კავკასიის საერთაშორისო უნივერსიტეტის

თორნიკე ზედელაშვილი

კიბერომი - ეროვნული უსაფრთხოების თანამედროვე საფრთხე და პოლიტიკური კონფლიქტის ახალი განზომილება

სოციალურ მეცნიერებათა ფაკულტეტი

პოლიტიკის მეცნიერების სადოქტორო-საგანმანათლებლო პროგრამა

პოლიტიკის მეცნიერების დოქტორის

აკადემიური ხარისხის მოსაპოვებლად წარმოდგენილია

დისერტაცია

კავკასიის საერთაშორისო უნივერსიტეტი

თბილისი, 0141, საქართველო

2020

სოციალურ მეცნიერებათა ფაკულტეტი

ჩვენ, ხელისმომწერნი ვადასტურებთ, რომ გავეცანით **თორნიკე ზედელაშვილის** მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: "**კიბერომი - ეროვნული უსაფრთხოების თანამედროვე საფრთხე და პოლიტიკური კონფლიქტის ახალი განზომილება**" და ვაძლევთ რეკომენდაციას კავკასიის საერთაშორისო უნივერსიტეტის სოციალურ მეცნიერებათა ფაკულტეტში სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

„ ....." ..... 2020 წელი

ხელმძღვანელი: პოლიტიკის მეცნიერებათა დოქტორი, კავკასიის საერთაშორისო უნივერსიტეტის პროფესორი,

ვახტანგ მაისაია _____

რეცენზენტი:

……...

……..... _____

რეცენზენტი:

…….....

……..... _____

კავკასიის საერთაშორისო უნივერსიტეტი

2020 წელი

ავტორი: თორნიკე ზედელაშვილი

თემის დასახელება: “**კიბერომი - ეროვნული უსაფრთხოების თანამედროვე საფრთხე და პოლიტიკური კონფლიქტის ახალი განზომილება“**

ფაკულტეტი: სოციალურ მეცნიერებათა

აკადემიური ხარისხი: დოქტორი

სხდომა ჩატარდა: „ .....“ ..... 2020 წელი

ავტორის ხელმოწერა

ანოტაცია

ნაშრომში განხილულია კიბერომის ისტორია, მისი არსი, საფუძვლები და წარმომავლობა, ინტერნეტი და ტექნოლოგიური მიღწევები. ასევე კიბერომისგან, კიბერშეტევებისგან მომდინარე საფრთხეები, სხვადასხვა ქვეყნების თავდაცვითი კიბერშესაძლებლობები, ვირუსები, მავნე პროგრამები და ჰაკერული თავდასხმები, საინფორმაციო ომი, პორპაგანდა, დეზინფორმაცია, ფეიკ-ნიუსი, უსაფრთხოების კონცეფციები და არსებული გამოწვევები. კვლევის ძირითად საკითხს წარმოადგენს კიბერომი, როგორც რეალური კონვენციური ომის თანმდევი პროცესი და ასევე ომის ალტერნატიული ვარიანტი. გაანალიზებულია გლობალური უსაფრთხოება, ამერიკის შეერთებული შტატების, დასავლეთ ევროპის, აღმოსავლეთ ევროპის, ევროკავშირისა და ნატოს როლი. საქართველოს გეოსტრატეგიული მდგომარეობა, უსაფრთხოება და რუსეთის მიერ განხორციელებული კიბერთავდასხმები. კვლევის საფუძველზე ნაშრომში გამიჯნული და განმარტებულია სხვადასხვა ტერმინები, ყურადღება გამახვილებულია დისკურს-ანალიზით ახალი გარემოების საფუძველზე წარმოდგენილი პოლიტიკური ტერმინი „სამოქალაქო კიბერომი“. ნაშრომში ყურადღება ეთმობა ირანის ისლამური რესპუბლიკის, ჩინეთისა და რუსეთის მიერ წარმოებულ ჰიბრიდული ომებს, ჰაკერულ თავდასხმებს, საინფორმაციო ომის წარმოებას, ასევე არასახელმწიფო აქტორებს, ტერორისტებს, რომლებიც სწრაფად ითვისებენ ახალ ტექნოლოგიებს.

ნაშრომში წარმოდგენილია როგორც საკუთარი მოსაზრებები, რეკომენდაციები (კვლევებზე დაყრდნობით), ასევე უცხოელი თუ ქართველი ექსპერტებისა და სპეციალისტების მიერ შემუშავებული ანალიზი და რეკომენდაციები.

დისერტაცია შეიცავს სამ თავს (თითო თავში მოცემულია სამი ქვეთავი), სიღრმისეულ ინტერვიუებს ექსპერტებთან, დისკურს-ანალიზს, დასკვნას და რეკომენდაციებს.

თავი პურველი - ეთმობა კომპიუტერის შექმნას და განვითარებას, ინტერნეტის შექმნას, პირველ კავშირს, „ვების კონცეფციის“ ისტორიას, ვირუსის შექმნას, კიბერომის არსს, ისტორიულ მიმოხილვას, კიბერშეტევებისა და კიბერომების წარმოების პირველ ეტაპს.

პირველი თავის პირველი ქვეთავი - 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, ამ ქვეთავში განხილულია კიბერომისა და კიბერშეტევის განსხვავება. წარმოდგენილია კიბერომის წარმოების სამი ძირითადი მეთოდი და კიბერომის წარმოების მაგალითები.

პირველი თავის მეორე ქვეთავი - 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.

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

მეორე თავის პირველი ქვეთავი - 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.**

მეორე თავის მეორე ქვეთავი - ეთმობა 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.

მეორე თავის მესამე ქვეთავი - 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 - 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.

მესამე თავის პირველი ქვეთავი - 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“.**

მესამე თავის მეორე ქვეთავი - ასიმეტრიული საფრთხეები და ჯიჰადისტების კიბერომი, 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.

მესამე თავის მესამე ქვეთავი - აღნიშნულ ქვეთავში გაანალიზებულია რუსეთ-საქართველოს 2008 წლის კიბერომი და რუსეთიდან მომდინარე კიბერსაფრთხეები.

ნაშრომში შემუშავებულია ავტორისეული პროექტი - **„საქართველოს კიბერუსაფრთხოების თავდაცვის ეროვნული დოქტრინა“,** ზოგადი სქემის სახით.

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.**

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.

The paper develops an authorial project - **"Georgian National Doctrine of Cyber Security Defense"** in the form of a general section.

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.

სარჩევი

ცხრილებისა და დიაგრამების ნუსხა

ცხრილები:

დიაგრამები:

გამოყენებული აბრევიატურა

ENIAK - Electronic Numerical Integrator and Computer, ელექტრონული რიცხვითი ინტეგრატორი და კომპიუტერი

MITS - Micro Instrumentation and Telemetry Systems, მიკრო აპარატურები და ტელემეტრიული სისტემები

IBM - International Business Machines, საერთაშორისო ბიზნეს მანქანები

ARPANET - Advanced Research Projects Agency Network, მოწინავე კვლევითი პროექტების სააგენტოს ქსელი

WWW - World Wide Web, მსოფლიო მასშტაბის ქსელი

WIFI - Workforce Investment Field Instructions

DoS - Denial-of-Service, მომსახურების უარყოფა

RBN - Russian Business Network, რუსეთის ბიზნეს ქსელი

NASA - National Aeronautics and space Administration, ეროვნული აერონავტიკა და კოსმოსური ადმინისტრაცია

SCADA - Supervisory Control and Data Acquisition, საზედამხედველო კონტროლი და მონაცემთა შეძენა

DDoS - Distributed Denial-of-Service, განაწილებული მომსახურების უარყოფა

MitM - Man-in-the-middle, ადამიანი (თავდამსხმელი, ჰაკერი) რომელიც ახორციელებს კიბერშეტევას ორი ობიექტის მონაცემების გაცვლის დროს

ICT - Information and Communications Technology, ინფორმაციისა და საკომუნიკაციო ტექნოლოგია

ITU - International Telecommunication Union, საერთაშორისო სატელეკომუნიკაციო კავშირი

ICANN - The Internet Corporation for Assigned Names and Numbers, მინიჭებული სახელების და ციფრების ინტერნეტკორპორაცია

NDI - National Democratic Institute, ეროვნული დემოკრატიული ინსტიტუტი

HTB - რუსეთის ტელევიზია „ენტევე“

ORT - რუსეთის „პირველი არხი“

RTR - Russia 1, რუსეთის ტელევიზია “რუსეთი 1“

URL - Uniform Resource Locator, რესურსების ერთიანი ლოკატორი

IP - Internet Protocol, ინტერნეტ პროტოკოლი

CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub, ნატოს კოოპერატიული კიბერ თავდაცვის ცენტრი, რომელიც წარმოადგენს მრავალეროვნულ და ინტერდისციპლინარულ კიბერთავდაცვის ცენტრს

RAP - Readiness Action Plan - მზადყოფნის სამოქმედო გეგმა

KSN - Kaspersky Security Network - კასპერსკის უსაფრთხოების ქსელი

CtfTool - Computerized Transmission Function Tool, გადაცემის კომპიუტერიზებული ფუნქციის ინსტრუმენტი

GEOIP – Geographical Internet Protocol, გეოგრაფიული ინტერნეტ-ადგილმდებარეობა.

VMWARE (Virtual Machine) Workstation - ვირტუალური მანქანის სამუშაო სადგური

Covid-19 - Coronavirus Disease of 2019, კორონავირუსის 2019 წლის დაავადება

ZDNet - Ziff Davis Network, ზიფ დევისის ქსელი

P2P - peer-to-peer - თანატოლი (ტექნოლოგია რომელზეც შეიძლება იყოს პროგრამა აგებული)

BTC - Bitcoin, ბიტკოინი (ციფრული ვალუტის ერთეული)

ICA - Iran's Cyber Army, ირანის კიბერ არმია

Yandex - Yet Another Indexer, კიდევ ერთი ინდექსერი

ID - Identity Document, პირადობის დამადასტურებელი დოკუმენტი

5G - 5th Generation Wireless Systems, მე -5 თაობის უკაბელო სისტემები

CYSEC - Cyber Security Studies and Education Center, კიბერუსაფრთხოების სწავლებისა და განათლების ცენტრი

HMR - Hammersmith Medical Research Clinic, ჰამერსმიტის სამედიცინო კვლევების კლინიკა

GHC - GEORGIAN HACKERS COMMUNITY, საქართველოს ჰაკერების საზოგადოება

მადლიერების გვერდი

აღნიშნული დისერტაცია ვერ განხორციელდებოდა, რომ არა პედაგოგების, პროფესორების, ამ საქმის პროფესიონალების, სპეციალისტების, ცნობილი ანალიტიკოსების დახმარება და მხარდაჭერა. განსაკუთრებულ მადლობას ვუხდი ჩემს უშუალო ხელმძღვანელს, პოლიტიკის მეცნიერებათა დოქტორს, პროფესორ **ვახტანგ მაისაიას,** რომელსაც მნიშვნელოვანი წვლილი მიუძღვის სადოქტორო ნაშრომის შექმნაში. კვლევის პროცესში დახმარებისთვის ასევე განსაკუთრებულ მადლობას ვუხდი სადოქტორო პროგრამის ხელმძღვანელს, ასოცირებულ პროფესორ **თამარ კიკნაძეს,** კავკასიის საერთაშორისო უნივერსიტეტის სამეცნიერო კვლევების დეპარტამენტის უფროსის მოადგილეს **ნინო მინდიაშვილს.** მადლობა კავკასიის საერთაშორისო უნივერსიტეტის კანცლერს, **ვახტანგ წივწივაძეს.** კავკასიის საერთაშორისო უნივერსიტეტის რექტორს **კახაბერ კორძაიას,** კსუ-ის აკადემიურ ასისტენტს, პოლიტიკის მეცნიერებათა დოქტორანტს, ახალგაზრდა ექსპერტთა ასოციაციის თავმჯდომარეს, **ალიკა გუჩუას.** მადლობას ვუხდი ექსპერტებს: **ამირან სალუქვაძეს, ზურაბ ბიგვავას, ანდრო გოცირიძეს, ლევან ნიკოლეიშვილს, ნიკა ჩიტაძეს.** მადლობა სახელმწიფო და კორპორაციული უსაფრთხოების სასწავლო-კვლევით ცენტრს (დირექტორი **დავით კუხალაშვილი**), შავი ზღვის საერთაშორისო უნივერსიტეტს, მადლობა უკრაინის განათლებისა და მეცნიერების სამინისტროს, **იური ჩერნივის ეროვნულ უნივერსიტეტს**.

მადლობა **ოსტროვისკის "Świętokrzyski"-ს ბიზნესისა და მეწარმეობის კოლეჯის ეროვნული უსაფრთხოების დეპარტამენტს.**

სადოქტორო ნაშრომის გეგმა

საკითხის წინაპირობა და თემის აქტუალურობა

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

ძირითადი საკვლევი საკითხები და კვლევის გეგმა

<u>სადისერტაციო ნაშრომის ძირითადი მიმართულებებია:</u>

- ✓ მსოფლიო უსაფრთხოების დღევანდელი გამოწვევები. სავარაუდო და მოსალოდნელი საფრთხეების კვლევა.
- ✓ რამდენი თაობის ტექნოლოგიები არსებობდა და არსებობს, რამაც გამოიწვია მეთოდების დახვეწა.
- ✓ კიბერომი, კიბერშეტევა, კიბერდანაშაული, საინფორმაციო ომის საფუძვლები, ამ მიმართულებით რა თავდაცვითი სისტემები არსებობს მსოფლიო დონეზე.
- ✓ კანონმდებლობა და უსაფრთხოების სტრატეგიები. პრობლემის არსის სწორი განსაზღვრა და მისი გადაჭრის ვარიანტების სისტემის შექმნა, რასაც რეკომენდაციების ფორმა უნდა ჰქონდეს.

კიბერომი, როგორც გლობალური საკითხი, ვერ იქნება ერთი მიმართულებით საკვლევი საგანი. მით უმეტეს, ამ მოვლენასთან წინააღმდეგობის გაწევა ვერ მოხერხდება ცალსახად. აქ საყურადღებოა

უამრავი ფაქტორი - კიბერომის არსი, კიბერომის წარმოშობისა და განვითარების ისტორიის გაანალიზება, გამომწვევი და ხელშემწყობი მიზეზების იდენტიფიკაცია, კიბერდანაშაულთან დაკავშირებული ტერმინოლოგიების განსაზღვრა, ვირუსებისა და კიბერშეტევების კლასიფიკაცია, საერთაშორისო ორგანიზებული ჰაკერული დაჯგუფებების გამოვლენა, მათი მხრიდან მომდინარე საფრთხეების შეფასება და უსაფრთხოების მექანიზმების შემუშავება, კომპიუტერული პროგრამები და მათი აგებულების კლასიფიკაცია, პროგრამირების ენები და მათი დანიშნულების აღწერა, ინტერნეტისა და ქსელის საფუძვლების შესწავლა-განსაზღვრა, კომპიუტერულ სისტემაში უნებართვო შეღწევის სხვადასხვა სტრატეგიების წარმოჩენა, ადამიანის წინააღმდეგ მიმართული კიბერდანაშაულის ფაქტების აღწერა, კიბერსივრცესთან მიმართებაში კანონმდებლობის დახვეწის სხვადასხვა ვარიანტების რეკომენდაციების სახით განსაზღვრა. კიბერდანაშაულის შესახებ ევროპული კონვენცია, კონვენციის შესაბამისობა საქართველოს კანონმდებლობასთან, კონვენციით გათვალისწინებული საგამოძიებო მოქმედებები და საერთაშორისო თანამშრომლობა, კიბერსივრცის მარეგულირებელი შიდა ნორმატიული აქტები, ვირტუალური სამყარო და ვირტუალური ქონება, კრიფტოგრაფია, კრიპტოვალუტა, ბიტკოინი და ელექტრონული ფული. კიბერდანაშაულის პრევენცია თავდაცვის მიზნით.

<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 პროცესში 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 ომის მეოთხე თაობა, ანუ ვირტუალური სივრცე - 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“, „პოსტ ტვ“**) 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

<u>თეორიული ღირებულება:</u> 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.

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

ნაშრომის აპრობაცია და პუბლიკაცია

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.

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. არსებობს ამ თეორიის რამდენიმე ფორმა: მეთოდოლოგიური ბიჰევიორიზმი, რადიკალური ბიჰევიორიზმი, ექსპერიმენტული ბიჰევიორიზმი. თეორია გამოყენებულია ნაშრომის **მესამე თავში,** კიბერბიჰევიორისტული მიდგომის თვალსაზრისით, რომელსაც ასევე აქტიურად იყენებს აშშ-ის არმია. **111-114 გვ.**

2. **პოლიტიკური რეალიზმის თეორია** - მეცნიერების მტკიცებით, პოლიტიკური რეალიზმი იყო პასუხი ლიბერალიზმზე, რომლის ამოსავალი დებულება მდგომარეობდა იმაში, რომ სახელმწიფოები **<u>არ</u>**

ცდილობენ თანამშრომლობას. ადრეული რეალისტები **ედვარდ ქარი** და **ჰანს მორგენთაუ** მიიჩნევდნენ, რომ საკუთარი უსაფრთხოებაზე ზრუნვის გამო სახელმწიფოები არიან **ეგოისტური რაციონალური აქტორები,** რომლებიც ისწრაფვიან ძალაუფლებისკენ. ნებისმიერი სახის თანამშრომლობა ქვეყნებს შორის აღიქმება როგორც შემთხვევითი. რეალისტებისთვის მეორე მსოფლიო ომი იყო მათი იდეების ერთგვარი დადასტურება. პოლიტიკური რეალიზმის თეორიის თანახმად, საერთაშორისო ურთიერთობები არის მკაცრი კონკურენცია ქვეყნებს შორის, რომლებსაც არანაირი მიზეზი არ აქვთ, ერთმანეთს მიენდონ მაშინ, როდესაც მათი არსებობის არსი თვითგადარჩენაა ისეთ გარემოში, სადაც ერთის დანაკარგი მეორის მონაპოვარია. მეთოდოლოგია გამოყენებულია **მეორე თავში, 76-81 გვ.** 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** - ეს ერთ-ერთი უძველესი კონცეფციაა საერთაშორისო ურთიერთობათა თეორიაში. იგი მჭიდროდ უკავშირდება **პოლიტიკურ რეალიზმს** და გამომდინარეობს საერთაშორისო სისტემის **ანარქიული სტრუქტურიდან.** ამ თეორიის თანახმად, იმის გამო, რომ საერთაშორისო სისტემა ანარქიულია, თითოეული სახელმწიფოს ძირითადი ამოცანაა ბრძოლა თვითგადარჩენისა და თვითდამკვიდრებისათვის. ამის აუცილებელი პირობა კი უსაფრთხოება და დამოუკიდებლობაა. 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. თეორია გამოყენებულია **მეორე თავის, 2.2. ქვეთავში, 88-92 გვ.**

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. თეორია გამოყენებულია **მეორე თავის, 2.3. ქვეთავში, 94-99 გვ.**

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. **მეთოდი გამოყენებულია პირველ თავში, ასევე 1.1. ქვეთავში და 1.2. ქვეთავში.** წარმოდგენილია ტექნოლოგიების, ინტერნეტის, კიბერშეტევების, ვირუსების, კიბერთაღლითობისა და კიბერომების ისტორიული მიმოხილვა - **42-67 გვ.** ასევე **1.2 ქვეთავში** წარმოდგენილია კიბერშეტევების და მავნე კოდის შედევების აღწერა-კლასიფიკაცია. - **63-65 გვ. მესამე თავის 3.3. ქვეთავში** აღწერილია **რუსეთ-საქართველოს ომის** ისტორია - **154-162 გვ. მესამე თავში** წარმოდგენილია **ირანის ისლამური სახალიფოს შემთხვევის გარჩევა** და ირანის ისლამური სახალიფოს კიბერშესაძლებლობები - **120-127 გვ.**
- **სიღრმისეული ინტერვიუ** - ინტერვიუს სახეობა, ნაწილობრივ სტრუქტურირებული ინტერვიუ, რომელიც აგებულია რესპონდენტთა მოსაზრებების საფუძველზე. მეთოდი გამოვიყენეთ ექსპერტებთან ინტერვიუების ჩაწერისას - **164-192 გვ.**
- **დისკურს-ანალიზი** - ეს მეთოდი გამოვიყენეთ სატელევიზიო გადაცემების განხილვა-გაანალიზების დროს. აღნიშნული კვლევა ნაშრომში **მესამე თავის, 3.2. ქვეთავშია მოცემული - 128-147 გვ.**
- **შინაარსის ანალიზი - Content-analyze** მეთოდი, რომელიც დაკავშირებულია მედიის მიერ გავრცელებული ინფორმაციის შესწავლასთან. მეთოდი გამოვიყენეთ მედიასაშუალებების მიერ

გავრცელებული ინფორმაციის გაანალიზება-განსაზღვრაში, რომელიც ნაშრომში **130-140 გვერდებზეა** მოცემული.

- **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. წყაროები შეირჩა შემდეგი კრიტერიუმებით:

- ადგილობრივი და საერთაშორისო წყაროები
- ინფორმატიულობა
- კომპეტენტურობა
- ხედვის მასშტაბურობა
- სიღრმისეული ხედვა
- ორიგინალური ხედვა

წყაროების შეფასებისას უნდა გავითვალისწინოთ თემის ის მხარე, რომელიც მოიცავს არაერთგვაროვან აზრს ექსპერტებისა და ავტორების მიერ. შეიძლება გარკვეული ნაწილში ვეთანხმებოდეთ ავტორების მოსაზრებებს, შეიძლება - არა. თუმცა 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.

1. **კიბერთავდაცვა, კიბერსივრცის მთავარი მოთამაშეები, კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები. ვლადიმერ სვანიძე, ანდრია გოცირიძე ნაშრომებისა და სტატიების კრებული; სსიპ კიბერუსაფრთხოების ბიურო, საქართველოს თავდაცვის სამინისტრო, თბილისი, 2015.** პირველი ქართულენოვანი კრებული, რომელშიც განხილულია კიბერსივრცის თავისებურებები, საფრთხეები და გამოწვევები. ნაშრომში მოცემულია საერთაშორისო კიბერუსართხოების სტრატეგიები აშშ-ისა და ევროპის წამყვანი ქვეყნების მაგალითებზე, წარმოჩენილია საქართველოსა და პოსტსაბჭოთა ქვეყნების ეროვნული უსაფრთხოების ასპექტები.
2. **„Cyber Operations - Building, Defending, and Attacking Modern Computer Networks“. ავტორი გახლავთ მაიკ ოლილე (Mike O'Leary), გამოიცა აშშ-ის მათემატიკის დეპარტამენტის მხარდაჭერით, 2015 წელს.** წიგნში პროფესიულ დონეზეა საუბარი კიბეროპერაციების მეთოდებზე, თავდასხმების ნაირსახეობასა და თავდაცვით სისტემებზე. განხილულია, თუ როგორ მიმდინარეობს ტექნოლოგიური განვითარება და სისტემების მშენებლობა.
3. **სახელმძღვანელო - "Cyber Dragon - Inside China's Information Warfare and Cyber Operations", ავტორი გახლავთ მკვლევარი დეკანი ჩენგი (Dean Cheng). წიგნი გამოიცა 2017 წელს აშშ-ში.** განხილულია, თუ რა მეთოდებს ეყრდნობა ჩინეთი კიბერომისა და საინფორმაციო ომის დროს. დეტალურადაა ახსნილი, თუ რა მოსაზრებებით დაიწყო ჩინეთის ხელისუფლებამ ახალი ტექნოლოგიების ათვისება-წარმოება და გამოყენება.

4. **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.** წიგნი საინტერესოა მეცნიერული თვალსაზრისით, გასაგებადაა აღწერილი კიბერუსაფრთხოება, როგორც თანამედროვე მსოფლიოს გადარჩენის შანსი. საუბარია, თუ რა დიდი მნიშვნელობა აქვს საფრთხეების ანალიზსა და რეაგირებას, ანუ გადაწყვეტილებების დროულ მიღებას.
5. **„XXI საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების თეორია: მითი და რეალობა - რეგიონული და გლობალური ასპექტები" - ვახტანგ მაისაია, გუგული მაღრაძე, გამომცებლობა „უნივერსალი", თბილისი, 2017 წელი.** წიგნში ძირეულადაა განხილული, რა საფრთხეები არსებობს საერთაშორისო პოლიტიკაში და რას ნიშნავს თანამშრომლობითი უსაფრთხოების თეორია, რა არის მითი, რა - რეალობა. ნაშრომში განხილულია გლობალური უსაფრთხოების XXI საუკუნის პარამეტრები სხვადასხვა სახელმწიფოებრივი და არასახელმწიფოებრივი აქტორების მაგალითზე. მოყვანილია ჰიბრიდული საფრთხეების ჩამონათვალი და დეფინიცია, ასიმეტრიული საფრთხეების მნიშვნელობა გლობალური უსაფრთხოების თვალსაზრისით. წიგნში აღწერილია კოლექტიური უსაფრთხოების თეორია და გაანალიზებულია თეორიის პრაქტიკული მაგალითები.
6. **„The NICE Cyber Security Framework - Cyber Security Intelligence and Analytics", წიგნის ავტორი გახლავთ ტეხასის უნივერსიტეტის პროფესორი იზზატ ალსმადი. გამოიცა აშშ-ი, 2019 წელს.** ეხება აშშ-ის ეროვნულ ინიციატივას კიბერუსაფრთხოების საგანმანათლებლო სისტემაში. როგორ ხდება გარკვეულ სფეროებში დანერგვა, განსაკუთრებით ისეთი მიმართულებები, როგორებიცაა - კიბერდაზვერვა და ანალიტიკა. თემის სიღრმიდან გამომდინარე, ეს არ

გახლავთ ყოვლისმომცველი წიგნი კიბერუსაფრთხოებასთან დაკავშირებით, მაგრამ შეიძლება ჩაითვალოს შესავლად ისეთი პროგრამისა, როგორიც არის კიბერუსაფრთხოების - NICE. ეს პროგრამა ნიშნავს აკადემიასა და ტექნოლოგიურ ინდუსტრიას შორის კონტაქტის გაღრმავებას. წიგნში აღწერილია სპეციალობები და სამუშაო როლები კიბერუსაფრთხოების ჩამოსაყალიბებლად.

7. **სახელმძღვანელო - „Biometric-Based Physical and Cybersecurity Systems". გამოიცა შვეიცარიაში, 2019 წელს, რომლის ავტორებიც არიან მოჰამედ ობაიდატი, ისა ტრაორე და ისააკ ვოუნგანგი.** ბიომეტრიკა წარმოადგენს ადამიანის გამოვლენის ერთ-ერთ ყველაზე მყარ და საიმედო ფორმას ფიზიკურ და კიბერუსაფრთხოებაში. ბოლო წლებში სენსორული ტექნოლოგიების, მონაცემთა დამუშავების ტექნიკის და ალგორითმების შემუშავების მიმართულებით ბევრი რამ განვითარდა და დაიხვეწა. წიგნში კარგად არის გაანალიზებული ბიომეტრიული ტექნოლოგიების როლი კიბერუსაფრთხოების მიმართულებით. მაგალითად, ანაბეჭდები, სახე, ირისი, ბადურა, გასაღების დინამიკა, ხმა. ამ ტექნოლოგიების განვითარებამ ეროვნულ უსაფრთხოებაზე დადებითად იმოქმედა. წიგნში განმარტებულია, რომ ბიომეტრიულმა ტექნოლოგიებმა ხელი შეუწყო სენსორების და სმარტფონების განვითარებას, რისი მეშვეობითაც ონლაინ ბანკინგის წარმოებაა შესაძლებელი, თუმდა აქვე აღნიშნულია, რომ ამან სხვა საფრთხეებიც გამოიწვია. წიგნში წარმოდგენილი დასაბუთებული მონაცემები, მაგალითები და მოსაზრებები მნიშვნელოვან ინფორმაციას წარმოადგენს კიბერუსაფრთხოების თვალსაზრისით.

კვლევის მოსალოდნელი შედეგები

საკვლევი თემის მოსალოდნელი შედეგი ითვალისწინებს აკადემიური ხასიათის ნაშრომის შექმნას, რომელშიც ასახული იქნება კიბერომი, როგორც ეროვნული უსაფრთხოების ახალი პრობლემა - პოლიტიკური კონფლიქტის

ახალი განსაზღვრება, მოსალოდნელი საფრთხეების აღმოფხვრის შესაძლო ვარიანტები.

საფრთხეები არსებობს, ინტერნეტომი, ინტერნეტთავდასხმები უკვე ხდება ყოველდღიური საშიშროება არა მხოლოდ სახელმწიფოებისთვის პოლიტიკური თვალსაზრისით, არამედ ეკონომიკური და სოციალური დივერსიების კუთხითაც. ასევე საშიშროებას წარმოადგენს თითოეული ადამიანის წინააღმდეგაც - სოციალური ქსელები ამის "გარანტიას" იძლევა. კიბერსაფრთხე დამოკლეს მახვილივით ჰკიდია ნებისმიერი ადამიანის, ორგანიზაციის, უწყებისა თუ სახელმწიფოს თავზე და ამიტომაც იხარჯება ყოველწლიურად მილიარდობით დოლარი თავდაცვითი სისტემების შემუშავება-გაუმჯობესებისთვის. საჭიროა შეთანხმება და ერთობლივი რეკომენდაციების შემუშავება, სამწუხაროდ, უმართავ კიბერომს ერთი, თუნდაც სუპერსახელმწიფო ვერ მოერევა.

შესაძლებელია, ნატო არ გაფართოვდეს სამხედრო თვალსაზრისით, მაგრამ ფაქტია, უნდა გაფართოვდეს კიბერომთან დაკავშირებული საკითხების კუთხით. აქ თითქმის აღარ არსებობს საზღვრები - თუ არ მოხდა, თუნდაც, პოსტსაბჭოთა სივრცის გაკონტროლება, ნატოს სამხედრო თვალსაწიერს არ ექნება დიდი მნიშვნელობა და წინ ვერ აღუდგება გლობალური ტიპის საფრთხეებს. ინტერნეტტექნოლოგიებმა საზღვრები წაშალა, ყველა სახის საფრთხე მოექცა ერთ სივრცეში, აღარ აქვს მნიშვნელობა, ტერაქტი საფრანგეთში განხორციელდება თუ იტალიაში, საფრთხის წინაშე მაინც დგება მთელი მსოფლიო. ამას კი მივყავართ როგორც კომპლექსურ კვლევებამდე, ასევე პრაქტიკულ თანამშრომლობამდე, უფრო ფართო და მძლავრი ინფრასტრუქტურის შექმნამდე. კვლევის მოსალოდნელი შედეგების მიმართულებები შეიძლება ჩამოვაყალიბოთ ასე:

- ისტორიული შემთხვევების ანალიზის საფუძველზე შეიძლება შეფასდეს ამჟამინდელი პრობლემები და გამოწვევები საერთაშორისო უსაფრთხოების კუთხით.

- რიგი საფრთხეებისა, რაც შეიძლება მოჰყვეს ტექნოლოგიების განვითარებას და კიბერომის მეთოდების გაფართოებას.
- გვექნება დებატები შესწავლილ საკითხებთან დაკავშირებით.
- ობიექტური შეფასება ახალი ტექნოლოგიების განვითარებისა და მოსალოდნელი საფრთხეების ფონზე.
- ევროატლანტიკური ალიანსის როლისა და მნიშვნელობის წარმოჩენა კიბერუსაფრთხოების უზრუნველყოფაში.
- ჩატარდეს ტრენინგები სტუდენტებისთვის აღნიშნულ თემატიკის ირგვლივ.

დისერტაციის სტრუქტურა

წარმოდგენილი დისერტაცია შედგება შესავლის, სამი თავის, დასკვნისა და გამოყენებული ლიტერატურის სიისგან.

თავი პირველი - კიბერომის არსი და ისტორიული მიმოხილვა

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.

როგორ შეიქმნა კომპიუტერი? ეს არ მომხდარა ხელის ერთი დარტყმით - მას საფუძვლად უდევს გამოთვლითი ტექნოლოგიების განვითარება. XX საუკუნეში მეცნიერების ეფექტურმა მუშაობამ გამოიწვია ტექნოლოგიური რევოლუცია. მაგალითად, ქაღალდი, ჟურნალი, გაზეთი, წიგნი, კინო, ტელევიზია ისეთი ხელმისაწვდომი გახდა, როგორც არასდროს. ამას მოჰყვა კომპიუტერი და ინტერნეტი. შეიძლება დაუჯერებლად მოგეჩვენოთ, პირველი კომპიუტერი იკავებდა ერთ მოზრდილ ოთახს და მხოლოდ რიცხვების გამოანგარიშება შეეძლო. ეს ის პერიოდია, როდესაც კალკულატორი არ არსებობს. XX საუკუნის დასაწყისი, მეცნიერებმა გამოიგონეს ელექტრონული ლამპა, რომელსაც იყენებდნენ რადიომიმღების სიგნალის გასაძლიერებლად. 1940-იან წლებში გაჩნდა იდეა, რომ ელექტრონული ლამპები გამოეყენებინათ კომპიუტერის გასაკეთებლად. მეორე მსოფლიო ომის პერიოდში მეცნიერები ცდილობდნენ, ტექნოლოგიები განევითარებინათ. თუმცა მეცნიერები გამომთვლელი მანქანის შექმნაზე საუკუნეების განმავლობაში ფიქრობდნენ - მაგალითად, XIX საუკუნეში დადგა საკითხი, გაეკეთებინათ ისეთი მოწყობილობა, რომელიც არა მხოლოდ გამოთვლიდა რიცხვებს, არამედ ამოხსნიდა მთელ მათემატიკურ ამოცანას. პირველი მცდელობა ჰქონდა კემბრიჯის უნივერსიტეტის პროფესორს, **ჩარლზ ბებიჯს,** 1791-1871 წლებში.

მცდელობა უშედეგოდ დამთავრდა. მარცხმა **ჩარლზ ბებიჯს** მეტი სტიმული მისცა, 1834 წელს დაიწყო მუშაობა გამომთვლელ მანქანაზე სახელწოდებით - **„ანალიტიკური ძრავი“ (Analytical Engine).** ამ მანქანას უნდა ამოეხსნა ყველა ამოცანა, რომელსაც მათემატიკოსები და ინჟინრები ხსნიდნენ. მანქანა აღჭურვილი იყო ცენტრალური პროცესორული მოწყობილობით, მეხსიერებით და პერფობარათებით. მნიშვნელოვანია, რომ **ჩარლზ ბებიჯის** მანქანას ოცნიშნა რიცხვების ოპერირება შეეძლო. მანქანას უნდა ემუშავა ადამიანის ჩარევის გარეშე. ის, რომ პერფობარათების საშუალებით ემართათ გამომთვლელი მანქანები, იყო წინასწარმეტყველური ჩანაფიქრი. ეს იდეა 1804 წელს განავითარა ფრანგმა გამომგონებელმა **ჟოზეფ მარი ჟაკარმა** საქსოვი დაზგის ავტომატიზაციით.[1]

მეცნიერების წინაშე დადგა ახალი ამოცანა - პროგრამირების შექმნა და განვითარება. 1843 წლის 19 ივლისი პირველი პროგრამის შექმნის თარიღად არის აღიარებული. პროგრამის შექმნაში დიდი წვლილი მიუძღვის ცნობილი ინგლისელი პოეტის, **ჯორჯ გორდონ ბაირონის** ქალიშვილს, **ადა აუგასტას,** რომელიც გახლდათ **გრად ლავლეისის** მეუღლე. 1843 წლის 19 ივლისს **აუგასტამ** შექმნა პირველი ბერძნული რიცხვების გამოსათვლელი პროგრამა. ამ დროს მანქანას შეეძლო შეესრულებინა არა მხოლოდ არითმეტიკული გამოთვლა, არამედ ლოგიკური ოპერაციებიც. ეს მას შემდეგ გახდა შესაძლებელი, რაც (1847 წელს) ინგლისელმა მათემატიკოსმა **ჯორჯ ბულმა** შექმნა ლოგიკურ გამონათქვამთა თეორია და ეწოდა **„ბულის ალგებრა“.[2]**

აქვე აღსანიშნავია, ქართველი მეცნიერის **გიორგი ნიკოლაძის** წვლილი (1888-1931). ნიკოლაძის გამოგონებამდე რაც კი არითმომეტრები არსებობდა, იყო მექანიკური, ხოლო საფრანგეთში ყოფნის პერიოდში მან შეისწავლა არსებული არითმომეტრები და გამოიგონა ახალი

[1] Freiberger A. P., Swaine R. M., Analytical Engine, Encyclopedia Britanica, 2020, p 1. https://www.britannica.com, უკანასკნელად იქნა გადამოწმებული - 03.07.2020.

[2] Loritz M. Who was Ada Lovelace? The life of the woman who envisioned the modern day computer, Media Website "EU-Startup", 2019, p 1. https://www.eu-startups.com, უკანასკნელად იქნა გადამოწმებული - 03.07.2020.

ელექტრონული გამომთვლელი, რომელსაც ეწოდა **„პირდაპირი გამრავლების ელექტრონული არითმომეტრი“**. იგი სხვა გამომთვლელებისაგან განსხვავდებოდა ელექტრონული გამანაწილებლით. ამ გამოგონებით მაშინვე დაინტერესდნენ ამერიკული და ევროპის კომპანიები, მაგრამ მან უარი თქვა მათთან თანამშრომლობაზე და გამოემგზავრა სამშობლოში, საქართველოში გააკეთა არითმომეტრის მოდელი, რომელიც შემდეგ გაიგზავნა გამოფენაზე მოსკოვში. სამწუხაროდ, **გიორგი ნიკოლაძეს** არ დასცალდა, დაეზუსტებინა არითმომეტრის მთლიანი კონსტრუქციის დოკუმენტაცია, 1931 წელს მოულოდნელად გარდაიცვალა.[3]

დიდი ხნის განმავლობაში აღიარებული იყო, პირველი კომპიუტერი შეიქმნა 1945 წელს, ამერიკელი ფიზიკოსების - **ჯონ ეკრტის** და **ჯონ მოუჩის** მიერ, რომლის სახელწოდებაც იყო **„ენიაკი“ (ENIAK – Electronic Numerical Integrator and Computer).** თუმცა ეს ისტორია მცდარი აღმოჩნდა - მართალია, **„ენიაკი“** მსოფლიოში პირველი კომპიუტერია, რომლის კონსტრუქტორებიც **ეკერტი** და **მოუჩი არიან**, დიდი წვლილი მიუძღვით გამოთვლითი ტექნიკის განვითარებაში, მაგრამ პირველი კომპიუტერის მუშაობის პრინციპები მათ არ მოუფიქრებიათ. ეს პრინციპები ჩამოყალიბდა 1937 წელს და პირველი კომპიუტერის შექმნის მცდელობაც იყო აიოვას შტატის ქალაქ ეიმსში მომუშავე ბულგარელი ფიზიკოსის, **ჯონ ატანასოვის** და მისი დამხმარის, **კლიფორდ ბეტისის** მიერ, რომელსაც უწოდეს **„ABC”,** მისი შექმნა 1942 წელს დამთავრდა. ამ დროს მხოლოდ დარჩენილი იყო პერიფერიული ნაწილის აწობა. თუმცა II მსოფლიო ომის გამო ექსპულატაციაში ვერ ჩაეშვა. 1973 წელს დაიწყო დავა ორი დიდ კომპანიას შორის, პირველი კომპიუტერის აწყობის საავტორო უფლებების თაობაზე. გაიმართა 135 სასამართლო სხდომა. საბოლოოდ დამტკიცდა, რომ 1940 წელს **ატანასოვს** მიუწვევია **მოუჩი**, მისთვის უჩვენებია ხელნაწერები,

[3] აბულაშვილი ი. "პირველი ელექტროგამომთვლელი მანქანის გამომგონებელი ქართველი", გაზეთი „რეზონანსი“, 2017, გვ. 1. http://www.resonancedaily.com, უკანასკნელად იქნა გადამოწმებული - 03.07.2020.

განუმარტავს და აუხსნია გამოთვლითი მოწყობილობის მუშაობის პრინციპები. შემდეგ კი **მოუჩიმ** შეძლო, შეექმნა ის, რასაც პირველი კომპიუტერი ეწოდა. თუმცა დადასტურებულად შეგვიძლია ვთქვათ, რომ პირველი კომპიუტერის შემქმნელი **ატანასოვია.**[4]

კომპიუტერი - ეს არის პროგრამის მიხედვით ავტომატურად მართვადი სწრაფი მოქმედების სისტემა. ელექტრონული მანქანა, რომლის ძირითადი დანიშნულებაა დიდი მოცულობის ინფორმაციის შენახვა, დამუშავება და გადაცემა. დღეს ეს ყველაფერი უფრო მრავალფეროვნად გვეჩვენება, მაგრამ კომპიუტერს ძირითადი ფუნქციები არ შეუცვლია. გადის წლები, მატულობს კომპიუტერების რაოდენობა და იხვეწება. ტექნოლოგიური მიღწევების წყალობით შესაძლებლობები ყველა ტექნიკურ სისტემაში გაიზარდა - მობილურ ტელეფონებში, ავტომობილებში, სხვადასხვა საოჯახო თუ სამეწარმეო დანადგარებში.

1974 წელს შეიქმნა პირველი პერსონალური მიკროკომპიუტერი **„Altair".** მისი მწარმოებელი იყო, **ედ რობერტსონის** დაარსებული კომპანია **MITS.** მიკროკომპიუტერი **„Altair"** წარმოადგენდა ასაწყობ კომპლექტს, არ ჰქონდა კლავიატურა და მონიტორი. მონაცემების შეყვანა ხორციელდებოდა წინა პანელზე მოთავსებული გადამრთველების საშუალებით. ამ კომპიუტერის ინტერპრეტატორი ბეისიქი შექმნა ბილ გეიტსის მიერ დაარსებულმა კომპანია **„Microsoft"-მა.** 1977 წელს გამოვიდა კიდევ რამდენიმე პერსონალური კომპიუტერი - **Tandy, Commodore, Apple II.** ამათგან გამოსარჩევია **Apple,** რომელიც შექმნა ორმა ახალგაზრდა მეგობარმა - **სტივ ჯობსმა** და **სტივ ვოზნეაკმა.** კომპიუტერის შექმნამდე (1976 წელს) მათ დაარსეს კომპანია **Apple Computer,** რომლის სამუშაო ოფისადაც გამოიყენეს ჯობსის მშობლების ბინის ერთ-ერთი საძინებელი ოთახი. მათი შექმნილი კომპიუტერი გამოირჩეოდა კარგი დიზაინით და საიმედოობით, ასევე მსოფლიო მასშტაბით პირველი იყო ფერადი გრაფიკით. ამ მოდელის შექმნა იმდენად წარმატებული აღმოჩნდა, რომ 1980 წელს **Apple Computer**-ის

[4] Levy S. The Brief History of the ENIAC Computer, Smithsonian Magazine, 2013, p 1. https://www.smithsonianmag.com, უკანასკნელად იქნა გადამოწმებული - 04.07.2020.

შემოსავალმა 117 მილიონ დოლარს მიაღწია. 1979 წელს გამოვიდა **Apple II-ის** მოდიფიცირებული მოდელი - **Apple II plus.** ის უფრო მეტად დახვეწილი იყო, ვიდრე წინა მოდელი. **Apple II plus-ისთვის** შექმნილმა „ელექტრონული ცხოვრების“ პირველმა პროგრამამ - **VisiCalc** ეს კომპიუტერი მცირე ფირმების ბუღალტერიის წარმოებისთვის სერიოზულ ინსტრუმენტად აქცია.[5]

<u>კომპიუტერი იყოფა თაობებად:</u>

პირველი თაობა - კომპიუტერები აწყობილი იყო ლამპებით, ასევე ელექტრონულ-სხივური მილაკებით. ასეთმა მანქანებმა იარსება 1950-1957 წლებში. „ენიაკი“ იწონიდა 27 ტონას, იგი შედგებოდა 18000 ლამპისგან, იკავებდა 200 მ2 ფართობს. კომპიუტერის სამუშაოდ საჭირო იყო უამრავი პროგრამისტი და ინჟინერი. მუშაობის სიმძლავრე წამში 10-15 ათასი არითმეტიკული ოპერაციის შესრულება იყო, რაც დღევანდელ კომპიუტერთან შედარებით ძალიან მცირეა. მეხსიერება მაგნიტურ დონეზე იყო წარმოდგენილი. ეს ფაქტობრივად წარმოადგენდა ექსპერიმენტულ მოწყობილობებს, იქმნებოდა სხვადასხვა თეორიული მოსაზრებების შესამოწმებლად. მნიშვნელოვანია ის ფაქტი, რომ **„ენიაკის“** პარალელურად, **დიდ ბრიტანეთში** საიდუმლოდ იწარმოებოდა კომპიუტერი **IBM**, რომელსაც შეეძლო კოდების გაშიფრვა. ამის გამო იყო ის გასაიდუმლოებული. უკვე ცნობილი ფაქტია, მას იყენებდნენ გერმანიაში პირველი და მეორე მსოფლიო ომების დროს. კოდების გაშიფრვის მათემატიკური მეთოდი შექმნილი იყო პროფესიონალ მათემატიკოსთა ჯგუფის მიერ, რომელშიც შედიოდა **ალან ტიურინგი.** 1943 წელს ლონდონში **მ. ნიუმენმა** და **ფ. ფლაუერიმ** გამოიგონეს მანქანა „**Colossus**“, რომელიც შედგებოდა 1500 ელექტრონული ლამპისგან. 1937 წელს მათემატიკოსმა **ჰოვარდ ეიკენმა** შეიმუშავა დიდი გამომთვლელი მანქანის შექმნის პროექტი. ამ საქმეში 500 ათასი დოლარი ჩადო **IBM**-ის პრეზიდენტმა **ტომას**

[5] Levy S. Steve Jobs American businessman, Encyclopedia Britanica, 2020, p 1. https://www.britannica.com, უკანასკნელად იქნა გადამოწმებული - 04.07.2020.

ვატსონმა. ამით დაიწყო **Mark-1-ის** დაპროექტება. პროდუქცია 1939 წელს **IBM**-ის სახელით გამოვიდა.

1955 წელს ფირმა **Ferrant**-მა გამოუშვა კომპიუტერი **Pegasus**, ამ კომპიუტერში გამოყენება ჰპოვა საერთო დანიშნულების რეგისტრების კონცეფციამ. შემდგომში კომპიუტერისთვის აშშ-ის საზღვაო ფლოტის ოფიცერმა (ადმირალმა), პროგრამისტმა, გრეის ხოპერმა შექმა პირველი კომპილატორი - პროგრამა, რომელიც ადამიანისთვის გასაგებ ენაზე დაწერილ პროგრამას თარგმნიდა მანქანის ენაზე. ამან საგრძნობლად გააადვილა პროგრამირების პროცესი. ისტორიულად, პირველი კომპიუტერის ფუძემდებლებად ითვლებიან, ინფორმაციის თეორიის შემქმნელი, კლოდ შენონი, პროგრამირების და ალგორითმების თეორიის შემქმნელი, მათემატიკოსი, ალან ტიურინგი და გამომთვლელი მოწყობილობების კონსტრუქციის ავტორი ჯონ ფონ ნეიმანი. **პირველი თაობის კომპიუტერებია:** „ენიაკი“, „ურალ-2“, „სტრელა“, M-20 და ა.შ.

მეორე თაობა - 1958 წლიდან ელექტრონული ტექნიკის განვითარებამ, რაშიც იგულისხმება ნახევარგამტარული ელემენტების გამოჩენა, განაპირობა კომპიუტერების განვითარება, ანუ მეორე თაობის კომპიუტერების შექმნა. ლამპა შეიცვალა უფრო სწრაფი და საიმედო ტრანზისტორით. ამ მანქანებს მეხსიერება ჰქონდათ მაგნიტურ გულანებზე, წარმოადგენდნენ პატარა რგოლებს, რომლებსაც შესაძლებლობა ჰქონდათ ორმაგი ინფორმაციის დამახსოვრების. წინა თაობისაგან განსხვავებით, ეს თაობა უფრო საიმედო და სწრაფი იყო. ასევე შემცირდა მისი ზომა, გამოყენების სფერო, ადამიანების რაოდენობა, ენერგია. მას იყენებდნენ სხვადასხვა ეკონომიკური და სტატისტიკური ამოცანების ამოსახსნელად. ითვლება, რომ მეორე თაობის კომპიუტერის წვლილი დიდი იყო სამეცნიერო-ტექნიკური ამოცანების გადაწყვეტის საქმეში. ის, რასაც დღეს ვეძახით ოპერატიულ სისტემას, პირველად II თაობის კომპიუტერში გამოიყენეს. ასევე, ამ პერიოდში შეიქმნა დაპროგრამების ენები: კობოლი,

ფორტრანი, ალგოლი. **მეორე თაობის კომპიუტერებია:** M-220, BESM-4, URAL-14, MINSK-2, MINSK-4 და ა.შ.

მესამე თაობა - 1964 წელს ფირმა **IBM**-მა ექვსმოდულიანი მოწყობილობა წარადგინა. კომპიუტერები ერთმანეთს უკავშირდებოდნენ ოპერატიული სისტემით და ჰქონდათ ბრძანების ერთიანი სისტემა. 1957 წელს რობერტ ნოისმა, რომელმაც შემდეგ ფირმა **Intel** დაარსა, გამოიგონა სრულყოფილი მეთოდი, რომლის საშუალებით ერთ ფირფიტაზე თავსდებოდა რამდენიმე ათეული ტანზისტორი და ყველა შემაერთებელი საშუალება. ამ სქემას ეწოდა **„ჩიპი“.** 1968 წელს პირველი ჩიპიანი კომპიუტერი გამოვიდა, 1970 წელს კი **Intel-მა** ჩიპის გაყიდვა დაიწყო. **Intel-მა** ამავე წელს დაიწყო ცენტრალური პროცესორის აწყობა ანალოგიური ჩიპით. ეს იყო პირველი მიკრო-პროცესორის გაჩენის პერიოდი - **Intel-4004.** ჩიპების გამოყენებამ მესამე თაობის კომპიუტერების მოქმედების სისწრაფე საგრძნობლად აამაღლა, რაც გულისხმობდა 80-100 ათას არითმეტიკულ ოპერაციას წამში. ამავე პერიოდში შეიქმნა დისკი, ანუ დისკური ტიპის მეხსიერება და ინფორმაციის შემტან-გამომტანი მოწყობილობა, რომელსაც უწოდეს **„დისფლეი“**. დისკი, ანუ გარე მეხსიერება განკუთვნილია იმ ინფორმაციის დასამახსოვრებლად, რომელიც შეიძლება მრავალჯერ იქნას გამოყენებული. სწორედ ამ წლებში **IBM-მა** დაიწყო კომპიუტერების გამოშვება, როგორც პატარა, ასევე დიდი და იმ დროისთვის ყველაზე მძლავრი, ძვირადღირებული კომპიუტერებისა.

ამავე პერიოდს უკავშირდება ისეთი მნიშვნელოვანი პირველი გლობალური ქსელის შექმნა, როგორიც **„Internet”-ია.** ასევე, გამოჩნდა ოპერატიული სისტემა **Unik** და პროგრამირების ენა **„C”,** ამ ყველაფერმა კი ძალიან დიდი გავლენა მოახდინა პროგრამულ სამყაროზე და ეს დღესაც გრძელდება. **მესამე თაობის კომპიუტერებია:** EC-1022, EC-1035, CM-2, CM-4, EC-1055 და ა.შ.

მეოთხე თაობა - 1975-1985 წლებში გამოშვებული კომპიუტერები ეკუთვნის მეოთხე თაობას. თუმცა არსებობს სხვა მოსაზრებებიც, რადგან იმ

პერიოდისთვის კომპიუტერის განვითარების დონე არც ისე მაღალი იყო. მნიშვნელოვანი მაინც ის არის, რომ 1980-იანი წლების დასაწყისიდან, პერსონალური კომპიუტერების გამოჩენის წყალობით, კომპიუტერული ტექნიკა საზოგადოებისთვის ხელმისაწვდომი გახდა.

მეხუთე თაობა - 1982 წელს იაპონიაში შეიქმნა კომპიუტერების აგების პროგრამა. ამ პროგრამის მიხედვით, 1991 წელს უნდა გამოსულიყო სრულიად ახალი ტიპის კომპიუტერები, რომლებიც ხელოვნური ინტელექტის ამოცანების ამოხსნაზე იქნებოდა ორიენტირებული. კომპიუტერების ძირითადი ამოცანა იქნებოდა არა ინფორმაციის, არამედ ცოდნის შენახვა და დამუშავება.[6]

ინტერნეტის შექმნა

1957 წელს საბჭოთა კავშირმა შექმნა ხელოვნური თანამგზავრი, რომელიც დედამიწის ორბიტაზე გაუშვა. ეს ფაქტი შეერთებული შტატების თავდაცვის უწყებამ მიიჩნია საბჭოთა კავშირის ტექნოლოგიური მიღწევების მაღალ ნიშნულად. იფიქრეს, რომ ფართომასშტაბიანი ომის შემთხვევაში ამერიკელებს ინფორმაციის გადაცემის საიმედო სისტემა დასჭირდებოდათ. სხვა არსებული სისტემების ერთ-ერთი ნაკლი იყო სამართავი ცენტრი, ადგილი, რომლის გათიშვის შემთხვევაში მთელი სისტემა გამოვიდოდა მწყობრიდან.. ამიტომ საჭირო იყო ისეთი ქსელის შექმნა, რომელსაც არ ექნებოდა მართვის ერთიანი ცენტრი და რომელიმე სეგმენტის გათიშვის დროს სისტემა შეუფერხებლად იმუშავებდა. ამ მიზანს ისახავდა მოწინავე პროექტების კვლევის სააგენტოს დაარსება - **Advanced Research Projects Agency**, იგი ცნობილია როგორც **ARPA.** ეს იყო ის ადგილი, სადაც შეიმუშავეს ინტერნეტის საწყისი კონცეფცია. ინტერნეტის შექმნის იდეა ამერიკელ სამხედროებს ეკუთვნით, ხოლო იდეის განხორციელება

[6] Burns D. The five generations of computers, Business to Business Company, 2016, p 1. https://btob.co.nz, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

ამერიკულმა უნივერსიტეტებმა შეძლეს. ამის შემდეგ შეიქმნა ინტერნეტის შემდეგი ვერსია - **ARPANET**-ი.[7]

პირველი ინტერნეტკავშირი

1969 წლის 29 ოქტომბერს **ARPANET**-ში ჩართულ ორ კომპიუტერს შორის პირველი კავშირი შედგა. ისინი ერთმანეთისგან 640 კილომეტრით იყო დაშორებული. პირველი კომპიუტერი სტენფორდის კვლევათა ინსტიტუტში, ხოლო მეორე კომპიუტერი კალიფორნიის უნივერსიტეტში, ქალაქ ლოსანჯელესში მდებარეობდა. სტენფორდის კვლევითი ინსტიტუტის კომპიუტერთან დაკავშირებას და მონაცემების გადაგზავნას ჩარლი კლაინი ცდილობდა, ხოლო მონაცემების გადაგზავნის პროცესს სტენფორდში ბილ დიუვალი ადევნებდა თვალ-ყურს. პირველი ჩართვისას მხოლოდ სამი სიმბოლოს გაგზავნა მოხერხდა, სიმბოლო იყო-**LOG**, მთლიანი გადასაგზავნი სიტყვა **LOGON**-ი, ანუ სისტემაში შესვლის ბრძანება, თუმცა ქსელი გაითიშა, მისი აღდგენა კი მხოლოდ საათნახევრის შემდეგ მოხერხდა. მომდევნო ცდა წარმატებული გამოდგა. ამას მოყვა აშშ-ის მსგავსად ევროპის სხვადასხვა ქვეყნებში ინტერნეტის ქსელების განვითარება. ამ საქმეში 1973 წელს ტრანსატლანტიკური კაბელის საშუალებით პირველი არაამერიკული ორგანიზაციები, დიდი ბრიტანეთი და ნორვეგია ჩაერთვნენ, რითაც ქსელი საერთაშორისო გახდა. 1983 წელს არსებულ გლობალურ ქსელს „ინტერნეტი“ უწოდეს და მის დიდ ნაწილს **ARPANET-ი** წარმოადგენდა. თავიდან ინტერეტით მხოლოდ ინფორმაციის გაგზავნა და მიღება იყო შესაძლებელი. ეს ძალიან წინგადადგმული ნაბიჯი გამოდგა. მანამდე დიდი მოცულობის ინფორმაციის გადაგზავნა და მიღება მხოლოდ ფაქსის მეშვეობით იყო შესაძლებელი. ფაქსით კი მრავალგვერდიანი ტექსიტს გაგზავნა და მიღება ბევრ სირთულესთან არის დაკავშირებული. ინტერნეტით ეს იოლად ხერხდება. ასევე, ინტერნეტით შესაძლებელია ერთი დოკუმენტის ერთდროულად რამდენიმე ადგილას

[7] Andrews E. The Invention of the Internet, Internet publisher History, 2019, p 1. https://www.history.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

გადაგზავნა, ფაქსით ეს გამორიცხულია. პირვანდელი ინტერნეტი დღევანდელი ინტერნეტისგან ძალიან განსხვავდება, იმ დროისთვის ადამიანები მხოლოდ ინფორმაციას უცვლიდნენ ერთმანეთს.[8]

ასე იყო იქამდე, სანამ მეცნიერმა **ტიმ ბერნერს ლიმ** 1989 წელს ევროპაში, ცერნის ლაბორატორიაში ვების კონცეფცია არ წარმოადგინა, ანუ ჩვენთვის ცნობილი როგორც - **„www" (World Wide Web),** ამ კონცეფციის იდეა ერთი შეხედვით მარტივი იყო, გულისხმობდა ინტერნეტის საშუალებით არა მხოლოდ ინფორმაციის გაცვლას, არამედ მომხმარებლის მიერ ინფორმაციის განთავსებას. ასე შეიქმნა ვებ-გვერდები, რომლებსაც დღეს დიდი მნიშვნელობა ენიჭება როგორც საინფორმაციო სააგენტოების, ასევე უამრავი კომპანიის, ბიზნესის ბრენდირებისთვის. აღსანიშნავია, რომ **ტიმ ბერნერს ლი** ამ კონცეფციის შექმნას არ დასჯერდა და თავისი გამოგონება უფრო ფართომასშტაბიანი გახადა, ვებ-გვერდები ერთმანეთთან ბმულებით დააკავშირა, რათა მომხმარებელი ადვილად გადასულიყო სხვა გვერდზე. **ტიმ ბერნერს ლიმ** თავისი გამოგონება არ დააპატენტა, მან ის კაცობრიობას აჩუქა, ამიტომაც ინტერნეტის მომხმარებლები სხვადასხვა ვებ-გვერდებს ყოველგვარი გადასახადის გარეშე ვსტუმრობთ.[9]

1990 წელს ახალი გამოგონების ხარჯზე ინტერნეტში სატელეფონო ხაზით შეერთება გახდა შესაძლებელი **(Dialup access).** ამით ინტერნეტის გამოყენება მარტივი და ყველასთვის ხელმისაწვდომი გახდა. დღეს უამრავი საშუალებაა ინტერნეტში ჩართვისთვის - თანამგზავრული კავშირი, ტელეფონი, ფიჭური კავშირი, სპეციალური ოპტიკურ-ბოჭკოვანი ხაზი **(wifi)** და სხვა. ცნობილია, რომ ინტერნეტის მომხმარებელთა რაოდენობა პირველი ხუთი წლის განმავლობაში 50 მილიონამდე გაიზარდა. 2010

[8] Weber M. october 29, 1969: Happy 40TH Birthday to a Radical Idea!, Computer History Museum, 2009, p 1. https://computerhistory.org, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

[9] Berners-Lee T. A short history of the Web - Where the Web was born, CERN Accelerating science, 2013, p 1. https://home.cern, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

წლიდან ინტერნეტით სარგებლობა საერთაშორისო კოსმოსური სადგურიდანაც გახდა შესაძლებელი.[10]

ეს გახლავთ მცირე ისტორია იმ პროცესების შესახებ, რასაც ტექნოლოგიური რევოლუცია ჰქვია და რამაც მიგვიყვანა, როგორც ბევრ სიკეთემდე, ასევე ბევრ საფრთხის შემცველ მოვლენამდე - მასობრივი სოციალური ქსელების განვითარება, მავნე ვებ-გვერდების შექმნა, ვირუსებისა და მასოვრივი თაღლითობის უწყვეტი რეჟიმი, კიბერტერორიზმი, კიბერდანაშაული, კიბერომი.

კიბერსივრცე (Cyberspace) - პირველად 1982 წელს გამოიყენეს ვრცელ სტატიაში. კიბერსივრცეში იგულისხმება ყველაფერი, რაც ინტერნეტს უკავშირდება. **კიბერპანკი (Cyberpunk)** - ეს არის, როგორც სამეცნიერო ფანტასტიკის ქვეჟანრი, ტერმინი პირველად 1960-იანი წლების ბოლოს და 1970-იანი წლების დასაწყისში **„New Wave"**-ის სამეცნიერო ფანტასტიკურ ნოველებში იხმარეს. **კიბერუსაფრთხოება (Cybersecurity)** - ამ სიტყვის პირველი გამოყენება 1989 წელს გვხვდება სამეცნიერო ლიტერატურაში. **კიბერდანაშაული (Cybercrime)** - არსებობს მრავალი დანაშაულის ფორმა: ფინანსური, თაღლითობა, კიბერდამცირების, ქურდობის და ნებისმიერი დანაშაულის ჩადენა ინტერნეტში. **კიბერდაცვა (Cyberdefense)** - ეს სიტყვა იგივეა, რაც კიბერუსაფრთხოება, ეს არის კიბერდანაშაულის გამოვლენა, პრევენცია და რეაგირება. ეს უფრო ხშირად ეხება სამხედრო და სამთავრობო სისტემებს. **კიბეროპები (Cyberops)** - კიბეროპერაციები, მოიცავს კიბერსივრცეს და ხორციელდება როგორც ტექნიკურად, ასევე არატექნიკურად. **კიბერდელიკი (Cyberdelic)** - ეხება ხელოვნებას, გაჯანსაღებას ან იმპრესიულ გამოცდილებას, რომელიც ინტერნეტის აქტიური მოხმარების ხარჯზე ხორციელდება. **კიბორგი (Cyborg)** - ტექნიკურად გულისხმობს კიბერნეტიკისა და ორგანიზმის შერწყმას, ეს ნიშნავს, რაც შედგება რობოტული ნაწილებისგან.

---

[10] Ambersariya D. Types of Internet Connections- Wireless, Dial-up, DSL, Fiber, Cable, ISDN, Technology Website Invention Sky, 2019, p 1. https://inventionsky.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

კიბრაული (Cybrarian) - კიბერბიბლიოთეკარი, უფრო მოკლედ - კიბრალეული, არის მკვლევარი, რომელიც ინფორმაციისთვის ძირითადად ინტერნეტს იყენებს. **კიბერნავტები (Cybernauts)** - კიბერნაუტი არის ადამიანი, რომელიც ქმნის სენსორული და ვირტუალური რეალობის მოწყობილობებს.

კიბერდანაშაული, კიბერომი, კიბერტერორიზმი, კიბერშეტევები და მსგავსი მოვლენები დღევანდელი ყოფის თანმდევია.[11]

პირველი ვირუსი 1982 წლის 30 იანვარს 15 წლის **რიჩარდ სკრენტასმა** ზამთრის არდადეგებზე დაწერა, ეს ვირუსი ითვლება პირველ ფართომასშტაბიან თვითგამანაწილებელ პერსონალურ კომპიუტერულ ვირუსად. სკრენტასი თავის მეგობრებს ეხუმრებოდა სხვადასხვა კომპიუტერული ხრიკებით, თუმცა ასეთ რამეს მაინც ვერავინ წარმოიდგენდა. მისი ვირუსი **„Elk Coner"**-ი, რომელიც 400 სტრიქონიანი იყო, შენიღბა როგორც Apple boot პროგრამა. თვითონ ავტორი ამ ვირუსს პატარა ხუმრობას უწოდებდა. იგი შემდგომში იყო საძიებო სისტემების დამწყები **Blekko**-ს აღმასრულებელი დირექტორი, **IBM Watson**-ის აღმასრულებელი დირექტორის მოვალეობის შემსრულებელი, ასევე თანამშრომლობდა სოციალური აქტივობის პლატფორმის - **Magnify Progress**-თან. **Linkedin**-მა რეკომენდაცია გაუწია **რიჩარდ სკრენტასს,** სადაც ნათქვამია: „გეშინოდეთ ამ ადამიანისა და მისი კიბორგების არმიის". ცნობილია, რომ პირველად ტერმინი **„კომპიუტერული ვირუსი"** გამოიყენეს 1983 წელს უსაფრთხოების სემინარზე.[12]

კიბერშეტევები ჯერ კიდევ იქამდე დაიწყო, სანამ ადამიანთა უმრავლესობას კომპიუტერი ექნებოდა. პირველი ჰაკერული თავდასხმა 1971 წელს განხორციელდა და სრულიად უწყინარი იყო, ექსპერიმენტს უფრო წარმოადგენდა ვიდრე დამაზიანებელ **კიბერშეტევას. ბობ თომასი** თავისი

[11] Coe T, Where does the word cyber come from?, Oxford University Press's Academic Insights for the Thinking World, 2015, p 1. https://blog.oup.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

[12] Deffere S. 1st computer virus is written, January 30, 1982, Electronics Design Network, 2019, p 1. https://www.edn.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

შექმნილი პროგრამით ისტორიაში შევიდა, რომელიც მიჩნეულია როგორც **„კომპიუტერული ჭია“.** იგი საერთოდ არ იყო მავნე და ყველა ინფიცირებულ ეკრანზე აჩვენებდა შეტყობინებას: **„მე ვარ მცოცავი, დამიჭირე, თუ შეგიძლია“.**[13]

რაც შეეხება დამაზიანებელ **კიბერშეტევას,** იგი განხორციელდა 1989 წელს **რობერტ მორისის** მიერ, მისმა პროგრამამ მნიშვნელოვნად შეანელა ადრეული ინტერნეტის მუშაობა. ამრიგად, ისტორიაში პირველი **DoS** შედევა 1989 წელს განხორციელდა. **მორისმა** განმარტა, რომ თავდასხმა იყო უსაფრთხოების ხარვეზების გამოსასწორებლად ჩადენილი, როგორიცაა **Unix sendmail** და სუსტი პაროლები. ამ შეტევამ გამოიწვია იმდროინდელი ინტერნეტის გაყოფა და გაგრძელდა რამდენიმე დღის განმავლობაში.[14]

ამავე წელს ისტორიაში საშინელი დღე აღინიშნა, როდესაც **ჯოსეფ პოპმა** შექმნა პირველი **გამოსასყიდი შეტევა.** გამოიყენა მავნე პროგრამა სახელწოდებით -**AIDS Trojan**, რომელიც გადაიგზავნა მისი ელფოსტის მეშვეობით. **პოპი** იმედოვნებდა, რომ ამ პროგრამით ხალხს გამოსძალავდა ფულს.[15]

რაც შეეხება ყველაზე დიდ კიბერშეტევას, იგი 1982 წელს, როდესაც ჯერ კიდევ **ცივი ომის** პერიოდი იყო, მაშინ განხორციელდა, **აშშ-ის ცენტრალურმა სადაზვერვო სააგენტომ** როგორღაც იპოვა გზა რუსეთის ციმბირის გაზსადენის მუშაობის ჩაშლისთვის - ბომბების, რაკეტების და სხვა ასაფეთქებელი მოწყობილობების გარეშე. ამერიკის ცენტრალურმა სადაზვერვო სამსახურმა გაზსადენის აფეთქება გამოიწვია კომპიუტერული

[13] Uhde A. A short history of computer viruses, Sentrian Pty Ltd, 2017, p 1. https://www.sentrian.com.au, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

[14] Long T. "July 26, 1989: First Indictment Under Computer Fraud Act", Media News Company - Wired, 2011, p 1. https://www.wired.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

[15] Rubens P. Common Types of Ransomware, Internet Website e Security Planet, 2017, p 1. https://www.esecurityplanet.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

სისტემის კოდის გამოყენებით. აფეთქება ისეთი მასშტაბის იყო, კოსმოსიდანაც ჩანდა.[16]

1999 წელს **Microsoft Windows 98** გამოვიდა, მსოფლიო მასშტაბით ხელმისაწვდომი გახდა სრულიად ახალი თაობის ტექნოლოგია. კომპიუტერის მოხმარების ზრდამ ხელი შეუწყო პროგრამული უზრუნველყოფისა და უსაფრთხოების სისტემების გავრცელებას. **„ვინდოუსმა“** გამოუშვა მრავალი პატჩი და კომერციული პროდუქტები. გარდა ამისა, ბევრმა კომპანიამ გამოუშვა ანტიჰაკერული პროგრამა სახლის კომპიუტერის გამოყენებისთვის.[17]

რა ვითარება გვაქვს დღეს და რა პრობლემების წინაშე დაგვაყენა ტექნოლოგიურმა რევოლუციამ? კაცობრიობას თავის დამშვიდების უფლება არ აქვს - ფაქტია, რაც უფრო მეტ სიმაღლეებზე ავა კომპიუტერული ტექნოლოგიები, მით მეტი საშიშროება შეიქმნება **კიბერდამნაშავეების** მხრიდან. თემის კვლევისას კიბერომი, როგორც მოვლენა, აუცილებლად უნდა დავყოთ რამდენიმე მიმართულებად: **პირველი** - ტექნოლოგიური მიღწევების ათვისება-გამოყენება; **მეორე** - პროპაგანდისტული მეთოდების დამუშავება-გამოყენება.

ამ მხრივ ყველაფერი ხელის გულზე დევს, კიბერშეტევები ყოველწლიურად იზრდება და იხვეწება, ჯერ კიდევ 2006 წელს **რუსეთის ბიზნესქსელმა (RBN)** დაიწყო მავნე პროგრამების გამოყენება პირადობის ქურდობისთვის, 2007 წლიდან **RBN**-ი მთლიანად მონოპოლიზირდა პირადობის ონლაინ ქურდობაში. 2007 წლისთვის მათი ვირუსი სახელწოდებით - **„შტორმი ჭია“** მუშაობდა დაახლოებით ერთ მილიონ კომპიუტერზე და ყოველდღე გზავნიდა მილიონობით ინფიცირებულ ელ-წერილს. 2008 წელს კიბერშეტევები პერსონალური კომპიუტერიდან სამთავრობო ინსტიტუტების სისტემებზე გადავიდა. 2008 წლის 27 აგვისტოს **NASA**-მ

[16] Vidisha J. America's Hidden Stories' tackles CIA's alleged involvement in the Trans-Siberian Pipeline explosion of 1982, Media Entertainment Arts WorldWide, 2019, p 1. https://meaww.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

[17] Thurrott P. Windows 98 rockets to 1998 sales of 25 million, News Media IT Pro Today, 1999, p 1. https://www.itprotoday.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

დაადასტურა, რომ საერთაშორისო კოსმოსურ სადგურში ლეპტოპებზე **„შტორმ ჭია“** იყო ნაპოვნი.

დაზუსტებით არ შეგვიძლია ვთქვათ, მაგრამ სამი თვის შემდეგ **პენტაგონის** კომპიუტერები, სავარაუდოდ, რუსმა ჰაკერებმა გატეხეს. შემდეგ იყო ფინანსური ინსტიტუტები, 2008 წლის 25 დეკემბერს მოხდა თავდასხმა ინდოეთის სახელმწიფო ბანკზე.[18]

რუსეთი ახორციელებდა და დღესაც ახორციელებს როგორც საქართველოს, ასევე უკრაინის წინააღმდეგ სამხედრო და კიბერომის შერწყმულ თავდასხმებს, იყენებს ჰიბრიდული ომის სხვადასხვა კომპონენტებს. კრემლს საბჭოთა მეთოდოლოგია არ შეუცვლია, შეცვალა მხოლოდ ტექნოლოგიები. თუ საკითხს განვიხილავთ რუსეთის მიერ ჩადენილი და ჯერ კიდევ "ჩაუდენელ" დანაშაულთა ჭრილში, ალბათ, ყველა აღიარებს, რომ ამ მხრივ საქმე გვაქვს არაპროგნოზირებად სახელმწიფოსთან. მიუხედავად ამისა, მსოფლიოს წამყვანი ქვეყნები ვალდებულნი არიან, ამ არაპროგნოზირებადი ქვეყნის ქმედება ერთიან სისტემაში მოაქციონ და წინააღმდეგობა გაუწიონ.

ჩვენი მსჯელობა რუსეთთან მიმართებაში უფრო საფუძვლიანი, რომ იყოს, მაგალითად შეგვიძლია მოვიყვანოთ - 2008 წლის რუსეთ-საქართველოს ომი, როდესაც ყველაზე მასშტაბური კიბერშეტევა განხორციელდა რუსეთის მხრიდან საქართველოს სახელმწიფო, სატელევიზიო და საინფორმაციო სააგენტოების ვებ-გვერდებზე. **(რუსეთ-საქართველოს ომი და მისი შედეგები, ვრცლად გვაქვს განხილული III თავის, 3.2. ქვეთავში)** ასეთი მაგალითი 2014 წელს რუსეთ-უკარინის ომთან მიმართებაშიც შეგვიძლია მოვიყვანოთ, სადაც სამხედრო ომს თან სდევდა ჰიბრიდული ომის სხვადასხვა კომპონენტები, ე.წ. ამოუცნობი ტიტუშკების გამოყენება და კიბერშეტევები სამთავრობო უწყებებზე. რამდენიმე წლის შემდეგ, კერძოდ 2017 წელს, უკრაინის მინისტრთა კაბინეტის შიდა სისტემა ჰაკერების

[18] Sciarrone M. Cyber Warfare: The New Front, George W. Bush Institute, 2017, p 1. https://www.bushcenter.org, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

თავდასხმის მსხვერპლი აღმოჩნდა, ამის შესახებ უკრაინის ვიცე-პრემიერმა, **პაველ როზენკომ „ტვიტერზე“** დაწერა და სურათიც გამოაქვეყნა:

„როგორც ჩანს, უკრაინის მინისტრთა კაბინეტის სამდივნო ჰაკერების თავდასხმის ობიექტი გახდა, ქსელი ამჟამად გაჩერებულია“.[19]

ამ დროს არა მხოლოდ უკრაინის მინისტრთა კაბინეტი იყო ჰაკერების თავდასხმის ობიექტი, არამედ შეფერხებით მუშაობდა ენერგოკომპანიები და ეროვნული ბანკი. კიბერშეტევის მსხვერპლი იყო მედიაჰოლდინგი **„ლუქსი“**, კიევის მეტროპოლიტენი, უკრაინის ფოსტა, ახალი ფოსტა და სხვა. სამიზნეებს შორის იყო ბორისპოლის აეროპორტის სისტემაც, რის მეშვეობითაც შესაძლებელია ავიარეისების შეყოვნება.

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.

[19] Perlroth N., Scott M., Frenkel S., Cyberattack Hits Ukraine Then Spreads Internationally, The New York Times, 2017, p 1. https://www.nytimes.com, უკანასკნელად იქნა გადამოწმებული: 05.08.2020.

განიხილება თუ არა კიბერშეტევა ომის წარმოებად? ეს დამოკიდებულია მრავალ ფაქტორზე - რას აკეთებენ, როგორ აკეთებენ და რა ზიანს აყენებენ სამიზნე ობიექტს. შეტევების კვალიფიკაცია უნდა იყოს მნიშვნელოვანი მასშტაბისა და სიმძიმის. ინდივიდი ჰაკერების, ან ჰაკერთა ჯგუფის თავდასხმები არ ითვლება კიბერომად, თუ სახელმწიფო არ ეხმარება ან არ ხელმძღვანელობს. მიუხედავად ამისა, ვირტუალურ სამყარო კიბერშეტევების მიმართულებით მაინც ბუნდოვნად არის წარმოდგენილი. არსებობენ სახელმწიფოები, რომლებიც მხარს უჭერენ ჰაკერებს დამაზიანებელი ქმედებების განხორციელებაში, ეს საშიში, მაგრამ ჩვეულებრივი ტენდენციაა.

მაგალითად, კიბერთაღლითები, რომლებიც ფულის მოპარვისას ბანკის კომპიუტერულ სისტემებს ანადგურებენ, ეს ქმედება არ მიიჩნევა კიბერომად, თუნდაც ისინი სხვა ქვეყნის წარმომადგენლები იყვნენ, მაგრამ სახელმწიფოს მიერ მხარდაჭერილი ჰაკერები იგივე საქმეს აკეთებენ სხვა ქვეყნის ეკონომიკის დესტაბილიზაციის მიზნით.

ასევე არის განსხვავება სამიზნე ობიექტსა და მასშტაბს შორის: ინდივიდუალური კომპანიის ვებგვერდის გაფუჭება კიბერომად არ მიიჩნევა, მაგრამ საჰაერო ბაზაზე სარაკეტო თავდაცვის სისტემების მწყობრიდან გამოყვანა აღიქმება კიბერომად. ამ შემთხვევაში მნიშვნელოვანია, თუ რა იარაღს იყენებს თავდამსხმელი. მაგალითად, მონაცემთა ცენტრისთვის რაკეტის სროლა კიბერომად არ ჩაითვლება, თუნდაც მონაცემთა ცენტრი შეიცავდეს მთავრობის საიდუმლო ჩანაწერებს. ჰაკერების გამოყენება ჯაშუშობისთვის ან მონაცემების მოპარვის მიზნით კიბერომს არ გულისხმობს და ეს კიბერჯაშუშობის კვალიფიკაციით განისაზღვრება. კიბერომთან მიმართებაში ბევრი ბნელი ხვრელია, მაგრამ ყველა შეტევის კიბერომად მიჩნევა შეუძლებელია.[20]

[20] Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict, Information Technology Company ZDnet, 2018, p 1. https://www.zdnet.com, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.

მიუხედავად იმისა, რომ ამ მიმართულებით არსებობს განსხვავებული მოსაზრებები, თუ როგორ უნდა განისაზღვროს **„კიბერომი“,** როგორც ტერმინი, დღეს ბევრ ქვეყანას, მაგალითად, ამერიკის შეერთებულ შტატებს, რუსეთს, ბრიტანეთს, ინდოეთს, პაკისტანს, ჩინეთს, ისრაელს, ირანის ისლამურ რესპუბლიკას და ჩრდილოეთ კოერას უკვე გააჩნიათ კიბერ შესაძლებლობები, როგორც შეტევითი, ასევე თავდაცვითი ოპერაციებისთვის.

კიბერომი საერთაშორისო კონფლიქტების სულ უფრო გავრცელებული და საშიში მოვლენა ხდება. ის ფაქტი, რომ კიბერომის მკაფიო წესები არ არსებობს, ნიშნავს იმას, რომ შეიძლება უახლოეს მომავალში ვირტუალური სივრცე უკონტროლო გახდეს. კიბერომის დროს უმეტესწილად მხოლოდ კომპიუტერული სისტემები არ არის საბოლოო სამიზნე, ის მიზნად ისახავს რეალურ სამყაროში ინფრასტრუქტურის მართვას, მაგალითად, აეროპორტების, ელექტროქსელების, ვინაიდან, ასეთი ინფრასტრუქტურა ყველა ქვეყნისთვის მნიშვნელოვანია. ღილაკზე ერთი თითის დაჭერით შეიძლება დახურონ აეროპორტები, მეტროსადგურები ან შეწყვიტონ ელექტროენერგიის მიწოდება.

კიბერომის უამრავი სცენარი არსებობს. ჩვენ ისეთ ეპოქაში ვცხოვრობთ, შეიძლება ერთ დღეს გაიღვიძოთ და საბანკო ანგარიშები განულებული დაგხვდეთ, რადგან ვიღაც ჰაკერმა მოინდომა ასე. მასობრივი თავდასხმების შემთხვევაში კი შესაძლებელია, ნებისმიერ ქვეყანაში გამოიწვიონ ქაოსი.

არსებობს კიბერომის სამი ძირითადი მეთოდი: დივერსია, ელექტრონული ჯაშუშობა, ანუ კომპიუტერებიდან ინფორმაციის მოპარვა ვირუსების საშუალებით და ელექტროენერგიის ქსელებზე თავდასხმა. მესამე, ალბათ, ყველაზე საგანგაშოა, **რომელიც კრიტიკულ ინფრასტრუქტურაზე კიბერშეტევას გულისხმობს.**[21]

[21] Gartzke E. Making Sense of Cyberwar, Harvard Kennedy School Belfer Center for Science and International Affairs, 2014, p 1. https://www.belfercenter.org, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.

მთავრობები უფრო და უფრო აცნობიერებენ, რომ თანამედროვე საზოგადოება ძალიან არის დამოკიდებული კომპიუტერულ სისტემებზე - დაწყებული ფინანსური მომსახურებით, დამთავრებული სატრანსპორტო ქსელებით. აქედან გამომდინარე, ჰაკერების მიერ ვირუსებით ან სხვა საშუალებების გამოყენებით, ამ სისტემების გაჩერება შეიძლება ისეთივე ეფექტური და საზიანო იყოს, როგორც ტრადიციული სამხედრო კამპანია შეიარაღებული ძალების გამოყენებით, იარაღით და რაკეტებით.

ტრადიციული სამხედრო თავდასხმებისგან განსხვავებით, კიბერშეტევა შეიძლება განხორციელდეს ნებისმიერი მანძილიდან. ისიც შესაძლებელია, რომ არავითარი კვალი არ დარჩეს და მტკიცებულება საერთოდ არ არსებობდეს. მთავრობები და სადაზვერვო სააგენტოები შიშობენ, რომ ციფრული შეტევები კრიტიკული ინფრასტრუქტურის წინააღმდეგ, საბანკო სისტემებზე ან ენერგეტიკულ ქსელებზე, თავდამსხმელებს საშუალებას მისცემს, გვერდი აუარონ ქვეყნის ტრადიციულ თავდაცვას. ამიტომ ყველა ქვეყანა ისწრაფვის კომპიუტერული უსაფრთხოების გაუმჯობესებისკენ.

2012 წელს ირანის ისლამური რესპუბლიკის ხელისუფლების მიერ დაქირავებულმა ჰაკერებმა ნიუ-იორკში ბოუმენის ავენიუს კაშხალზე სრული კონტროლი მოიპოვეს. კრიტიკულ ინფრასტრუქტურაზე კიბერშეტევის ყველაზე გახმაურებული მაგალითია **“Stuxnet”** კომპიუტერული ვირუსით თავდასხმა, რომელმაც ირანის ბირთვული პროგრამა შეაჩერა, ვირუსმა ბირთვული მასალის გამოყოფისთვის გამოყენებული ცენტრიფუგები გაანეიტრალა. ამ ინციდენტმა დიდი შეშფოთება გამოიწვია, რადგან **“Stuxnet”-ზე** ეჭვობდნენ, რომ შეიძლება ადაპტირებული ყოფილიყო **“SCADA”** სისტემებზე თავდასხმისთვისაც. **“SCADA”** სისტემებს იყენებს მრავალი კრიტიკული ინფრასტრუქტურა და საწარმო ინდუსტრია ევროპასა და აშშ-ში.

ასეთი თავდასხმა 2014 წელს გერმანიაში დაფიქსირდა, რომელმაც ფოლადის ქარხანას დიდი ზიანი მიაყენა - კიბერშეტევამ გამოიწვია

ღუმელების გათიშვა. თავდამსხმელებმა გამოიყენეს სოციალური ინჟინერიის ტექნიკა.[22]

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

[22] Lohrmann D. How Vulnerable Is Critical Infrastructure to a Cyberattack?, Governament Technology, 2020, p 1. https://www.govtech.com, უკანასკნელად იქნა გადამოწმებული: 05.08.2020.

საფრთხის წინაშე. როდესაც კიბერომის ტრანსფორმაციის ახსნას ვცდილობთ, აუცილებლად უნდა გამოვყოთ, თუ რა ცვლის ამ ყველაფერს. ეს უმეტესად კიბერთავდასხმების ტექნოლოგიების დახვეწას და მავნებლური ჰაკერული სტრატეგიების, პროგრამებისა თუ ვირუსების შექმნას უკავშირდება. აქედან გამომდინარე, უნდა გამოვყოთ შეტევის ტიპები: **არსებობს პასიური და აქტიური კიბერშეტევები, პასიური შეტევა** გულისხმობს ტრაფიკის ანალიზს და დაუცველი კომუნიკაციების მონიტორინგს. **აქტიური შეტევის** დროს ჰაკერი დაცულ სისტემებს უტევს. ეს უმეტესწილად ვირუსებით ხორციელდება.[23]

გამოვყოფთ რამდენიმე ყველაზე გავრცელებულ კიბერშეტევების და „**Malware**“ ანუ მავნე კოდის შეტევების ტიპებს, **რომლის საშუალებითაც აქტუალურად ახორციელებენ ჰაკერები თავდასხმებს:**

Denial-of-service (DoS)	**ამ შეტევის დროს დიდი რაოდენობის გამოუსადეგარი ტრაფიკი იგზავნება და ქსელი მწყობრიდან გამოდის. მომხმარება იმ დროს ფერხდება, ანუ წყდება, როდესაც ვებ-სერვერი ივსება და ლეგიტიმურ მოთხოვნებს აღარ პასუხობს.**
distributed denial-of-service (DDoS)	**შეტევის დროს რამდენიმე ჰაკერი ან გატეხილი სისტემა აკეთებს ბევრ მოთხოვნას ვებ-სერვერზე და გამოუსადეგარი ტრაფიკით ბლოკავს სერვისს. კოორდინირებულ შეტევას დიდი ზიანის მოტანა შეუძლია.**
Man-in-the-middle (MitM)	**როდესაც ვიღაც ერევა და აკონტროლებს თქვენი კომუნიკაციის პროცესს, თქვენ გგონიათ, ესაუბრებით ნაცნობ ადამიანს, ან გაქვთ სერვერთან უშუალ წვდომა, მაგრამ ამ დროს, ყველა თქვენს პირად ინფორმაციას ხედავს ჰაკერი.**
Phishing	**თავდამსხმელი ქმნის რეალური ვებ-გვერდის კლონს, მიზანში ამოღებულ მომხმარებელს ელ-ფოსტაზე უგზავნის ყალბი ვებ-გვერდის ბმულს, თუ მომხმარებელი გადავა ამ ბმულზე და**

[23] Digiacomo J. Active vs Passive Cyber Attacks Explained, Intellectual Property Lawyer Revision Legal, 2017, p 1. https://revisionlegal.com, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.

	შეიყვანს პირად მონაცემებს, ჰაკერი მიიღებს წვდომას ამ მონაცემებზე.
War Drive	უკაბელო კომპიუტერულ ქსელებში შესვლის მოპოვების მეთოდი, მაგალითად, ლეპტოპი, ანტენები და უკაბელო ქსელის ადაპტერი, რომელიც გულისხმობს უნებართვო წვდომის მიღებას.
Password	პაროლების მოპოვება ჩვეულებრივი და ეფექტური შეტევის მეთოდია. ეს შეიძლება გაკეთდეს შემთხვევითი ან სისტემატური გზით.

ცხრილი 1 - კიბერშეტევების ტიპები

Malware attack - მავნე კოდის შეტევა:

არასასურველი პროგრამა, რომელიც თქვენი თანხმობის გარეშე სისტემაში არის გაშვებული, მას შეუძლია, ლეგიტიმურ კოდს დაერთოს და გამრავლდეს. ასევე შეუძლია, სხვადასხვა პროგრამებში გამრავლება, ან ინტერნეტთან ინტერპრეტაცია. აღსანიშნავია, რომ ყველა ვირუსი არის **Malware.** თუმცა ყველა **Malware** არ არის ვირუსი, შეიძლება იყოს პროგრამა, აპლიკაცია და ასე შემდეგ, რომელიც ჰაკერს აძლევს უფლებას, ჰქონდეს უნებართვო წვდომა პირად მონაცემებზე.[24]

გამოვყოფთ მავნე კოდის შეტევის რამდენიმე აქტუალურ ფორმას:

Ransomware	სისტემაში არსებულ ფაილებს შიფრავს და დროებით მიუწვდომელს ხდის, ამ თავდასხმის შემთხვევაში ჰაკერები ინფორმაციის დაბრუნების სანაცვლოდ გამოსასყიდს ითხოვენ.
Logic bombs	ის შეიძლება იყოს პროგრამული უზრუნველყოფის ნაწილი, რომელიც გარკვეული თარიღის დადგომის შემდეგ

[24] Zamora W. 10 easy ways to prevent malware infection, Software Company Malwarebytes, 2016, p 1. https://blog.malwarebytes.com, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.

	იქცევა ზიანის შემცველ პროგრამად.
Trojan horse	იმალება სასარგებლო პროგრამაში. მას ჩვეულებრივ აქვს დამაზიანებელი ფუნცია. ჰაკერს შეუძლია, ვირუსი გამოიყენოს მოსასმენად და თავდასხმების განსახორციელებლად.
Worm	დამოუკიდებელი კომპიუტერული პროგრამა, რომელიც ქსელში თავად მრავლდება ერთი სისტემიდან მეორეზე.

ცხრილი 2 - მავნე კოდის შეტევების ტიპები.

ჩვენი კვლევის საფუძველზე და წარმოდგენილი ჩამონათვალით, კიბერშეტევების სამიზნე ჯგუფის სამ კატეგორიას გამოვყოფთ - ესენია:

მიზნობრივი შეტევები აპარატურაზე (კინეტიკური)	მიზნობრივი შეტევები პროგრამულ უზრუნველყოფაზე (დაჰაკვა)	მიზნობრივი შეტევები ადამიანებზე (ჯაშუშობა-შპიონაჟი)
Denial of Service (DoS), Distributed DoS	Ransomware, Logic Bombs, Trojan, Worm	Phishing, Trojan

ცხრილი 3 - კიბერშეტევების სამიზნე ჯგუფების კატეგორიები

როგორც ხედავთ, თავდამსხმელებს აქვთ მრავალი ვარიანტი, რათა შეეცადონ, უნებართვო წვდომა მოიპოვონ კრიტიკულ ინფრასტრუქტურაზე და მნიშვნელოვან მონაცემებზე. ამიტომ სახელმწიფოები ქმნიან სამართლებრივ ნორმებს ტექნოლოგიური უსაფრთხოების უზრუნველყოფის მიზნით. კიბერშეტევები ისტორიულად არ იყო ისეთი დამაზარალებელი, როგორიც დღეს. არსებობს უამრავი სტატისტიკური მონაცემები ფაქტებზე დაყრდნობით, რაც ადასტურებს ჩვენს მოსაზრებებს.

მსოფლიოს წამყვანი სამეცნიერო-საკონსულტაციო კომპანია „Gartner"-ი ასაჯაროებს მონაცემებს კიბერუსაფრთხოების ხარჯებთან დაკავშირებით, ამ მონაცემებში შედარებულია და განხილულია 2017-2019 წლის მსოფლიო კიბერუსაფრთხოების დანახარჯი სეგმენტის მიხედვით.

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	**101,544**	**114,152**	**124,116**

ცხრილი 4 *- მსოფლიოს წამყვანი სამეცნიერო-საკონსულტაციო კომპანია „Gartner“-ის 2017-2018-2019 წლის მონაცემები კიბერუსაფრთხოების ხარჯებთან დაკავშირებით*

წყარო: *https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019*

ცხრილში ვხედავთ, ***(ცხრ. 4)*** რომ კიბერუსაფრთხოების კუთხით, მსოფლიო მასშტაბით, ძალიან დიდი თანხები იხარჯება და ყოველწლიურად იზრდება. მაგალითად, 2017 წელს დანახარჯი შეადგენდა 101.544 მილიარდ დოლარს, 2018 წელს 114,152 მილიარდ დოლარამდე გაიზარდა, ხოლო 2019 წელს 124,116 მილიარდ დოლარს მიაღწია.[25] ასევე **“Gartner“**-ის ინფორმაციით, 2022 წელს მსოფლიო კიბერუსაფრთხოების ხარჯები 133.7 მილიარდ აშშ დოლარს მიაღწევს.[26] თუმცა აქ საყურადღებოა შემდეგი ფაქტი, რომ მსოფლიოსთვის მიყენებული ზარალი ბევრად აღემატება უსაფრთხოებისთვის დახარჯულ თანხებს, **„Cybersecurity Ventures”**-ის ანგარიშში ნავარაუდებია, რომ 2021 წლისთვის კიბერშეტევებისგან

[25] Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, Consulting Agency Gartner, 2018, p 1. https://www.gartner.com, უკანასკნელად იქნა გადამოწმებული - 07.08.2020.

[26] Sobers R. 110 Must-Know Cybersecurity Statistics for 2020, Software Company Varonis, 2020, p 1. https://www.varonis.com, უკანასკნელად იქნა გადამოწმებული - 07.08.2020.

მიყენებული ზარალი 6 ტრილიონი აშშ დოლარი იქნება, რაც 2015 წელს 3 ტრილიონ აშშ დოლარს შეადგენდა.[27]

ეს კი ნიშნავს იმას, რომ კიბერომების და კიბერშეტევების ტენდენცია ბოლო დროს მასშტაბურ სახეს იძენს და განიციდის ტრანსფორმაციას. **რუსეთს** აქვს დიდი შესაძლებლობები კიბერომის თვალსაზრისით და არაერთი ეჭვი და მოვლენა ადასტურებს ამას. რუსეთმა გამოიყენა კიბერიარაღი საქართველოზე 2008 წლის ომის დროს, ასევე 2019 წელს იგივე მეთოდით კიბერშეტევები განახორციელა საქართველოს სამთავრობო უწყებების ვებ-გვერდებზე და სატელევიზიო ინფრასტრუქტურაზე. როგორც უცხოური მედია იუწყება, 2020 წლის გაეროს უშიშროების საბჭოს დახურულ სხდომაზე ამერიკის შეერთებულმა შტატებმა, ბრიტანეთმა და ესტონეთმა აღნიშნული ფაქტი შეაფასეს როგორც რუსეთის მხრიდან წარმოებული კიბერშეტევა. იგივე ხელწერა შეინიშნება 2014 წლის დასაწყისში უკრაინაზე თავდასხმისას.[28]

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. ამ ტიპის

[27] Morgan S. Cybersecurity Ventures - 2017 Cybercrime Report, Canada, Herjavec Group, 2015, pp 3-4.

[28] Evansky B. US, UK and Estonia call out Russia over cyber attacks against Georgia in UN Security Council first, Fox News Channel, 2020, p 1. https://www.foxnews.com, უკანასკნელად იქნა გადამოწმებული - 07.08.2020.

განსაზღვრებები მნიშვნელოვანია კიბერომთან დაკავშირებული საკითხების მოგვარებისას, რაც ხან კინეტიკურ, ხან არაკინეტიკურ თავდასხმებს გულისხმობს. ზევით უკვე განვიხილეთ კიბერშეტევისა და კიბერომის განსხვავებაზე - მსოფლიო მასშტაბით მრავალი მცდელობა იყო, ზუსტად განესაზღვრათ კიბერომის არსი კონცეპტუალურ დონეზე, მაგალითად ნატოს „კიბერთავდაცვის სფეროში თანამშრომლობის უნარების ცენტრის“ ხელმძღვანელობით შეიქმნა **„ტალინის სახელმძღვანელო“** - სადაც საერთაშორისო სამართლის კანონების მიხედვით არის განხილული კიბერომებში გამოყენებული კანონდარღვევები. თუმცა იგი არ წარმოადგენს ნატოს პოლიტიკურ, ოფიციალურ დოკუმენტს. ამ შემთხვევაში სირთულე ის არის, რომ ნაციონალური სახელმწიფოები და არასახელმწიფო აქტორები ყოველთვის არ იცავენ კანონებს. ვფიქრობთ **„ტალინის სახელმძღვანელოში“** ზოგიერთი თემა ზოგადი, ზედაპირული და კიბერსივრცის თეორიულ განმარტებებთან შეუთავსებელია, საჭიროებს დახვეწას. მაგალითად, **„ტალინის სახელმძღვანელოში“,** კიბერომი გაიგივებულია კიბერშეტევასთან - ნათქვამია, რომ ის წარმოადგენს შეტევით ან თავდაცვით ოპერაციას, რომელმაც შეიძლება გამოიწვიოს ადამიანის სიკვდილი, დაზიანება ან ობიექტების განადგურება.[29]

ჩვენი აზრით, აღნიშნული დეფინიცია გამორიცხავს ფსიქოლოგიურ ზეწოლას კიბეროპერაციების დროს, ან კიბერდაზვერვას. ამ განმარტების მთავარ ნაკლს კი წარმოადგენს კიბერომის და კიბერშეტევის ერთ ტერმინად განხილვა. ასევე, აღნიშნული განსაზღვრება გამორიცხავს კიბეროპერაციებს, რომლებიც შეიძლება მიზნად ისახავდეს სახელმწიფოების ფინანსურ სისტემაზე დესტაფილიზაციის განხორციელებას. ამ შემთხვევაში კიბერთავდასხმას სიკვდილი ან ფიზიკური განადგურება არ მოჰყვება.

როდესაც კიბერომის კონცეფციაზე ვსაუბრობთ და უსაფრთხოების საკითხს ვეხებით, აუცილებლად უნდა განვიხილოთ ჩრდილოატლანტიკური

[29] Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict, Information Technology Company ZDnet, 2018, p 1. https://www.zdnet.com, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.

ალიანსის კონტექსტში - უსაფრთხოება და კიბერთავდაცვა უშუალოდ უკავშირდება ნატოს. კიბერთავდასხმებისგან თავდაცვის განმტკიცების აუცილებლობა ნატოში გაწევრიანებულმა ქვეყნებმა პირველად 2002 წელს პრაღაში გამართულ სამიტზე განიხილეს. მას შემდეგ კიბერუსაფრთხოება გახდა ნატოს დღის წესრიგის მნიშვნელოვანი კომპონენტი. 2008 წელს მიიღეს პირველი კიბერთავდაცვის პოლიტიკური დოკუმენტი. 2012 წლიდან დღემდე აქტიურად მიმდინარეობს ნატოს თავდაცვის სისტემაში კიბერუსაფრთხოების ინტეგრაციის პროცესი. 2014 წელს **უელსის სამიტზე** მოკავშირეებმა კიბერთავდაცვა კოლექტიური თავდაცვის ძირითადი ნაწილი გახადეს და განაცხადეს, რომ კიბერშეტევამ შეიძლება გამოიწვიოს ნატოს ხელშეკრულებაში განსაზღვრული კოლექტიური თავდაცვის მე-5 მუხლის გამოყენება. 2016 წელს **ვარშავის სამიტზე** ალიანსის წევრმა ქვეყნებმა ინფორმაციული და საკომუნიკაციო ქსელის უსაფრთხოება ერთ-ერთ ძირითად თავდაცვით სფეროდ აღიარეს და შეთანხმდნენ, რომ კიბერსივრცეში **ნატომ** ისევე ეფექტურად უნდა დაიცვას თავი, როგორც ხმელეთზე, ზღვასა და ჰაერში. კიბერუსაფრთხოების სფეროში **ნატოს** ძირითადი პარტნიორია **ევროკავშირი**, რომელთანაც ალიანსმა 2016 წლის თებერვალში **ურთიერთდახმარებისა და თანამშრომლობის ტექნიკური ხელშეკრულება გააფორმა.**[30]

მთავარი საკითხები, რაც **ვარშავის სამიტზე** განიხილეს, ეს იყო, როგორ უნდა გამოყოფილიყო კიბერუსაფრთხოებასთან დაკავშირებით რესურსები საუკეთესო ეფექტის მისაღწევად - აღიარეს, რომ ამ პრობლემის მოსაგვარებლად დიდი რესურსები იყო საჭირო. ასევე, კითხვები იყო იმასთან დაკავშირებით, თუ რა თანხა უნდა დახარჯულიყო, რა იქნებოდა ინვესტიციის მინიმალური დონე? მაგალითად, 2014 წლიდან, საფრანგეთში **"Pacte Défense Cyber"-ის** ბიუჯეტი მოიცავდა 1 მილიარდ ევროს კიბერთავდაცვისთვის. 2016 წელს დიდმა ბრიტანეთმა გამოაცხადა, რომ

[30] Karasev P. NATO's Cyber Defense Evolution - NATO's New Digital Wall, Russian Council RIAC, 2016, p 1. https://russiancouncil.ru, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.

კიბერუსაფრთხოების პროგრამის გასამყარებლად 1,9 მილიარდი გირვანქა სტერლინგი გამოყო.[31]

2018 წელს **ბრიუსელის სამიტზე** მოკავშირეები შეთანხმდნენ ახალი კიბერსივრცის ოპერაციების ცენტრის შექმნაზე. საერთო გამოწვევების გათვალისწინებით, ნატო და ევროკავშირი აძლიერებენ თანამშრომლობას კიბერთავდაცვის სფეროში, განსაკუთრებით ინფორმაციის გაცვლაში. ტარდება ერთობლივი ტრენინგები და კვლევები.[32]

ცალკე აღსანიშნავია ამერიკის შეერთებული შტატების დამსახურება, რომელიც არ იშურებს ძალისხმევას, რათა შეიმუშაოს კიბერუსაფრთხოებასთან დაკავშირებით ახალი რეგულაციები და ასევე არ იშურებს თანხებს. აშშ-ის ბიუჯეტში კიბერუსაფრთხოებასთან დაკავშირებით ხარჯები ყოველწლიურად იზრდება, 2015 წელს **ბარაკ ობამას** ადმინისტრაციამ გამოყო 14 მილიარდი დოლარი ოფიციალურად, შემდეგ კი გაჩნდა ინფორმაცია, რომ დაიხარჯებოდა გაცილებით მეტი.[33] მსოფლიო მასშტაბით თავდაცვითი ხარჯები დღითი-დღე მატულობს, მაგრამ აშშ-ის ფინანსები შთამბეჭდავია. უკვე ცნობილია, რომ 2021 წლისთვის ეს სფერო 18,8 მილიარდი დოლარით დაფინანსდება.[34] ჯერ კიდევ 2007 წელს შეერთებული შტატების სამხედრო-საჰაერო ძალებში შეიქმნა კიბერსარდლობა, რომელმაც 2008 წლის ბოლომდე იარსება, შემდეგ

[31] Pennetier M. France to invest 1 billion euros to update cyber defences, Media News Reuters, 2014, p 1. https://www.reuters.com, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.

[32] Brussels Summit Declaration - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, NATO, 2018, p 1. https://www.nato.int, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.

[33] Kerr D. Obama asks for $14 billion to step up cybersecurity - The president urges Congress to pass legislation that would strengthen the country's hacking detection system and counterintelligence capabilities, Media News CNet, 2015, p 1. https://www.cnet.com, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.

[34] Department of Homeland Security Statement on the President's Fiscal Year 2021 Budget, Homeland Security, 2020, p 1. https://www.dhs.gov, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.

კი ეს ფუნქციები გადაეცა სამხედრო-საჰაერო ძალების კოსმოსურ სარდლობას.[35]

2011 წლის მაისში შეერთებულმა შტატებმა გამოაქვეყნა თავისი სტრატეგია კიბერსივრცის დაცვაზე, რომელსაც საფუძვლად უდევს საერთაშორისო პარტნიორებთან და კერძო სექტორთან თანამშრომლობის მოდელი. ღონისძიებები უნდა გატარდეს შვიდი მიმართულებით:

1. **ეკონომიკა** - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ღია და ლიბერალური ბაზარი;
2. **ეროვნული ქსელის დაცვა** - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა;
3. **სამართალებრივი მხარე** - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება;
4. **სამხედრო სფერო** - უსაფრთხოების თანამედროვე გამოწვევებზე მზადყოფნა;
5. **სამთავრობო ინტერნეტის ქსელი** - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება;
6. **საერთაშორისო განვითარება** - უსაფრთხოების ორგანიზება, საერთაშორისო კომპეტენციების განვითარება და ეკონომიკური აყვავება;
7. **თავისუფლება ინტერნეტში** - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა.[36]

რამდენი სახის კონცეფცია შეიძლება არსებობდეს დღევანდელ მსოფლიოში? გარდა იმისა, რომ მნიშვნელოვანი კონცეფციები გააჩნიათ აშშ-ს, ევროკავშირს, ნატოს, ყველა ქვეყანას აქვს საკუთარი სამოქმედო ეროვნული გეგმა, ყველაზე საყურადღებოდ მაინც 2010 წელს **ლისაბონის**

[35] ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., "მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო", ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018, გვ. 17-32.

[36] Inter National Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, The White House, 2011, pp 3-24. https://www.hsdl.org, უკანასკნელად იქნა გადამოწმებული - 10.08.2020

სამიტზე დამტკიცებული ახალი სტრატეგიული კონცეფცია[37] ითვლება, რომლის თანახმადაც ამერიკის შეერთებულმა შტატებმა ჩამოაყალიბა კიბერსარდლობა. ეს იყო პასუხი რუსეთის ქმედებებზე. **ვლადიმერ პუტინი** მოვიდა თუ არა ხელისუფლებაში, დაამტკიცა საინფორმაციო უსაფრთხოების ახალი დოქტრინა,[38] რომლის სტრატეგია იყო ის, რომ ხელისუფლებას მიანიჭა საინფორმაციო და მედიაქსელებზე კონტროლის უფლებები. **პუტინმა** ასევე ხელი მოაწერა საკანონმდებლო ცვლილებას - საგადასახადო პოლიციას, შინაგან საქმეთა სამინისტროს, კრემლის საპარლამენტო და საპრეზიდენტო დაცვის სამსახურებს, საზღვრის დაცვას და საბაჟო სამსახურს იგივე უფლებები მიენიჭა, რაც მხოლოდ უსაფრთხოების ფედერალურ სამსახურს ჰქონდა.

2017 წლის 18 დეკემბერს გამოქვეყნდა აშშ-ის პრეზიდენტის, დონალდ ტრამპის პირველი **„ეროვნული უსაფრთხოების სტრატეგია“,[39]** რომელიც საფუძვლად დაედო სტრატეგიულ დოკუმენტებს, როგორიცაა აშშ-ის თავდაცვის დეპარტამენტის **„ეროვნული თავდაცვის სტრატეგია“.** სტრატეგია ეფუძნება ოთხ მნიშვნელოვან ეროვნულ ინტერესს:

1. **ამერიკელი ხალხისა და ამერიკული ცხოვრების წესის დაცვა;**
2. **ამერიკის კეთილდღეობის ზრდა;**
3. **მშვიდობის შენარჩუნება;**
4. **ამერიკის გავლენის გაზრდა.**

საინტერესოა მე-3 თავი, რომლის სათაურია: **„ძალის მეშვეობით მშვიდობის შენარჩუნება“**, სადაც ორი სახელმწიფოს – რუსეთისა და ჩინეთის მიმართ პრეტენზიებია გამოთქმული:

„ამერიკის შეერთებული შტატებისათვის რუსეთი ეგზისტენციალურ საფრთხედ აღიქმება. რუსეთი ცდილობს, აღიდგინოს დიდი სახელმწიფოს

[37] Edited by Jens Ringsmose and Sten Rynning, NATO's New Strategic Concept: a Comprehensive Assessment, DIIS. Danish Institute for International Studies, Copenhagen, NATO, 2011, pp 23-43.
[38] Information Security Doctrine of The Russian Federation, Moscow: Russian Federation, 2000, pp 1-32.
[39] National Security Strategy, Washington: United States governments, 2017, pp 1-2.

სტატუსი და საზღვრების სიახლოვეს საკუთარი გავლენის სფეროები შექმნას. მის მიზანს აშშ-ის გავლენის შესუსტება, მოკავშირეებისა და პარტნიორების ჩამოცილება წარმოადგენს. ჩინეთიდან მომდინარე საფრთხედ აღიქმება ბირთვული არსენალისა და სამხედრო ძლიერების ზრდა, ასევე აშშ-ის ინდოეთისა და წყნარი ოკეანის რეგიონებიდან გაძევების სურვილი, რეგიონში წესრიგის ცვლილებისა და სასურველი ეკონომიკური წესების დამყარების მცდელობა“.[40]

სახელმძღვანელოში - **„კიბერ დრაკონი - ჩინეთის საინფორმაციო ომი და კიბერ ოპერაციები“,** რომლის ავტორიც გახლავთ მკვლევარი **დეკანი ჩენგი,** აღნიშნავს, რომ გასული საუკუნეების განმავლობაში ჩინეთის ლიდერებმა გაანალიზეს, რომ ყველაზე მნიშვნელოვანია ტექნოლოგიური განვითარება, რაც ხელს უწყობს ჩინეთს გლობალური მასშტაბით პოზიციების გაუმჯობესებას. მათ გააცნობიერეს ინფორმაციის კონტროლის მნიშვნელობა, როგორც ძალაუფლების შენარჩუნების ერთ-ერთი ძლიერი ელემენტი. **ჩენგი** ასევე ყურადღებას ამახვილებს ომის სახეობების განვითარებაზე:

„ტექნოლოგიების განვითარებამ, როგორც ეკონომიკასა და საზოგადოებაზე, ასევე ომის ბუნებაზე მოახდინა გავლენა. ისტორიულად ომი ვითარდებოდა, კაცობრიობამ ხმლები, შუბები და სხვა სახის „ცივი იარაღი“ განავითარა, ანუ შეცვალა თოფებით, ყუმბარებით, ავტომატებით და ა.შ. დღეს კი კაცობრიობა, ტექნოლოგიების განვითარების ხარჯზე „ცხელი იარაღიდან“ „რბილ ძალამდე“ მივიდა“.[41]

ამიტომ **აშშ-ის** ახალი სტრატეგიის მე-4 თავის სათაური პირდაპირ, დაუფარავად აცხადებს:

---

[40] "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", ამერიკის შეერთებული შტატების საელჩო საქართველოში, 2017, გვ. 1. https://ge.usembassy.gov, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.

[41] Cheng D. Cyber dragon, inside China s information warfare and cyber operations, United States: Publishing House Praeger, 2017, pp 79-82.

„ამერიკის გავლენის გაზრდა“, სადაც განსაკუთრებული აქცენტი კეთდება საერთაშორისო ინსტიტუტებში ამერიკის როლზე, გავლენასა და აქტიურ მონაწილეობაზე. იმ შემთხვევაში, თუ არსებული ინსტიტუტები და წესები საჭიროებენ მოდერნიზებას, შეერთებული შტატები უხელმძღვანელებს ამ პროცესს,“ – აღნიშნულია დოკუმენტში.[42]

როდესაც **დონალდ ტრამპის** სტრატეგიაში საუბარია ამერიკის გავლენის გაზრდაზე, აქვე თვალშისაცემია, თუ როგორ ფაქიზად უდგება თეთრი სახლი საერთაშორისო ურთიერთობებს, თუმცა ძნელი სათქმელია, რამდენად იქნება რეალური, როცა საქმე გვაქვს რუსეთთან, რომლისთვისაც პოლიტიკა და ეთიკა, პირობის შესრულება და სამართალი ძალიან შორსაა.

[42] "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", ამერიკის შეერთებული შტატების საელჩო საქართველოში, 2017, გვ. 1. https://ge.usembassy.gov, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.

თავი მეორე - კონფლიქტების ტრანსფორმაცია ახალი გეოპოლიტიკური წესრიგის პირობებში

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.[43]

პოლიტიკური რეალიზმის თეორიის მიმდევრების **პაულ დ. სენეზის** და **ჯონ ა. ვასქეზის (Paul D. Senese and John A. Vasquez)** მტკიცებით, არსებობს ფაქტორები, რაც ზრდის საფრთხეებს - მაგალითად სამხედრო შენაერთები,

[43] Karpowicz W. Political Realism in International Relations, Stanford Encyclopedia of Philosophy, 2017, p 1, https://plato.stanford.edu, უკანასკნელად იქნა გადამოწმებული - 16.08.2020.

კავშირები, გაერთიანებები, ალიანსები, ხშირად არაპროდუქტიულია და ზრდის კონფლიქტის ალბათობას.[44]

ამის მიუხედავად, უსაფრთხოების და კონფლიქტის საკითხებზე ფოკუსირებით, **რეალიზმი**, როგორც ჩანს, არის ბუნებრივი თეორია კიბერუსაფრთხოების მწვავე საკითხების გარკვევაში. ზოგადად, კიბერკონფლიქტის შესწავლა მაშინ დაიწყო, როდესაც **ჯონ არკილამ** და **დევიდ რონფელდტმა (John Arquilla, David Ronfeldt)** განავითარეს **"კიბერომის"** და **"ინტომის"** კონცეფციები და იწინასწარმეტყველეს ომის ტრანსფორმაცია **ICT**– ის სწრაფი წინსვლის შესაბამისად.[45]

რეალიზმის მიმდევრები, **ბრენდონ ვალერიანო** და **რაიან კ, მანესი (Brandon Valeriano and Ryan C. Maness)** საკითხს ასე განიხილავენ, კონფლიქტის ეს ფორმა ხდება **კიბერსივრცეში** და გულისხმობს "კიბერსივრცეში გამოთვლითი ტექნოლოგიების გამოყენებას ბოროტი ან/და დესტრუქციული მიზნებისთვის, სუბიექტებს შორის დიპლომატიური და სამხედრო ურთიერთქმედების გავლენის შეცვლის მიზნით".[46]

ჩვენ სწორედ ამ პოლიტიკურად მოტივირებულ ურთიერთობებზე ვამახვილებთ ყურადღებას, რადგან ისინი პირდაპირ გავლენას ახდენენ ეროვნულ უსაფრთხოებაზე. ერთობლივი სამხედრო შენაერთები ან ხელშეკრულებების დადება ხშირად აღიქმება საფრთხედ სხვა სახელმწიფოების მიერ, რომლებიც შემდეგ იღებენ მსგავს ზომებს საკუთარი უსაფრთხოების გასაძლიერებლად. ამ პროცესს ხშირად უწოდებენ სპირალურ მოდელს. სპირალური მოდელი წარმოადგენს ესკალაციას, რაც იწვევს ძალთა ბალანსის სწრაფ ცვლას, ასევე საერთაშორისო დაძაბულობის ზრდას და კონფლიქტების რისკს. კიბერდომენს არ გააჩნია ეფექტური გლობალური ინსტიტუციური მმართველობა.

---

[44] Senese D. P., Vasquez A. J., The Steps to War: An Empirical Study, United States: Princeton University Press, 2018, pp 11-20.

[45] Arquilla J., Ronfeldt D., Swarming and the Future of Conflic, Santa Monica: RAND National Defense Research Institute, 2000, pp 7-25.

[46] Valeriano B., Maness C. R., Cyber War versus Cyber Realities, New York: Oxford University Press, 2015, pp 2-31.

შესაბამის ორგანიზაციებში შედის საერთაშორისო სატელეკომუნიკაციო კავშირი (ITU) და მინიჭებული სახელების და ციფრების ინტერნეტკორპორაცია (ICANN), მაგრამ მათი ფუნქციები და კომპეტენციები არ ვრცელდება კონფლიქტების მართვაში. უსაფრთხოების დილემა უფრო მკაცრია, როდესაც თავდასხმითი და თავდაცვითი შესაძლებლობები ერთმანეთისგან არ განსხვავდება. ამ შემთხვევაში სახელმწიფოების მიერ კიბერუსაფრთხოების განვითარება და ფინანსების გაზრდა ტექნოლოგიების გაუმჯობესემისთვის, პოტენციურ საფრთხედ განიხილება. კიბერსივრცეში შესაძლებლობების გარჩევა რთულია. მეტიც, კიბერსამხედრო ორგანიზაციებს, როგორიცაა აშშ კიბერ სარდლობა, როგორც თავდაცვითი, ასევე შეტევითი როლი აქვთ და თუკი ამბობენ, რომ ბიუჯეტს ან პერსონალს ზრდიან, აშკარაა, რომ ეს როგორც თავდაცვითი, ასევე თავდასხმითი გაძლიერებაა, ეს კი ამძაფრებს გაურკვევლობას და კონკურენციას სახელმწიფოებს შორის - ისინი ეძებენ უსაფრთხოებას კიბერსივრცეში.

პოლიტიკური რეალიზმის კლასიკური გაგებით, შეიარაღების გაუმჯობესება ზრდის ომის ალბათობას, მაგრამ **ბარნი გლეიზერის (Barney Glaser)** აზრით, სამხედრო დანაზოგი რევიზიონისტული ძალაუფლების შეკავების აუცილებელი საშუალებაა,[47] ამ შემთხვევაში ისმება კითხვა: გადაიზრდება თუ არა უსაფრთხოების კონკურენცია რეალურ კონფლიქტში? გამოიწვევს თუ არა კიბერშეიარაღების გაზრდა ახალ კონფლიქტებს?

კრისტინ მ. ლორდი და ტრევის შარპი (Kristin M. Lord and Travis Sharp) ამტკიცებენ, კონფლიქტი კიბერსივრცეში ცალსახად არის განპირობებული ესკალაციისთვის.[48]

[47] Glaser B. Grounded Theory: The Philosophy, Method, and Work, Florida: BrownWalker Press, 2011, pp 175-187.

[48] Lord M. K., Sharp T., America's Cyber Future: Security and Prosperity in the Information Age, United States: Center for a New American Security, 2011, pp 7-9.

პოლიტიკური რეალიზმის თანახმად, ძალაუფლებას დიდი მნიშვნელობა ენიჭება, მას შეუძლია, უზრუნველყოს სახელმწიფოს დამოუკიდებლობა და გადარჩენა. როგორც **მორგენთაუ (Morgenthau 1948, 80-108)** ამბობს: "რაც არ უნდა იყოს საერთაშორისო პოლიტიკის საბოლოო მიზანი, ძალა ყოველთვის არის მისი უახლოესი თანმდევი."[49]

რეალისტები ხშირად ათანაბრებენ ძალაუფლებას სახელმწიფოს ქონებასთან - ბუნებრივი რესურსები, ინდუსტრიული შესაძლებლობები, სამხედრო შეიარაღება და მოსახლეობის რაოდენობა. მიუხედავად იმისა, რომ **რეალისტურ** ლიტერატურაში არ არსებობს **კიბერძალაუფლების თეორია,** ის მაინც გვთავაზობს ჩარჩოს აქტორებს შორის ძალაუფლების განაწილებაზე. საერთოდ, ინფორმაციული რევოლუცია ეჭვქვეშ აყენებს სახელმწიფოთა პირველობას, რადგან ხშირად არასახელმწიფო აქტორები ემუქრებიან ტრადიციული ძალაუფლების დინამიკას, ისინი დროთა განმავლობაში უფრო მნიშვნელოვანნი ხდებიან. თუმცა, როდესაც საქმე ეხება კიბერკონფლიქტს, სახელმწიფოები მაინც დომინანტები არიან.

არსებობს მოსაზრება, რომ კიბერსივრცესთან მიმართებაში, სუსტი სახელმწიფოები კიდევ უფრო აძლიერებენ ძლიერ სახელმწიფოებს და ახდენენ სისტემაში განაწილების კონფიგურაციას. მაგალითად, დიდი სკანდალი გამოიწვია ჩრდილოეთ კორეაში ათასობით ჰაკერის მომზადებამ, ასევე ჩინეთის აქტიურობამ, რომელიც ბრალდებულია **აშშ-ის** წინააღმდეგ მუდმივ კიბერჯაშუშურ კამპანიასა და **ირანის ისლამური სახალიფოს** კიბერომის ტაქტიკის დახვეწაში. ბუნებრივია, მოწინავე ქვეყნები ყველაზე მეტად არიან დამოკიდებულნი ციფრულ ინფრასტრუქტურაზე და შესაბამისად, ყველაზე დაუცველები არიან დამანგრეველი კიბერშეტევისგან.[50] თუმცა **ჯონ ლინდსი** ამტკიცებს, რომ მხოლოდ

[49] Rösch J. F. Hans J. Morgenthau, the "marginal man" in International Relations. A "Weltanschauungsanalyse", United Kingdom: Newcastle University School of Geography, Politics and Sociology, 2011, pp 9-18.

[50] Popescu N., Secrieru S., Hacks, leaks and disruptions Russian cyber strategies, Paris: European Union Institute for Security Studies, 2018, Chaillot paper №148, pp 53-75.

ტექნოლოგიურ ზესახელმწიფოს აქვს ყველაზე დახვეწილი კიბერშეიარაღების განვითარების შესაძლებლობა.[51]

კიბერსივრცე გახდა ახალი საერთაშორისო ბრძოლის ველი. ინტერნეტი შესანიშნავად ერგება უსაფრთხოების რეალისტურ მოდელს. ამ წყობაში ყველა სახელმწიფო არის მარტო ან თავის მოკავშირეებთან, რომლებსაც ვერასდროს ენდობა და ცდილობს, ააშენოს თავისი კიბერინდუსტრია და თავდაცვა იმის შიშით, რომ სხვა სახელმწიფოს მიერ განხორციელებული ყოველი გარღვევა პირდაპირ საფრთხეს უქმნის მათ უსაფრთხოებას. ამისი საუკეთესო მაგალითია რუსეთი, რომელსაც ჰყავს ე.წ. მოკავშირეები (ჩინეთი, ირანის ისლამური რესპუბლიკა), მაგრამ სინამდვილეში არავის ენდობა. ეს ქვეყანა უტევს ყველა სახელმწიფოს საკუთარი შოვინისტური ინტერესებიდან გამომდინარე.

21-ე საუკუნეში არსებობს საერთაშორისო სამართლის ნორმები. საერთაშორისო ორგანიზაციები პრობლემების მოგვარებას ცდილობენ ცივილიზებული მეთოდებით. დემოკრატიული ქვეყნები მოქმედებენ პრინციპით - თავისუფლება, სუვერენიტეტი, კანონი. კონფლიქტების მშვიდობიანად მოგვარება, ასევე თანაარსებობა არის დღევანდელი მსოფლიო წესრიგის არსი და საფუძველი, თუმცა ეს არ გამორიცხავს ომების შესაძლებლობას. ყველა სახელმწიფო ცდილობს ქვეყნის უსაფრთხოების უზრუნველყოფას და ამავე დროს მზად არის ომისთვის - **ეკონომიკური, ინფორმაციული, ბიოლოგიური და კიბერომისთვის.**

ბოლო დროის დაკვირვებები და მაგალითები გვიჩვენებს, რომ ნებისმიერ ქვეყანაზე ეკონომიკური ზეწოლა უფრო ადვილია, ვიდრე სამხედრო ლაშქრობა. ამის ნათელი მაგალითია აშშ-ისა და დიდი ბრიტანეთის მიერ სანქციების დაწესება კუბისთვის, სერბეთისა და ბელორუსისთვის, თუნდაც რუსეთისთვის სანქციების დაწესება ევროკავშირის მიერ. პოლიტიკური მიზნების მისაღწევად აღარ არის აუცილებელი საომარი მოქმედებების

[51] Lindsay R. J. The Impact of China on Cybersecurity, United States: the President and Fellows of Harvard College and the Massachusetts Institute of Technology, 2015, pp 1-3.

წარმოება. თუმცა მიზანსაც გააჩნია, თუ მიზანი ტერიტორიის ოკუპაცია ან ბუფერული ზონის შექმნაა, მაშინ შეიარაღებული ძალების გამოყენების გარეშე ეს ვერ მოხდება. ამ მხრივ გვაქვს მაგალითები უკრაინასა და საქართველოში., სადაც რუსეთმა სამხედრო ძალებით და კიბერომის დახმარებით მოახდინა ტერიტორიების ანექსია.

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.

საინფორმაციო-პროპაგანდისტული ომის ფენომენი ახალი არ გახლავთ, ის ისეთივე ძველი მეთოდია, როგორც ყველაზე უძველესი ხელობა. უბრალოდ იცვლებოდა და ალბათ მომავალშიც შეიცვლება (პროგრესირდება) ტექნოლოგიების განვითარებასთან ერთად. **პროპაგანდა** - გულისხმობს ნებისმიერი საკომუნიკაციო ფორმის გეგმაზომიერ გამოყენებას, ადამიანთა გონებაზე, ქცევასა და ემოციებზე ზემოქმედების მიზნით. ეს საშუალება ბევრი ადამიანის რაიმეში დარწმუნებისთვის ყველაზე ეფექტურ და გავრცელებულ საშუალებად მიიჩნევა, რომელსაც პოლიტიკურ საქმიანობას

უკავშირებენ. სადაზვერვო სამსახურები პროპაგანდას ისტორიულად დიდიხანია იყენებენ. **პროპაგანდისტული ომის** მთელი სიძლიერე გამოვლინდა **მეორე მსოფლიო ომის** პერიოდში და აქტუალურია დღემდე. ძნელი დასაჯერებელია, მაგრამ ფაქტია, როდესაც მეორე მსოფლიო ომი დასრულდა, გერმანიაში ძალიან ბევრი აცხადებდა: **„დიახ, ადოლფ ჰიტლერი დამნაშავეა, ცოტა გადააჭარბა, მაგრამ კარგი უფრო ბევრი გააკეთა, აღგვიდგინა ღირსება და დაგვიგო ავტობანები“.**[52] მეტიც, პოსტჰიტლერულ გერმანიაში იმდენად ძლიერი იყო **გებელსის** იდეოლოგიისა და პროპაგანდის გავლენა, რომ 1948 წელს **ნიურბერგის** სასამართლო პროცესებზე მოწმეები არ გამოდიოდნენ.[53] ომის დამთავრებიდან სამი წლის შემდეგაც კი ადამიანებს სჯეროდათ (ბევრს ეშინოდა), რომ ნაცისტები ხელისუფლებაში ისევ დაბრუნდებოდნენ. მაშინ არ იყო ინტერნეტი, არ იყო კომპიუტერი, მაგრამ იყო რადიო, იყო იდეოლოგია, იყო მოსახლეობაში გაჩაღებული აგიტაცია-პროპაგანდა, იყო ზეწოლა იარაღის ქვეშ. ამ მხრივ შეგვიძლია ვთქვათ, რომ რუსეთს დიდი საინფორმაციო, პროპაგანდისტულ-დეზინფორმაციული ისტორია აქვს, მაგრამ ტექნოლოგიური რევოლუციების ეპოქაში, ამ საქმიანობამ უფრო ეფექტური ხასიათი მიიღო. რუსული **პროპაგანდა** არ არის სიმართლეზე ორიენტირებული, თუმცა ეს არ ნიშნავს იმას, რომ ყველაფერი ტყუილია. აქ გვაქვს შერეული მეთოდი, როდესაც სიმართლეში შერეული დეზინფორმაცია ვრცელდება. არის შემთხვევები, როდესაც მთლიანად დეზინფორმაციასთან და **„ფეიკ-ნიუსთან“** გვაქვს საქმე. მაგალითად, 2014 წლის 11 სექტემბერს გავრცელებული **ფეიკ-ინფორმაცია,** რომელიც გვამცნობდა, რომ **ლუიზიანაში** არსებული **ქიმიკატების** საწარმო აფეთქდა.[54] იმ დროისთვის ეს ინფორმაცია სარწმუნო ჩანდა, თითქმის ყველა

[52] Jaffe E. How Highway Construction Helped Hitler Rise to Power, Bloomberg City Lab, 2014, p 1. https://www.bloomberg.com, უკანასკნელად იქნა გადამოწმებული - 19.08.2020

[53] Bazyler J. M., Tuerkheimer M. F., Forgotten Trials of the Holocaust, United States: NYU Press, 2014, p 384.

[54] Szal A. Report: Russian 'Internet Trolls' Behind Louisiana Chemical Explosion Hoax, Industrial Media - Manufacturing, 2015, p 1. https://www.manufacturing.net, უკანასკნელად იქნა გადამოწმებული - 20.08.2020.

სოციალური ქსელი მოიცვა. საერთოდ, ყალბი ახალი ამბავი სწრაფად ვრცელდება და იოლად დასაჯერებელია. მით უმეტეს, როცა ინფორმაციას ავრცელებს არა ერთი, არამედ რამდენიმე მედიასაშუალება. ამ შემთხვევაში მნიშვნელოვანია საზოგადოების გაფრთხილება მოსალოდნელი დეზინფორმაციის თაობაზე. ზოგადად მოგვიწოდებენ, რომ გადავამოწმოთ ფაქტები, ვნახოთ რამდენიმე წყარო, მაგრამ მასასთან მიმართებაში ეს არაეფექტურია - ფაქტების გადამოწმება მოითხოვს დროსა და ცოდნას, როდესაც დასტურდება, რომ ინფორმაცია იყო ყალბი, უკვე ჩავლილი ამბავია, თავის მართლება ან უბრალოდ უარყოფა შედარებით არაეფექტურია, უსარგებლოა. თუმცა სხვა გზაც არ არსებობს. საქართველოში კრემლის პროპაგანდის ძირითადი საყრდენი მედიასაშუალებები და სოციალური ქსელებია. მინიმუმ, ერთი ტელევიზია, რამდენიმე ინტერნეტ-ტელევიზია, ბეჭდური გამოცემა და ვებ-გვერდი გამოირჩევა ანტიდასავლური „მესიჯ-ბოქსით“, ისინი ინფორმაციის გავრცელებისას ძირითადად ეყრდნობიან რუსულ წყაროებს. თვალშისაცემია რუსული პროპაგანდის გამავრცელებლების მიერ სოციალური ქსელების აქტიური გამოყენებაც, როდესაც ხდება დეზინფორმაციის ან ანტიდასავლური ნარატივის შემცველი ინტერნეტმასალების ვირუსული გავრცელება. საზოგადოებრივი აზრის არაერთი გამოკითხვა აჩვენებს, რომ საქართველოში ინფორმაციის მიღების ძირითადი წყარო ტელევიზიაა. **ეროვნულ-დემოკრატიული ინსტიტუტის (NDI)** 2016 წლის გამოკითხვის თანახმად, საქართველოს მოსახლეობის 77% პოლიტიკისა და მიმდინარე მოვლენების შესახებ ინფორმაციის მიღების პირველწყაროდ ტელევიზიას ასახელებს. გამოკითხვები ასევე აჩვენებს, რომ ქართველი ტელემაყურებლების თითქმის ნახევარი (47%) ქართული არხების გარდა უცხოურ არხებსაც უყურებს. ყველაზე პოპულარული უცხოური არხები კი რუსულია **(HTB, ORT** და **RTR).**[55] აღსანიშნავია, რომ

[55] ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., "კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის

არის ქვეყნები, სადაც აქტიურად აკონტროლებენ ინტერნეტსივრცესა და საკომუნიკაციო ქსელებს. მაგალითად, **ჩინეთი,** რომელიც ასევე აკონტროლებს ტელევიზიებს და სოციალურ მედიას. ცნობილია, რომ **ჩინეთის** მთავრობას დაქირავებული ჰყავს ორ მილიონამდე ადამიანი, ისინი ინსტრუქციის მიხედვით წერენ კომენტარებს და ზეგავლენას ახდენენ, მართავენ საზოგადოებრივ აზრს. ამასთან დაკავშირებით **კარი კინგის, მარგარეტ რობერტსისა** და **ჯენიფერ პანის** კვლევაც გამოქვეყნდა, რომელსაც საფუძვლად უდევს ინტერნეტში გაჟონილი სამთავრობო იმეილები. აღნიშნულ კვლევაში ნათქვამია, რომ **ჩინეთის** მთავრობა წელიწადში **448 მილიონი** კომენტარის ფაბრიკაციას ახდენს. სოციალურ ქსელებში დაქირავებულები ხშირად განადიდებენ **ჩინეთს** და **ჩინეთის კომუნისტურ პარტიას,** ისინი ცდილობენ, ხალხს ყურადღება სხვა, ნაკლებად მნიშვნელოვან საკითხებზე გადაატანინონ.[56]

რა უნდა დავუპირისპიროთ დეზინფორმაციას, ფეიკ-ნიუსს, ცრუ ახალ ამბებს, საინფორმაციო ომის წარმოებას? ამის განსაზღვრა არც ისე მარტივია. ამ შემთხვევაში მნიშვნელოვანია დასწრება, ანუ რეალური ინფორმაციის გავრცელება. დაგვიანების შემთხვევაში კი საჭიროა ალტერნატიული ვარიანტის გავრცელება. როგორც ზევით აღვნიშნეთ, ვირტუალურ სივრცეში საფრთხეები მრავალმხრივია - ერთ-ერთი გახლავთ **შავი ბაზარი,** რომელიც ინტერნეტსივრცეში, ყველასთვის არ არის ხელმისაწვდომი. ამ შემთხვევაში საჭიროა გამოვყოთ ინტერნეტის ოთხი სივრცე:

1) **Surface Web** - ნიშნავს **ზედაპირულ ქსელს**. ასევე მოიხსენიებენ **Clear Web-ის** სახელითაც (**სუფთა ვები).** ეს ქსელი იძებნება სტანდარტული ვებსაძიებო სისტემებით. ქსელი არის ინდექსირებული საძიებო სისტემების მიერ. ამ ქსელში შედის „**Google“-ი, „Facebook“-ი, „Yahoo“, „Wikipedia“, „Instagram”-ი** და ა.შ.

აუცილებლობა", თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016, გვ. 5-23.

[56] Waddell K. 'Look, a Bird!' Trolling by Distraction, The Atlantic Magazine, 2017, p 1. https://www.theatlantic.com, უკანასკნელად იქნა გადამოწმებული - 21.08.2020.

2) **Deep Web - ღრმა ქსელი,** მისი **შინაარსი შეიძლება იქნას ნაპოვნი პირდაპირ URL-ს ან IP მისამართით. თუმცა** შესაძლოა, ვებ-საიტების სანახავად საჭირო გახდეს პაროლის ან უსაფრთხოების სხვა რეჟიმის გავლა. თუმცა გულისხმობს ჩვეულებრივ გამოყენებას. მაგალითად, როდესაც მომხმარებელს აქვს შეზღუდული წვდომა სხვადასხვა ვებ-გვერდებზე, სადაც საჭიროებს რეგისტრაციას შინაარსის სანახავად. ისეთ საიტებზე, სადაც საჭიროა თანხის გადახდა ელჟურნალის ან ელგაზეთის გადმოსატვირთად. ამ **სივრცეს მიეკუთნება, „Paypal“-ი, „Facebook”-ი, “Twitter”-ი, “Wathsapp”-ი, “Gmail”-ი და ა.შ.**

3) **Dark Web - ბნელი ქსელი.** ეს არის სისტემა, რომელიც არ არის ინდექსირებული ვებ-საძიებო სისტემების მიერ. აქ მოსახვედრად საჭიროა სპეციალური პროგრამა, კონფიგურაცია ან ავტორიზაცია. შესაძლებელია ანონიმურად დაკავშირება, კონფიდენციალურობის დაცვა, პრივატული კომუნიკაცია, უკანონო ინფორმაციის მოპოვება, უკანონო ვაჭრობა, მაგალითად, ნარკოტიკით, იარაღით და ა.შ.

4) **Darknet - ბნელი ქსელი.** ასევე ცნობილია, როგორც **„დაფარული ქსელი“.** ეს არის სისტემა, რომელიც ხელმისაწვდომია არასტანდარტული პორტების გამოყენებით. **დარქნეტი** განსხვავდება სხვა ქსელებისგან იმით, რომ ფაილის გაზიარება ხდება ანონიმურად, ანუ IP მისამართები საჯაროდ არ არის ხელმისაწვდომი. ამ სივრცეში კომუნიკაცია უკონტროლოა და შეიცავს სხვადასხვა საფრთხეებს. შეგვიძლია პარალელი გავავლოთ იატაკქვეშა არალეგალურ საქმიანობასთან, რაც რეალურ სივრცეში ხორციელდება და **დარკნეტს** შორის, რომელიც ვირტუალურ სივრცეში ხორციელდება. ამ სისტემაში მოხვედრა არ არის იოლი, საწიროა კონკრეტული პროგრამული უზრუნველყოფა და ავტორიზაცია. **დარკნეტი** შეიძლება ასევე განხილულ იქნას როგორც ალტერნატიური ინტერნეტი, ან ინტერნეტის ბნელი მხარე, ეს უზარმაზარი ქსელია, რომელიც ათასობით არალიცენზირებულ და უკანონო ვებ-გვერდებს აერთიანებს. აქ ხელმისაწვდომია უამრავი რამ -

არალეგალურად იარაღის ყიდვა, კლონირებული კარტების შეძენა, ყალბი პასპორტების ყიდვა, მონის გამოწერა, ნარკოტიკების ყიდვა, ქილერის დაქირავება და ა.შ. **დარკნეტში** უამრავი არალეგალური ფორუმი, სოციალური ქსელი და არასტანდარტული ვებ-გვერდებია. ნაშრომში შეგნებულად არ განვიხილავთ ამ სისტემაში შესვლის ინსტრუქციას, შეიძლება გაგებული იყოს წახალისებად.

კნაფ კენეტი თავის წიგნში, - **"კიბერუსაფრთხოება და ინფორმაციის გლობალური უზრუნველყოფა - საფრთხეების ანალიზისა და რეაგირების გადაწყვეტილებების შესახებ",** რომელიც გამოქვეყნდა კოლორადოში, აშშ-ის საჰაერო ძალების აკადემიის მიერ, ხაზგასმით არის აღნიშნული, რომ პროგრამული უზრუნველყოფის ერთ-ერთი დიდი ხარვეზი შავი ბაზარია. მისი აზრით, კიბერსივრცის მომხმარებელთა თავდაცვისუნარიანობა ჩვეულებრივ ჩამორჩება კიბერთავდამსხმელების შეტევებს. **კენეტი** ასევე განმარტავს, რომ **შავი ბაზრების** შესაძლო ზრდა პროგრამულ უზრუნველყოფაზე დაუცველობის შანსებს ზრდის. ძნელია **შავი ბაზრების** შესახებ სტატისტიკური მონაცემების მოპოვება დაუცველ მომხმარებლებზე და მათთან დაკავშირებულ ოპერაციებზე. ჩვენი დაკვირვება გამოხატულია როგორც სისტემის დინამიური მოდელი. ვატარებთ სიმულაციებს, რათა დავაკვირდეთ, იზრდება თუ მცირდება მოხმარებელთა რაოდენობა. ჩვენი დაკვირვებით, შეგვიძლია ვთქვათ, რომ მაჩვენებელი იზრდება. თუმცა რა განაპირობებს, ამის თქმა რთულია. კენეტი წერს, რომ მათი ოპერაციების სიმულაციური სცენარი იწვევს ბაზრის დროებით შემცირებას:

„უსაფრთხოების კომპანიები, როგორებიცაა **IBM ISS X-Force (2007), PandaLabs (2007) და Symantec (2008)** აღნიშნავენ კიბერშეტევების ზრდას, მაგალითად, **Symantec**-ის მოხსენების თანახმად, იგი აკვირდება შავი ბაზრის სხვადასხვა ფორუმებს და აღნიშნავს, რომ სავარაუდოდ ფორუმებს უმეტესწილად იყენებენ ჰაკერები, კრიმინალები და კრიმინალური ორგანიზაციები, ისინი ვაჭრობენ სხვადასხვა სახის პროდუქციით. მათ მიზანი კი საბოლოო ჯამში პირადი მონაცემების ქურდობაა. **Symantec**-ის

მოხსენებაში მკაფიოდ არის აღნიშნული, რომ შავი ბაზრები წარმოადგენენ სერიოზულ საფრთხეს, როგორც პერსონალურ, ასევე გლობალურ დონეზე. შავი ბაზრის გამოყენებით სერიოზული საფრთხე ექმნება პერსონალური ინფორმაციის დაცულობას. ჰაკერები ასევე იყენებენ კონკრეტული მომხმარებლებისა და კონკრეტული საიტების წინააღმდეგ, ბრაუზერებზე და ვებ-გვერდებზე კიბერშეტევების განსახორციელებლად".[57]

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

[57] Kenneth J. K. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions, Colorado: U.S. Air Force Academy, 2009, pp 26-27.

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.

ძალთა ბალანსის კონცეფცია გულისხმობს: თუ ერთი სახელმწიფო გაძლიერდება, ისარგებლებს სხვა სახელმწიფოების სისუსტით, რაც გამოიწვევს სუსტი სახელმწიფოების გაერთიანებას თავდაცვის მიზნით. ეს არის ჯაჭვური რეაქცია, რომელიც განვითარდა ტექნოლოგიების განვითარების ფონზე და ხელი შეუწყო კიბერომების წარმოებას. ამან კი ზოგიერთი ქვეყნის უსაფრთხოების საკითხი კითხვის ნიშნის ქვეშ დააყენა. როგორც წინა თავებში აღვნიშნეთ, **ამერიკის შეერთებული შტატები** განაგრძობს ლამის გაათმაგებული ფინანსების დახარჯვას კიბერშესაძლებლობების გასაძლიერებლად. ეს არც არის გასაკვირი, რადგან **აშშ-ი შეიქმნა ინტერნეტი** და ამ ქვეყანაშივე დაინერგა მრავალი ახალი ტექნოლოგია. საერთოდ, კიბერინსტრუმენტების ფართო სპექტრი პოლიტიკაშიც უზრუნველყოფს სტრატეგიული მოქნილობის სხვადასხვა ვარიანტებს, რაც ადრე თითქმის წარმოუდგენელი იყო. აქვე აღსანიშნავია **რუსეთის** ფაქტორი, რომელიც კიბერშესაძლებლობების თვალსაზრისით ასევე მოწინავე პოზიციებზეა. რას წარმოადგენს რუსული კიბერძალა და რა როლს ასრულებს **ძალთა ბალანსის** თვალსაზრისით? რუსეთი ნამდვილად მუშაობს ინოვაციურად სხვადასხვა კონფლიქტებში. სპეციფიკური გეოპოლიტიკური გარემოდან გამომდინარე, რუსეთმა წარმატებით

მოახერხა კიბერშეტევების ადაპტირება საკუთარი ინტერესების გასაფართოებლად. ნაშრომში უამრავი მაგალითი გვაქვს განხილული რუსეთთან მიმართებაში. ერთ-ერთი 2007 წლის კიბერშეტევებია ესტონეთის წინააღმდეგ. ეს იყო მარტივი **DDoS** შეტევა, რომელსაც მნიშვნელოვანი ზარალი არ მოჰყოლია, მაგრამ დადებითად იმოქმედა **ესტონეთისა** და **ნატოს ურთიერთობის გაძლიერებაზე უსაფრთხოების თვალსაზრისით.** იგივე განმეორდა 2008 წელს **რუსეთ-საქართველოს ომის პერიოდში,** რაც უკვე არაერთხელ აღვნიშნეთ. ასევე - **უკრაინასთან** მიმართებაში, სადაც კიბერშეტევები უფრო „დახვეწილი“ და დამაზიანებელი აღმოჩნდა. მაგალითები მრავლად გვაქვს, რაც **რუსეთის** გაძლიერებულ კიბერშესაძლებლობებზე მიანიშნებს. **რუსეთის** მიერ განხორციელებული კიბერთავდასხმები უმეტესად გამოყენებულია ასიმეტრიული კონფლიქტის პირობებში. თუმცა 2016 წელს **აშშ-ის** საპრეზიდენტო არჩევნებში ჰაკერების ჩარევა განსხვავებული იყო იმ გაგებით, რომ რუსეთმა არ გამოიყენა კიბერშეტევა, ეს არ იყო სადამსჯელო ღონისძიება, აღნიშნული მიზნად ისახავდა კიბერშესაძლებლობების მოსინჯვას არჩევნებზე ზეგავლენის მოსახდენად. ბუნებრივია, **რუსეთის** შესაძლებლობებსაც აქვს ზღვარი. როდესაც ანხორციელებს კიბერშეტევას გარკვეული სტრატეგიით, პოტენციურ მოწინააღმდეგეებს შესაძლებლობა აქვთ, მოემზადონ თავდაცვითი მიმართულებით. შეიძლება **რუსეთის** მიერ განხორციელებული კიბერშეტევები **საქართველოსა** და **უკრაინაზე** ჩაითვალოს ექსპერიმენტებად, მაგრამ სწორედ ეს აძლევს **საშუალებას წამყვან ქვეყნებს,** სრულყოფილად შეისწავლონ ე.წ. **რუსული** მეთოდები ტექნოლოგიური თვალსაზრისით. შემდეგ კი უფრო იოლად ხდება თავდაცვითი მექანიზმების გაუმჯობესება. მაგალითად, **საფრანგეთის, იტალიის, ჰოლანდიისა** და **გერმანიის** არჩევნებში **რუსი** ჰაკერების ჩარევა იმდენად ეფექტური არ იყო, როგორც ეს შეიძლება ყოფილიყო წინა შემთხვევებში. აქვე აღსანიშნავია **ჩინეთის** როლი კიბერშესაძლებლობების მიმართულებით. **ჩინეთის** კიბერჯაშუშობის ინტენსიურმა გამოყენებამ

თეთრი სახლის ადმინისტრაცია უკიდურესად გააღიზიანა. სწორედ ამ თავდასხმების ხარჯზე მოხდა საიდუმლო მასალების გატანა **ჩინეთის** დაზვერვის მიერ. ერთ-ერთი ყველაზე დამაზიანებელი იყო, როცა აშშ-ის ადმინისტრაციის პერსონალის მართვის ოფისის სისტემაზე მიიტანეს იერიში - 20 მილიონზე მეტი ადამიანის პერსონალური მონაცემი მოიპოვეს.[58]

რუსეთთან ერთად **ირანის ისლამური სახალიფოს** ძლიერ კიბერმოთამაშეს წარმოადგენს არა მხოლოდ რეგიონში, არამედ მსოფლიოში. **ირანის ისლამური სახალიფოს,** როგორც **რუსეთი,** არ გახლავთ პროგნოზირებადი სახელმწიფო, მით უფრო მაშინ, როცა მისი კიბერდოქტრინა აგებულია ასიმეტრიული ომის ტაქტიკაზე და ძირითადად დაფუძნებულია ჰაკერულ თავდასხმებზე. კიბერდოქტრინის თითოეულ დეტალს აკონტროლებს **ირანის ისლამური სახალიფოს** ხელისუფლება, რომლის წიაღშიც შექმნილია **კიბერსივრცის უმაღლესი საბჭო**, სადაც შედიან ამავე ხელისუფლების უმაღლესი წარმომადგენლები, **პრეზიდენტით** დაწყებული, **მინისტრებით** დამთავრებული.

ამ სახელმწიფოებს ემატება **ჩრდილოატლანტიკური ალიანსი,** რომელიც კიბერუსაფრთხოების თვალსაზრისით, მნიშვნელოვან როლს თამაშობს მსოფლიო მასშტაბით და თანამშრომლობს წევრ თუ არაწევრ ქვეყნებთან. **ნატო ევროკავშირის** დახმარებით ცდილობს ვირტუალურ სივრცეში წარმოქმნილ საფრთხეებთან გამკლავებას, რაც უფრო მეტად აბალანსებს მდგომარეობას, ამცირებს რისკებს და საფრთხეებს. ნათელია, რომ დღეს, კიბერტექნოლოგიების თვალსაზრისით, სისტემა არ გახლავთ ერთპოლუსიანი. ამ შემთხვევაში პოტენციური მოკავშირეების რიცხვი მეტია და უფრო მარტივია პოლიტიკის წარმოებაც. დღევანდელი საერთაშორისო გარემო მრავალპოლარულია სხვადასხვა განზომილებით. შეიძლება იმდენ ფინანსებს არავინ ხარჯავს, რამდენსაც **ამერიკის**

[58] Zengerle P., Megan Cassella M., Millions more Americans hit by government personnel data hack", Media Company Reuters, 2015, p 1. https://uk.reuters.com, უკანასკნელად იქნა გადამოწმებული - 25.08.2020.

შეერთებული შტატები, არც სამხედრო ალიანსს ქმნის არავინ, თუნდაც **ჩინეთი და რუსეთი,** მაგრამ ისინი მაინც აძლიერებენ სამხედრო თანამშრომლობას და კოორდინაციას უწევენ საგარეო პოლიტიკას. გასათვალისწინებელია ის ფაქტიც, რომ **აშშ-მ** გააორმაგა ძალისხმევა **ჩინეთის** საპირწონედ მთელ მსოფლიოში, განსაკუთრებით **აღმოსავლეთ აზიაში.** საერთოდ, **ჩინეთი** განიხილება ნომერ პირველი საფრთხედ **აშშ-ისთვის**. საქმე ეხება გლობალურ პოლიტიკაში **ამერიკის** პირველობას.

ნაშრომში წარმოდგენილი მიმოხილვა ცხადყოფს, როგორი მაღალი აქტივობით იყენებენ სხვადასხვა ქვეყნები კიბერტექნოლოგიებს საერთაშორისო პოლიტიკის წარმოებისას. კიბერელემენტის მნიშვნელობა დადებითად მოქმედებს ძალთა ბალანსის დაცვაზე, რადგან აქ ერთი დომინანტი ძალა არ არსებობს. თუმცა კიბერტექნოლოგიების ის შესაძლებლობა, რომ მარტივად გამოსაყენებელია ასიმეტრიული თავდასხმებისთვის, ეს ცხადყოფს, თუ რა რისკებისა და გამოწვევების წინაშე დგას მსოფლიო.

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._რუსეთის ეროვნული უსაფრთხოების დოქტრინის **2015 წლის** ვარიანტში **მე-16** და **მე-17** პარაგრაფებში მთავარ

მოწინააღმდეგეებად მოიაზრებიან **აშშ** და **ნატო,** ხოლო **მე-7** პარაგრაფში პირდაპირ არის დაფიქსირებული რუსეთის ფედერაციის როლის ამაღლება მსოფლიო წესრიგის მოწყობის საქმეში.[59]

რუსეთის ფედერაცია ამბობს, რომ ის კი არ წარმოადგენს სხვა ქვეყნებისთვის საფრთხეს, არამედ თავად არის მსხვერპლი და მას აქვს ასამაღლებელი შესაძლებლობები, რათა გაუმკლავდეს **აშშ-დან** და **ნატოდან** მომდინარე საფრთხეებს. რეალური სიტუაცია და ფაქტები კი საპირისპიროს გვიმტკიცებს - მაგალითად, **რუსეთმა** სწორედ **„ჰიბრიდული ომის“** ელემენტების გამოყენებით შეძლო სერიოზული დარტყმის მიყენება **აშშ-სთვის,** საპრეზიდენტო არჩევნების დროს შეიტანა პოლიტიკური არასტაბილურობის ნიშნები ამ სახელმწიფოს მონოლითურ პოლიტიკურ სისტემაში. საპრეზიდენტო არჩევნებში ჰაკერული ჩარევის ამბავი სრული სიცრუეც რომ იყოს, მაინც **რუსეთი** იღებს სარგებელს, აღნიშნული ფაქტი აჩენს განცდას, რომ იგი ყოვლისშემძლეა, სწორედ ეს იწვევს ნიჰილიზმს ამერიკის შეერთებული შტატების მოსახლეობაში. თუმცა რატომ მხოლოდ ამ ქვეყნის მოსახლეობაში? როდესაც მთელი ევროპა, აზია თუ აფრიკა ხედავს, რომ სუპერსახელმწიფოც კი დაუცველია გარკვეულ მომენტებში, ყველას უჩნდება იმედგაცრუებისა და უმწეობის განცდა. ერთ-ერთ მაგალითად აშშ-ზე 2001 წლის 11 სექტემბრის ტერაქტებიც გამოდგება. აი, აქ გაჩნდა პირველად არა მხოლოდ **"ამერიკული ნიჰილიზმი",** არამედ **"მსოფლიო ნიჰილიზმი".** ამერიკის შეერთებულ შტატებს სწორედ ამ პერიოდში ჰქონდა ე.წ. მოფერება-გადატვირთვის პოლიტიკა - სახელმწიფო მდივანი **ჰილარი კლინტონი** მოსკოვში ჩაბრძანდა და რუსეთის საგარეო საქმეთა მინისტრს, **სერგეი ლავროვს** გადატვირთვის სიმბოლური ღილაკი აჩუქა, ხოლო იმჟამინდელ დოქტრინაში პირდაპირ ჩაწერეს, რომ **რუსეთთან** აუცილებელია კონსტრუქციული თანამშრომლობა, **ნატო-რუსეთის** უსაფრთხოება გადაჯაჭვულია და ასე შემდეგ. როგორც შემდგომში ვნახეთ, ამგვარმა მიდგომამ არ გაამართლა.

[59] Russian National Security Strategy, Moscow: Russian Federation, 2015, No. 683, pp 1-4.

კონკრეტულად რა წერია აშშ-ის ეროვნული უსაფრთხოების სტრატეგიაში, რომელიც 2017 წლის დეკემბერში გამოქვეყნდა? სტრატეგიის შესავალშივე აღნიშნულია, რომ ამერიკის კეთილდღეობა და უსაფრთხოება დამოკიდებულია იმაზე, თუ როგორ უპასუხებს **კიბერსივრცეში** არსებულ შესაძლებლობებსა და გამოწვევებს. აქვე აღნიშნულია, რომ კრიტიკული ინფრასტრუქტურა, ეროვნული თავდაცვა და ამერიკელების ყოველდღიური ცხოვრება ეყრდნობა კომპიუტერულ და ინფორმაციულ ტექნოლოგიებს.[60]

ანუ აშშ-ის ეროვნული უსაფრთხოების დოკუმენტის პირველივე გვერდზე ვკუთხულობთ კიბერტექნოლოგიების მნიშვნელოვან ფაქტორებზე, რაც იმას ნიშნავს, რომ კიბერსივრციდან მომდინარე საფრთხეები ყველა სფეროზე ახდენს ზეგავლენას და აზიანებს როგორც მატერიალური, ასევე არამატერიალური თვალსაზრისით. მნიშვნელოვანია, რომ ეს საკითხი განვიხილოთ ისეთ კონტექსტში და ისეთი დოქტრინით, რომელსაც **„კოლექტიური თავდაცვა“** ქვია.

„კოლექტიური თავდაცვითი“ მოდელი ეკუთვნის ამერიკელ პოლიტოლოგს **რიჩარდ კოენს,** მან შეიმუშავა **„თანამშრომლობითი უსაფრთხოების“** კონცეფცია, რომელიც იყოფა ოთხ ნაწილად - **ინდივიდუალური უსაფრთხოება, კოლექტიური უსაფრთხოება, კოლექტიური თავდაცვა და სტაბილურობის შენარჩუნება. ინდივიდუალური უსაფრთხოება** გულისხმობს ქვეყნის უნარს, დამოუკიდებლად დაიცვას საკუთარი ტერიტორია, გაეროს წესდების 51-ე მუხლის თანახმად, მათ შორის სამხედრო გზით. **კოლექტიური უსაფრთხოება** გულისხმობს ქვეყნების გაერთიანებას საერთო სახის სამხედრო რისკების და გამოწვევების წინააღმდეგ. **კოლექტიური თავდაცვა** ნიშნავს ქვეყნების გაერთიანებას სხვა ქვეყნებისგან თავდაცვის მიზნით, რაც დღეს ნატოს მოდელს უდევს საფუძვლად - ტრანსატლანტიკური სოლიდარობის პრინციპი.

[60] National Security Strategy of the United States of America, Washington: The White House, 2017, pp 1-2.

სტაბილურობის მიღწევა საერთო ძალისხმევით, ეს ნიშნავს და უფრო მეტად არის იდალური ვარიანტი მაღალი დონის კოლექტიური უსაფრთხოების გლობალური სცენარის დროს - მაგალითად, **„ისლამური სახალიფოს“** წინააღმდეგ.[61]

რეალობა გვიჩვენებს, რომ ეს კონცეფცია საკმაოდ აქტუალურია XI საუკუნეშიც. უფრო მეტად მნიშვნელოვანი გახადა კიბერტექნოლოგიების განვითარებამ. **„კოლექტიური თავდაცვა“** ნატოს წესდებაში მკაფიოდ არის გაწერილი და წევრ ქვეყნებს ავალდებულებს, დაიცვან ერთმანეთი. კოლექტიური თავდაცვა ნიშნავს, რომ თავდასხმა რომელიმე ერთ მოკავშირეზე ითვლება თავდასხმად ყველაზე - ეს პრინციპი გათვალისწინებულია ვაშინგტონის ხელშეკრულების მე-5 მუხლითაც. **ნატომ** პირველად მე-5 მუხლი აამოქმედა **აშშ-ზე** 11 სექტემბერს ტერორისტული თავდასხმის შემდეგ. კოლექტიური თავდაცვის პრინციპის საკითხი ასევე წამოიჭრა, როდესაც რუსეთმა უკრაინის წინააღმდეგ წამოიწყო სამხედრო აგრესია. 2014 წლის 1-ელ აპრილს ნატოს საგარეო საქმეთა მინისტრმა ალიანსის სამხედრო ხელმძღვანელობას მიმართა, რათა შეემუშავებინათ დამატებითი ზომები კოლექტიური თავდაცვის გასაძლიერებლად.[62]

საერთაშორისო სამართლის თანახმად, სახელმწიფოებს უფლება აქვთ, გამოიყენონ ძალა შეიარაღებული თავდასხმისგან თავის დასაცავად. კიბერშეტევის შედეგად დაზარალებულ სახელმწიფოს უფლება აქვს, კიბერომის კვალიფიკაციის მქონე თავდასხმებს უპასუხოს სამხედრო ძალის გამოყენებით. მიუხედავად იმისა, რომ მსგავსი ფაქტი ჯერ არ მომხდარა, მთავრობები მაინც აქტიურად განიხილავენ ასეთი შესაძლებლობების დარეგულირების საკითხს. მაგალითად, 2014 წელს ნატომ გამოაქვეყნა დეკლარაცია, რომელშიც ნათქვამია, რომ კიბერშეტევების გავლენა

[61] Cohen R., Mihalka M., Cooperative Security: New Horizons for International Order, London: European Center for Security Studies, The Marshall Center Papers, 2001 No. 3. pp 3-15.

[62] Collective defence - Article 5, NATO, 2019, p 1. https://www.nato.int ბოლოს იქნა გადამოწმებული - 04,08.2020.

შეიძლება ისეთივე მავნე იყოს თანამედროვე საზოგადოებისთვის, როგორც ჩვეულებრივი სამხედრო თავდასხმა. ამავე დეკლარაციაშივე აღნიშნულია, რომ ნატოს წევრ ქვეყანაზე კიბერშეტევამ შეიძლება გამოიწვიოს ჩრდილოატლანტიკური ალიანსის მე-5 მუხლის გამოყენება. ალიანსის სტრატეგიულ კონცეფციაში დიდი ყურადღება ეთმობა პარტნიორობის, თანამშრომლობისა და დიალოგის ფაქტორს. ალიანსი ცდილობს, ევროატლანტიკურ პარტნიორობის საბჭოს წევრებს შორის ყველა საკითხში იყოს ნდობა და გამჭვირვალობა. ეს კი ევროკავშირისა თუ ნატოს არაწევრ ქვეყნებსაც ავალდებულებს, აქტიურად იყვნენ ჩაბმულნი საერთაშორისო უსაფრთხოების პროცესებში. 2016 წელს ნატოს წევრმა ქვეყნებმა კიბერსივრცე აღიარეს როგორც საომარი მოქმედებების სფერო.[63]

ჩამოყალიბებულია არაერთი თავდაცვითი საერთაშორისო ორგანიზაცია. ერთ-ერთი ასეთი ცენტრი გახლავთ, **CCDCOE - ნატოს „კოოპერატიული კიბერთავდაცვის ცენტრი“,** რომელიც წარმოადგენს **მრავალეროვნულ და ინტერდისციპლინარულ** კიბერთავდაცვის ორგანიზაციას. აღნიშნული ცენტრის დირექტორი, პოლკოვნიკი **ჯააკ ტარიენი** განმარტავს, რომ ოპერატიული ცენტრი არ არის შექმნილი ოპერაციების ჩასატარებლად. მისივე თქმით, მათი საქმიანობა მოიცავს კვლევებს, ტრენინგებსა და სავარჯიშოებს:

„ჩვენი სასწავლო პროცესი მოიცავს წელიწადში 17 კურსს. კურსებზე განიხილება და ისწავლება, მაგალითად, კრიტიკული ინფრასტრუქტურის დაცვა, საერთაშორისო სამართალი და კიბერთავდაცვითი ოპერაციების დაგეგმვა“.[64]

კიბერთემის შესწავლის თვალსაზრისით მნიშვნელოვან ობიექტს წარმოადგენს საქართველო, რომელიც გლობალური პოლიტიკური პროცესების შემადგენელ ნაწილს წარმოადგენს. შესაბამისად, საქართველოს

[63] Brent L. NATO's role in cyberspace, NATO, 2019, p 1. https://www.nato.int, უკანასკნელად იქნა გადამოწმებული - 16.06.2020.

[64] Riazi T. Know The CCDCOE: Interview with Director Col. Jaak Tarien, NATO Assotiation of Canada - NAOC, 2020, p 1. http://natoassociation.ca, უკანასკნელად იქნა გადამოწმებული - 16.06.2020.

ეროვნული კონცეფციის განხილვაც და ქვეყნის კიბერტექნოლოგიური უსაფრთხოების შეფასება-განსაზღვრაც მნიშვნელოვანია. საქართველოს ეროვნული უსაფრთხოების კონცეფცია არის დოკუმენტი, რომლითაც ხელისუფლებამ უნდა იხელმძღვანელოს არა მხოლოდ ექსტრემალურ სიტუაციაში, არამედ დასახოს პრიორიტეტები.

რა არის ქვეყნის პრიორიტეტები? უსაფრთხოება, კეთილდღეობა, მშვიდობა. რას წარმოადგენს საქართველოს ეროვნული ინტერესები? როგორც კონცეფციაშია აღნიშნული, ეს გახლავთ სუვერენიტეტისა და ტერიტორიული მთლიანობის უზრუნველყოფა, სახელმწიფო ინსტიტუტების განვითარება და დემოკრატიის განმტკიცება, ეროვნული უსაფრთხოების ეფექტიანი სისტემის განვითარება, ეროვნული ერთიანობისა და სამოქალაქო თანხმობის განმტკიცება, ევროპული და ევროატლანტიკური ინტეგრაცია, ეკონომიკის სტაბილური ზრდის, ენერგეტიკული უსაფრთხოების და რეგიონული სტაბილურობის უზრუნველყოფა, კიბერუსაფრთხოების განმტკიცება და ასე შემდეგ. კონცეფციაში განმარტებულია:

"რუსეთის ფედერაციის მიერ საქართველოს ტერიტორიების ოკუპაცია და ოკუპირებული ტერიტორიებიდან რუსეთის ფედერაციის მიერ ორგანიზებული ტერორისტული აქტები, რუსეთის ფედერაციის მხრიდან ახალი სამხედრო აგრესიის რისკი".[65]

კონცეფციაში არაერთხელაა ნახსენები ქვეყნის უსაფრთხოება და კიბერუსაფრთხოება. თუმცა საქართველოს უსაფრთხოების გარემოს აღწერისას ყურადღება გამახვილებულია მხოლოდ რუსეთზე და იმაზე, თუ როგორ გაუარესდა გარემო 2008 წლის შემდეგ, რაც მეზობელმა გამოამჟღავნა არნახული აგრესია. შემდეგ თავებშიც, სადაც საუბარია გამოწვევებზე, საფრთხეებსა და რისკებზე, კვლავ გვეუბნებიან, რომ საშიშროება გვემუქრება მხოლოდ რუსეთიდან. თუმცა გაკვრით მაინც არის

[65] "საქართველოს ეროვნული უსაფრთხოების კონცეფცია", თბილისი: საქართველოს მთავრობა, 2018, გვ. 3-30.

ნახსენები საერთაშორისო ტერორიზმი, ტრანსნაციონალური ორგანიზებული დანაშაული და ისიც, რომ თანამედროვე მსოფლიოს უსაფრთხოებისთვის მნიშვნელოვან გამოწვევად იქცა ცალკეული სახელმწიფოებისა და არასახელმწიფოებრივი სუბიექტებისაგან მომდინარე ტერორისტული საფრთხეები. აქვე დაფიქსირებულია, რომ საქართველოს ტერიტორიაზე ოკუპირებული რეგიონების არსებობა ხელსაყრელ გარემოს ქმნის საერთაშორისო ტერორიზმისა და ტრანსნაციონალური ორგანიზებული დანაშაულისათვის. არ არის დაკონკრეტებული, რას ნიშნავს ცალკეული სახელმწიფოები და არასახელმწიფოებრივი სუბიექტები. ეროვნული უსაფრთხოების კონცეფციაში საერთოდ არ არის ნახსენები სიტყვა "მედია", რომელიც მე-4 ხელისუფლებას წარმოადგენს. ასევე არ არის ნახსენები "სოციალური ქსელები" და სხვა ინტერნეტ-საშუალებები.

<u>კიბერუსაფრთხოების გლობალური ინდექსი</u>

მსოფლიოში არსებობს კიბერუსაფრთხოების გლობალური ინდექსი, სადაც 2017 წელს 165 ქვეყანას შორის საქართველო იყო მე-8 ადგილზე. ინდექსს ადგენს გაერთიანებული ერების ორგანიზაციის სპეციალიზებული ორგანო - საერთაშორისო სატელეკომუნიკაციო კავშირი (ITU) და 2 წელიწადში ერთხელ აქვეყნებს. კვლევის საანგარიშო პერიოდი გახლდათ 2015 წლიდან 2017 წლის დასაწყისამდე. მაშინ საქართველოს იუსტიციის სამინისტროში აცხადებდნენ, რომ ეს იყო იმ პროგრესის აღიარება, რომელსაც ქვეყანა კიბერუსაფრთხოების სფეროში წლიდან წლამდე აჩვენებს. ეს ადასტურებს, რომ კიბერუსაფრთხოების თვალსაზრისით საქართველო აღიარებულია, როგორც მსოფლიოში ერთ-ერთი ყველაზე დაცული და უსაფრთხო ქვეყანა. კვლევის საგანს წარმოადგენდა 5 ძირითადი კომპონენტი - საკანონმდებლო ბაზა, ტექნიკური მზაობა, ორგანიზაციული მოწყობა, შესაძლებლობების განვითარება და თანამშრომლობისთვის ღიაობა. ამ 5 კომპონენტიდან, რა თქმა უნდა, ყველა მნიშვნელოვანია, მაგრამ მთავარი მაინც ტექნიკური ბაზაა. თუ კვლევის საგანია მხოლოდ მზაობა, მაშინ საქართველოსთვის

მიკუთვნებული რეიტინგი დამაჯერებელია. როგორც ჩანს, ამ შემთხვევაში საქმე გვაქვს მხოლოდ ორგანიზაციულ მოწყობასთან, თანამშრომლობის ღიაობასთან და არა დღევანდელ შესაძლებლობასთან. 2017 წელს იუსტიციის სამინისტროში აცხადებდნენ, რომ ამის მიღწევა-შენარჩუნება-განვითარება კომპლექსური საკითხი იყო და სხვადასხვა უწყებები დაუღალავად იშრომებდნენ. ეს უწყებებია: **იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტო**, კრიზისებისა და უსაფრთხოების საბჭო, რომელიც შემდგომში გაუქმდა. ასევე, თავდაცვის სამინისტროს **კიბერუსაფრთხოების ბიურო**, შინაგან საქმეთა სამინისტრო და სახელმწიფო უსაფრთხოების სამსახური. ოფიციალური ინფორმაციის თანახმად, ინდექსის შედეგებზე მნიშვნელოვანი გავლენა იქონია კომპიუტერულ ინციდენტებზე სწრაფი დახმარების ჯგუფის (CERT.GOV.GE) არსებობამ და წარმატებულმა მუშაობამ როგორც ადგილობრივ, ისე საერთაშორისო ასპარეზზე. ეს ჯგუფი იუსტიციის სამინისტროს **"მონაცემთა გაცვლის სააგენტოს"** სტრუქტურის ნაწილია და პასუხისმგებელია კიბერუსაფრთხოების განვითარება-შენარჩუნებაზე, კიბერინციდენტების წინააღმდეგ მიმართული ღონისძიებების გატარებაზე და ასე შემდეგ.[66]

რა მოხდა ამ კუთხით ბოლო ორ წელიწადში? მერამდენე ადგილზე ვართ 2019 წლის მონაცემებით? კიბერუსაფრთხოების ინდექსით საქართველო მსოფლიოში მე-19 ადგილზეა. ინდექსში საქართველოს 100 სარეიტინგო ქულიდან 64.94 აქვს. ციფრული განვითარების დონით კი საქართველოს სარეიტინგო ქულა 59.66-ია. რეიტინგში პირველ ადგილზე საფრანგეთია - 83.12 ქულით. მას მოსდევს გერმანია 83.12 ქულით და ესტონეთი 81.82 ქულით. რომელ ქვეყნებს ვუსწრებთ? იტალიას, რუსეთს, ნორვეგიას, ლუქსემბურგს, შეერთებულ შტატებს. თუ საქართველო 2017 წელს იყო მე-8 ადგილზე და ორ წელიწადში ჩამოქვეითდა მე-17 ადგილამდე, ამ

[66] "კიბერუსაფრთხოების ინდექსში საქართველო მე-8 ადგილზეა". ტელეკომპანია "იმედი", 2017, გვ. 1. https://imedinews.ge, უკანასკნელად იქნა გადამოწმებული: 14.06.2020.

შემთხვევაში არსებობს ორი ვერსია: პირველი - საქართველოში გაუარესდა მდგომარეობა; მეორე - სხვა ქვეყნებმა გააუმჯობესეს სიტუაცია.[67]

კიბერომი ევროკავშირის სივრცეში

დღეს მთელი ევროპა ლაპარაკობს რუსეთიდან მომდინარე საფრთხეებზე. სწორედ ამის გამო ვარშავაში მიღებული გადაწყვეტილების საფუძველზე ნატომ 2017 წლის დასაწყისში ბალტიისპირეთის ქვეყნებში (ლიტვა, ლატვია, ესტონეთი) და პოლონეთში განათავსა ბატალიონის ტიპის 4 სამხედრო ქვედანაყოფი, რომლებიც ადგილობრივ სამხედრო ქვედანაყოფებთან შეთანხმებულად მოქმედებენ. ამ გადაწყვეტილებას წინ უძღვოდა ნატო-ს 2014 წლის უელსის სამიტზე მზადყოფნის სამოქმედო გეგმის **RAP**-ის დამტკიცება, რომელიც ძირითადად სწორედ რუსეთიდან მომდინარე საფრთხეებისა და მათი სტრატეგიული გავლენის საპასუხოდ იქნა მიღებული. ვარშავის სამიტის დეკლარაციაში ისიც აღინიშნა, რომ 2014 წლის შემდეგ საფრთხე დაემუქრა ბალტიის ზღვის რეგიონის უსაფრთხოებას. კერძოდ, ხაზი გაესვა რუსეთის გააქტიურებულ სამხედრო აქტივობებს და ახალი სამხედრო ტექნოლოგიების განლაგებას, რაც დამატებით გამოწვევებს უქმნის რეგიონის უსაფრთხოებას. რასაკვირველია, ახალი სამხედრო ტექნოლოგიები თავისთავად გულისხმობს კიბერსივრცის გაკონტროლებასაც და კიბერთავდასხმებსაც.[68]

ევროკავშირმა ასევე დაიწყო ყალბ ახალ ამბებთან ბრძოლის გაძლიერება და ევროკომისიამ დეზინფორმაციის გავრცელების წინააღმდეგ სამოქმედო გეგმაც კი წარადგინა. ამ გეგმის პრეამბულაში ნათქვამია, რომ უნდა შევინარჩუნოთ ერთიანობა და გავაერთიანოთ ძალისხმევა, რათა ჩვენი დემოკრატია უკეთ დავიცვათ დეზინფორმაციისგან. ვიხილეთ არჩევნებსა

[67] "კიბერუსაფრთხოების ინდექსით, საქართველო მსოფლიოში მე-19 ადგილზეა". ტელეკომპანია "იმედი", 2018, გვ. 1. https://imedinews.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020.

[68] "ნატო-ს ვარშავის სამიტის დეკლარაციის მოკლე მიმოხილვა (გავლენა საქართველოზე)", თბილისი: საქართველოს უსაფრთხოების და განვითარების ცენტრი, 2014, გვ. 2-3.

და რეფერენდუმებში ჩარევის არაერთი შემთხვევა და ყველა მტკიცებულება მიუთითებს, რომ დამნაშავე უმრავლეს შემთხვევაში რუსეთია.

სამოქმედო გეგმის თანახმად, უკვე გაიზარდა ევროკავშირის საგარეო პოლიტიკური უწყების ბიუჯეტი - კერძოდ, 2019 წლის ბიუჯეტში სტრატეგიულ კომუნიკაციებზე 5 მილიონი ევრო დაიხარჯება. ორი წლის განმავლობაში დაგეგმილია იმ უწყების თანამშრომელთა გაზრდა, რომელსაც დეზინფორმაციის გამოვლენა ევალება.

2019 წლის მარტიდან დეზინფორმაციულ კამპანიებზე სწრაფი რეაგირების სისტემაც ამოქმედდა, რომლის საშუალებითაც ევროკავშირის წევრი ქვეყნები ყალბი ამბების გავრცელების შესახებ ინფორმაციას მარტივად და სწრაფად მიიღებენ.

სახელმძღვანელოში - **„კიბერუსაფრთხოება და პოლიტიკა, სოციალურად და რელიგიურად მოტივირებული კიბერთავდასხმები“,** რომელიც 2009 წელს **ევროპარლამენტმა** გამოსცა, განმარტებულია, რომ კიბერუსაფრთხოების ნებისმიერი ანალიზისას პირველი ნაბიჯი უნდა იყოს კიბერსაფრთხეების სპექტრის დიაგრამა, რაც არსებული გამოწვევებით არის განპირობებული და გამოწვეულია **ICT**-ის **(Information and communications technology)** აღჭურვილობის საშუალებით. **ICT**-ი არის საკომუნიკაციო ტექნოლოგია, არის ინფრასტრუქტურა და კომპონენტები, რომლებიც იძლევა თანამედროვე გამოთვლის საშუალებას. **ICT**-ის ერთიანი უნივერსალური განსაზღვრება არ არსებობს, ეს არის ზოგადად მიღებული ტერმინი და გულისხმობს ყველა მოწყობილობას, ქსელის კომპონენტებს, პროგრამებსა და სისტემებს, რომლებიც კომბინირებულ საშუალებას აძლევს ხალხს და ორგანიზაციებს, ურთიერთქმედებაში იყვნენ ციფრულ სამყაროსთან. მაგალითად - ბიზნესი, არაკომერციული სააგენტოები, მთავრობები და კრიმინალური საწარმოები.

„კომუნიკაციების საშუალებამ მკვეთრად შეცვალა გლობალური კიბერსაფრთხის განტოლება. **ICT** სისტემა შეიძლება გამოყენებულ იქნეს ბოროტი საქმიანობისთვის, როგორც ინსტრუმენტი სახელმწიფო დონის

აგრესიაში. ამის გაკეთება შესაძლებელია ინდივიდუალურადაც - მაგალითად ჰაკინგი სხვადასხვა დაჯგუფებების, კრიმინალების, ტერორისტების, მთავრობების მიერ ორკესტრირებული გეგმის განხორციელებით“.[69]

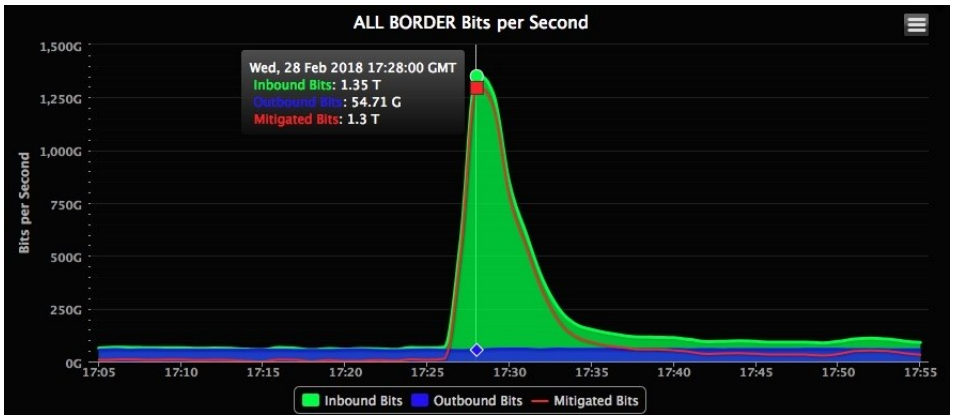
როდესაც საქმე ეხება ჰიბრიდულ ომს, კიბერ-თავდასხმებს, ჰაკერულ თავდასხმებს, ფეიკ-ნიუსების, ანუ ყალბი ახალი ამბების გავრცელებას, დასავლეთში მუდმივად რატომ მიუთითებენ რუსეთზე? მაგალითად, 2019 წლის 17 იანვარს სოციალურ ქსელ **"ფეისბუქიდან"** და **"ინსტაგრამიდან"** ასობით გვერდი, ჯგუფი და ანგარიში წაშალეს. ყველა ეს გვერდი, ჯგუფი და ანგარიში იმართებოდა რუსეთიდან, კოორდინირებულად მოქმედებდა და სხვადასხვა ქვეყნების აუდიტორიაზე გათვლილ ინფორმაციას ავრცელებდა. მათ შორის იყო რამდენიმე, რომლის სამიზნე ქართველი მომხმარებლები იყვნენ. როგორც **"ფეისბუქის"** ადმინისტრაციაში განმარტეს, ანგარიშების და გვერდების უმრავლესობა რუსული საინფორმაციო სააგენტო **„სპუტნიკის“** თანამშრომლებს ეკუთვნოდათ. ეს არ არის პირველი შემთხვევა, როდესაც საქართველო რუსეთიდან მომავალი ყალბი ინფორმაციისა და კოორდინირებული საინფორმაციო კამპანიის მსხვერპლი ხდება. როგორც ჰელსინკში მდებარე ჰიბრიდული საფრთხეების საწინააღმდეგო ევროპული ცენტრის თანამშრომელი **ვიტაუტას კერსანსკასი** აცხადებს, რუსეთის ამოცანაა, საზოგადოების სხვადასხვა ჯგუფებს შორის უთანხმოების გამოწვევა, დაძაბულობის ესკალაცია საზოგადოებასა და მთავრობას შორის, ასევე მოკავშირე ქვეყნების დაპირისპირება. უნდა ვებრძოლოთ დეზინფორმაციას და ყალბ ამბებს, რადგან ის ნეგატიურ ზემოქმედებას ახდენს მოქალაქეთა აზროვნებაზე. მეტიც, არსებობს შესაძლებლობა, რომ მოქალაქეებმა სხვა სახელმწიფოების კარნახით დაიწყონ მოქმედება. მაგალითად, არჩევნებში ხმა მისცენ უცხო ქვეყნის

[69] Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks, London: Publisher European Parliament, 2009, pp 8-9.

მიერ მხარდაჭერილ კანდიდატს ან მიიღონ მონაწილეობა ისეთ საპროტესტო აქციაში, რომელიც უცხო ქვეყნის ინტერესებშია.[70]

რეკორდული სიძლიერის კიბერთავდასხმა

ჩვენ შეგვიძლია უამრავი მაგალითის მოყვანა გახმაურებულ ან არც თუ ისე მასშტაბურ კიბერთავდასხმებზე. ყველაზე მასშტაბური თავდასხმა მსოფლიოში ერთ-ერთ წარმატებულ კომპანიაზე - **„Github"**-ზე მოხდა. აღნიშნული კომპანია წარმოადგენს დეველოპერების ინტერესის სფეროს. **„Github"**-ის ვებ-გვერდზე შეგიძლიათ ატვირთოთ და მართოთ თქვენი პროექტები, შექმნათ სხვადასხვა პროგრამები. კომპანია აერთიანებს 40 მილიონზე მეტ დეველოპერს. 2018 წელს **„Github"**-ზე განცხორციელდა **DDos** რეკორდული კიბერთავდასხმა და რეალურად ვებ-გვერდმა ამ კიბერშეტევას გაუძლო.



***დიაგრამა 1** - DDos რეკორდული კიბერთავდასხმა „Github"-ზე*

***წყარო:** https://www.wired.com/story/github-ddos-memcached/*

დიაგრამა 3-ზე ვხედავთ, რომ 1.3 ტერაბაიტი სიმძლავრის თავდასხმა განხორციელდა, მაგრამ თავდაცვისთვის 1.35 ტერაბაიტი იყო გამოყოფილი, კიბერთავდასხმის პროცესში, რამდენიმე საათის განმავლობაში საიტი თითქმის გაჩერდა, სისწრაფე დაცემული იყო და პროექტები არ ჩანდა, უამრავი პროექტი დაიკარგა, მაგრამ ეს ყველაფერი შემდგომ აღადგინეს. **"Github"**-ს იცავს მსოფლიოში ერთ-ერთი ყველაზე წარმატებული კომპანია

[70] კერსანსკასი ვ. "დეზინფორმაციასთან და ყალბ ამბებთან საბრძოლველად მარტივი და სწრაფი გზა არ არსებობს, ეს გრძელვადიანი სტრატეგიაა". საქართველოს საზოგადოებრივი მაუწყებელი, 2019, გვ. 1. https://1tv.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020

კიბერუსაფრთხოების მიმართულებით - **„Akamai”.** აღნიშნული შეტევის შემდეგ რამდენიმე საათში „**Akamai”**-ს ვებ-უსაფრთხოების ვიცე-პრეზიდენტმა **ჯოშ შულმა** განაცხადა, რომ მათ თავიანთი შესაძლებლობები გაზარდეს ხუთჯერ, რაც ინტერნეტსივრცეში არავის უნახავს. შულმა აღნიშნა, რომ შეუძლიათ, იგივე სიმძლავრის შეტევას კიდევ გაუმკლავდნენ: „ჩვენ გავზარდეთ შესაძლებლობები ხუთჯერ, ეს რეკორდული კიბერთავდასხმა იყო. მე დარწმუნებული ვარ, შემდეგ შეტევასაც გაუმკლავდებით, თუ ის 1.3 Tbps არ აღემატება. თავდაჯერებულობა ერთია, მაგრამ მეორეა რეალობა, არ ვიცით, შემდეგი თავდასხმა რამდენად მძლავრი იქნება“.[71]

ანტივირუსი როგორც ერთ-ერთი თავდაცვითი მექანიზმი

ვირუსების და კიბერთავდასხმების ფონზე აქტიურად ხდება მათი შემაკავებელი მექანიზმების გამოგონება, პირველი ანტივირუსი **1984 წელს ჰოპკინზმა შექმნა,**[72] დღეს კი არსებობს უამრავი ანტივირუსული კომპანია, რომლებიც მუშაობენ ანტივირუსების შექმნაზე, ისინი გვთავაზობენ გარკვეულ ფასად ჩვეულებრივ ანტივირუსულ პროგრამებს, თუმცა ასევე დიდი კომპანიებისთვის შემუშავებული აქვთ ბიზნეს-ანტივირუსებიც, რომელიც ანტივირუსის სრულ პაკეტს მოიცავს. რთული სათქმელია, რომელ ანტივირუსზე შეიძლება ვთქვათ, რომ სრულიად უზრუნველყოფს დაცვას, რადგან ყველა ანტივირუსს აქვს რაღაც პლიუსი და რაღაც მინუსი, მაგრამ ჩვენ შეგვიძლია განვიხილოთ მონაცემები, თუ როგორ მუშაობენ ისინი. ამ მხრივ ერთ-ერთ ყველაზე დიდ კორპორაციას წარმოადგენს **„კასპერსკი“**.

„კასპერსკი“ წარმოადგენს რუსულ კომპანიას, რომელსაც ოფიციალურად იყენებენ სხვადასხვა ქვეყნებში, მათ შორის აშშ-ის სახელმწიფო

[71] Newman H. L. GitHub Survived the Biggest DDoS Attack Ever Recorded, Media Company Wired, 2018, p 1. https://www.wired.com, უკანასკნელად იქნა გადამოწმებული - 16.06.2020.
[72] Leiden J. The 30-year-old prank that became the first computer virus, Information Technology Company The Register, 2012, p 1. https://www.theregister.com, ბოლოს იქნა გადამოწმებული - 09.08.2020.

სააგენტოებში. არსებობს ეჭვი, რომ ის არის მოქცეული რუსეთის მთავრობის გავლენის ქვეშ და შესაძლოა, წარმოებულ პროდუქციაში დამატებულია ჰაკერული სისტემა ინფორმაციის გადმოსაქაჩად. თუმცა **„კასპერსკი“** ყველა წაყენებულ ბრალდებას თუ მსგავს მოსაზრებას უარყოფს. გავეცნოთ **Kaspersky Security Network**-ის სტატისტიკას, რომელიც გამოქვეყნებულია ელექტრონულად და მოპოვებულია **KSN**-ის განაწილებული ანტივირუსული ქსელების გამოყენებით, რომელიც მუშაობს ანტიმავნე დამცავი კომპონენტებით. მონაცემები შეგროვდა **KSN**-ის მომხმარებლებისგან, რომლებიც დათანხმდნენ ინფორმაციის მიწოდებაზე. **Kaspersky Lab**-ის მილიონობით მომხმარებელი მონაწილეობს მავნე საქმიანობის შესახებ ინფორმაციის გლობალურ გაცვლაში. მისი უსაფრთხოების ქსელის თანახმად: **Kaspersky Lab**-ის გადაწყვეტილებებმა დაბლოკა **989 432 403** შეტევა, რომლებიც განხორციელებულია ონლაინ რესურსებიდან მსოფლიოს **203** ქვეყანაში. **560 025 316** უნიკალური **URL** იქნა აღიარებული, როგორც მავნე ვებ-გვერდის საწინააღმდეგო კომპონენტები. **Malware** პროგრამის მეშვეობით, რომელიც შექმნილია ფულის მოპარვის მიზნით, საბანკო ანგარიშებზე ინტერნეტით წვდომის გზით, **197 559** მომხმარებლის კომპიუტერებში დაიბლოკა. **Ransomware** შეტევებს, რომელიც იყო **229 643** უნიკალური მომხმარებლების კომპიუტერებზე „კასპერსკის“ ანტივირუსი გაუმკლავდა. ამ ანტივირუსმა აღმოაჩინა **230 051 054** უნიკალური მავნე და პოტენციურად არასასურველი ობიექტები. „კასპერსკის“ პროგრამებმა მობილური მოწყობილობებისთვის დასაცავად გამოავლინა **870 617** მავნე ინსტალაციის პაკეტი, **13 129** სამონტაჟო პაკეტი და მობილური საბანკო ტროიანები. ასევე **13 179** სამონტაჟო პაკეტი მობილური **Ransomware Trojan**-ი.

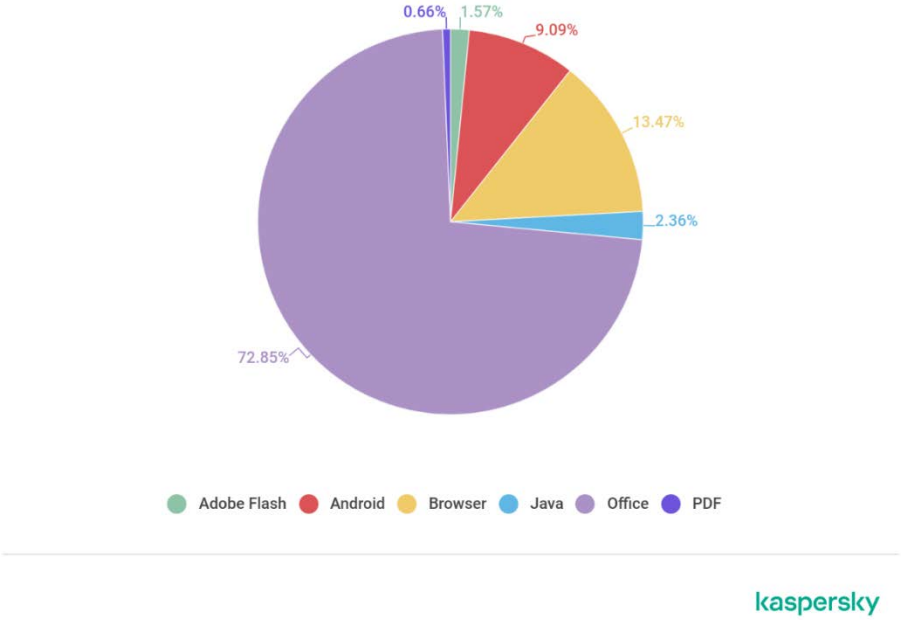
კიბერდანაშაულების მიერ გამოყენებული ექსპლუატაციების განაწილების შესახებ სტატისტიკის თანახმად, **Microsoft Office**-ის აპლიკაციების ნაკრებში დიდი ნაწილი დაუცველია **(73%)**. ყველაზე გავრცელებული შეცდომები ბოლო კვარტალში იყო **(CVE-2017-11882, CVE-2018-0802) Equation Editor**

პროგრამაში, რომელიც ადრე **Microsoft Office**-ის შემადგენლობაში შედიოდა. ბოლო მონაცემებით, **Microsoft Office**-ში დაუცველია **CVE-2017-8570, CVE-2017-8759, CVE-2017-0199.**

თანამედროვე ვებ-ბრაუზერი კომპლექსური და მოცულობითია კოდური პროგრამული უზრუნველყოფის თვალსაზრისით, რაც იწვევს ახალი ხარვეზების აღმოჩენას **(13%)**. კიბერთავდასხმებისთვის ყველაზე გავრცელებული სამიზნე მასობრივ გარემოში **Microsoft Internet Explorer** ბრაუზერია. მაგალითად, **Google Chrome**-ს ბრაუზერში, რომელმაც მიიღო განახლებული ინფორმაცია რამდენიმე კრიტიკულ დაუცველობაზე **(CVE-2019-13685, CVE-2019-13686, CVE-2019-13687, CVE-2019-13688),** არ იყო პრობლემების გარეშე.

სისტემაში პრივილეგიის ესკალაციისკენ მიმართული დაუცველობის უმეტესი ნაწილი მოდის ოპერატიული სისტემის ინდივიდუალურ სერვისებზე და მომხმარებლებს შორის პოპულარულ პროგრამებზე. პრივილეგიების ესკალაციის დაუცველობებს განსაკუთრებული როლი ენიჭებათ, რადგან ისინი ხშირად იყენებენ მავნე პროგრამებს **(malware)** სამიზნე სისტემის შემდგომი გამოსწორებისთვის.

Google-ის მკვლევარმა გამოაქვეყნა ინსტრუმენტი ამ პრობლემის დემონსტრირებისთვის - **CtfTool**, რომელიც საშუალებას გაძლევთ, დაიწყოთ პროცესები სისტემის პრივილეგიებით, ასევე შეიტანოთ ცვლილებები სხვა პროცესების მეხსიერებაში და შეიყვანოთ თვითნებური კოდი.

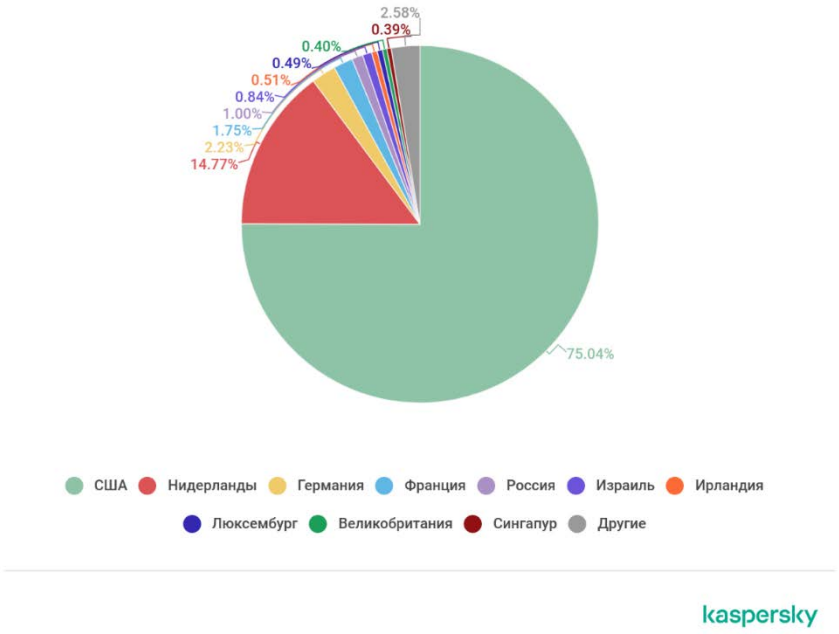


დიაგრამა 2 *- დაუცველი აპლიკაციების დიაგრამა*

წყარო: *https://securelist.ru/it-threat-evolution-q3-2019-statistics/95163/*

Kaspersky laborator- ასევე აქვეყნებს მონაცემებს წყარო ქვეყნების ვებ-თავდასხმების ტოპ-ათეულს. ვებ-გვერდებზე კიბერშეტევების გეოგრაფიული წყაროს დასადგენად **„კასპერსკიმ“** გამოიყენა დომენის სახელის შედარებადი რეალური **IP** მისამართი, რომელზეც მდებარეობს აღნიშნული დომენი,. შესაბამისად, დაადგინეს ამ **IP** მისამართის **(GEOIP)** გეოგრაფიული ადგილმდებარეობა.

როგორც ზემოთ აღვნიშნეთ, 2019 წლის მესამე კვარტალში Kaspersky Lab-ის გადაწყვეტილებებმა მოიგერია **989 432 403** თავდასხმა, რომელიც განხორციელდა ინტერნეტრესურსებიდან მსოფლიოს **203** ქვეყანაში. დაფიქსირდა **560 025 316** უნიკალური **URL,** რომლებზეც იქნა დაყენებული ვებ-ანტივირუსი. ტოპ ქვეყნების სია კი სტატისტიკურად ასე გამოიყურება:



დიაგრამა 3 *- კომპანია კასპერსკის დიაგრამა, სადაც გამოსახულია ვებ-თავდასხმების ტოპ-ათი ქვეყანა*

წყარო: *https://securelist.ru/it-threat-evolution-q3-2019-statistics/95163/*

აშშ (75,04%), ნიდერლანდები (14,77%), გერმანია (2,23%), საფრანგეთი (1,75%), რუსეთი (1,00%), ისრაელი (0,84%), ირლანდია (0,51%), ლუქსემბურგი (0,49%), დიდი ბრიტანეთი (0,40%), სინგაპური (0,39%), და სხვა (2,58%).

როგორ უნდა დავიცვათ თავი კომპიუტერულ ქსელებზე კიბერთავდასხმებისგან? ამის შესახებ თეორიულ მეთოდებს შეგვიძლია გავეცნოთ სახელმძღვანელოში - **„კიბერ ოპერაციები, მშენებლობა, დაცვა და თავდასხმა, თანამედროვე კომპიუტერული ქსელები“**, რომლის ავტორიც გახლავთ **მაიკ ოლილე.** ის თავის წიგნში კომპიუტერულ ოპერაციებს განიხილავს სისტემურ დონეზე:

„კიბერდაცვა, ეს ვერ აიხსნება, თუ არ ავხსნით **“windows”**-ის და **Linux**-ის მთელი სამუშაო პროცესის. მათ შორის **Centos, Mint, OpenSuSE** და **Ubuntu** სისტემები. ეს შეიძლება იყოს ფიზიკური ან ვირტუალური სისტემები, რომლებიც აშენებულია **VMWARE Workstation**-ით ან **VirtualBox**-ით. კიბერშეტევისას თავდამსხმელს, რომელიც იმყოფება სისტემაში, სურს

შეინარჩუნოს ე.წ. დაშვება, ამიტომ ის მუდმივად ახორციელებს თავდასხმას. ჩვენ შეგვიძლია ვაჩვენოთ შეტევების სპექტრი, მათ შორის, **internet Exprorer**-ის, **Firefox**-ის, **Java**-ს და **Adobe Flash**-ის წინააღმდეგ გამოყენებული. ასეთი კიბერშეტევები ქსელში ტოვებს კვალს და თუ ჩვენ გვაქვს პროგრამულად ჭკვიანური დაცვა, მაშინ შეგვიძლია ამის ნახვა".[73]

[73] Mike O. Cyber Operations Building, Defending, and Attacking Modern Computer Networks, Marilend: Publishing House Apress, Department of Mathematics, Towson University, 2015, pp 237-265.

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

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".**[74]

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** ამ საკითხს ასე განმარტავს: "მხოლოდ მოყვარულები უტევენ მანქანებს, პროფესიონალები მიზანში იღებენ ადამიანებს".[75]

მაგალითისთვის ავიღოთ ჰაკერების ერთ-ერთი თავდასხმის ტექნიკა, რომელსაც ჰქვია **"ფიშინგი"**. ფიშინგის შეტევისას თავდამსხმელი, რომელიც ცდილობს, კომპიუტერულ სისტემაში შეაღწიოს, უპირველეს სამიზნეს წარმოადგენს მომხმარებელი და არა ავტომატიზებული დაცვის მექანიზმის გატეხვა. თავდამსხმელი მომხმარებლებს უგზავნის შეტყობინებას ელფოსტით, სადაც ყალბი ვებ-გვერდია მითითებული, თუმცა ის

[74] Cherry K. History and Key Concepts of Behavioral Psychology, publisher very well mind company, 2019, p 1. https://www.verywellmind.com/, ბოლოს იქნა გადამოწმებული - 27.08.2020.

[75] Schneier B. Psychology and Usability - Only amateurs attack machines; professionals target people, London: University of Cambridge, Department of Computer Science and Technology The Computer Laboratory, 2017, Chapter 3, pp 1-2.

ორიგინალს ჰგავს. მაგალითად, ეს შეიძლება იყოს ბანკის შეტყობინება, რომელიც თითქოს სანდოობის გარანტია, მაგრამ თუ ადრესატი ყალბ ბმულს გახსნის, ამან შეიძლება უნებლიედ გამოიწვიოს თავდამსხმელის წვდომა პირად ინფორმაციაზე.

სისტემა, რომელიც მიზნად ისახავს მომხმარებლების დაცვას, საჭიროებს **ბიჰევიორისტული** მეთოდოლოგიის გამოყენებას. მეცნიერებს შეუძლიათ, კიბერუსაფრთხოების ექსპერტებს ორ ფრონტზე დაეხმარონ: პირველი - სისტემის დაცვის გაუმჯობესებაში, ასწავლონ მომხმარებლებს, თუ როგორ შეიძლება ადამიანურმა ბუნებამ მომხმარებლები დაუცველები გახადონ; მეორე - მათ შეუძლიათ, გამოიყენონ ცოდნა ადამიანის ბუნებაში, დაეხმარონ საგანმანათლებლო კამპანიების შემუშავებაში, რომლებიც მომხმარებლებს აფრთხილებენ კიბერშეტევების შესახებ.

კიბერშეტევების წინააღმდეგ ბრძოლისთვის ამერიკის შეერთებული შტატების არმია აქტიურად იყენებს ბიჰევიორიზმის თეორიას. კიბერბიჰევიორიზმის მოდელის ანალიზი, ანუ თანამედროვე კომერციული მეთოდი, გაჩნდა აშშ-ის არმიის მიერ ჩატარებული **(Cyber Quest 2017)**[76] ღონისძიების შემდეგ, როგორც კიბერ საფრთხეზე ერთ-ერთი პასუხი. **პოლკოვნიკ სტივენ რენის** აზრით, მთავარია კიბერქსელში ტრეფიკის და მომხმარებლის ქცევის ნორმალური მონიტორინგი, ამის შემდეგ შეიძლება განისაზღვროს სიტუაცია და ქმედება, რომელიც მიუთითებს ჰაკერის მხრიდან კიბერთავდასხმაზე ან კიბერშეჭრაზე სისტემაში.[77]

კომერციული დეველოპერების მტკიცებით, კიბერსივრცეში არსებობს ოთხი ფენა - **ფიზიკური, ქსელური, სოციალური და პერსონალური.** საფრთხეების მონიტორინგი მოიცავს **ბიჰევიორისტული** მონაცემების შეგროვებას თითოეულ ფენაზე, შემდეგ ამ მონაცემების კორელაციასა და კომბინირებას.

[76] Schmidt R. Cyber Quest, Action Impact LLC, 2017, p 1. https://www.actionimpact.com, ბოლოს იქნა გადამოწმებული - 27.08.2020.

[77] Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, p 1. https://www.mitre.org, ბოლოს იქნა გადამოწმებული - 27.08.2020.

ამერიკელი სამხედრო პოლკოვნიკის, **რენის** აზრით, ბიჰევიორიზმის თეორია არ იხილავს წესებს, არამედ ამ თეორიის საშუალებით ჩვენ ვუყურებთ კიბერქსელში ცხოვრების წესს. ეს სისტემა კი ასე მუშაობს: მონიტორინგის დროს, მაგალითად, ერთი სერვერი ყოველთვის ამყარებს კონტაქტს მეორე სერვერთან, მაგრამ რაღაც დროის გასვლის შემდეგ იგი როუტერთან შედის კავშირში ან სხვა სერვერთან. ამ შემთხვევაში ხდება დეტალური დაკვირვება და ანალიზი. სერვისების შიდა ქსელებზე გამოყენების შემთხვევაში, ქცევითი ანალიზის მეთოდი მნიშვნელოვანი ინსტრუმენტი იქნება იმისთვის, რომ შეამცირონ კიბერშეტევებისა და უსაფრთხოების დარღვევის რისკები.[78]

გასაკვირი არ არის, რომ ამ მეთოდოლოგიის გამოყენება ქმნის ფართო მონაცემების პრობლემას. თუმცა **გენერალ მორისონის** თქმით: "გამოსავალი ხელოვნური ინტელექტისა და მანქანიდან მანქანაში სწავლის ტექნოლოგიის შექმნაა, ხელოვნური ინტელექტი საშუალებას მოგვცემს, გაცილებით სწრაფი რეაგირება მოვახდინოთ კიბერსივრცეში მიმდინარე მოვლენებზე. უნდა იყოს თითოეული ბიტის და ბაიტის მონაცემების ანალიზი, მანქანა კი ამბობს, რომ ხდება რაღაც, რაც ჩვეულებრივ არ ხდება ხოლმე ქსელში, შემდეგ კი იქმნება სიტუაცია, რომ ყველაფერი შემოწმებას დაექვემდებაროს".[79]

ბიჰევიორიზმის თეორიის შესწავლა, გარჩევა, გაანალიზება და ათვისება საჭიროა როგორც კერძო სექტორში მომუშავე პროგრამისტებისთვის, ასევე სახელმწიფო უწყებებში დასაქმებულთათვის. ჩვენ ელფოსტის საშუალებით თითქმის ყოველდღიურად ვიღებთ უამრავ შეტყობინებას სხვადასხვა ქვეყნებიდან თუ ორგანიზაციებიდან, ამ დროს არ ვიცით, რა არის ყალბი და რა არის ნამდვილი. თუ გვინდა, თავი დავაღწიოთ სერიოზულ საფრთხეებს,

[78] Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, p 1. https://www.mitre.org, ბოლოს იქნა გადამოწმებული - 27.08.2020.

[79] Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, p 1. https://www.mitre.org, ბოლოს იქნა გადამოწმებული - 27.08.2020.

ჰაკერებს არ ჰქონდეთ წვდომა ჩვენს პირად ინფორმაციაზე, ადგილი არ ჰქონდეს ეფექტურ კიბერთავდასხმებს, მაშინ უნდა გავიაზროთ და ვისწავლოთ ასევე ეფექტური წინააღმდეგობის გაწევა.

აქვე მნიშვნელოვანია განვსაზღვროთ, თუ რა შეცვალა და რა შეიძლება შეცვალოს **Covid-19**-მა მსოფლიო მასშტაბით, რას შეცვლის კიბერომების თვალსაზრისით? ფაქტია, ვირუსმა ცხოვრების დღის წესრიგი შეცვალა, საფრთხე შეუქმნა როგორც ადამიანის ჯანმრთელობას, ასევე ეკონომიკას. საფრთხე მრავალმხრივია - ჩაიკეტა საზღვრები, აიკრძალა ფრენები, უამრავ ქვეყანაში გამოცხადდა კარანტინი, საგანგებო სიტუაცია, კომენდანტის საათი, გადაადგილების შეზღუდვა. მოვლენების ასე დრამატულ განვითარებას არავინ ელოდა. ყველა თანხმდება იმაზე, რომ ვირუსი გაივლის, ოდესღაც გაქრება, მაგრამ ცხოვრება ისეთი აღარ იქნება, როგორიც **მანამდე** იყო. რეალურმა სამყარომ დიდი დოზით გადაინაცვლა ვირტუალურ სივრცეში, უამრავი კომპანია და სახელმწიფო უწყება გადავიდა დისტანციურ მუშაობაზე. ამ ფონზე ძალიან დიდ სარგებელს იღებენ ჰაკერები, სპამერები, თაღლითები და ისეთი ადამიანები, რომლებიც ინტერნეტსივრცეს და სოციალურ ქსელებს პირადი ინტერესებისთვის იყენებენ.

მაგალითად, ამ მხრივ **(„ფიშინგით“)** თაღლითობა აქტიურად დაიწყო ვირუსის გავრცელების დღიდან. მავანნი ცდილობენ, უფრო მეტი შიში და დაბნეულობა დანერგონ ინტერნეტმომხმარებლებში. გახშირდა ჰაკერული თავდასხმები სამედიცინო კლინიკებზე გამოსასყიდის სანაცვლოდ. თავდასხმებმა შეაჩერა ოპერაციები და გამოიწვია გადადება. ასეთი შეტევები უდიდეს საფრთხეს უქმნის პაციენტების ჯანმრთხელობას.

მოვლენების კვალდაკვალ, **„ვაშინგტონ პოსტმა“** გამოაქვეყნა სტატია სათაურით: **„ჰაკერები კორონავირუსთან დაკავშირებულ შიშებს იყენებენ პირადი მონაცემების მოსაპარად“**. აღნიშნულ სტატიაში განხილულია კორონავირუსის შემდეგ ჰაკერული თავდასხმების ნაკადის მზარდი მატება. ისრაელში მომუშავე კიბერუსაფრთხოების ორგანიზაციამ **„Check Point“**-მა

გამოაქვეყნა ანგარიში, სადაც გამოკვეთილია ყველაზე ეფექტურად მომუშავე ჰაკერული ჯგუფის მიერ წამოწყებული კამპანია, რომელსაც უწოდეს **“Vicious Panda”** („მოწინავე საფრთხე“). ანგარიშში ნათქვამია, რომ **“Vicious Panda”**-მ, ანუ ჰაკერულმა ორგანიზაციამ, გამოიყენა ყალბი დოკუმენტები, გაავრცელა ფეიკ-ინფორმაციები მონღოლეთის ჯანდაცვის მინისტრის სახელით. თითქოს ის საშინელ მდგომარეობას ამცნობდა მსოფლიოს. ჰაკერების მიზანი იყო, რაც შეიძლება ბევრ ადამიანს უნდა გაეხსნა ეს ინფორმაცია, შემდეგ კი მათ წვდომა ექნებოდათ მომხმარებელთა პირად მონაცემებზე. ეს იქნებოდა სმარტოფნებისა თუ კომპიუტერების საშუალებით. ანგარიშში **“Check Point”**-ის თავდაცვის დაზვერვის უფროსის, **ლატე ფინკლინტინის** განცხადებაცაა მოცემული, ის აფრთხილებს საჯარო სექტორს, სატელეკომუნიკაციო კომპანიებს: „**Covid-19** წარმოადგენს არა მხოლოდ ფიზიკურ საფრთხეს, არამედ კიბერსაფრთხესაც, ყველა საჯარო სექტორის სუბიექტი და სატელეკომუნიკაციო კომპანია უნდა იყოს ფრთხილად კორონავირუსის გარშემო არსებულ დოკუმენტაციასთან და ვებსაიტებთან“.[80]

კიბერუსაფრთხოების დამოუკიდებელი ექსპერტის, **ლუკას ოლეჯინიკის (Lukasz Olejnik)** თქმით, დღეს ამ მასშტაბური გლობალური კრიზისის დროს მსოფლიო სრულიად არის დაუცველი და შესაძლოა, ვითარება უფრო გაუარესდეს.[81]

ამ შემთხვევაში არც საქართველოა გამონაკლისი, აქ უფრო მცირე დოზით, მაგრამ მაინც ხდება მსგავსი თავდასხმები, როგორც ჰაკერულ, ასევე ინფორმაციულ დონეზე. მაგალითად, ჰაკერებმა საქართველოს **4 934 863** მოქალაქის (მათ შორის გარდაცვლილი პირების) პერსონალური ინფორმაცია გამოაქვეყნეს. ამ საკითხს ამერიკულმა გამოცემამ - **ZDNet**-მა

[80] Timberg C., Romm T., Hackers are seizing on coronavirus fears to steal data, researchers and U.S. regulators warn", The washingtonpost, 2020, p 1. https://washingtonpost.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.

[81] Newman H. L. Coronavirus Sets the Stage for Hacking Mayhem, Media Company Wired, 2020, p 1. https://www.wired.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.

ვრცელი სტატია მიუძღვნა.[82] რა საჭირო იყო პირადი მონაცემების მოპოვება-გავრცელება? ეს ადამიანების დაუცველობის სინდრომის გაღვივებას და პანიკის დათესვას ემსახურება. მით უმეტეს, როდესაც ქვეყანაში დეზინფორმაციული სააგენტოები და ტელეკომპანიები სჭარბობს, რომლებიც ამ მასალას უფრო მეტად მძაფრად აწვდიან მოსახლეობას, ვიდრე ეს რეალურადაა. აღნიშნული ბაზების ლინკებზე მითითებული იყო, რომ ინფორმაციის წყაროს ცენტრალური საარჩევნო კომისიის სისტემა წარმოადგენდა. თუმცა ეს ინფორმაცია არ დადასტურდა. ცენტრალურმა საარჩევნო კომისიამ გააკეთა განცხადება, სადაც ხაზგასმით წერია, რომ მონაცემთა ბაზა რადიკალურად განსხვავდება იმისგან, რაც მათ სისტემაში ინახება. ფაქტობრივად, ეს ბაზა არ შეიცავს ისეთ პირად მონაცემებს, რაც ჩვენს მოსახლეობას შეუქმნის საფრთხეს, მაგრამ ამ მონაცემების გავრცელება მაინც დანაშაულია. ისეთ ადამიანებზე, ვინც ტექნოლოგიებში ვერ ერკვევა, უჩნდება შიში და დაუცველობის განცდა, მიზანიც ზუსტად ეს იყო.

საქართველოს მოსახლეობას საგანგებო მდგომარეობის პერიოდში უგზავნიდნენ შეტყობინებებს, რომლებიც შეიცავდა დეზინფორმაციას: **“UCKEBA”**, რომლის შინაარსია: ,,თქვენ დაჯარიმდით კომენდანტის საათის დარღვევის გამო, ჯარიმის ოდენობა 3000 ლარი. **R.M. police.ge".**[83] ეს კიდევ უფრო ამყარებს ეჭვებს, რომ მიზანმიმართულად ხდებოდა მოსახლეობაში პანიკის დათესვა. შინაგან საქმეთა სამინისტრომ განაცხადა, რომ აღნიშნული მოკლე ტექსტური შეტყობინებები არ შეესაბამებოდა სინამდვილეს და ეს არ იყო გაგზავნილი მათ მიერ. ინტერნეტსივრცეში გაჩნდა უამრავი ვებ-გვერდები და სტატისტიკური მონაცემები, რომლებიც რეალობას სცდებოდა, ჰაკერები სხვადასხვა ვებ-გვერდების საშუალებით მანიპულირებდნენ კორონავირუსის სტატისტიკით. რიცხვებით თამაშმა კი

[82] Catalin C. Personal details for the entire country of Georgia published online, 2020, p 1. https://www.zdnet.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.

[83] "შსს-ს სახელით მოქალაქეებს მესიჯები მიუვიდათ - რა განცხადებას ავრცელებს სამინისტრო", საქართველოს შინაგან საქმეთა სამინისტრო 2020, გვ. 1. https://www.ambebi.ge, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.

საზოგადოებაში პანიკა გამოიწვია. ინტერნეტმომხმარებლები უნებურად ხდებიან ინტერნეტვირუსების მსხვერპლნი, ინფორმაციის მოძიებისას ავტომატურად გადადიან ისეთ ვებ-გვერდებზე, სადაც ხდება დავირუსებული პროგრამის ჩამოტვირთვა. ჰაკერები უნებართვო წვდომას იღებენ სხვადასხვა მანიპულაციების საშუალებით. ასეთი მაგალითები უკვე გამოქვეყნდა და შესწავლაც აქტიურად მიმდინარეობს. ერთ-ერთი ასეთი ვიდეო გამოაქვეყნა **GEORGIAN HACKERS COMMUNITY – GHC**-მა. ვიდეოში ნაჩვენებია, **Corona-virus-map.com.exe**, რომლის ფაილიც შეიცავს თავისი შიგთავსით **AZORult malware**-ის, რომელიც წლების წინ შეიქმნა ინფორმაციის მოპარვისთვის. **AZORult** თქვენი ბრაუზერის **cooki**-ებიდან იპარავს მონაცემებს, ყველაფერი, რაც კი დამახსოვრებული აქვს ბრაუზერს თქვენს კომპიუტერში - პაროლები, პირადობის ნომერი და ა.შ. აძლევს ჰაკერს წვდომას თქვენს მონაცემებზე, რაც ძალიან დიდ საფრთხეს უქმნის პირადი მონაცემების დაცვას და მათ გამოყენებას უნებართვოდ.[84]

ციფრული ვალუტა

კრიპტო-ვალუტა - ბოლო წლებში საბანკო-საფინანსო სფერომ ძალიან დიდი განვითარება ჰპოვა. სწორედ ამას უკავშირდება ელექტრონული ვალუტის შექმნა. რა არის ციფრული ფული? რით განსხვავდება სტანდარტული, ანუ ტრადიციული ვალუტისგან?

მაგალითისთვის ავიღოთ ერთ-ერთი პირველი და პოპულარული **კრიპტო-ვალუტა - ბიტკოინი,** რომელიც ქსელში 2008 წელს გამოჩნდა. მისი შექმნა **სატოში ნაკამოტოს** სახელით ცნობილ პროგრამისტს უკავშირდება. კრიპტო-ვალუტა სტანდარტული ვალუტისგან განსხვავებით არ იბეჭდება. იგი წარმოიქმნება, ინახება და იხარჯება ელექტრონულად. ის არ კონტროლდება არც ერთი სახელმწიფოს და არც ერთი ბანკის მიერ. **ბიტკოინის** წარმოშობა ხდება რთული მათემატიკური ფორმულირების შედეგად კომპიუტერული

[84] ზედელაშვილი თ. „ჰაკერები კორონავირუსთან დაკავშირებულ შიშებს იყენებენ პირადი მონაცემების მოსაპარად“ - უნდა ველოდოთ მასშტაბურ კიბერშეტევებს", მედიაჰოლდინგი "ჯორჯიან თაიმსი", 2020, გვ. 1. http://geotimes.com.ge, უკანასკნელად იქნა გადამოწმებული - 25.06.2020

ქსელების საშუალებით. ტრადიციული ვალუტა ეფუძნება ოქროს ღირებულებას, ხოლო ციფრული ვალუტა ეფუძნება მათემატიკას. ბიტკოინის შექმნის პროცესს მაინინგი ეწოდება.[85]

ციფრული ვალუტის მაინინგისთვის აუცილებელია კომპიუტერებისა და სერვერების სისტემა. ბოლო დროს აქტიურად ჩნდება სპეციალური აპლიკაციები, რომლებიც ციფრული ვალუტის გენერირებას სმარტფონიდან ხდის შესაძლებელს. რაც შეეხება ბიტკოინს, მისი რაოდენობა მსოფლიო მასშტაბით ვერ იქნება **21 000 000-ზე** მეტი. ზოგადად, ციფრულ ვალუტაზე უამრავი ინფორმაცია და დეზინფორმაცია ვრცელდება, მაგრამ უშუალოდ ბიტკოინით განხორციელებული ტრანზაქციის გაყალბება თითქმის შეუძლებელია. ცნობილია, რომ ტრანზაციის მონაცემები ინახება ფრაგმენტულად და არა ერთ სერვერზე. მნიშვნელოვანია, რომ ბიტკოინით ანგარიშსწორება დიდი ხანია დაშვებულია ისეთ ონლაინ-მაღაზიებში, როგორიცაა **eBay, Amazon** და ა.შ.[86]

არსებული რეალობის გათვალისწინებით, შეიძლება გამოვთქვათ ვარაუდი, რომ ციფრული ვალუტის წარმატებით გამოყენებამ გლობალური მასშტაბით და მისმა პოპულარიზაციამ შეიძლება გამოიწვიოს ბეჭდური, ტრადიციული ვალუტის სრულად ჩანაცვლება. დღეს ყველაზე მყარი ციფრული ფული **ბიტკოინია (BTC).**

ელექტრონული ფული „P2P“ ტექნოლოგიაზეა აგებული, ის სრულიად დამოუკიდებელი და დეცენტრალიზირებული ქსელია. სწორედ ეს ქმნის შესაძლებლობას, ნებისმიერმა მომხმარებელმა პირდაპირ გადაიხადოს ან გადასცეს. გადარიცხვას, გადაცემას ამ შემთხვევაში ადასტურებენ ქსელის სხვა მომხმარებლები, რომლებსაც მაინერები ეწოდებათ. დასტური ხერხდება კრიპტოგრაფიული ხელმოწერით და ყოველი ხელმოწერის

[85] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, America: Bitcoin Organization, 2009, pp 1-9.

[86] Hayes A. What Happens to Bitcoin After All 21 Million Are Mined?, Business & Economy Website Investopedia, 2020, p 1. https://www.investopedia.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.

შემდეგ მომხმარებელი გარკვეულ საკომისიოს იღებს. ელექტრონული ვალუტის მინუსს წარმოადგენს არასტაბილურობა, მისი საბაზრო ღირებულება დამოკიდებულია მოთხოვნაზე. ასევე ტრანზაქცია არ არის დაზღვეული, გადარიცხულ ვალუტას უკან ვეღარ დაიბრუნებთ. ელექტრონული ფულის ყიდვისთვის და ვაჭრობისთვის ონლაინ-სავაჭრო ბირჟებია შექმნილი, ყველაზე აქტუალური ბირჟები, **bitpanda** და **binance**-ა. ამ ბირჟების მეშვეობით თქვენ შესაძლებლობა გაქვთ, თქვენივე ბარათით იყიდოთ და გაყიდოთ კრიპტო-ვალუტა.[87] რა თქმა უნდა, აქ არ არის მხოლოდ ბიტკოინი, დღეს უამრავი მსგავსი ვალუტა არსებობს.

საქართველოში **ციფრული ვალუტა** არც თუ პოპულარობით სარგებლობს. თუმცა შეგვიძლია, ისეთი ქვეყნებიც მოვიყვანოთ მაგალითად, სადაც ბიტკოინი ოფიციალურ ღირებულებადაა დაშვებული - აშშ-ში ბიტკოინით დაშვებულია სავაჭრო საქმიანობის წარმოება. თუმცა იმ ქვეყნების რაოდენობა ბევრად სჭარბობს მსოფლიოში, სადაც ცდილობენ, ელექტრონული ვალუტა სამართლებრივად შეზღუდონ და აკრძალონ კიდეც, რადგან ვირტუალური ფული არ არის არც ერთი ეკონომიკური სისტემით ან ფიზიკური ღირებულებებით გამაგრებული. საყურადღებოა ის ფაქტიც, რომ 2015 წელს ევროპის უმაღლესი სასამართლოს დადგენილებით ბიტკოინის ყიდვა ფიზიკური ფულით შესაძლებელი იქნება დღგ-ს გარეშე.[88]

ამ ყველაფრის გათვალისწინებით, კრიპტო-ვალუტის მომავალი მაინც გაურკვეველია. თუმცა ის საკმაოდ მომხიბლავად გამოიყურება, როგორც მსხვილი კომპანიებისთვის, ასევე ცალკეული ადამიანებისთვის. აქვე აღსანიშნავია, რომ ჰაკერები კრიპტოვალუტასაც ძალიან კარგად იყენებენ თაღლითობისთვის, **Ransomware** - ის, ანუ გამოსასყიდის მოთხოვნით ჰაკერები შიფრავენ თქვენს მონაცემებს კომპიუტერში, შემდეგ კი ითხოვენ

[87] გოგუაძე მ. "მომავლის ვალუტა ბიტკოინი – კრიპტოვალუტა", სესხების შემდარეებელი კომპანია „ფინანსერი“, 2017, გვ. 1. https://financer.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.

[88] ჭყოიძე ნ., ტომარაძე გ., "ვირტუალური/კრიპტოგრაფიული ვალუტა და მისი თავისებურებები ვირტუალური ვალუტების რეგულირება (bitcoin-ის მაგალითზე)", თბილისი: გამოცემა “ეკონომიკა და საბანკო საქმე“, 2014, გვ. 41-55.

დიდ ანაზღაურებას მონაცემებზე წვდომის აღდგენის მიზნით. თუმცა გადახდის შემთხვევაშიც თქვენს მონაცემებზე წვდომა არ აღდგება. ამ ტიპის თაღლითობა მეტწილად ხდება ანონიმური კრიპტოვალუტების წყალობით - მაგალითად, ბიტკოინით.

<u>ირანის ისლამური სახალიფოს შემთხვევის გარჩევა</u>

2020 წლის 3 იანვარს ერაყში, ბაღდადის აეროპორტის მახლობლად აშშ-ის სარაკეტო დარტყმას **ირანის ისლამური რევოლუციის** გუშაგთა კორპუსის სპეცდანიშნულების რაზმ **„ალ-კუდსის“** ლიდერი, გენერალი **ყასემ სოლეიმანი** ემსხვერპლა. მოგვიანებით პენტაგონმა ასეთი ინფორმაცია გაავრცელა:

„აშშ-ის პრეზიდენტის, **დონალდ ტრამპის** ბრძანებით, ჩვენმა სამხედროებმა უცხოეთში მყოფი ამერიკელების დასაცავად ქმედითი თავდაცვითი ზომები მიიღეს და გენერალი ყასემ სოლეიმანი მოკლეს. დაჯგუფება **„ალ-კუდსი“**, რომელსაც ის ხელმძღვანელობდა, აშშ-ში ტერორისტული ორგანიზაციების სიაში იყო შეყვანილი. გენერალი **სოლეიმანი** ამერიკელ დიპლომატებზე ერაყსა და მთელ რეგიონში მყოფ სამხედროებზე თავდასხმებს გეგმავდა. **„ალ-კუდსი“** პასუხისმგებელია ასობით ამერიკელი და კოალიციური ჯარის სამხედროთა სიკვდილზე“.[89]

რა იყო მიზეზი, რამაც ასე ფეთქებადსაშიში გახადა ახლო აღმოსავლეთი და რამაც გადააწყვეტინა **ირანის ისლამური რესპუბლიკა,** გამოეცხადებინა **„ჯიჰადი“** მოწოდებით: **„სიკვდილი ამერიკას“?** 2019 წლის 31 დეკემბერს ბაღდადში აშშ-ის მიერ ერაყში **„კატაიბ ჰეზბოლას“** ობიექტებზე მიტანილი იერიშის გამო დაწყებული საპროტესტო აქციის მონაწილეებმა აშშ-ის საელჩოზე თავდასხმა განახორციელეს. მანამდე აშშ-ის ქმედებები ერაყის საგარეო საქმეთა სამინისტრომ დაგმო, ირანმა კი, რომელიც **„კატაიბ ჰეზბოლას“** უჭერს მხარს, თავდასხმას **„ტერორიზმის ნათელი მაგალითი“**

[89] US Dept of Defense, Statement by the Department of Defense", U.S. Department of Defense (DoD), 2020, p 1. https://www.defense.gov, უკანასკნელად იქნა გადამოწმებული - 27.05.2020.

უწოდა. აშშ-ის საჰაერო ძალებმა სირიასა და ერაყში დაჯგუფება **„კატაიბ ჰეზბოლას“** ობიექტებზე იერიში 29 დეკემბერს მიიტანეს.

სოლეიმანის სიკვდილიდან მეორე დღესვე ამერიკის შეერთებული შტატების უსაფრთხოების უწყებამ გაავრცელა განცხადება, რომ შესაძლოა, შეერთებულ შტატებზე **ირანის ისლამური რესპუბლიკის** მხრიდან კიბერთავდასხმა განხორციელდეს:

„ირანის ისლამურ რესპუბლიკას საკმაოდ ძლიერი კიბერპროგრამა აქვს და თეირანი ცნობილია პოლიტიკურად მოტივირებული კიბერთავდასხმების განხორციელებით“.[90]

როგორც ხედავთ, <u>თეთრი სახლიც</u> კი აღიარებს, რომ ირანს საკმაოდ ძლიერი კიბერპროგრამა აქვს. აქვე უნდა აღინიშნოს ერთი ფრიად საყურადღებო ფაქტი: ირანელი გენერლის განეიტრალების შემდეგ თვით პრეზიდენტი **ტრამპი** და სხვა მაღალჩინოსნები თავიანთი აზრის გამოსახატავად და განცხადებების გასავრცელებლად აქტიურად იყენებდნენ სოციალურ ქსელებს, კერძოდ - **„ტვიტერს“**. ამავე ხერხს მიმართეს ირანელმა მოხელეებმაც. **აშშ-ირანის ისლამური რესპუბლიკის** სამხედრო დაპირისპირება მიმდინარეობს საინფორმაციო ომის ფონზე. ფაქტია, სოციალურ ქსელებში **დონალდ ტრამპის** მხრიდან არაერთხელ დაფიქსირდა მუქარა, <u>თუ **ირანის ისლამური რესპუბლიკა** ჩვენს ქვეყანაზე თავდასხმებს განახორციელებს, 52 ირანულ ობიექტს დავბომბავთ, დარტყმა სწრაფი და ძლიერი იქნებაო.</u> **<u>„ირანელ ხალხს არასოდეს დაემუქრო“</u>**, - <u>ამ სიტყვებით მიმართა ქვეყნის პრეზიდენტმა **ჰასან როუჰანმა** დონალდ ტრამპს.</u>[91]

ირანის ისლამურმა რესპუბლიკამ უყურადღებოდ არ დატოვა სოლეიმანთან დაკავშირებული „შეურაცხყოფა“ და <u>ერაყში აშშ-ის სამხედრო ბაზების</u>

[90] რუხაძე თ. "ირანის მხრიდან შესაძლოა, აშშ-ზე კიბერთავდასხმა განხორციელდეს", საქართველოს საზოგადოებრივი მაუწყებელი, 2020, გვ. 1. https://1tv.ge, უკანასკნელად იქნა გადამოწმებული - 05.01.2020.

[91] Rouhani H. Never threaten the Iranian nation: Rouhani tells Trump, Alarabiya, 2020, p 1. https://english.alarabiya.net, უკანასკნელად იქნა გადამოწმებული - 06.01.2020.

მიმართულებით 35 ბალისტიკური რაკეტა გაუშვა. მოგვიანებით გაჩნდა ინფორმაცია, რომ ერაყის ხელისუფლებამ ამერიკელები გააფრთხილა და სამხედროებმა ბუნკერებში ჩასვლა მოასწრეს.[92]

მთელი მსოფლიო ელოდებოდა საპასუხო შეტევას აშშ-ის მხრიდან, მაგრამ პრეზიდენტმა **ტრამპმა** გონივრული გზა აირჩია - არავითარი ომი, მხოლოდ მკაცრი სანქციები. ნუ გამოვრიცხავთ, რომ ეს იყოს დროებითი მშვიდობა, შესაძლოა, **ირანის ისლამურმა რესპუბლიკამ** სხვა ხერხები გამოიყენოს - ტერორისტული აქტები, კიბერთავდასხმები და ასე შემდეგ. ცხადია, სამხედრო დაპირისპირების ჩაცხრობის შემთხვევაში მთელი ყურადღება გადატანილი იქნება კიბერთავდასხმებსა და საინფორმაციო ომზე.

ირანს ასევე თავის ტკივილად ექცა თეირანის აეროპორტში ჩამოვარდნილი უკრაინული თვითმფრინავი, სადაც 178 მგზავრი და ეკიპაჟის 9 წევრი დაიღუპა. ამერიკელების მტკიცებით, სამგზავრო თვითმფრინავი ირანელებმა ააფეთქეს რუსული რაკეტის გასროლით. **ირანის ისლამური რესპუბლიკა ამერიკის შეერთებულ შტატებს** დიდ ტყუილში ადანაშაულებს. მთავრობის პრესსპიკერმა, **ალი რაბიეიმ** განაცხადა, რომ ასეთი დიდი სიცრუისთვის პასუხისმგებლობას არავინ აიღებს. მისივე თქმით, ეს არის ფსიქოლოგიური სპეცოპერაცია **ირანის ისლამური რესპუბლიკის** წინააღმდეგ. თუმცა ამ მხრივ საინფორმაციო ომი დიდხანს არ გაგრძელებულა, 11 იანვარს **ირანის ისლამური რესპუბლიკის** ხელისუფლებამ აღიარა, რომ თვითმფრინავი შეცდომით ჩამოაგდეს და ამას „ადამიანური შეცდომა“ უწოდეს.[93]

ვაღიაროთ, ამ სამხედრო დაპირისპირებასა და საინფორმაციო ომში **ირანის ისლამური რესპუბლიკა** პირწმინდად დამარცხდა. თუმცა რას მოიმოქმედებს შემდგომში ეს არაპროგნოზირებადი რესპუბლიკა, რთული

[92] Trump D. Trump says 'Iran appears to be standing down' following its retaliatory attacks against Iraqi bases housing US troops, CNN, 2020, p 1. https://edition.cnn.com, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.

[93] კუპრეიშვილი თ. "ყველაფერი, რაც ვიცით უკრაინული თვითმფრინავის კატასტროფაზე". საინფორმაციო სააგენტო "ნეტგაზეთი", 2020, გვ. 1. https://netgazeti.ge, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.

სავარაუდო არის და არც არის - წესით, აშშ-ის და დანარჩენი სამყაროს წინააღმდეგ ომი უნდა გადავიდეს კიბერსივრცეში. არ უნდა დაგვავიწყდეს, რომ ირანმა აშშ-ის სამხედრო ძალები უკვე გამოაცხადა **„ტერორისტულ ორგანიზაციად“**. შესაბამისი კანონპროექტი **ირანის ისლამური რესპუბლიკის** პარლამენტმა ერთხმად დაამტკიცა და „ის ყველა ამერიკელ სახმედროზე, პენტაგონის თანამშრომელზე და იმ პირებზე ვრცელდება, ვინც ირანელ გენერალ **სოლეიმანის** მკვლელობაზეა პასუხისმგებელი. **ირანის ისლამური რესპუბლიკის** პარლამენტმა ასევე მხარი დაუჭირა **„ისლამური რევოლუციის გუშაგთა კორპუსის“** ელიტური ქვედანაყოფის **„ალ-კუდსის“** დაფინანსების 200 მილიონი ევროთი გაზრდას. აღნიშნული ქვედანაყოფი **ირანის ისლამური რესპუბლიკის** ფარგლებს გარეთ სპეცოპერაციების ჩატარებაზეა პასუხისმგებელი.[94]

ირანის ისლამური სახალიფოს შესაძლებლობები და კიბერუსაფრთხოების სისტემები

ამერიკის შეერთებული შტატები დათმობას არ აპირებს. უკმაყოფილო **დონალდ ტრამპმა** კიდევ ერთხელ აღნიშნა, რომ ნატოსთვის მთავარ კონტრიბუციას აშშ იღებს, რაც სამართლიანი არ არის. მანამდე კი განაცხადა, რომ ევროპის დაცვის მიზნით აშშ მილიარდებს ხარჯავს მაშინ, როცა თავად აშშ კრიტიკულ მომენტებში ვერ იღებს სათანადო მხარდაჭერას. მედიის ცნობით ტრამპმა ნატოს გენერალურ მდივანს, სტოლტენბერგს განუცხადა, რომ ნატო ახლო აღმოსავლეთშიც უნდა გაფართოვდეს:

„მე ვფიქრობ, ნატო უნდა გაფართოვდეს, ჩვენ ახლო აღმოსავლეთიც უნდა მოვიცვათ. სტოლტენბერგი ამ აზრით აღფრთოვანებულია. ახალ ალიანსს

[94] ახალაია ლ. "ირანმა აშშ-ის სამხედრო ძალები „ტერორისტულ ორგანიზაციად“ გამოაცხადა", საქართველოს საზოგადოებრივი მაუწყებელი, 2020, გვ. 1. https://1tv.ge, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.

შეგვიძლია დავარქვათ ნატო+ახლო აღმოსავლეთი“. რა მშვენიერი სახელწოდებაა. სახელებს კარგად ვიგონებ“.[95]

და ამ ფონზე, როდესაც ნატო ახლო აღმოსავლეთში გაფართოებას აპირებს, რა შესაძლებლობები გააჩნია მის მთავარ სამიზნეს, **ირანის ისლამურ რესპუბლიკას,** რომ თუნდაც კიბერუსაფრთხოების თვალსაზრისით გაუწიოს წინააღმდეგობა ევროპა-აშშ-ის სამხედრო ალიანსს? სად არის ამ დროს საქართველო, რომელიც აშშ-ის საიმედო პარტნიორია? საქართველოს თავდაცვის სამინისტროს **კიბერუსაფრთხოების ბიურომ** 2015 წელს შეიმუშავა სტრატეგია, სადაც (თავი 35) საუბარია **ირანის ისლამური რესპუბლიკის** კიბერშესაძლებლობებსა და ამ სახელმწიფოს ინტერესებზე. დღეს ყველა ექსპერტი აღნიშნავს, რომ საქართველოსა და ირანს შორის კი არის ნორმალური ურთიერთობა ეკონომიკური და კულტურული ურთიერთობის თვალსაზრისით, მაგრამ ის მაინც ითვლება საფრთხედ, რადგან რუსეთთან ერთად წარმოადგენს ძლიერ კიბერმოთამაშეს არა მხოლოდ რეგიონში, არამედ მსოფლიოში. ირანის ისლამურ რესპუბლიკაში შექმნილია ასეულობით კიბერორგანიზაცია, რომლებიც მუშაობენ სხვადასხვა საკითხებზე - მაგალითად, პოლიტიკურ კულტურულ და რელიგიურ თემებზე. ამათგან ყველაზე ძლიერ დანაყოფს წარმოადგენს **ICA**, რომელიც შეიქმნა **"ისლამური რევოლუციის მცველების"** მიერ 2005 წელს და კავშირშია ქვეყნის შეიარაღებულ ძალებთან. ეს ორგანიზაცია კიბერთავდასხმებს ანხორციელებს ირანის საზღვრებს გარედან, დიდი ბრიტანეთიდან, ჩინეთიდან, პაკისტანიდან და საუდის არაბეთიდან.

როგორ უნდა გაუმკლავდეს საქართველო ასეთ დიდ საფრთხეს, რომელიც შეიძლება ერთ დღესაც მთელი ძალებით ამუშავდეს? რასაკვირველია, გამოსავალი მხოლოდ ერთია - მჭიდრო თანამშრომლობა უსაფრთხოების კუთხით ამერიკის შეერთებულ შტატებთან, ევროპის წამყვან

[95] ტრამპი დ. "ნატო-მ ახლო აღმოსავლეთიც უნდა მოიცვას და ახალ ალიანსს დავარქვათ „ნატო+ახლო აღმოსავლეთი“ – რა მშვენიერი სახელწოდებაა, სახელებს კარგად ვიგონებ". საინფორმაციო "ინტერპრესნიუსი", 2020, გვ. 1. https://www.interpressnews.ge, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.

სახელმწიფოებთან და ნატოსთან, რასაც შედეგად უნდა მოჰყვეს კვალიფიციური კადრების მომზადება და ახალი ტექნოლოგიების ათვისება. ასევე, დაზვერვისა და კონტრდაზვერვის გაძლიერება მთელი რეგიონის მასშტაბით.

2019 წლის სექტემბერში ირანის ისლამური რესპუბლიკის საგარეო საქმეთა მინისტრმა **ჯავად ზარიფმა** კომპიუტერული ვირუსი **Stuxnet**-ი ახსენა და აშშ-ის 2020 წლის საპრეზიდენტო არჩევნებში ჩარევის ბრალდებებიც უარყო. მისი თქმით, თეირანი არჩევნებზე უპირატესობას არცერთ მხარეს არ ანიჭებს და არც სხვა სახელმწიფოების შიდა საქმეებში ერევა.

ირანის ისლამურ რესპუბლიკასა და აშშ-ს შორის ურთიერთობა განსაკუთრებით 14 სექტემბერის შემდეგ გამწვავდა, როცა საუდის არაბეთში ორ ნავთობტერმინალზე თავდასხმა განხორციელდა. მიუხედავად იმისა, რომ პასუხისმგებლობა იემენელმა ჰუსიტებმა აიღეს, აშშ და საუდის არაბეთი მომხდარში ირანს ადანაშაულებენ. თეირანი ბრალდებას უარყოფს, მაგრამ ვაშინგტონმა ირანს 20 სექტემბერს ახალი სანქციები მაინც დაუწესა.

ურთიერთობა ორ ქვეყანას შორის მას შემდეგ გაუარესდა, რაც ვაშიგტონმა თეირანთან დადებული ბირთვული შეთანხმებიდან გასვლის თაობაზე განაცხადა. 2018 წლის მაისში, ევროპელი პარტნიორების კრიტიკის მიუხედავად, აშშ-მა ირანის ისლამურ რესპუბლიკასთან დადებული ბირთვული შეთანხმება ცალმხრივად დატოვა. ნოემბერში კი ვაშინგტონმა თეირანს სანქციები აღუდგინა და მოკავშირე სახელწმიფოებისგან მოითხოვა, ირანისგან ნავთობის შეძენა შეეწყვიტათ. წინააღმდეგ შემთხვევაში აშშ შესაბამის კომპანიებს სანქციების დაწესებით დაემუქრა. სხვათა შორის, აშშ-ის სპეცსამსახურებისთვის იმთავითვე ცნობილი იყო, რომ ირანი ემზადებოდა თავდასხმისთვის სირიასა და ერაყში. დაზვერვის მიერ მოპოვებული ინფორმაცია გამართლდა, ოღონდ იმ გაგებით, რომ ირანმა ეს **სოლეიმანის** განეიტრალების შემდეგ განახორციელა.

როდესაც ვსაუბრობთ ირანზე, უნდა გავიხსენოთ ისიც, რომ ამ ქვეყანას 2012 წლიდან მოყოლებული, კიბერკონფლიქტი აქვს მეზობელ აზერბაიჯანთანაც, რასაც ასეულობით ვებგვერდის „დაბომბვა“ მოჰყვა. 2012 წლის იანვარში აზერბაიჯანელ ჰაკერთა ჯგუფმა, რომელიც საკუთარ თავს **„ნამდვილი აზერბაიჯანის კიბერარმიას“** უწოდებს, შეტევა განახორციელა ირანის ვებსაიტებზე, რაც გახლდათ პასუხი წინა დღეს განხორციელებულ იერიშებზე . აზერბაიჯანის ათამდე ოფიციალური - მათ შორის, პრეზიდენტ **ალიევის**, მმართველი პარტიის, საკონსტიტუციო სასამართლოს, შინაგან და კომუნიკაციების სამინისტროების საიტები გახდა მიუღწეველი. თუკი ვინმე ამ საიტებზე შესვლას შეეცდებოდა, პირველ გვერდზე ხვდებოდა ინფორმაცია, რომ ამაში პასუხისმგებელი აზერბაიჯანას კიბერარმიაა და ბაქო „ებრაელებს ემსახურება“. იმავე დღეს მოხდა თავდასხმა ისრაელის ვებსაიტებზე. მათ შორის იყო საავიაციო კომპანია **„ელ ალის“** და თელ-ავივის ბირჟის საიტები. ირანსა და აზერბაიჯანს შორის იმ პერიოდში ურთიერთობა დაიძაბა იმის გამო, რომ თეირანმა ბაქო ისრაელთან თანამშრომლობაში დაადანაშაულა. ისრაელი ნავთობის მნიშვნელოვან ნაწილს აზერბაიჯანისგან იღებს. იმავე წლის დეკემბერში აზერბაიჯანის საგარეო საქმეთა მინისტრი ვაშინგტონში სიტყვით გამოვიდა და ირანი სომხეთთან თანამშრომლობაში ამხილა, ამ ქვეყანას მთიანი ყარაბახის ოკუპაციაში ეხმარებაო. მოკლედ, პერიოდულად იქმნება შთაბეჭდილება, რომ ირანსა და აზერბაიჯანს შორის თბილი ურთიერთობაა (თუნდაც ერთმორწმუნეობის გამო), მაგრამ სინამდვილეში საქმე სხვანაირადაა - ირანისთვის ყველა მტერია, ვინც საქმეს დაიჭერს ამერიკის შეერთებულ შტატებთან და ისრაელთან, თუნდაც ეკონომიკური თვალსაზრისით.

ჩრდილო ატლანტიკური ალიანსის სტრატეგიის ყველა კონცეფცია ითვალისწინებს კიბერთავდაცვის საკითხებს და ყოველწლიურად იხარჯება მილიარდობით დოლარი. მით უმეტეს, მეტი იქნება საჭირო, თუკი ჩრდილო-ატლანტიკური ალიანსი ახლო აღმოსავლეთშიც დაფუძნდება და

შემდეგ დაიწყებს გაფართოებას. ბუნებრივია, ეს ყველაფერი ვერ განხორციელდება კიბერთავდაცვის სისტემების შექმნისა და არსებული სისტემების გაძლიერების გარეშე.

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.

<u>დისკურს-ანალიზი</u>

2012 წლის შემდეგ საქართველოში ჩამოყალიბდა ორპოლუსიანი სატელევიზიო მედია. თუ მანამდე, ყალბი დემოკრატიის პირობებში იყო ერთპოლუსიანი და თითქმის ყველა ტელეარხი წარმოდაგენდა სახელისუფლებო რუპორს, შემდგომში გაჩნდა სამი ტელეარხი, **„მთავარი არხი“**, **„ტვ პირველი“** და **„ფორმულა“.** 2004 წელს ხელისუფლებაში მოსულმა **„ნაციონალურმა მოძრაობამ“** ძალისმიერი მეთოდებით თავის სამსახურში ჩააყენა **„იმედი“** და **„მაესტრო“**, ხოლო **„იბერია“** საერთოდ გააქრო სატელევიზიო სივრციდან. ძალაუფლების დაკარგვის შემდეგ **„ნაცმოძრაობამ“** მაინც შეინარჩუნა **„რუსთავი 2“**, რომელიც ფაქტობრივად იყო ფეიკ-ნიუსებზე მომუშავე იარაღი. მას შემდეგ, რაც ეს ტელევიზია, ევროპული სასამართლოს გადაწყვეტილებით, კანონიერ მფლობელს დაუბრუნდა, საზოგადოებაში გაჩნდა მოლოდინი, რომ ტელემედია, ასე თუ ისე, დაბალანსდებოდა, მაგრამ ერთი ფეიკ-ნიუსებზე მომუშავე

ტელევიზიის ნაცვლად გაჩნდა სამი. როგორც ცნობილია, **„მთავარი არხი“** ძირითადად ექვემდებარება ძებნილ ექს-პრეზიდენტ **მიხეილ სააკაშვილს**, **„ფორმულას“** აფინანსებს ასევე ძებნილი, თავდაცვის ყოფილი მინისტრი **დავით კეზერაშვილი**, ხოლო **„ტვ პირველი“** ეკუთვნის ფულის გათეთრებაში ეჭვმიტანილ, სიგარეტის მაგნატ **ავთანდილ წერეთელს.** ამ სამი ე.წ. მედიამფლობელის პირადი ინტერესია, რადაც არ უნდა დაუჯდეთ, დაამარცხონ **„ქართული ოცნება“** და **ბიძინა ივანიშვილი.** ამას არც მალავენ. შეიძლება ნებისმიერ მოქალაქეს ჰქონდეს პოლიტიკური ამბიციები, სწორედ ეს არის დემოკრატიის მთავარი ღირებულება, მაგრამ იერიში მიიტანო სახელმწიფოზე და იოცნებო სახელმწიფო სტრუქტურების ჩამოშლაზე, ეს უკვე დაუშვებელია. **„ტვ პირველისა“** და **„მთავარი არხის“** მეპატრონეები, დაქირავებული ჟურნალისტების ხელშეწყობით, რომლებსაც ასევე გააჩნიათ პირადი ინტერესები, ამოფარებულნი არიან ე.წ. თავისუფალ მედიას, რათა გადაარჩინონ საკუთარი ბიზნესები, თავი დააღწიონ მართლმსაჯულებას და მეტიც, აკრძალული ილეთებით მოვიდნენ ხელისუფლებაში. მათ ხელისუფლებაში მოსვლა სჭირდებათ მხოლოდ რევანშისთვის.

სამთავიანი მედიამუტანტის მიერ წამოსულ ფეიკ-ნიაღვარს თითქოს პერიოდულად ორი სატელევიზიო არხი - **„იმედი“** და **„პოსტვ“** ეწინააღმდეგება, მაგრამ ამ შემთხვევაში ვიღებთ მეორე პოლუსს, ანუ დაპირისპირებულ მედიამხარეს.

ელემენტარული წესია, ოპოზიცია ნებისმიერ ქვეყანაში ხელისუფლებას უნდა უწევდეს ოპონირებას, მაგრამ საქართველოში ასე არ ხდება, ადგილი აქვს პოლიტიკურ დივერსიას, ნიჰილიზმისა და პანიკის თესვას, სამოქალაქო დაპირისპირების მცდელობას, როგორც ირეალურ, ანუ ინტერნეტსივრცეში, სოციალურ ქსელებში, ასევე რეალურ ცხოვრებაში, საზოგადოებრივ ურთიერთობებში. დღევანდელი განვითარებული ტექნოლოგიების წყალობით, არსებობა გვიწევს ორ განზომილებაში - კიბერგანზომილებასა და რეალურ განზომილებაში, აქედან გამომდინარე,

პოლიტიკურ ლექსიკონში შემოგვაქვს ახალი ტერმინი **„სამოქალაქო კიბერომი“.**

რა იგულისხმება „სამოქალაქო კიბერომში“? პირველი, რითაც ე.წ. ოპოზიცია საქართველოში აგრესიას და სამოქალაქო დაპირისპირებას ხელს უწყობს, ეს გახლავთ სამი სატელევიზიო არხი, რომელიც ჩამოყალიბდა რეალურად ერთ არხად. დიდი დაკვირვება და კვლევაც არ არის საჭირო, ნებისმიერი მიხვდება, რომ სამივე „ფრონტისთვის“ ტექსტები, პროგრამები, ინფორმაციის მიწოდების სტილი, შინაარსი თუ თანმიმდევრობა მუშავდება ერთ წერტილში და შემდეგ მარაოსავით იშლება თავისუფალი სიტყვის ეგიდით. საქართველოში ფაქტობრივად უკვე ჩამოყალიბდა ანტი-სატელევიზიო და ანტი-ჟურნალისტური სივრცეები, სადაც მიმდინარეობს საინფორმაციო დივერსია და მოსახლეობის ფსიქოლოგიური ტერორი.

ოფიციალური მონაცემების თანახმად, მარტო „ფეისბუქით“ მსოფლიოში სარგებლობს 2 მილიარდ 700 მილიონი ადამიანი.[96] საქართველოში - 2 მილიონ 500 ათასი.[97] საერთოდ კი, 50 წელს გადაცილებულ ადამიანთა უმეტესობას უჭირს სოციალურ ქსელებსა თუ სხვა მედიასაშუალებებით გავრცელებული ყალბი ამბების რეალურისგან გარჩევა. საქართველოში ამ მხრივ მეტად სავალალო მდგომარეობაა - რეგიონებში ტელევიზიის „ტყვეობაში“ იმყოფება ხანდაზმული ადამიანების დაახლოებით 90%, ამას კი აქვს ორი მიზეზი: **პირველი** - სოციალიზმის პერიოდში გაზრდილ ადამიანებს ჯერ კიდევ სჯერათ, დარწმუნებულნი არიან, რომ ტელევიზორში ტყუილს არ იტყვიან და არც უჭკუოს გამოიყვანენ სასაუბროდ. აქ უკვე მენტალიტეტის პრობლემაა; **მეორე** -კი დაიწყო საქართველოს რეგიონების ინტერნეტიზაცია, მაგრამ ჯერ კიდევ შორსაა ის დრო, როცა მოსახლეობას ექნება სათანადო განათლება და ფართო

[96] Clement J. Number of monthly active Facebook users worldwide as of 2nd quarter 2020, Global No.1 Business Data Platform, 2020, p 1. https://www.statista.com, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.

[97] “სად უყვართ Facebook?", ფორბსი, 2018, გვ. 1. https://bm.ge, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.

არჩევანის საშუალება, ანუ ინფორმაციის მიღების მრავალფეროვანი წყარო, ალტერნატიული ვარიანტები.

სწორედ მოსახლეობის ასეთ ფენებზეა გათვლილი **„სამოქალაქო კიბერომის“** წარმოება და ფეიკ-ნიუსის გასაღება სინამდვილედ.

დავაკვირდეთ, რას აკეთებს ე.წ. ოპოზიცია კიბერსივრცეში და როგორ გადმოაქვს სიცრუის მთელი კასკადი რეალობაში: გავიხსენოთ 2018 წლის საპრეზიდენტო არჩევნების პერიოდი, როცა **„რუსთავი 2“** ჯერ კიდევ ე.წ. ოპოზიციის ხელში იყო და მას მთავარი პროკურორის ყოფილი მოადგილე **ნიკა გვარამია** ხელძღვანელობდა. რამდენიმე თვის განმავლობაში სატელევიზიო სივრცე და სოციალური ქსელები გაჯერებული იყო ცილისწამებით, თურმე საფრანგეთში დაბადებული და გაზრდილი **სალომე ზურაბიშვილი** არის რუსეთუმე, სამშობლოს მოღალატე, ხოლო რუსეთში განსწავლული და ნამოღვაწარი **გრიგოლ ვაშაძე** არის ევროპული ცნობიერებისა და რუსეთთან მებრძოლი ადამიანი. ყველაზე საყურადღებო კი ის გახლავთ, რომ **ვაშაძის** სასარგებლოდ მუშაობდნენ რუსი **„პიარშიკები“** ვინმე **ვიტალი შკლიაროვის** ხელმძღვანელობით. მიუხედავად იმისა, რომ ეს იყო პარადოქსი, ე.წ. ოპოზიციამ გარკვეულ შედეგს მაინც მიაღწია - არჩევნებში მიიღო 700 ათასზე მეტი ხმა და დაინიშნა კიდეც მეორე ტური. ამის შემდეგ დაიწყო შეტევა **ბიძინა ივანიშვილზე,** მომზადდა უამრავი სიუჟეტი თუ გადაცემა, თუ როგორ გლეჯდა ის ხეებს გურიაში, აჭარაში და მიათრევდა სახლში. გაიხსნა დენდროლოგიური პარკი და აღმოჩნდა, რომ ყველაფერი იყო გამიზნული სიცრუე. ამას მოჰყვა კორონა-ვირუსის აფეთქება მთელ მსოფლიოში. აღნიშნულმა სამმა ფეიკ-ნიუსებზე მომუშავე ტელევიზიებმა, რა თქმა უნდა, სცადეს, ეს თემაც გადაეყვანათ პოლიტიკურ ჭრილში და პოლიტიკოსების დახმარებით ემტკიცებინათ, რომ ეს ყველაფერი საკუთარი მიზნებისთვის სჭირდებოდა **ბიძინა ივანიშვილს.** ამის საუკეთესო მაგალითად გამოდგება **„ლეიბორისტული პარტიის“** ლიდერის, **შალვა ნათელაშვილის** გამოსვლები. მისი თქმით, ბუნებაში არანაირი ვირუსი არ არსებობს, ეს არის **ივანიშვილის** მიერ მოგონილი

ამბავი. სამწუხაროდ, ასეთი გულუბრყვილო პროპაგანდა ბევრმა დაიჯერა. ამას მოჰყვა ფეხბურთელ **გიორგი შაქარაშვილის** მკვლელობა მცხეთაში, რომლის ტრაგიკული პერიპეტიები ასევე გამოიყენეს **„ნაცმოძრაობის“** ფესვებზე დამყნობილმა ტელევიზიებმა და სცადეს, ეს საშინელება მიებათ **ბიძინა ივანიშვილის** ოჯახისთვის, თითქოს მკვლელებს, რომლებიც უკვე ციხეში სხედან, მფარველობდა **ბერა ივანიშვილი.** ამ ამბიდან **„გირგვლიანიზაცია“** არ გამოვიდა, რადგან **შაქარაშვილების** ოჯახი ვერ ჩაითრიეს ცრუ სკანდალში. მომდევნო ტრაგიკული შემთხვევა გახლდათ **თამარ ბაჩალიაშვილის** თვითმკვლელობა თეთრიწყაროს ერთ-ერთ სოფელში. ამ შემთხვევაშიც დაიწყეს იგივე სცენარის ამუშავება, როგორმე ტრაგედია უნდა მიეყვანათ მაღალჩინოსნებამდე, თითქოს ეს იყო სახელისუფლებო წრეებში დაგეგმილი მკვლელობა. ჯერ გაავრცელეს ინფორმაცია, თითქოს პროგრამისტმა **თამარ ბაჩალიაშვილმა** მაღალჩინოსნების კომპიუტერულ სისტემებში შეაღწია და მნიშვნელოვანი ინფორმაცია გამოიტანა, შემდეგ ალაპარაკდნენ, თითქოს **ბერა ივანიშვილის** კომპიუტერში შეაღწია, ბოლოს კი დაიწყეს იმის მტკიცება, თითქოს გარდაცვლილმა მოიპოვა ინფორმაცია, თუ როგორ ჰყიდდნენ იარაღს ქართველი მაღალჩინოსნები **ყარაბაღში.** სამწუხაროდ, ამ შემთხვევაში ოჯახი კი ჩაერთო ამ ტელევიზიების მიერ მოწყობილ ავანტიურაში, მაგრამ მათი ე.წ. მტკიცებულებები იმდენად მყიფე აღმოჩნდა, საზოგადოების დიდ ნაწილში უარყოფითი რეაქცია გამოიწვია. თუმცა უნდა ვაღიაროთ, აღმოჩნდნენ ადამიანები, რომლებმაც ეს ყველაფერი დაიჯერეს. დაახლოებით რამდენი პროცენტი იქნება, ვისაც უპირობოდ, ეჭვის შეტანის გარეშე სჯერა ფეიკ-ნიუსებით გაჯერებული ტელევიზიებისა. ჩვენი დაკვირვებით, გამოკითხვებით, კერძო საუბრებით, საქართველოში ასეთი „მიმნდობი“ არის საზოგადოების დაახლოებით 15-20%. აქედან 8-10% იმიტომ ენდობა **ნიკა გვარამიას** „სკოლის“ მიერ გამომუშავებულ ყალბ ამბებს, რომ გაუნათლებელია, საერთოდ უჭირს სიცრუისა და სიმართლის გარჩევა. ასეთი კატეგორია ინფორმაციას იღებს მხოლოდ ამ

ტელევიზიებიდან. დაახლოებით 10%-ს კი იმიტომ სჯერა, რომ **„ნაცმოძრაობისა“** თუ მათი განაყოფების მხარდამჭერია.

განსახილველად ავიღოთ **„ნოდარ მელაძის შაბათი“ „ტვ პირველიდან“,** რომელიც ყოველთვის იწყება მძიმე მუსიკით და უცნაური ტექსტებით. დასაწყისშივე ისმება კითხვები: როგორ მოკლეს, რანაირად მოკლეს, ვინ მოკლა, რატომ მოკლა, სად გადააგდეს, როგორ გადააგდეს, ვინ დაურეკა ბერას, რატომ დაურეკა ბერას, როგორ ჩაუვარდა ხელში **ნოდარ მელაძეს** ტელეფონი, საიდანაც დაურეკეს ბერას? მართალია, გათვითცნობიერებული ადამიანი დასაწყისიდანვე უნდა მიხვდეს, რომ უკვე საქმე გვაქვს ფეიკ-კასკადთან, მაგრამ საზოგადოების ნაწილი მაინც გაყურსული უსმენს.

რაკიღა ყველა სიუჟეტსა თუ გადაცემას **ნიკა გვარამიას** ხელი ატყვია, განსახილველად ავიღოთ მისი გადაცემა **„მთავარი აქცენტები“,** რომელიც **2020 წლის მაისში** გავიდა ეთერში.

ნიკა გვარამია გადაცემას იწყებს მონოლოგით **(სტილი დაცულია)**:

„სამწუხაროდ, დღეს უნდა გესაუბროთ იმაზე, ვინც ისევ კომუნისტების შემოგზავნილები არიან და გვმართავენ, უნდა გესაუბროთ აი, ამ კაცზე“.

აქ აჩვენებს რამდენიმე ამონარიდს პრემიერ-მინისტრ **გიორგი გახარიას** გამოსვლიდან, როცა ის იმყოფებოდა ანგარიშის ჩასაბარებლად: „ბატონო **გიგა (მიმართავს დეპუტატ გიგა ბოკერიას),** მე ვფიქრობ, თქვენ მოიპოვეთ ექსკლუზიური უფლება ჩვენი საერთაშორისო პარტნიორების თარგმნისა. არადა, ასეთი უფლება თქვენ არ გაქვთ... რა კორუფცია, რის კორუფცია? მე არ მაქვს სურვილი, ზოგიერთის დემაგოგიურ შეკითხვებს ვუპასუხო... ჩვენს ოპოზიციას უბრალოდ კომპეტენცია არ ჰყოფნის, ეს ქვეყანა უფრო კომპეტენტურ ოპოზიციას იმსახურებს“.

ნიკა გვარამია დასაწყისშივე ამტკიცებს, რომ **გიორგი გახარია** კომუნისტებმა გამოაგზავნეს. არადა, ეს ხომ სრული აბსურდია, სად **გახარია**, სად - **კომუნისტები?** მეტიც, **გვარამიას** აზრით, პრემიერ-მინისტრი ძველი ბიჭია, რადგან ამბობს, სახელმწიფო დონეზე კორუფცია არ არსებობს, შეიძლება

ვიღაცამ ვიღაცას ჯიგრულად რაღაცა გაუკეთაო. შეიძლება პირველ პირს ასე არ უნდა ეთქვა, მაგრამ პათოსი მაინც გასაგებია. თუმცა **გვარამისათვის,** წინა ხელისუფლებიდან მოვლენილი „წმინდანისთვის“ მიუღებელი აღმოჩნდა და **გვარამია** დახატა ბნელეთის მოციქულად, რომელიც ასევე ბნელმა კომუნისტებმა გამოაგზავნეს.

ნიკა გვარამია: „ამ რუსეთიდან შემოგზავნილის დანიშნულება ის არის, რომ რუსეთის არმია შევინახოთ, როგორც ვინახავდით 70 წლის განმავლობაში“.

რა შუაშია **რუსეთის** არმია? ან რატომ უნდა შეინახოს **საქართველომ?** რომც გვინდოდეს, სად აქვს საქართველოს ამის შესაძლებლობა? როგორც ხედავთ, ორ წინადადებაში სამი-ოთხი ისეთი ფეიკია, რაც არანაირ ლოგიკაში არ ჯდება. რჩება შთაბეჭდილება, რომ გადაცემის წაყვანისას **ნიკა გვარამია** ან მთვრალია ან კიდევ დაბოლილი. ერთსაათიან გადაცემაში ის გვიმტკიცებს, რომ **გიორგი გახარია** გამოაგზავნა **პუტინმა,** ხოლო ვინც მას ემხრობა, ის არის **პუტინი,** ხოლო თვითონ თავის **„ნაციონალურ“** პარტიასთან ერთად წარმოადგენს პროდასავლურ ძალას.

ახლა ვნახოთ, როგორ აგებს თემატურად გადაცემას **ნოდარ მელაძე,** რომელსაც ჰქვია **„ნოდარ მელაძის შაბათი“ რომელიც ეთერში გავიდა, 2020 წლის 13 ივლისს:** „ეჭვებს ვხსნით, საგულდაგულოდ გადამალული ფეშენებელური რეზიდენციის კადრები, სადაც ცხოვრობს პრემიერი **გახარია!**“

აქ კადრში ჩანს ერთ-ერთი სოფელი, სადაც ერთი ჩვეულებრივი სახლია.

„რეზიდენცია, რომელსაც ეძებდა სრულიად ქართული მედია, იპოვა მხოლოდ **„შაბათის“** ეთერმა, 17 კვადრატულის მფლობელ მამაკაცზე გადაფორმებული მიწები, სახლები და მშენებარე სასტუმრო. ჩვენ მოგიყვებით, ეკუთვნის თუ არა ეს ქონება რეალურად **გიორგი გახარიას**“!

გადაცემაში მოწმეებად მოჰყავთ **„ნაციონალები“**, რომლებიც ამტკიცებენ, რომ **გახარიას** სახელზე არავითარი ქონება არ ირიცხება, მაგრამ მას ფეშენებელური სახლები გადამალული აქვს. ამ დროს წარმოუდგენელია,

როგორ შეიძლება საქართველოში გადამალო ფეშენებელური სახლები. აქ ოდნავ წესიერმა ჟურნალისტმა უნდა თქვას, გადაფორმებული აქვსო, მაგრამ სიტყვა **„გადამალული“** უფრო მძაფრია, უფრო დამაჯერებელია.

„მამაკაცი, რომელიც **„ტვ პირველის“** ჟურნალისტს ემუქრება, **ბიძინა ივანიშვილის** ძმაა. მოგიყვებით ალექსანდრე **ივანიშვილის** კავშირებზე ნავთობის შავ ბიზნესთან. ნავთობის ბაზრის ერთ-ერთი მოთამაშე თავად მოგვიყვება, როგორ დაიბარეს საპატრიარქოში მღვდელთმთავრებმა და როგორ ანაწილებდნენ ნავთობის შავ ბაზარს მამაკაცები შავი ანაფორით“.

არადა, კადრებში ჩანს, რომ **ალექსანდრე ივანიშვილი „ტვ პირველის“** ჟურნალისტს არ ემუქრება, ის პოლიციას იძახებს და აცხადებს, რომ არ სურს გადაღება. აქაც ჩვეულებრივი სახლი ჩანს, ოღონდ რომელიღაც ფილმიდან ამოღებული კადრების ფონზე, გადაღებულია ნავთობის გადაზიდვის პროცესი. ვინაიდან, ამ ყველაფერს მძიმე მუსიკა და ასევე რომელიღაც ფილმიდან ამიღებული მღვდლების კადრები ადევს, სიუჟეტი უფრო მეტ სიმძაფრეს იძენს. გადაცემის ნახვის შემდეგ მიხვდებით, რომ გონებაში არაფერი დაგრჩათ, მტკიცებულებები ყალბია ან საერთოდ არ არსებობს, მაგრამ მასკარადი შედგა, ე.წ. რეალით შოუს ბევრმა უყურა და რეიტინგმაც აიწია.

აქვე განვიხილოთ **„გიორგი თარგამაძის ფორმულა“** ტელეკომპანია **„ფორმულა“**-ს ეთერში. საერთოდ, ჟურნალისტი **გიორგი თარგამაძე** ასოცირდება ტელე **„იმედთან“**, რომელიც 2007 წლის 7 ნოემბერს **მიხეილ სააკაშვილის** ბანდამ დაარბია და შემდეგ ვინმე **ჯოზეფ ქეის** ხელით მიიტაცა. **თარგამაძე** იჯდა იმ საღამოს ეთერში, რომელმაც განაცხადა, ამ შავი ძალების შეჩერება უკვე შეუძლებელიაო. ახლა კი ის ზის **კეზერაშვილის** მიერ დაფინანსებულ ტელევიზიაში და აცხადებს, რომ ქვეყანაში ტოტალიტარიზმი მძვინვარებს. კი, მაგრამ ქვეყანაში ტოტალიტარიზმი რომ მძვინვარებდეს, **თარგამაძეს** ამას ვინ ათქმევინებდა?

„გიორგი თარგამაძის ფორმულა“. 2020 წლის 3 ივნისი. თემა - **ოპოზიციის საარჩევნო სტრატეგია.** სტუმრები: **გიგა ბოკერია** და **შალვა ნათელაშვილი.** თარგამაძის აზრით, **„ქართულ ოცნებას“** ორი სახის მომხრეები ჰყავს, ერთი ნაწილი სახელმწიფო სამსახურებში მუშაობს და ხელფასის დაკარგვისა ეშინია, მეორე ნაწილს კი მიშას დაბრუნებისა ეშინია. გამოდის, ივანიშვილს ჰყავს მხოლოდ შეშინებული მომხრეები. რაც შეეხება თავად გიორგი თარგამაძეს, ის ნაკურთხი წყალივით ანკარაა, არავისი არ ეშინია. როგორც ხედავთ, აქ სახეზეა საზოგადოების დიდი ნაწილის აბუჩად აგდებისა და რეალობის გაყალბების მცდელობა. შეიძლება მსგავსი ფაქტები არის, შეიძლება ზოგს სამსახურის დაკარგვისა ეშინია, ზოგს - **მიშას** დაბრუნებისა, ზოგს - მღვდლისა, ზოგს - მღვდლის ცოლისა, მაგრამ ყველას წარმოჩენა ასეთ კონტექსტში, თვით თარგამაძისთვის არის არასახარბიელო.

გიგა ბოკერია: „თუ ხელისუფლება არ შეასრულებს ყველა დაპირებას, თუ ციხიდან არ გამოუშვებს გიორგი რურუას, ჩვენ ვიქნებით ბოიკოტის მუდმივ რეჟიმში“.

ხელისუფლებამ არ გაათავისუფლა **რურუა.** მეტიც, ის ყველას დაავიწყდა და არც **„ევროპული საქართველო“** დარჩა მუდმივი ბოიკოტის რეჟიმში. შემდგომში კი აღმოჩნდა, რომ **რურუას** გათავისუფლებაზე არანაირი შეთანხმება არ ყოფილა. რასთან გვაქვს საქმე? რა თქმა უნდა პოლიტიკურ შულერობასთან.

შალვა ნათელაშვილი: „სამწუხაროდ, ჩვენ ის ქვეყანა ვართ, რომელსაც მართავს მილიარდერთა კლასტერი. ამ დროს 300 ათასი ბავშვი იღუპება შიმშილით, ხოლო 700 ათასი ბავშვი შიმშილობს“.

კარგად იცის **შალვა ნათელაშვილმა,** რომ **საქართველოში** ყოველწლიურად 300 ათასი ბავშვი არ იღუპება, მაგრამ ახლა ასეა საჭირო. წავიდეს და იმან ამტკიცოს სიმართლე, ვისაც ეს ეხება. ამდენი ბავშვი რომ იღუპებოდეს, ხომ წარმოგიდგენიათ, რა ამბავი იქნებოდა ქვეყანაში? რა უნდა გააკეთოს ამ დროს გადაცემის წამყვანმა? უნდა მიუთითოს, რომ ეს სიცრუეა. თუმცა ამას

არ იზამს, რადგან ისიც დაინტერესებული მხარეა, ისიც სამოქალაქო კიბერომშია ჩართული და საზოგადოებას ფსიქოლოგიურ ტერორს ახვევს თავზე.

როგორც ზემოთ აღვნიშნეთ, ამ მედიატერორს წინააღმდეგობას უწევს ორი ტელეარხი - **„იმედი“** და მოგვიანებით გამოჩნდა **„პოსტვ“,** რომელიც უფრო იუმორისტული ჟანრის გამოყენებით ცდილობს გაბათილებას, ამ ტელევიზიის მთავარი მიმართულებაა მხილება. თუმცა არის მცდელობა, შეიქმნას თოქ-შოუ, სადაც დეტალურად იქნება გამოკვლეული მიხეილ სააკაშვილისა და სხვა ბობოლა „ნაციონალების“ ავკაცობანი.

გადაცემა **„სამნი“.** აქ სამი ადამიანი **(შალვა რამიშვილი, ბაჩო ოდიშარია, გური სულთანიშვილი)** ზის სტუდიაში, ისინი სპონტანურად იღებენ პოლიტიკოსების არასერიოზულ ან უცნაურ გამონათქვემებს და ძმაკაცურად განიხილავენ. საერთოდ, იუმორისტული ჟანრი ძალიან საინტერესოა ჟურნალისტიკაში და ასეთი მიდგომაც ეფექტურია, მაგრამ პრობლემა ის გახლავთ, რომ ეს ტელეარხიც დაინტერესებული მხარეა.

შალვა რამიშვილი: „ჩვენ არ ვმალავთ, რომ დაინტერესებული მხარე ვართ, ჩვენ წარმოვადგენთ **„ქართული ოცნების“** მხარდამჭერებს“.

ამ შემთხვევაში იხატება ასეთი სურათი: რომ არა **„ნაციონალების“** მიერ შექმნილი მუტანტი არხები, არ შეიქმნებოდა **„პოსტვ“.**

რაც შეეხება **„იმედს“,** აქ უფრო სერიოზულად უდგებიან ამ საკითხს.

გადაცემა **„არენა“. 2019 წლის 24 დეკემბერი.**

თემა: **ინფორმაციული ქაოსი. აშშ-ის სახელმწიფო დეპარტამენტის განცხადება - რა შეუკვეთა ოპოზიციამ და რა ჩამოვიდა ვაშინგტონიდან.** ჩვენ მაღალ შეფასებას ვაძლევთ სასამართლო რეფორმას საქართველოში, მხარს ვუჭერთ საარჩევნო რეფორმაზე მმართველ პარტიასა და ოპოზიციას შორის დიალოგს.

„ფეისბუქის“ გაუქმებული გვერდები საქართველოსა და ამერიკის შეერთებულ შტატებში.

პარალელური კვლევა **ატლანტიკური საბჭოს** სახელით, რომელიც ოპოზიციამ „ფეისბუქის“ საქმეს მიზანმიმართულად დაუკავშირა. რუსი პიარ-ტექნოლოგების მიერ დაგეგმილი **„ნაცმოძრაობის“** პროპაგანდა საპრეზიდენტო არჩევნების დროს. პოლიტიკურ იარაღად ქცეული სოციალური ქსელი. ფეიკ-ნიუსისა და ყალბი პროპაგანდის როლი ქართულ პოლიტიკაში, თითქოს ხელისუფლება ანტიდასავლურ პოლიტიკას ანხორციელებს.

დისკუსიის მონაწილეები: რეჟისორი **გოგა ხაინდრავა,** ანალიტიკოსი **ამირან სალუქვაძე,** ყოფილი დეპუტატი **ხათუნა ხოფერია,** ჟურნალისტი **ნუგზარ რუხაძე,** ჟურნალისტი **გიორგი პაპუაშვილი,** ჟურნალისტი **გურამ ნიკოლაშვილი,** ახალგაზრდული ცენტრის დამფუძნებელი **ზურაბ ქადაგიძე** და კინოკრიტიკოსი **ბაჩო ოდიშარია.**

გადაცემის წამყვანი **ვაკა გორგილაძე.**

ინტერაქტივი: ვისი იარაღია ფეიკ-ნიუსი, ხელისუფლების თუ ოპოზიციის?

დისკუსიის მთავარი თემა გახლდათ ფეიკ-ნიუსი და იმ საკთხის გარჩევა, თუ რატომ დაბლოკა „ფეისბუქის“ ადმინისტრაციამ ის გვერდები და ანგარიშები, რომლებიც ხელისუფლებასთან იყო აფილირებული. სამწუხაროდ, გადაცემის მესვეურებმა სტუდიაში არ მიიწვიეს პროფესიონალები, სოციალური ქსელებისა თუ ინტერნეტსივრცის მცოდნე ადამიანები და ამიტომაც საუბარი ვერ გასცდა პოლიტიკურ არეალს. სტუდიაში არ აღმოჩნდა ერთი პიროვნებაც კი, რომელიც დეტალურად ახსნიდა, თუ რა არის ე.წ. **ბოტი, ტროლი, ფეიკ-ნიუსი, ყალბი ინფორმაცია** და ასე შემდეგ.

გადაცემას წინ უძღვოდა ზედაპირული სიუჟეტი, სადაც საუბარი იყო იმაზე, რომ დღეს საზოგადოებას დეზინფორმაცია აღარ უკვირს, არჩევნების პერიოდში და შემდეგაც **„ფეისბუქში“** არსებობდა ათასობით ყალბი გვერდი,

მაგრამ ე.წ. ოპოზიციამ და არასამთავრობო სექტორმა სირაქლემას პოზიცია არჩია. შემდეგ გამოჩნდა სარეკლამო სააგენტო **„პანდა“**, რომელიც ფეიკ-ნიუსის გამავრცელებლებს დაუპირისპირდა. მანამდე არსებობდა ატლანტიკური საბჭო, სადაც არის მხოლოდ ორი ადამიანი - ვინმე ეთო გოძიაშვილი და გივი გიგიტაშვილი. ამავე პერიოდში დაიბლოკა აშშ-ის პრეზიდენტის მხარდამჭერი გვერდი, რომელსაც 55 მილიონი გამომწერი ჰყავდა. 2019 წელს „ფეისბუქმა“ 5 მილიარდზე მეტი ყალბი ანგარიში დახურა და ასე შემდეგ. ვერ ვიტყვით, რომ ამ სიუჟეტში ხელშესახები არაფერი ითქვა, მაგრამ შეიძლებოდა უფრო სიღრმისეული მსჯელობა.

რაც შეეხება კონკრეტულად სტუდიაში მიწვეულ სტუმრებს შორის დისკუსიას, აქ მსჯელობა წავიდა მხოლოდ ერთი მიმართულებით - ყველაფერში დამნაშავეა **„ნაციონალური მოძრაობა“** და ამ პარტიის წევრები თავად არიან ბოტები, ტროლები თუ ყალბი ინფორმაციის გამავრცელებლები. დიახ, შეიძლება ეს სრული სიმართლეა, მაგრამ ფაქტი ფაქტად რჩება, დაიბლოკა ხელისუფლების ინტერესების გამტარებელი გვერდები და ანგარიშები. სხვათა შორის, აქ არ თქმულა ერთი მნიშვნელოვანი რამ - დავუშვათ, ხელისუფლებამ და მმართველმა პარტიამ არ დააფინანსა ინტერნეტ-აქტივისტები (ამ შემთხვევაში არც დადებულა მტკიცებულება, რომ ხელისუფლება ვინმეს აფინანსებდა), რა ხდება, ბოტები და ტროლები გაქრებიან? შესაძლოა, მათი რიცხვი შედარებით შემცირდეს, მაგრამ ასეთი თვითშემოქმედებითი კერძო პირები ყოველთვის იარსებებენ. დავუშვათ, „ფეისბუქის“ ადმინისტრაციამ დაბლოკა 500 გვერდი, მერე რა? სოციალურ ქსელებში რჩება ათასობით და მილიონობით ყალბი გვერდი. დაბლოკავ? იმავე წამს გაგიხსნის ახალ გვერდებს, რა ბერკეტი გაქვს სისტემის გასაკონტროლებლად? ფაქტობრივად, არავითარი.

როგორც უკვე აღვნიშნეთ, სტუდიაში მიიწვიეს ადამიანები, საკუთარი საქმის კარგი მცოდნეები, მაგრამ არა ამ საქმის სპეციალისტები, თუნდაც ერთი-ორი მაინც.

ნიმუშად ავიღოთ რეჟისორ **გოგა ხაინდრავას** გამოსვლა:

„ე.წ. ოპოზიცია ზის სიცრუეში. **გრიგოლ ვაშაძე** არის **რუსეთის** ჩეკისტი, შეკრებებზე მის გვერდით ზის **რუსეთის** პოლიტიკის გამტარებელი **ნინო ბურჯანაძე.** ფსევდოლიბერალურმა საზოგადოებამ სრული კრახი განიცადა მსოფლიოში. ამის მაგალითი იყო ბრიტანეთის არჩევნები, სადაც კონსერვატორმა **ბორის ჯონსონმა** არნახული გამარჯვება მოიპოვა. ეს საზოგადოება იღებს უცხოეთიდან დაფინანსებას. კაპიტანი **გიგაური** ფინანსდება ცილისწამებისთვის, ის ებრძვის სახელმწიფოს და არა კონკრეტულ პარტიას. მაგალითი - ვითომ ყალბი პასპორტები რომ დაბეჭდა ხელისუფლებამ არჩევნების პერიოდში. **ბოკერია, ჩერგოლეიშვილი, გიგაური** და მისთანანი გველაპარაკებიან ქართველი ხალხის სახელით. **სააკაშვილი** თავად არის ჩრდილოეთის ვექტორი. **ელენე ხოშტარია** იყო **გავრილოვის** სტუდენტი. აგვისტოს ომში გავიმარჯვეთო, წინა ხელისუფლებამ ხალხი აზეიმა. **გვარამიას** ტელევიზიაში ვინც მუშაობენ, ისინი არ არიან ჟურნალისტები, ისინი არიან აქტივისტები. **„ნაცმოძრაობა“** არის დამარცხებული ბნელი ძალა, რომელიც ფულს ხარჯავდა იმისთვის, რომ გავლენის აგენტები შეექმნა. ეს აგენტები ხელისუფლებაზე იქნებოდნენ მიმაგრებულნი და დააშვებინებდნენ შეცდომებს. დღეს **„ვაშინგტონ პოსტიც“** კი არ არის თავისუფალი სიტყვის ფლაგმანი, ანონიმური წერილი გამოაქვეყნა. ეს მეტყველებს იმაზე, რომ ყველაფრის ყიდვა შეიძლება. რა არის „ფეისბუქი“? ეს არის შეუმდგარი ადამიანების სამყარო, დაფარული ვნებების სამყარო, მე არასოდეს ვყოფილვარ იქ“.

თუკი თემას შევხედავთ პოლიტიკური (ემოციური) კუთხით, რა თქმა უნდა, საინტერესოა, მაგრამ სტუდიაში მოიწვიო ადამიანი, რომელიც არ გახლავთ არც ერთი სოციალური ქსელის მომხმარებელი და მეტიც, რომელიც ამბობს, „ფეისბუქი“ არშემდგარი ადამიანების სამყაროაო, რბილად რომ ვთქვათ, უხერხულია. ვინაიდან, საქმე გვაქვს სრულიად ახალ მოვლენასთან, საჭირო იყო დეტალური განხილვა, რათა მოსახლეობამ გაიგოს, რას ნიშნავს საინფორმაციო ომი თავისი ატრიბუტებით. ასევე უხერხულია განცხადება იმის თაობაზე, რომ თურმე რაკი **„ვაშინგტონ პოსტმა“** რაღაც ანონიმური

წერილი გამოაქვეყნა, მსოფლიო მასშტაბით სიტყვის თავისუფლება საბოლოოდ დასამარდა. ამ შემთხვევაში გაუგებარი დარჩა, რა წერილზეა საუბარი, აქ გადაცემის წამყვანი უნდა დაინტერესებულიყო, რას გულისხმობდა **გოგა ხაინდრავა**. თუმცა წამყვანმა ამ მომენტს ყურადღება არ მიაქცია და „გაატარა“. ფრაზა - „ყველაფრის ყიდვა შეიძლება“, ასევე დარჩა სრულიად გაუგებარი, მაყურებელი ვერ მიხვდა, რაში და რატომ აიღო ფული გავლენიანმა გამოცემამ? რაც შეეხება შეუმდგარი ადამიანების სამყაროს, ანუ „ფეისბუქს“, ვფიქრობთ, ესეც მცდარი მოსაზრებაა. როგორც ჩანს, ბატონ გოგას სოციალური ქსელი მხოლოდ საჭორაო ტრიბუნა ჰგონია. არადა, ნებისმიერმა გათვითცნობიერებულმა ადამიანმა იცის, რომ სოციალური ქსელი წარმატებით გამოიყენება როგორც პოლიტიკაში, ასევე ეკონომიკასა თუ ბიზნესში. თავი რომ დავანებოთ ჩვენი კვლევის თემას, ეს არის ძალიან დიდი სარეკლამო ბაზარი. გადაცემაში სწორი აქცენტი დასვა აშშ-ში განსწავლულმა ჟურნალისტმა **ნუგზარ რუხაძემ:**

„ჩვენ დემოკრატიაში ვცხოვრობთ, შეიძლება ეს კარგია, მაგრამ ალბათ უკეთესიც არსებობს. როგორც დემოკრატია შემოიჭრა ჩვენში, ჩვენს ცხოვრებაში, შეიძლება ასევე შემოიჭრას **„ტროლოკრატია“**, ანდა **„ბოტიზმი“.** ერთ მშვენიერ დღეს იღვიძემ და ხედავ, ერთ მხარეს დგას **ერეკლე მეორე,** მეორე მხარეს - **აღა მაჰმად-ხანი,** მათ ჰყავთ არა ჯარისკაცები, არამედ **ტროლები** და **ბოტები.** ჩვენ დროში ცხელი ომი აღარ არის, იქნება ცივი, ანუ რბილი ძალების ომი, სადაც **ტროლები** ემრძვიან ერთმანეთს. ყველა სოციალური მოვლენა ჩვენზეა დამოკიდებული, როგორ ვიყენებთ, ცუდად თუ კარგად? ყველაფერი დამოკიდებულია ადამიანთა განწყობაზე. საბოლოო ჯამში **ბოტი** და **ტროლი** არ არის საფრთხობელა, შეიძლება კარგი საქმეებისთვის გამოვიყენოთ“.

ნუგზარ რუხაძე უფრო მსუბუქად უდგება საკითხს, მისი თქმით, შეიძლება ე.წ. ტროლები და ბოტები სასიკეთოდაც გამოვიყენოთ. მან აღნიშნა, რომ ხშირად უცნობი პიროვნებების მხრიდან შეიძლება სასარგებლო კრიტიკაც წამოვიდეს და ეს იყოს სასარგებლო. მართალია, მან სიმბოლურად ერეკლე

მეორე და აღა მაჰმად-ხანი ახსენა იუმორისტული ფორმით, მაგრამ სინამდვილესთან ახლოსაა, თუ კარგად გავიხსენებთ საპრეზიდენტო არჩევნების პერიოდს, აუცილებლად დავდგებით მსგავსი ფაქტის წინაშე - ეს ძირითადად იყო ბრძოლა ტროლებისა და ბოტების მეშვეობით. არის თუ არა დიდი პრობლემა კაცობრიობისთვის **„ტროლოკრატია“** და ყალბი ინფორმაციის გავრცელება? რა თქმა უნდა, არის პრობლემა, მაგრამ ამ მოვლენას აუცილებლად უნდა დავუპირისპიროთ სისტემა, რომელიც მუდმივად ამხელს სიცრუეს. გადაცემის წამყვანი **ვაკა გორგილაძე** ამტკიცებს, რომ პირველი **ტროლები** და **ბოტები,** საერთოდ **ტროლინგი** შექმნა **„ნაციონალურმა მოძრაობამ“.** ამაში ვერ დავეთანხმებით, ე.წ. **ტროლინგი** ამ ფორმით შეიქმნა სოციალური ქსელების გაჩენისთანავე. მეტიც, მსგავსი სისტემა არსებობდა კომპიუტერისა და ინტერნეტის **„აღზევებამდეც“.** ამ შემთხვევაში მეთოდი კარგად ჩაინერგა თანამედროვე ტექმოლოგიებში, თორემ ჭორისა თუ ყალბი ინფორმაციის გავრცელების უნიკალურ მეთოდებს ფლობდა ნაცისტური გერმანიის იდეოლოგიის მამის, **იოზეფ გებელსის** მიერ შექმნილი სპეცსამსახური. სწორედ გებელსის დამსახურება გახლდათ, რომ ბუნკერში ჩაკარგული **ადოლფ ჰიტლერი** გერმანიის მოსახლეობას რადიოს საშუალებით არწმუნებდა, ჩვენ აუცილებლად გავიმარჯვებთო. ჩვენს მიერ ჩატარებულმა კვლევამ დაადასტურა, რომ თითქმის იგივე ხელწერა აქვთ **„ნაციონალური მოძრაობის“** ლიდერებს - ისინი არასოდეს აღიარებენ წაგებას, 2012 წლის არჩევნებში დამარცხებასაც კი გარეშე ფაქტორებით ხსნიან და ამტკიცებენ, რომ ეს მოხდა **რუსეთის** ჩარევით, ოლიგარქის ფულით, დადგმული სპექტაკლებით და ასე შემდეგ. დამარცხების შემდეგ ისინი ყოველი არჩევნებისას თავიანთ მომხრეებს აჯერებენ გარდაუვალ გამარჯვებაში და იგონებენ ახალ-ახალ ზღაპრებს, თუ როგორ დამთავრდება რამდენიმე თვეში არსებული ხელისუფლება.

გადაცემის შემდეგი მონაწილე **ხათუნა ხოფერია** ამბობს, დიდად ვერ ვერკვეოდი **ტროლებსა** და **ბოტებში**, შემდეგ გავერკვიეო:

„ტროლებთან შეხება მქონია. არიან მოაზროვნე ტროლები, არიან უზრდელი ტროლები. საერთოდ, ბოტიზმი და ტროლოკრატია **„ნაციონალების“** დაწყებულია. 2008 წლიდან მოყოლებული, იყო და არის **„თბილისის ფორუმი“,** სადაც აქტიური დებატები მიდიოდა და ყველა იყო **ტროლი,** საკუთარი გვარ-სახელით არავინ გამოდის. 2012 წლის შემდეგ გაირკვა, რომ ესენი ძირითადად იყვნენ შინაგან საქმეთა სამინისტროს თანამშრომლები და წარმოიდგინეთ, გარემოს დაცვის სამინისტროს წარმომადგენლები. ვანო მერაბიშვილს დაახლოებით 500 კაცამდე ჰყავდა ამ მხრივ დასაქმებული. გასამრჯელოს უხდიდნენ და აძლევდნენ თემებს. ტრამპმა გააკეთა განცხადება, „გუგლი“ და „ფეისბუქი“ მებრძვისო, თუ ტრამპს ებრძვიან, მეც თანახმა ვარ, მებრძოლონ“.

ამ შემთხვევაშიც, ცოტა არ იყოს, გულუბრყვილო მსჯელობასთან გვაქვს საქმე. მაგალითად, **„თბილისის ფორუმი“** იყო და დღესაც არის სრულიად ღია ე.წ. სოციალური ქსელი, სადაც **„მოღვაწეობდნენ“** და **„მოღვაწეობენ“** ათასი ჯურის ადამიანები. შეიძლება ამ ფორუმზე მართლაც იყვნენ შინაგან საქმეთა სამინისტროს ან სხვა სამსახურების თანამშრომლები დარეგისტრირებულნი და ანხორციელებდნენ სახელისუფლებო იდეოლოგიას, მაგრამ თემატიკას ცოტა უკეთესად თუ შევისწავლით, არ გვაქვს იმის მტკიცებულება, რომ თემატურად ცალმხრივია ან მიკერძოებული. ამის სურვილი რომც ჰქონდეს ვინმეს, ფორუმის სრული გაკონტროლება შეუძლებელია. კვლევის შედეგად დავადგინეთ, რომ ამ ქსელში ანტისახელისუფლებო პროპაგანდა უფრო მეტია, ვიდრე სახელისუფლებო. რაც შეეხება აქტივისტების, ანუ ე.წ. **„იუზერების“** დასაქმებას, ეს უკვე დამსაქმებლის სურვილი უფროა, ვიდრე ფორუმის ადმინისტრაციისა. დღეს შესაძლოა, „ნაცმოძრაობამ“ დაიქირავოს ასობით ან ათასობით ადამიანი, გადაუხადოს ფული, გაახსნევინოს გვერდები „ფეისბუქში“ (ფაქტობრივად ასეც ხდება) და დაიწყოს მიზანმიმართული პროპაგანდა, არავის მოუვა აზრად, ამაში დაადანაშაულოს სოციალური ქსელის ადმინისტრაცია. ქალბატონი ხათუნა ამბობს, ვერ ვერკვეოდი და

შემდეგ გავერკვიეო. ამ დროს აშკარად ჩანს, რომ ბოლომდე ვერ გაერკვია, მას ე.წ. **„ტროლიზმი“** ჰგონია მხოლოდ შენიღბული ადამიანი, რომელიც ერთ მშვენიერ დღეს თავის გვერდზე შეუხტება და წაეუზრდელება. რა თქმა უნდა, ესეც არ გახლავთ ფრიად სასიამოვნო მოვლენა, მაგრამ გადაცემაში (წამყვანიც კი) არავინ ეცადა, აეხსნა, ტექნიკური თვალსაზრისით რა საშიშროებასთან გვაქვს საქმე.

ამ კუთხით საინტერესო აქცენტი დასვა **გურამ ნიკოლაშვილმა:**

„ოპოზიციის მხრიდან ჯერ იქმნება ნარატივი - თითქოს **„ქართულ ოცნებას“** აღარ აქვს მხარდაჭერა არც უცხოეთიდან, არც მოსახლეობის მხრიდან და რაც მთავარია, ხელისუფლება არის პრორუსული. ამ ნარატივის გასამყარებლად ოპოზიცია იყენებს ფეიკ-ნიუსს“.

აი, ეს არის სწორი მიგნება - ოპოზიცია ქმნის ნარატივს, შემდეგ კი თემატურად შლის სოციალურ ქსელებში. ეს გახლავთ იდეოლოგია, რომელიც, რა თქმა უნდა, უარყოფითად აისახება ხელისუფლების მუშაობაზე. თუ დავაკვირდებით, ერთი პერიოდი „ქართული ოცნება“ ასეთმა მიდგომამ, ასეთმა პროპაგანდამ დააბნია და დააკომპლექსა კიდეც - ის ჩადგა თავის მართლების მუდმივ რეჟიმში. ის, რომ მმართველი გუნდი ნელ-ნელა გამოვიდა ამ რეჟიმიდან, განაპირობა თვით ოპოზიციის უნიჭობამ და შეცდომებმა. სად გაბითურდა ოპოზიცია? ამის შესახებ კარგ განმარტებას იძლევა **ამირან სალუქვაძე:**

„ტრამპმა განაცხადა, რომ შეამცირებს ნატოს დაფინანსებას. გამოთავისუფლებულ თანხებს წარმართავს უკრაინისა და საქართველოს დასახმარებლად, უსაფრთხოებისა და თავდაცვისუნარიანობის ასამაღლებლად. აშშ ნატოს აკლებს თანხებს და ახმარს **საქართველოს - 132 მილიონი.** თან ეს არის გათვალისწინებული ერთი წლის ბიუჯეტში. საგარეო ვექტორი არ უნდა იყოს საკამათო. რბილი ძალის მთავარი სამიზნე არის საგარეო ვექტორი, დეოკუპაციის თემა, რუსეთს მეტი არაფერი არ აინტერესებს“.

როდესაც **ამერიკის შეერთებული სტატები** მიდის ასეთ უპრეცედენტო გადაწყვეტილებამდე და შენ ხელისუფლებას მაინც პრორუსულობაში ადანაშაულებ, ეს უკვე მეტყველებს, რომ საქმე გვაქვს დიდ სიყალბესთან, ანუ ცილისწამებასთან. როგორც ზურაბ ქადაგიძე ამბობს გადაცემაში, არ შეიძლება, ტელევიზიით გამოდიოდეს რამდენიმე კაცი და ლაპარაკობდეს საზოგადოების სახელით, რომ თურმე საზოგადოება აღშფოთებულია, ივანიშვილის ხელისუფლება დამთავრდა, მალე დავამხობთ და ასე შემდეგ. მისივე თქმით, საქართველოში გაჩნდნენ სნობი ექსპერტები, რომლებიც ყოველთვის მსჯელობენ მოტივით: მხოლოდ ჩვენ ვართ და დანარჩენი საქართველო. როგორც გიორგი პაპუაშვილი ამბობს, „ნაცმოძრაობის“ წევრები არიან ტროლები. ამათ გასაღები აქვთ დაკარგული, ისეთ რაღაცებს ლაპარაკობენ, ჩვენ რომ ვერასოდეს მოვიფიქრებთ“.

თუ დესტრუქციული ოპოზიცია დასაწყისში უფრო დამაჯერებელი იყო, ბოლო ორი-სამი წლის განმავლობაში ესეც წყალში ჩაყარა, რადგან სიცრუის სიმართლედ გასაღება ძალიან გაჭირდა. გარდა ამისა, 8 წლის განმავლობაში ერთი და იგივეს გამეორება საზოგადოებისთვის არის მომაბეზრებელი. კი განვითარდა ტექნოლოგიები, მნიშვნელოვნად გაფართოვდა და უკიდეგანო გახდა ინფორმაციის გავრცელების არეალი, მაგრამ ოპოზიციის მიერ შემუშავებული მეთოდები იგივე დარჩა. რა უხარია მუდმივად **„ნაცმოძრაობას“? ბაჩო ოდიშარიას** თქმით, **„ნაცმოძრაობას“** უხარია, თითქოს „ქართული ოცნება“ ამხილა ანტიამერიკულ სენტიმენტებში:

„დავუშვათ, აშშ-ის საელჩომ ან სახელმწიფო დეპარტამენტმა გაავრცელა რაიმე განცხადება, ოპოზიცია ამას თარგმნის თავისებურად, დამახინჯებულად და საზოგადოებას აწვდის ცრუ ინფორმაციას, თითქოს ჩვენი სტრატეგიული პარტნიორები აღშფოთებულნი არიან. ნახავთ ტექსტს, მსგავსი არაფერია. ამას ჰქვია ტექსტებით მანიპულაცია“.

ტექსტებით მანიპულაცია ოპოზიციისთვის არახალია და აშკარად ჩანს, რომ ეს მეთოდიც გაცვდა. გადაცემაში ჩართულმა ინტერაქტივმაც დაადასტურა, რომ ქართული საზოგადოება საზოგადოება მნიშვნელოვნად გაიზარდა:

ინტერაქტივი: ვისი იარაღია ფეიკნიუსი, ხელისუფლების თუ ოპოზიციის? 12% ფიქრობს, რომ ხელისუფლების, 88%-ის აზრით - ოპოზიციის.

2020 წლის 30 აპრილს ფეისბუქის ადმინისტრაციამ ათობით გვერდი და ანგარიში დაბლოკა. დაზუსტებით შეიძლება ითქვას, რომ დაბლოკილია და სოციალურ ქსელში აღარ იძებნება **„ნაციონალურ მოძრაობასთან“** დაკავშირებული გვერდები და ანგარიშები. „ფეისბუქის“ ადმინისტრაციის განცხადებით, **„ნაცმოძრაობის“** ყალბი ანგარიშების სამიზნეს წარმოადგენდნენ **საქართველოს მართლმადიდებლური ეკლესია,** მმართველი პარტია და კორონავირუსის პანდემიის პირობებში მთავრობის ძალისხმევა. ამ კამპანიაში იხარჯებოდა დიდი რაოდენობით თანხა, რასაც „ფეისბუქმა“ მიაკვლია. სხვათა შორის, ყალბი გვერდებისა და ანგარიშების გაუქმება მოხდა მომხმარებელთა და არა რომელიმე ორგანიზაციის მიმართვების საფუძველზე. ყოველ შემთხვევაში, ასეთია ოფიციალური ინფორმაცია. ეს კი არის იმის საპირისპირო, რა მიზეზითაც მომზადდა გადაცემა.

დასკვნა: საქართველოში (მით უმეტეს, წინასაარჩევნო პერიოდებში) მიმდინარეობს სამოქალაქო კიბერომი, სადაც ცალკე მიმართულებებად შეიძლება განვიხილოთ, როგორც ინტერნეტ თავდასხმები, ასევე საინფორმაციო ომის ელემენტები, ფეიკ-ნიუსის მასშტაბები, მისი მავნე ზემოქმედება საზოგადოების მნიშვნელოვან ნაწილზე და სოციალური ქსელების ე.წ. პოლიტიკურ ქსელებად ჩამოყალიბება. სამოქალაქო კიბერომი არ გახლავთ თავდასხმა მხოლოდ კომპიუტერულ ქსელებსა თუ პროგრამებზე ინფორმაციის მოპოვების ან იგივე ქსელებისა და პროგრამების მწყობრიდან გამოყვანის მიზნით, ამ შემთხვევაში იგულისხმება ადამიანების ტვინებში შეღწევა, მავნე ინფორმაციის ჩანერგვა, აზრის დამახინჯება და აგრესიულ განწყობაზე დაყენება. საქართველოში ამ მხრივ სავალალო მდგომარეობაა, ერთი მხარე იბრძვის ხელისუფლებაში დასაბრუნებლად, მეორე მხარე - ამხელს. საბოლოო ჯამში, ვიღებთ ორ დაპირისპირებულ მხარეს და რასაკვირველია, ზარალდება საზოგადოება.

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.

საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მიერ გამოქვეყნებულ 2018 წლის ანგარიშში ვრცლად არის წარმოდგენილი, თუ რას წარმოადგენს ჯიჰადისტური კიბერომი და რა საშიშროებასთან შეიძლება გვქონდეს საქმე.

საქართველოსთვის, ისევე როგორც მსოფლიოს მრავალი ქვეყნისთვის, ძირითად გამოწვევას ტერორისტული ორგანიზაცია **„ისლამური სახალიფოს“** (**„დაეში“**) და მასთან დაკავშირებული დაჯგუფებები წარმოადგენენ. **„დაეში“** მოქმედებას აგრძელებდა დასუსტებისა და ტერიტორიული დანაკარგების შემდეგ შემუშავებული ახალი სტრატეგიით.

აღნიშნულის ფარგლებში **„დაეშისთვის“** პრიორიტეტული აღარ იყო მხარდამჭერების სირიასა და ერაყში მობილიზება. ტერორისტული ორგანიზაციის მოქმედების მთავარ იარაღად იქცა კონფლიქტის ზონის მიღმა ტერორისტული აქტების განხორციელება. **„დაეში“** მსოფლიოს სხვადასხვა ქვეყნებში მცხოვრებ რადიკალიზებულ პირებს ნებისმიერი საშუალებით ტერორისტული თავდასხმების განხორციელებისკენ მოუწოდებდა. ეს ორგანიზაცია თანამედროვე ტექნოლოგიების, მათ შორის, ინტერნეტსივრცისა და სოციალური ქსელების გამოყენებით, კვლავ აქტიურად ავრცელებდა საკუთარ იდეოლოგიას, ახდენდა ადამიანების გადაბირებას. როგორც ანგარიშში ვკითხულობთ:

„ალ-კაიდა“ აქტივობებს, ძირითადად ახლო აღმოსავლეთსა და აფრიკის კონტინენტზე მოქმედი რეგიონული დაჯგუფებების მეშვეობით ახორციელებდა. „თალიბანი“ განაგრძობდა ავღანეთის სამთავრობო ძალებსა და ქვეყანაში საერთაშორისო მისიით მყოფ სამხედროებზე თავდასხმებს".[98]

ამ თემაზე საფუძვლიანი გამოკვლევა ჩაატარა პროფესორმა **ვახტანგ მაისაიამ,** მის ნაშრომში მკაფიოდაა ასახული, თუ რას წარმოადგენენ **ისლამური სახალიფო** - **"დაეში“** და ასევე **„ალ-კაიდა“**:

"ესენია ტერორისტული ორგანიზაციები, რომლებიც ახლო აღმოსავლეთში ერთიანი **„ისლამური სახალიფოს“** შექმნის იდეებით არიან შთაგონებულნი.[99]

ინტერნეტსივრცეში ყოველდღიურად ჩნდება **ჯიჰადისტური** ქსელები მრავალნაირი ფორმით. ამ მხრივ მიდის სელექციური მუშაობა ახალი თაობის **ჯიჰადისტების** აღსაზრდელად. როგორც **ვახტანგ მაისაია**

---

[98] "საქართველოში მცხოვრებ „დაეშის“ შესაძლო მხარდამჭერთა რაოდენობა და გავლენა შემცირდა". საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, 2019, გვ. 1. https://imedinews.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020.

[99] მაისაია ვ. „ისლამური ხალიფატის“ საინფორმაციო-პროპაგანდისტული/კიბერ-ვირტუალური ომის სპეციფიკა - „რბილი ძალის“ კონცეფტი", მედიაჰოლდინგი "ჯორჯიან-თაიმსი", 2017, გვ. 1. http://geotimes.com.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.

აღნიშნავს, ესენი არიან მეორე და მესამე თაობის **ჯიჰადისტები**, რომლებმაც უნდა იმუშაონ "მტრის ზურგში".

დღეს კიბერსივრცეში მოქმედებს 10 ათასზე მეტი ვებ-საიტი, რომლის მეშვეობითაც ვრცელდება **ჯიჰადისტური** იდეოლოგია და ტერორიზმის პრაქტიკა. 10 ათასზე მეტ ვებს-საიტს თუ დავუმატებთ მრავალფეროვან სოციალურ ქსელებს, მივიღებთ ძალიან დიდ საშიშროებას, რომელსაც ასევე სჭირდება უფრო მეტი სიმძლავრეებით წინააღმდეგობის გაწევა. თანამედროვე მსოფლიოსთვის ერთ-ერთი უმთავრესი გამოწვევა ისეთი ტიპის ასიმეტრიული საფრთხეებია, როგორიცაა საერთაშორისო ტერორიზმი და ტრანსნაციონალური ორგანიზებული დანაშაული.

რას წარმოადგენს **ჯიჰადი** და რა საფრთხე შეიძლება იყოს საქართველოსთვის? სიტყვა „**ჯიჰადი**“ არაბული წარმოშობისაა, სწრაფვასა და ძალისხმევას ნიშნავს. იგი კლასიკურ ტექსტებში მეტწილად ბრძოლისა და ომის მნიშვნელობით გამოიყენება. ხშირად იმოწმებენ ფრაზას ყურანიდან - **„ღვთის გზაზე ბრძოლა“**, რასაც მრავალი ინტერპრეტაცია მოეძებნა ზნეობრივი სწრაფვიდან დაწყებული, შეიარაღებული ბრძოლით დამთავრებული. მუსლიმური სამართლის მიხედვით, ომის წარმოება 4 ტიპის მტრის წინააღმდეგ არის გამართლებული: ურწმუნონი, განდგომილნი, ამბოხებულნი და ყაჩაღები. მართალია, ოთხივე ტიპის ბრძოლა ლეგიტიმურია, მაგრამ მხოლოდ პირველი 2 ითვლება **ჯიჰადად**. ამრიგად, **ჯიჰადი** რელიგიური ვალდებულებაა. წმინდა ომის ფენომენის განხილვისას, მუსლიმი სამართალმცოდნენი შემტევ და თავდაცვით **ჯიჰადს** განასხვავებენ. იერიშის დროს **ჯიჰადი** ზოგადად მუსლიმური საზოგადოების მოვალეობაა და იგი მოხალისეთა და პროფესიონალთა მიერ იწარმოება. თავდაცვით ომში ეს თითოეული მუსლიმის მოვალეობა ხდება. **ბინ ლადენმა** სწორედ ეს პრინციპი წამოსწია წინ თავის საომარ დეკლარაციაში შეერთებული შტატების წინააღმდეგ. მუსლიმური ტრადიციის მიხედვით მსოფლიო იყოფა ორ ნაწილად: **ისლამის სახლი (დარ ალ-ისლამი)**, სადაც მუსლიმური მმართველობაა და **ომის სახლი (დარ**

ალ-ჰარბი) - დანარჩენი მსოფლიო, სადაც ურწმუნონი სახლობენ. **ჯიჰადი** უნდა გაგრძელდეს მანამ, სანამ მთელი მსოფლიო ან ისლამურ რჯულზე არ მოექცევა, ან მუსლიმურ სამართალს არ დაემორჩილება. ის, ვინც **ჯიჰადს** აწარმოებს, დაჯილდოვებულ იქნება ორივე ცხოვრებაში. მას ექნება ქონება მიწიერ ცხოვრებაში და სამოთხე - შემდგომში. ზოგჯერ **ჯიჰადს** ჯვაროსნული ბრძოლის მუსლიმურ სინონიმად მოიაზრებენ და ეს ორი ფენომენი მეტ-ნაკლებად ერთნაირად აღიქმება.[100]

2013 წლის 6 ივნისს "იუთუბზე" შოკისმომგვრელი ვიდეო გავრცელდა სახელწოდებით: **"ჯიჰადი ავღანეთში საქართველოს ჯარების წინააღმდეგ"**,[101] რომელიც შეიცავდა მუქარას ავღანეთის მისიაში მონაწილე საქართველოს შეიარაღებული ძალების წინააღმდეგ. მუქარისშემცველი ვიდეოს გავრცელებას მოჰყვა მსხვერპლი. სანამ ქართველი ჯარისკაცების დაღუპვის შესახებ გახდებოდა ცნობილი, ამ ვიდეოს საქართველოს ხელისუფლებაში სერიოზულად არ აღიქვამდნენ. მისი წარმომავლობის დადგენაზე მოკვლევა დაიწყო თავდაცვის სამინისტრომაც. გავრცელებული ტექსტი კი ასეთი გახლდათ:

"ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!"[102]

იმ პერიოდში **ჯიჰადისტები** საქართველოში ტერაქტებითაც იმუქრებოდნენ. სამხედრო ექსპერტ **გიორგი თავდგირიძის** განცხადებით, როდესაც ავღანეთში მისიას ვუშვებთ, მარტო ის კი არ არის, რომ იქ გვყავს ჯარისკაცები და ამით მორჩა. გარკვეული უსაფრთხოების ზომები ქვეყანაშიც უნდა იქნას მიღებული:

---

[100] ქაზუმოვი ო. "ძალადობა რელიგიის სახელით და ინტერპრეტაციის მნიშვნელობა". ტოლერანტობისა და მრავალფეროვნების ინსტიტუტი (TDI), 2018, გვ. 1. https://www.tdi.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.

[101] ზამან ჰ. "Youtub-ზე გავრცელებული ვიდეოს წარმომავლობა გაურკვეველია", საინფორმაციო "ფორ.ჯი", 2013, გვ. 1. https://for.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.

[102] ზამან ჰ. "თალიბანი საქართველოს შურისძიებით ემუქრება? - შოკისმომგვრელი ვიდეო YouTube-იდან". მედიაჰოლდინგი "პალიტრა", 2013, გვ. 1. https://www.palitravideo.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.

"საქართველოს ბიუჯეტიდან საკმაოდ მნიშვნელოვანი სახსრებია გამოყოფილი ასეთი საქმიანობისთვის, საზღვრებისა და აეროპორტების გაკონტროლებისთვის, ამიტომ შესაბამისი სამსახურები უნდა მოიქცნენ ისე, როგორც მსგავსი მუქარის შემთხვევის დროს იქცევიან".[103]

მართალია, ტერორისტების მთავარ სამიზნედ საფრანგეთი, ზოგადად დასავლეთი ევროპა და ამერიკის შეერთებული შტატები ითვლება, მაგრამ ეს იმას არ ნიშნავს, რომ საქართველო სრულიად დაცულია და საფრთხე არ არსებობს. კავკასია, საქართველო, როგორც სატრანზიტო ფუნქციის მატარებელი, მომგებიანი ტრასაა ნარკომოვაჭრეებისთვის.

აქ გადამწყვეტი სიტყვა ეკუთვნის სახელმწიფო უსაფრთხოების სამსახურს, დაზვერვას, რომლის ერთ-ერთი უმთავრესი პრიორიტეტია ტერორიზმის წინააღმდეგ ბრძოლა. 2015 წლის ნოემბრიდან საქართველოში შეიზღუდა წვდომა რადიკალური იდეოლოგიის გამავრცელებელ ვებ-გვერდებსა და სოციალურ მედიაში დარეგისტრირებულ ჯგუფებზე. თუმცა პანკისის ხეობიდან **"ისლამურ სახალიფოში"** გადახვეწილთა რაოდენობამ (იმ პერიოდში 200-მდე ახალგაზრდა) აშკარად გვაჩვენა, რომ ვებ-გვერდებზე წვდომის შეზღუდვა და სოციალურ მედიაში ტერორისტული ჯგუფების დაბლოკვა საკმარისი არ არის - კერძოდ, პანკისის ხეობაში გასაძლიერებელია იდეოლოგიური და პროპაგანდისტული მუშაობა. სახელმწიფო უსაფრთხოების სამსახურის მიერ გავრცელებული ინფორმაციის თანახმად, პრევენციის მიზნით, მუდმივად ტარდება ღონისძიებები - პარტნიორი სახელმწიფოების შესაბამის უწყებებს შორის მუდმივად ხდება ინფორმაციის გაცვლა ტერორისტულ ორგანიზაციაში გაწევრიანებულ ან კავშირში მყოფ პირებზე, ასევე ტრანზიტულად გადაადგილების მსურველებზე:

[103] "ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!". ტერორისტული ორგანიზაცია „ჯიჰადი“, 2013, გვ. 1. https://for.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.

"ტერორისტული საქმიანობისთვის ქვეყნიდან გამგზავრებისა და შემოსვლის პრევენციის მიზნით, შსს-სთან თანამშრომლობით სათანადოდ ხორციელდება სასაზღვრო კონტროლი (საზღვრის მწვანე ზოლის, ასევე სასაზღვრო გამტარი პუნქტების). ხდება ვიზიტორებთან გასაუბრება. ყველა სასაზღვრო-გამტარი პუნქტი აღჭურვილია ბირთვული და რადიოაქტიური მასალების, ნივთიერებების დეტექტორებით".[104]

აღსანიშნავია, რომ ზუსტად ტერორიზმითა და ორგანიზებული დანაშაულით გამოწვეული საფრთხეების წინააღმდეგ ბრძოლამ საჭირო გახადა საერთაშორისო თანამშრომლობის ზრდა, ამის გამო, შეიქმნა ტრანსნაციონალური, საერთაშორისო საპოლიციო სისტემა - **ინტერპოლი.** თანამშრომლობა მკვეთრად გააუმჯობესა საქმეში ინტერნეტის ჩართვამ, რომლის წყალობითაც მყისიერად ვრცელდება დოკუმენტები, ფილმები, ფოტოები მთელი მსოფლიოს მასშტაბით.

ოფიციალური მონაცემებით, ჯიჰადისტთა რაოდენობა სხვადასხვა ქვეყნების მიხედვით ასე გამოიყურება: სირიაში – 43 600 კაცი, ავღანეთში – 27 000, პაკისტანში – 40 000, ერაყში – 15 000, ლიბიაში – 10 000, ნიგერიაში – 7 000, სომალიში – 7 000, იემენში - 3 500 კაცი, მალიში - 3 200. მთელ მსოფლიოში დაახლოებით მოქმედებს 67 ჯიჰადისტური დაჯგუფება, რაც წლებთან შედარებით 180%-ით არის გაზრდილი.

ექსპერტების მტკიცებით, ჯიჰადისტებმა კი დაკარგეს ერაყსა და სირიაში გავლენა, მაგრამ ისინი საბოლოოდ არ დამარცხებულან - მათ გააჩნიათ თანამედროვე ტექნოლოგიები და როდის რას მოიმოქმედებენ, არავინ იცის. ჯიჰადისტების მიზანი ურყევია, მათ „დიად“ იდეად კვლავ რჩება ისლამური სახალიფოს ჩამოყალიბება. ამ ეტაპზე კი ცდილობენ, დაამხონ მთავრობები ახლო აღმოსავლეთის ქვეყნებში და გააძლიერონ ბრძოლას აშშ-ის წინააღმდეგ. თუმცა, მიუხედავად მათ მიერ განხორციელებული

[104] "ტერორიზმთან ბრძოლა". საქართველოს სახელმწიფო უსაფრთხოების სამსახური, 2015, გვ. 1. https://ssg.gov.ge, უკანასკნელად იქნა გადამოწმებული: 15.06.2020.

ტერორისტული აქტებისა და სახელმწიფოს შექმნის არაერთი მცდელობისა, იდეა ოცნებად რჩება.

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.

იყო თუ არა მოულოდნელი აღნიშნული კიბერთავდასხმა საქართველოსთვის და საერთაშორისო თანამეგობრობისთვის? როგორც შემდგომი შეფასებებისას აღმოჩნდა, თავდასხმა მოულოდნელი არ იყო, მაგრამ ასეთი სიძლიერის შეტევას არავინ ელოდა. მოგვიანებით კი შეფასდა, როგორც გაკვეთილი. ყოფილი ხელისუფლების ჩინოვნიკები აცხადებენ, რომ მაშინ საერთაშორისო პარტნიორების დახმარებით სახელმწიფო ვებ-გვერდები ამერიკულ სერვერებზე გადაიყვანეს და პრობლემა ასე მოაგვარეს, მაგრამ საკითხი მაინც ღია დარჩა - რუსეთმა საწადელს მიაღწია, პირწმინდად ჩაიგდო ხელში როგორც რეალური საომარი პოლიგონი, ასევე ინტერნეტსივრცე. საქართველოს თავდაცვის სამინისტროს კვლევის შედეგად კი აღმოჩნდა, რომ თავდასხმა მზადდებოდა ომამდე ორი წლით ადრე. თავდაცვის მინისტრის ყოფილი მოადგილე, ბათუ ქუთელია ამბობს, რომ ამის დამადასტურებელი არაერთი ფაქტი არსებობს:

"კიბერშეტევა ხდებოდა იმ ვებპლატფორმებიდან, რომლებიც მანამდე კრიმინალს ემსახურებოდა. კონკრეტულად, ეს იყო დარქვები, რომლებიც რუსული ორგანიზებული დანაშაულის პლატფორმაა. დიფეისებში,

რომელბსაც შეტევისას იყენებდნენ, კონკრეტული ქივორდები იყო: ნატო, საქართველო და ამერიკა, სამხედრო თანამშრომლობა. გარდა ამისა, რამდენიმე დიფეისი, გაკეთებული იყო ომამდე 2 წლით ადრე, უბრალოდ, 2008-ში აამოქმედეს".[105]

კიბერუსაფრთხოების ექსპერტის, **ანდრია გოცირიძის** თქმით, 2007-2008 წლებში ესტონეთისა და ლიეტუვას წინააღმდეგ განხორციელებული **DDoS** კიბერშეტევები სადამსჯელო ოპერაციას და ერთგვარ პოლიტიკურ გზავნილს წარმოადგენდა, რომლის მიზანიც სამოქალაქო მღელვარებისა და მასობრივი არეულობის გამოწვევა იყო, თუმცა არ უკავშირდებოდა ამა თუ იმ სამხედრო ამოცანის შესრულებას და არც საომარი მოქმედებების ინფორმაციულ უზრუნველყოფას ემსახურებოდა. რაც შეეხება რუსეთ-საქართველოს ომს, აქ კიბერელემენტის გამოყენება უშუალოდ კონვენციური მოქმედებების ორგანიზებულ თანმხლებ პროცესს წარმოადგენდა, რომლის მიზანიც რუსეთის შეიარაღებული ძალებისათვის სამხედრო მიზნების შესრულების გაიოლება, საინფორმაციო ვაკუუმის შექმნა, ინფორმაციული უპირატესობის მოპოვება და კონფლიქტის შესახებ რუსული ნარატივის დამკვიდრება იყო.[106]

რუსეთის მხრიდან კიბერთავდასხმა ყოველდღე არ ხდება. თუმცა რუსული პროპაგანდა რომ მუდმივად ძლიერდება, ამას ოფიციალურ დონეზეც აფიქსირებენ სახელმწიფო უსაფრთხოების სამსახურის ანგარიშებში. ექსპერტების მტკიცებით, კრემლმა არა მხოლოდ ტონი შეარბილა, დეცენტრალიზაციის პრინციპსაც მიმართავს - ქმნის პატარ-პატარა მარგინალურ ჯგუფებს, რომლებიც რადიკალურ მოსაზრებებს ავრცელებენ. ეს ჰგავს იმ შეტევას, როცა მოდის ბევრი ინფორმაცია ერთად, სერვერი იტვირთება და ჩერდება. პროდასავლური არასამთავრობო ორგანიზაციები თავიანთ ანგარიშებში ასევე მიუთითებენ, რომ საქართველოში კრემლის

[105] გეგიძე თ. "როგორ მოვიგერიეთ კიბერთავდასხმა და პროპაგანდა 2008 წელს", სააგენტო "ონ.ჯი", 2019, გვ. 1. https://on.ge/, უკანასკნელად იქნა გადამოწმებული - 19.09.2020.
[106] გოცირიძე ა. "რუსეთ-საქართველოს 2008 წლის ომის კიბერგანზომილება", საქართველოს სტრატეგიისა და საერთაშორისო უსაფრთხოებების კვლევის ფონდი, 2019, გვ. 1. https://www.gfsis.org, უკანასკნელად იქნა გადამოწმებული - 19.09.2020.

პროპაგანდის კიდევ ერთი მნიშვნელოვანი საყრდენია ბოლო დროს მომრავლებული პრორუსული არასამთავრობო ორგანიზაციების ქსელი, რომელთა შორის განსაკუთრებით ორი ორგანიზაციის გამოყოფა შეიძლება - **„ევრაზიის ინსტიტუტი“** და **„ევრაზიული არჩევანი“**.[107] მათი მტკიცებით, ეს ორგანიზაციები გამოირჩევიან ანტიდასავლური რიტორიკით და ანალიტიკური ნაშრომებისა თუ სტატიების გამოქვეყნებისას ეფუძნებიან რუსულ წყაროებს. საჯარო რეესტრის მონაცემების მიხედვით, პრორუსული არასამთავრობო ორგანიზაციების დამფუძნებელთა და ხელმძღვანელთა სიაში ხშირად ერთი და იგივე პირები ფიქსირდებიან. ორგანიზაციებს შორის კავშირი მათ ვებ-გვერდებზეც არის მითითებული. გარდა ამისა, პრორუსული არასამთავრობო ორგანიზაციების ქსელს კავშირი აქვს ანტიდასავლური რიტორიკით გამორჩეულ საინფორმაციო საშუალებებთან. შესაძლოა, პროდასავლური არასამთავრობო ორგანიზაციები ნაწილობრივ არც ტყუიან, მაგრამ მათ მიერ დასახელებული ორგანიზაციები ამტკიცებენ, რომ საქმე პირიქითაა - დასავლურ კურსს ხელს უშლიან ის ორგანიზაციები, რომლებიც ყალბი პროდასავლური შეფუთვით არიან წარმოდგენილნი. თუ ე.წ. **"ევრაზიული"** დასახელების ორგანიზაციები თავიანთ ორიენტაციას არ მალავენ და ხშირად ამბობენ, რომ ისინი რუსულ კი არა, ქართულ საქმეს აკეთებენ, პროდასავლურად შეფუთულ ორგანიზაციებში ხშირად მართლაც ჭირს გარკვევა - არის შემთხვევები, როცა ამა თუ იმ საკითხის კვლევისას აშკარად შეინიშნება პირადი ინტერესები.

არასამთავრობო ორგანიზაციების ნაწილი იმაზეც წერს, რომ საქართველოში მომრავლდა პრორუსული ორიენტაციის პოლიტიკური პარტიები. ხშირად კეთდება განცხადებები, თითქოს რიგი პოლიტიკური პარტიები და პოლიტიკოსები, პირდაპირ ან ირიბად, ავრცელებენ კრემლისთვის სასარგებლო პროპაგანდას. პოლიტიკურ პარტიებს ყოფენ ორ ნაწილად:

[107] ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., "კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016, გვ. 1.

პირველი - რომლებსაც ღიად პრორუსული დღის წესრიგი აქვთ, ხვდებიან რუს პოლიტიკოსებს და სტუმრობენ მოსკოვს; მეორე - პარტიები, რომლებიც დეკლარირების დონეზე ემიჯნებიან რუსულ პოლიტიკურ ელიტას და სანაცვლოდ საკუთარ თავს აცხადებენ პროქართულ, ნეიტრალიტეტის მომხრე პარტიებად. განსხვავების მიუხედავად, ორივე სახის პოლიტიკური პარტიების ძირითადი გზავნილები ერთნაირია - მათი მოწოდებები ევროპულ და ევროატლანტიკურ სტრუქტურებში გაწევრიანების მიმართ სკეპტიციზმის გაღვივებას უწყობს ხელს. დასავლური ინსტიტუტებისკენ საქართველოს სწრაფვა წარმოჩენილია, როგორც უშედეგო, როგორც ოცნება. სანაცვლოდ კი ხდება პრორუსული განწყობისა და საქართველოს ნეიტრალიტეტის იდეის პოპულარიზაცია.

არასამთავრობო ორგანიზაციების ნაწილი ეჭვობს, რომ ანტიდასავლურ კამპანიაში ჩართულნი არიან სასულიერო პირებიც. ისინი ავრცელებენ მითს, თითქოს ქართული ტრადიციები დასავლურ კულტურასთან შეუთავსებელია. ზოგიერთი სასულიერო პირი ქადაგებაში ავითარებს აზრს რუსეთთან ცივილიზაციური ერთობისა და დასავლეთთან იდეური თუ მორალური წინააღმდეგობის შესახებ. კრემლის პროპაგანდისტული გზავნილების ირიბად თუ პირდაპირ გავრცელება სერიოზულ პრობლემას წარმოადგენს, ქართულ საზოგადოებაში სამღვდელოება მაღალი ნდობით და გავლენით სარგებლობს. პროდასავლური არასამთავრობო ორგანიზაციების აზრით, ეს არ შეიძლება შემთხვევითი იყოს, გამოდის, საზოგადოებას მოსწონს და აღიარებს მათ ორიენტაციას. თუ საზოგადოება მოხიბლულია ასეთთა ქადაგებებით, მაშინ პრობლემა ნაწილობრივ მოსახლეობაშია.

რუსეთი რომ საქართველოსთვის მრავალი პრობლემის სათავეა, ეს ცხადია, მაგრამ საზოგადოებაში არსებობს კიდევ ერთი სახის ილუზია, რომელიც მეზღაპრეთა მიერ გახლავთ მოგონილი: ბევრი ქადაგებს იმის თაობაზე, თითქოს რუსეთი დღე-დღეზე დაიშლება, გაცამტვერდება და გვეშველება; მეორე - რუსეთში მოვა დემოკრატიული ხელისუფლება და ტერიტორიებს

უპრობლემოდ შემოვიერთებთ; მესამე - რუსეთს მალე ნავთობი შემოაკლდება, გაკოტრდება და ასევე გვეშველება. შესაძლოა, ოდესღაც ყველაფერი მოხდეს, მაგრამ ასეთი მოსაზრებებით შორს ვერ წავალთ. რა მოჰყვება რუსეთის დაშლას კაცობრიობისთვის და ასევე რა მოჰყვება რუსეთში დემოკრატიული ხელისუფლების მოსვლას, ეს ჯერ არავინ იცის.

ამ ფონზე არსებობს ვირტუალური საფრთხე - კიბერომი და საინფორმაციო ფრონტი, რომელიც გახსნილია რამდენიმე მიმართულებით. ერთია ღია პროპაგანდა, მეორეა - შენიღბული პროპაგანდა, ანუ პროდასავლური შირმით რუსეთის ინტერესების გატარება. რუსეთი ამერიკის შეერთებულ შტატებს, ბალტიის ქვეყნებს, უკრაინას, საქართველოს, ევროპასა და დანარჩენ სამყაროს უტევს კიბერმეთოდებით, წინასწარ დამუშავებული ჰიბრიდული ხერხებით და დეზინფორმაციით. მაგალითად, რუსები სლოვაკეთსა და ჩეხეთში ამერიკის ენერგეტიკული პოლიტიკის კრიტიკაზე არიან ორიენტირებულნი და ცდილობენ წარმოაჩინონ, თითქოს აშშ მხოლოდ საკუთარი ინტერესებიდან გამომდინარე მოქმედებს, მსოფლიოს სხვადასხვა კუთხეში კონფლიქტების პროვოცირებას უწყობს ხელს. რუმინეთში რუსეთიდან დაფინანსებული მედიასაშუალებები ცდილობენ, ევროკავშირში გაწევრიანება შეცდომად წარმოაჩინონ და დემოკრატიული ინსტიტუტები დააკნინონ. შვედეთში მთავრობა სექსუალური გარყვნილების მიმდევრად არის წარმოჩენილი. უკრაინაში მიდის პროპაგანდა კორუფციაზე, სიღარიბეზე, უწესრიგობასა და დასავლეთის მიერ მართულ „მარიონეტულ“ რეჟიმზე. ლიტვაში, ლატვიასა და ესტონეთში პროპაგანდისტული მანქანა მუშაობს იმაზე, თუ როგორი დისკრიმინაციის ქვეშ არიან ამ ქვეყნებში რუსები მათი ეთნიკური თუ ენობრივი მახასიათებლების გამო.[108]

[108] ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., "კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016, გვ. 5-25.

მიუხედავად რუსული აგრესიისა, ყველა პოსტსაბჭოთა ქვეყნის სასახელოდ უნდა ითქვას, რომ საბჭოთა კავშირის დაშლის შემდეგ არსად დაწყებულა რუსებისა და რუსულენოვანი მოსახლეობის მასობრივი დევნა-შევიწროება, ადგილი არ ჰქონია სისხლისღვრასა და სისასტიკეს. ალბათ ამ შემთხვევაში გადამწყვეტი როლი შეასრულა იმ ფაქტორმა, რომ 70 წლის განმავლობაში მაინც ჩამოყალიბდა ნათესაური კავშირები და სხვა სახის კულტურული თუ სოციალური ურთიერთობები. იმის ნაცვლად, რომ რუსეთი გაფრთხილებოდა ამ ურთიერთობებს, დაიწყო საბჭოთა კავშირის მსგავსი სივრცის შექმნა, სადაც მუდმივად ანხორციელებს სამხედრო აგრესიას და ეწევა ჰიბრიდულ ომს. ცნობილია, რომ ბალტიისპირეთში რუსეთის პროპაგანდის მთავარი მამოძრავებელი ძალაა **„Первый Балтийский канал“,** ასევე ონლიაინსაიტი **Regnum.ru**, რომელიც 10 წელზე მეტია ფუნქციონირებს. ბოლო დროს რუსებმა აამუშავეს საიტი **Baltnews**, სადაც ანონიმურად თავსდება ინფორმაცია და ახალი ამბები ესტონურ, ლიეტუვურ და ლატვიურ ენებზე.[109]

როგორც გერმანული გამოცემა **"ბილდი"** საკუთარ წყაროებზე დაყრდნობით წერს, თუ 2008 წლის საქართველო-რუსეთის ომში ამერიკის შეერთებული შტატები ღიად ჩაერეოდა, რუსებს ბალტიის ქყვეყნებზე თავდასხმა ჰქონდათ გადაწყვეტილი, ხოლო თუ ამერიკელები ბალტიის ქვეყნებსაც გაუწევდნენ დახმარებას, მაშინ ბირთვული იარაღის გამოყენებასაც ფიქრობდნენ. **"ბილდის"** მიმომხილველი ასევე წერს, რომ ფართომასშტაბიანი სამხედრო სწავლების - "დასავლეთ 2017"-ის ფარგლებში რუსეთი რეპეტიციობდა არა ტერორიზმის წინააღმდეგ ბრძოლაში, არამედ ნატოს წინააღმდეგ ომში და მათ ეს ინფორმაცია დასავლეთის სადაზვერვო მონაცემებზე დაყრდნობით აქვთ. გამოცემა ამტკიცებს, რომ სწავლების სცენარი ეფუძნებოდა ბალტიის ქვეყნებისა და ბელორუსის ოკუპაციას რამდენიმე დღეში. ასევე, სწავლება ეხებოდა

[109] ვაჩარაძე ა. "რუსეთის საინფორმაციო ომი - სტრატეგიები და მიზნები", სააგენტო "დამოუკიდებლობა", 2015, გვ. 1. http://www.damoukidebloba.ge, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.

"შოკურ კამპანიას" ნატოს წევრი ქვეყნების წინააღმდეგ, მათ შორის იყო გერმანია, ნიდერლანდები, პოლონეთი, ნორვეგია, ნეიტრალური შვედეთი და ფინეთი. გამოცემის წყაროს მტკიცრბით, რუსეთი ვარჯიშობდა ბალტიის ქვეყნების აეროპორტებისა და პორტების განეიტრალებასა და მათზე კონტროლის დამყარებაზე. ამონარიდი გამოცემიდან:

"იმ შემთხვევაში, თუ ომი რეალურად იქნება, მათი მიზანი კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურა გახდება, მათ შორის აეროპორტები, ნავსადგურები, სადგურები და სხვა ინფრასტრუქტურა, რათა ამ ქვეყნებში შოკი გამოიწვიოს და ადგილობრივმა მოსახლეობამ ხელისუფლებისგან ზავი ითხოვოს".[110]

გამოცემის ცნობით, სწავლების ფარგლებში რუსეთმა დატესტა ნორვეგიის ქალაქ შპიცბერგენის დაბომბვა და ხელში ჩაგდება. როგორც ვნახეთ, ეს გეგმა პრაქტიკულად არ განხორციელდა, 2008 წლის მოვლენებში ამერიკის შეერთებული შტატები არ წამოეგო რუსეთის პროვოკაციაზე, მაგრამ რაკი არსებობს მსგავსი მოდელირებული გეგმა, რუსეთი ჰიბრიდული ომით და კიბერთავდასხმებით მაინც აკეთებს თავის საქმეს, ნუ გამოვრიცხავთ, რომ იგივე კრიზისული სიტუაცია ისევ დადგეს.

2018 წლის ივნისში პენტაგონმა აღიარა, რომ რუსეთის შეჭრის შემთხვევაში, ბალტიისპირეთის ქვეყნების და პოლონეთის დაცვას ვერ მოასწრებს. **"ვაშინგტონ პოსტის"** ცნობით, ამ დასკვნამდე პენტაგონში ევროკავშირის ქვეყნებისა და რუსეთის სამხედრო წინააღმდეგობის სიმულაციის შედეგად მივიდნენ. როგორც გამოცემა იტყობინება: „სანამ აშშ-ის არმიის შტაბი 17 ფორმას შეავსებს იმისათვის, რომ ნატოს მოწინავე ძალები გერმანიიდან პოლონეთში გადაისროლოს, რუსეთი ბალტიისპირეთის ქვეყნების დაკავებას შეძლებს“. გაზეთი წერს, რომ ამერიკული ჯარისთვის კიდევ ერთი მნიშვნელოვანი პრობლემა ვიწრო ქუჩები და არასაიმედო

[110] ბასილაია ე. "გერმანული მედია: რუსები 2008 წელს ბირთვული იარაღის გამოყენებას აპირებდნენ". გაზეთი "რეზონანსი", 2017, გვ. 1. http://www.resonancedaily.com, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.

სატრანსპორტო ინფრასტრუქტურაა, ხიდებიც კი ისეთი სუსტია, ამერიკული ტექნიკის წონას ვერ გაუძლებს. საზღვრებზე პრობლემებს ქმნის ევროპული ბიუროკრატიაც.[111]

რუსეთს პოსტსაბჭოთა სივრცეში გახსნილი აქვს რამდენიმე ფრონტი, სადაც ჩართულნი არიან ხელისუფლების მაღალჩინოსნები. მაგალითად, 2019 წლის სექტემბერში საგარეო საქმეთა მინისტრმა **სერგეი ლავროვმა** აღნიშნა, რომ ბალტიისპირეთის ქვეყნები დღემდე ევროკავშირის დოტაციაზე ცხოვრობენ და მათ დახმარება მალე შეუწყდებათ.[112] რასაკვირველია, ეს არის გამიზნული დეზინფორმაცია, რომლის მეშვეობითაც რუსები ცდილობენ, ბალტიის ქვეყნების მოსახლეობას გაუჩინონ ნიჰილიზმი და უიმედობის შეგრძნება - აგერ, დღეს ევროკავშირი გეხმარებათ, დასავლეთის კმაყოფაზე ხართ, მაგრამ ხვალ ეს დახმარება შეგიწყდებათო. რუსეთი ანხორციელებს მუდმივ იდეოლოგიურ ზეწოლას - მაგალითად, კრემლი დაუსრულებლად ამტკიცებს, რომ ბალტიის სახელმწიფოების გასაბჭოება საერთაშორისო სამართლის ნორმების შესაბამისად მოხდა და ტერმინი **”ოკუპაცია”** აქ არ შეიძლება იქნას გამოყენებული. კრემლი მალავს ფაქტს, როცა ამ ქვეყნების საგარეო საქმეთა მინისტრებს ე.წ. შეთანხმებაზე ხელის მოწერა არ სურდათ, ისინი შიშობდნენ, რომ ეს მათ ნეიტრალიტეტს დაარღვევდა. უარის შემდეგ კი **მოლოტოვმა** ესტონეთის წარმომადგენელს ასე მიმართა:

"ჩვენ დიდხანს ლოდინი არ შეგვიძლია. გირჩევთ, დაეთანხმოთ საბჭოთა კავშირის სურვილს, რათა თავიდან აიცილოთ უარესი. ნუ აიძულებთ საბჭოთა კავშირს ძალის გამოყენებას.".[113]

---

[111] Person R. 6 reasons not to worry about Russia invading the Baltics, The Washington Post, 2015, p 1. https://www.washingtonpost.com, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.

[112] იაგორაშვილი ი. "რუსეთის 2 მითი ბალტიისპირეთის ქვეყნების შესახებ". ვებ-გვერდი "My the Detector", 2019, გვ. 1. https://www.mythdetector.ge, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.

[113] იაგორაშვილი ი. "მარია ზახაროვა სსრკ-ის მიერ ესტონეთის ოკუპაციას უარყოფს". ვებ-გვერდი "My the Detector", 2020, გვ. 1. https://www.mythdetector.ge, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.

ეს ისეთივე "მიწვევაა" რუსეთის ჯარებისა, როგორც საქართველოში "მოიწვიეს" ბოლშევიკები **სერგო ორჯონიკიძის** მეთაურობით. ისტორიის გაყალბება - ეს გახლავთ რუსეთის კიდევ ერთი მიმართულება, ანუ დიდი სტრატეგიის ერთ-ერთი ნაწილი, რაც „მშვენივრად“ ჯდება ჰიბრიდული ომის ფარგლებში.

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.

სიღრმისეული ინტერვიუები ექსპერტებთან

ამირან სალუქვაძე

(ინტერვიუ ჩაწერილია 2020 წლის, 2 მაისს.)

(ბრიგადის გენერალი, სამხედრო საჰაერო ძალების სარდლის ყოფილი მოადგილე, საჰაერო თავდაცვის ყოფილი უფროსი (2000-2003), საქართველოს თავდაცვის სამინისტროს საჰაერო ძალების მთვარი სამმართველოს შტაბის ყოფილი უფროსი (2004-2005).

2020 წლის მარტიდან მსოფლიო მნიშვნელოვანი პრობლემის წინაშე დადგა - კორონავირუსის (COVID 9) აფეთქებამ ბევრი რამ შეცვალა დედამიწაზე და არნახული დოზით „ააყვავა“ საინფორმაციო სივრცე, სადაც მთელი ძალებით ამუშავდნენ ყალბი ამბების გამავრცელებლები.

რამდენად დიდი საფრთხეა დღევანდელი მსოფლიოსთვის კიბერთავდასხმები, საინფორმაციო ომი და ე.წ. ფეიკ-ნიუსი, როგორც მოვლენა? როგორ შეაფასებთ ამჟამინდელ მდგომარეობას? ამ შეკითხვაზე ამირან სალუქვაძე პასუხობს:

„საკმაოდ ძლიერი საინფორმაციო მანქანაა ამუშავებული, რომლის მიზანიც ხალხის დაზაფვრა და დაფეთებაა. ეს კამპანია დღეს არ დაწყებულა, წლების განმავლობაში მიმდინარეობს. ჩემი დაკვირვებით, მალე წარმოუდგენლად მძლავრი ტექნოლიგიური ინფრასტრუქტურა ამოქმედდება მსოფლიოში, რაც სრულიად ახალ შესაძლებლობებს გახსნის. ეს დაახლოებით იმ ტექნოლოგიური რევოლუციის ტოლფასია, როგორიც ინტერნეტი იყო, მანამდე კი პერსონალური კომპიუტერი, იქნებ მეტიც. ნავთობის სახელმწიფოების დრო დასრულდა - თან მგონი სამუდამოდაც. მსოფლიო კაპიტალი ახლა უკვე სხვა მიმართულებით აიღებს გეზს.

რა არის საჭირო იმისთვის, რომ ვირტუალური სივრცე უფრო უსაფრთხო გახდეს?

„ჩვენ საზოგადოებას აქვს სერიოზული პრობლემა. აქ ციციკორე მახსენდება - რკინიგზის გაყვანას რომ აპროტესტებდა და მატარებელს ეშმაკის მანქანას ეძახდა, რომელიც გარყვნილებას, ავადმყოფობას, გადაჯიშებას და ათას უბედურებას მოიტანდა სოფელში, სადაც მარიტას ტალახს ესროდნენ და კლავდნენ. ამ უსაგნო კამათს მიკროტალღებზე და რადიაციაზე, მიკროჩიპებზე და ბავშვიჭამია კანიბალებზე ძალიან ტრივიალური ამბავი უდევს საფუძვლად - როცა ზოგიერთი დერჭავა ვერაფერს უპირისპირებს პროგრესს, მას ხან ეშმაკისეულს ეძახის, ხან აპოკალიფსურს, ხანაც მასონურს. არადა, წინ შესანიშნავი შესაძლებლობები იხნსება, მათ შორის ბიზნესების თვალსაზრისითაც და შიშით და ფეთებით სადღაც სოროში შეძრომას, ისევ იმაზე სჯობს ვიფიქროთ, სად შეიძლება ჩვენი ადგილი ვიპოვოთ ამ ახალ შესაძლებლობებში - ქვეყანასაც ვგულისხმობ და თითოეულ ჩვენგანსაც. ვირტუალური სივრცე უფრო უსაფრთხო რომ გახდეს, საჭიროა მეტი განათლება. დღეს მსოფლიოში ორი პანდემია მძვინვარებს, ერთი COVID 19-ის, მეორე - შეთქმულების თეორიების. მსოფლიოს ისტორიაში ვერ იპოვით ეპიდემიას ან სხვა კრიზისს, ომებს, მნიშვნელოვან მოვლენებს, რომლებსაც თან არ ახლდა ჭორები, შიშები, დეზინფორმაციები, შეთქმულების თეორიები. 1816 წლიდან 1975 წლამდე მსოფლიომ ქოლერის 7 ეპიდემია გადაიტანა. მეორე ეპიდემია რუსეთ-სპარსეთის 1828-1829 წლების შემდეგ დაიწყო და მთელ რუსეთს მოედო. ქოლერის პირველი შემთხვევები 1930 წელს თბილისსა და ასტრახანში აღმოაჩინეს. ეპიდემიამ მოსკოვსა და სანკტ-პეტერბურგს 1931 წელს მიაღწია. როგორც რუსეთის მთელ იმპერიაში, ისე მის დედაქალაქში ბუნტი დაიწყო - მოქალაქეებს, რომლებმაც იცოდნენ, რომ ინფექცია ორგანიზმში ცუდი საკვების და წყლის მეშვეობით ხვდებოდა, ეგონათ რომ მათ სპეციალურად ხოცავდნენ. დაიწყეს საავადმყოფოების დაზიანება, კლავდნენ ექიმებსა და პოლიციელებს. ახლაც იგევე ეჭვებს აღვივებდნენ, თითქოს მსოფლიო მთავრობა სპეციალურად ხოცავს მოხუცებს“.

შესაძლებელია თუ არა კიბერომის შეჩერება და ლიკვიდაცია ტექნოლოგიური მიღწევებით? - როგორი მდგომარეობაა ამ მხრივ საქართველოში? გასაგებია, რომ გვეხმარებიან, არსებობს საერთაშორისო სტანდარტები, რეკომენდაციები, თანამშრომლობის მემორანდუმები, მაგრამ ჩვენ თვითონ რა შეგვიძლია?

„სახელმწიფოს წინაშე ძალიან ბევრი გამოწვევა არსებობს, ამ გამოწვევებს მხოლოდ სახელმწიფო უსაფრთხოების სამსახური ვერ გაუმკლავდება. ყველაზე დიდი გამოწვევა რუსული აგრესიაა, ის ქმედებები, რასაც ოკუპირებულ ტერიტორიებზე აქვს ადგილი. ჩვენ არ უნდა დავსახოთ არარეალური ამოცანები და შეუძლებელი არ უნდა მოვითხოვოთ სხვადასხვა უწყებებისგან. თუნდაც საერთაშორისო თანამეგობრობისგან. ვხედავთ, როგორ მოქმედებს რუსეთი თავის საზღვრებს გარეთ, ამისი ნათელი მაგალითია სირიაში განვითარებული მოვლენები. ზესახელმწიფოებიც კი ცდილობენ, არ წავიდნენ რუსეთთან დაპირისპირებაზე. ჩვენ უნდა ვიმოქმედოთ არსებული რეალობის გათვალისწინებით. საჭიროა შეთანხმებული მოქმედება, ახლა პოლიტიკური ქულების მიღებისთვის ბრძოლის დრო არ არის. სახელმწიფო უსაფრთხოების სამსახურის მიერ გამოქვეყნებული ანგარიშებიდანაც კარგად ჩანს, რომ უცხო ქვეყნების სპეცსამსახურები კვლავაც აქტიურად მოქმედებენ ჩვენს ტერიტორიაზე, იგივე ხდება ვირტუალურ სივრცეშიც“.

რა როლს ასრულებს რუსეთი კიბერომის თვალსაზრისით და არის თუ არა წამყვანი სახელმწიფო ამ კუთხით?

„რუსეთს ისეთი კანონმდებლობა აქვს, სპეცსამსახურები ყველა ინტერნეტ სერვისს (ელექტრონული ფოსტა, სოციალური ქსელები, საიტები, ფაილების შენახვის სივრცეები და სხ.) შეუზღუდავად აკონტროლებენ. კიბერსივრცის კუთხით საკანონმდებლო ბაზა დასავლურმა ქვეყნებმაც გაამკაცრეს, თუმცა რუსეთში უფრო სხვაგვარად არის ყველაფერი.

მაგალითად ავიღოთ **Mail.ru**-ს პორტალი. რატომ იზიდავს ხალხს ეს სერვისი? უნდა ვაღიაროთ, ეს ერთ-ერთი მოხერხებული, ინფორმაციულად დატვირთული და კვალიფიციურად შექმნილი პორტალია მთელ მსოფლიოში. ერთ სივრცეში მომხმარებელი ხედავს საძიებო სისტემას, ახალ ამბებს, გაცნობის სერვისებს (**Знакомства**, რომელიც პოპულარულია საქართველოში), სოციალურ ქსელებს **(Мой мир, Вконтакте, Одноклассники),** ელექტრონულ ფოსტას, განცხადებებს, კითხვა-პასუხის სერვისს, ფაილების შენახვის უფასო სივრცეს და ა.შ.

მედიაში ღიად იწერებოდა, თუ როგორ მოხდა **„Вконтакте“-ს** და **„Одноклассники“-ს** გამოსყიდვა **Mail.ru-ს** მიერ. მიზანი კი ზუსტად ყველა ამ სერვისის სამთავრობო კონტროლის ქვეშ მოქცევა იყო.

Mail.ru-ს გარდა არსებობს სხვა ცნობილი პორტალები, რომლებსაც ანალოგიური სერვისები გააჩნიათ. კერძოდ, ესენია **Yandex.ru, Rambler.ru** და სხვა. **Yandex.ru** რუსეთში ყველაზე პოპულარული საძიებო სისტემაა.

აღნიშნულ პორტალებს გააჩნიათ საკმარისი მონაცემთა ბაზები (სერვერები), რათა განუსაზღვრელი ვადით შეინახონ განუსაზღვრელი მოცულობის ინფორმაცია. საჭიროების შემთხვევაში კი სპეცსამსახურებს შეგროვებული ინფორმაციის სრულად გამოყენება შეეძლება. ამ პორტალებს გარდა, რა თქმა უნდა, უამრავი სხვა საიტი, სპეციალური ვირუსული თუ სხვა სახის პროგრამები, თამაშები და აპლიკაციებია, რომლებიც შესაძლოა ასევე სპეცსამსახურების პირდაპირი კონტროლის ქვეშ იყოს, ან საჭიროებისამებრ გამოიყენონ.მე დაგისახელეთ ერთი კომპლექსური მაგალითი, რომელიც ნათლად გვიჩვენებს, თუ ვისთან გვაქვს საქმე“.

როგორ დავიცვათ თავი რუსული ჰიბრიდული ომისგან და ჰაკერული თავდასხმებისგან?

„არსებობს სხვა წარმომავლობის **(ამერიკული, ევროპული, ჩინური)** ინტერნეტ სერვისები. თუ რომელიმე ინტერნეტ პროდუქტი (საიტი, ელ-ფოსტა, პროგრამები და სხვა) არაა განთავსებული რუსულ სივრცეში

(xxx.ru), ეს არ ნიშნავს, რომ მის გაკონტროლებას ვერ შესძლებენ რუსული სპეცსამსახურები. მაგალითად, ცნობილია, რომ **Viber**-ის რეგიონული სერვერები განთავსებულია რუსეთის ტერიტორიაზე. შესაბამისად, მათი კონტროლი პრობლემას არ წარმოადგენს. ბევრი ინტერნეტ საიტი სხვა, არარუსულ სივრცეში, შესაძლოა რუსეთის სპეცსამსახურების ან რუსეთის მოქალაქეების მიერ იყოს შექმნილი. ამას გარდა, საქართველოს მიმართ ინტერესები გააჩნია არა მხოლოდ რუსეთს, არამედ უამრავ ქვეყანას, განსაკუთრებით სამეზობლოს ან ქვეყნებს, რომლებსაც რეგიონში ინტერესები აქვთ. მაგალითად, Yandex ტაქსი მომხმარებელს სრულ სერვისს და დაბალ ფასებს სთავაზობს. საკმარისია, ერთხელ მაინც ისარგებლოთ მისი სერვისით და თქვენი ტელეფონის ნომერი და თქვენი გადაადგილების მარშრუტი სამუდამოდ დარჩება **Yandex-ის** ბაზაში. თუ ხშირად სარგებლობთ, ჩათვალეთ, რომ თქვენი მარშრუტები, მისამართები ასევე თქვენს ვინაობაზე და საკონტაქტო მონაცემებზე მიბმული, **Yandex-ის** მონაცემთა ბაზის ბინადარი გახდება.

რა ინფორმაციის აღება შეიძლება მობილური ნომრის მეშვეობით? არ დაკვირვებიხართ, როცა რეკავთ მაგალითად ცნობათა ბიუროში, თქვენ არ გეკითხებიან, როგორ მოგმართონ და იმ წამსვე სახელით გპასუხობენ? ეს ნიშნავს, რომ უამრავ სერვისს დაშვება აქვთ მობილური ქსელების მონაცემთა ბაზებთან. დიდი ალბათობით, ასეთივე დაშვება ექნება Yandex-ტაქსსაც. შესაბამისად, მობილურ ნომერთან ერთად ეცოდინებათ თქვენი მისამართიც, ვინაობაც, პირადი ნომერიც. ამას დაუმატებენ თქვენი მოძრაობის მარშრუტებს.

Yandex ტაქსი მომხმარებელს სთავაზობს მობილურ აპლიკაციას, რომლის მეშვეობით თქვენ ერთის მხრივ მოხერხებულ სერვისს იღებთ, ავტომატურად იძახებთ ავტომობილს, აკონტროლებთ თქვენს მიერ გამოძახებული ტაქსის მოძრაობას, მეორეს მხრივ - მობილურ აპლიკაციას აძლევთ თქვენს სმარტფონზე სახიფათო წვდომას. მობილურ ოპერატორებს, ინტერნეტ პროვაიდერებს ძალიან დიდი შესაძლებლობები გააჩნიათ,

შეაგროვონ სადაზვერვო ინფორმაციები როგორც პიროვნებების, ასევე კომპანიებისა და ორგანიზაციების შესახებ. ფაქტობრივად, ეს არის ობობას ქსელი, რომლისგან თავის დაღწევაც შეიძლება მხოლოდ ცოდნით. განსაცდელის დროს ადამიანს ყველაზე მეტად აწუხებს გაურკვევლობა. შესაბამისად, ის ცდილობს მონახოს პასუხები ყველაფერზე, რაც მას აფიქრებს, განსაკუთრებით პრობლემის წარმომავლობაზე, მისი გაჩენის მიზეზებზე და მომავლის პროგნოზირებაზე. იმისათვის, რომ ინფორმაციები, ვერსიები, თეორიები დამაჯერებელი იყოს, ის დეტალურად უნდა იყოს აღწერილი და გაანალიზებული“.

რას შეიძლება მიაღწიოს რუსეთმა პოსტსაბჭოთა ქვეყნებსა და აღმოსავლეთ ევროპაში გამალებული პროპაგანდით თუ უწყვეტი დეზინფორმაციით? ხედავთ თუ არა ამის ნიშნებს?

„მოდით, ჯერ ის ვთქვათ, რა ინფორმაცია აინტერესებთ უცხო ქვეყნების (ანუ, არა მხოლოდ რუსეთის) სპეცსამსახურებს, რასაც სადაზვერვო ინფორმაციას ვეძახით?

რატომ აღვწერე ზემოთ, როგორ კონტროლდება ინტერნეტ ან მობილური სერვისები? იმიტომ, რომ თუ თქვენ, ან თქვენი მეზობელი, ნათესავი, ოჯახის წევრი ან თქვენი სამსახური წარმოადგენს უცხო ქვეყნის სპეცსამსახურის ინტერესს და წვდომა ექნებათ თქვენს კომპიუტერზე, ელექტრონულ ფოსტაზე ან მობილურ ტელეფონზე, მათთვის საინტერესო იქნება ყველაფერი.

ასეთი ინფორმაციების შეგროვებისას წვრილმანი არ არსებობს: ფოტოები, წერილები, კონტაქტები, მიდრეკილებები, სუსტი ადგილები და ა.შ. ეს რაც ეხება პიროვნებებს. ანალოგიურად ხდება ორგანიზაციებთან, კომპანიებთან მიმართებაში.

ჩვენ ძალიან ბევრ საკითხს დაუდევრად ვეპყრობით. მაგალითად, ძალოვანი სტრუქტურების თანამშრომლების მიერ სოციალურ ქსელებში, კერძოდ „ფეისბუქში“ პირადი გვერდების ქონა და წარმოება. იყო დრო, როცა

ძალოვანი სტრუქტურების მოსამსახურეებს აკრძალული ჰქონდათ სოციალურ ქსელებში დარეგისტრირება. ერთ დღეს გადაწყვიტეს, რომ ანაკლიის პროექტისთვის ბევრი „ლაიქი“ დაეწერათ და გაიცა ბრძანება: „შექმენით ფეისბუქის პროფილი და მოიწონეთ“. ახლა მოდით და აკრძალეთ, როგორია?

კიდევ ერთი მაგალითი, კორპორატიული ნომრები. წარმოიდგინეთ, მობილურ პროვაიდერს ვაწვდით მთელი უწყების სიას, თანამდებობების, პირადი ნომრების და მობილური ნომრების მითითებით. ეს უკვე არის ძალიან ბევრი ინფორმაცია. გჭირდებათ დამატებითი ინფორმაციის მოპოვება ადამიანზე? თუ გაქვთ ადამიანის სახელი, გვარი, თანამდებობა, მობილური და პირადი ნომერი, გჭირდება მისამართის დადგენა. არ დავასახელებ რომელ საიტზეა შესაძლებელი, მაგრამ პირადი ნომრით შეგიძლიათ პიროვნების ზუსტი მისამართი ამოიღოთ, ხოლო paybox.ge-ზე მთელ მის მიკროსაფინანსო ორგანიზაციების კრედიტების თუ სხვა საქმიანობის გადამოწმება შეიძლება.

სამოქალაქო უწყებების ხელმძღვანელებს ვურჩევ, გაიარონ კონსულტაციები.

სპეცსამსახურების ერთ-ერთი სამიზნე ახალგაზრდობაც არის. დღეს სტუდენტია, ხვალ - ჩინოვნიკი, ზეგ - მინისტრი.

ბევრისგან მომისმენია, შეაგროვონ, არაფერი მაქვს დასამალიო. ზოგმა ისიც არ იცის, რომ თუ „ფეისბუქში“ ან ელ-ფოსტაში წაშალა მიმოწერა ან ფოტოები წაშლილი ჰგონია. ყველა ჩინოვნიკი ვალდებულია, იფიქროს ამ ყველაფერზე და მკაცრად შეასრულოს უწყებრივი რეგულაციები. ორგანიზაციებს აწყენთ თუ კიდევ ერთხელ მოახდენენ კიბერუსაფრთხოების თვალსაზრისით თანამშრომელთა პირადი ინფორმაციების დაცვის საკითხების რევიზიას. შესაძლოა, ამ მხრივ უამრავი პრობლემა აღმოჩნდეს“.

რა შეიცვლება მსოფლიოში და მათ შორის საქართველოში პანდემიის შემდეგ?

„შიში დეზინფორმაციის მთავარი მამოძრავებელი ძალაა. ამ ეპიდემიას სხვადასხვა კონსპიროლოგიური თეორიები ახლავს. ჩიპიზაციის და 5G ტექნოლოგიების გარდა, ბევრი ვერსიებია ვირუსის წარმომავლობის და მისი არსებობის შესახებ. ზოგის ვარაუდით, ვირუსი ჩინეთის ლაბორატორიიდან "გაექცათ", ზოგიერთით კი ნოვოსიბირსკიდან. ზოგი ამერიკელებს აბრალებს, თითქოს სპორტული ფორუმის დროს გაავრცელეს. ბევრი ავრცელებდა ძველ სტატიებს, გაოცებული კომენტარებით, ნახეთ, რომ ამბობენ ახალი კორონავირუსიაო, არაა ახალი, ადრეც იყოო და აფრიალებენ გაყვითლებული საბჭოთა გაზეთებიდან "აღმოჩენების" ფოტოასლებს. ამ სიახლის დადგენაში, ურთიერთბრალდებების, ხანგრძლივი საინფორმაციო ომის მომსწრენი ვიქნებით. ყველაზე მავნე, რაც ხდება, ესაა თავად ეპიდემიის არსებობის კითხვის ნიშნის ქვეშ დაყენება. ეს კი იწვევს მოსახლეობის მხრიდან უსაფრთხოების ნორმების დაცვის უგულებელყოფას. ხელს უწყობს ეპიდემიის გავრცელებას და საფრთხეს უქმნის მოსახლეობის დიდ ნაწილს. **რას ნიშნავს ე.წ. ჩიპიზაცია, ვაქცინაცია და გლობალური კონტროლი?** ვაქცინაციის წინააღმდეგ პროტესტი ჯერ კიდევ მე-19 საუკუნეში დაიწყო, როცა ედვარდ ჯონერმა ჩუტყვავილას საწინააღმდეგო ვაქცინა შექმნა. მეცნიერება, რა თქმა უნდა, წინ წავიდა. ნანოტექნელოგიების წყალობით. დღეს მართლაც შესაძლებელია მინი ჩიპების დამზადება, მათი კანის ქვეშ ჩაყენება, მაგრამ ყველაფერი არაა ისე მარტივად, როგორც საუბრობენ. არსებობს მიკროჩიპის ორგანიზმში ნემსით შეყვანის გამოცდილება, მაგრამ ნახეთ ვიდეოები, უხვადაა ინტერნეტში, რა ზომის ჩიპზეა საუბარი და როგორი ნემსით, უფრო სწორად, შპრიცით ხდება. ამავე დროს, ყოველ ადამიანზე მისი ინდივიდუალური ჩიპი რომ შეიყვანო ორგანიზმში, ე.ი. ჯერ ამ ჩიპებზე ინფორმაცია უნდა დაიტანო. ვინც ჩიპი უნდა შეიყვანოს კანის ქვეშ, მან უნდა იცოდეს, რომელი ჩიპი ვის ორგანიზმში მოახვედროს. ეს პროცესი ვერ მოხდება ფარულად.

ტექნოლოგიურად რომც იყოს ასეთი "ჩიპიზაციის" შესაძლებლობა, მის ორგანიზებაში ჩართული იქნება უამრავი ადამიანი, რამდენიმე უწყებიდან. რადგანაც ფარულობა შეუძლებელია, მას დასჭირდება საკანონმდებლო რეგულირება. ანუ, არათუ ტექნიკურად, როცა მეცნიერება შეძლებს ასეთი ამოცანის გადაჭრას, უამრავ ქვეყანაში იდეის დონეზეც კი არ მიიღებენ. რაც შეეხება ევროპის ზოგიერთ ქვეყანაში უკვე დაწყებულ ჩიპიზაციას. ესაა დაახლოებით ისეთი ტიპის ჩიპები, როგორებიც ჩვენს ID ბარათებზეა, ოქროსფერი ფირფიტა, რომელზეც დატანილია პირადი მონაცემები. შესაძლოა დატანილი იქნას საბანკო რეკვიზიტები, სამგზავრო ტალონები, სადარბაზოს კიდები და სხვა. არსებობს სხვა ფორმის და ზომის მინი ჩიპები, რომელთა კანს ქვეშ შეყვანა ხდება საკმაოდ მსხვილი შპრიცებით. ასევე ცნობილია ისიც, რომ ასეთი ჩიპების კიბერდაცულობა საკმაოდ დაბალია და შესაძლებელია მათი გატეხვა. მოკლედ, ფარულად, ჩიპიზაციის საფარქვეშ, ვერავინ ვერავის "დაჩიპავს". ვიმეორებ, ტექნიკური მზადყოფნაც რომ არსებობდეს, ორგანიზაციულად, ადამიანების ნების გარეშე ეს ვერ მოხდება. რაც შეეხება ვაქცინაციას, ჯერ-ჯერობით არც ისეთი ვაქცინა არსებობს, რომელსაც შეუძლია გარკვეულ რასებზე, ან გარკვეული ასაკის ან სქესის ადამიანებზე გამორჩეულად ზემოქმედება. ოდესმე, შესაძლოა, მივიდნენ აქამდე. **რატომ გამოიწვია პანიკა 5G ტექნოლოგიამ?** მოთხოვნა იწვევს ქსელის გაფართოების, მისი გამტარუნარიანობის და სისწრაფის გაზრდის საჭიროებას. მობილური ტელეფონები, კომპიუტერები, ინტერნეტ ტელევიზია, სიგნალიზაციები, საგზაო კამერები და ა.შ. ყველაფერს ინტერნეტი სჭირდება. დღევანდელ "ფასტ-ფუდების" და ინტერნეტის ეპოქაში, როცა ყველაფერი, ჰაერიც კი მომწამვლელია, 5G-ს შიში აშკარად ან ახირება, ან კონსპიროლოგიის გავლენაა. ადამიანთა დიდმა ნაწილმა არ იცის, რა არის იონიზირებადი და არაიონიზირებადი გამოსხივება. არაიონიზირებადი გამისხივება, ანუ რადიოტალღები, ინფრაწითელი, ხილვადი გამისხივება, საშიშად არ მიიჩნევა, ხოლო იონიზირებადი, ანუ რადიაცია, რომელიც ახდენს ნივთიერების იონიზაციას, საშიშია.

იონიზირებადია გამა-გამოსხივება, რენტგენული გამისხივება. ისიც უნდა ვიცოდეთ, რომ სიხშირეზე მეტად მნიშვნელოვანია გამისხივების სიმძლავრე. ჩვენ ამ გარემოს უკვე ვეღარ გავექცევით. სხვათაშორის, სახლში ჩართული ნოუთბუქები, მობილურები, ისინიც წარმოქმნიან ველს. სიგნალის გაცვლა ორმხრივია. ზოგადად, უნდა ვიცოდეთ, რომ 5G-სგან განსხვავებით, 4G ანტენები გაცილებით მძლავრია, სიგნალს ასხივებენ ყველა მიმართულებით, ხშირად ფუჭად ხარჯავენ ენერგიას. 5G ანტენები სიგნალს უფრო მოკლე ტალღებზე გადასცემენ, სიგნალი უფრო მიმართულია, ანტენები უფრო პატარა და ნაკლები სიმძლავრის. მთავარი "ბრალდება" 5G-ს წინააღმდეგ, ის აღწევს ორგანიზმში. როგორ უნდა დააჯეროთ კონსპიროლოგიით შეპყრობილი და ფიზიკის მასწავლებელზე გაბრაზებული ადამიანი, რომ გრძელი ტალღებისგან გაბსხვავებით, მილიმეტრულ ტალღებს გააჩნიათ ცუდი შეღწევადობის უნარი“?

არის თუ არა ფეიკ-ნიუსი სერიოზული საფრთხე? ვგულისხმობთ ყალბ საინფორმაციო პროპაგანდას.

„ფეიკ-ნიუსი სერიოზული საფრთხეა და მისგან თავდაცვის ერთადერთი მეთოდია ანალიზი. ასევე, უნდა გვქონდეს ერთი წესი, რომელიც ეთიკის ნორმებიდან გამომდინარეობს: ყველა ადამიანს აქვს უფლება, დაიჯეროს რაც სურს, მაგრამ არ უნდა დაკავდეს პროპაგანდით, თუ ამის ინტერესი არ აქვს. წაკითხვის შემდეგ დააკვირდით საკუთარ ემოციებს, ემოცია ცუდი მრჩეველია. შეამოწმეთ წყარო (ვრცელი თემაა). ხშირად სათაურშიც იგრძნობა "სიყვითლე". დაფიქრდით, ხომ არაა დეზინფორმაციის ნიშნები. გადაამოწმეთ ფაქტები. დაფიქრდით, რამდენად ობიექტურად აღიქვამთ. თუ არ ხართ დარწმუნებული, ნუ გაავრცელებთ. უმჯობესია, არ გაავრცელოთ, ვისაც უგზავნით, თავისით იპოვის. გავრცელება ქმნის აჟიოტაჟს, რაც უკან დაგიბრუნდებათ“.

ანდრო გოცირიძე

(ინტერვიუ ჩაწერილია 2020 წლის, 20 მაისს.)

კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის - CYSEC-ის დამფუძნებელი და თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს ყოფილი დირექტორი (2014 -2016 წწ). მისი უშუალო მონაწილეობით დამუშავდა ეროვნული და თავდაცვის სამინისტროს კიბერუსაფრთხოების პოლიტიკა და სტრატეგია. ჩვენთან ინტერვიუში ამბობს, რომ თანამედროვე სამყაროში ნებისმიერი ომი თუ კონფლიქტი კიბერშეტევების გარეშე არ მიმდინარეობს. არაკონფლიქტურ სიტუაციებშიც კი კიბერელემენტები გამოიყენება გეოპოლიტიკური, ეკონომიკური და პოლიტიკური უპირატესობის მოსაპოვებლად და სამხედრო ამოცანების გადასაწყვეტად.

რამდენად დიდი საფრთხეა დღევანდელი მსოფლიოსთვის კიბერთავდასხმები, საინფორმაციო ომი და ე.წ. ფეიკ-ნიუსი, როგორც მოვლენა? როგორ შეაფასებთ ამჟამინდელ მდგომარეობას?

„თავისთავად, კიბერშეტევებს ახასიათებს ორი სახის ეფექტი: ერთი არის კლასიკური, ანუ ტექნიკური შეტევა, რაც გულისხმობს სისტემების წაშლას, განადგურებას; მეორე - ფსიქოლოგიური ეფექტი, ანუ პროპაგანდაზე დაყრდნობილი ოპერაციები, რომელიც გულისხმობს ინფორმაციის გავრცელებას, მოსახლეობის, ანუ სამიზნე აუდიტორიის აღქმის შეცვლას, მოსახლეობის შეხედულებების შეცვლას. სახელმწიფოსთვის უაღრესად საჭიროა, ჰქონდეს კიბერუსაფრთხოების სტრატეგია, რომელიც უნდა შეიცავდეს რამდენიმე პოსტულატს: პირველი - აუცილებელია კერძო სექტორთან საჯარო თანამშრომლობა, რადგან ფიზიკური ინფრასტრუქტურის უმეტესი ნაწილი მოქცეულია კერძო სექტორში. ფიზიკური ინფრასტრუქტურა არის ის სერვისები, რომელთა გამართული ფუნქციონირება სახელმწიფოსთვის გახლავთ სასიცოცხლოდ აუცილებელი. შეიძლება ეს იყოს საბანკო სექტორი ან ჰოსპიტალური სექტორი. დღეს უკვე ვხედავთ, ჰოსპიტალურ სექტორზე რამხელა დაწოლაა. ასევე, შეიძლება იყოს ენერგეტიკული, ჰიდრო, ატომური და ასე შემდეგ. კი, ბატონო, ჩვენ ვიცავთ სახელმწიფო სერვერებს, ეს კარგია, მაგრამ ყურადღების მიღმა გვრჩება ძალიან დიდი და მნიშვნელოვანი მასივი, სადაც უამრავი პროექტია

თავმოყრილი. განათლება, ყურადღება, გამოცდილება წინაპირობაა უნარიანი თავდაცვისა. რასაკვირველია, დღევანდელი და ხვალინდელი მსოფლიოსთვის კიბერომები, კიბერთავდასხმები არის ძალიან სახიფათო, შეიძლება ითქვას, გადამწყვეტიც კი.

არის თუ არა საქართველო მნიშვნელოვანი ამ ომში გეოსტრატეგიული თვალსაზრისით და რა არის საჭირო, რომ უფრო დაცულ სახელმწიფოდ გარდავიქმნათ?

<u>**ანდრო გოცირიძის**</u> განმარტებით, კიბერუსაფრთხოების კუთხით, <u>საქართველო არ არის ჩამორჩენილი ქვეყანა, გვაქვს საკმაოდ გამართული ინფრასტრუქტურა:</u>

„რა თქმა უნდა, ეს ყველაფერი ჩვენი პარტნიორების დახმარებით გაკეთდა, მაგრამ რაც გვაქვს, რატომ უნდა უარვყოთ? თუმცა არის პატარ-პატარა ხარვეზები - ჩვენი კრიტიკული ინფრასტრუქტურა არ მოიცავს კერძო სექტორს და 2020 წლის სტრატეგიაც არ გაგვაქვს მიღებული. საერთოდ, კანონმდებლობის კუთხითაც დეტალები დასახვეწია. მაგალითად, არ არის კანონში დაფიქსირებული, როგორ უნდა მოხდეს კომპიუტერული ტექნიკის შემოტანა ქვეყანაში. მსგავსი ტექნიკა შემოდის, როგორც ბანანი. არ არსებობს არავითარი კონტროლი. მიუხედავად ამისა, მაინც ვერ ვიტყვით, რომ კიბერუსაფრთხოების კუთხით ჩამოვრჩებით, გრანდებში არ შევდივართ, მაგრამ ევროპულ დონეზე ვთამაშობთ“.

რა როლს ასრულებს რუსეთი კიბერომის თვალსაზრისით და არის თუ არა წამყვანი სახელმწიფო ამ კუთხით?

ანდრო გოცირიძის თქმით, რუსეთი არის ერთ-ერთი ყველაზე ძლიერი კიბერ-აქტორი, რომელიც მიდის ყველაფერზე. <u>მსოფლიოში **დესტრუქციულ კიბერ-აქტორებად** მოიაზრებენ **რუსეთს, ჩინეთს, ირანსა და ჩრდილოეთ კორეას:**</u>

„ზოგადად, რუსული კიბერომისგან სრული თავდაცვა არ არსებობს, ეს დიდი პრობლემაა ამერიკის შეერთებული შტატებისთვისაც,

გერმანიისთვისაც, საფრანგეთისთვისაც და მთელი ევროპისთვის, მაგრამ თუ ჩვენ კონტრნაბიჯებს გადავდგამთ, ეფექტური თავდაცვის საშუალებები ნამდვილად გაგვაჩნია. უპირველესად უნდა მივაღწიოთ იმას, რომ მტრულად განწყობილი ქვეყნიდან კომპიუტერული ტექნიკის შემოტანა უნდა იყოს განსაკუთრებული კონტროლის ქვეშ, თუ არ იქნება სრულად აკრძალული. ასევე, თავდაცვის კუთხით საქმეში აუცილებლად უნდა ჩავრთოთ კერძო სექტორი, სადაც არის ძალიან მნიშვნელოვანი ინტელექტუალური პოტენციალი. მაგალითად, მე თავდაცვის სამინისტროში თანამშრომელს ვუხდიდი 1000 ლარს, ბანკში უხდიან 5000 ლარს, გამოდის, ინტელექტი კერძო სექტორში უფრო ძლიერია. დღეს კომპიუტერის კარგი სპეციალისტი ძალიან ძვირად ფასობს. რასაკვირველია, ასევე საჭიროა რუსეთის მხრიდან მოსალოდნელი საფრთხეების გაანალიზება. ჩვენ უნდა ვიცოდეთ, რა შეიძლება მოიმოქმედოს მეზობელმა სახელმწიფომ ნებისმიერ შემთხვევაში. ეს არ ნიშნავს იმას, რომ სახელმწიფო ჩაერიოს კერძო სექტორის საქმიანობაში, უნდა არსებობდეს სტანდარტი - თუ ხარ კრიტიკული ინფრასტრუქტურის წარმომადგენელი, მაშინ შენი სისტემა უნდა იყოს დაცული“.

შესაძლებელია თუ არა კიბერომის შეჩერება და ლიკვიდაცია ტექნოლოგიური მიღწევებით? - როგორი მდგომარეობაა ამ მხრივ საქართველოში? გასაგებია, რომ გვეხმარებიან, არსებობს საერთაშორისო სტანდარტები, რეკომენდაციები, თანამშრომლობის მემორანდუმები, მაგრამ ჩვენ თვითონ რა შეგვიძლია?

„დასავლური ორიენტაციის ახალ დემოკრატიულ ქვეყნებში, როგორიც საქართველოა, რუსეთი ცდილობს, პროდასავლური განწყობები შეცვალოს რუსული განწყობებით და იქონიოს შესაბამისი შესაძლებლობა, შემდგომში განავითაროს რუსული პოლიტიკა. მეტიც, მთავარი მიზანია, ამა თუ იმ ქვეყანაში მოიყვანოს მისთვის სასურველი ხელისუფლება. ევროპაში და მათ შორის ჩვენთანაც, რუსეთი ცდილობს, დემოკრატიას გამოუთხაროს ძირი, მოსახლეობა დაარწმუნოს, რომ დემოკრატია არის ილუზია, სწორი ფორმა

არის საბჭოთა სტილის მმართველობა. რუსეთი არის კიბერთავდასხმების ოსტატი, ეს ქვეყანა ანხორციელებს შეტევებს ხალიფატის სახელით, ანხორციელებს შეტევებს სხვა ქვეყნების სახელით, თითქოს კვალს ფარავს, მაგრამ ხელწერა ნაცნობია. მაგალითად, ბრიტანულმა გამოცემამ („დეილი მეილი“) გამოაქვეყნა სტატია, თითქოს საქართველოში ზის ჰაკერების ჯგუფი, რომელიც ასრულებს რუსების დავალებას და ბრიტანეთის კლინიკებიდან იპარავს პირად მონაცემებს. ამერიკულმა სპეცსამსახურებმა განაში აღმოაჩინეს გრუ-ს დანაყოფი, ასევე ალპებში აღმოჩნდა საიდუმლო ბაზა. მე არ მგონია, საქართველოში რაიმე მსგავსი არსებობდეს. თუმცა ამ შემთხვევაში არ უნდა გამოგვრჩეს, რომ შესაძლებელია, საქართველოში არსებული რუსული კორპორატიული სამსახურები რუსულმა დაზვერვამ გამოიყენოს მსგავსი მოქმედებებისთვის. კიბერომების, კიბერთავდასხმების შეჩერება ან სრულად ლიკვიდაცია შეუძლებელია, რადგან ყოველდღიურად ჩნდება ახალი ტექნოლოგია, რაღაც ახალი მიღწევა და შესაბამისად, ფართოვდება კიბერომის არეალიც“.

როგორ დავიცვათ თავი რუსული ჰიბრიდული ომისგან და ჰაკერული თავდასხმებისგან?

„მე პოლიტიკის სპეციალისტი არ ვარ, მაგრამ აშკარაა, რომ ძალიან ხშირად ოპოზიციაც და ხელისუფლებაც იყენებს საინფორმაციო ომის ელემენტებს. სჯობს, ასე არ იყოს. თუმცა, როგორც ჩანს, საქართველოს ეს ეტაპიც გასავლელი აქვს. მსოფლიოში არსებობს უფრო მნიშვნელოვანი საკითხები - მაგალითად, ტერორიზმი. თუ ადრე ტერორისტები კიბერმეთოდებს ნაკლებად იყენებდნენ, ახლა წამოვიდა უფრო განათლებული თაობა, რომელიც უკეთესად ერკვევა კომპიუტერულ სისტემებში. ჩვენ ამ მხრივ უფრო გვჭირდება თავდაცვა, რუსეთი აქ მოწინავე პოზიციებზეა. გასაძლიერებელია თავდაცვის მეთოდები . დღეს კიბერ-ტერორისტები კარგად იყენებენ სოციალურ ქსელებს, მათთვის ხელმისაწვდომია ინფორმაცია თითქმის ყველა ადამიანზე. საჭიროა საზოგადოებრივი ცნობიერების ამაღლება, რათა ადამიანი არ გახდეს მავნე პროპაგანდის

მსხვერპლი. სოციალური ქსელების მომხმარებლები არ უნდა ტოვებდნენ ისეთ ინფორმაციულ კვალს, რომ შემდგომში სამიზნეებად იქცნენ. თუმცა უნდა ვაღიაროთ, სოციალური მედია არის პროგრესი და შიში არ არის გამოსავალი, საჭიროა ცოდნა და სიფრთხილე“.

ლევან ნიკოლეიშვილი

(ინტერვიუ ჩაწერილია 2020 წლის, 21 მაისს.)

(სახელმწიფო უშიშროების მინისტრის ყოფილი მოადგილე (2004), გენერალური შტაბის ყოფილი უფროსი (2005-2006), პოლკოვნიკი:

როგორი ისტორიული პერიოდი უძღვოდა წინ კიბერომის წარმოშობას?

„თუ მივყვებით თანმიმდევრობით, საინფორმაციო ომი უფრო ადრინდელი პრობლემაა, ვიდრე კიბერომი და ფეიკ-ნიუსი. საინფორმაციო ომი გაცილებით ადრე დაიწყო, ჯერ კიდევ მაშინ, როცა არ არსებობდა ამდენი მედიასაშუალება და სოციალური ქსელი. ეს არის ერთ-ერთი მძლავრი იარაღი, რომლის საშუალებითაც შესაძლებელია არეულობის შეტანა მოწინააღმდეგის ბანაკში. ჩვეულებრივი ომების დროს შეაგზავნიდნენ მსტოვრებს, გაავრცელებდნენ ყალბ ინფორმაციას და აქ მიზანი იყო ორი სახის: პირველი - არეულობის შეტანა, მეორე - სარგებელი უნდა ენახა იმ მხარეს, რომელიც აწყობდა პროვოკაციას. ამის საუკეთესო მაგალითი გახლავთ ფაშისტური გერმანიის მიერ წარმოებული პროპაგანდა მეორე მსოფლიო ომის პერიოდში. იღებდნენ ე.წ. დოკუმენტურ ფილმებს სხვა ქვეყნების ლიდერებზე, მდგომარეობაზე, მოსახლეობაზე და ავრცელებდნენ სხვადასხვა ფორმებით. ეს, რა თქმა უნდა, იწვევდა გარკვეულ დემორალიზაციას და ნერგავდა შიშს, იმედგაცრუებას. იგივე მეთოდს იყენებდა საბჭოთა კავშირიც. ომის დასრულების შემდეგ დაიწყო ახალი ერა, სამმა ზესახელმწიფომ - საბჭოთა კავშირმა, დიდმა ბრიტანეთმა და ამერიკის შეერთებულმა შტატებმა გადაინაწილეს მსოფლიო. ბუნებრივია, ამავე დროს დაიწყო კიბერომების ახალი ეტაპი. თითქოს ქვეყნებს შორის დაპირისპირება აღარ არსებობდა, მაგრამ ბოლოს საქმე იქამდე მივიდა, რომ

საბჭოთა კავშირიც დაინგრა და ვარშავის პაქტიც გაუქმდა. ეს კი გამოიწვია დიდძალმა ფინანსებმა და საინფორმაციო ომმა. მე მახსენდება, ცივი ომის დროს ისეთი საინფორმაციო დაპირისპირება იყო საბჭოთა კავშირსა და აშშ-ს შორის, პრესაში ერთმანეთს კაციჭამიებად ხატავდნენ. ნოდარ დუმბაძის მოგონებები გავიხსენოთ: როდესაც ის პირველად ამერიკაში ჩავიდა, ბავშვები დიდი ინტერესით ათვალიერებდნენ, თუ როგორი იყო საბჭოთა ადამიანი. პირად მაგალითს გეტყვით, 1990-იან წლებში, შეერთებულ შტატებში ერთ-ერთ კონფერენციაზე ვიმყოფებოდი და მეცვა ჩვეულებრივი სამხედრო ფორმა, რომელიც ფერით არ განსხვავდებოდა საბჭოთა ფორმისგან, განსხვავება იყო მხოლოდ სიმბოლიკაში. კონფერენციის დასრულების შემდეგ რამდენიმე ადამიანმა გავისეირნეთ ერთ-ერთ სავაჭრო ცენტრში, სადაც მოულოდნელად მოვიდნენ გამვლელები, აინტერესებდათ, როგორი იყო საბჭოთა ოფიცერი. კი ვეუბნებოდი, არ ვარ საბჭოთა-მეთქი, მაგრამ მაინც ასე აღიქვამდნენ. ყველაზე საოცარი ის იყო, რომ განწყობა არ იყო მტრული. ერთ-ერთმა ამერიკელმა სამხედრო პირმა სურათიც გადაიღო ჩემთან, თავისი ნაცნობ-მეგობრებისთვის უნდა ეჩვენებინა, რომ ნახა ოფიცერი მტრის ბანაკიდან, რომელმაც არც უკბინა, არც ესროლა და არც შეჭამა. აი, ეს იყო გასული საუკუნის პროპაგანდისა და საინფორმაციო ომის შედეგი“.

რამდენად დიდი საფრთხეა დღევანდელი მსოფლიოსთვის კიბერთავდასხმები, საინფორმაციო ომი და ე.წ. ფეიკ-ნიუსი, როგორც მოვლენა? როგორ შეაფასებთ ამჟამინდელ მდგომარეობას?

„ჩვენი საზოგადოება არის მუდმივად დაძაბულ მდგომარეობაში, მუდმივად მიდის საინფორმაციო ომი, ანუ ფეიკ-ნიუსებით ბრძოლა. დღეს თამამად შეგვიძლია ვთქვათ, რომ „ფეიკის მამა“ საქართველოში არის ნიკა გვარამია, ხან პროკურორი რომ იყო, ხან განათლების მინისტრი, ხან კიდევ ჟურნალისტი. ახლა გახლავთ ერთ-ერთი ტელევიზიის („მთავარი არხი“) დირექტორი. მახსენდება ერთი მაგალითი - საქართველოს პატრიარქმა თქვა: „ნუ შეგეშინდებათ, უფალი ჩვენ არ მიგვატოვებს“. გვარამიამ

დაამონტაჟა ასე: „გეშინოდეთ, უფალმა ჩვენ მიგვატოვა“. რატომ ათქმევინა პატრიარქს ასეთი რამ? იმიტომ, რომ თურმე ხელისუფლება არ გვივარგა. სამწუხაროდ, მე ქადაგება არ მქონდა მოსმენილი და როცა ეს ვიდეო ვნახე, გამიკვირდა, ნუთუ პატრიარქმა ეს მართლა თქვა-მეთქი? ეს არ არის უნებლიე შეცდომა, რაც შეიძლება ნებისმიერ ჟურნალისტს მოუვიდეს, ეს არის პროვოკაცია, ანუ ფეიკ-ნიუსი, ყალბი ამბავი, რომლის მიზანიც არის საზოგადოებაში არეულობის შეტანა, ნიჰილიზმის დათესვა, უიმედობის ჩანერგვა და ასე შემდეგ. დღეს მსოფლიოსთვის ყველაზე დიდი საშიშროებაა ტერორიზმი, კიბერომი, საინფორმაციო ომი და გაჩნდა ამოუცნობი საფრთხე - პანდემია. როგორ შეიძლება განვითარდეს მოვლენები? ამ შემთხვევაში კიბერთავდასხმები შეიძლება განვითარდეს ორი მიმართულებით: პირველი - დამოუკიდებლად, როგორც იყო პანდემიამდე, მეორე - უკვე ამ პრობლემაზე მორგებული, რომელსაც შეუძლია, მოშალოს სახელმწიფო სისტემები და თვით სახელმწიფოც. დღეს უკვე შესაძლებელია, პანდემია დამხმარე ძალაც კი იყოს კიბერთავდასხმის დროს, ან პირიქით, კიბერთავდასხმა იყოს პანდემიისთვის ხელშემწყობი. კიბერთავდასხმის დროს ხდება ორი რამ, ითიშება სახელმწიფო ინსტიტუტები და ვრცელდება დეზინფორმაცია. დაუკვირდით, საომარი მოქმედებების დროს არის საბრძოლო ქვედანაყოფი, უზრუნველყოფის ქვედანაყოფი, პირველს მეორის გარეშე არ შეუძლია ნორმალური ფუნქციონირება, ეს არის დამხმარე ძალა. არის პანდემია და ამას ემატება კიბერთავდასხმა გარკვეული მიზნებისთვის, ფაქტობრივად ორ ფრონტს გიხსნიან. მაგალითად ავიღოთ ბრიტანული გამოცემის - „დეილი მეილის“ მიერ გამოქვეყნებული სტატია, სადაც დიდი სიყალბე წერია: თურმე, ჰაკერები, რომლებმაც ბრიტანეთის სამედიცინო ცდების ჩანაწერები მოიპარეს, საქართველოში არიან ბაზირებული და რუსეთის უსაფრთხოების სამსახურებთან არიან დაკავშირებული. მართალია, **ლონდონის ჰამერსმიტის სამედიცინო კვლევის კლინიკურმა დაწესებულებამ (HMR)** აღიარა, რომ პასპორტების, ეროვნული სადაზღვევო ბარათებისა და სავიზო

დოკუმენტების სკანირებული მასალები, ასევე პაციენტების ფოტოები, ჯანმრთელობის კითხვარი და სამედიცინო ისტორიის დოკუმენტები 2020 წლის 14 მარტს მოიპარეს, მაგრამ რა შუაშია აქ საქართველო? ვფიქრობ, აქ უკვე დაკვეთასთან გვაქვს საქმე. შეიძლება სადღაც რაღაცა მოხდა, ჟურნალისტმა ფაქტი დაიჭირა, დაინტერესებული პირებისგან აიღო ფული და რუსებს მიაწება საქართველოც, შექმნა ყალბი სკანდალი, მაგრამ ყველა ხომ ვერ მიხვდა, რომ ყალბია? გარდა ამისა, ჩვენს ქვეყანაშია ცოტა უცნაური მიდგომა - თუ უცხოურმა გაზეთმა დაბეჭდა, სრული სიმართეა, თუ უცხოელმა პოლიტიკოსმა რამე თქვა, აუცილებლად ჭკვიანურია და ასე შემდეგ. ამ სტატიაში მითითებულია, რომ საქართველოს ხელისუფლება ჩართულია რუსულ თამაშში, ის ვერ აკონტროლებს პანდემიას. ფაქტობრივად, ბრიტანულმა გამოცემამ თქვა ის, რასაც ლაპარაკობს ოპოზიცია, რა სიცრუესაც ავრცელებს ოპოზიცია. არადა, ეს ის ადამიანები არიან, რომლებსაც სურდათ არეულობა და მეტი მსხვერპლი თავიანთი პოლიტიკური მიზნებისთვის“.

რა არის საჭირო იმისთვის, რომ ვირტუალური სივრცე უფრო უსაფრთხო გახდეს?

„ჩვენ აუცილებლად უნდა ავითვისოთ, გავიზიაროთ და დავნერგოთ საერთაშორისო გამოცდილება, საერთაშორისო მიღწევები და სტანდარტები. სხვა გამოსავალი უბრალოდ არ არსებობს. სამწუხაროდ, გვიწევს ფიქრი იმაზე, თუ როგორ გავუწიოთ წინააღმდეგობა რუსეთს, მის პოლიტიკას, პროპაგანდას და აგრესიას. რუსეთის ხელისუფლების მიზანია, საკუთარი ქვეყანა ისევ დააბრუნონ იმ რელსებზე, რომელზეც იყო საბჭოთა კავშირი. რუსეთი საამისოდ იყენებს ყველა ხერხს, მათ შორის კიბერომს, კიბერთავდასხმებს, ჰაკერულ ჯგუფებს, საინფორმაციო ომს და ასე შემდეგ“.

რა როლს ასრულებს რუსეთი კიბერომის თვალსაზრისით და არის თუ არა წამყვანი სახელმწიფო ამ კუთხით?

„რუსეთი არ ებრძვის მხოლოდ საქართველოს, ის ებრძვის თითქმის მთელ მსოფლიოს. როდესაც ნატო-ს ეგიდით გამართულ კონფერენციებს ვესწრებოდი წლების წინ, იქ იყო ხოლმე საუბარი ჩინეთიდან მომდინარე საფრთხეებზე. მაშინ მეცინებოდა, ჩინეთიდან რა საფრთხეები უნდა წამოვიდეს-მეთქი? თუმცა აღმოჩნდა, რომ ყველაფერი წინასწარ იყო შესწავლილი და გათვლილი. ჩვენ რუსეთის მხრიდან დღეს წავაწყდით პრობლემებს, თორემ ასეთი გეგმები არ მუშავდება სპონტანურად, ამას სჭირდება ათეული წლები. რუსეთის მთავარი მიზანი არის გავლენის აღდგენა პოსტსაბჭოთა სივრცეში და აღმოსავლეთ ევროპაში, მას სჭირდება სიძლიერის აღიარება დასავლეთისა და აშშ-ის მხრიდან. მიუხედავად იმისა, რომ საერთაშორისო შეხვედრების დროს რუსეთის წარმომადგენლებს კეთროვნებივით უყურებენ და ამ ეტაპზე „დიდ შვიდეულშიც“ არ აბრუნებენ, ეს იმას არ ნიშნავს, რომ ამ სახელმწიფოს ხელისუფლებას არ ელაპარაკებიან. თუნდაც თურქეთის მაგალითზე ვთქვათ, ზოგს ჰგონია, ერდოღანმა ჩამოგდებული თვითმფრინავის გამო უხადა ბოდიშები და შეეშინდა, დღეს ყველა ფიქრობს ეკონომიკურ სარგებელზე, გავლენაზე და ასე შემდეგ“.

არის თუ არა საქართველო მნიშვნელოვანი ამ ომში გეოსტრატეგიული თვალსაზრისით და რა არის საჭირო, რომ უფრო დაცულ სახელმწიფოდ გარდავიქმნათ?

„ჩვენ მუდმივად ვამბობთ, რომ ამერიკის შეერთებული შტატები არის სტრატეგიული პარტნიორი. ჩვენ სუპერ-სახელმწიფოს იმაზე კი არ უნდა ვაწუხებდეთ, რა სისტემით ჩავატაროთ არჩევნები, ან რამდენი დეპუტატი უნდა გვყავდეს პარლამენტში . ეს იმდენად წვრილმანი საკითხებია, არც კი უნდა ვკადრულობდეთ, გიგი უგულავა გარეთ იქნება თუ ციხეში იჯდება, ეს არ არის მთავარი თემა. ჩვენ უფრო დიდი საფრთხეების წინაშე ვდგავართ, უფრო დიდი გეგმები გვაქვს, ტერიტორიების 20 პროცენტი ოკუპირებულია, ტერორიზმის საკითხები მისახედია, უსაფრთხოების თემა მოსაგვარებელია. რა თქმა უნდა, ამ საკითხებზე მუშაობს ხელისუფლება,

მაგრამ დრო ფუჭად იხარჯება. მაგალითად, გამოდის აშშ-ის ელჩი საქართველოში და აცხადებს, ოპოზიციისა და ხელისუფლების წარმომადგენლები უნდა დასხდნენ მოლაპარაკების მაგიდასთანო. დრო, ნერვები, ფული, ენერგია იხარჯება ასეთ საკითხებზე, როცა გასაძლიერებელი გვაქვს ინფრასტრუქტურა, გასაძლიერებელი გვაქვს სისტემები. ერთი შემთხვევა მახსენდება: ამერიკელებს აქვთ პროგრამა, რომლის თანახმადაც ჩვენი კურსანტები გადიან სამხედრო მომზადებას. ერთ-ერთი არის საპარაშუტო მომზადება. თავის დროზე უარი ვთქვი ასეთი კურსების დანერგვაზე და კინაღამ გადამიყოლეს. რატომ ვთქვი უარი? კი, მაგარი პროგრამაა, მშვენიერი, საჭირო, მაგრამ არ გვქონდა გადმოსახტომი ზონები, ქუთაისში რომ კაცი გადმომხტარიყო პარაშუტით, ზესტაფონში ხედავდნენ. აი, ასეთი საკითხების მოგვარებაზე უნდა იხარჯებოდეს დრო, ფული და ენერგია, ჩვენ გვჭირდება ახალი ტექნოლოგიების ათვისება, სწავლება, ხალხის გაწვრთნა, ამ ტექნოლოგიების დანერგვა და ასე შემდეგ“.

შესაძლებელია თუ არა კიბერომის შეჩერება და ლიკვიდაცია ტექნოლოგიური მიღწევებით? - როგორი მდგომარეობაა ამ მხრივ საქართველოში? გასაგებია, რომ გვეხმარებიან, არსებობს საერთაშორისო სტანდარტები, რეკომენდაციები, თანამშრომლობის მემორანდუმები, მაგრამ ჩვენ თვითონ რა შეგვიძლია?

„დღეს ტექნოლოგიები ისეთი სისწრაფით ვითარდება, ოდნავი მოდუნება და მორჩა, შეიძლება კატასტროფის წინაშე დადგე. ვინაიდან, ეს არის ომის ერთ-ერთი სახეობა და შეიარაღების თანმდევი ინსტრუმენტი, ამ ომის შეჩერება შესაძლებელია მხოლოდ მოლაპარაკებით, სხვანაირად მშვიდობა არ იქნება. თუ არ დაისახა ერთობლივი გეგმები, წინაარმდეგობის გაწევა და ეფექტური შედეგების მიღება გაჭირდება. მაგალითად, სანამ ბრიტანეთმა, საბჭოთა კავშირმა და აშშ-მ მეორე მსოფლიო ომის დროს ერთობლივი გეგმა არ შეიმუშავეს, ფაშიზმის დამარცხება ვერ მოხერხდა. ყველა სფეროში ასეა, ერთობლივი ბრძოლა ყოველთვის ეფექტურია“.

ბოლო რამდენიმე წლის განმავლობაში აშკარად გამოიკვეთა სოციოლოგიური ომის ნიშნები. მაგალითად, არჩევნების წინა პერიოდში ხშირად ხდება ქართული საზოგადოების მანიპულირება-მოტყუება და შეცდომაში შეყვანა ავტორიტეტული თუ არაავტორიტეტული კვლევითი ორგანიზაციების მიერ.

რამდენად კვალიფიციურად ატარებენ ეროვნულ-დემოკრატიული ინსტიტუტი (NDI) და საერთაშორისო რესპუბლიკური ინსტიტუტი (IRI) კვლევებს პოლიტიკური პარტიების რეიტინგების შესახებ და რამდენად მაღალია საზოგადოების ნდობის ხარისხი ამ ორგანიზაციის მუშაობის მიმართ? სამწუხაროდ, ეს თემა ჯერაც მსჯელობის საგანია და ამ ორგანიზაციების მოღვაწეობა კრიტიკას ვერ უძლებს.

ზურაბ ბიგვავა

(ინტერვიუ ჩაწერილია 2020 წლის, 25 მაისს.)

საკვლევ-საკონსულტაციო ცენტრ „ფსიქოპროექტის“ დამფუძნებელი და დირექტორი, ფსიქოლოგიის მეცნიერებათა დოქტორი, სოციოლოგი პასუხობს ჩვენს შეკითხვებს:

საქართველოში, წლების განმავლობაში მიმდინარეობს თუ არა სოციოლოგიური ომი?

„ჩვეულებრივ სიტუაციაში სოციოლოგია არის მეცნიერება, რომელსაც გააჩნია თავისი მათემატიკური აპარატი - თუ მეთოდოლოგია არის სწორი, კვლევის მონაცემებიც იქნება სწორი. ყველა კვლევას აქვს ვალიდობა, ანუ სანდოობა, რომელიც უნდა იყოს მაღალი. რაც შეეხება ტერმინ „სოციოლოგიურ ომს“, ჩვენ შეიძლება განვიხილოთ ასეთი სიტუაცია: დავუშვათ, ერთი ან მეორე მხარე ცდილობს, გვერდი აუაროს ზუსტ მეთოდოლოგიას, რათა გავლენა მოახდინოს არჩევნებზე, ეს უკვე არაკვალიფიციური მიდგომაა კერძო ინტერესების გამო, ეს არის მიზანმიმართული კამპანია და რასაკვირველია, სოციოლოგიასთან არანაირი კავშირი არ გააჩნია. ამ ყველაფერს აქვს მეორე შრეც - მაგალითად,

მე შემიძლია, ნებისმიერი მეთოდოლოგიით, ნებისმიერი გათვლებით ჩავატარო კვლევა და ისეთი საკითხები დავაყენო დღის წესრიგში, რომლის შედეგები წინასწარ ვიცი და ეს გავასაღო კვლევის შედეგად, რომელსაც შეუძლია, ირიბად, რელევანტურად ან პირდაპირ მოახდინოს გავლენა არჩევნებზე. სოციოლოგიური მეთოდოლოგიის ერთ-ერთი უპირველესი მოთხოვნაა, კითხვა არ უნდა იყოს ზემოქმედების მომხდენი, არ უნდა იყოს წარმმართველი, მაგრამ მე შემიძლია, ისეთი კითხვა დავსვა, უკვე ვიცი, რა პასუხსაც მივიღებ. მაგალითად, თუ ბაზრობაზე ადამიანს ვკითხავ: რას შვრებით, როგორია თქვენი მოგება? 100-დან 90 მოგცემს გაზეპირებულ პასუხს - რათქმა უნდა, არა, შემოსავალი არ მაქვს, სახელმწიფო ბევრს მახდევინებს და ასე შემდეგ. არადა, თუ მოგება არ აქვს, არ იმუშავებს. სოციოლოგიური ომი არის, როცა ყველაფერი გადადის პოლიტიკურ ჭრილში და მხარეები იყენებენ ყალბ მონაცემებს“.

რა მოაქვს სოციოლოგიური კვლევებისას ყალბი შედეგების გავრცელებას და არის თუ არა ეს საინფორმაციო ომის ერთ-ერთი შემადგენელი ნაწილი?

„მაგალითად, „ლეიბორისტებმა“ ჩაატარეს კვლევა, გამოკითხეს დაახლოებით 500 ადამიანი. ეს იყო პირდაპირი გამოკითხვა, მეტროსთან დადგნენ და ხალხს უსვამდნენ კითხვებს. აღმოჩნდა, რომ „ლეიბორისტებს“ რეიტინგი ჰქონდათ 55%. ამ პარტიას ასეთი რეიტინგი არასოდეს ჰქონია თავისი ისტორიის განმავლობაში, რეალობა სხვანაირია. გამოაცხადეს, უახლოეს არჩევნებში ჩვენ ვიმარჯვებთო. აი, ეს არის ყალბი შედეგი. სხვათა შორის, პოლიტიკურ პარტიებს ხშირად ახასიათებთ ასეთ რაღაცაზე წასვლა. ასეთი ყალბი კვლევები ძირითადად ისევ განკუთვნილია თავიანთივე მომხრეებისთვის, რომ შეუძახონ: აი, ჩვენ მაღალი რეიტინგი გვაქვს, ვიმარჯვებთ, გული არ გაიტეხოთ. სამწუხაროდ, ამ გაუგებრობაში ხშირად ეხვევიან ის კომპანიები, ორგანიზაციები, რომლებიც წესით პროფესიონალურ დონეზე უნდა მუშაობდნენ“.

რა არის სოციოლოგიური მანიპულაცია, გულუბრყვილო ადამიანებზე გათვლილი ინფორმაცია? კი, მაგრამ 2011 წლიდან მოყოლებული, მიზანს

მაინც ვერ აღწევენ. რატომ ფლანგავენ ამდენ დროს, ფულსა და ნერვებს თუნდაც ცნობილი „აირაი“ და „ენდიაი“?

„ერთია გამოკითხვის ემოციური ფონი და მეორეა - როგორ უნდა დაისვას კითხვა. თუ ადამიანს ვკითხავთ ასე: როგორ ფიქრობთ, დავით ბაქრაძე იქნება თუ არა ქვეყნის ეფექტური მმართველი? ამ შემთხვევაში რეიტინგი ექნებოდა გაცილებით დაბალი.

თუ კითხვა იქნება ასეთი: როგორ ფიქრობთ, დავით ბაქრაძე არის თქვენთვის მისაღები პოლიტიკური ფიგურა? ამ შემთხვევაში შეიძლება მევრმა უპასუხოს, რომ მისაღებია, რას აშავებს? მოგწონთ თუ არა ესა და ეს პოლიტიკოსი? ეს კითხვა ემოციაზეა გათვლილი. განწყობის თეორიას გააჩნია სამი კომპონენტი - ემოციური, ქცევითი და ინტელექტუალური. ამ სამი კომპონენტის გამოყენებით, შეიძლება ერთ ადამიანს ერთ შემთხვევაში ჰქონდეს სხვა რეიტინგი, მეორე შემთხვევაში - მეორე რეიტინგი. მაგალითად, ედუარდ შევარდნაძეს დადებითი რეიტინგიც ჰქონდა მაღალი და უარყოფითიც - მაღალი. თავის დროზე ასეთივე რეიტინგი ჰქონდა, მაგალითად, ირინა სარიშვილს. აქ უცნაური არაფერია, თუ სიტუაცია პოლიტიზებულია, ძლიერ ადამიანებს ყოველთვის აქვთ ორი სახის რეიტინგი, რადგან ისინი ყოველთვის ებრძვიან ვიღაცას. საქართველოში არიან ადამიანები, რომლებსაც მხოლოდ დადებითი რეიტინგები აქვთ, ისინი არავის არ ებრძვიან. ეს ლოგიკური პროცესია“.

რა უნდა დაუპირისპიროს ხელისუფლებამ ყალბი კვლევებისა და ე.წ. გამოკითხვების კამპანიას? თქვენ იტყვით, რომ სიმართლე უნდა დაუპირისპიროს, მაგრამ ისინი უფრო მობილიზებულნი არიან. ისინი ქმნიან ისეთ სინამდვილეს, როგორიც თვითონ აწყობთ და მაგალითად, „აირაის“ და „ენდიაის“ რაში აწყობთ ყალბი სინამდვილე, ანუ ილუზია?

„სიყალბეს უნდა დაუპირისპირდეს ობიექტურობა. თუმცა ამისთვის საჭიროა მოდელი, როგორიც არსებობს ამერიკის შეერთებულ შტატებში. „ენდიაი“ და „აირაი“ სერიოზული ორგანიზაციებია, მათი დაფინანსება

თითქმის განუსაზღვრელია. თუ ისინი არ ჩაატარებენ რეალურ კვლევებს და ადგილი ექნება მანიპულაციების მცდელობას, ბუნებრივია, ხელისუფლებამ ამას უნდა დაუპირისპიროს ობიექტურობა. ამ ორი ორგანიზაციის მიერ ჩატარებული კვლევები ზოგ შემთხვევაში მართლაც არის ყალბი. მაგალითად, ერთ-ერთ კვლევაში იყო ასეთი მომენტი - ადამიანებს ეკითხებოდნენ, უჭერდნენ თუ არა მხარს ბიძინა ივანიშვილს? „ქართული ოცნების“ ლიდერს ამ გამოკითხვის შედეგად ჰქონდა 17%. ამავე კვლევაში იყო ასეთი კითხვა: ბიძინა ივანიშვილმა ქუჩაში გამოსვლისკენ რომ მოგიწოდოთ, გახვალთ? 57-მა პროცენტმა განაცხადა, რომ მის მხარდასაჭერად ქუჩაში გავა. აქედან ანალიზის გაკეთება არის ძალიან მნიშვნელოვანი - არ შეიძლება, გამოიტანო დასკვნა, რომ ბიძინა ივანიშვილს აქვს დაბალი რეიტინგი. ერთია, მოგწონს თუ არა, მაგრამ როცა ადამიანის გამო ქუჩაში გადიხარ, როცა რისკავ, ფაქტობრივად ბრძოლაში ებმები, მისი პოლიტიკური წონა 17%-ზე გაცილებით მეტია“.

რამდენად არის დახვეწილი ჩვენი კანონმდებლობა ამ კუთხით?

„იყო ინიციატივა, რომ საქართველოში გაერთიანებულიყო ძლიერი კვლევითი ორგანიზაციები, რომლებიც ობიექტურობით შეეწინააღმდეგებოდნენ სიყალბეს, მაგრამ ბოლოს ისე მოხდა, რომ ამ ინიციატივას არავინ არ დაუჭირა მხარი. მაგალითად, აშშ-ში არსებობს 200-მდე ასოციაცია, რომლებიც იძლევიან ლიცენზიებს და მერე სიტუაციასაც აკონტროლებენ. ძალიან დიდი ავტორიტეტი აქვთ ასეთ ასოციაციებს. ჩვენთან ასეთი არაფერი არსებობს, რაც არ უნდა კარგი კვლევა ჩაატარო, მეორე მხარე იტყვის, ამისი არ მჯერაო, დაკვეთაა, ვინც აფინანსებს, ის ზეწოლას ანხორციელებსო და ასე შემდეგ. თუნდაც ასეთი მსჯელობა არის საინფორმაციო ომის ერთ-ერთი შემადგენელი ნაწილი. რა თქმა უნდა, ჩვენში ყველაფერი ხდება, მაგაზე უკვე ვთქვი, ბევრი სიყალბე მოდის ამ კუთხით, მაგრამ კარგისა და ავის გარჩევა რაღაც დონეზე მაინც უნდა ხდებოდეს“.

ნიკა ჩიტაძე

(ინტერვიუ ჩაწერილია 2020 წლის, 29 მაისს.)

პოლიტოლოგი და ექსპერტი, საერთაშორისო და უსაფრთხოების საკითხებში, განმარტავს - კიბერომი არის ერთ-ერთი სერიოზული საფრთხე კაცობრიობისთვის. საქმე იქამდეც კი მივიდა, რომ უკვე სახელმწიფოები აწარმოებენ ერთმანეთის წინააღმდეგ ე.წ. საინფორმაციო ომს და კიბერთავდასხმებს.

რამდენად დიდი საფრთხეა დღევანდელი მსოფლიოსთვის კიბერთავდასხმები, საინფორმაციო ომი და ე.წ. ფეიკ-ნიუსი, როგორც მოვლენა? როგორ შეაფასებთ ამჟამინდელ მდგომარეობას?

„კიბერომში მხოლოდ სახელმწიფოები არ მონაწილეობენ, გამოჩნდებიან ხოლმე ავტორიტეტები. როგორც ყველა შემთხვევაში, კიბერომის განხილვისას გვერდს ვერ ავუვლით რუსეთის ფაქტორს, რომელიც საქართველოსთვის კარგადაა ცნობილი. რუსეთის მიერ წარმოებულ კიბერთავდასხმებს საქართველოზე, ამას საკმაო ისტორია აქვს, ეს ჯერ კიდევ 2008 წლის ომამდე დაიწყო, როცა დააზიანეს საქართველოს პრეზიდენტის ვებგვერდი. შემდეგ რაც ომის პერიოდში მოხდა, ეს ყველამ ნახა. ჩემი ინფორმაციით, არსებობს 5 ათასამდე ვებგვერდი, რომლითაც ტერორისტები სარგებლობენ. მაშინ, როცა მსოფლიო მოსახლეობის 50 პროცენტს ხელი მიუწვდება ინტერნეტზე, რასაკვირველია, ეს უკვე დიდი საშიშროებაა“.

შესაძლებელია თუ არა კიბერომის შეჩერება და ლიკვიდაცია ტექნოლოგიური მიღწევებით? - როგორი მდგომარეობაა ამ მხრივ საქართველოში? გასაგებია, რომ გვეხმარებიან, არსებობს საერთაშორისო სტანდარტები, რეკომენდაციები, თანამშრომლობის მემორანდუმები, მაგრამ ჩვენ თვითონ რა შეგვიძლია?

„ინტერნეტსივრცის ბოლომდე გაკონტროლება შეუძლებელია. თუმცა არსებობს მეთოდები, რომლის გამოყენებისას, შესაძლებელია, შედარებით

განეიტრალდეს მსოფლიო დონის მავნებლობა. ინტერნეტსივრცე შედარებით უსაფრთხო რომ გახდეს, ჩემი აზრით, საჭიროა თავდაცვითი პროგრამების შემუშავება ნატოს სისტემების ფარგლებში. კიბერთავდაცვა უნდა ავიდეს კოლექტიური თავდაცვის დონემდე და იგივე მე-5 მუხლი უნდა შეეხოს კიბერსივრცეს. შეიძლება ეს კეთდება კიდეც, მაგრამ უფრო გასაძლიერებელია. ამ შემთხვევაში არ აქვს მნიშვნელობა, რომელ ქვეყანაზე განხორციელდება კიბერთავდასხმა. აქტიურობა გამოიხატება ინფორმაციის გაცვლაში, თავდაცვითი სისტემების დანერგვაში და ასე შემდეგ. მხოლოდ ამ შემთხვევაშია შესაძლებელი, მსოფლიო წინ აღუდგეს კიბერთავდასხმებს. რაც ამჟამად კეთდება, ეს არ არის საკმარისი, აშშ-ის თავდაცვის დეპარტამენტის ვებ-გვერდიც კი რამოდენიმეჯერ დააზიანეს. როცა ასეთი მნიშვნელოვანი დეპარტამენტიც არ არის ბოლომდე დაცული, ეს იმაზე მიანიშნებს, რამდენად მოწყვლადია კიბერსივრცე“.

დადგა თუ არა დრო, შეიქმნას კიბერუსაფრთხოების მსოფლიო ცენტრი, რომელიც გლობალური თვალსაზრისით გააკონტროლებს მიმდინარე მოვლენებს და დასახავს გეგმებს. როგორ წარმოგიდგენიათ ასეთი ცენტრის შექმნა?

„შესაძლებელია, შეიქმნას რამდენიმე საერთაშორისო ორგანიზაცია, რომლებიც პირდაპირ იმუშავებენ ამ საკითხებზე. ჩემი აზრით, ეს აუცილებელია, უნდა შეიქმნას სპეციალური ორგანიზაციები ნატოს ფარგლებში ცალკე, ევროკავშირის ფარგლებში ცალკე. არსებობს ორგანიზაციები ეკონომიკის მიმართულებით, ფინანსების მიმართულებით, ინტელექტუალური საკუთრების მიმართულებით, არსებობს საზღვაო სფეროში, საავიაციო სფეროში და ამ დროს არ არსებობს კიბერსფეროში“.

არის თუ არა საქართველო მნიშვნელოვანი ამ ომში გეოსტრატეგიული თვალსაზრისით და რა არის საჭირო, რომ უფრო დაცულ სახელმწიფოდ გარდავიქმნათ?

„საქართველოში ამ მხრივ მიდის მუშაობა - თავდაცვის სამინისტროში შეიქმნა კიბერუსაფრთხოების ბიურო. არის სხვა ოფისებიც, მაგრამ ეს არ არის საკმარისი. აქ კიდევ ერთი მნიშვნელოვანი პრობლემაა - კიბერუსაფრთხოების ერთ-ერთი მიმართულება არის საინფორმაციო ომი, მაგალითად ავიღოთ ლუგარის ლაბორატორია, რომლის შესახებაც არაერთხელ გავრცელდა ყალბი ინფორმაცია, საქართველო ყოველთვის იკავებს თავის მართლების პოზიციას და კეთდება განცხადებები, თუ უნდათ, რუსი ექსპერტები ჩამოვიდნენ, ადგილზე გაეცნონ ვითარებას და ასე შემდეგ. ამ შემთხვევაში საინფორმაციო ომი წაგებული გვაქვს. ჩვენ ვართ თავდაცვით რეჟიმში და რატომღაც ვამტკიცებთ უდანაშაულობას. არადა, რუსეთის პასუხისმგებლობის საკითხი საერთოდ არ დგება, როდესაც ასეთი სახის დეზინფორმაციას ავრცელებენ. მეორე მაგალითი: 2019 წლის ივლისში ვლადიმერ პუტინმა ინტერვიუ მისცა უცხოურ და რუსულ მედიას, ილაპარაკა საქართველოზე, ცხინვალზე, აფხაზეთზე, როგორ ეწეოდა ქართველი ხალხი ოსებისა და აფხაზების გენოციდს. აი, ეს არის საინფორმაციო ომის ერთ-ერთი შემადგენელი ნაწილი - რუსეთი აქეთ გვადანაშაულებს, რათა საერთაშორისო საზოგადოების წინაშე მოგვიწიოს თავის მართლება. არც ამ შემთხვევაში იყო სათანადო პასუხი ჩვენი მხრიდან. მე უკვე მაქვს პასუხი მზად და მინდა, უცხოეთში გამოვცე, რათა ჩვენი ისტორიული სამართლიანობა დავამტკიცოთ. სამწუხაროდ, საქართველო საინფორმაციო ომის კუთხით ხშირად აგებს. თუნდაც 2008 წლის ომის მაგალითზე ვიმსჯელოთ, აქაც თავის მართლების რეჟიმში ვართ, რომ ომი ჩვენ არ დაგვიწყია. არსებობს საერთაშორისო კონვენციები, ომი იყო საქართველოს ტერიტორიაზე, ფაქტია, რომ რუსეთი შემოვიდა. რა თქმა უნდა, რუსეთს სამხედრო თვალსაზრისით ვერ დაამარცხებ, მაგრამ არსებობს სამართლებრივი ბერკეტები და არსებობს საინფორმაციო ველი, სადაც შეგვიძლია, მოვიგოთ“.

შეჯამება:

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.

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.

ბიბლიოგრაფია

1. ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., "კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016.
2. "ნატო-ს ვარშავის სამიტის დეკლარაციის მოკლე მიმოხილვა (გავლენა საქართველოზე)", თბილისი: საქართველოს უსაფრთხოების და განვითარების ცენტრი, 2014.
3. "საქართველოს ეროვნული უსაფრთხოების კონცეფცია", თბილისი: საქართველოს მთავრობა, 2018.
4. ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., "მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო", ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018.
5. ჭყოიძე ნ., ტომარაძე გ., "ვირტუალური/კრიპტოგრაფიული ვალუტა და მისი თავისებურებები ვირტუალური ვალუტების რეგულირება (bitcoin-ის მაგალითზე)", თბილისი: გამოცემა "ეკონომიკა და საბანკო საქმე", 2014.
6. Arquilla J., Ronfeldt D., Swarming and the Future of Conflic, Santa Monica: RAND National Defense Research Institute, 2000.
7. Abolhassan F. Cyber Security. Simply. Make it Happen, Bonn: Telekom Deutschland GmbH, 2017.
8. Andress J., Winterfeld S., Abron L., Cyber Warfare (Techniques, Tactics and Tools for Security Practitioners), United States: Publisher Elsevier, 2014.
9. Bazyler J. M., Tuerkheimer M. F., Forgotten Trials of the Holocaust, United States: NYU Press, 2014.
10. Bayuk L. J., Healey J., Rohmeyer P., Sachs H. M., Schmidt J., Weiss J. Cyber Security Policy Guidebook, Canada: Publishing House Wiley, 2012.
11. Cheng D. Cyber dragon, inside China s information warfare and cyber operations, United States: Publishing House Praeger, 2017.
12. Cohen R., Mihalka M., Cooperative Security: New Horizons for International Order, London: European Center for Security Studies, The Marshall Center Papers, 2001 No.3.
13. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks, London: Publisher European Parliament, 2009.
14. Cleary F., Felici M., Cyber Security and Privacy, Brussels: Springer Nature Singapore Pte Ltd, Communications in Computer and Information Science 530, 4th Cyber Security and Privacy Innovation Forum, 2015.
15. Cleary F., Felici M., Cyber Security and Privacy, Athens: Springer Nature Singapore Pte Ltd, Communications in Computer and Information Science 470, Third Cyber Security and Privacy EU Forum, 2014.
16. Cavelty D. M. Cyber-Security and Threat Politics, London: Publishing House routledge, 2008.

17. Cox A. Hacker's Manual 2016, Palo alto: Journal "Guru Guide", 2016.
18. Clarke A., Knake K. R., Cyber War: The Next Threat to National Security and What to Do About It, United Kingdom: Publisher Ecco, 2010.
19. Edited by Jens Ringsmose and Sten Rynning, NATO's New Strategic Concept: a Comprehensive Assessment, DIIS. Danish Institute for International Studies, Copenhagen: NATO, 2011.
20. Glaser B. Grounded Theory: The Philosophy, Method, and Work, Florida: BrownWalker Press, 2011.
21. Graham J., Howard R., Olson R., Cyber Security Essentials, London: CRC Press, Auerbach Publications Taylor & Francis Group, 2018.
22. Geers K. cyber war in perspective: russian aggression against ukraine, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015.
23. Hadnagy C. Social Enginering: The Art of Human Hacking, Canada: Wiley Publishing. Inc. 2011.
24. Information Security Doctrine of The Russian Federation, Moscow: Russian Federation, 2000.
25. Kenneth J. K. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions, Colorado: U.S. Air Force Academy, 2009.
26. Klipper S. Cyber Security, Deutschland: Publishing House Springer, 2015, 198 p.
27. Kim P. The Hacker Playbook: Practical Guide To Penetration Testing, South Carolina: Publisher: Secure Planet LLC 2014.
28. Lord M. K., Sharp T., America's Cyber Future: Security and Prosperity in the Information Age, United States: Center for a New American Security, 2011.
29. Lindsay R. J. The Impact of China on Cybersecurity, United States: the President and Fellows of Harvard College and the Massachusetts Institute of Technology, 2015.
30. Mike O. Cyber Operations Building, Defending, and Attacking Modern Computer Networks, Marilend: Publishing House Apress, Department of Mathematics, Towson University, 2015.
31. Morgan S. Cybersecurity Ventures - 2017 Cybercrime Report, Canada: Herjavec Group, 2015.
32. Moore A., Edward J. L., Cyber Self-Defense (Expert advice to Avoid Online Predators, Identity Theft, and Cyberbullying), United States: Lyons Press, 2014.
33. Masud M., Khan L., Thuraisingham B. Data Mining Tools for Malware Detection, United states: CRC Press, 2012.
34. National Security Strategy, Washington: Unitet States of America administration, 2017.
35. National Security Strategy of the United States of America, Washington: The White House, 2017.
36. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, America: Bitcoin Organization, 2009.
37. Nakajima S., Toyoshima M., Yu H., Cyber-Physical System Design from an Architecture Analysis Viewpoint, Singapore: Springer Nature Singapore Pte Ltd, 2017.

38. Nato Summit in Warsaw, Warsaw: Polish 20 economic magazine Market, 2017.
39. Popescu N., Secrieru S., Hacks, leaks and disruptions Russian cyber strategies, Paris: European Union Institute for Security Studies, 2018, Chaillot paper №148.
40. Perry B. Gray Hat C# A Hacker's Guide to Creating and Automating Security Tools, San Francisco: Publishing House No Sach Press, , 2017.
41. Rösch J. F. Hans J. Morgenthau, the "marginal man" in International Relations. A "Weltanschauungsanalyse", United Kingdom: Newcastle University School of Geography, Politics and Sociology, 2011.
42. Russian National Security Strategy, Moscow: Russian Federation, 2015, No. 683.
43. Richards J. Cyber-War: The Anatomy of the Global Security Threat, United States: Palgarave Macmillan, 2014.
44. Senese D. P., Vasquez A. J., The Steps to War: An Empirical Study, United States: Princeton University Press, 2018.
45. Schneier B. Psychology and Usability - Only amateurs attack machines; professionals target people, London: University of Cambridge, Department of Computer Science and Technology The Computer Laboratory, 2017, Chapter 3.
46. Touhill J, G., Touhill C. J., Cybersecurity for Executives (A Practical Guide), Canada: Publishing House Wiley, the American Institute of Chemical Engineers, Inc. 2014.
47. Uma M., Padmavathi G., A Survey on Various Cyber Attacks and Their Classification, Coimbatore: Department of Computer Science, Avinashilingam Deemed University for Women, 2011.
48. Valeriano B., Maness C. R., Cyber War versus Cyber Realities, New York: Oxford University Press, 2015.
49. Voller G. J. Cyber Security, Canada: Publishing House Wiley, 2014.
50. Willson D. Cyber Security Awareness for CEOs and Management, United States: Publishing House Elsevier, 2016.
51. Zubairi A. J., Mahboob A., Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies, United States: Information Science Reference an imprint of IGI Global, 2012, 336 p.

<u>ინტერნეტ წყაროები:</u>

52) აბულაშვილი ი. "პირველი ელექტროგამომთვლელი მანქანის გამომგონებელი ქართველი", გაზეთი „რეზონანსი", 2017, http://www.resonancedaily.com, უკანასკნელად იქნა გადამოწმებული - 03.07.2020.
53) "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", ამერიკის შეერთებული შტატების საელჩო საქართველოში, 2017, https://ge.usembassy.gov, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.
54) ახალაია ლ. "ირანმა აშშ-ის სამხედრო ძალები „ტერორისტულ ორგანიზაციად" გამოაცხადა", საქართველოს საზოგადოებრივი მაუწყებელი, 2020, https://1tv.ge, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.
55) ბასილაია ე. "გერმანული მედია: რუსები 2008 წელს ბირთვული იარაღის გამოყენებას აპირებდნენ". გაზეთი "რეზონანსი", 2017,

http://www.resonancedaily.com, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.

56) გოგუაძე მ. "მომავლის ვალუტა ბიტკოინი – კრიპტოვალუტა", სესხების შემდარებელი კომპანია „ფინანსერი“, 2017, https://financer.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.
57) გეგიძე თ. "როგორ მოვიგერიეთ კიბერთავდასხმა და პროპაგანდა 2008 წელს", სააგენტო "ონ.ჯი", 2019, https://on.ge/, უკანასკნელად იქნა გადამოწმებული - 19.09.2020.
58) გოცირიძე ა. "რუსეთ-საქართველოს 2008 წლის ომის კიბერგანზომილება", საქართველოს სტრატეგიისა და საერთაშორისო უსაფრთხოებების კვლევის ფონდი, 2019, https://www.gfsis.org, უკანასკნელად იქნა გადამოწმებული - 19.09.2020.
59) ვაჩარაძე ა. "რუსეთის საინფორმაციო ომი - სტრატეგიები და მიზნები", სააგენტო "დამოუკიდებლობა", 2015, http://www.damoukidebloba.ge, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.
60) ზედელაშვილი თ. „ჰაკერები კორონავირუსთან დაკავშირებულ შიშებს იყენებენ პირადი მონაცემების მოსაპარად“ - უნდა ველოდოთ მასშტაბურ კიბერშეტევებს", მედიაჰოლდინგი "ჯორჯიან-თაიმსი", 2020, http://geotimes.com.ge, უკანასკნელად იქნა გადამოწმებული - 25.06.2020
61) ზამან ჰ. "Youtub-ზე გავრცელებული ვიდეოს წარმომავლობა გაურკვეველია", საინფორმაციო "ფორ.ჯი", 2013, https://for.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.
62) ზამან ჰ. "თალიბანი საქართველოს შურისძიებით ემუქრება? - შოკისმომგვრელი ვიდეო YouTube-იდან". მედიაჰოლდინგი "პალიტრა", 2013, https://www.palitravideo.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.
63) რუხაძე თ. "ირანის მხრიდან შესაძლოა, აშშ-ზე კიბერთავდასხმა განხორციელდეს", საქართველოს საზოგადოებრივი მაუწყებელი, 2020, https://1tv.ge, უკანასკნელად იქნა გადამოწმებული - 05.01.2020.
64) იაგორაშვილი ი. "რუსეთის 2 მითი ბალტიისპირეთის ქვეყნების შესახებ". ვებ-გვერდი "My the Detector", 2019, https://www.mythdetector.ge, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.
65) იაგორაშვილი ი. "მარია ზახაროვა სსრკ-ის მიერ ესტონეთის ოკუპაციას უარყოფს". ვებ-გვერდი "My the Detector", 2020, https://www.mythdetector.ge, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.
66) კერსანსკასი ვ. "დეზინფორმაციასთან და ყალბ ამბებთან საბრძოლველად მარტივი და სწრაფი გზა არ არსებობს, ეს გრძელვადიანი სტრატეგიაა". საქართველოს საზოგადოებრივი მაუწყებელი, 2019, https://1tv.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020.
67) კუპრეიშვილი თ. "ყველაფერი, რაც ვიცით უკრაინული თვითმფრინავის კატასტროფაზე". საინფორმაციო სააგენტო "ნეტგაზეთი", 2020, https://netgazeti.ge, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.

68) "კიბერუსაფრთხოების ინდექსში საქართველო მე-8 ადგილზეა". საქართველოს იუსტიციის სამინისტრო, 2017, https://imedinews.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020.
69) "კიბერუსაფრთხოების ინდექსით, საქართველო მსოფლიოში მე-19 ადგილზეა". e-governance academy, 2018, https://forbes.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020.
70) "კიბერუსაფრთხოების ინდექსში საქართველო მე-8 ადგილზეა". ტელეკომპანია "იმედი", 2017, https://imedinews.ge, უკანასკნელად იქნა გადამოწმებული: 14.06.2020.
71) "კიბერუსაფრთხოების ინდექსით, საქართველო მსოფლიოში მე-19 ადგილზეა". ტელეკომპანია "იმედი", 2018, https://imedinews.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020.
72) კერსანსკასი ვ. "დეზინფორმაციასთან და ყალბ ამბებთან საბრძოლველად მარტივი და სწრაფი გზა არ არსებობს, ეს გრძელვადიანი სტრატეგიაა". საქართველოს საზოგადოებრივი მაუწყებელი, 2019, https://1tv.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020
73) მაისაია ვ. „ისლამური ხალიფატის“ საინფორმაციო-პროპაგანდისტული/კიბერ-ვირტუალური ომის სპეციფიკა - „რბილი ძალის“ კონცეფტი", მედიაჰოლდინგი "ჯორჯიან-თაიმსი", 2017, http://geotimes.com.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.
74) “სად უყვართ Facebook?", ფორბსი, 2018, https://bm.ge, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.
75) "საქართველოში მცხოვრებ „დაეშის“ შესაძლო მხარდამჭერთა რაოდენობა და გავლენა შემცირდა". საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, 2019, https://imedinews.ge, უკანასკნელად იქნა გადამოწმებული - 14.06.2020.
76) ტრამპი დ. "ნატო-მ ახლო აღმოსავლეთიც უნდა მოიცვას და ახალ ალიანსს დავარქვათ „ნატო+ახლო აღმოსავლეთი“ – რა მშვენიერი სახელწოდებაა, სახელებს კარგად ვიგონებ". საინფორმაციო "ინტერპრესნიუსი", 2020, https://www.interpressnews.ge, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.
77) "ტერორიზმთან ბრძოლა". საქართველოს სახელმწიფო უსაფრთხოების სამსახური, 2015, https://ssg.gov.ge, უკანასკნელად იქნა გადამოწმებული: 15.06.2020.
78) ქაზუმოვი ო. "ძალადობა რელიგიის სახელით და ინტერპრეტაციის მნიშვნელობა". ტოლერანტობისა და მრავალფეროვნების ინსტიტუტი (TDI), 2018, https://www.tdi.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.
79) "შსს-ს სახელით მოქალაქეებს მესიჯები მიუვიდათ - რა განცხადებას ავრცელებს სამინისტრო", საქართველოს შინაგან საქმეთა სამინისტრო, 2020, https://www.ambebi.ge, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.
80) "ჯიჰადი: ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!". საინფორმაციო სააგენტო „ფორ.ჯი“, 2013, https://for.ge, უკანასკნელად იქნა გადამოწმებული - 15.06.2020.

81) Andrews E. The Invention of the Internet, Internet publisher History, 2019, https://www.history.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
82) Ambersariya D. Types of Internet Connections- Wireless, Dial-up, DSL, Fiber, Cable, ISDN, Technology Website Invention Sky, 2019, https://inventionsky.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
83) Burns D. "The five generations of computers", Business to Business Company, 2016, https://btob.co.nz, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
84) Berners-Lee T. A short history of the Web - Where the Web was born, CERN Accelerating science, 2013, https://home.cern, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
85) Brussels Summit Declaration - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, NATO, 2018, https://www.nato.int, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.
86) Brent L. NATO's role in cyberspace, NATO, 2019, https://www.nato.int, უკანასკნელად იქნა გადამოწმებული - 16.06.2020.
87) Coe T, Where does the word cyber come from?, Oxford University Press's Academic Insights for the Thinking World, 2015, https://blog.oup.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
88) Collective defence - Article 5, NATO, 2019, https://www.nato.int ბოლოს იქნა გადამოწმებული - 04,08.2020.
89) Cherry K. History and Key Concepts of Behavioral Psychology, publisher very well mind company, 2019, https://www.verywellmind.com, ბოლოს იქნა გადამოწმებული - 27.08.2020.
90) Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, https://www.mitre.org, ბოლოს იქნა გადამოწმებული - 27.08.2020.
91) Clement J. Number of monthly active Facebook users worldwide as of 2nd quarter 2020, Global No.1 Business Data Platform, 2020, https://www.statista.com, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.
92) Deffere S. 1st computer virus is written, January 30, 1982, Electronics Design Network, 2019, https://www.edn.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
93) Department of Homeland Security Statement on the President's Fiscal Year 2021 Budget, Homeland Security, 2020, https://www.dhs.gov, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.
94) Evansky B. US, UK and Estonia call out Russia over cyber attacks against Georgia in UN Security Council first, Fox News Channel, 2020, https://www.foxnews.com, უკანასკნელად იქნა გადამოწმებული - 07.08.2020.
95) Freiberger A. P., Swaine R. M., Analytical Engine, Encyclopedia Britanica, 2020, https://www.britannica.com, უკანასკნელად იქნა გადამოწმებული - 03.07.2020.

96) Gartzke E. Making Sense of Cyberwar, Harvard Kennedy School Belfer Center for Science and International Affairs, 2014, https://www.belfercenter.org, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.
97) Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, Consulting Agency Gartner, 2018, https://www.gartner.com, უკანასკნელად იქნა გადამოწმებული - 07.08.2020.
98) Hayes A. What Happens to Bitcoin After All 21 Million Are Mined?, Business & Economy Website Investopedia, 2020, https://www.investopedia.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.
99) Inter National Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, The White House, 2011, https://www.hsdl.org, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.
100) Jaffe E. How Highway Construction Helped Hitler Rise to Power, Bloomberg City Lab, 2014, https://www.bloomberg.com, უკანასკნელად იქნა გადამოწმებული - 19.08.2020.
101) Karasev P. NATO's Cyber Defense Evolution - NATO's New Digital Wall, Russian Council RIAC, 2016, https://russiancouncil.ru, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.
102) Kerr D. Obama asks for $14 billion to step up cybersecurity - The president urges Congress to pass legislation that would strengthen the country's hacking detection system and counterintelligence capabilities, Media News CNet, 2015, https://www.cnet.com, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.
103) Karpowicz W. Political Realism in International Relations, Stanford Encyclopedia of Philosophy, 2017, https://plato.stanford.edu, უკანასკნელად იქნა გადამოწმებული - 16.08.2020.
104) Loritz M. Who was Ada Lovelace? The life of the woman who envisioned the modern day computer, Media Website "EU-Startup", 2019, https://www.eu-startups.com, უკანასკნელად იქნა გადამოწმებული - 03.07.2020.
105) Levy S. The Brief History of the ENIAC Computer, Smithsonian Magazine, 2013, https://www.smithsonianmag.com, უკანასკნელად იქნა გადამოწმებული - 04.07.2020.
106) Levy S. Steve Jobs American businessman, Encyclopedia Britanica, 2020, https://www.britannica.com, უკანასკნელად იქნა გადამოწმებული - 04.07.2020.
107) Long T. July 26, 1989: First Indictment Under Computer Fraud Act, Media News Company - Wired, 2011, https://www.wired.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
108) Lohrmann D. How Vulnerable Is Critical Infrastructure to a Cyberattack?, Governament Technology, 2020, https://www.govtech.com, უკანასკნელად იქნა გადამოწმებული: 05.08.2020.
109) Leiden J. The 30-year-old prank that became the first computer virus, Information Technology Company The Register, 2012, https://www.theregister.com, ბოლოს იქნა გადამოწმებული - 09.08.2020.

110) Newman H. L. GitHub Survived the Biggest DDoS Attack Ever Recorded, Media Company Wired, 2018, https://www.wired.com, უკანასკნელად იქნა გადამოწმებული - 16.06.2020.
111) Newman H. L. Coronavirus Sets the Stage for Hacking Mayhem, Media Company Wired, 2020, https://www.wired.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.
112) Perlroth N., Scott M., Frenkel S., Cyberattack Hits Ukraine Then Spreads Internationally, The New York Times, 2017, https://www.nytimes.com, უკანასკნელად იქნა გადამოწმებული: 05.08.2020.
113) Pennetier M. France to invest 1 billion euros to update cyber defences, Media News Reuters, 2014, https://www.reuters.com, უკანასკნელად იქნა გადამოწმებული - 10.08.2020.
114) Person R. 6 reasons not to worry about Russia invading the Baltics, The Washington Post, 2015, https://www.washingtonpost.com, უკანასკნელად იქნა გადამოწმებული - 18.06.2020.
115) Rubens P. Common Types of Ransomware, Internet Website e Security Planet, 2017, https://www.esecurityplanet.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
116) Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict, Information Technology Company ZDnet, 2018, https://www.zdnet.com, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.
117) Riazi T. Know The CCDCOE: Interview with Director Col. Jaak Tarien, NATO Assotiation of Canada - NAOC, 2020, http://natoassociation.ca, უკანასკნელად იქნა გადამოწმებული - 16.06.2020.
118) Rouhani H. Never threaten the Iranian nation: Rouhani tells Trump, Alarabiya, 2020, https://english.alarabiya.net, უკანასკნელად იქნა გადამოწმებული - 06.01.2020.
119) Sciarrone M. Cyber Warfare: The New Front, George W. Bush Institute, 2017, https://www.bushcenter.org, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
120) Sobers R.110 Must-Know Cybersecurity Statistics for 2020, Software Company Varonis, 2020, https://www.varonis.com, უკანასკნელად იქნა გადამოწმებული - 07.08.2020.
121) Szal A. Report: Russian 'Internet Trolls' Behind Louisiana Chemical Explosion Hoax, Industrial Media Manufacturing, 2015, https://www.manufacturing.net, უკანასკნელად იქნა გადამოწმებული - 20.08.2020.
122) Schmidt R. Cyber Quest, Action Impact LLC, 2017, https://www.actionimpact.com, ბოლოს იქნა გადამოწმებული - 27.08.2020.
123) Thurrott P. Windows 98 rockets to 1998 sales of 25 million, News Media IT Pro Today, 1999, https://www.itprotoday.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.

124) Timberg C., Romm T., Hackers are seizing on coronavirus fears to steal data, researchers and U.S. regulators warn", The washingtonpost, 2020, https://washingtonpost.com, უკანასკნელად იქნა გადამოწმებული - 25.06.2020.
125) Trump D. Trump says 'Iran appears to be standing down' following its retaliatory attacks against Iraqi bases housing US troops, CNN, 2020, https://edition.cnn.com, უკანასკნელად იქნა გადამოწმებული - 13.06.2020.
126) Uhde A. A short history of computer viruses, Sentrian Pty Ltd, 2017, https://www.sentrian.com.au, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
127) US Dept of Defense, Statement by the Department of Defense, U.S. Department of Defense (DoD), 2020, https://www.defense.gov, უკანასკნელად იქნა გადამოწმებული - 27.05.2020.
128) Vidisha J. America's Hidden Stories' tackles CIA's alleged involvement in the Trans-Siberian Pipeline explosion of 1982, Media Entertainment Arts WorldWide, 2019, https://meaww.com, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
129) Weber M. october 29, 1969: Happy 40TH Birthday to a Radical Idea!, Computer History Museum, 2009, https://computerhistory.org, უკანასკნელად იქნა გადამოწმებული - 04.08.2020.
130) Waddell K. 'Look, a Bird!' Trolling by Distraction, The Atlantic Magazine, 2017, https://www.theatlantic.com, უკანასკნელად იქნა გადამოწმებული - 21.08.2020.
131) Zamora W. 10 easy ways to prevent malware infection, Software Company Malwarebytes, 2016, https://blog.malwarebytes.com, უკანასკნელად იქნა გადამოწმებული - 05.08.2020.
132) Zengerle P., Megan Cassella M., Millions more Americans hit by government personnel data hack, Media Company Reuters, 2015, https://uk.reuters.com, უკანასკნელად იქნა გადამოწმებული - 25.08.2020.

დანართები

დანართი 1.

<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.

დანართი 2.

კითხვარი

ნაშრომში გამოყენებულია სიღრმისეული ინტერვიუს მეთოდი. ხუთმა ექსპერტმა - **ამირან სალუქვაძემ, ზურაბ ბიგვავამ, ლევან ნიკოლეიშვილმა, ნიკა ჩიტაძემ და ანდრო გოცირიძემ** უპასუხეს შემდეგ კითხვებს:

1. რამდენად დიდი საფრთხეა დღევანდელი მსოფლიოსთვის კიბერთავდასხმები, საინფორმაციო ომი და ე.წ. ფეიკ-ნიუსი, როგორც მოვლენა? როგორ შეაფასებთ ამჟამინდელ მდგომარეობას?
2. რა არის საჭირო იმისთვის, რომ ვირტუალური სივრცე უფრო უსაფრთხო გახდეს?
3. შესაძლებელია თუ არა კიბერომის შეჩერება და ლიკვიდაცია ტექნოლოგიური მიღწევებით? - როგორი მდგომარეობაა ამ მხრივ საქართველოში? გასაგებია, რომ გვეხმარებიან, არსებობს საერთაშორისო სტანდარტები, რეკომენდაციები, თანამშრომლობის მემორანდუმები, მაგრამ ჩვენ თვითონ რა შეგვიძლია?
4. რა როლს ასრულებს რუსეთი კიბერომის თვალსაზრისით და არის თუ არა წამყვანი სახელმწიფო ამ კუთხით?
5. როგორ დავიცვათ თავი რუსული ჰიბრიდული ომისგან და ჰაკერული თავდასხმებისგან?
6. რას შეიძლება მიაღწიოს რუსეთმა პოსტსაბჭოთა ქვეყნებსა და აღმოსავლეთ ევროპაში გამალებული პროპაგანდით თუ უწყვეტი დეზინფორმაციით? ხედავთ თუ არა ამის ნიშნებს?
7. ტერორიზმისა და კიბერტერორიზმის წინააღმდეგ რა ერთობლივი გეგმა უნდა შეიმუშავონ ევროკავშირმა, ამერიკის შეერთებულმა შტატებმა და ნატომ, რათა ბრძოლა უფრო ეფექტური იყოს?
8. ჩინეთი, რუსეთი, ირანის ისლამური რესპუბლიკა - არის თუ არა ეს სამი სახელმწიფო კიბერთავდასხმების მხრივ დანარჩენი მსოფლიოსთვის საშიში?

9. არის თუ არა საქართველო მნიშვნელოვანი ამ ომში გეოსტრატეგიული თვალსაზრისით და რა არის საჭირო, რომ უფრო დაცულ სახელმწიფოდ გარდავიქმნათ?
10. რა შეიცვლება მსოფლიოში და მათ შორის საქართველოში პანდემიის შემდეგ?
11. რას შეცვლის რეალურ ცხოვრებაში "5G"-ის სისტემის დანერგვა?
12. საქართველოში, წლების განმავლობაში მიმდინარეობს თუ არა სოციოლოგიური ომი?
13. რამდენად არის დახვეწილი ჩვენი კანონმდებლობა ამ კუთხით?
14. დადგა თუ არა დრო, შეიქმნას კიბერუსაფრთხოების მსოფლიო ცენტრი, რომელიც გლობალური თვალსაზრისით გააკონტროლებს მიმდინარე მოვლენებს და დასახავს გეგმებს. როგორ წარმოგიდგენიათ ასეთი ცენტრის შექმნა?
15. როგორი ისტორიული პერიოდი უძღვოდა წინ კიბერომის წარმოშობას?

<u>შეკითხვები სოციოლოგიური კვლევების შესახებ</u>

1. რა არის სოციოლოგიური მანიპულაცია, გულუბრყვილო ადამიანებზე გათვლილი ინფორმაცია? კი, მაგრამ 2011 წლიდან მოყოლებული, მიზანს მაინც ვერ აღწევენ. რატომ ფლანგავენ ამდენ დროს, ფულსა და ნერვებს თუნდაც ცნობილი „აირაი" და „ენდიაი"?
2. დავუშვათ, რა აზრი აქვს დავით ბაქრაძის „პირველობას" , როცა რეალობა სხვანაირია?
3. რა უნდა დაუპირისპიროს ხელისუფლებამ ყალბი კვლევებისა და ე.წ. გამოკითხვების კამპანიას? თქვენ იტყვით, რომ სიმართლე უნდა დაუპირისპიროს, მაგრამ ისინი უფრო მობილიზებულნი არიან. ისინი ქმნიან ისეთ სინამდვილეს, როგორიც თვითონ აწყობთ და მაგალითად, „აირაის" და „ენდიაის" რაში აწყობთ ყალბი სინამდვილე, ანუ ილუზია?
4. არის თუ არა ფეიკ-ნიუსი სერიოზული საფრთხე? როგორ უნდა გაუწიოს წინააღმდეგობა საქართველოს ხელისუფლებამ ფეიკ-ტერორს, როცა აშშ-ისა და დასავლეთ ევროპის წამყვან ქვეყნებსაც კი უჭირთ?

ვგულისხმობთ ყალბ საინფორმაციო პროპაგანდას. უნდა იბრძოლოს იგივე მეთოდებით, საკმარისია მხილება თუ სხვა უფრო ეფექტური სტრატეგიაა შესამუშავებელი?