacks and cyber wars.

The first subsection of the first chapter discusses the theoretical and practical aspects of cyber warfare, its place in modern world politics. Based on the fact that various experts argue about the definition of cyber warfare and there are frequent cases around the world when cyber warfare and cyber-attack are considered as one term, this section

discusses the difference between cyber war and cyber-attack. Three basic methods of cyber warfare and examples of cyber warfare are presented.

The second subsection of the first chapter analyses the historical aspects of the transformation of cyber warfare. Since the refinement and development of cyber warfare production methods is directly related to technology upgrades, this chapter analyses the forms of cyber-attacks and cyber warfare - what technologies have been and how they have become. Active and passive cyber-attacks are discussed. The most active types of cyber-attacks and malicious code attacks are presented. Based on the research, we identified three target groups of cyber-attacks. This chapter presents the financial data of the international research company "**Gartner**" on the development of cyber technologies in financial terms; also a report by **Cybersecurity Ventures**, where the losses from cyber-attacks by 2021 are counted. The focus is on the threats posed by Russia.

The third subsection of the first chapter discusses various theories of the concept of cyber warfare. The **Tallinn Manual**, developed under the auspices of the NATO Cooperative Cyber Defence Centre, discusses violations of cyber warfare under international law. Brief historical sections of NATO-EU on cyber security are presented. The focus is on the US attitude towards financial investment in terms of cyber technology development. US cyber security strategy, national security strategy, Russian information war doctrine are analysed. This subsection includes a quote from Dean Chang's book, **Cyber Dragon – China's Information Warfare and Cyber Operations**, which describes the development of China Information Warfare and cyber operations.

Chapter Two - In this chapter, based on the methodology of political realism, we discuss the transformation of conflicts in the context of the new geopolitical order and how important this methodology is in international cyber politics.

The first subsection of the second chapter - virtual threats are discussed where not only cyber-attacks and cyber wars are considered. Information, propaganda and disinformation manipulations, brief history and development in cyberspace are analysed. The focus is on fake news

and these issues are supported by various examples. It analyses how all this works in relation to Georgia and cites the 2016 NDI survey. In this subsection, our research presents the classification of cyberspace and discusses the **black market**, which is a major threat worldwide. From the book by **Kenneth Knapp**, a cyber-security specialist the information provided on "**Cyber Security and Global Information Assurance - Threat Analysis and Response Solutions**", published by the US Air Force Academy in Colorado, deals with the **black market** in cyberspace.

The second subsection of the second chapter is devoted to the analysis of the impact of modern high technologies on international security processes. It is noted that the development of technology and the Internet has had an impact on international security processes. It is discussed in the framework of the force balance method, or force balance methodology. Numerous examples are given of Russia's cyber-technological capabilities, as well as those of the United States, China, and the Islamic Republic of Iran. Attempts by Russian hackers to intervene in various elections, including the 2016 US presidential election, as well as examples of Chinese cyber-attacks, which are of great political importance internationally and an important element in the balance of power, are discussed.

The third subsection of the second chapter - this chapter discusses the phenomenon of cyber warfare in national strategies, NATO-EU cyber security strategies, the threats identified in the Russian state security strategy, the US security strategy and the importance of cyber technologies. Cyber politics based on Richard Cohen's "collective defence" methodology is analysed. Various historical aspects are discussed, as well as in relation to Georgia. The data of the Global Cyber Security Index are given, cyber war is analysed in the EU space - an example of a record-breaking cyber-attack and a defence company that dealt with this attack. Antivirus companies are considered as a defence mechanism against computer systems and programs.

Chapter Three - the analysis in this chapter is based on the methodology of behaviourism, which occupies an important place in terms of cyber

security. Not only is cyber war, cyber-attack, and cyber security analysed by our behaviourist methodology, but also the example of the US Army working on this methodology. Four layers of cyberspace are separated. The threats posed by Covid-19 in cyberspace, high activity of hackers and manipulations related to the virus are analysed. Data from an active hacker group has been recorded. The opinions of cyber security expert Lucas Olejnik are used. Here is an analysis of what Covid-19 has caused in the areas of hacking, information warfare, disinformation-propaganda, an article published by **Znet**, which deals with the disclosure of personal data of Georgian citizens. The importance of **digital currency**, its brief history and essence, as well as the case of the Islamic Republic of Iran - capabilities and cyber security systems are studied.

The first subsection of the third chapter presents our research, discourse-analysis of "Mtavari Arkhi", "Formula", "TV Pirveli", which represent a politically motivated one party. Hate speech is felt in the programs, misinformation is spread almost continuously. On the other side are **Imedi** and **Postv**. These TVs try to neutralize or balance, but they are also representing the side. We have given a review, discourse-analysis of the programs of these TV companies and the idea has arisen to introduce a new term in the political dictionary - "**Civil Cyber War**".

The second subsection of the third chapter is about asymmetric threats and jihadists cyber warfare, this chapter analyses in whose hands technological advancement is becoming a dangerous weapon; terrorist activities of the terrorist organization "**Islamic State" ("Daesh")** and its affiliated groups. Examples are given of how cyber technologies are used to produce cyber terrorism. According to the report of the State Security Service of Georgia, high terrorist threats are given. Based on the research of a security expert, Professor Vakhtang Maisaia, this subsection provides information on cyber terrorism, which allows us to conduct an in-depth analysis of terrorism and cyber terrorism.

The third subsection of the third chapter - this chapter analyses the 2008 Russia-Georgia cyber war and cyber threats from Russia.

In-depth interviews with experts - In-depth interviews with security experts and sociologists related to cyberspace, cyber technologies, cyber warfare, cyber-attacks and cyber security. There are list of selected experts: Amiran Salukvadze, Nika Chitadze, Levan Nikoleishvili, Andro Gotsiridze, Zurab Bigvava.