კავკასიის საერთაშორისო უნივერსიტეტის

თორნიკე ზედელაშვილი

კიბერ-ომი როგორც ეროვნული უსაფრთხოების ახალი საფრთხე და პოლიტიკური კონფლიქტის ახალი განსაზღვრება

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: **„კიბერ-ომი, როგორც ეროვნული უსაფრთხოების ახალი საფრთხე და პოლიტიკური კონფლიქტის ახალი განსაზღვრება“** 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, როგორც ეროვნული უსაფრთხოების ახალი საფრთხე და პოლიტიკური კონფლიქტის ახალი განსაზღვრება“**

ფაკულტეტი: სოციალურ მეცნიერებათა

აკადემიური ხარისხი: დოქტორი

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

ავტორის ხელმოწერა

ანოტაცია

ნაშრომში განხილულია კიბერომის არსი, საფუძვლები და წარმომავლობა. კვლევის ძირითად საკითხს წარმოადგენს საინფორმაციო ომი, როგორც ცივი ომის გაგრძელება ტექნოლოგიური მიღწევების ფონზე. გლობალური უსაფრთხოება, ამერიკის შეერთებული შტატების, დასავლეთ ევროპის, აღმოსავლეთ ევროპის, ევროკავშირისა და ნატოს როლი, დღევანდელი რეალობა. საქართველოს გეოსტრატეგიული მდგომარეობა და უსაფრთხოება. ნატო-ს გაფართოება აღმოსავლეთის მიმართულებით. ირანის, ჩინეთისა და რუსეთის მიერ წარმოებული ჰიბრიდული ომები, ჰაკერული თავდასხმები და დაპყრობითი ხასიათის პროპაგანდა.

ვინაიდან, კიბერსივრცე უკვე გადაიქცა უსაზღვრო შესაძლებლობების იარაღად მთელი მსოფლიოსთვის და გახდა როგორც სიკეთის მომტანი, ასევე ბოროტების არეალი ტერორისტებისთვის, კაცობრიობა დადგა უდიდესი საფრთხის წინაშე. კვლევის საგანს ასევე წარმოადგენს, თუ სად არის ამ დროს საქართველო და რა ფუნქცია აკისრია. სახელმწიფო უსაფრთხოების სამსახურის 2018 წლის ანგარიშში ხაზგასმით არის ნათქვამი, რომ "საქართველოში გავლენის გაძლიერებით დაინტერესებული ქვეყნები საკუთარი მიზნების მისაღწევად აქტიურად იყენებენ ჰიბრიდული ომის მეთოდებს".[1] ჰიბრიდული ომის მნიშვნელოვან ინსტრუმენტს წარმოადგენს დეზინფორმაციული კამპანია, ყალბი ახალი ამბები, მცდარი შეხედულებებისა და შიშის დანერგვა, საზოგადოებრივ აზრზე მანიპულირებით მნიშვნელოვან პროცესებზე გავლენის მოხდენა. ნაშრომში წარმოდგენილია როგორც საკუთარი მოსაზრებები, რეკომენდაციები (კვლევებზე დაყრდნობით), ასევე უცხოელი თუ ქართველი ექსპერტებისა და სპეციალისტების მიერ შემუშავებული მოსაზრებები და რეკომენდაციები.

[1] https://1tv.ge/news/sus-saqartveloshi-gavlenis-gadzlierebit-dainteresebuli-qveynebi-hibriduli-omis-metodebs-iyenebdnen-romlis-mnishvnelovan-instruments-dezinformaciuli-kampania-warmoadgenda/, უკანასკნელად იქნა გადამოწმებული: 10.06.2020

ნაშრომი შეიცავს სამ თავს, ექსპერტების დასკვნებს, დისკუსიას და შემთხვევების განხილვას.

პირველი თავი ეთმობა კიბერომის არსს და ისტორიულ მიმოხილვას. მსოფლიო მასშტაბით ტექნოლოგიების განახლება-განვითარება საჭიროა გლობალური უსაფრთხოებისთვის. მათ შორის, მნიშვნელოვანია საქართველოსთვის. საფრთხეების არსებული დონე კიბერსივრცეში ძალიან მაღალია. ყველა ქვეყანა ცდილობს, თავი დაიცვას, მაგრამ რომ არა ევროკავშირისა და ნატო-ს მიერ შემუშავებული პროგრამები, თავდაცვა იქნებოდა ინდივიდუალურ დონეზე და იქნებოდა არაეფექტური.

პირველი თავის პირველ ქვეთავში განხილულია საკითხი, თუ როგორ მიმდინარეობს კონფლიქტების ტრანსფორმაცია ახალი გეოპოლიტიკური წესრიგის პირობებში და რა ღონისძიებები თუ ზომებია მიღებული მსოფლიო მასშტაბით, სხვადასხვა ქვეყნების მიერ.

პირველი თავის მეორე ქვეთავი - კიბერომის თეორია და მისი ადგილი თანამედროვე მსოფლიო პოლიტიკაში. განხილულია, თუ რა კეთდება ევროკავშირისა და ნატო-ს ერთობლივი თანამშრომლობით უსაფრთხო გარემოს შესაქმნელად. ყურადღება ეთმობა ახალი საინფორმაციო სივრცის გლობალურ მნიშვნელობას, მის დადებით და უარყოფით ფაქტორებს. საუბარია საფრთხეებზე, რაც არსებობს კიბერსივრცეში, ამ საფრთხეების წარმოქმნის წყაროებსა და მათ სახეობებზე საერთაშორისო და რეგიონულ დონეზე. გაანალიზებულია კიბერუსაფრთხოების პოლიტიკისა და სტრატეგიის როლი, საქართველოს კიბერუსაფრთხოების სტრატეგია და არსებული საფრთხეები.

პირველი თავის მესამე ქვეთავი - ვირტუალური საფრთხე და ასიმეტრიული სამხედრო გამოწვევები. შესაძლოა, 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 გლობალურ საფრთხეებს.

მეორე თავი - კიბერომი, როგორც ასიმეტრიული საფრთხის ფენომენი. გაანალიზებულია, თუ როგორ უნდა მოხდეს უსაფრთხოების მექანიზმების მზარდი მოდერნიზება, რათა კიბერომი, როგორც მოვლენა, გაკონტროლდეს. თუ რა საფრთხეების წინაშე დგას საქართველო, რა კუთხით მიმდინარეობს საერთაშორისო თანამეგობრობასთან თანამშრომლობა, რა ურთიერთობები ჩამოყალიბდა ევროპის წამყვან სახელმწიფოებთან თუ ამერიკის შეერთებულ შტატებთან, ევროკავშირის წევრ ქვეყნებთან და ნატოსთან.

მეორე თავის პირველი ქვეთავი -კიბერუსაფრთხოების პოლიტიკა და ჰიბრიდული ომი (ირანის ისლამური რესპუბლიკის შემთხვევის გარჩევა). დოკუმენტურ მასალებზე დაყრდნობით ჩავატარეთ კვლევა და გავაანალიზეთ, თუ რა მოხდა 2020 წლის 3 იანვარს ერაყში, ბაღდადის აეროპორტის მახლობლად, როცა აშშ-ის სარაკეტო დარტყმას ირანის ისლამური რევოლუციის გუშაგთა კორპუსის სპეცდანიშნულების რაზმ „ალ-ქუდსის“ ლიდერი, გენერალი ყასემ სოლეიმანი ემსხვერპლა. ამ შემთხვევაში დიდი სკანდალი იყო კიბერთავდასხმებთან დაკავშირებით.

ნაშრომში წარმოდგენილია კიბერუსაფრთხოების გლობალური ინდექსი, რომლის თანახმადაც 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.

კიბერომი ევროკავშირის სივრცეში - გაანალიზებულია რუსეთიდან მომდინარე საფრთხეები და განხილულია ვარშავაში მიღებული გადაწყვეტილება, რომლის საფუძველზეც ნატომ 2017 წლის დასაწყისში ბალტიისპირეთის ქვეყნებში (ლიტვა, ლატვია, ესტონეთი) და პოლონეთში განათავსა ბატალიონის ტიპის 4 სამხედრო ქვედანაყოფი.

მეორე თავის მეორე ქვეთავი - კიბერსივრცის მთვარი აქტორები და საქართველო. 2013 წლის მაისში საქართველოს პრეზიდენტმა ხელი მოაწერა საქართველოს კიბერ უსაფრთხოების სტრატეგიას, რომელიც წარმოადგენს კიბერ უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ მთავარ დოკუმენტს. რა გამოწვევები არსებობს ამ მხრივ და რა საკანონმდებლო ბაზა გააჩნია საქართველოს? ეს არის ერთ-ერთი მნიშვნელოვანი საკითხი.

მეორე თავის მესამე ქვეთავი - ასიმეტრიული საფრთხეები და ჯიჰადისტების კიბერომი. საქართველოსთვის, ისევე როგორც მსოფლიოს მრავალი ქვეყნისთვის, ძირითად გამოწვევას ტერორისტული ორგანიზაცია „ისლამური სახელმწიფო“ („დაეში“) და მასთან დაკავშირებული დაჯგუფებები წარმოადგენენ. ჩავატარეთ კვლევა, თუ რას წარმოადგენს ჯიჰადისტური კიბერომი და რა საშიშროებასთან შეიძლება გვქონდეს საქმე.

მესამე თავი - კიბერომის კონცეფცია და 21-ე საუკუნის საერთაშორისო უსაფრთხოების სისტემა. საუბარია იმაზე, თუ რა ელემენტებია გამოკვეთილი „ჰიბრიდულ ომებში – ეკონომიკური კიბერ შეტევები, ბირთვული მუქარები, საინფორმაციო ომები“.

მესამე თავის პირველი ქვეთავი - თანამედროვე მაღალი ტექნოლოგიების გავლენა საერთაშორისო უსაფრთხოების პროცესებზე. კიბერომი, კიბერთავდასხმები და მოგერიება, ეს უწყვეტი პროცესია. რაც უფრო განვითარდება ინტერნეტ-სივრცე და დაინერგება ახალი მეთოდები, მით მეტად გაძლიერდება საფრთხეებიც. აქ დეტალურადაა გამოკვლეული, თუ რა რაოდენობის თანხები იხარჯება ამ მხრივ მსოფლიოში.

მესამე თავის მეორე ქვეთავი - კიბერომის ტრანსფორმაციის ისტორიული ასპექტები: სამხედრო კონფლიქტების სივრცული მახასიათებლები. გაანალიზებულია, თუ როდის გაჩნდა კიბერომის შესაძლებლობა, როდიდან შეიძლება დავიწყოთ ისტორიული ათვლა? ეს არის 21-ე საუკუნის „ეპიდემია“.

მესამე თავის მესამე ქვეთავი - კიბერომის ფენომენის ასახვა ეროვნული უსაფრთხოების სტრატეგიებში - მითი და რეალობა. ამ ქვეთავში განხილულია ეროვნული სტრატეგიის არსი და რუსული საფრთხე.

ნაშრომში წარმოდგენილია **დისკუსიის გარჩევა** - ტელეკომპანია „იმედი“, გადაცემა „არენა“. 2019 წლის 24 დეკემბერი. თემა: ინფორმაციული ქაოსი. აშშ-ის სახელმწიფო დეპარტამენტის განცხადება - რა შეუკვეთა ოპოზიციამ და რა ჩამოვიდა ვაშინგტონიდან.

სიღრმისეული ინტერვიუები ექსპერტებთან - ამირან სალუქვაძე, ნიკა ჩიტაძე, ლევან ნიკოლეიშვილი, ანდრო გოცირიძე, ზურაბ ბიგვავა, დავით კუხალაშვილი. მათ უპასუხეს ჩვენს მიერ დასმულ კითხვებს.

ფოკუს ჯგუფი, შემთხვევის განხილვა კავკასიის საერთაშორისო უნივერსიტეტის სტუდენტების მიერ. თემა: 2008 წლის რუსეთ-საქართველოს ომი და კიბერთავდასხმა. ნაშრომი ასევე შედგება დანართებისგან და კითხვარებისგან.

Annotation

The work discusses the essence, basics and origins of cyberwar. The main topic of the research is the information war, as a continuation of the Cold War amid technological advances. Global security, the role of the United States, Western Europe, Eastern Europe, the European Union and NATO, today's reality. Geostrategic situation and security of Georgia. NATO expansion to the east. Hybrid wars waged by Iran, China, and Russia, hacking attacks, and propaganda of a conquering nature.

Since cyberspace has already become an instrument of endless possibilities for the whole world and has become a source of good and an area of evil for terrorists, humanity has been in great danger. The subject of the study is also where Georgia is at this time and what functions it performs. The 2018 report of the State Security Service emphasizes that "countries interested in strengthening their influence in Georgia are actively using hybrid warfare methods to achieve their goals."[2] An important tool of hybrid warfare is the disinformation campaign, fake news, the introduction of misconceptions and fears, the manipulation of public opinion to influence important processes. This work presents its own opinions, recommendations (based on research), as well as opinions and recommendations developed by foreign or Georgian experts and specialists.

The work contains three chapters, expert opinions, discussions, and case studies.

The first chapter is devoted to the essence of the cyberwar and the historical overview. Global technology upgrades are needed for global security. It is also important for Georgia. The current level of threats in cyberspace is very high. Every country is trying to defend itself, but if not for the programs developed by the

[2] https://1tv.ge/news/sus-saqartveloshi-gavlenis-gadzlierebit-dainteresebuli-qveynebi-hibriduli-omis-metodebs-iyenebdnen-romlis-mnishvnelovan-instruments-dezinformaciuli-kampania-warmoadgenda/, უკანასკნელად იქნა გადამოწმებული: 10.06.2020

European Union and NATO, the defense would be on an individual level and would be ineffective.

The first subsection of the first chapter discusses the issue of how conflicts are transformed under the new geopolitical order and what events or measures have been taken by different countries around the world.

The second subsection of the first chapter is Cyber War Theory and its place in modern world politics. It discusses what is being done in cooperation with the EU and NATO to create a safe environment. Attention is paid to the global importance of the new information space, its positive and negative factors. We are talking about the threats that exist in cyberspace, the sources of these threats and their species at the international and regional levels. The role of cyber security policy and strategy, Georgia's cyber security strategy and existing threats are analyzed.

The third subsection of the First Chapter - Virtual Danger and Asymmetric Military Challenges. NATO may not expand militarily, but the fact is, it has to expand in terms of cyber warfare issues. There are almost no borders here - even if the post-Soviet space is not controlled, NATO's military perspective will not matter much and it will not be able to withstand global threats.

Chapter Two - Cyber Warfare as a Phenomenon of Asymmetric Danger. Analyzed how to increase the modernization of security mechanisms to control the cyberwar as an event. What are the threats facing Georgia, what is the cooperation with the international community, what relations have been established with the leading European countries or the United States, EU member states and NATO.

The first subsection of the second chapter - Cyber Security Policy and Hybrid War (Discussing the Case of the Islamic Republic of Iran). Based on the documentary material, we conducted a study and analyzed what happened on January 3, 2020 in Iraq, near Baghdad Airport, when Al-Quds leader, General Qasem Soleimani, the leader of the Islamic Revolutionary Guard Corps (IRGC) was killed in a U.S. airstrike. In this case, there was a big scandal over cyber-attacks.

The work presents the Global Cyber Security Index, according to which Georgia was ranked 8th among 165 countries in 2017. The index is compiled by a specialized body of the United Nations - the International Telecommunication Union (ITU) and published every 2 years.

Cyber War in the European Union - the threats from Russia are analyzed and the decision made in Warsaw is discussed , on the basis of which NATO put up 4 battalion-type military units in the Baltic states (Lithuania, Latvia, Estonia) and Poland in early 2017.

The second subsection of the second chapter - the main actors of cyberspace and Georgia. In May 2013, the President of Georgia signed the Cyber Security Strategy of Georgia, which is the main document defining the state policy in the field of cyber security. What are the challenges in this regard and what is the legal basis for Georgia? This is one of the most important issues.

The third subsection of the second chapter is Asymmetric Threats and the Cyber War of the Jihadists. For Georgia, as well as for many countries around the world, the main challenge is the Islamic State terrorist organization (Daesh) and its affiliated groups. We conducted research on what constitutes jihadist cyber warfare and what dangers we may be dealing with.

Chapter Three - The Concept of Cyber Warfare and the 21st Century International Security System. We are talking about the elements that have been identified in the "hybrid wars - economic cyber-attacks, nuclear threats, information wars."

The first subsection of the third chapter - The Impact of Modern High Technology on International Security Processes. Cyber warfare, cyber-attacks and repulsion, it is a continuous process. The more the Internet space is developed and new methods are introduced, the more the threats will intensify. Here is a detailed study of how much money is spent in this regard in the world.

The second subsection of the third chapter is Historical Aspects of the Transformation of the Cyber War: Spatial Characteristics of Military Conflict.

Analyzed when the possibility of cyber warfare arose, when can we begin a historical count? This is the "epidemic" of the 21st century.

The third subsection of the third chapter - Reflecting the Phenomenon of Cyber Warfare in National Security Strategies - Myth and Reality. This section discusses the essence of the national strategy and the Russian threat.

The work presents **a discussion** –on Imedi TV, in the program Arena. On December 24, 2019. The Topic: Information chaos. Statement by the US State Department - What the opposition ordered and what arrived from Washington.

In-depth interviews with experts - Amiran Salukvadze, Nika Chitadze, Levan Nikoleishvili, Andro Gotsiridze, Zurab Bigvava, Davit Kukhalashvili. They answered our questions.

Focus group, discussion of the case by students of Caucasus International University. Topic: Russia-Georgia war of 2008 and cyber-attack. The paper also consists of appendices and questionnaires.

სარჩევი

ცხრილებისა და დიაგრამების ნუსხა

ცხრილები:

დიაგრამები:

ფიგურები:

გამოყენებული აბრევიატურები

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, 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, დავით კუხალაშვილს.**

მადლობა სახელმწიფო და კორპორაციული უსაფრთხოების სასწავლო-კვლევით ცენტრს, ინოვაციისა და სამოქალაქო განვითარების ცენტრს (თავმჯდომარე **ლაშა ბოდაველი**), შავი ზღვის საერთაშორისო უნივერსიტეტს (სოციალურ მეცნიერებათა ფაკულტეტის დეკანი **რამაზან აკბა**), ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტს (ჰუმანიტარულ მეცნიერებათა დაკულტეტის პროფესორები **თამარ პაიჭაძე** და **კახაბერ ლორია**), საქართველოს საპატრიარქოს წმინდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტს (რექტორი **სერგო ვარდოსანიძე**), 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 აქტუალობა

კიბერომი უკვე ნიშნავს შეიარაღებულ ომთან გათანაბრებას. პროპაგანდა საინფორმაციო ომის ხელსაყრელი საშუალებაა. მეცნიერები ეძებენ ახალ ტერმინებს, იკვლევენ მიმდინარე მოვლენებს და მივიდნენ დასკვნამდე, რომ კაცობრიობა გადადის „მეხუთე თაობის“ კიბერომების ეპოქაში.

საქართველოს უსაფრთხოების სამსახურის ანგარიშებში ნათქვამია, რომ დღეს ქვეყნის უსაფრთხოებისთვის მნიშვნელოვან რისკს წარმოადგენს უცხო ქვეყნების სპეცსამსახურებისა და მათ მიერ კონტროლირებადი ჰაკერული ჯგუფების მიერ სამთავრობო თუ ინფრასტრუქტურის ობიექტებზე კიბერშეტევებისა და კიბერსადაზვერვო ოპერაციების განხორციელება. რასაკვირველია, მსგავსი საფრთხეების თავიდან აცილება შეუძლებელია თანამედროვე ტექნოლოგიების, პროფესიონალი კადრებისა და წამყვან სახელმწიფოებთან თანამშრომლობის გარეშე.

საქართველოსთვის, უასფრთხოების თვალსაზრისით, კვლავაც გასაძლიერებელია ნატო-სთან და წამყვანი სახელმწიფოების უსაფრთხოების სამსახურებთან თანამშრომლობა, რათა დროულად მოხერხდეს პრევენციული ზომების გატარება. მით უმეტეს, უფრო მჭიდრო თანამშრომლობაა საჭირო მეზობელი სახელმწიფოების უსაფრთხოების სამსახურებთან. კიბერსივრცის დაცვა ეროვნული უსაფრთხოების პრიორიტეტულ მიმართულებად უნდა იყოს აღიარებული.

რამდენი სახის ელემენტს შეიცავს საინფორმაციო ომი? სქემა ასეთია: პირველი - ფსიქოლოგიური ტერორი, ანუ ადამიანთა ტვინების გამორეცხვა მასობრივი საინფორმაციო საშუალებებით. მეორე - ინტერნეტ და სატელევიზიო სიმძლავრეების ამუშავება ტექნიკურად, ანუ ზემოქმედება წარმოსახვით უნარზე და შავის თეთრად გასაღება; მესამე - კიბერომის ელემენტების გამოყენება, ანუ მოწინააღმდეგის ტექნიკური დაზიანება, ზოგჯერ კი ვითომ თავდაცვა.

განყენებულად ვერ განვიხილავთ „ახალი ცივი ომის“ სტრატეგიას და დღევანდელი „რბილი ძალის“ მიმართულებებს, თუ არ გავიხსენეთ ე.წ. „ძველი ცივი ომის“ დეტალები. ე.წ. „ძველი ცივი ომი“ არც თუ მარტივი მეთოდებით წარმოებდა აშშ-სა და სსრკ-ს (USSR) შორის, ანუ საბჭოთა ბანაკსა და შეერთებულ შტატებს შორის, სადაც რასაკვირველია, შედიოდა დასავლეთი ევროპაც. ერთმანეთს უპირისპირდებოდა ორი მძლავრი სისტემა და გაჩაღებული იყო დაუნდობელი პროპაგანდა. აღსანიშნავია, რომ „ჰიბრიდული ომი“, როგორც ასეთი, არ გაჩენილა ცარიელ ადგილზე, ის არსებობდა და ვითარდებოდა ტექნოლოგიებთან ერთად.

ყოველ საუკუნეს თან სდევს თავისი პრობლემები, თუ წინა ორი საუკუნის განმავლობაში კაცობრიობა ჩააბეს მსოფლიო ომებში, 21-ე საუკუნეში ყველაზე საშიშ მოვლენად იქცა კიბერთავდასხმები, საინფორმაციო და ჰიბრიდული ომები, სადაც ყოველწლიურად ზარალდება მილიონობით ადამიანი, ზარალდება ასი ათასობით კერძო კომპანია, ზარალდება ასი ათასობით სახელმწიფო დაწესებულება. თავდაცვის მიზნით კი იხარჯება ასეულობით მილიარდი დოლარი. სპეციალისტები ვარაუდობენ, რომ 2021 წლისთვის კიბერშეტევები გამოიწვევს 6 ტრილიონი დოლარის ზარალს. როგორც ჩანს, შორს აღარ არის ის დრო, როცა კიბერაგრესორები ატომური ობიექტების სისტემებში შეღწევასაც შეეცდებიან და მსოფლიოს დააყენებენ ძალიან დიდი საფრთხის წინაშე.

იქმნება შთაბეჭდილება და ალბათ ასეც უნდა იყოს, რომ მთელი დასავლეთი თუ აღმოსავლეთი ევროპა, არ აქვს მნიშვნელობა, არიან თუ არა ნატო-ს წევრები, ხელმძღვანელობენ ნატო-ს სტრატეგიით, ეს ორგანიზაცია, უსაფრთხოების თვალსაზრისით, ერთგვარი ქოლგაა ყველასთვის და მათ შორის საქართველოსთვის. სწორედ ამიტომაც შემუშავდა ნატო-საქართველოს არსებითი პაკეტი (SNGP), სადაც საუბარია ჩვენი ქვეყნის უსაფრთხოების მხარდაჭერაზე. კერძოდ, თავდაცვითი სისტემების ტრანსფორმაციაზე, მის გაძლიერებასა და ახალი ინფრასტრუქტურის შექმნა-განვითარებაზე. ნატოს ყველა კონცეფციასა თუ დოქტრინაში ხაზგახმითაა

აღნიშნული, რომ ძირითადი პრინციპებიდან გამომდინარე, მისი წევრი არც ერთი ქვეყანა არ უნდა იყოს იძულებული, დაეყრდნოს მხოლოდ საკუთარ ძალისხმევას. ალიანსის სტრატეგია საშუალებას აძლევს თითოეულ წევრ სახელმწიფოს, კოლექტიური მეთოდებით მოახდინონ ეროვნული უსაფრთხოების მიზნების რეალიზება. რა თქმა უნდა, ეს კურსი სწორია, მაგრამ ნატოს 1991 წლიდან მოყოლებული, ანუ ცივი ომის დასრულების შემდეგ, რასაც მოჰყვა სხვა ტიპის „ცივი ომები“, გაუჩნდა უფრო მეტი საზრუნავი - გაფართოება აღმოსავლეთ ევროპაში და ერთგვარი მფარველობის გაძლიერება პოსტსაბჭოთა სივრცეში. 1991 წლის შემდეგ პოსტსაბჭოთა სივრცისთვის საჭირო იყო ადაპტაციის პერიოდი დანარჩენ სამყაროსთან, რასაც აუცილებლად უნდა მოჰყოლოდა ძირეული ცვლილებები მენტალობისა და თექნოლოგიური გადაიარაღების თვალსაზრისით. ალიანსის ზედა ეშელონებში ფიქრობდნენ, რომ მოკლევადიან პერიოდში ფართომასშტაბიანი აგრესია ნატოს წინააღმდეგ ნაკლებ სავარაუდო იყო, მაგრამ გრძელვადიან პერსპექტივაში ალიანსის უსაფრთხოება რჩება სამხედრო და არასამხედრო ხასიათის რისკების ობიექტად, ამ რისკების მრავალფეროვნების გამო კი საფრთხეები ხშირად არაპროგნოზირებადია. რა რისკებზეა საუბარი? ეთნიკურ და რელიგიურ ქიშპზე, ტეროტორიულ დავებზე, ადამიანის უფლებების შელახვაზე, სახელმწიფოთა რღვევებზე, ტერორიზმზე და ასე შემდეგ. ამას უნდა დავუმატოთ სხვა რისკებიც - საბოტაჟი, ორგანიზებული დანაშაული და ასე შემდეგ.

ნატო ერთადერთი ორგანიზაციაა, რომელსაც ტექნიკურად, ფინანსურად თუ ადამიანური რესურსების მხრივაც შესწევს ძალა, წინააღმდეგობა გაუწიოს კიბერშემოტევებს. ამიტომ მნიშვნელოვანია დღევანდელი მდგომარეობისა და სამომავლო გეგმების შესწავლა, გაანალიზება, კვლევა, პრაქტიკული კუთხით წარმოჩენა და ასე შემდეგ. მკვლევართა მტკიცებით, თუ იქნება სწორი მიდგომა მეცნიერული კუთხით, კიბერომის შედეგები არ გახდება ისეთი დამაგრეველი, როგორც ეს იყო წინა თაობების პერიოდში.

კვლევის მიზნები და ამოცანები

კვლევის ძირითადი მიზანია:

ჩვენს მიერ შერჩეული თემა მიზნად ისახავდა კიბერომის მნიშვნელოვანი საფრთხის შემცველი როლის წარმოჩენას მსოფლიოს მასშტაბით და ახალი პოლიტიკური კონფლიქტის გაანალიზება-შეფასებას, განსაზღვრას. შემდეგი საკითხებიდან გამომდინარე:

- **კიბერომი, როგორც ახალი საფრთხეების ფაქტორები**
- **ქვეყნების უსაფრთხოების საკითხები**

სადისერტაციო ნაშრომის ამოცანებია:

თემის დამუშავებისას დასახული ამოცანები თავის მხრივ ასახავს ქმედებას, რომელიც მიმართულია დასახული მიზნების მისაღწევად და მოიცავს:

- **ახალი გეოსტრატეგიული ამოცანების ანალიზი და ახალი საფრთხის შემცველი გამოწვევები.**
- **კიბერომის განვითარების ისტორია და მისი კომპონენტების საშიშროების განსაზღვრა.**
- **კონფლიქტების ტრანსფორმაცია ახალი გეოპოლიტიკური წესრიგის პირობებში.**
- **კიბერომის თეორია და მისი ადგილი თანამედროვე მსოფლიო პოლიტიკაში.**
- **ვირტუალური საფრთხე და ასიმეტრიული სამხედრო გამოწვევები.**
- **კიბერომი როგორც ასიმეტრიული საფრთხის ფენომენი.**
- **კიბერუსაფრთხოების პოლიტიკა და ჰიბრიდული ომი.**

ძირითადი საკვლევი საკითხები და კვლევის გეგმა

სადისერტაციო ნაშრომის ძირითადი მიმართულებებია:

ძირეულად უნდა იყოს განხილული მსოფლიო უსაფრთხოების დღევანდელი გამოწვევები. რამ გამოიწვია ის ტერორისტული

კატაკლიზმები, რაც დღეს მიმდინარეობს სხვადასხვა ქვეყნებში. რა ტექნოლოგიები არსებობდა და არსებობს, რომ თავიდან იქნას აცილებული საფრთხეები. საინფორმაციო ომის საფუძვლები. კიბერომი და კიბერდანაშაული. რა თავდაცვითი სისტემები არსებობს ამჟამად მსოფლიო დონეზე. კანონმდებლობა - რათა თავდაცვა და თავდასხმა განხორციელდეს ცივილიზებულად და არა მეკობრული წესებით. ზემოთ ჩამოთვლილი საკითხების სერიოზული შესწავლისა და ანალიზის გარეშე ვერ მოხდება ობიექტური და ღრმა პროდუქტის შექმნა. პრობლემის არსის სწორი განსაზღვრა და მისი გადაჭრის ვარიანტების სისტემის შექმნა, რომელთაც რეკომენდაციების ფორმა უნდა ჰქონდეს.

კიბერტერორიზმი, კიბერომი, კიბერდანაშაული, ეს გახლავთ წინასწარ განზრახული, პოლიტიკურად მოტივირებული ძალადობა, მშვიდობიანი სამიზნის წინააღმდეგ, რაც გამოხატულია ინფორმაციაზე, კომპიუტერულ სისტემებზე, პროგრამებსა და მონაცემთა ბაზებზე შეტევასა და განადგურებაზე.

2002 წელს პრაღის სამიტზე ნატოს წევრ სახელმწიფოთა ლიდერებმა კიბერტერორიზმი მნიშვნელოვან საფრთხედ აღიარეს და საჭიროდ მიიჩნიეს, შექმნილიყო კიბერთავდაცვის პროგრამა, რომელიც მოიცავდა მოქმედების სამ ფაზას. პირველი ფაზისას შეიქმნა „ნატოს კომპიუტერული ინციდენტის საპასუხო უნარიანობა“ (NCIRC), რომელიც მეორე ფაზისას სრულ სამუშაო რეჟიმში შევიდა. მესამე ფაზა მოიცავს პირველი ორი ფაზისგან მიღებული გამოცდილების პრაქტიკაში დანერგვას და კიბერტერორიზმთან ბრძოლაში თანამედროვე თავდაცვითი საშუალებების გამოყენებას. ამას აქვს გადამწყვეტი მნიშვნელობა.[3]

[3] http://studinfo.edu.aris.ge/2013/11/12/nato-%E1%83%99%E1%83%98%E1%83%91%E1%83%94%E1%83%A0-%E1%83%A2%E1%83%94%E1%83%A0%E1%83%9D%E1%83%A0%E1%83%98%E1%83%96%E1%83%9B%E1%83%98%E1%83%A1-%E1%83%AC%E1%83%98%E1%83%9C%E1%83%90%E1%83%90/, უკანასკნელად იქნა გადამოწმებული: 11.06.2020

კიბერომი, როგორც გლობალური საკითხი, ვერ იქნება ერთი მიმართულებით საკვლევი საგანი. მით უმეტეს, ამ მოვლენასთან წინააღმდეგობის გაწევა ვერ მოხერხდება ცალსახად. აქ საყურადღებოა უამრავი ფაქტორი - მაგალითად: კიბერდანაშაულის არსი, კიბერდანაშაულის წარმოშობა-განვითარება, გამომწვევი და ხელშემწყობი მიზეზები, კიბერდაზარალებულის ცნება, კიბერდამნაშავეთა საერთაშორისო ორგანიზებული დაჯგუფებები, კომპიუტერული პროგრამები და მათი აგებულება, პროგრამირების ენები და მათი დანიშნულება, ინტერნეტისა და ქსელის საფუძვლები, კიბერდანაშაულთან დაკავშირებული ტერმინოლოგია, კომპიუტერულ სისტემაში უნებართვო შეღწევა, კომპიუტერული სისტემის ხელყოფა, ადამიანის წინააღმდეგ მიმართული კიბერდანაშაული, პრობლემური საკითხები კიბერსივრცის კანონმდებლობასთან დაკავშირებით, კიბერსივრცის მარეგულირებელი შიდა და საერთაშორისო სამართალი - 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, მათი გამომუშავება და სამართლებრივი კონტროლის საკითხები. ასევე, ცალკე კვლევის საგანია გავრცელებული კიბერდანაშაულის ჩადენის მეთოდები - ქარდინგი, ფიშინგი, ფოსტის ჰაკინგი, სოციალური ქსელების ჰაკინგი, ტროიანები და სხვა მსგავსი კოდები, ვირუსები, სოციალური ინჟინერია, მეტასპლოიტები, მობილურ ტელეფონებთან დაკავშირებული დანაშაული და ასე შემდეგ. საყურადღებოა ციფრული მტკიცებულებები - კიბერდანაშაულის კვალი, ციფრული მტკიცებულების არსი, ციფრული მტკიცებულებების სახეები და მათი მოპოვება, ციფრულ მტკიცებულებებთან მოპყრობა, ანალიზი, კომპიუტერული სისტემების ჩხრეკა-ამოღება და სხვა. ცალკე გამოსაყოფია, თუ როგორ მოქმედებენ

კიბერუსაფრთხოებაზე პასუხისმგებელი ორგანოები საქართველოში და საექსპერტო დაწესებულებები, რათა თავიდან იქნას აცილებული კიბერსივრცეში არსებული საფრთხეები - კიბერტერორიზმი, კიბერომი, პირადი მონაცემების დაცვა ინტერნეტში, კიბერდანაშაულის პრევენცია თავდაცვის მიზნით.

ნაშრომის ძირითადი საკვლევი კითხვები:

1. რა გავლენა შეიძლება იქონიოს საერთაშორისო საზოგადოებაზე „კიბერომმა“?
2. როგორია სამოქმედო გეგმა და სამხედრო სტრატეგიის შემადგენელი ნაწილები კიბერ ომის პირობებში?
3. რა მნიშვნელობა ენიჭებათ ამ შემთხვევაში სტრატეგიულ პარტნიორებს?

ჰიპოთეზა

ვინაიდან, კიბერსივრცე დროთა განმავლობაში გარდაიქმნა რეალობის ალტერნატიულ ვარიანტად, ვირტუალური სამყარო გადხა ცხოვრების ერთგვარი დამატებითი სივრცე. უამრავი საკითხი ეფუძნება ვარაუდს, ერთგვარ წინასწარმეტყველებას ან გონივრულ ეჭვს. როდესაც საქმე გვაქვს მიმდინარე პროცესთან, ტექნოლოგიურ რევოლუციასთან, ყველაფრის წინასწარ განსაზღვრა და ზუსტი რეცეპტის დადება შეუძლებელია. გლობალურ პოლიტიკაში ერთ-ერთი მნიშვნელოვანი და საკვანძო საკითხია პოლიტიკური კონფლიქტების ახალი განზომილებები. საინფორმაციო ბრძოლის თეორია, როგორც ჰიბრიდული ომის შემადგენელი ნაწილი, მნიშვნელოვანია, თუ რამდენად განსაზღვრავს საერთაშორისო უსაფრთხოების პროცესების მიმდინარეობას და რაობას.

კიბერომს „ომის ახალ ხელოვნებასაც“ უწოდებენ. სწორედ ამ თემაზე 2017 წლის 10 აპრილს საქართველოში ჩატარდა ფორუმი ნატოს ეგიდით, რომელშიც ქართველი, ესტონელი, რუმინელი და ბრიტანელი სპეციალისტები მონაწილეობდნენ. ფორუმის მონაწილეთა საუბრის თემა იყო ნატოს სტრატეგიის ახალი კონცეფცია, გამოცდილების გაზიარება და სამომავლო თანამშრომლობის დაგეგმვა. ვინაიდან, კიბერომის ერთ-ერთი მნიშვნელოვანი კომპონენტი მოულოდნელობის ეფექტია, ამიტომ მუდმივად ჩართული უნდა იყოს მოლოდინის რეჟიმი, როგორც წამზომი. სადაც არსებობს მოულოდნელობის ეფექტი და ჩართულია წამზომი, ბუნებრივია, იქ ყველაფერის გათვლა შეუძლებელია და აუცილებლად არის ასამუშავებელი ასევე „ვარაუდის, გათვლისა და წინასწარმეტყველების ეფექტი“.

თემის მეცნიერული სიახლე

ტრადიციული მედია და საინფორმაციო ომი. სოციალური მედია და საინფორმაციო ომი. ახალი გამოწვევებისა და ახალი ტექნოლოგიების, ასევე ახალი თეორიული ასპექტების ჩამოყალიბება. ეროვნული უსაფრთხოების

სტრატეგია და შესაძლებლობები. ევროკავშირის, ნატოსა და აშშ-ის კიბერუსაფრთხოების სტრატეგია, თანამშრომლობისა და ახალი ტექნოლოგიების დანერგვის შესახებ ანალიზი, ახალი მონაცემები. რუსეთის, როგორც კიბერომის მთავარი მონაწილის მეთოდების აღწერა. ჩინეთი და ირანი, ამ ქვეყნებიდან მომდინარე კიბერსაფრთხეების ანალიზი. კიბერუსაფრთხოების საერთო სტრატეგიის გამოკვეთა მსოფლიო მასშტაბით, რეკომენდაციები.

ნაშრომის პრაქტიკული ღირებულება

აღნიშნული ნაშრომის კვლევის შედეგები შესაძლებელია გამოადგეს კიბერუსაფრთხოების სპეციალისტებს, ტერორიზმის წინააღმდეგ მებრძოლ ორგანიზაციებს, ჰიბრიდული ომების ანალიტიკოსებს, დარგით დაინტერესებულ კერძო პირებს, ასევე საგარეო უსაფრთხოების მიმართულებების ფაკულტეტების სტუდენტებს.

კვლევები და რეკომენდაციები გამოსადეგია საქართველოს მთავრობის მიერ ქვეყნის უსაფრთხოების სტრატეგიის ძირითადი მიმართულებების განსაზღვრის დროს. კვლევის შედეგები შესაძლოა 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. დოქტორანტი მონაწილეობდა სხვადასხვა სახის კონფერენციებში, ტრენინგ-სემინარებში, გამოაქვეყნა პუბლიკაციები სამეცნიერო ჟურნალებში: 2017 წ. სახელმწიფო და კორპორაციული უსაფრთხოების სასწავლო-კვლევითი ცენტრი. დირექტორი: დავით კუხალაშვილი.

სამეცნიერო პრაქტიკული კონფერენცია: „ეროვნული და კორპორაციული უსაფრთხოება“. 2017 წ. ინოვაციისა და სამოქალაქო განვითარების ცენტრი. თავმჯდომარე: ლაშა ბოდაველი. ტრენინგი თემაზე - “ტექნოლოგიები

წარმატების მისაღწევად“. 2018 წ. კავკასიის საერთაშორისო უნივერსიტეტი. პროფესორი კახაბერ კორძაია. მეექვსე საერთაშორისო კონფერენცია ბაკალავრებისთვის, მაგისტრანტებისთვის და დოქტორანტებისთვის. 2018 წ. შავი ზღვის საერთაშორისო უნივერსიტეტი. სოციალურ მეცნიერებათა ფაკულტეტის დეკანი რამაზან აკბა. პარტნიორობა მშვიდობისათვის კონსორციუმის რეგიონალური სტაბილურობის სამხრეთ კავკასიის სასწავლო ჯგუფის თანათავმჯდომარე ფრედერიკ ლაბარე. ლექციების ციკლი - "კანადის საგარეო და თავდაცვის პოლიტიკა". 2018 წ.

კავკასიის საერთაშორისო უნივერსიტეტი. კირილე და ველიკო ტარნოვოს სახელობის უნივერსიტეტის პროფესორი ტოდორ გალუნოვი. ლექციების ციკლი - “ევროპული ინსტიტუტები და პოლიტიკური მენეჯმენტის ტექნოლოგიები”. 2018 წ. „ახალგაზრდა ექსპერტთა ასოციაცია“ - ტრენინგებისა და სემინარების კურსი - „ასიმეტრიული საფრთხეები და ჰიბრიდული ომის გავლენა გლობალურ უსაფრთხოებაზე“. 2019 წ. კავკასიის საერთაშორისო უნივერსიტეტი. პროფესორი კახაბერ კორძაია. ბიზნესის და მეწარმეობის კოლეჯი „Ostrowiec Świętokrzyski“, პოლონეთი, ასოცირებული პროფესორი: prezemyslaw furgacz პრეზემისლავ ფურგაცი. ლექციების კურსი - „ეკონომიკური ომის თეორია და გლობალური უსაფრთხოება“.

2019 წ. კავკასიის საერთაშორისო უნივერსიტეტი. პროფესორი კახაბერ კორძაია მეშვიდე საერთაშორისო კონფერენცია ბაკალავრებისთვის, მაგისტრანტებისთვის და დოქტორანტებისთვის.

2019 წ. უსაფრთხოების მეცნიერებათა დოქტორი სოციალურ მეცნიერებათა დარგში, ომის სასწავლო უნივერსიტეტის ასისტენტ-პროფესორი, ვარშავაში: მარსენა ზაკოვსკა. ლექციების კურსი - „ეროვნული უსაფრთხოება და თანამედროვე ომის თეორია XXI საუკუნის საერთაშორისო ურთიერთობებში: მიდგომები და გამოწვევები“. 2019 წ. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. კონფერენციის ხელმძღვანელი, ორგანიზატორი თსუ-ის ჰუმანიტარულ მეცნიერებათა დაკულტეტის პროფესორი თამარ პაიჭაძე. სტუდენტთა XI საერთაშორისო

სამეცნიერო კონფერენცია. 2019 წ. ეროვნული და კორპორაციული უსაფრთხოების სასწავლო კვლევითი ცენტრის დირექტორი, თადარიგის პოლკოვნიკი დავით კუხალაშვილი. სამეცნიერო კონფერენცია - „ეროვნული და კორპორაციული უსაფრთხოება“. 2019 წ. საქართველოს საპატრიარქოს წმინდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტი. სამეცნიერო კონფერენცია: „ევროკავშირის გაერთიანება - პრობლემები და პერსპექტივები“. 2019 წ. შავი ზღვის საერთაშორისო უნივერსიტეტი კომპიუტერული და სარედაქციო დახმარება. 2019 წ. შავი ზღვის საერთაშორისო უნივერსიტეტი. ამერიკული კვლევების მიმართულება.

საკონფერენციო მასალები

შავი ზღვის საერთაშორისო სამეცნიერო კონფერენცია და სამეცნიერო ჟურნალი: „ამერიკული კვლევების პერიოდული №12 გამოცემა“. 2019 წ. უკრაინის განათლებისა და მეცნიერების სამინისტრო. იური ფედკოვიჩ ჩერნივის ეროვნული უნივერსიტეტი. ჟურნალი ისტორიულ და პოლიტიკურ მეცნიერებებში. ტომი 40. ისტორიის ფაკულტეტი, პოლიტიკური მეცნიერება და საერთაშორისო კვლევები საერთაშორისო ურთიერთობების განყოფილება. თანამედროვე ისტორიული და პოლიტიკური საკითხები. 2020 წ. კავკასიის საერთაშორისო უნივერსიტეტი. სამეცნიერო ჟურნალი - „პოლიტოლოგოსი“. საერთაშორისო სამეცნიერო კონფერენცია „ასიმეტრიული კომფლიქტები და ჰიბრიდული ომი 21-ე საუკუნეში“, რეფირირებადი ჟურნალი ,,ANTE PORTAS Security Studies”, სამეცნიერო სტატია, 2019 წლის გამოცემა. პუბლიკაციები დაბეჭდილია რეფერირებად ჟურნალებში საზღვარგარეთ, რომლებიც ინდექსირებულია საერთაშორისო ელექტრონულ ბაზებში.

კვლევის მეთოდოლოგია

კრიტიკული თეორიის სკოლა - საერთაშორისო ურთიერთობების ტრადიციული თეორიების წინააღმდეგ შექმნილი ლიტერატურა, რომელშიც უარყოფილია საერთაშორისო ურთიერთობების, როგორც მეცნიერების

ცალკე დარგის არსებობა. ამ სკოლის წარმომადგენლებს მიაჩნიათ, რომ საერთაშორისო ურთიერთობების ანალიზი უფრო ფართო სოციალურ, პოლიტიკურ, კულტურულ და ფილოსოფიურ კონტექსტში უნდა მოხდეს და არა ერთი დისციპლინის ფარგლებში. თეორია ასოცირდება ფრანკფურტის სკოლის ფილოსოფიურ ტრადიციასთან და მის დამაარსებელ იურგენ ჰაბერმასთან. მისი კომპლექსური სოციალური თეორია და ფილოსოფია კანტის, შელინგის, ჰეგელის, დითის, ჰუსერლის და გადამეროს ინტელექტუალურ ტრადიდიცებს ეყრდნობა. ჰაბერმასმა შექმნა დისკურსისა და კომუნიკაციური მოქმედებების ახლებური თეორიები, რამაც დასაბამი მისცა კანონისა და დემოკრატიის ახალ პერსპექტივებს. გვთავაზობს კრიტიკული სოციალური თეორიის ახალ საფუძველს და თავისუფალ და თანაბარი უფლებების მქონე მოქალაქეებში დისკურსის შესაძლებლობას განიხილავს. რაც შეეხება საერთაშორისო ურთიერთობებსა და ამ სფეროს მეცნიერულ კვლევას, როგორც ცალკე დარგისას, ეს შეიძლება საკამათოც კი იყოს. ყოველ შემთხვევაში, ყველაფერი მაინც მეცნიერულ მიდგომებზეა დამოკიდებული. თუკი არსებობს პოლიტიკური მეცნიერება, მაშინ საერთასორისო ურთიერთობებიც შეიძლება განვიხილოთ ამავე კუთხით. სადოქტორო ნაშრომში მრავლად გვაქვს მოყვანილი ფაქტები, სადაც სახელმწიფოთა და მათ ლიდერთა ურთიერთობებზეა საუბარი. ხშირ შემთხვევაში ურთიერთობები არ სცილდება ბრალდებებსა და მუქარას. ამის საუკეთესო მაგალითებად გამოდგება აშშ-ირანის, აშშ-ჩინეთისა თუ აშშ-რუსეთის ურთიერთობები. ამავე ჭრილში უნდა განვიხილოთ რუსეთ-უკრაინისა და რუსეთ-საქართველოს ურთიერთობები. ჰაბერმასის თეორია საინტერესოა, რათა გავიგოთ, რა სახის ურთიერთობები ჩამოყალიბდა სახელმწიფოებს შორის.

პოლიტიკური რეალიზმის თეორია - მეცნიერების მტკიცებით, პოლიტიკური რეალიზმი იყო პასუხი ლიბერალიზმზე, რომლის ამოსავალი დებულება მდგომარეობდა იმაში, რომ სახელმწიფოები არ ცდილობენ თანამშრომლობას. ადრეული რეალისტები ედვარდ ქარი და ჰანს

მორგენთაუ მიიჩნევდნენ, რომ საკუთარი უსაფრთხოებაზე ზრუნვის გამო სახელმწიფოები არიან ეგოისტური რაციონალური აქტორები, რომლებიც ისწრაფვიან ძალაუფლებისკენ. 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. ეს თეორია გამოყენებულია კიბერუსაფრთხოების გლობალური აქტორების ინტერესებისა და მიზნების გასაანალიზებლად.

ნეოკლასიკური რეალიზმის თეორია - ეს გახლავთ უძველესი თეორია საერთაშორისო ურთიერთობების შესახებ, რომელიც სათავეს ჯერ კიდევ ძველი წელთაღრიცხვით მე-5 საუკუნეში არსებობდა, ხოლო ყველაზე მეტად მე-20 და 21-ე საუკუნის დასაწყისში გააქტიურდა. 1948 წელს ამერიკელმა მეცნიერმა ჰანს მორგენთაუმ გამოსცა წიგნი "ქვეყნების პოლიტიკა - ბრძოლა ძალაუფლებისა და მშვიდობისათვის". როგორც ამბობენ, ეს თეორია არის მაკიაველისა და ჰობსის იდეების გაგრძელება და ქადაგებს, რომ ადამიანის ბუნება არის მტაცებლური, ბუნებრივად მზაკვარი და ბნელი, რომ ეს ფაქტი აისახება პოლიტიკურ ურთიერთობებზე. პოლიტიკა და ეთიკა ერთმანეთისგან შორსაა, რომ პოლიტიკური ძალა და ძლიერება არის მშვიდობის ერთადერთი გარანტი. მორგენთაუს თეორიას უწოდებენ ნეოკლასიკურ რეალიზმს, რაც იმას ნიშნავს, რომ ის არის მეოცე საუკუნის განახლებული კლასიკური ტრადიცია საერთაშორისო ურთიერთობების თეორიაში.

ნეოკლასიკური რეალიზმის თეორიას ემთხვევა ნაშრომში გამოკვეთილი არასახელმწიფოებრივი სუბიექტების გაზრდილ როლს კიბერუსაფრთხოების სფეროში.

ნეოლიბერალიზმის თეორია - კლასიფიკაციის მიხედვით, ნეოლიბერალიზმი პოზიტივისტური თეორიების რიცხვს განეკუთვნება - ლიბერალიზმი, იდეალიზმი, ლიბერალური ინტერნაციონალიზმი და ასე შემდეგ.

ლიბერალიზმის აღმავლობა დაკავშირებულია პირველი მსოფლიო ომის შემდგომ პერიოდთან, როგორც პასუხი სახელმწიფოების უმოქმედობაზე ომის წინააღმდეგ საერთაშორისო ურთიერთობებში. ადრეული მიმდევრები - ვუდრო ვილსონი და ნორმან ენჯელი ომს მიიჩნევდნენ, როგორც უსარგებლოს მისი ყველა მონაწილისთვის. მათი აზრით, სახელმწიფოები თანამშრომლობის დროს მეტს იგებენ, ვიდრე ომის დროს. ლიბერალიზმი არ ითვლებოდა თანმიმდევრულ თეორიად, სანამ ედვარდ ქარმა არ მოაქცია იგი ტერმინ „იდეალიზმის“ ჩარჩოში. საერთაშორისო უსაფრთხოების თვალსაზრისით კი ჩამოყალიბდა სხვადასხვა ზომებისა და ღონისძიებების კომპლექსი, რომელიც, ასე თუ ისე, უზრუნველყოფს დედმიწაზე ერთობლივ ცხოვრებასა და უსაფრთხოებას, საერთაშორისო და ეროვნული უსაფრთხოება უცვლელ კავშირშია ერთმანეთთან, მაგრამ ფაქტია, სახელმწიფოებს შორის მაინც მიმდინარეობს როგორც სამხედრო ომები, ისე კიბერომები.

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. თავიანთი დამოუკიდებლობისა და უსაფრთხოების შესანარჩუნებლად სახელმწიფოები, ჩვეულებრივ, ერთად მოქმედებენ ხოლმე, 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 გარანტია საერთაშორისო სისტემაში, ამ სისტემის მდგრადობის ძირითადი პირობა.

ამ თეორიას ეთანხმება ვირტუალური ტექნოლოგიების არათანაბარი ინტეგრაციის ფაქტი სხვადასხვა სახელმწიფოთა მაგალითზე. გარდა ამისა, გამოკვეთილია თვალსაჩინო სხვაობა სამართლებრივი დარეგულირების მექანიზმებისა და კომპიუტერული ტექნოლოგიების განვითარების ტემპებს შორის.

რიჩარდ კოენის „კოლექტიური უსაფრთხოების“ თეორია - რიჩარდ კოენის უსაფრთხოების მოდელის თანახმად, საერთაშორისო უსაფრთხოების თვალსაზრისით, არსებობს ორ კონცეფცია - კოლექტიური უსაფრთხოება და კოლექტიური თავდაცვა. ამას ემატება ორი კომპონენტი, რომელიც მოიცავს ინდივიდუალურ უსაფრთხოებასა და სტაბილურობის შენარჩუნებას. ამ კომპონენტების დამატების აუცილებლობა განაპირობა ახალმა საფრთხეებმა - ტერორიზმი, კიბერტერორიზმი და ასე შემდეგ. თეორიის მიხედვით განხილულია კიბერუსფართხოების უზრუნველყოფის ეფექტიანობა კოლექტიური უსაფრთხოების სტრატეგიის შესაბამისად.

თემის დამუშავების დროს გამოყენებული მეთოდები

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

თვისობრივი კვლევის მეთოდები:

- **ნარატიული და დესკრიფციული,** რომელიც ითვალისწინებს თხრობით, მოთხრობით წყაროებს, მაგალითად: ისტორიის, დღიურების, ბიოგრაფიების, მემუარებისა და აღწერითს. აღნიშნული მეთოდი დაგვეხმარა ნაშრომში არსებული მასალების, წყაროების წარმოსადგენად.
- **სიღრმისეული ინტერვიუ** - ინტერვიუს სახეობა, ნაწილობრივ სტრუქტურირებული ინტერვიუ, რომელიც აგებულია ინტერვიუერთა

მოსაზრებების საფუძველზე. მეთოდი დაგვეხმარა ექსპერტებთან ინტერვიუების ჩაწერისას.

- **ფოკუს ჯგუფი (ფოკუსირებული დისკუსია)** - ეს არის ჯგუფური ინტერვიუს მეთოდი, რომლის დროს ერთდროულად რამდენიმე რესპონდენტს ვესაუბრებით, ეს მეთოდი გამოვიყენეთ 2008 წლის რუსეთ-საქართველოს ომისა და კიბერთავდასხმის ჯგუფური დისკუსიის დროს, რომელი კვლევაც ჩავატარეთ ბაკალავრის და მაგისტრატურის სტუდენტებთან.
- **ისტორიულ აღწერილობითი მეთოდი** - ისტორიული რეალობისა და აწმყოს შესწავლა-ანალიზი. დაგვეხმარა ისტორიული ფაქტების ანალიზში.
- **დისკუსიის ანალიზი** - ეს მეთოდი გამოვიყენეთ სატელევიზიო დისკუსიის განხილვა- გაანალიზებაში.

რაოდენობრივი კვლევის მეთოდები:

- **შინაარსის ანალიზი - Content-analyze** მეთოდი, რომელიც დაკავშირებულია მედიის მიერ გავრცელებული ინფორმაციის შესწავლასთან. აღნიშნული მეთოდი დაგვეხმარა ქართული და უცხოური მედიით გავრცელებული ინფორმაციის ანალიზში.
- **ივენტ-ანალიზის მეთოდი** - პოლიტიკური რეალობის შესწავლა. მეთოდი გამოიყენება პოლიტიკოსების ურთიერთქმედების დინამიკის გასაანალიზებლად.
- **პოლიტიკის კვლევის ანალიზი** - მეთოდი გამოვიყენეთ პოლიტიკურ მოვლენათა შეფასებაში, შესწავლასა და გაანალიზებაში.

ლიტერატურის მიმოხილვა

1. **კიბერთავდაცვა, კიბერსივრცის მთავარი მოთამაშეები - კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები. ვლადიმერ სვანიძე, ანდრია გოცირიძე ნაშრომების და სტატიების კრებული; სსიპ კიბერუსაფრთხოების ბიურო, საქართველოს თავდაცვის სამინისტრო,**

თბილისი, 2015. პირველი ქართულენოვანი კრებული, რომელშიც სრულყოფილადაა განხილული კიბერსივრცის თავისებურებები, საფრთხეები და გამოწვევები. ნაშრომში განხილულია საერთაშორისო კიბერუსართხოების სტრატეგიები ამერიკისა და ევროპის წამყვანი ქვეყნების მაგალითებზე და წარმოჩენილია საქართველოსა და პოსტ-საბჭოთა ქვეყნების ეროვნული უსაფრთხოების ასპექტები კიბერუსაფრთხოების საკითხებში.

2. **XXI საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების თეორია: მითი და რეალობა - რეგიონული და გლობალური ასპექტები“ - ვ. მაისაია, გ. მაღრაძე, გამომცებლობა „უნივერსალი“, თბილისი, 2017.** წიგნში ძირეულადაა განხილული, თუ 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 აქტორის მაგალითზე. მოყვანილია ჰიბრიდული საფრთხეების ჩამონათვალი და დეფინიცია და ხაზგასმულია ასიმეტრიული საფრთხეების მნიშვნელობა გლობალური უსაფრთხოების თვალსაზრისით. წიგნში აღწერილია კოლექტიური უსაფრთხოების თეორია და გაანალიზებულია თეორიის პრაქტიკული მაგალითები.
3. **სახელმძღვანელო - „კიბერდრაკონი - ჩინეთის საინფორმაციო ომი და კიბეროპერაციები“. ავტორი გახლავთ მკვლევარი დეკანი ჩენგი. წიგნი გამოიცა 2017 წელს აშშ-ში.** განხილულია, თუ რა მეთოდებს ეყრდნობა ჩინეთი კიბერომისა და საინფორმაციო ომის დროს. ასევე, დეტალურადაა ახსნილი, თუ რა მოსაზრებებით დაიწყო ჩინეთის ხელისუფლებამ ახალი ტექნოლოგიების ათვისება-წარმოება და გამოყენება.
4. **„კიბეროპერაციები, მშენებლობა, დაცვა და თავდასხმა, თანამედროვე კომპიუტერული ქსელები“. ავტორი გახლავთ მაიკ ოლილე. გამოიცა მათემატიკის დეპარტამენტის მხარდაჭერით, აშშ-ში. 2015 წ.** წიგნში

პროფესიულ დონეზეა საუბარი კიბეროპერაციების მეთოდებზე, თავდასხმების ნაირსახეობებსა და თავდაცვით სისტემებზე. ასევე განხილულია, თუ როგორ მიმდინარეობს ტექნოლოგიური განვითარება და სისტემების მშენებლობა.

5. **კნაფ კენეტის წიგნი - "კიბერუსაფრთხოება და ინფორმაციის გლობალური უზრუნველყოფა - საფრთხეების ანალიზისა და რეაგირების გადაწყვეტილებების შესახებ", რომელიც გამოქვეყნდა კოლორადოში, აშშ-ის საჰაერო ძალების აკადემიის მიერ, 2009 წ.** წიგნი საინტერესოა მეცნიერული თვალსაზრისით, სადაც გასაგებადაა ასახული კიბერუსაფრთხოება, როგორც თანამედროვე მსოფლიოს გადარჩენის შანსი. საუბარია, თუ რა დიდი მნიშვნელობა აქვს საფრთხეების ანალიზსა და რეაგირებას, ანუ გადაწყვეტილებების დროულ მიღებას.
6. **„ჰიბრიდული ომი და ევრო-ატლანტიკური სივრცის უსაფრთხოების ლანდშაფტის ცვლილება, პოლიტიკური და ეკონომიკური შედეგები“ - გრიგოლ მგალობლიშვილი, ბათუ ქუთელია, ირინა გურული, ნინო ევგენიძე; ეკონომიკური პოლიტიკის კვლევის ცენტრი, ფონდი „ღია საზოგადოება - საქართველო“. თბილისი, 2016.** ნაშრომი ეხება რუსეთის ფედერაციის პოლიტიკას ევრო-ატლანტიკურ ალიანსში გაწევრიანების სურვილის მქონე სახელმწიფოების მიმართ, საქართველოს მაგალითზე. განხილულია რუსეთის ამგვარი პოლიტიკური კურსის საინფორმაციო და ეკონომიკური შედეგები, როგორც ნატო-ს, ასევე საქართველოს შემთხვევაში.

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. რა გავლენა შეიძლება ჰქონდეს კიბერომს ნატოს წევრ და მის პარტნიორ ქვეყნებზე? ამ თემაზე ჩატარდა თბილისში თავდაცვისა და

უსაფრთხოების ფორუმი, რომელიც ჰიბრიდული ომის განხილვით დაიწყო. ატლანტიკური საბჭოს მკვლევარმა დოქტორმა, **არიელ კოენმა** საქართველოს ჰიბრიდული ომის მსხვერპლი უწოდა:

„ჰიბრიდული ომის საფრთხე ისტორიული გამოწვევაა. საჭიროა, ვისწავლოთ, თუ როგორ გავუმკლავდეთ მსგავს კრიზისებს.".[4]

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

ანალიტიკურ დოკუმენტში, რომელიც მომზადდა პროექტის „ეკონომიკური ნატო, საქართველოს ნატოში ინტეგრაციის ეკონომიკური პერსპექტივა“-ს ფარგლებში, ვკითხულობთ:

"ჰიბრიდული ომის, როგორც კონფლიქტის ახალი ფორმის აღმოცენება, ძირეულად ცვლის უსაფრთხოების არსებულ ლანდშაფტს და უამრავ კითხვას აჩენს არა მარტო იმ საფრთხეების ბუნების შესახებ, რომელთა წინაშეც ვდგავართ, არამედ უსაფრთხოების არსებული ინსტიტუტების შესაძლებლობების შესახებ, წინ აღუდგეს ამ საფრთხეებს. ეს უდავოდ

[4] https://mod.gov.ge/ge/news/read/4266/hibriduli-omi-da-misi-gavlena-natos-cevr-da-partnior-qveknebze, უკანასკნელად იქნა გადამოწმებული: 11.06.2020

მოახდენს მნიშვნელოვან გავლენას ნატოს გაფართოებასთან დაკავშირებით მიმდინარე დებატებზე“.[5]

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 საერთოდ წაშალა, ანუ ყველა სახის საფრთხე მოექცა ერთ სივრცეში. ამჟამად აღარ აქვს მნიშვნელობა, ტერაქტი საფრანგეთში განხორციელდება თუ იტალიაში, საფრთხის წინაშე მაინც დგება მთელი მსოფლიო. ამას კი მივყავართ როგორც კომპლექსურ კვლევებამდე, ასევე კომპლექსურ და პრაქტიკულ თანამშრომლობამდე, უფრო ფართო და მძლავრი ინფრასტრუქტურის შექმნამდე. რა როლი აკისრია საქართველოს საერთაშორისო უსაფრთხოების სფეროში? მაგალითად, ბერი სალოსის ქუჩაზე დატრიალებულმა ტრაგედიამ გვაჩვენა, რომ უკვე აღარ არსებობს დიდი და პატარა ქვეყნები, ტერორიზმი იბუდებს იქ, სადაც ხელსაყრელ პირობებს ნახულობს და არსებობს ე.წ. შავი ხვრელები. მართალია, საქართველოს საკუთარ თავზე არ გამოუცდია ტერორიზმის სიმწარე, მაგრამ რეალური საფრთხის წინაშე ნამდვილად იდგა. არც იმას აქვს მნიშვნელობა, ტერორისტები შენს ტერიტორიაზე განახორციელებენ თუ არა ტერაქტს - თუ შენს წიაღში შემოაღწიეს და დაიწყეს მომზადება სხვაგან უბედურების მოსაწყობად, ეს არ გვათავისუფლებს პასუხისმგებლობისგან. კვლევა ეყრდნობა ზემოთ განხილულ საკითხებს და ბუნებრივია, შედეგებიც შესწავლა-გაანალიზებიდან გამომდინარეობს.

[5] მგალობლიშვილი, გ., ქუთელია, ბ., გურული, ი., & ევგენიძე, ნ. (2016). *"ჰიბრიდული ომი და ევრო-ატლანტიკური სივრცის უსაფრთხოების ლანდშაფტის ცვლილება პოლიტიკური და ეკონომიკური შედეგები".* ეკონომიკური პოლიტიკის კვლევის ცენტრი (EPRC), 2016, დოკუმენტი №1, გვ. 9, მოპოვებული: http://old.infocenter.gov.ge/uploads/files/2016-08/1471530452_hybrid-warfare-report-geo_web.pdf-დან, უკანასკნელად იქნა გადამოწმებული: 11.06.2020

თეორიული ჩარჩო

მოცემული კვლევის ძირითად ამხსნელს წარმოადგენს კიბერომის, ჰიბრიდული ომის, საინფორმაციო ომის წარმოების თეორია. განხილულია საქართველოს, ბალტიისპირეთის ქვეყნების, უკრაინის, ევროკავშირის, ნატოს, აშშ-ის კიბერომების მოდელები და თეორიული ასპექტები. რუსეთის კიბერშესაძლებლობები, საერთაშორისო და ქართული კანონმდებლობა, თანამშრომლობის პრობლემატიკა. ყურადღება გამახვილებულია უსაფრთხოების თეორიის მნიშვნელობასა და მიმართულებაზე.

აღნიშნული თეორია, როგორც პროფესორი **ვახტანგ მაისაია** აღნიშნავს თავის წიგნში („21-ე საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების თეორია“: მითი და რეალობა - რეგიონული და გლობალური ასპექტები“), უსაფრთხოება გლობალიზირებული სამყაროში გახდა კომპლექსური, მრავალწახნაგოვანი და მრავალფეროვანი, თვით პოლიტიკურ ლექსიკონში შემოვიდა ტერმინი „უსაფრთხოების კომპლექსი“.

ნაშრომში წარმოდგენილია სოციოლოგიური კვლევა სიღრმისეული ინტერვიუების სახით. ასევე კიბერუსაფრთხოების ფენომენი, როგორც ახალი მოვლენა. კვლევაში მონაწილეობა მიიღეს ქართველმა ექსპერტებმა და ანალიტიკოსებმა. შემდეგი კვლევა ჩატარებულია დისკუსიის მეთოდით, რომელშიც მონაწილეობდნენ კავკასიის საერთაშორისო უნივერსიტეტის ბაკალავრიატისა და მაგისტრატურის სტუდენტები. სადისერტაციო ნაშრომში წარმოდგენილია სატელევიზიო დისკუსიის გარჩევა-ანალიზი, სადაც საუბარია საინფორმაციო ომის ელემენტებზე ქართულ სინამდვილეში.

წინამდებარე ნაშრომი ასევე მიმოიხილავს ქართველ ექსპერტთა მიერ შემუშავებულ თეორიულ ჩარჩოს. ავტორთა დიდი უმრავლესობა თანხმდება იმაზე, რომ კიბერომი არის ახალი ტიპის დიდი საშიშროება ვირტუალურ სამყაროში, რომელიც ასევე მნიშვნელოვან გავლენას ახდენს რეალურ სამყაროზე და დაუყოვნებლივ საჭიროებს უსაფრთხოების უფრო მოქნილი

სტრატეგიის შემუშავებას, თეორიული რეკომენდაციების დაზუსტებას თანამედროვე ტექნოლოგიების დანერგვის მიზნით.[6]

ჰიბრიდული ომის თეორია - პროფესორი **ბესო ალადაშვილი** ჰიბრიდული ომის საინტერესო განმარტებას იძლევა:

„ჰიბრიდული ომი - ეს არის ომი მართვადი ქაოსის მეშვეობით, რომლის ერთ-ერთი მთავარი შემადგენელია საინფორმაციო ომი, მოწინააღმდეგის სრული დემორალიზების მიზნით. სწორედ საინფორმაციო ომის კომპონენტის არსებობა წარმოადგენს ე.წ. „მეოთხე თაობის ომის“ კონცენფციის შემადგენელ ნაწილს. თავის მხრივ კი, საინფორმაციო ომის ერთ-ერთ ნაირსახეობას შეადგენს კიბერომის თეორია“.[7]

ამ მხრივ საინტერესოა ამერიკის თავდაცვის დეპარტამენტის ყოფილი თანამშრომლის, ვიცე-პოლკოვნიკ **ნათან ფრაიერის** მოსაზრებები, რაც ფაქტობრივად წარმოადგენს კიბერომის თეორიას. ფრაიერი აშშ-ის ეროვნული თავდაცვის სტრატეგიაზე მუშაობისას მონაწილეობდა 2006 წლის **„Quadrennial Defense Review Report“**-ის მომზადებაში, სადაც მისი თაოსნობით მოცემული იქნა საფრთხეების დიაგრამა. მასში მოცემულია ის საფრთხეები, რომელიც აშშ-ს უახლოეს მომავალში დაემუქრებოდა და შედგება ტრადიციული, არატრადიციული, კატასტროფული ტერორიზმის და სხვა დესტრუქციული საფრთხეებისგან. **ფრენკ ჰოფმანმა,** რომელიც აშშ-ის ეროვნული თავდაცვის უნივერსიტეტში მოღვაწეობს, 2007 წელს გამოაქვეყნა სტატია („კონფლიქტი 21-ე საუკუნეში - ჰიბრიდული ომის აღმასვლა“). ამ ნაშრომის მიხედვით, აშშ-ს ბრძოლა მოუწევს ისეთ ოპონენტებთან, რომლებიც არა მხოლოდ არატრადიციული ან ტრადიციული ფორმით იომებენ, ან ტერორისტები არიან, არამედ შეძლებენ ერთდროულად ყველა

---

[6] მაისაია, ვ., & მაღრაძე, გ. *„21-ე საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების თეორია“: მითი და რეალობა - რეგიონული და გლობალური ასპექტები“.* თბილისი, საქართველო: უნივერსალი, 2017, გვ. 14-193.

[7] მაისაია, ვ. „ჰიბრიდული ომის“ რაობა და მისი გეოსტრატეგიული ასპექტები (მეოთხე თაობის ომი) - კიბერომის მაგალითზე". *The Georgian Times*, 2017 წლის 30, 03. გვ 1. მოპოვებული http://geotimes.com.ge/blogi/?m=82&post_id=10-დან, უკანასკნელად იქნა გადამოწმებული: 11.06.2020

ამ მეთოდისა და საშუალების გამოყენებას. ჰოფმანი აღნიშნავს, რომ ისტორიაში არის მაგალითები, როდესაც არატრადიციული და ტრადიციული ტაქტიკები ერთდროულად, კომბინირებულად გამოიყენებოდა, მაგრამ თანამედროვე ტექნოლოგიურმა განვითარებამ ომის წარმოება იმდაგვარად შეცვალა, რომ იგი წარმოგვიდგება როგორც ჰიბრიდული საფრთხე.[8]

და ბოლოს, სადისერტაციო ნაშრომში წარმოდგენილი მასალები და გამოვლენილი ტენდენციები, მოსაზრებები, რეკომენდაციები, კვლევები, სავარაუდოდ, კიდევ უფრო შეავსებს მეცნიერულ ლიტერატურას სახელმწიფო უსაფრთხოების თვალსაზრისით.

დისერტაციის სტრუქტურა

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

[8] ანთაძე, გ. "*ჰიბრიდული ომის თეორია და რუსული პრაქტიკა".* 2019.07.12. გვ. 1, მოპოვებული "საზოგადოებრივი მაუწყებელი": https://1tv.ge/video/hibriduli-omis-teoria-da-rusuli-praqtika/-დან, უკანასკნელად იქნა გადამოწმებული: 11.06.2020

თავი I. კიბერომის არსი და ისტორიული მიმოხილვა

კაცობრიობას თავის დამშვიდების უფლება არ აქვს - რაც უფრო მეტ სიმაღლეებზე ავა კომპიუტერული ტექნოლოგიები, მით მეტი საშიშროება შეიქმნება კიბერტერორისტების მხრიდან. იხვეწება ტექნოლოგიები? იხვეწება კიბერომის, ტერორიზმის და საინფორმაციო ომის მეთოდებიც. ესეც ჩვეულებრივი ომია, მეცნიერები სწავლობენ ტერორისტების "მიღწევებს" და ასევე ტერორისტები სწავლობენ მეცნიერების მიღწევებს. 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 - ვიცით, ახორციელებდა რუსეთი საქართველოს წინააღმდეგ სამხედრო და კიბერომის შერწყმულ თავდასხმებს. კრემლს საბჭოთა მეთოდოლოგია არ შეუცვლია, შეცვალა მხოლოდ ტექნოლოგიები. პენტაგონის განმარტებით, ინტერნეტსივრცე ისეთივე ბრძოლის ველი ხდება, როგორც ხმელეთი, ზღვა, ცა და კოსმოსი. 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.

მსოფლიო საჭიროებს უსაფრთხოების მექანიზმების მზარდ მოდერნიზებას, კიბერსივრცეში არსებული საფრთხეების, რისკებისა და გამოწვევების დონე საკმაოდ მაღალია. ყველა ქვეყანა ცდილობს, დამოუკიდებლად დაიცვას თავი, ნაწილობრივ ასეც უნდა იყოს, ნებისმიერ სახელმწიფოს უნდა ჰქონდეს საკუთარი ბაზა, თუმცა გატარებული ზომები და ღონისძიებები ხშირად საკმარისი არ არის. კიბერუსაფრთხოების საკითხებში მნიშვნელოვანია საერთაშორისო ორგანიზაციების ჩართვა, მათ მიერ ერთიანი სტრატეგიული დოკუმენტებისა და თავდაცვის მექნიზმების შემუშავება.

ამერიკასა და რუსეთს შორის საინფორმაციო ომს ხანგრძლივი ისტორია აქვს. მიმომხილველები ხშირად იხსენებენ პრეზიდენტ **რეიგანის** მმართველობის პერიოდს. დროს, როდესაც ინფორმაცია ეროვნული უსაფრთხოების სტრატეგიის ერთ-ერთ უმნიშვნელოვანეს ნაწილად იქცა.

სეტ ჯონსი, "სტრატეგიული და საერთაშორისო კვლევების ცენტრის" უსაფრთხოების პროგრამის უფროსი მრჩეველი ამბობს, რომ თუკი მაშინდელ დოკუმენტებს გადავხედავთ და სიტყვა "საბჭოთას" - "რუსეთით" ჩავანაცვლებთ, შეიძლება გაგვიჭირდეს კიდეც იმის განსხვავება, თუ ისტორიის რომელი პერიოდის შესახებაა საუბარი.

"რონალდ რეიგანმა ბევრ სხვა ღონისძიებასთან ერთად, შექმნა სააგენტოთაშორისი სამუშაო ჯგუფი, რომლის მიზანიც სწორედ ის იყო, რომ მოეყარა თავი დაზვერვის სხვადასხვა წყაროს ინორმაციისთვის და გამოევლინა საბჭოთა ხელისუფლების მავნე ქმედებები მთელ მსოფლიოში", - ამბობს ჯონსი და იქვე დასძენს, რომ მნიშვნელოვანი იყო საზოგადოების ინფორმირების ნაწილიც. სწორედ ამიტომ ამ ჯგუფს საჯაროდ უნდა აეხსნა რას და რატომ აკეთებდა.[9]

საქართველოს სახელმწიფო უსაფრთხოების სამსახურის 2019 წლის ანგარიშში ოფიციალურად არის ნათქვამი, რომ ჩვენს ქვეყანაში გავლენის გაძლიერებით დაინტერესებული ქვეყნები საკუთარი მიზნების მისაღწევად აქტიურად იყენებდნენ ჰიბრიდული ომის მეთოდებს. რა მეთოდებზეა საუბარი, რა სახის ხერხებს იყენებენ უცხო ქვეყნების სპეცსამსახურები, რა მიზანი ამოძრავებთ მათ? ისინი მიზნად ისახავდნენ და ისახავენ საქართველოში მცხოვრები სხვადასხვა ეთნიკური და რელიგიური ჯგუფების დაპირისპირებას, მოსახლეობაში ანტიდასავლური განწყობების გაღვივებას, საქართველოს ორმხრივი ურთიერთობების გაუარესებას

[9] ჯონსი, ს. *"საინფორმაციო ომის გაკვეთილები საქართველოსა და დასავლეთისთვის".* 2018.15.06. გვ. 1. მოპოვებული amerikiskhma.com: https://www.amerikiskhma.com/a/georgia-is-a-laboratory-of-how-russian-active-measures-work/4440995.html-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020

რეგიონის ქვეყნებსა და სტრატეგიულ პარტნიორებთან, საქართველოს, როგორც დემოკრატიული და სტაბილური ქვეყნის იმიჯის შელახვას, ეკონომიკური ზეგავლენის ბერკეტების მოპოვებას, მუდმივი შიდაპოლიტიკური დაძაბულობის ხელშეწყობას, საზოგადოებაში გაურკვევლობისა და ნიჰილიზმის დანერგვას. ამ მიზნების განსახორციელებლად კი აქტიურად ხდება არა მხოლოდ დესტრუქციული პოლიტიკური ძალების, არამედ მედიასაშუალებებისა და სოციალური ქსელების გამოყენება. ჰიბრიდული ომის მნიშვნელოვან ინსტრუმენტს წარმოადგენს დეზინფორმაციული კამპანია, ყალბი ახალი ამბები, მცდარი შეხედულებებისა და შიშის გავრცელება, საზოგადოებრივ აზრზე მანიპულირებით მნიშვნელოვან პროცესებზე გავლენის მოხდენა.

საქართველოსთვის მნიშვნელოვან რისკს წარმოადგენს უცხო სახელმწიფოების სპეცსამსახურებისა და მათ მიერ კონტროლირებადი ჰაკერული ჯგუფების მიერ სამთავრობო და კრიტიკული ინფრასტრუქტურის ობიექტებზე კიბერშეტევებისა თუ კიბერსადაზვერვო ოპერაციების განხორციელება. მტერი ცდილობს, დაყოს კავკასია და იბატონოს. დაყოფილ-დაშლილი კავკასია დიდი პრობლემა ხდება როგორც ნატოსთვის, ისე ევროკავშირისთვის. ამ შემთხვევაში რუსეთი იჭერს რამდენიმე კურდღელს: **პირველი** - პოლიტიკური თვალსაზრისით შლის ამიერკავკასიას, **მეორე** - ეკონომიკურად ასუსტებს სამივე რესპუბლიკას, **მესამე** - კავკასიას აქცევს საფრთხის შემცველ რეგიონად, სამივე სახელმწიფოში მინიმუმამდე მცირდება ინვესტიციების მოზიდვის შანსი და კვდება ტურიზმი.

სად არის გამოსავალი? საქართველოსთვის, უსაფრთხოების თვალსაზრისით, კვლავაც გასაძლიერებელია ნატოსთან და წამყვან სახელმწიფოებთან თანამშრომლობა. შესასწავლია უცხოეთის ქვეყნების გამოცდილება და ასევე ასათვისებელია ტექნოლოგიებიც.

განვითარებული ტექნოლოგიების წყალობით დღევანდელი მსოფლიო ცხოვრობს უწყვეტი ფსიქოლოგიური ომის პირობებში. მეცნიერებისა და

პრაქტიკოსი სპეციალისტების თავსატეხად იქცა ე.წ. ინტერნეტქაოსის მართვა, დახარისხება, დალაგება, თეორიული კონცეფციების შემუშავება, უსაფრთხოების სისტემების ამოქმედება, ყველა საკითხის გაშიფრვა, ყველა მოვლენისთვის თავისი სახელის დარქმევა. ჩვენს მიერ ჩატარებული კვლევისა და მოპოვებული ინფორმაციის თანახმად, კიბერომი, კიბერთავდასხმა ტექნიკური თვალსაზრისით (როგორც სტრუქტურა), ასე გამოიყურება:

კიბერშეტევა არის კომპიუტერული ინფორმაციული სისტემების, ინფრასტრუქტურების, კომპიუტერული ქსელების ან პერსონალური კომპიუტერის მოწყობილობების სხვადასხვა მეთოდების გამოყენებით მონაცემების ან ინფორმაციის სისტემების მოპარვა, შეცვლა ან განადგურება.

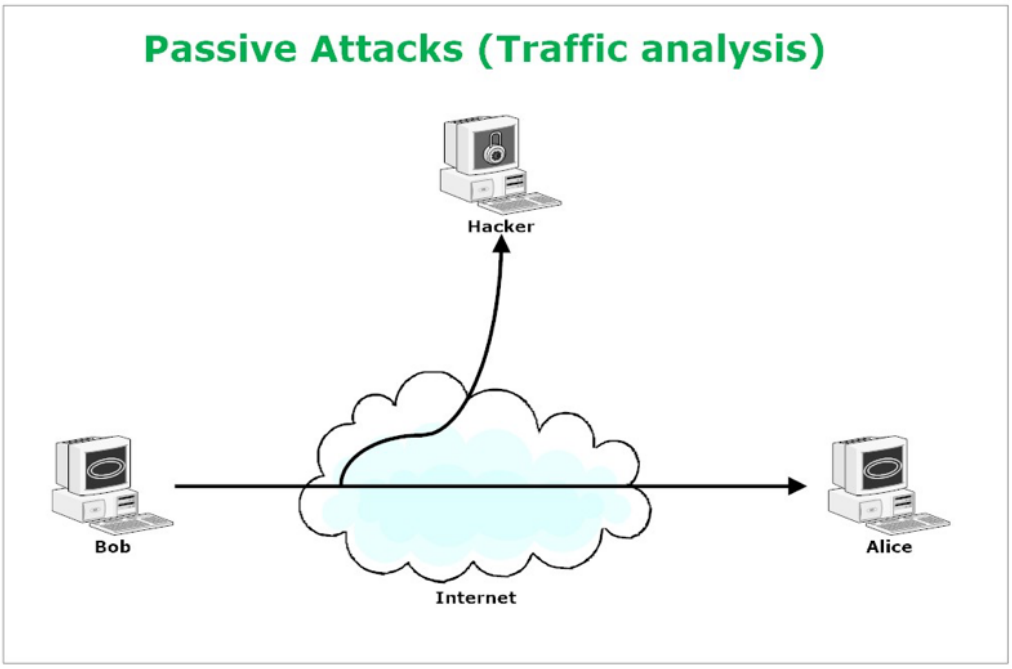
ყველაზე გავრცელებული კიბერშეტევების ტიპებია:

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
2. Man-in-the-middle (MitM) attack
3. Phishing and spear phishing attacks
4. Drive-by attack
5. Password attack
6. SQL injection attack
7. Cross-site scripting (XSS) attack
8. Eavesdropping attack
9. Birthday attack
10. Malware attack

არსებობს პასიური და აქტიური შეტევები:

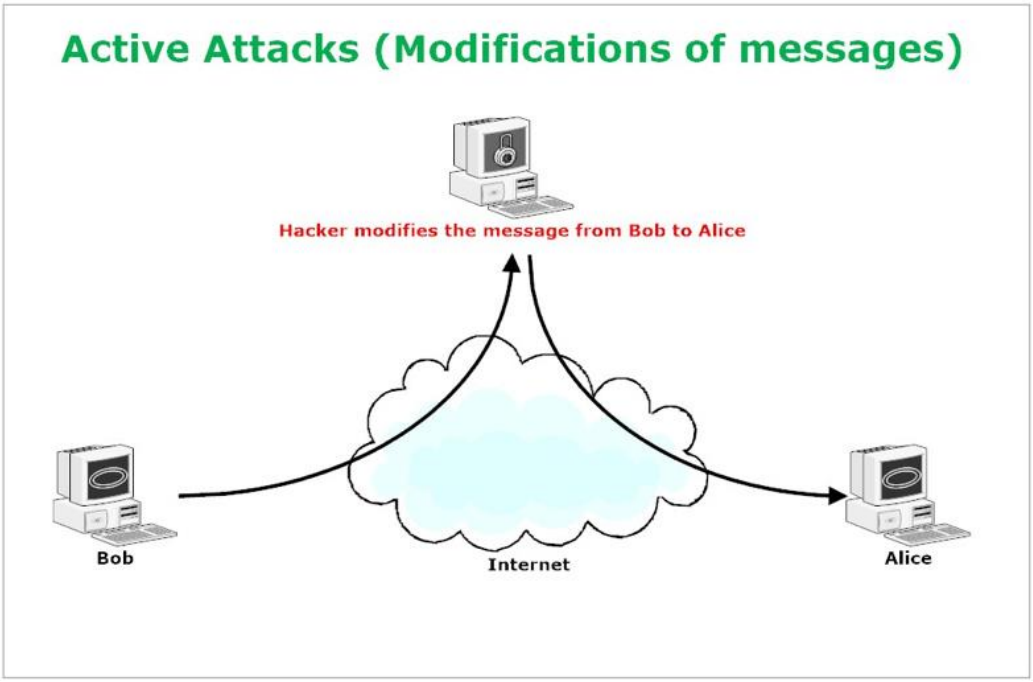
Passive Attack - პასიური შეტევა: ამ დროს ხდება ქსელების დაუცველი ტრაფიკის მონიტორინგი, რათა იპოვონ, ამოიღონ ინფორმაცია და პაროლები, ეს დაეხმარებათ სხვა ტიპის კიბერშეტევებისთვის. პასიური შეტევა გულისხმობს ტრაფიკის ანალიზს და დაუცველი კომუნიკაციების მონიტორინგს.

Active Attack - აქტიური შეტევა: ამ დროს ჰაკერი დაცულ სისტემებს უტევს. ეს უმეტესწილად ვირუსებით ხორციელდება. აქტიური შეტევს დროს ჰაკერი ცდილობს, დააზიანოს backbone-ი, ანუ ქსელის ხერხემალი და ახორციელებს სატრანზიტო ინფორმაციის გამოყენებას ან ავტორიზებულ მომხმარებელზე დისტანციურ თავდასხმას.



ფიგურა 1

პასიური კიბერშეტევები, წყარო: *https://www.venafi.com/blog/what-active-attack-vs-passive-attack-using-encryption, 2019 წ.*

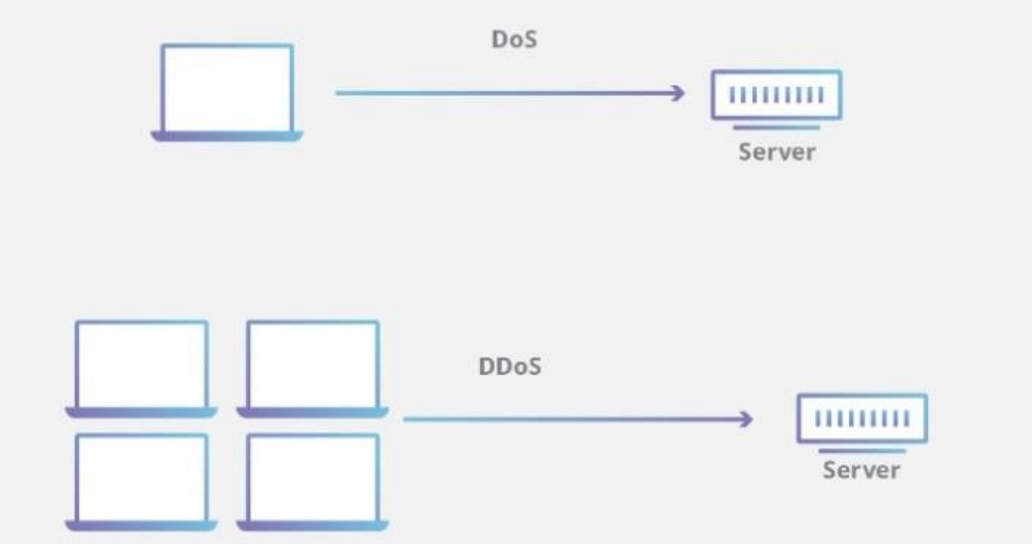


ფიგურა 2

აქტიური კიბერშეტევები, წყარო: https://www.venafi.com/blog/what-active-attack-vs-passive-attack-using-encryption, 2019 წ.

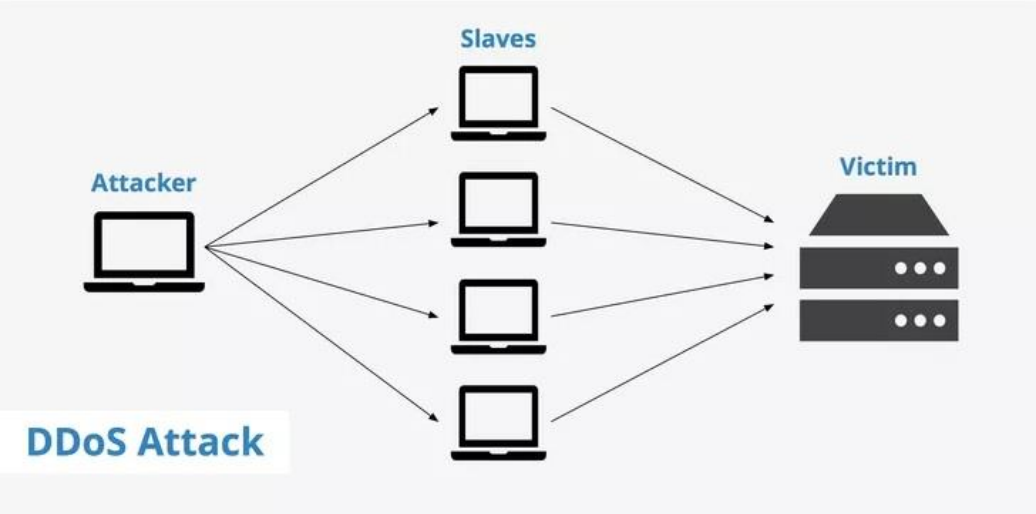
Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

DoS კიბერშეტევა არის სპეციფიკური ტიპის შეტევა, რომლის მიზანია დიდი ვებ-გვერდების დაჰაკვა. 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, ხოლო **DDoS** შეტევის დროს რამდენიმე ჰაკერი ან გატეხილი სისტემა აკეთებს ბევრ მოთხოვნას ვებ-სერვერზე და გამოუსადეგარი ტრაფიკით ბლოკავს სერვისს. ამ შეტევის დროს ჰაკერს პირველ რიგში უნდა ჰქონდეს დიდი რაოდენობის ინტ-ჰოსტებთან წვდომა. შემდეგ ხორციელდება შემტევი პროგრამების დაყენება. **DDoS** კოორდინირებულ შეტევას დიდი ზიანის მოტანა შეუძლია.



ფიგურა 3

Dos და DDos თავდასხმები სერვერზე, წყარო:
https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/



ფიგურა 4

DDoS შეტევები, თავდამსხმელი, შეტევის ხელსაწყოები, შეტევის სამიზნე, წყარო:
https://www.keycdn.com/support/ddos-attack

არსებობს სხვადასხვა ტიპის DoS და DDoS შეტევები:

ყველაზე გავრცელებულია **TCP SYN flood attack, Teardrop attack, Smurf attack, Ping of death attack** და **Botnets.**

TCP SYN flood attack - წყალდიდობის შეტევა:

ამ შეტევის დროს თავდამსხმელი იყენებს ბუფერულ სივრცეს, გადაცემის კონტროლის პროტოკოლის სესიის დანიშვნის ინიციალიზაციის დროს. **(TCP)** არის ერთერთი მთავარი მონაცემთა გადაცემის პროტოკოლი,

რომელიც შექმნილია მონაცემთა გადაცემის გასაკონტროლებლად). ამ დროს მთლიანად ივსება სივრცე და როდესაც სისტემა ლეგიტიმურ მოთხოვნას პასუხობს, სისტემას აზიანებს, რაც საბოლოო ჯამში გამოუსადეგარს ხდის.

Teardrop attack - ცრემლსადენი შეტევა:

ეს შეტევა იწვევს **(IP)** ინტერნეტ პროტოკოლის ფრაგმენტაციის დროს ოფსეტური ველების ერთმანეთში არევას. ამ დროს დაზიანებული სისტემა ცდილობს რეკონსტრუქციას, მაგრამ ამას ვერ ახერხებს, სისტემაში ყველაფერი ირევა და იშლება.

ამ შეტევებისგან რამდენიმე თავდაცვითი საშუალება არსებობს, რომელიც ტექნიკურ საკითხს წარმოადგენს. თუ შეტევების სამიზნე მომხმარებლებს არ აქვთ საშუალება **DoS ან DDoS** შეტევებისგან თავდაცვისა, მაშინ საჭიროა SMBv2-ის გამორთვა და პორტების დაბლოკვა - **139** და **445.**

Smurf - შეტევა:

კიბერშეტევა, რომლის დროსაც ჰაკერი აგზავნის **IP** პინგის მოთხოვნებს მიმღებ ვებ-გვერდზე. შედეგად ვებ-გვერდი იღებს ბევრ პასუხებს, რომლებსაც სწორად და სწრაფად ვერ ამუშავებს. ამ დროს, დიდი ალბათობით, ქსელის მთავარი კომპიუტერი მწყობრიდან გამოვა.

Ping of death attack - პინგს სიკვდილის შეტევა:

აღნიშნული შეტევის დროს **IP** პაკეტებს იყენებენ ზომით **- 65.535 ბაიტი,** რაც დაუშვებელია სისტემის დასახელების მიზნით.

ამ შეტევების შეჩერება შესაძლებელია **firewall**-ის საშუალებით, იგი შეამოწმებს ფრაგმენტულ **IP** პაკეტებს მაქსიმალური სიზუსტით და ზომით.

Botnets - ბოტნეტები:

ეს არის ჰაკერების კონტროლის ქვეშ დაინფიცირებული მილიონობით სისტემა, რათა **DDoS** შეტევები იქნეს განხორციელებული. ბოტები ან დაზომბირებული სისტემები გამოიყენება სამიზნე სისტემების წინააღმდეგ, თავდასხმისთვის. ის ხშირად აჭარბებს სამიზნე სისტემების სიჩქარეს და დამუშავების შესაძლებლობებს. ასეთი **DDoS** შეტევების მოძიება რთულია, რადგან ბოტნეტები ერთ ადგილზე არ მუშაობენ, სხვადასხვა გეოგრაფიულ ადგილებში არიან განთავსებულნი.

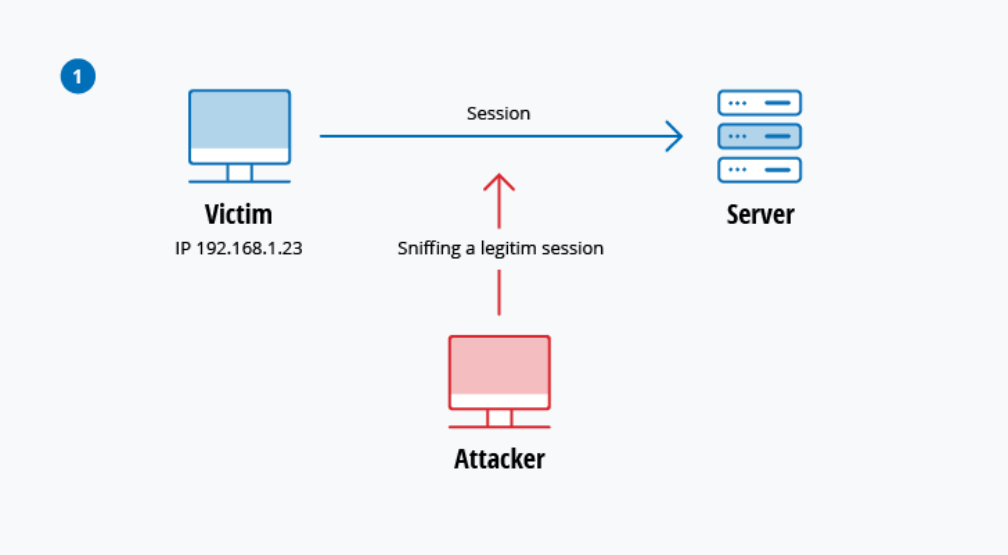
Botnets შეტევების შემსუბუქება შემდეგნაირად არის შესაძლებელი:

RFC3704-ის გაფილტვრა, რომელიც უარს ეტყვის აქტივობას გაფუჭებული მისამართებიდან და ხელს შეუწყობს ტრეფიკის მიწოდებას. მაგალითად, **RFC3704** ფილტრაცია ჩამოაგდებს პაკეტებს ბოგონის სიის მისამართებიდან.

შავი ხვრელის გაფილტვრა, რომელიც არასასურველ ტრაფიკს უშვებს დაცულ ქსელში შესვლამდე. როდესაც **DDoS** შეტევა გამოვლენილია, **BGP** (სასაზღვრო კარიბჭის პროტოკოლი) მასპინძელმა უნდა გაგზავნოს მარშრუტიზაციის განახლებები **ISP** მარშრუტიზატორებზე, რათა ყველა ტრაფიკისკენ გაემართონ დაზიანებულ სერვერებზე, **null0** ინტერფეისზე და შემდეგ მთავარ სისტემაზე.

Man-in-the-middle (MitM) attack - შუაში შეტევა:

აღნიშნული შეტევითი ტექნიკა იყენებს **TCP/IP** პროტოკოლის არქიტექტურაში არსებულ სისუსტეებს. როდესაც ვიღაც ერევა და აკონტროლებს თქვენი კომუნიკაციის პროცესს, ხდება ამგვარი კიბერთავდასხმა. თუ კომპიუტერები ურთიერთობენ ქსელის დაბალ დონეებზე, შეიძლება ვერ დაადგინონ, ვისთან ცვლიან მონაცემებს. თქვენ გგონიათ, ესაუბრებით ნაცნობ ადამიანს, მაგრამ ამ დროს, ყველა თქვენს პირად ინფორმაციას ხედავს ჰაკერი. **მაგალითი:**

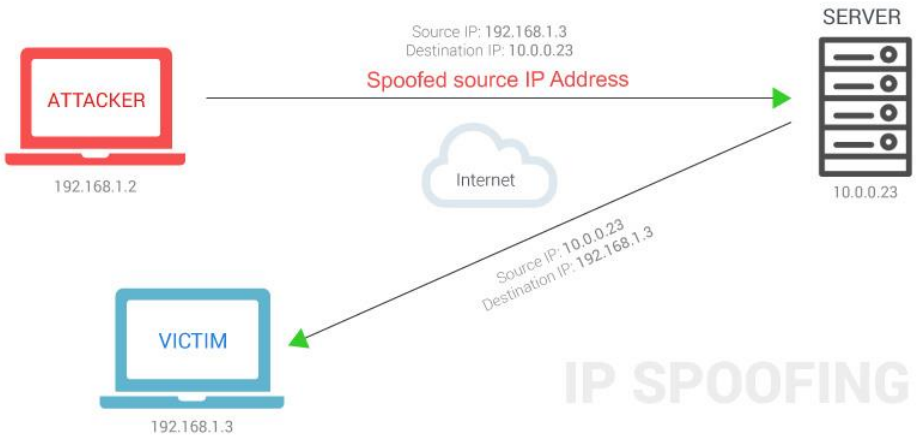


ფიგურა 5

***Man-in-the-middle** შეტევა, თავდამსმელი, მომხმარებელი და სერვერი, წყარო:*
https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

IP Spoofing attack - გამფუჭებელი, შეურაცხმყოფელი შეტევა:

თავდამსხმელი იყენებს **IP Spoofing**-ს სისტემის მოსატყუებლად. ის ცდილობს, სისტემა დაარწმუნოს, რომ კომუნიკაციას ამყარებს ახლობელ, სანდო პირთან, ამ დროს თავდამსხმელს სისტემაზე ხელი მიუწვდება. თავდამსხმელი აგზავნის პაკეტს სანდო, ახლობელ **IP** მისამართით, საკუთარი **IP** მისამართის ნაცვლად, თუ სამიზნე მიიღებს ამ პაკეტს, ეს იმოქმედებს მასზე.

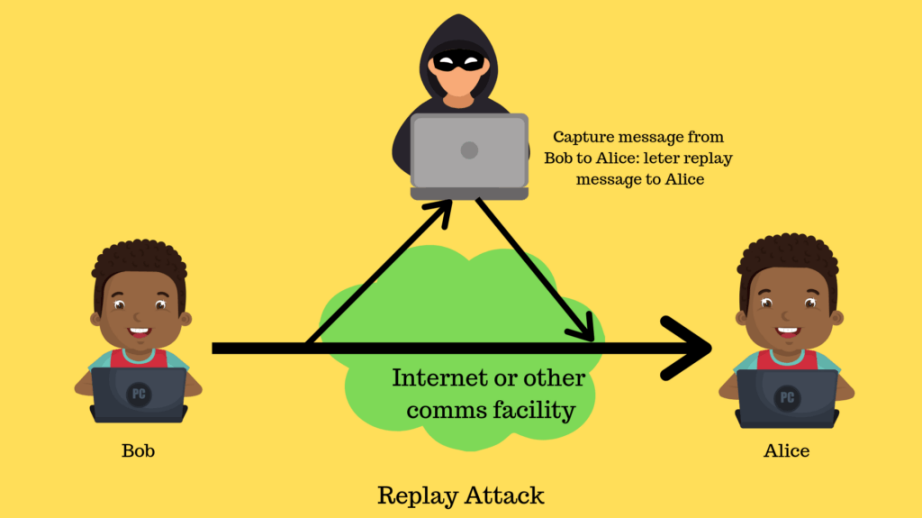


ფიგურა 6

IP Spoofing შეტევები, თავდამსმელი ახორციელებს სერვერზე შეტევასდა სერვერიდან მომხმარებელზე, წყარო: https://www.cyberpunk.rs/whats-spoofing-and-how-to-defend-against-it

Replay - გამეორება:

ეს კიბერშეტევა ხდება მაშინ, როდესაც თავდამსხმელი ინახავს ძველ მესიჯებს და შემდეგ ცდილობს, მოგვიანებით გააგზავნოს. ამჟამად არ არსებობს ერთი ტექნოლოგია და კონფიგურაცია, რომ არ მოხდეს ყველა **MitM** შეტევა. ზოგადად, დაშიფვრა **MitM** შეტევებისგან იძლევა ეფექტურ დაცვას, რაც უზრუნველყოფს კომუნიკაციების საიდუმლოებასა და მთლიანობას, მაგრამ შეიძლება თავდასხმა მოხდეს საკომუნიკაციო სისტემის შუაში ისე, რომ დაშიფრვა ვერაფერს იზამს.



ფიგურა 7

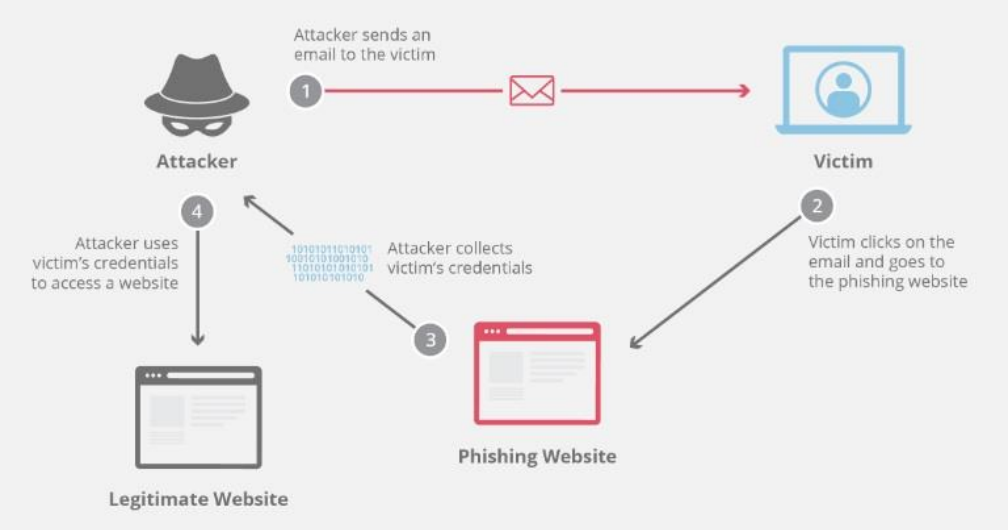
Replay შეტევა, ჰაკერი ერევა კონტაქტში და ახორციელებს კიბერშეტევას, წყარო: https://thecoderzone.com/security-attacks-in-network-security/

Phishing and spear phishing attacks - ფიშინგისა და სათადარიგო ფიშინგის შეტევები

Phishing კიბერთავდასხმის დროს თავდამსხმელი ქმნის პოპულარული და რეალური ვებ-გვერდის კლონ ვებ-გვერდს, შემდეგ თავდამსხმელი უგზავნის წერილს მიზანში ამოღებულ მომხმარებელს, სადაც არის ყალბ ვებ-გვერდზე განთავსებული ბმული. როდესაც მომხმარებელი გადადის ამ ვებ-გვერდზე და შეიყვანს პირად მონაცემებს, ჰაკერი მიიღებს წვდომას ამ მონაცემებზე, ეს შეიძლება იყოს სოციალური ქსელების მომხმარებლის სახელები და

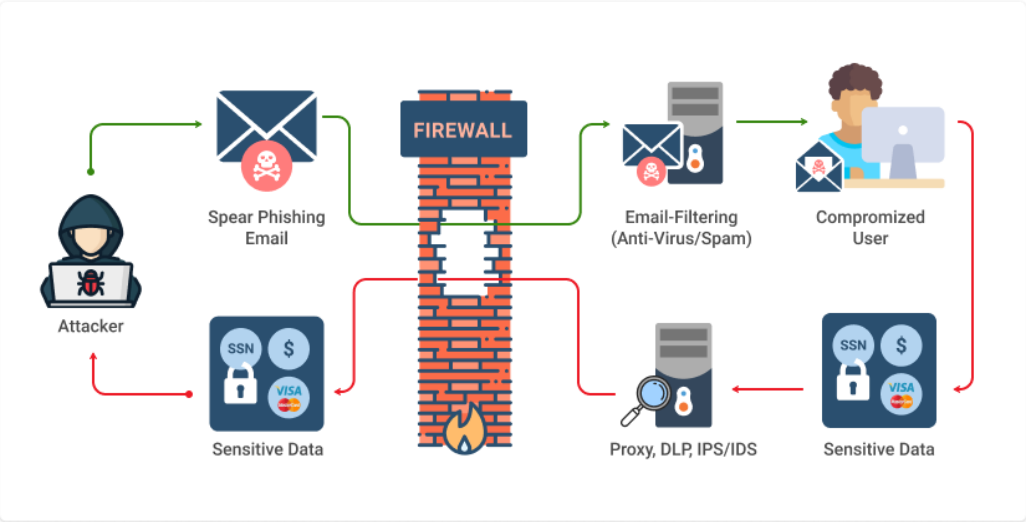
პაროლები, მაილების და ა.შ. შემდეგ ჰაკერი ეცდება, მონაცემები გამოიყენოს რეალურ საიტზე. რეალურად ფიშინგის შეტევა არის ელექტრონული ფოსტის გაგზავნის პრაქტიკა, რომელიც სანდო წყაროებიდან არის პირადი ინფორმაციის მოპოვების ან/და მომხმარებლებზე ზეგავლენის მოხდენის მიზნით. ეს შეიძლება იყოს ელ.ფოსტის დანართი, რომელიც ატვირთულია **(malware)** თქვენს კომპიუტერზე. შეიძლება იყოს არალეგიტიმური ვებ-გვერდის ბმული, რომელსაც ექნება საშუალება, ხელი შეუშალოს **malware**-ს პროგრამის ჩამოტვირთვაზე ან/და პირადი მონაცემების, ინფორმაციის მოპოვებაში.

Spear Phishing-ის შეტევა არის მიზანმიმართული ფიშინგის ტიპი. ჰაკერები ხარჯავენ დროს, რათა განახორციელონ სამიზნეში ამოღებული ადამიანების კვლევა, შექმნან ყალბი შეტყობინებები და ასე შემდეგ. ამ დროს ჰაკერებს უადვილდებათ თავდასხმა, რადგან შეუძლიათ მარტივად მოახდინონ ელ.ფოსტის დაზიანება. ეს კი ისე გამოიყურება, თითქოს არის თქვენი მენეჯმენტი ან პარტნიორი კომპანია.



ფიგურა 8

***Phishing** შეტევები, ჰაკერი ნახულობს ორიგინალ ვებ-გვერდს, აკეთებს ანალოგ ყალბ ვებ-გვერდს, ბმულს უგზავნის მომხმარებელს და ახორციელებს შეტევას. წყარო:*
https://www.cloudflare.com/learning/access-management/phishing-attack/



ფიგურა 9

Spear Phishing შეტევა, წყარო: https://www.msp360.com/resources/blog/types-of-phishing/

ფიშინგის რისკის შესამცირებლად შეგიძლიათ გამოიყენოთ ეს ტექნიკა:

Critical thinking კრიტიკული აზროვნება - ნუ იფიქრებთ, რომ ელ.ფოსტა არის ნამდვილი, შეიძლება ხართ ძალიან დაკავებული და გაქვთ **150** სხვა წაუკითხავი შეტყობინება თქვენს ელ.ფოსტაზე, მაგრამ გაჩერდით ერთი წუთით და გადახედეთ თქვენს ელ.ფოსტას.

Hovering over the links – გადადით ლინკებზე - მაუსი მიიტანეთ ბმულზე, მაგრამ არ დააჭიროთ მას! მაუსის კურსორით შეამოწმეთ ბმული, მიმართეთ კრიტიკულ აზროვნებას **URL**-ის გადასაწყვეტად.

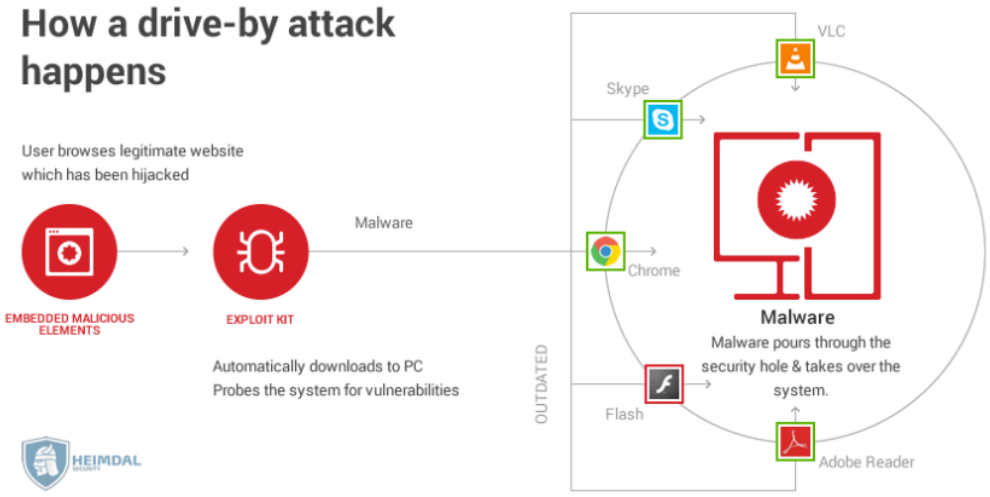
Analyzing email headers – ელექტრონული ფოსტის სათაურების ანალიზი - ელექტრონული წერილი განმარტავს ,თუ როგორ მიიღო ელფოსტა თქვენს მისამართზე. ყველა დომენი უნდა იყოს ანალოგიური, როგორიც წერია ელფოსტაზე.

Sandboxing – შეგიძლიათ შეამოწმოთ ელფოსტის შინაარსი, ჩართვის აქტივობით ან ელფოსტის შიგნით ბმულების დაჭერით.

Drive-by attack - დრაივის ჩამოტყვირთვის შეტევა:

Drive-ის ჩამოტყვირთვის შეტევების დროს ჰაკერები ეძებენ დაუცველ ვებ-გვერდებს და დამაზიანებელ სკრიპტს დებენ **http** ან **php** კოდის ერთ გვერდზე. ამ სკრიპტის ჩასმა შეიძლება მოხდეს დამაზიანებელი პროგრამით ვინმეს კომპიუტერზე, რომელიც ნახავს ვებ-გვერდს. **Drive**-ის გადმოტვირთვა შეიძლება მოხდეს ვებ-გვერდის, ელფოსტის წერილის ან pop-up ბანერის ნახვისას. ეს შეტევა არ ხორციელდება აქტიურად, თუ მომხმარებელი დააჭერს ღილაკს „ჩამოტვირთვა“, ან გახსნის დავირუსებული ელფოსტის დანართს, ამ შემთხვევაში ხდება დავირუსება.

დისტანციური კიბერშეტევებისგან თავის დასაცავად თქვენ უნდა ეცადოთ, შეხვიდეთ მხოლოდ იმ ვებ-გვერდებზე, რომლებიც თქვენთვის სანდოა და არ გადახვიდეთ სხვა ბმულებზე, რომლებიც არ იცით, რას წარმოადგენს. კომპიუტერში კი გქონდეთ ის ბრაუზერები და პროგრამები, რომლებსაც იყენებთ, ნუ შეინახავთ ზედმეტ პროგრამებს თქვენს მოწყობილობაზე. რაც უფრო მეტი დანამატი გაქვთ, მით მეტად ხართ დაუცველი.



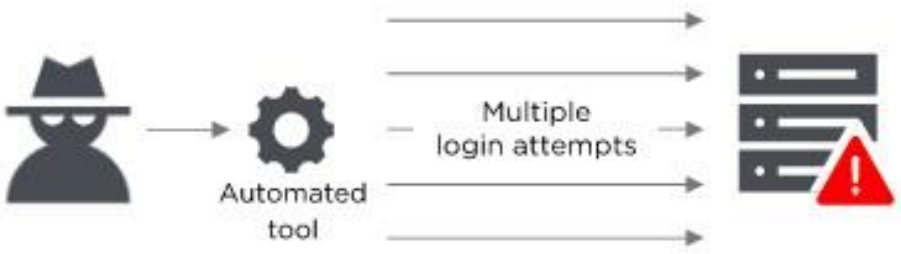
ფიგურა 10

როგორ დრაივის ჩამოტყვირთვის შეტევა, წყარო: *https://remgs.com/drive-by-download-attacks-exploit-vulnerabilities-in-web-systems/*

Password attack - პაროლის შეტევა

იმის გამო, რომ პაროლები ყველაზე ხშირად იყენებენ მექანიზმს მომხმარებელთა ინფორმაციული სისტემის დასადასტურებლად, პაროლების მოპოვება ჩვეულებრივი და ეფექტური შეტევის მეთოდია. ეს შეიძლება გაკეთდეს შემთხვევითი ან სისტემატური გზით:

Brute-force ანუ უხეში ძალის პაროლის გამოცნობა ნიშნავს შემთხვევითი მიდგომის გამოყენებას სხვადასხვა პაროლების გამოყენებით და იმ იმედით, რომ ერთი იქნება სწორი. ლოგიკური მიდგომის საფუძველზე პაროლი შეიძლება იყოს დაკავშირებული, მაგალითად: პირის სახელთან, სამუშაოს სათაურთან, გართობასთან ან სხვა ნივთთან.

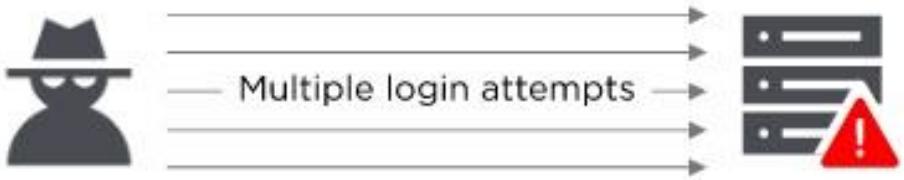


ფიგურა 11

Brute-force-ის შეტევა, წყარო: *https://www.onelogin.com/learn/6-types-password-attacks*

dictionary attack ანუ ლექსიკონის შეტევა - გულისხმობს საერთო პაროლების ლექსიკონის გამოიყენებას მომხმარებლის კომპიუტერში და ქსელში წვდომის მისაღწევად. ერთი მიდგომა არის დაშიფრული ფაილის კოპირება, რომელიც შეიცავს პაროლებს, გამოიყენეთ იგივე დაშიფრვა ჩვეულებრივ გამოყენებული პაროლების ლექსიკონში და შეადარეთ შედეგები.

იმისათვის, რომ დაიცვათ თავი უხეში ძალის ან ლექსიკონის შეტევებისგან, თქვენ უნდა განახორციელოთ ანგარიშის ჩაკეტვის პოლიტიკა, რომელიც ჩაკეტავს ანგარიშს რამდენიმე არასწორი პაროლის მცდელობის შემდეგ.



ფიგურა 12

ლექსიკონის შეტევა, მომხმარებლის კომპიუტერში სხვადასხვა პაროლების გამოყენება, წყარო: https://www.onelogin.com/learn/6-types-password-attacks

SQL (structured query language) injection attack - სტრუქტურირებული შეკითხვის ენის ინექციის შეტევა:

SQL ინექციის შეტევა გახდა საერთო საკითხი მონაცემთა ბაზაზე ორიენტირებული ვებსაიტებისთვის. **SQL (სტრუქტურირებული შეკითხვის ენა)** არის პროგრამირების ენა, რომელიც გამოიყენება მონაცემთა ბაზის მართვის შესაბამისი სისტემის მიერ და ახლავს მონაცემთა ბაზის მართვის შესაბამისი სისტემა.

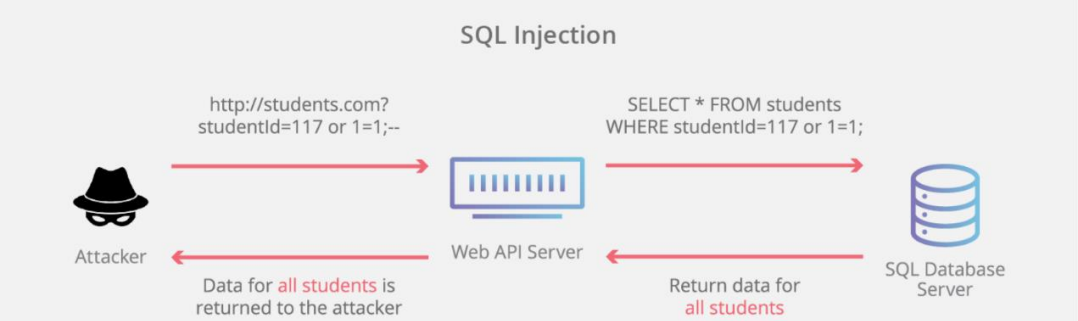
უპირველეს ყოვლისა, ეს ინფორმაციულ-ლოგიკური ენაა, რომელიც შექმნილია ურთიერთობის მონაცემთა ბაზებში დაცული მონაცემების აღწერის, შეცვლისა და გადატანისთვის. **SQL** ითვლება პროგრამირების ენად, **ზოგადად (თანამედროვე რიგი დანამატების გარეშე)** ეს არ არის **Turing-ს** რულყოფილი ვერსია, მაგრამ ამავე დროს, ენის სტანდარტი **SQL/PSM** სპეციფიკით ითვალისწინებს მისი საპროცესო გაფართოებების შესაძლებლობას.

აღნიშნული შეტევა ხდება მაშინ, როდესაც **malfactor** ასრულებს **SQL** მოთხოვნას მონაცემთა ბაზაში კლიენტის სერვერზე შესვლის მონაცემების მეშვეობით. **SQL** ბრძანებები შედის მონაცემების (მაგალითად, შესვლის ან პაროლის ნაცვლად) წინასწარ განსაზღვრული **SQL** ბრძანებების

შესასრულებლად. **SQL** ინექციის წარმატებულ მიზნობრივ გამოყენებას, ანუ ექსპლოატს შეუძლია მონაცემთა ბაზაში მნიშვნელოვანი ინფორმაციის წაკითხვა, ბაზის მონაცემების შეცვლა (ჩასმა, განახლება ან წაშლა), ადმინისტრირების ოპერაციების შესრულება (მაგალითად, გამორთვა), აღადგინოს მოცემული ფაილის შინაარსი და, ზოგ შემთხვევაში, გამოსცემს ბრძანებებს ოპერაციული სისტემისთვის.

ამ ტიპის თავდასხმის დროს **SQL** ინექციები მუშაობს ძირითადად იმ შემთხვევაში, თუ ვებსაიტს იყენებს დინამიური **SQL.**

SQL ინექციის შეტევებისგან თავის დასაცავად, თქვენს მონაცემთა ბაზაში გამოიყენეთ ნებართვების მინიმუმ ნულოვანი პრიორიტეტის მოდელი. შეინახეთ პროცედურები **(დარწმუნდით, რომ ამ პროცედურებში არ შედის დინამიური SQL)** და მომზადებული განცხადებები. კოდი, რომელიც შესრულებულია მონაცემთა ბაზის საწინააღმდეგოდ, საკმარისად ძლიერი უნდა იყოს ინექციის შეტევების თავიდან ასაცილებლად.



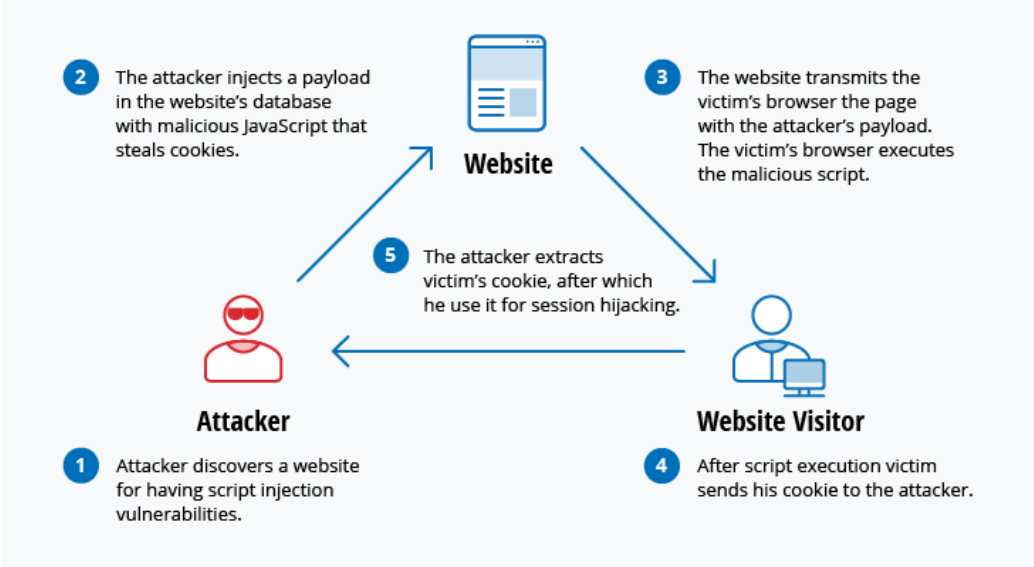
ფიგურა 13

SQL შეტევა, თავდამსხმელი ახორციელებს შეტევას ვებ აპლიკაციის სერვერზე და შემდეგ SQL დატაბეის სერვერზე, წყარო: *https://towardsdatascience.com/being-aware-of-malicious-data-corruption-as-a-data-scientist-sql-injection-attack-63f235fb2a97*

Cross-site scripting (XSS) attack - ჯვარედინი სკრიპტის (XSS) შეტევები:

XSS შეტევებისას იყენებენ მესამე მხარის ვებ-რესურსებს, რათა აწარმოონ სკრიპტები დაზარალებულის ბრაუზერში ან სკრიპტის პროგრამაში. კერძოდ, თავდამსხმელი ახორციელებს თავდასხმას **JavaScript**-ით, ვებ-გვერდის მონაცემთა ბაზაში. როდესაც მსხვერპლი ითხოვს ვებ-გვერდს, ამ დროს თავდამსხმელი, როგორც **HTML** ორგანოს ნაწილი, აგზავნის

დავირუსებულ ვებ-გვერდს, სადაც არის თავდამსხმელის მიერ დაწერილი დამაზიანებელი სკრიპტი. მაგალითად, შესაძლოა მას მსხვერპლის ქუქი გაუგზავნოს თავდამსხმელს სერვერზე, ხოლო თავდამსხმელს შეუძლია მისი ამოღება და გამოყენება სესიის გატაცებისთვის. ყველაზე საშიში შედეგები ხდება მაშინ, როდესაც **XSS** გამოიყენება დამატებითი დაუცველი მექანიზმების გამოსაყენებლად. ეს დაუცველი მხარეები საშუალებას აძლევს თავდამსხმელს. არა მხოლოდ მოიპაროს ქუქი-ფაილები, არამედ დაწეროს კლავიშით, გადაიღოს ეკრანის ანაბეჭდები, მოიძიოს, შეაგროვოს ქსელის ინფორმაცია, დისტანციურად ჰქონდეს წვდომა და გააკონტროლოს დაზარალებულის მოწყობილობა.



ფიგურა 14

ჯვარედინი სკრიპტის შეტევა, თავდამსხმელი შეტევას ახორციელებს ვებ-გვერდზე javaScript-ის საშუალებით და ვებ-გვერდის სტუმარის ქუქიები ავტომატურად ეგზავნება ჰაკერს. წყარო: *https://medium.com/@sharmin11/what-is-cross-site-scripting-xss-attack-c6c0046890ac*

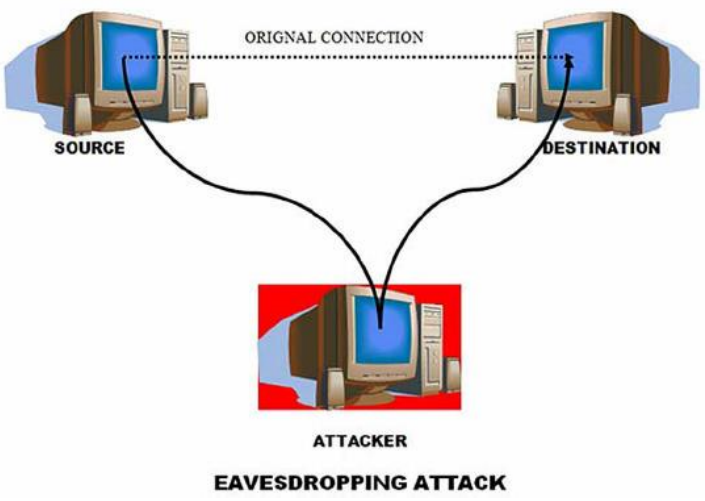
XSS შეტევებისგან დასაცავად დეველოპერებს შეუძლიათ **http** თხოვნით მომხმარებლების მიერ მონაცემების შეყვანა გაფილტრონ, სანამ უშუალოდ ასახავენ. დარწმუნდით, რომ ყველა მონაცემი დადასტურებულია, ანუ გაფილტრული.

Eavesdropping attack - მოსმენის შეტევა:

მოსმენების შეტევები ხდება ქსელის ტრაფიკის ჩარევით. გაფრთხილების საშუალებით. თავდამსხმელს შეუძლია, მოიპოვოს პაროლები, საკრედიტო ბარათის ნომრები და სხვა კონფიდენციალური ინფორმაცია, რომელსაც მომხმარებელი შესაძლოა ქსელს უგზავნის. მოსმენა შეიძლება იყოს პასიური ან აქტიური:

Passive eavesdropping პასიური მოსმენა - ჰაკერი ცნობს ინფორმაციას ქსელში შეტყობინებების გადაცემის მოსმენით.

Active eavesdropping აქტიური მოსმენა - ჰაკერი აქტიურად ითვისებს ინფორმაციას საკუთარი თავის შენიღბვით. ამას ეწოდება გამოძიება ან სკანირება, **პასიური მოსმენის** შეტევების გამოვლენა ხშირად უფრო მნიშვნელოვანია, ვიდრე აქტიურის, რადგან აქტიური შეტევები მოითხოვს თავდამსხმელს. მონაცემთა დაშიფრვა არის საუკეთესო საწინააღმდეგო ღონისძიება მოსმენის გადამისამართებისთვის.

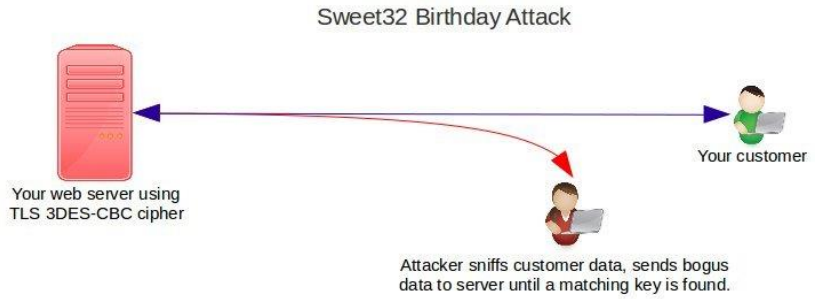


ფიგურა 15

მოსმენის შეტევა, თავდამსხმელი დაკავშირებულია ორ კომპიუტერთან და ახორციელებს მოსმენას, წყარო: *https://www.researchgate.net/figure/Eavesdropping-attack_fig2_284031789*

Birthday attack - დაბადების დღის შეტევა:

დაბადების დღის შეტევები ჰაშის ალგორითმის საწინააღმდეგოდ ხორციელდება, რომელიც გამოიყენება მესიჯის, პროგრამული ან ციფრული ხელმოწერის გადამოწმების მიზნით. ჰაშის ფუნქციით დამუშავებული შეტყობინება აწარმოებს ფიქსირებული სიგრძის შეტყობინებას **(MD),** შეყვანის შეტყობინების სიგრძისგან დამოუკიდებლად; ეს **MD** ცალსახად ახასიათებს შეტყობინებას. დაბადების დღეზე თავდასხმა ეხება ორი შემთხვევითი გზავნილის პოვნის ალბათობას, რომლებიც წარმოქმნიან იმავე **MD**-ს, როდესაც დამუშავებულია ჰაშ-ფუნქციით. თუ თავდამსხმელი გამოითვლის იმავე **MD**-ს მისი შეტყობინებისთვის, როგორც მომხმარებელს აქვს, მას შეუძლია უსაფრთხოდ შეცვალოს მომხმარებლის შეტყობინება მისი საშუალებით, ხოლო მიმღები ვერ შეძლებს ჩანაცვლების დაფიქსირებას, თუნდაც მან შეაპაროს **MD**-ები.



ფიგურა 16

დაბადების დღის შეტევა, თავდამსხმელი ახორციელებს MD ალგორითმით შეტევას ვებ სერვერზე რომელზეც დაკავშირებულია ე.წ. მსხვერპლი, წყარო: *https://bobcares.com/blog/how-to-fix-sweet32-birthday-attacks-vulnerability-cve-2016-2183/*

Malware attack - მავნე შეტევები:

მავნე შეტევები შეიძლება შეფასდეს როგორც არასასურველი პროგრამა, რომელიც თქვენი თანხმობის გარეშე სისტემაში არის დაინსტალირებული, მას შეუძლია, ლეგიტიმურ კოდს დაერთოს და გამრავლდეს; ასევე შეუძლია სხვადასხვა პროგრამებში გამრავლება, ან ინტერნეტთან ინტერპრეტაცია.

ყველაზე გავრცელებული ტიპის malware:

Macro viruses - ეს ვირუსები აინფიცირებს პროგრამებს, როგორიცაა **Microsoft Word** ან **Excel.** მაკრო-ვირუსები ანიჭებენ პროგრამის ინიციალიზაციის თანმიმდევრობას. განაცხადის გახსნისას ვირუსი ასრულებს ინსტრუქციებს კონტროლზე გადასვლამდე პროგრამაში. ვირუსი რეპლიკაციას ახდენს და კომპიუტერულ სისტემაში სხვა კოდებს ანიჭებს.

File infectors - როგორც წესი, თავს იწერენ შემსრულებელ კოდთან, როგორიცაა **.exe** ფაილები. კოდი დატვირთვისას ვირუსი ჩაკერებულია. ამ ვირუსის კიდევ ერთი ვერსია ასოცირდება ამავე სახელწოდების ვირუსის ფაილის შექმნით, მაგრამ exe გაფართოებით.

System or boot-record infectors - ჩატვირთვისას ვირუსი მყარ დისკზე ატარებს მასტერის ჩატვირთვის ჩანაწერს. სისტემის დამუშავებისას იგი დაათვალიერებს ჩატვირთვის სექტორს და ატვირთავს ვირუსს მეხსიერებაში, სადაც მას შეუძლია სხვა დისკებზე და კომპიუტერებზე გავრცელება.

Polymorphic viruses - ეს ვირუსები მალავს თავს დაშიფრვის და გაშიფრვის სხვადასხვა ციკლის საშუალებით. დაშიფრული ვირუსი და მასთან დაკავშირებული მუტაციური ძრავი თავდაპირველად გაშიფრულია დეშიფრაციის პროგრამით. ვირუსი აგრძელებს კოდის არეალს. მუტაციის ძრავი შემდეგ შეიმუშავებს დეშიფრაციის ახალ რუტინას და ვირუსი დაშიფვრავს მუტაციის ძრავს და ვირუსის ასლს ალგორითმით, რომელიც შეესაბამება ახალ რუტინას. მუტაციის ძრავისა და ვირუსის დაშიფრული პაკეტი თან ერთვის ახალ კოდს, ხოლო პროცესი მეორდება. ასეთი ვირუსების აღმოჩენა რთულია, მაგრამ აქვთ ინტროპიის მაღალი დონე, კოდის მრავალი შეცვლის გამო. ანტივირუსული პროგრამის ან უფასო ხელსაწყოების მსგავსად, პროცესორის ჰაკერს შეუძლია გამოიყენოს ეს ფუნქცია მათ გამოსავლენად.

Stealth viruses - ფარული ვირუსები იკავებენ სისტემის ფუნქციებს, რათა დამალონ ისინი. ამას ახდენენ მავნე პროგრამების დაფიქსირებით. ასე რომ,

პროგრამული უზრუნველყოფა აცნობებს ინფიცირებულ ადგილს, როგორც დეზინფექციას. ეს ვირუსები მალავს ინფიცირებული ფაილის ზომის ზრდას ან ფაილში ცვლილების თარიღსა და დროს.

Trojans - პროგრამა „ტროას ცხენი“ არის ვირუსი, რომელიც იმალება სასარგებლო პროგრამაში. მას ჩვეულებრივ აქვს დამაზიანებელი ფუნცია. ვირუსებსა და ტროიანებს შორის არის განსხვავება, ტროიანები არ ახდენენ თვითრეალიზაციას, ტროას შეუძლია შექმნას უკანა კარი, რომელსაც თავდამსხმელების ექსპულატაცია შეუძლიათ. მაგალითად, Trojan შეიძლება დაპროგრამდეს და გახსნას მაღალრიცხვიანი პორგი, ამ შემთხვევაში ჰაკერს შეუძლია, გამოიყენოს ეს მოსასმენად და თავდასხმების განსახორციელებლად.

Logic bombs - არის მავნე პროგრამის ტიპი, რომელიც დამატებულია აპლიკაციაში და გამოწვეულია კონკრეტული მოვლენით, როგორიცაა ლოგიკური მდგომარეობა ან კონკრეტული თარიღი და დრო.

Worms – „ჭიები“ - ვირუსებისგან განსხვავდება იმით, რომ ისინი არ უერთდებიან მასპინძელ ფაილს. „ჭიები“ ჩვეულებრივ ვრცელდება ელფოსტაზე, დანართის გახსნა ააქტიურებს „ჭიების“ პროგრამას. მისი ტიპიური ექსპლუატაცია გულისხმობს ინფიცირებულ კომპიუტერში ელექტრონული ფოსტის მისამართის ყველა კონტაქტს საკუთარი თავის ასლის გაგზავნას. მავნე საქმიანობის განხორციელების გარდა, „ჭიამ“, რომელიც ვრცელდება ინტერნეტში, შეიძლება ელექტრონული ფოსტის სერვერების გადატვირთვის შედეგად გამოიწვიოს მომხმარებელზე შეტევა.

Dropper - წვეთოვანი არის პროგრამა, რომელიც კომპიუტერში ვირუსების დაყენების მიზნით გამოიყენება. ხშირ შემთხვევაში dropper არ არის ინფიცირებული მავნე კოდით და შესაბამისად, არ შეიძლება გამოვლენილი იყოს ვირუსის სკანირების პროგრამით.

Ransomware - გამოსაქვეყნებელი არის **malware**, რომელიც ბლოკავს მსხვერპლის მონაცემებზე წვდომას და საფრთხეს უქმნის გამოქვეყნებას ან

წაშლას, თუ გამოსასყიდი არ იქნა გადახდილი. მიუხედავად იმისა, რომ რამდენიმე მარტივი კომპიუტერის **ransomware**-ს შეუძლია სისტემის ჩაკეტვა ისე, უფრო მოწინავე **malware** იყენებს ტექნიკას, რომელსაც ეწოდება კრიპტოვირუსული გამოძალვა, რომელიც დაშიფვრავს მსხვერპლის ფაილებს ისე, რომ თითქმის შეუძლებელი იქნება აღმოიფხვრას დაშიფრვის გასაღები.

Adware - სარეკლამო რგოლები არის პროგრამა, რომელსაც კომპანიები იყენებენ მარკეტინგული მიზნებისთვის; სარეკლამო ბანერები ნაჩვენებია ნებისმიერი პროგრამის შესრულებისას.

Spyware - ჯაშუში არის პროგრამის ტიპი, რომელიც დაინსტალირებულია მომხმარებლების, მათი კომპიუტერების ან ბრაუზერის ჩვევების შესახებ ინფორმაციის მოსაგროვებლად. ის აკონტროლებს ყველაფერს, რასაც აკეთებთ თქვენი ცოდნის გარეშე და მონაცემებს უგზავნის დისტანციურ მომხმარებელს. მას ასევე შეუძლია, ჩამოტვირთოს და დააინსტალიროს სხვა მავნე პროგრამები ინტერნეტიდან. **Spyware** მუშაობს როგორც adware, მაგრამ როგორც წესი, არის ცალკე პროგრამა, რომელიც რომელიმე უფასო პროგრამას მოყვება და როდესაც აინსტალირებთ **Spyware**-ც ინსტალირდება უნებურად.[10]

კარგი თავდაცვის მექანიზმების შემუშავება მოითხოვს დანაშაულის აღმოჩენას და გაგებას, ეს არის 10 ყველაზე გავრცელებული კიბერშეტევა, რომელსაც ჰაკერები იყენებენ წარმატებით. როგორც ხედავთ, თავდამსხმელებს აქვთ მრავალი ვარიანტი, რათა შეეცადონ უნებართვო წვდომა მოიპოვონ კრიტიკულ ინფრასტრუქტურებზე და მნიშვნელოვან მონაცემებზე. ამ საფრთხეების შემსუბუქების და აღმოფხვრის ზომები განსხვავდება, მაგრამ უსაფრთხოების საფუძვლები ერთნაირია: განაახლეთ თქვენი სისტემები და ანტივირუსული მონაცემთა ბაზები, განახორციელეთ

[10] Melnick Jeff. (Director, Global Solutions Engineering), „Top 10 Most Common Types of Cyber Attacks“, March 10, 2020 Y. P. 1. Extracted: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/, უკანასკნელად იქნა გადამოწმებული: 24.06.2020

თქვენი შეტყობინებების კონფიგურაცია, შეინახეთ პაროლები ჭკვიანურად და დაცულად, გამოიყენეთ მინიმალური შეღავათები თქვენი IT გარემოს გასაუმჯობესებლად. მუდმივად შეამოწმეთ საეჭვო საქმიანობების ალბათობის მიზნით თქვენი IT სისტემები.

1.1. კონფლიქტების ტრანსფორმაცია ახალი გეოპოლიტიკური წესრიგის პირობებში

ზოგიერთი მკვლევარი ფიქრობს, რომ რუსეთი იმთავითვე მოქმედებდა და დღესაც მოქმედებს მესამე რომის კონცეფციით, სადაც წინა პლანზე წამოწეულია თვითლეგიტიმაცია, ანუ მსოფლიოზე ბატონობის მოპოვება რევოლუციური წიაღსვლებით. ფაქტობრივად, ეს არაფრით განსხვავდება მესამე რაიხის, ანუ **იოზიფ გებელსის** დოქტრინისგან. ცხადია, თავის დროზე ჰიტლერის ფაშისტურმა რეჟიმმა, იდეოლოგიური თვალსაზრისით, ბევრი რამ წამოიღო მესამე რომის კონცეფციიდან და ასევე ბევრი რამ გადმოიღეს ბოლშევიკებმა. რუსეთის ურთიერთობას დანარჩენს სამყაროსთან საფუძვლად უდევს გებელსის უკვე „დახვეწილი“ დოქტრინა - "მომეცით მასობრივი ინფორმაციის საშუალება და ნებისმიერ ერს ვაქცევ ღორების კოლტად".[11] თუ გებელსის პერიოდში მასობრივი ინფორმაციის საშუალებების დეფიციტი იყო, ხოლო მესამე რომის პერიოდში ცხენების დახმარებით "ზიდავდნენ" ინფორმაციას, დღეს ამ მხრივ რუსეთს აქვს "სრული ბედნიერება" და იყენებს კიდეც ყველა მიმართულებით. მეტიც, კრემლის მიერ წარმოებულ პროპაგანდას დიდიხანია აღარ გააჩნია საზღვრები. ყველა ქვეყნის ეროვნულ კონცეფციაში ხაზგასმითაა აღნიშნული რუსეთიდან მომდინარე საფრთხეების შესახებ. მეტიც, აშშ-ის შეიარაღებული ძალების კომიტეტში არაერთი ნაშრომია წარდგენილი, რომელიც ეხება რუსული ჰიბრიდული ომის, კიბერომის მოგერიებას. ერთ-ერთი მათგანია **RAND**-ის კორპორაციის მკვლევარის **კრისტოფერ ჩივისის** ნაშრომი. რა არის

[11] გობრონიძე, გ.. *(იოზეფ გებელსის დოქტრინა) "გებელსი, პროპაგანდა, გეორგიევსკის ბაფთა და უკრაინა".* 2014.16.06. გვ. 1. მოპოვებული iveria.biz: http://iveria.biz/559-gebelsi-propaganda-georgievsks-bafta-da-ukraina.html-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

რუსული ჰიბრიდული ომი და რა შეიძლება გააკეთოს შეერთებულმა შტატებმა? **პირველი** - რუსეთის ჰიბრიდული ომი რამდენიმე მიზანს ემსახურება: შეასუსტოს ნატო: შეარყიოს პროდასავლური მთავრობები, შექმნას ომის წინაპირობა, ტერიტორიის დაპყრობა, ეკონომიკური სარგებელი; **მეორე** - ჰიბრიდული ომი რუსეთს აძლევს საშუალებას, მინიმუმამდე დაიყვანოს სამხედრო ძალის გამოყენების აუცილებლობა, ამავდროულად მიაღწიოს თავის საგარეო პოლიტიკურ მიზნებს; **მესამე** - ჰიბრიდული ომი შლის ტრადიციულ ზღვარს ომსა და მშვიდობას შორის, ჰიბრიდული ომი მუდმივად მიმდინარეობს; **მეოთხე** - ტერიტორიის დაპყრობა ღია სამხედრო დაპირისპირების გარეშე. ამის მაგალითია ყირიმის ანექსია, როდესაც მწვანე უნიფორმაში გადაცმულმა სპეციალური დანიშნულების რუსულმა სამხედრო ძალებმა საინფორმაციო ომის ფონზე და ადგილობრივი გავლენის ჯგუფების დახმარებით უსისხლოდ დაიკავეს ყირიმი.[12]

საჭიროა რუსული ჰიბრიდული ქმედებების გამოკვლევა. აუცილებელია მოკავშირეებთან ინფორმაციის გაცვლის გაგრძელება. ბალკანეთსა და უკრაინაში შიდაუსფრთხოების აპარატის რეფორმისა და თავდაცვითი ინსტიტუციების მშენებლობის მხარდაჭერა. სამოქალაქო საზოგადოების ხელშეწყობა დეზინფორმაციის კამპანიებთან საბრძოლველად. ჰიბრიდული ომის დაძლევის ევროპული მცდელობების მხარდაჭერა. ფინეთში, ლატვიას და ესტონეთში გახსნილი ცენტრების მხარდაჭერა და ევროპის კიბერთავდაცვის გაძლიერება. ნაშრომში, რომელიც აშშ-ის ყველაზე მნიშვნელოვან უწყებაში წარადგინეს, საქართველო (დაკარგული ტერიტორიებით) საერთოდ არ არის ნახსენები, აქ ყურადღება

[12] ჩივისის, კ. *"რუსეთის ჰიბრიდული ომის დამახასიათებელი ნიშნები"*. 2017.19.04. გვ. 1. მოპოვებული gmas.ge: https://gmas.ge/2017/%E1%83%A1%E1%83%98%E1%83%90%E1%83%AE%E1%83%9A%E1%83%94%E1%83%94%E1%83%91%E1%83%98/%E1%83%A0%E1%83%A3%E1%83%A1%E1%83%94%E1%83%97%E1%83%98%E1%83%A1-%E1%83%B0%E1%83%98%E1%83%91%E1%83%A0%E1%83%98%E1%83%93%E1%83%A3%E1%83%9A%E1%83%98-%E1%83-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

გამახვილებულია მხოლოდ ბაკლანეთსა და უკრაინაზე. თუმცა ნებისმიერი კონცეფცია, ნებისმიერი განხილვა ჩვენთვის საინტერესოა, რადგან რუსეთს უნდა თუ არა, მაინც ვართ იმ ევროპის გაგრძელება, რომელიც თავს იცავს რუსული კიბერომისგან და შესაბამისად, ვიმყოფებით აშშ-ის გავლენის სფეროში უსაფრთხოების თვალსაზრისით.

საქართველოს კიბერუსაფრთხოების ეროვნულ სტრატეგიაში ცალკე თავადაა გამოტანილი, რომ აუცილებელია საზოგადოებრივი ცნობიერების ამაღლება და საგანმანათლებლო ბაზის ჩამოყალიბება. აქვე ხაზგასმითაა აღნიშნული, რომ ჩვენში საზოგადოებრივი ცნობიერება საკმაოდ დაბალია. ცნობიერების ამაღლების საკითხი ასევე დიდი გამოწვევაა სახელმწიფო სექტორისთვისაც, სადაც დასაქმებული მოხელეების მნიშვნელოვანი ნაწილი ვერ ფლობს კიბერუსაფრთხოების ბაზისური ნორმების ცოდნას და აუცილებელია მომზადება-გადამზადება. უსაფრთხოების ქართული სტრატეგია, ანუ გეგმა ღიად აღიარებს, რომ დღეს კიბერუსაფრთხოების უზრუნველყოფა შეუძლებელია საკუთარი ძალებით, რადგან კიბერინციდენტები უკვე გადასულია ტრანსნაციონალურ ჭრილში და ამ შემთხვევაში აუცილებელია საერთაშორისო სისტემაში ჩართვა. აქ კი ისევ მივდივართ ნატო-ს და აშშ-ის მიერ შემუშავებულ გეგმებამდე და გამოცდილებამდე, შემდეგ კი თანამშრომლობამდე.[13]

ჩვენ გვთავაზობენ სტრატეგიებს, პროგრამებს, გეგმებს, კონცეფციებს, სადაც ყველა სიტყვა თითქმის აფთიაქის სასწორზეა აწონილი და დიდი სიზუსტით ასახავს რეალობას, მაგრამ უცხოელი ექსპერტების აზრით, კიდევ რაღაც არის საჭირო. ისინი სვამენ შეკითხვას: რომელ კანონებს უნდა მივმართოთ მაშინ, როდესაც ომები კიბერსივრციდან იმართება? ამ კითხვაზე პასუხის გაცემას ისახავს მიზნად ახალი სახელმძღვანელო, რომელიც ნატოს კიბერთავდაცვის

[13] საქართველოს მთავრობის დადგენილება №14. *"საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ".* 2017.13.01. გვ. 1-38, მოპოვებული gov.ge: http://gov.ge/files/469_59439_212523_14.pdf-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

სფეროში „თანამშრომლობის უნარების ცენტრის“ ხელმძღვანელობით ცნობილმა ექსპერტებმა შექმნეს:

„მომავალში შესაძლო კიბერომებთან დაკავშირებულ კითხვებზე პასუხებს საერთაშორისო სამართლის 20 ექსპერტისგან შემდგარი კომისია ჟენევისა და ჰააგის კონვენციებში, ასევე გაეროს ქარტიაში რამდენიმე წლის განმავლობაში ეძებდა. ამ კომისიის დასკვნითი შედეგები ახლახან გამოქვეყნდა 300 -გვერდიან სამართლებრივ ცნობარში, რომელსაც „ტალინის სახელმძღვანელო“ ეწოდება“.[14]

რას წარმოადგენს **„ტალინის სახელმძღვანელო“** და რით განსხვავდება კრემლის მიერ შემუშავებული „რუსული სურვილებისგან“, რომელიც ამავე დონეზე ითხოვს რეგულაციების დაწესებას მხოლოდ სათავისოდ? ჯერ ერთი, ეს არის მხოლოდ სახელმძღვანელო და მეორეც, შედგენილია პროფესიონალების მიერ. კომისიას, რომელმაც სახელმძღვანელო დაწერა, აშშ-ის საზღვაო ძალთა ომის კოლეჯის პროფესორი **მაიკლ შმიტი** ხელმძღვანელობდა. ის 25 წელი მუშაობდა აშშ-ის სამხედრო საჰაერო ძალებსა და არმიაში. შმიტის თქმით, **„ტალინის სახელმძღვანელო“** სამხედრო იურისტებისთვის არის განკუთვნილი, მათთვის, ვინც რჩევებს აძლევს იმ სამხედრო ხელმძღვანელობას, რომელსაც კიბერშესაძლებლობების გამოყენება შეუძლია:

„ჩვენ ვაპირებთ სამართლებრივ რჩევებზე მომუშავე ადამიანებს შევთავაზოთ ისეთი მექანიზმი, რომელიც მათი სამართლებრივი რჩევის ხარისხს გააუმჯობესებს“.[15]

ზემოხსენებული ცნობარი ნატოს კიბერთავდაცვის სფეროში თანამშრომლობის უნარების ცენტრის ხელმძღვანელობით შეიქმნა, მაგრამ

[14] ლიკლიკაძე, კ. *როგორი წესებით უნდა ვიომოთ კიბერომში?* 2013.07.04. გვ. 1. მოპოვებული radiotavisupleba.ge: https://www.radiotavisupleba.ge/a/military-programm/24950058.html-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

[15] ლიკლიკაძე, კ. *როგორი წესებით უნდა ვიომოთ კიბერომში?* 2013.07.04. გვ. 1. მოპოვებული radiotavisupleba.ge: https://www.radiotavisupleba.ge/a/military-programm/24950058.html-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

იგი არ წარმოადგენს ნატოს პოლიტიკურ, ოფიციალურ დოკუმენტს. როგორც **მაიკლ შმიტი** განმარტავს, სახელმძღვანელო ცდილობს, პასუხი გასცეს ორ მნიშვნელოვან შეკითხვას: რომელი კანონით რეგულირდება ან რა საფრთხეთა მიმართ სჭირდება სახელმწიფოს კიბეროპერაციის ჩატარება მშვიდობიან დროს?

ექსპერტები ადგენენ გეგმებს, სწავლობენ სიტუაციას, მაგრამ აქვე დიდი სიფრთხილით აღნიშნავენ, რომ კიბერიერიშები, რაც „მღელვარებასა და გაღიზიანებას“ იწვევს, არ შეიძლება კვალიფიცირდეს, როგორც ძალის გამოყენება. ასევე კიბერშეტევის ობიექტად არ განიხილავს სახელმძღვანელო ჰაკერებს, რომლებსაც გაზეთების მყვირალა სათაურები კიბერდამნაშავეებად მოიხსენიებენ:

„ჩვენ არასოდეს გვითქვამს, რომ ჰაკერებზე შეგიძლიათ იერიშის მიტანა. ჩვენ მხოლოდ ის ვთქვით, რომ თუკი შეიარაღებული კონფლიქტი გაქვთ და ვინმე გადაწყვეტს, ისე მძლავრად ჩაერიოს ამ კონფლიქტში, რომ მწყობრიდან გამოიყვანოს თქვენი სამხედრო შესაძლებლობები, მაშინ აღნიშნული პიროვნება დაკარგავს მრავალი წლის განმავლობაში არსებული ჰუმანიტარული სამართლით მისთვის მინიჭებულ ხელშეუხებლობის უფლებას და სამიზნედ გადაიქცევა. ამას არაფერი აქვს საერთო არც იმ ჰაკერებთან, რომლებსაც მშვიდობიან დროს, ან საომარ ვითარებაში მწყობრიდან გამოჰყავთ ვებსაიტი“, - ამბობს პროფესორი **მაიკლ შმიტი.**[16]

პროფესორ **ვახტანგ მაისაიას** თქმით, საერთო ჯამში სამხედრო სტრატეგიული პარამეტრების ზოგადი მიმართულებები შეიძლება წარმოდგენილი იქნას შემდეგი სახით:

„მოწინააღდეგის არა ფიზიკური, არამედ მორალური და პოლიტიკური დამარცხება, კომბინირებული საომარი ტაქტიკური ელემენტების გამოყენება, საინფორმაციო-პროპაგანდისტური ბრძოლის წარმოება,

[16] ლიკლიკაძე, კ. *როგორი წესებით უნდა ვიომოთ კიბერომში?* 2013.07.04. გვ. 1. მოპოვებული radiotavisupleba.ge: https://www.radiotavisupleba.ge/a/military-programm/24950058.html-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

კიბერომი, კულტურული ექსპანსია, პარტიზანული ტიპის საომარი კამპანიის წარმოება“.[17]

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. პროპაგანდისტული ომის მთელი სიძლიერე გამოვლინდა მეორე მსოფლიო ომის პერიოდში და ცოცხლობს დღემდე. ძნელი დასაჯერებელია, მაგრამ ფაქტია, როდესაც მეორე მსოფლიო ომი დასრულდა, გერმანიაში ძალიან ბევრი ადამიანი აცხადებდა: დიახ, ადოლფ ჰიტლერი დამნაშავეა, ცოტა გადააჭარბა, მაგრამ კარგი უფრო ბევრი გააკეთა, აღგვიდგინა ღირსება და დაგვიგო ავტობანები. მეტიც, პოსტჰიტლერულ გერმანიაში იმდენად ძლიერი იყო გებელსის იდეოლოგიისა და პროპაგანდის გავლენა, რომ 1948 წელს ნიურბერგის სასამართლო პროცესებზე მოწმეები არ გამოდიოდნენ, ამერიკელი გამომძიებლები მათ სანთლით ეძებდნენ. 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. 1945 წლის გაზაფხულზე, როცა კოალიციური ჯარები ბერლინს 12 კილომეტრით მიუახლოვდნენ და რაიხსტაგი უკვე იბომბებოდა, ჰიტლერი იჯდა ბუნკერში და თავისი ავადმყოფური მიმართვებით გერმანელ ხალხს „ამხნევებდა“, ჩვენ გავიმარჯვებთო.

ძველი დროიდან მოყოლებული, დღემდე, პროპაგანდისტულ ომს თან ახლავს მისტიკური საბურველი. ასეთივე საბურველში გაეხვია ჰიბრიდული ომის პროცესიც. რასაკვირველია, როცა საქმე გვაქვს გასაიდუმლოებულ და

[17] მაისაია, ვ. „ჰიბრიდული ომის“ რაობა და მისი გეოსტრატეგიული ასპექტები (მეოთხე თაობის ომი) - კიბერომის მაგალითზე". The Georgian Times, 2017 წლის 30, 03. გვ 1. მოპოვებული http://geotimes.com.ge/blogi/?m=82&post_id=10-დან, უკანასკნელად იქნა გადამოწმებული: 11.06.2020

ხშირად მიუწვდომელ, გაუხსნელ მოვლენებთან, თავისთავად წარმოიშობა მისტიციზმიც, მაგრამ რაც მეტად შევძლებთ მის შემცირებას, მით მეტი სიცხადე გვექნება ამ სფეროში.

კიბერომს არ გააჩნია საზღვრები და ამ მხრივ ბევრი რამ ჯერ კიდევ აუთვისებელი „ყამირია“, გამოდის, წინ ჯერ კიდევ მრავალი „სიურპრიზი“ გველოდება. ამ მხრივ კარგი მაგალითია რუსეთის გენშტაბის უფროსის, **ვალერი გერასიმოვის** 2013 წელს გამოქვეყნებული ნაშრომი **„ახალი თაობის ომის წარმოების მეთოდები“**, სადაც განხილულია **„არაბული გაზაფხულის“** მოვლენები და აღნიშნულზე დაყრდნობით გაკეთებულია დასკვნა, რომ „ახალი თაობის ომში“ სამხედრო ძალა გამოყენებული იქნება ფარულად, ოფიციალური დეკლარირების გარეშე. რას ნიშნავს, ფარული ომი დეკლარირების გარეშე? **გერასიმოვის** განმარტებით, ახალი თაობის ომის არსი მდგომარეობს შემდეგში: სამხედრო მოქმედებები იწყება მშვიდობიან პერიოდში, ანუ ოფიციალურად ომი გამოცხადებული არ არის, ფართომასშტაბიანი სამხედრო მოქმედებების ნაცვლად, კონფლიქტი ხასიათდება მცირე მასშტაბის, ლოკალური შეტაკებებით. ადგილი აქვს საბრძოლო მოქმედებებში სპეცდანიშნულების ქვედანაყოფების და შეიარაღებული სამოქალაქოების გამოყენებას. ბრძოლა მიმდინარეობს არა სამ, არამედ ოთხ სივრცეში - ხმელეთზე, ჰაერში, ზღვაში და საინფორმაციო ველზე. ჰიბრიდული ომის წარმოება შეუძლებელია პროპაგანდისა და საინფორმაციო-ფსიქოლოგიური ოპერაციების გამოყენების გარეშე.[18]

2008 წლის აგვისტოს ომის დროს რუსული მხარე ზუსტად იცავდა **გერასიმოვის** მიერ შემუშავებულ დოქტრინას. იგივე განმეორდა უკრაინაში და იგივე განმეორდება მომავალ ჰიბრიდულ ომებში, რომელსაც რუსეთი დაგეგმავს.

[18] გერასიმოვი, ვ. *"ჰიბრიდული ომი რუსულ სამხედრო თეორიაში"*. 2017.10.07. გვ. 1. მოპოვებული eugeorgia.info: http://eugeorgia.info/ka/article/637/hibriduli-omi-rusul-samxedro-teoriashi/-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

ჰიბრიდული ომი ნიშნავს პერმანენტულ ომს მთელი მსოფლიოს მასშტაბით, სადაც საერთოდ აღარ არსებობს წითელი ხაზები და აკრძალული ზონები. ეს არის ყოველდღიურად მზარდი საფრთხე და „დამოკლეს მახვილი“ კაცობრიობის თავზე. ამ ფონზე კი, როგორც CSIS-ის ვიცე-პრეზიდენტი **ჰეთერ კონლი** აცხადებს, საქართველო და უკრაინა არის რუსეთის პრაქტიკის, მისი გავლენისა და კიბერქმედებების ლაბორატორია.

ამ შემთხვევაში უპრიანია **რიჩარდ კოენის „კოლექტიური უსაფრთხოების“ თეორია,** რომლის თანახმად, საერთაშორისო უსაფრთხოების თვალსაზრისით არსებობს ორ კონცეფცია - კოლექტიური უსაფრთხოება და კოლექტიური თავდაცვა. ამას ემატება ორი კომპონენტი, რომელიც მოიცავს ინდივიდუალურ უსაფრთხოებასა და სტაბილურობის შენარჩუნებას. ამ კომპონენტების დამატების აუცილებლობა განაპირობა ახალმა საფრთხეებმა - ტერორიზმი, კიბერტერორიზმი და ასე შემდეგ.

ნეოლიბერალიზმის თეორიის თანახმად, ნებისმიერი ომი, როგორც სამხედრო, ასევე კიბერ თუ ჰიბრიდული ომები უსარგებლოა ყველა მონაწილისთვის. სახელმწიფოები თანამშრომლობის დროს მეტს იგებენ, ვიდრე ომის დროს. თუმცა კაცობრიობა ჯერაც ვერ მივიდა იმ დონემდე, რომ დედმიწაზე ჩამოყალიბდეს ერთობლივ ცხოვრების პირობები და უსაფრთხო გარემო.

1.2. კიბერომის თეორია და მისი ადგილი თანამედროვე მსოფლიო პოლიტიკაში

2012 წლიდან დღემდე აქტიურად მიმდინარეობს ნატოს თავდაცვის სისტემაში კიბერუსაფრთხოების ინტეგრაციის პროცესი. 2014 წლის უელსის სამიტზე გამოცხადებული ახალი კიბერპოლიტიკის თანახმად, რომელიმე წევრ სახელმწიფოზე მასობრივი და გამანადგურებელი ჰაკერული თავდასხმის განხორციელების შემთხვევაში, ამოქმედდება ორგანიზაციის ხელშეკრულების მე-5 მუხლი, ხოლო 2016 წლის ვარშავის სამიტზე ალიანსის წევრმა ქვეყნებმა ინფორმაციული და საკომუნიკაციო ქსელის უსაფრთხოება

ერთ-ერთ ძირითად თავდაცვით სფეროდ აღიარეს და შეთანხმდნენ, რომ კიბერსივრცეში ნატომ ისევე ეფექტიანად 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. შთამბეჭდავია ნატო-ს გენერალური მდივნის იენს სტოლტენბერგის სიტყვები: "ნატოს 30-ვე წევრი ქვეყანა უპასუხებს რომელიმე მათგანზე სერიოზულ კიბერშეტევას".[19]

ამერიკის შეერთებულ შტატებში არ იშურებენ ძალისხმევას, რათა შეიმუშაონ კიბერუსაფრთხოებასთან დაკავშირებით ახალი რეგულაციები და ასევე არ იშურებენ 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. 2007 წელს შეერთებული შტატების სამხედრო-საჰაერო ძალებში შეიქმნა კიბერსარდლობა, რომელმაც იარსება 2008 წლის ბოლომდე, შემდეგ კი ეს ფუნქციები გადაეცა სამხედრო -საჰაერო ძალების კოსმოსურ სარდლობას.[20]

2011 წლის მაისში შეერთებულმა შტატებმა გამოაქვეყნა თავისი სტრატეგია კიბერსივრცის დაცვაზე, რომელსაც საფუძვლად უდევს საერთაშორისო პარტნიორებთან და კერძო სექტორთან თანამშრომლობის მოდელი, სადაც ღონისძიებები უნდა გატარდეს შვიდი მიმართულებით: **ეკონომიკა** - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ეროვნული ქსელის დაცვა - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა, სამართლებრივი მხარე - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება, **სამხედრო სფერო** - უსაფრთხოების თანამედროვე

[19] Stoltenberg Jens, "Nato: Cyber-attack on one nation is attack on all", 2019, 27 August, P. 1. https://www.bbc.com/news/technology-49488614, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

[20] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო. 2018. მოპოვებული https://rm.coe.int-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020

გამოწვევებზე მზადყოფნა, **სამთავრობო ინტერნეტის ქსელი** - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება, **თავისუფლება ინტერნეტში** - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა.

როდესაც კიბერთავდასხმების ყველაზე გავრცელებულ შეტევებს განვიხილავთ, ყურადღება უნდა გავამახვილოთ ტექნიკურ თავდაცვით მექანიზმებზეც, ანუ ვირუსების საწინააღმდეგო ვაქცინაზე, რომელსაც ანტივირუსს ვუწოდებთ. რომელია ყველაზე ეფექტური ანტივირუსები? საუკეთესო ანტივირუსული პროგრამებია: **Bitdefender Antivirus, Norton AntiVirus, Kaspersky Anti-Virus, Trend Micro Antivirus, Webroot SecureAnywhere AntiVirus, Avast antivirus, Sophos Home, ESET Antivirus,** ესენი გახლავთ ფასიანი ანტივირუსები, რომლებსაც გვთავაზობენ სხვადასხვა კომპანიები. თუმცა არსებობს „გატეხილი“ ვერსიებიც, ასევე ეს კომპანიებიც გვთავაზობენ საცდელ ვერსიებს ან უბრალოდ დაპალი ხარისხის პაკეტებს უფასოდ. 2020 წლისთვის საუკეთესო უფასო ანტივირუსებია: **Bitdefender Antivirus Free Edition, Avira Free Antivirus, Kaspersky Free, Avast Free Antivirus, Sophos Home.** როდესაც თქვენ გაქვთ მცირე თუ დიდი ბიზნესი, რა თქმა უნდა, თქვენს სისტემას უფრო დიდი დაცვა სჭირდება, ვიდრე ეს ჩვეულებრივ ინდივიდუალურ დონეზე ხდება. სხვადასხვა ანტივირუსულ კომპანიებს გააჩნიათ შესაბამისი მომსახურება. 2020 წლისთვის საუკეთესო ბიზნეს-ანტივირუსებია: **Avast Business Antivirus Pro, Bitdefender GravityZone Business Security, Symantec Endpoint Protection, Avira Antivirus for Endpoint, Kaspersky Endpoint Security Cloud.**[21]

რამდენად ეფექტურია აღნიშნული ანტივირუსები? განვიხილოთ ერთ-ერთი მათგანი, გავეცნოთ მის მონაცემებს. ამ მხრივ ერთ-ერთ ყველაზე დიდ კორპორაციას წარმოადგენს **„კასპერსკი“**.

[21] Williams Mike, "The best antivirus software for 2020", techradar - THE SOURCE FOR TECH BUYING ADVICE, 2020 Y. P. 1. Extracted: https://www.techradar.com/best/best-antivirus/, უკანასკნელად იქნა გადამოწმებული: 23.06.2020

„კასპერსკი“ წარმოადგენს რუსულ კომპანიას, რომელსაც ოფიციალურად იყენებენ სხვადასხვა ქვეყნებში, მათ შორის აშშ-ის სახელმწიფო სააგენტოებში. არსებობს ეჭვები, 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. „კასპერსკის“ 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.

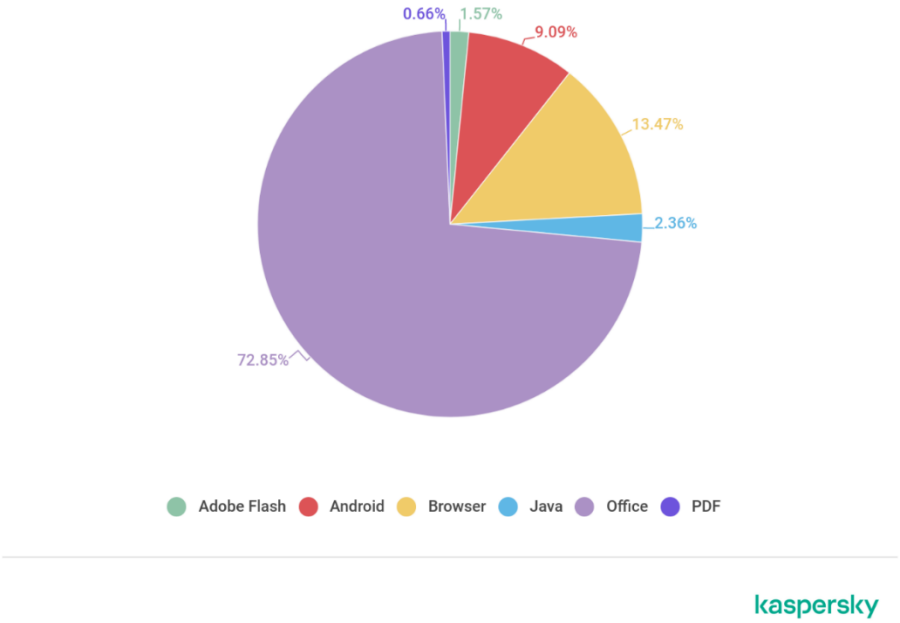
კიბერდანაშაულების მიერ გამოყენებული ექსპლუატაციების განაწილების შესახებ სტატისტიკის თანახმად, **Microsoft Office**-ის აპლიკაციების ნაკრებში

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.

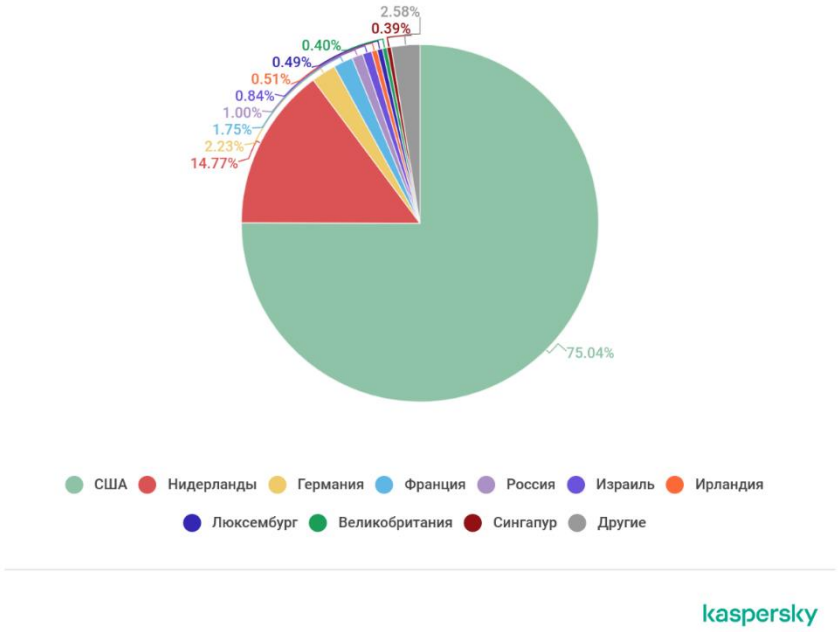


დიაგრამა 1

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 2

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** da 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".[22]

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 ხარვეზია შავი ბაზარი **(BM).** მისი აზრით, კიბერსივრცის მომხმარებელთა თავდაცვისუნარიანობა ჩვეულებრივ ჩამორჩება კიბერთავდამსხმელების შეტევებს. **კენეტი ასევე განმარტავს,** რომ შავი ბაზრების შესაძლო ზრდა პროგრამულ უზრუნველყოფაზე დაუცველობის შანსებს ზრდის. ძნელია **BM**-ების 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 ეს მაჩვენებელი ზრდადია. თუმცა რა განაპირობებს ზრდას, ამის თქმა რთულია. კენეტი წერს, რომ მათი ოპერაციების სიმულაციური სცენარი იწვევს ბაზრის დროებით შემცირებას, ინტერვენცია საბოლოოდ ხვდება პოლიტიკის წინააღმდეგობას და ვერ ახდენს განეიტრალებას. წიგნში ასევე მოყვანილია ცნობები სხვადასხვა უსაფრთხოების კომპანიების შესახებ:

„მრავალი უსაფრთხოების კომპანიის ცნობები, როგორიცაა **IBM ISS X-Force (2007), PandaLabs (2007) და Symantec (2008)** აღნიშნავენ კიბერშეტევების

[22] O'Leary Mike. "Cyber Operations Building, Defending, and Attacking Modern Computer Networks", Publishing House "Apress", Department of Mathematics, Towson University, MD, US, 2015 Y. P. 237-265.

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 საქონლით და პროდუქციით, მათ მიზანს საბოლოო ჯამში კი პირადი მონაცემების ქურდობა წარმოადგენს. **Symantec**-ის მოხსენებაში მკაფიოდ არის აღნიშნული, რომ შავი ბაზრები წარმოადგენს სერიოზულ საფრთხეს, როგორც პერსონალურ, ასევე გლობალურ დონეზე. შავი ბაზრის გამოყენებით სერიოზული საფრთხე ექმნება პერსონალური ინფორმაციის დაცულობას, ამას ჰაკერები ასევე იყენებენ კონკრეტული მომხმარებლებისა და კონკრეტული საიტების წინააღმდეგ, ბრაუზერებზე და ვებგვერდებზე კიბერ შეტევების განსახორციელებლად“.[23]

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 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.

[23] J. Knapp Kenneth, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", U.S. Air Force Academy, Colorado, USA, 2009 Y. P. 26-27

„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“.[24]

ამ მხრივ ყურადსაღებია ნატოს კიბერუსაფრთხოების მიმართულებები. ნატო, როგორც დახვეწილი თავდაცვითი პოლიტიკური და სამხედრო ალიანსი, დიდი ხანია მუშაობს ელექტრონული და ინფორმაციული ბრძოლის თავდაცვით მექანიზმებზე. მრავალი წლის განმავლობაში ნატო მჭიდროდ იყო ჩაბმული აშშ-ის მიერ განხორციელებულ პროექტებში, რათა მომხდარიყო სამხედროების „გარდაქმნა“.

ნატოს კომუნიკაციებისა და ინფორმაციის სისტემების მომსახურების სააგენტო (NCSA) წარმოდგენილია, როგორც ალიანსის პირველი ხაზი კიბერტერორიზმისგან თავდაცვის სფეროში. ასევე **ნატოს ინფორმაციის უსაფრთხოების ტექნიკური ცენტრი (NITC)**, რომელიც პასუხისმგებელია კომუნიკაციებსა და კომპიუტერულ უსაფრთხოებაზე. ეს ცენტრი ასევე პასუხისმგებელია მენეჯმენტზე, კრიპტოგრაფიულ აპარატურასა და კიბერშეტევებზე რეაგირების კოორდინაციაზე. **ნატოს კომპიუტერული ინციდენტების რეაგირების ცენტრს (NCIRC)** კი დაევალა ალიანსის დაშიფრული კომუნიკაციებისა და სისტემების დაცვა.

2007 წლის აპრილსა და მაისში ესტონეთის წინააღმდეგ კიბერშეტევების შემდეგ, ნატოს შტაბბინაში შეათანხმეს კიბერთავდაცვის კონცეფცია, ხოლო

[24] Dr Paul Cornish, "CYBER SECURITY AND POLITICALLY, SOCIALLY AND RELIGIOUSLY MOTIVATED CYBER ATTACKS", (Policy Department External Policies), FOREIGN AFFAIRS, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION DIRECTORATE B, POLICY DEPARTMENT, (Study carried out within the framework agreement between ISIS Europe and the European Parliament), Publisher European Parliament, Chatham House, London, February 2009, P. 8-9.

2008 წლის აპრილში ბუქარესტის სამიტზე მიღებულ იქნა კიბერთავდაცვითი პოლიტიკა შემდეგი პირობებით:

„ჩვენ მივიღეთ პოლიტიკური დოკუმენტი კიბერთავდაცვის შესახებ, რათა დავიცვათ ნატოში შემავალი სახელმწიფოები. ყველაზე მნიშვნელოვანია პრაქტიკის გაზიარება კიბერშეტევების მოგერიებისთვის. ჩვენ უნდა გავაძლიეროთ კიბერთავდაცვითი მექანიზმები და ქვეყნებს შორის კავშირები“.[25]

საქართველოს კიბერუსაფრთხოების ეროვნული სამოქმედო გეგმა ძალაში შევიდა 2017 წლის 13 იანვარს, სადაც შესავალშივე მითითებულია, რომ ეროვნული სტრატეგია ითვალისწინებს 2008 წელს განვითარებულ მოვლენებს. თუ კარგად წავიკითხავთ, ეს გეგმა აშკარად გამომდინარეობს ამერიკელების მიერ შემუშავებული სტრატეგიიდან, რომელიც ეფუძნება თითქმის იგივე პრინციპებს: მთავრობის მიდგომა, თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის, აქტიური საერთაშორისო თანამშრომლობა, ინდივიდუალური პასუხისმგებლობა, ადეკვატური ზომები. თუ აშშ-ში შექმნეს კიბერსარდლობა, რომლის უფლებამოსილება შემდგომში გადაეცა კოსმოსურ კიბერსარდლობას, საქართველოში 2014 წელს კიბერუსაფრთხოების უზრუნველყოფის მიზნით, თავდაცვის სამინისტროს დაქვემდებარებაში შეიქმნა **კიბერუსაფრთხოების ბიურო**, რომელიც ანხორციელებს კიბერინციდენტების პრევენციას უწყვეტ რეჟიმში. რაც შეეხება სამართალდაცვით საქმიანობას, აქ უკვე ჩაერთო შინაგან საქმეთა სამინისტრო, სადაც შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო. 2015 წელს შინაგან საქმეთა სამინისტროს გამოეყო ეროვნული უსაფრთხოების ბლოკი და ჩამოყალიბდა დამოუკიდებელ უწყებად - უსაფრთხოების სამსახურად, რომელიც პასუხისმგებელია კიბერსივრცეში აქტივობების გამოვლენაზე, პრევენციასა და აღკვეთაზე. 2013 წელს ახალი

[25] Dr Paul Cornish, "CYBER SECURITY AND POLITICALLY, SOCIALLY AND RELIGIOUSLY MOTIVATED CYBER ATTACKS", Publisher European Parliament, Chatham House, London, February 2009, P. 24.

კონსტიტუციის ამოქმედების შედეგად, ეროვნულ უსაფრთხოებასთან დაკავშირებული საკითხების დიდი ნაწილი გადავიდა მთავრობის დაქვემდებარებაში. საქართველოს მთავრობის კომპეტენციაში შევიდა ასევე კიბერუსაფრთხოების საკითხი.

1.3. ვირტუალური საფრთხე და ასიმეტრიული სამხედრო გამოწვევები

როგორც ზემოთ აღვნიშნეთ, 2002 წელს პრაღის სამიტზე ნატოს წევრ სახელმწიფოთა ლიდერებმა კიბერ-ტერორიზმი მნიშვნელოვან საფრთხედ აღიარეს და საჭიროდ მიიჩნიეს, შექმნილიყო „ნატოს კიბერთავდაცვის პროგრამა“, რომელიც მოიცავდა მოქმედებათა პროგრამის სამ ფაზას. პირველი ფაზისას შეიქმნა „ნატოს კომპიუტერული ინციდენტის საპასუხო უნარიანობა“ (NCIRC), რომელიც მეორე ფაზისას სრულ სამუშაო რეჟიმში შევიდა. მესამე ფაზას მოიცავს პირველი ორი ფაზისგან მიღებული გამოცდილების პრაქტიკაში დანერგვას და კიბერ-ტერორიზმთან ბრძოლაში თანამედროვე თავდაცვითი საშუალებების გამოყენებას. ამას აქვს გადამწყვეტი მნიშვნელობა.[26]

როგორც ჩანს, უკვე დადგა დრო, შეიქმნას კიბერუსაფრთხოების მსოფლიო ცენტრი, რომელიც გლობალური თვალსაზრისით გააკონტროლებს მიმდინარე მოვლენებს და დასახავს გეგმებს. ეს საკითხი უკვე დგას დღის წესრიგში.

აღსანიშნავია, რომ საქართველოში 2016 წელს გაიხსნა თავდაცვის ინსტიტუციური აღმშენებლობის სკოლა, რომელიც უზრუნველყოფს პროფესიული განვითარების ფართო შესაძლებლობებს, ხელს უწყობს გამოცდილების გაზიარებას, ასევე თავდაცვისა და უსაფრთხოების სფეროში თანამშრომლობის გაღრმავებას როგორც ეროვნულ, ისე რეგიონალურ და

[26] http://studinfo.edu.aris.ge/2013/11/12/nato-%E1%83%99%E1%83%98%E1%83%91%E1%83%94%E1%83%A0-%E1%83%A2%E1%83%94%E1%83%A0%E1%83%9D%E1%83%A0%E1%83%98%E1%83%96%E1%83%9B%E1%83%98%E1%83%A1-%E1%83%AC%E1%83%98%E1%83%9C%E1%83%90%E1%83%90/, უკანასკნელად იქნა გადამოწმებული: 11.06.2020

საერთაშორისო დონეზე. თავდაცვის ინსტიტუციური აღმშენებლობის სკოლის მიზანია ეროვნული, რეგიონალური და საერთაშორისო კურსების მეშვეობით გამოცდილების და საუკეთესო პრაქტიკის გაზიარება როგორც თავდაცვის, ასევე ფართო უსაფრთხოების სექტორისა და სამოქალაქო საზოგადოების წარმომადგენლებისთვის. სკოლა თანამშრომლობს ნატოს წევრ და პარტნიორ ქვეყნებთან, სასწავლო ფორმატში მათთან ერთად განიხილავს თავდაცვისა და უსაფრთხოების სფეროში არსებულ გამოწვევებს. სკოლა 2012 წელს ნატო-ს პროფესიული განვითარების პროგრამის მხარდაჭერით ჩამოყალიბებულ საქართველოს თავდაცვის აკადემიის პროფესიული განვითარების ცენტრის ბაზაზე დაარსდა.

აშშ-სა თუ ევროპულ ქვეყნებში რუსეთის ფაქტორს ახალი მიდგომებით განიხილავენ. სწორედ აშშ-ში ჩატარებულ არჩევნებში ჩარევის შემდეგ დააფიქრა მსოფლიო მომავალ საფრთხეებზე. თუკი რუსეთი ამდენს ბედავს სუპერ-სახელმწიფოს წინააღმდეგ, მაშინ რას უზამს განვითარებად ქვეყნებს? აშშ-ის ადმინისტრაცია ცდილობს, პრობლემები სანქციებით გადაჭრას. თუ რა ეფექტი აქვს ამ სანქციებს, ეს კვლევის ცალკე თემაა, არსებობენ ანალიტიკოსები, რომლებიც ამას დადებითად აფასებენ, მაგრამ ასევე არსებობენ უკმაყოფილონიც. მაგალითად, 2018 წლის ივნისში შეერთებული შტატების ხაზინის დეპარტამენტმა რუსეთის 3 მოქალაქეს და მათთან დაკავშირებულ 5 კომპანიას სანქციები დაუწესა. ხაზინის განმარტებით, ეს პირები რუსეთის სადაზვერვო სამსახურებთან თანამშრომლობდნენ და მათ შეერთებულ შტატებსა თუ მის მოკავშირეებზე კიბერთავდასხმების მოწყობაში ეხმარებოდნენ. სანქციების თანახმად, „გაიყინა“ ქონება, რომელსაც ეს პირები და კომპანიები შეერთებულ შტატებში ფლობენ. ნებისმიერ ამერიკელს კი მათთან ბიზნესსაქმიანობა აეკრძალა.

"შეერთებული შტატები აგრძელებს მავნე აქტორების წინააღმდეგ ბრძოლას, ძალისხმევას მათ წინააღმდეგ, ვინც მუშაობს რუსეთის ფედერაციის, მისი თავდაცვისა და დაზვერვის სამსახურების დავალებით, რათა გაზარდონ

რუსეთის კიბერთავდასხმების შესაძლებლობები", - განაცხადა სტივენ მნუჩინმა, ხაზინის მდივანმა.[27]

აშშ-ის დაზვერვის ცენტრალური სააგენტოს ყოფილი დირექტორი **მაიკლ ჰეიდენი** ამბობს, რომ გამოცდილების მსგავსებასთან ერთად, ბევრი მნიშვნელოვანი საკითხი "ცივი ომის" პერიოდის დროინდელი ვითარებისგან განსხვავებულია:

"ჩვენ, საზოგადოებას, ნასწავლი გვაქვს, რომ ახალი ამბები გამოცდილების შესაბამისად მივიღოთ. ვიცით, რომ ჩვენამდე ახალი ამბები გადამუშავებული ნაკადით, კარგად შერჩეული წყაროებიდან მოდის. არც ერთი ჩვენგანი ასეთ სამყაროში აღარ ცხოვრობს. ახალი ამბების მიღებასთან დაკავშირებული ჩვევები უკვე აღარ შეესაბამება ახალ რეალობას“.[28]

ევროპისა და რუსეთის საკითხებზე მომუშავე ექსპერტებს მიაჩნიათ, რომ გარდა აშშ-ისა თუ სხვა ქვეყნების გამოცდილებისა, მნიშვნელოვანი მაგალითი იყო საქართველოსა და უკრიანის წინააღმდეგ მიმართული კიბერ და საინფორმაციო ომები არა თუ ამ ქვეყნებისთვის, არამედ სხვებისთვისაც. **“სტრატეგიული და საერთაშორისო კვლევების ცენტრის"** ევროპის პროგრამის დირექტორი და ვიცე-პრეზიდენტი **ჰეთერ კონლი** "ამერიკის ხმასთანს" საუბარში ამბობს, რომ საქართველო და უკრაინა არის "რუსეთის პრაქტიკის, მისი გავლენისა და კიბერქმედებების ლაბორატორია".

"ორივე ქვეყანაზე იყო თავდასხმები, მათ გამოიმუშავეს მდგრადობა, ატარებენ რეფორმებს, ქმნიან ინსტიტუტებს, რომლებსაც ხალხი ენდობა“, - ამბობს **კონლი** და დასძენს, რომ დღევანდელ ვითარებაში ეს ყველაფერი არც ისე ადვილია. სანქციების პირობებშიც კი შეერთებული შტატების

---

[27] მნუჩინი, ს. *"საინფორმაციო ომის გაკვეთილები საქართველოსა და დასავლეთისთვის".* 2018.15.06. გვ. 1. მოპოვებული amerikiskhma.com: https://www.amerikiskhma.com/a/georgia-is-a-laboratory-of-how-russian-active-measures-work/4440995.html-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020

[28] ჰეიდენი, მ. *"საინფორმაციო ომის გაკვეთილები საქართველოსა და დასავლეთისთვის".* 2018.15.06. გვ. 1. მოპოვებული amerikiskhma.com: https://www.amerikiskhma.com/a/georgia-is-a-laboratory-of-how-russian-active-measures-work/4440995.html-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020

მთავრობის ერთიანი სტრატეგია რუსეთის მიმართ ნათელი და მკაფიო არ არის. მისი თქმით, სანქციების პარალელურად, ამერიკის ხელისუფლების ყოვლისმომცველი პოლიტიკისა თუ სტრატეგიის ჩვენებაა საჭირო. ვაშინგტონში გამართულ შეხვედრაზე კონლიმ ასევე ვრცლად ისაუბრა იმაზეც, რომ კრემლის მავნე ქმედებების, პროპაგანდისა თუ საინფორმაციო ომებისას გამოყენებული სხვა ტექნოლოგიების წინააღმდეგ ღონისძიებები რამდენიმე კატეგორიად შეიძლება დაიყოს, ესენია: იდენტიფიცირება, სტაბილიზება და მობილიზება. ანალიტიკოსი ხსნის, რომ პირველ ეტაპზე აუცილებელია მოსახლეობისთვის იმის ახსნა თუ რა ხდება და ვინ ვინ არის.[29]

უცხოელი ექსპერტები უკრაინასა და საქართველოს, საინფორმაციო ომის თვალსაზრისით, რუსეთის ლაბორატორიად მოიხსენიებენ და აღნიშნავენ, რომ ეს გაკვეთილი უნდა იყოს სხვა ქვეყნებისთვისაც. **"ინფორმაციის თავისუფლების განვითარების ინსტიტუტის" (IDFI)** მიერ შემუშავებულ დოკუმენტში - **"კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ"**, კარგადაა ჩამოყალიბებული, თუ რაში მდგომარეობს მთავარი საფრთხე. ბოლო წლებში გაზრდილი მასშტაბის გათვალისწინებით, კრემლის საინფორმაციო ომი თვისობრივად ახალ პრობლემად უნდა ჩაითვალოს, რომელიც ასევე გადაჭრის ახალ გზებს საჭიროებს. ამ დასკვნამდე უკვე მივიდნენ კრემლის პროპაგანდის მთავარი სამიზნე ქვეყნები და ინსტიტუტები, რომლებიც ბოლო წლების განმავლობაში აქტიურად მუშაობენ პროპაგანდასთან დაპირისპირების სტრატეგიებზე. თუ საქართველოს მთავრობა ვერ შეძლებს კრემლის პროპაგანდისთვის წინააღმდეგობის გაწევას, შესუსტდება ევროპული და ევროატლანტიკური ინტეგრაციის მიმართ საქართველოს მოსახლეობის მხარდაჭერა და გაიზრდება რუსეთთან დაახლოების მხარდამჭერთა რიცხვი, რითიც

[29] ჰეთერ, კ.. *"საინფორმაციო ომის გაკვეთილები საქართველოსა და დასავლეთისთვის".* 2018.15.06. გვ. 1. მოპოვებული amerikiskhma.com: https://www.amerikiskhma.com/a/georgia-is-a-laboratory-of-how-russian-active-measures-work/4440995.html-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020

საფრთხე შეექმნება ქვეყნის ევროატლანტიკურ კურსს და უსაფრთხოებას. მტრულ ძალას მიეცემა საშუალება, იქონიოს გავლენა ქვეყნის პოლიტიკურ დღის წესრიგზე, რითიც საფრთხე შეექმნება საქართველოს სუვერენიტეტს. დეზინფორმაციული კამპანიის შედეგად საქართველოს ამომრჩეველთა შორის გაიზრდება გაურკვევლობისა და დისონანსის დონე, რაც ხელს შეუშლის ამომრჩეველს, მიიღოს ფაქტებზე და არა ემოციებზე დაფუძნებული გადაწყვეტილება. საზოგადოებაში გაძლიერდება ქსენოფობია და გაღვივდება ეთნიკური და რელიგიური შუღლი, შესუსტდება სამოქალაქო ერთიანობა და გართულდება ეთნიკური უმცირესობების პოლიტიკური და საზოგადოებრივი ინტეგრაცია.

კრემლის საინფორმაციო ომი, მისი მასშტაბებიდან გამომდინარე, ისეთი დონის პრობლემაა, რომ მხოლოდ სახელმწიფოს აქვს საკმარისი ბერკეტი და რესურსი, გაუწიოს მას ეფექტური წინააღმდეგობა.

საქართველოში კრემლის პროპაგანდის ძირითადი საყრდენი მედიასაშუალებები და სოციალური ქსელებია. მინიმუმ ერთი ტელევიზია, რამდენიმე ინტერნეტ-ტელევიზია, ბეჭდური გამოცემა და ვებ-გვერდი გამოირჩევა ანტიდასავლური „მესიჯ-ბოქსით“ და ინფორმაციის გავრცელებისას ძირითადად ეყრდნობა რუსულ წყაროებს. თვალშისაცემია რუსული პროპაგანდის გამავრცელებლების მიერ სოციალური ქსელების აქტიური გამოყენებაც, როდესაც ხდება დეზინფორმაციის ან ანტიდასავლური ნარატივის შემცველი ინტერნეტმასალების ვირუსული გავრცელება. საზოგადოებრივი აზრის გამოკითხვები აჩვენებს, რომ საქართველოში ინფორმაციის მიღების ძირითადი წყარო ტელევიზიაა. **ეროვნულ-დემოკრატიული ინსტიტუტის (NDI)** 2016 წლის გამოკითხვის მიხედვით, საქართველოს მოსახლეობის 77% პოლიტიკისა და მიმდინარე მოვლენების შესახებ ინფორმაციის მიღების პირველ წყაროდ 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).[30]

პროდასავლური არასამთავრობო ორგანიზასციები თავიანთ ანგარიშებში ხშირად მიუთითებენ, რომ საქართველოში კრემლის პროპაგანდის კიდევ ერთი მნიშვნელოვანი საყრდენია ბოლო დროს მომრავლებული პრორუსული არასამთავრობო ორგანიზაციების ქსელი, რომელთა შორის განსაკუთრებით ორი ორგანიზაციის გამოყოფა შეიძლება - **„ევრაზიის ინსტიტუტი“** და **„ევრაზიული არჩევანი“**. მათი მტკიცებით, ეს ორგანიზაციები გამოირჩევიან ანტიდასავლური რიტორიკით და იმით, რომ ანალიტიკური ნაშრომების თუ სტატიების გამოქვეყნებისას ეფუძნებიან რუსულ წყაროებს. საჯარო რეესტრის მონაცემების მიხედვით, პრო-რუსული არასამთავრობო ორგანიზაციების დამფუძნებელთა და ხელმძღვანელთა სიაში, ხშირად, ერთი და იგივე პირები მეორდებიან. ორგანიზაციებს შორის კავშირი მათ ვებ-გვერდებზეც არის მითითებული. გარდა ამისა, პრორუსული არასამთავრობო ორგანიზაციების ამ ქსელს ასევე აქვს კავშირები ანტიდასავლური რიტორიკით გამორჩეულ ზოგიერთ საინფორმაციო საშუალებასთან. შეიძლება პროდასავლური არასამთავრობო ორგანიზაციები ნაწილობრივ არც ტყუიან, მაგრამ მათ მიერ დასახელებული პრორუსული არასამთავრობოები ამტკიცებენ, რომ საქმე პირიქითაა - ანუ საქართველოს პროდასავლურ კურსს ხელს უშლიან ის ორგანიზაციები, რომლებიც 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

[30] "ინფორმაციის თავისუფლების განვითარების ინსტიტუტის" (IDFI). *"კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", პოლიტიკის დოკუმენტი.* 2016.22.08. გვ. 5-23. მოპოვებული idfi.ge: https://idfi.ge/public/upload/Meri/Russian%20Propaganda%20in%20Georgia%20-%20Policy%20Paper.PDF-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020

აშკარად შეინიშნება პირადი ინტერესები. ეს უფრო გამოკვეთილად გამოჩნდა საპრეზიდენტო არჩევნებში. შეიძლება ჩვენ **"საერთაშორისო გამჭვირვალობა - საქართველოს"** ორიენტაციაში ეჭვი არ შევიტანოთ, მაგრამ როცა გადაუმოწმებელ ინფორმაციაზე სკანდალს აგებ, ეს მიანიშნებს, რომ არსებული ხელისუფლების მიმართ მტრულად ხარ განწყობილი და გინდა თუ არა, სახელმწიფოებრიობასაც უთხრი ძირს. ამ შემთხვევაში ვგულისხმობთ ყალბი პირადობის მოწმობების ვითომ დაბეჭდვის თემას. გამოდის ქალბატონი **ეკა გიგაური** კიდევ ორი არასამთავრობოს ხელმძღვანელთან ერთად, ატარებს პრესკონფერენციას, მოსახლეობას არწმუნებს, რომ ხელისუფლება საარჩევნოდ ბეჭდავს ყალბ პირადობის მოწმობებს და ამ დროს ირკვევა, რომ ის, ვინც მათ ინფორმაცია მიაწოდა, საერთოდ არ ესწრებოდა სერვისების განვითარების ცენტრში ჩატარებულ თათბირს და მოგვიანებით ისიც ირკვევა, რომ მსგავსი თათბირი საერთოდ არ ჩატარებულა. არის თუ არა ეს ყველაფერი საინფორმაციო ომის შემადგენელი ნაწილი? რა თქმა უნდა, არის. 2019 წლის საპრეზიდენტო არჩევნებში ცილისწამება და სიცრუე განუსაზღვრელი დოზით იყო წარმოდგენილი - მაგალითად, ასევე სიცრუე კარგად შეფუთა რუსულმა პიარ-ჯგუფმა **გრიგოლ ვაშაძის** სასარგებლოდ 400-ლარიანი პენსიის თემაც. მიუხედავად იმისა, რომ იგივე **ვაშაძემ** კარგად იცოდა, პრეზიდენტობის შემთხვევაში, ვერანაირ პენსიას ვერ გაზრდიდა, ეს მხოლოდ მთავრობის პრეროგატივაა, მაინც წავიდა ავანტიურაზე და თქვენ წარმოიდგინეთ, ბევრმა პენსიონერმა დაიჯერა, მით უფრო რეგიონებში. ეს გახლავთ ნათელი მაგალითი, თუ როგორ უნდა "აჭამო" საკუთარ ხალხს და როგორ უნდა იკადრო ყველაფერი. ასეთივე ეფექტი ჰქონდა ყალბი პირადობების ბეჭდვის ამბავსაც - კი, ბატონო, არ არსებობდა რეალური ფაქტი, არ არსებობდა მტკიცებულება, მაგრამ რაკი ე.წ. ავტორიტეტულმა ორგანიზაციებმა გაავრცელეს ინფორმაცია, ლამის მთელმა საქართველომ დაიჯერა. რა მოჰყვა ამას? არავითარი ბოდიში, არავითარი ახსნა-განმარტება, არავითარი სინანული - გამოდის, ეს გახლდათ გამიზნული პროვოკაცია და

საინფორმაციო ომის ერთი დეტალი. არასამთავრობო ორგანიზაციების ნაწილი იმაზეც წერს, რომ საქართველოში მომრავლდა პრორუსული ორიენტაციის პოლიტიკური პარტიები. ხშირად კეთდება განცხადებები, რომ რიგი პოლიტიკური პარტიები და პოლიტიკური მოღვაწეები, პირდაპირ ან ირიბად, ავრცელებენ კრემლის პროპაგანდას. ამ პოლიტიკური პარტიებს ყოფენ ორ ნაწილად: პარტიები, რომლებსაც ღიად პრორუსული დღის წესრიგი აქვთ, ხვდებიან რუს პოლიტიკოსებს და სტუმრობენ მოსკოვს; პარტიები, რომლებიც დეკლარირების დონეზე ემიჯნებიან რუსულ პოლიტიკურ ელიტას და სანაცვლოდ საკუთარ თავს აცხადებენ „პრო-ქართულ“, ნეიტრალიტეტის მომხრე პარტიებად.

განსხვავების მიუხედავად, ორივე სახის პოლიტიკური პარტიების ძირითადი გზავნილები ევროპულ და ევროატლანტიკურ სტრუქტურებში გაწევრიანების მიმართ სკეპტიციზმის გაღვივებას უწყობს ხელს. საქართველოს დასავლური ინსტიტუტებისკენ სწრაფვა წარმოჩენილია, როგორც უშედეგო; სანაცვლოდ, ხდება პრორუსული განწყობისა და საქართველოს ნეიტრალიტეტის იდეის პოპულარიზაცია. აღსანიშნავია, ასევე, საქართველოს პარლამენტის მოქმედი თუ ყოფილი წევრების მხრიდან საქართველოს ევროპულ და ევროატლანტიკურ სტრუქტურებში ინტეგრაციასთან დაკავშირებით წინააღმდეგობრივი გზავნილების და ზოგჯერ მკაფიოდ ანტიდასავლური განცხადებების გავრცელება, რაც, ირიბად თუ პირდაპირ, კრემლის პროპაგანდის მიზნებს ემსახურება. მეტიც, არასამთავრობო ორგანიზაციების ნაწილი ეჭვობს, რომ ანტიდასავლურ კამპანიაში ჩართულნი არიან სასულიერო პირებიც, რომლებიც დასავლურ კულტურასთან ქართული ტრადიციების შეუთავსებლობის მითს ასევე ავრცელებენ საქართველოს ეკლესიის კონსერვატიული ფრთის წარმომადგენლები. ბევრი სასულიერო პირი ქადაგებაში ავითარებს აზრს რუსეთთან ცივილიზაციური ერთობისა და დასავლეთთან იდეური თუ მორალური შეუთავსებლობის შესახებ. სასულიერო პირების ზოგიერთი წარმომადგენლის მხრიდან კრემლის პროპაგანდისტული გზავნილების

ირიბად თუ პირდაპირ გავრცელება, სერიოზულ პრობლემას წარმოადგენს, ვინაიდან, ქართულ საზოგადოებაში ისინი მაღალი ნდობით და გავლენით სარგებლობენ. პრორუსული ორიენტაციის მღვდელთმსახურები საზოგადოებაში სარგებლობენ მაღალი ნდობით და გავლენით. ეს არ შეიძლება შემთხვევითი იყოს, გამოდის, საზოგადოებას მოსწონს და აღიარებს მათ ორიენტაციას. თუ საზოგადოება მოხიბლულია ასეთთა ქადაგებებით, მაშინ პრობლემა მოსახლეობაშია და ისევ მივდივართ პროდასავლური ძალების უნიათობამდე, ანუ მუშაობის არადამაკმაყოფილებელ შედეგებამდე.

რუსეთი არის ჩვენთვის ყველა უბედურების სათავე და ყველაზე დიდი პრობლემა. თუმცა ეს უბედურება და პრობლემა რომ არ გადაიქცეს მარადიულ შავ ჭირად, ოქროს შუალედია მოსაძებნი. ბევრი ქადაგებს უტოპიურ ჟანრში იმის თაობაზე, რომ აგერ, რუსეთი დღე-დღეზე დაიშლება, გაცამტვერდება და ჩვენც, რასაკვირველია, გვეშველება. მეორე - რუსეთში მოვა დემოკრატიული ხელისუფლება და ტერიტორიებს უპრობლემოდ შემოვიერთებთ. 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. ვინც რუსულ პოლიტიკურ ხასიათს კარგად იცნობს, რაც არ უნდა დიდ დემოკრატიასთან გვქონდეს საქმე, ის მაინც შოვინისტური იქნება. ჩვენ ამ ეტაპზე გვჭირდება საინფორმაციო ომის მაღალ დონეზე წარმოება და ამ სფეროში საუკეთესო თავდაცვა.

თავი II. კიბერომი, როგორც ასიმეტრიული საფრთხის ფენომენი

საერთაშორისო უსაფრთხოების გარემო რომ უსაფრთხოების მექანიზმების მზარდ მოდერნიზებას საჭიროებს, ამ მხრივ ორი აზრი აღარ არსებობს. საინფორმაციო ომის საფრთხეების, რისკების და გამოწვევების დონე საკმაოდ მაღალია. საინფორმაციო ომისგან და მისი ყველაზე მძლავრი კომპონენტისგან - დეზინფორმაციისგან თავის დაცვა არც თუ ისე მარტივია. ცალკეული ქვეყნების მიერ გატარებული ზომები და ღონისძიებები ხშირ შემთხვევაში საკმარისი არ არის. კიბერ და საინფორმაციო ომების ეფექტურობას ხელი შეუწყო მეცნიერულმა და ტექნოლოგიურმა წინსვლამ, რამაც გამოიწვია გარკვეული მასების მანიპულაცია და კონტროლი. ამ მხრივ მნიშვნელოვანია საერთაშორისო ორგანიზაციების ჩართულობა, ერთიანი სტრატეგიული დოკუმენტებისა და თავდაცვის მექანიზმების შემუშავება. საინფორმაციო ომის გაჩაღებამ და ტექნოლოგიების ათვისებამ გლობალური მასშტაბით გავლენა მოახდინა დიდ სახელმწიფოებზეც, როგორებიც არიან რუსეთი და აშშ. მათი ინტერესები ბევრი მიმართულებით მცირე ქვეყნების მოსახლეობასა და ტერიტორიებზე გადის, მათ შორის საქართველოზეც. რუსეთი აქტიურად აწარმოებს საინფორმაციო ომს ბალტიის ქვეყნებთან - ლიტვა, ლატვია, ესტონეთი. ასევე მასშტაბურ საინფორმაციო-დეზინფორმაციულ თავდასხმებს ახორციელებს ისეთ ქვეყნებზე, როგორიც საქართველო და უკრაინაა. ამას სათანადო წინააღმდეგობას ვერც ერთი ნახსენები ქვეყანა დამოუკიდებლად ვერ გაუწევს. ამიტომაც ნატოსა და ევროკავშირის დახმარებით ხორციელდება და ვითარდება თავდაცვითი მექანიზმები. ამ მიმართულებით აქტიურ მონაწილეობას იღებს სამხედრო თუ ტექნიკური თვალსაზრისით აშშ-ც. ბალტიისპირეთის ქვეყნებმა - ესტონეთმა, ლატვიამ და ლიტვამ კი დაიხსნეს თავი საბჭოთა რეჟიმისგან, 2004 წელს სამივე სახელმწიფო ევროკავშირსა და ნატოშიც გაწევრიანდა, მაგრამ ამ რეგიონში რუსეთს კვლავ გააჩნია შოვინისტური ინტერესები და დასავლეთთან დაპირისპირების წყალობით წითელ ხაზად, ანუ ერთგვარ ბუფერულ ზონადაც აქცია. პოლიტოლოგების მტკიცებით, დღეს რუსეთი

ვეღარ წავა შეიარაღებულ გამწვავებაზე, ვეღარ გამოიყენებს პირდაპირი აგრესიის ფორმებს, რადგან ფიზიკურად, ასე ვთქვათ, ეჯახება ჩრდილო ატლანტიკურ ალიანსს და ასევე ევროკავშირის ინტერესებს. თუმცა არსებობს ე.წ. ცივი ომის სხვადასხვა ფორმები, რაც გამოიხატება კიბერთავდასხმებისა და საინფორმაციო ომის მეთოდებით.

იბადება კითხვა: რა ინტერესი აქვს რუსეთს დამოუკიდებელი სახელმწიფოების მიმართ? უპირველესად ის, რომ დაპყრობაზე ორიენტირებული უზარმაზარი ქვეყანა ამ სამი სახელმწიფოს მიღებას ნატოში, ლამის საკუთარი საზღვრების ხელყოფად აღიქვამს. 2004 წელს სტამბულის სამიტზე მიღებული გადაწყვეტილება შოკისმომგვრელი აღმოჩნდა კრემლისთვის და აქედან დაიწყო კიდეც მზადება, რათა ნატო მეტად აღარ გაფართოვებულიყო. ფაქტობრივად, აღმოსავლეთ ევროპაში დასავლეთის ასეთი ხისტი ნაბიჯი მოულოდნელი იყო რუსეთისთვის. რომ არა დასავლეთისა და აშშ-ის მონდომება, კრემლი შეეცდებოდა, ისეთივე სცენარი გაეთამაშებინა, როგორიც გაათამაშა უკრაინასა და საქართველოში, ანუ სამივე ქვეყანაში სიტუაციას არევდა სამხედრო გზით. შესაძლოა, ბალტიისპირეთში განხეთქილების შეტანა გასჭირვებოდა, მაგრამ რუსეთი მაინც დაიწყებდა რეგიონის გახლეჩვის პროცესს, რაც ხელს შეუშლიდა ნატოში გაწევრიანებას. მით უმეტეს, როცა ამ სახელმწიფოებში საბჭოთა დროს ჩასახლებული რუსულენოვანი მოსახლეობა არცთუ ცოტაა - 10%. ასე ბალტიის ქვეყნებმა "გაასწრეს", განაპირობა რამდენიმე ფაქტორმა: პირველი - 2004 წლამდე თვით რუსეთშიც არ იყო მთლად დალაგებული სიტუაცია, მეორე - როდესაც კრემლმა გამოსცა ე.წ. დეკრეტი საკუთარი მოქალაქეების დაცვის თაობაზე ნებისმიერ ქვეყანაში, ბალტიისპირელებმა თავიდანვე გაითვალისწინეს და შეძლებისგვარად გაწმინდეს საკუთარი სახელმწიფოები, ანუ რუსულენოვანი მოსახლეობის დიდ ნაწილს არ მისცეს მოქალაქეობა, ამ მხრივ დაწესდა მთელი რიგი შეზღუდვები. გარდა ამისა, მას შემდეგ, რაც ამ სამმა სახელმწიფომ თავი შეაფარა ნატოს „ქოლგას“, ტექნოლოგიებისა და თავდაცვითი სისტემების წყალობით, შედარებით

ეფექტურად შეუძლია კიბერთავდასხმების მოგერიება, რაც (ვაღიაროთ) ვერ ხერხდება საქართველოსა და უკრაინის შემთხვევაში. მიუხედავად ყველაფრისა, რუსეთი პერიოდულად მაინც ანხორციელებს კიბერთავდასხმებს ბალტიის ქვეყნებზე - მაგალითად, 2007-2009 წლებში დიდი შეტევა იყო ესტონეთზე, რის შემდეგაც კრემლის ახალგაზრდული ორგანიზაციის - **"ნაში"-ს** ერთ-ერთმა აქტივისტმა აღიარა, რომ ის იყო ბალტიისპირეთის ქვეყნებზე კიბერთავდასხმის სულისჩამდგმელი.[31]

საერთოდ, რუსულ ჰიბრიდულ ომებს ახასიათებს ზეთის ე.წ. თვისება, თუ დაიღვარა, ყველა თავისუფალ ჭუჭრუტანაშიც კი აღწევს. ფაქტია, ბალტიისპირეთის სახელმწიფოების მესვეურებმა საბჭოთა სისტემის დაშლის შემდეგ უკეთესად იმუშავეს, უკეთესად ამოქოლეს შავი ხვრელები, ვიდრე ეს მოხდა უკრაინასა და საქართველოში. უკვე აღვნიშნეთ, კრემლის ინტერნეტსაბრძოლო „ხელოვნებაში" ახალი არაფერია - მეთოდები ისევ საბჭოთაა, მაგრამ რუსებმა ყოველივე კარგად მოარგეს ახალ ტექნოლოგიებს.

რა შეცვალა და რა შეიძლება შეცვალოს **Covid-19**-მა მსოფლიო მასშტაბით და რას შეცვლის კიბერომების თვალსაზრისით? ფაქტია, ვირუსმა მთელი მოსახლეობაზე გავლენა იქონია და ადამიანების ცხოვრების დღის წესრიგი შეცვალა, საფრთხე შეუქმნა როგორც ადამიანის ჯანმრთელობას, ასევე ეკონომიკას. საფრთხე მრავალმხრივია - ჩაიკეტა საზღვრები, აიკრძალა ფრენები, მსოფლიო მასშტაბით უამრავ ქვეყანაში გამოცხადდა საყოველთაო კარანტინი, საგანგებო სიტუაცია, კომენდანტის საათი, გადაადგილების შეზღუდვა. დაიკეტა მაღაზიები, ქარხნები, შეჩერდა და შეფერხდა სწავლა-განათლება. როგორც ამბობენ, მოვლენების ასე დრამატულად და სწრაფად განვითარებას არავინ ელოდა. სხვადასხვა გამოცემები მსოფლიო მასშტაბით, უამრავი პოლიტიკოსი და ექსპერტი თანხმდება იმაზე, რომ ვირუსმა

[31] ლოლაძე, გ. *"დეზინფორმაცია, თითქოს რუსეთის კიბერშეტევებს მხოლოდ ერთი წყარო ადასტურებს"*. 2019.26.03. გვ. 1. მოპოვებული mythdetector.ge: http://www.mythdetector.ge/ka/myth/dezinpormatsia-titkos-rusetis-kibershetevebs-mkholod-erti-cqaro-adasturebs-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020

შეცვალა ადამიანების ყოველდღიური ცხოვრება და ურთიერთობები. იმ აზრსაც მოისმენთ, რომ ეს ვირუსიც გაივლის, მაგრამ ცხოვრება ისეთი აღარასდროს იქნება, როგორიც **Covid-19**-ის გავრცელებამდე იყო. ამ მოსაზრებებს კი ნამდვილად უნდა დავეთანხმოთ. ცხოვრება აღარასდროს იქნება ისეთი, როგორიც იყო ვირუსამდე.

რეალურმა სამყარომ დიდი დოზით გადაინაცვლა ვირტუალურ სივრცეში, უამრავი კომპანია და სახელმწიფო უწყება გადავიდა დისტანციურ მუშაობაზე. ალბათ ეს არც არის გასაკვირი, მაგრამ ამ ფონზე ძალიან დიდ სარგებელს იღებენ ჰაკერები, სპამერები, თაღლითები და ისეთი ადამიანები, რომლებიც ინტერნეტსივრცეს და სოციალურ ქსელებს პირადი ინტერესებისთვის თაღლითურად იყენებენ.

მაგალითად, კორონათი **(„ფიშინგით“)** თაღლითობა აქტუალურად დაიწყო ვირუსის გავრცელების დღიდან. მავანნი ცდილობენ, უფრო მეტი შიში და დაბნეულობა დანერგონ ინტერნეტმომხმარებლებში. დაიწყო ჰაკერული თავდასხმები ჰოსპიტალებზე გამოსასყიდის სანაცვლოდ, რამაც ხელი შეუშალა კორონავირუსით დაინფიცირებული ხალხის სწრაფად გამოკვლევას და მოქმედებებს. ამ თავდასხმებმა შეაჩერა ოპერაციები და გამოიწვია მათი გადადება. ასეთი შეტევები უდიდეს საფრთხეს უქმნის პაციენტების ჯანმრთელობას. ასეთი კიბერთავდასხმები განსაკუთრებით საშიშია პანდემიის დროს, რომელიც მსოფლიო ჯანდაცვის სისტემას ახლა კისერზე აწევს.

კრიზისის დროს არავინ არის დაცული. ვითარება დიდი გამოწვევების წინაშე აყენებს ციფრულ უსაფრთხოებას. მოვლენების კვალდაკვალ, **„ვაშინგტონ პოსტმა“** გამოაქვეყნა სტატია სათაურით: **„ჰაკერები კორონავირუსთან დაკავშირებულ შიშებს იყენებენ პირადი მონაცემების მოსაპარად“** - გაფრთხილება ექსპერტებისგან და აშშ-ის რეგულატორებისგან“. აღნიშნულ სტატიაში განხილულია კორონავირუსის შემდეგ ჰაკერული თავდასხმების ნაკადის მზარდი მატება, ამასთან დაკავშირებით ისრაელში მომუშავე კიბერუსაფრთხოების ორგანიზაციამ

„Check Point“-მა გამოაქვეყნა ანგარიში, სადაც გამოკვეთილია ყველაზე დახვეწყილად მომუშავე ჰაკერული ჯგუფის წამოწყებული კამპანია, რომელსაც უწოდეს **“Vicious Panda”**, ანუ „მოწინავე საფრთხე“. ანგარიშში ნათქვამია, რომ **“Vicious Panda”**-მ, ანუ ჰაკერულმა ორგანიზაციამ, გამოიყენა ყალბი დოკუმენტები, გაავრცელა ფეიკ-ინფორმაციები მონღოლეთის ჯანდაცვის მინისტრის სახელით, რომელიც კორონავირუსის ინფექსიის შესახებ სავალალო მდოგმარეობას ამცნობდა მსოფლიოს. ჰაკერებს მიზნად ჰქონდათ, რომ ბევრ ადამიანს გაეხსნა აღნიშნული ინფორმაცია, რის შედეგადაც მათ წვდომა ექნებოდათ მომხმარებლების პირად მონაცემებზე, ეს იქნებოდა სმარტოფნების თუ კომპიუტერების საშუალებით. ანგარიშში **“Check Point”**-ის თავდაცვის დაზვერვის უფროსის, ლატე ფინკლინტინის განცხადებაცაა მოცემული, სადაც ის აფრთხილებს ყველა საჯარო სექტორის სუბიექტს და სატელეკომუნიკაციო კომპანიებს: „**Covid-19** წარმოადგენს არა მხოლოდ ფიზიკურ საფრთხეს, არამედ კიბერ საფრთხესაც, ყველა საჯარო სექტორის სუბიექტი და სატელეკომუნიკაციო კომპანია უნდა იყოს ფრთხილად კორონავირუსის გარშემო არსებული დოკუმენტაციასთან და ვებსაიტებთან“.[32]

მსოფლიო მასშტაბით უამრავი ექსპერტის მოსაზრებას შეგვიძლია გავეცნოთ. მაგალითად, კიბერუსაფრთხოების დამოუკიდებელი ექსპერტის, **ლუკას ოლეჯინიკის (Lukasz Olejnik)** თქმით, დღეს ამ მასშტაბური გლობალური კრიზისის დროს მსოფლიო სრულიად არის დაუცველი და შესაძლოა, ვითარება უფრო გაუარესდეს.[33]

ამ შემთხვევაში არც საქართველოა გამონაკლისი, აქ უფრო მცირე დოზით, მაგრამ მაინც ხდება მსგავსი თავდასხმები, როგორც ჰაკერულ, ასევე

[32] Timberg Craig & Romm Tony, "Hackers are seizing on coronavirus fears to steal data, researchers and U.S. regulators warn", March 12, 2020. P. 1. Extracted https://www.washingtonpost.com/technology/2020/03/12/hackers-are-using-coronavirus-fears-target-people-looking-information-infection-maps/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

[33] Lily Hay Newman, "Coronavirus Sets the Stage for Hacking Mayhem", 03.19.2020, P. 1. Extracted: https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

ინფორმაციულ დონეზე. მაგალითად ჰაკერებმა საქართველოს **4 934 863** მოქალაქის (მათ შორის გარდაცვლილი პირების) პერსონალური ინფორმაცია გამოაქვეყნეს. ამის საკითხს ამერიკულმა ინტერნეტ-გამოცემამ - **ZDNet**-მა ვრცელი სტატია მიუძღვნა.[34] 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, მაგრამ 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 არის.

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".**[35] ეს კიდევ უფრო ამყარებს ეჭვებს, რომ მიზანმიმართულად ხდებოდა მოსახლეობაში პანიკის დათესვა. შინაგან საქმეთა სამინისტრომ განაცხადა, რომ აღნიშნული

[34] Cimpanu Catalin, "Personal details for the entire country of Georgia published online", March 30, 2020. P. 1. Extracted: https://www.zdnet.com/article/personal-details-for-the-entire-country-of-georgia-published-online/?fbclid=IwAR0Jp5j_NCrdw9Et4k80WGwhWW3r2l2FV6COSv7MYWTqj6Qd9YpV_50jcA8, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

[35] საქართველოს შინაგან საქმეთა სამინისტრო, "შსს-ს სახელით მოქალაქეებს მესიჯები მიუვიდათ - რა განცხადებას ავრცელებს სამინისტრო", 02.04.2020, გვ. 1. მოპოვებულია: https://www.ambebi.ge/article/243012-shss-s-saxelit-mokalakeebs-mesijebi-miuvidat-ra-g/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

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 საზოგადოებაში პანიკა გამოიწვია. ინტერნეტმომხმარებლები უნებურად ხდებიან ინტერნეტვირუსების მსხვერპლნი, ინფორმაციის მოძიებისას თავისთავად ხვდებიან ისეთ ვებ-გვერდებზე, რომელიც ავტომატურ რეჟიმში ახდენს დავირუსებული პროგრამის ჩამოტვირთვას. ჰაკერები აყალბებენ სხვადასხვა რუკებს, პროგრამებს, რომელიც უშუალოდ უკავშირდება კორონავირუსს. ისინი 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. ეს აძლევს ჰაკერს წვდომას თქვენს მონაცემებზე. რაც რეალურად ძალიან დიდ საფრთხეს უქმნის პირადი მონაცემების დაცვას და მათ გამოყენებას უნებართვოდ.[36]

2.1. კიბერუსაფრთხოების პოლიტიკა და ჰიბრიდული ომი (ირანის ისლამური რესპუბლიკის შემთხვევის გარჩევა)

2020 წლის 3 იანვარს ერაყში, ბაღდადის აეროპორტის მახლობლად აშშ-ის სარაკეტო დარტყმას ირანის ისლამური რევოლუციის გუშაგთა კორპუსის სპეცდანიშნულების რაზმ **„ალ-ქუდსის“** ლიდერი, გენერალი **ყასემ**

[36] კიბერმედია, "კორონა ვირუსით ჰაკერები მანიპულირებენ", მარტი, 14, 2020. გვ. 1. მოპოვებულია: https://seclab.ge/post/CoronaCovid19, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

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-ქუდსი“**, რომელსაც ის ხელმძღვანელობდა, აშშ-ში ტერორისტული ორგანიზაციების სიაში იყო შეყვანილი. გენერალი **სოლეიმანი** ამერიკელ დიპლომატებზე ერაყსა და მთელ რეგიონში მყოფ სამხედროებზე თავდასხმებს გეგმავდა. **„ალ-ქუდსი“** პასუხისმგებელია ასობით ამერიკელი და კოალიციური ჯარის სამხედროთა სიკვდილზე“.[37]

სოლეიმანის სიკვდილი იმდენად შოკისმომგვრელი აღმოჩნდა ირანისთვის, თითქმის არავის გახსენებია, რომ სარაკეტო დარტყმას ასევე ემსხვერპლა შიიტური შეიარაღებული დაჯგუფება **„ქატაიბ ჰეზბოლას“** ლიდერი **აბუ მაჰდი ალ-მუჰანდისი**.

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 **„ქატაიბ 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 **„ქატაიბ ჰეზბოლას“** უჭერს მხარს, თავდასხმას **„ტერორიზმის ნათელი მაგალითი“** უწოდა. აშშ-ის საჰაერო ძალებმა სირიასა და ერაყში დაჯგუფება **„ქატაიბ ჰეზბოლას“**ობიექტებზე იერიში 29 დეკემბერს მიიტანეს.

[37] https://imedinews.ge/ge/msoflio/124873/amerikelma-samkhedroebma-iraneli-generali-kasem-suleimani-mokles, უკანასკნელად იქნა გადამოწმებული: 27.05.2020

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

„ირანს საკმაოდ ძლიერი კიბერპროგრამა აქვს და თეირანი ცნობილია პოლიტიკურად მოტივირებული კიბერთავდასხმების განხორციელებით“.[38]

როგორც ხედავთ, თეთრი სახლიც 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 იყენებენ სოციალურ ქსელებს, კერძოდ - **„ტვიტერს“**. ამავე ხერხს მიმართეს ირანელმა მოხელეებმაც. ამიტომ, თამამად შეგვიძილია ვთქვათ, რომ აშშ-ირანის სამხედრო დაპირისპირება მიმდინარეობს საინფორმაციო ომის ფონზე. **აქ აშკარად გამოიკვეთა კრიტიკული თეორიის სკოლა, ანუ მეთოდი, რომელიც ამსხვრევს საერთაშორისო ურთიერთობების ტრადიციულ თეორიებს და ხშირ შემთხვევაში ურთიერთობები გადადის ბრალდებებსა თუ მუქარაში.**

ფაქტია, სოციალურ ქსელებში **დონალდ ტრამპის** მხრიდან არაერთხელ დაფიქსირდა მუქარა, თუ ირანი ჩვენს ქვეყანაზე თავდასხმებს განახორციელებს, 52 ირანულ ობიექტს დავბომბავთ, დარტყმა სწრაფი და ძლიერი იქნებაო. „ირანელ ხალხს არასოდეს დაემუქრო“, - ამ სიტყვებით მიმართა ქვეყნის პრეზიდენტმა ჰასან როუჰანმა დონალდ ტრამპს.[39]

ირანმა ბოლომდე მაინც არ გადაყლაპა სოლეიმანთან დაკავშირებული „შეურაცხყოფა“ და ერაყში აშშ-ის სამხედრო ბაზების მიმართულებით 35 ბალისტიკური რაკეტა გაუშვა.მოგვიანებით გაჩნდა ინფორმაცია, რომ ერაყის

[38] https://1tv.ge/news/ashsh-is-usafrtkhoebis-uwyeba-iranis-mkhridan-shesadzloa-ashsh-ze-%E2%80%8Bkibertavdaskhma-gankhorcieldes/, უკანასკნელად იქნა გადამოწმებული: 05.01.2020.

[39] https://imedinews.ge/ge/msoflio/125067/rouhani-52-iranuli-obieqtis-shesakheb-trampis-gantskhadebas-pasukhobs, უკანასკნელად იქნა გადამოწმებული: 06.01.2020.

ხელისუფლებამ ამერიკელები გააფრთხილა და სამხედროებმა ბუნკერებში ჩასვლა მოასწრეს.[40]

მთელი მსოფლიო ელოდებოდა საპასუხო შეტევას აშშ-ის მხრიდან, მაგრამ პრეზიდენტმა **ტრამპმა** გონივრული გზა აირჩია - არავითარი ომი, მხოლოდ მკაცრი სანქციები. თუმცა, ნუ გამოვრიცხავთ, რომ ეს იყოს დროებითი მშვიდობა, რადგან შესაძლოა, ირანმა სხვა ხერხები გამოიყენოს - ტერორისტული აქტები, კიბერთავდასხმები და ასე შემდეგ. ცხადია, სამხედრო დაპირისპირების ჩაცხრობის შემთხვევაში მთელი ყურადღება გადატანილი იქნება კიბერთავდასხმებსა და საინფორმაციო ომზე. არადა, საინფორმაციო ომი ისედაც მუდმივად თან სდევს აშშ-ირანის ურთიერთობას, რომელიც უფრო გამძაფრდა სამხედრო შეტევების დროს. მაგალითად, ირანული საინფორმაციო საშუალებები აცხადებენ, რომ გარდაცვლილი გენერალი ეროვნული გმირი იყო, ხოლო დასავლური და ამერიკული მედია აცხადებს, რომ ის მუდმივად გეგმავდა თავდასხმებს ამერიკელ დიპლომატებზე და სამხედრო პერსონალზე. ტრამპის, მტკიცებით, ირანის რევოლუციური გვარდიის **„ყუდსის ძალების“** სარდალი, **ყასემ სოლეიმანი** 20 წლის განმავლობაში ახლო აღმოსავლეთში დესტაბილიზაციას უწყობდა ხელს და რაც ახლა გააკეთა, დიდი ხნით ადრე უნდა გაკეთებინა, რადგან ბევრი სიცოცხლე გადარჩებოდა.

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. ირანი ამერიკის შეერთებულ შტატებს დიდ ტყუილში ადანაშაულებს. მთავრობის პრესსპიკერმა, **ალი რაბიეიმ** განაცხადა, რომ ასეთი დიდი სიცრუისთვის

[40] CNN. *"Trump says 'Iran appears to be standing down' following its retaliatory attacks against Iraqi bases housing US troops"*. 2020.08.01. გვ. 1. მოპოვებული edition.cnn.com: https://edition.cnn.com/2020/01/07/politics/rockets-us-airbase-iraq/index.html-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020

პასუხისმგებლობას არავინ აიღებს. მისივე თქმით, ეს არის ფსიქოლოგიური სპეცოპერაცია ირანის წინააღმდეგ. თუმცა ამ მხრივ საინფორმაციო ომი დიდხანს არ გაგრძელებულა, 11 იანვარს ირანის ხელისუფლებამ აღიარა, რომ თვითმფრინავი შეცდომით ჩამოაგდეს და ამას „ადამიანური შეცდომა“ უწოდეს.[41]

რაც არ უნდა უწოდონ ირანელებმა ამ ფაქტს, მთელი მსოფლიო მაინც მოჰყვება იმის მტკიცებას და მართალიც იქნება, რომ ეს არის ტერორისტული აქტი რამდენიმე სახელმწიფოს წინააღმდეგ. ვაღიაროთ, ამ სამხედრო დაპირისპირებასა და საინფორმაციო ომში ირანი პირწმინდად დამარცხდა. თუმცა რას მოიმოქმედებს შემდგომში ეს არაპროგნოზირებადი ისლამური რესპუბლიკა, რთული 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 პარლამენტმა ერთხმად დაამტკიცა და „ის ყველა ამერიკელ სახმედროზე, პენტაგონის თანამშრომელზე და იმ პირებზე ვრცელდება, ვინც ირანელ გენერალ **სოლეიმანის** მკვლელობაზეა პასუხისმგებელი. ირანის პარლამენტმა ასევე მხარი დაუჭირა **„ისლამური რევოლუციის გუშაგთა კორპუსის“** ელიტური ქვედანაყოფის **„ალ-უდსის“** დაფინანსების 200 მილიონი ევროთი გაზრდას. აღნიშნული ქვედანაყოფი ირანის ფარგლებს გარეთ სპეცოპერაციების ჩატარებაზეა პასუხისმგებელი.[42]

რაზეა წამსვლელი ირანი? ქვეყანა, რომელიც ერთი სამხედრო ლიდერის დაკრძალვაზე ჭყლეტვაში კარგავს 52 ადამიანს და შავდება 200-ზე მეტი

---

[41] კუპრეიშვილი, თ. *"ყველაფერი, რაც ვიცით უკრაინული თვითმფრინავის კატასტროფაზე"*. 2020.08.01. გვ. 1. მოპოვებული netgazeti.ge: https://netgazeti.ge/news/418935/-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020

[42] საზოგადოებრივი მაუწყებელი. *"ირანმა აშშ-ის სამხედრო ძალები „ტერორისტულ ორგანიზაციად“ გამოაცხადა"*. 2020.07.01. გვ. 1. მოპოვებული 1tv.ge: https://1tv.ge/news/iranma-ashsh-is-samkhedro-dzalebi-teroristul-organizaciad-gamoackhada/-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020

ადამიანი,[43] ყველაფერზეა წამსვლელი. რაც მთავარია, ალბათ, ირანის ხელისუფლებამ უნდა გამოიგონოს ისეთი ახალი პროვოკაცია, რომელიც მსოფლიო მასშტაბით გადაფარავს უკრაინული სამგზავრო თვითმფრინავის ჩამოგდების ფაქტს და დაადანაშაულებს ამერიკის შეერთებული შტატების ხელისუფლებას. მით უმეტეს, საამისო პირობები უკვე არსებობს, ირანის პრეზიდენტი **ჰასან რუჰანი** უკრაინული თვითმფრინავის შეცდომით ჩამოგდებას აშშ-ის ქმედებებს უკავშირებს. მისი თქმით, მუქარის გამო, ირანის ძალების სრული მობილიზაცია მოხდა და ტრაგედია სწორედ ამან გამოიწვია:

„გენერალ **ყასემ სოლეიმანის** მოწამეობრივი სიკვდილის შემდეგ, აგრესიული ამერიკული რეჟიმის მხრიდან მუქარის გარემოში, ამერიკული არმიის შესაძლო თავდასხმისგან თავდაცვის მიზნით, ირანის ისლამური რესპუბლიკის შეიარაღებული ძალების სრული მობილიზაცია მოხდა. ადამიანურმა შეცდომამ კი, სამწუხაროდ საშინელი კატასტროფა გამოიწვია, რასაც ათობის უდანაშაულო ადამიანი შეეწირა“.[44]

როგორც ხედავთ, ირანის პრეზიდენტი მაინც ცდილობს, ყველაფერი აშშ-ის ხელისუფლებას გადააბრალოს. მისი ე.წ. ახსნა-განმარტებიდან ასე გამოდის: როდესაც **სოლეიმანი** „მოწამეობრივად“ მოგვიკლეს, ჩვენი ჯარების სრული მობილიზაცია გამოცხადდა, იყო დაბნეულობა და ვინ საით ისროდა ბომბებს, ვეღარ გავიგეთ.

ასეთმა პროპაგანდამ მაინც არ გაჭრა ირანის მოსახლეობის ერთ ნაწილში, უფრო მეტად ახალგაზრდობაში და დაიწყო კიდეც საპროტესტო აქციები, რომლის შედეგებიც, ალბათ, იქნება ამ სახელმწიფოს „რეორგანიზაციის“ დასაწყისი, ანუ დრომოჭმული ხელისუფლების გაუქმების წინაპირობა.

---

[43] http://www.tabula.ge/ge/story/162804-iranshi-kasem-soleimanis-dakrdzalvaze-chkletashi-sul-mcire-35-adamiani-daighupa, უკანასკნელად იქნა გადამოწმებული: 13.06.2020

[44] რუჰანი, ჰ. *"ირანის პრეზიდენტი უკრაინული თვითმფრინავის შეცდომით ჩამოგდებას აშშ-ს ქმედებებს უკავშირებს"*. 2020.11.01. გვ. 1. მოპოვებული 1tv.ge: https://1tv.ge/news/iranis-prezidenti-ukrainuli-tvitmfrinavis-shecdomit-chamogdebas-ashsh-s-qmedebebs-ukavshirebs/-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020

ირანის 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 შეგვიძლია დავარქვათ ნატო+ახლო აღმოსავლეთი“. რა მშვენიერი სახელწოდებაა. სახელებს კარგად ვიგონებ“.[45]

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 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,

---

[45] ტრამპი, დ. *"ნატო-მ ახლო აღმოსავლეთიც უნდა მოიცვას და ახალ ალიანსს დავარქვათ „ნატო+ახლო აღმოსავლეთი“ – რა მშვენიერი სახელწოდებაა, სახელებს კარგად ვიგონებ".* 2020.10.01. გვ. 1. მოპოვებული interpressnews.ge: https://www.interpressnews.ge/ka/article/580527-donald-trampi-nato-m-axlo-agmosavletic-unda-moicvas-da-axal-alianss-davarkvat-natoaxlo-agmosavleti-ra-mshvenieri-saxelcodebaa-saxelebs-kargad-vigoneb/-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020

არამედ მსოფლიოში. აქვე უნდა დავამატოთ, რომ ირანი, ისევე როგორც რუსეთი, არ გახლავთ პროგნოზირებადი სახელმწიფო, მით უფრო მაშინ, როცა მისი კიბერდოქტრინა აგებულია ასიმეტრიული ომის ტაქტიკაზე და ძირითადად დაფუძნებულია ჰაკერულ თავდასხმებზე. მეტიც, კიბერდოქტრინის თითოეულ დეტალს აკონტროლებს ირანის ხელისუფლება, რომლის წიაღშიც შექმნილია კიბერსივრცის უმაღლესი საბჭო და სადაც შედიან ამავე ხელისუფლების უმაღლესი წარმომადგენლები, პრეზიდენტით დაწყებული, მინისტრებით დამთავრებული. გარდა იმისა, რომ ირანის მთავარი სამიზნე გახლავთ ამერიკის შეერთებული შტატები, დასავლეთი ევროპა და ისრაელი, განსაკუთრებული ინტერესი გააჩნია კავკასიაშიც, კერძოდ კი საქართველოში. საამისოდ აქვს ორი მიზეზი: **პირველი** - თითქმის ყველა საკითხში მხარს უჭერს რუსეთს; **მეორე** - ვინაიდან, საქართველო საუკუნეების განმავლობაში იყო მის მიერ დაპყრობილი, თვლის, რომ ეს ტერიტორია მისი საკუთრებაა. შესაძლოა, ირანის ხელისუფლება ამას ოფიციალურად არ/ვერ აცხადებს, მაგრამ საზოგადოების დაბალ თუ საშუალო ფენებში ეს აზრი ხშირად დომინირებს, რასაც ხელს უწყობს არაერთი ე.წ. სამეცნიერო გამოხტომა - ხან რუკებს ბეჭდავენ, სადაც საქართველო მათ ტერიტორიადაა დაფიქსირებული, ხან ნაშრომებს გამოსცემენ, სადაც ისტორიას აყალბებენ.

როგორც უკვე აღვნიშნეთ, დღეს საქართველო-ირანის ურთიერთობა ნორმალურია, მაგრამ ამ ურთიერთობაში შეინიშნება ერთგვარი სიმყიფეც და შესაძლოა, კიბერ თუ სამხედრო კონფლიქტის მიზეზი გახდეს საქართველოს პოლიტიკური ორიენტაცია. ვინაიდან, ჩვენ გვსურს ევროკავშირსა და ჩრდილო-ატლანტიკურ ალიანსში გაწევრიანება, ბუნებრივია, ეს კატეგორიულად ეწინააღმდეგება რუსეთ-ირანის ინტერესებს და ისიც ბუნებრივია, რომ იარნს რუსეთთან ერთად შემუშავებული ექნება სპეციალური ე.წ. დოქტრინა თუ სტრატეგია. ამჟამად ირანში 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 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 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.

ირანსა 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 ირანთან 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 ტელ-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 ყარაბაღის 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. გავიხსენოთ **პოლიტიკური რეალიზმის თეორია,** რომლის ამოსავალი დებულება მდგომარეობს იმაში, რომ საკუთარი უსაფრთხოებაზე ზრუნვის გამო სახელმწიფოები არიან ეგოისტური რაციონალური აქტორები, რომლებიც ისწრაფვიან ძალაუფლებისკენ. 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.

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.

ჩვენ უნდა ველოდოთ დიდ ომს როგორც რეალურ, ისე ირეალურ სივრცეში. ამიტომ, საქართველოს, როგორც აშშ-ის სტრატეგიულ პარტნიორს და ირანის არეალში ახლო მყოფ ქვეყანას, მართებს დიდი სიფრთხილე. ნუ გამოვრიცხავთ, რომ 2008 წლისა და 2019 წლების მაგალითზე საქართველო გახდეს კიბერთავდასხმებისა და საინფორმაციო ომის საცდელი პოლიგონი.

კიბერუსაფრთხოების გლობალური ინდექსი

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.[46]

რა მოხდა ამ კუთხით ბოლო ორ წელიწადში? მერამდენე ადგილზე ვართ 2019 წლის მონაცემებით?

ამჟამად 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 შემთხვევაში არსებობს ორი ვერსია: პირველი - ჩვენთან გაუარესდა სიტუაცია; მეორე - სხვა ქვეყნებმა გააუმჯობესეს მდგომარეობა.[47]

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

[46] იუსტიციის სამინისტრო. *"კიბერუსაფრთხოების ინდექსში საქართველო მე-8 ადგილზეა"*. 2017.19.06. გვ. 1. მოპოვებული: https://imedinews.ge/ge/politika/16724/kiberusaprtkhoebis-indeqsshi-saqartvelo-me8-adgilzea-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

[47] Forbes Georgia. *"კიბერუსაფრთხოების ინდექსით, საქართველო მსოფლიოში მე-19 ადგილზეა"*. 2018.02.08. გვ. 1. მოპოვებული imedinews.ge: https://imedinews.ge/ge/teqnologiebi/72543/kiberusaprtkhoebis-indeqsit-saqartvelo-msoplioshi-me19-adgilzea-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

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.[48]

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 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. ევროკომისიის პრეზიდენტი **ჟან-კლოდ იუნკერი** აცხადებს, რომ, ხშირ შემთხვევაში, ყალბი ახალი ამბები არა მხოლოდ მედიით, არამედ ევროკავშირის წევრი სახელმწიფოების პრემიერ-

[48] საქართველოს უსაფრთხოების და განვითარების ცენტრი. *ნატო-ს ვარშავის სამიტის დეკლარაციის მოკლე მიმოხილვა (გავლენა საქართველოზე).* 2014 წ. გვ. 2-3. მოპოვებული gcsd.org.ge: http://gcsd.org.ge/storage/files/doc/NATO-Warsaw-Summit-FINAL.pdf-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

მინისტრებისგანაც ვრცელდება. მაგალითისთვის **იუნკერმა** უნგრეთის პრემიერი **ვიქტორ ორბანი** მოიყვანა.

„მაგალითად, როდესაც ბატონი ორბანი ამბობს, რომ მიგრანტები არიან პასუხისმგებელნი ბრექსიტზე, ეს არის არასწორი განცხადება. შეიძლება ითქვას, ყალბი ახალი ამბავი. ასე რომ, მხოლოდ მედიას ნუ დავადანაშაულებთ".[49]

როდესაც საქმე ეხება ჰიბრიდულ ომს, კიბერ-თავდასხმებს, ჰაკერულ თავდასხმებს, ფეიკ-ნიუსების ანუ ყალბი ახალი ამბების გავრცელებას, დასავლეთსა და ამერიკის შეერთებულ შტატებში 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 აუდიტორია 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 ინფორმაციის და კოორდინირებული საინფორმაციო კამპანიის მსხვერპლი ხდება. შარშან რუსული მედია მთელი წლის განმავლობაში ავრცელებდა ყალბ ინფორმაციას **რიჩარდ ლუგარის** სახელობის ლაბორატორიაზე. როგორც ჰელსინკში მდებარე ჰიბრიდული საფრთხეების საწინააღმდეგო ევროპული ცენტრის თანამშრომელი **ვიტაუტას კერსანსკასი** აცხადებს, რუსეთის ამოცანაა, საზოგადოების სხვადასხვა ჯგუფებს შორის უთანხმოების

[49] იუნკერი, ჟ.-კ. *"ჟან-კლოდ იუნკერი აცხადებს, რომ ყალბი ამბები არა მხოლოდ მედიით, არამედ ევროკავშირის წევრი ქვეყნების პრემიერებისგანაც ვრცელდება"*. 2018.14.12. მოპოვებული 1tv.ge: https://1tv.ge/news/djan-klod-iunkeri-ackhadebs-rom-yalbi-ambebi-ara-mkholod-mediit-aramed-evrokavshiris-wevri-qveynebis-premierebisganac-vrceldeba/-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

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 მიერ მხარდაჭერილ კანდიდატს ან მიიღონ მონაწილეობა ისეთ საპროტესტო აქციაში, რომელიც უცხო ქვეყნის ინტერესებშია.[50]

2.2. კიბერსივრცის მთავარი აქტორები და საქართველო

როდესაც ვსაუბრობთ ჰიბრიდულ ომებზე, კიბერ-ომებზე, საინფორმაციო ომებზე და მათ შემადგენელ კომპონენტებზე, უსაფრთხოებაზე და სხვადასხვა კუთხით განვიხილავთ ამ საკითხს, უნდა გამოვყოთ და ყურადღება გავამახვილოთ ჩრდილო-ატლანტიკური ალიანსის მიდგომებსა და პოზიციებზე. 2016 წლის ვარშავის სამიტის შემდეგ, ნატომ ძირეული რეფორმები განახორციელა და აქტიურად დაიწყო პარტნიორ ქვეყნებთან თანამშრომლობა კიბერუსაფრთხოების თვალსაზრისით.

საქართველოს მაგალითზე შეგვიძლია ვთქვათ, რომ 2010 წლიდან მუშაობს **„უსაფრთხოების ექსპერტთა კავკასიის აკადემია“ – (CASE)**, რომელიც გადამზადებას და სწავლებას უწევს სამხედროებს, სამართალდამცავებს, დიპლომატებს, მსხვილ კორპორაციებს და სტუდენტებს.[51]

2012 წლიდან, საქართველოს განათლების, მეცნიერების, კულტურისა და სპორტის სამინისტროს ინიციატივით საქართველოში **კიბერუსაფრთხოების სკოლა** ამოქმედდა, სადაც ნებისმიერ მსურველს შეუძლია გადამზადდეს.[52]

---

[50] კერსანსკასი, ვ. *"დეზინფორმაციასთან და ყალბ ამბებთან საბრძოლველად მარტივი და სწრაფი გზა არ არსებობს, ეს გრძელვადიანი სტრატეგიაა"*. 2019.24.01. გვ. 1. მოპოვებული 1tv.ge: https://1tv.ge/video/vitautas-kersanskasi-dezinformaciastan-da-yalb-ambebtan-sabrdzolvelad-martivi-da-swrafi-gza-ar-arsebobs-es-grdzelvadiani-strategiaa/-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

[51] https://globalcase.org/page/about-case/, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

[52] https://www.emis.ge/news/708/, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

2013 წლის მაისში საქართველოს პრეზიდენტმა ხელი მოაწერა **საქართველოს კიბერ უსაფრთხოების სტრატეგიას** 2013-2015 წლებისთვის, რომელიც წარმოადგენს კიბერ უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ მთავარ დოკუმენტს.[53]

2014 წლის 6 თებერვალს საქართველოს თავდაცვის მინისტრის N8 ბრძანების საფუძველზე შეიქმნა სსიპ **"კიბერუსაფრთხოების ბიურო"** და დამტკიცდა მისი დებულება.[54] საქართველოში ასევე ფუნქციონირებს **„კიბერუსაფრთხოების ასოციაცია“ (SCSA)**, რომელიც ახორციელებს ტრენინგებს და გადამზადებას, კიბერ უსაფრთხოების სფეროში. კიბერდანაშაულის გამოძიება ერთ-ერთი მნიშვნელოვანი საკითხია სახელმწიფოს გამართული ფუნქციონირების კუთხით. ამას კი სჭირდება სათანადო ტექნიკური და საკანონმდებლო ბაზა, კვალიფიციური კადრები, თანამშრომლობა პარტნიორ ქვეყნებთან და ასე შემდეგ. საქართველოს მთავარ პროკურატურაში პერიოდულად კიბერდანაშაულის გამოძიებისა და ელექტრონული მტკიცებულებების თემაზე სამართალდამცავი უწყებების წარმომადგენლებისთვის მიმდინარეობს ერთობლივი ტრენინგი. ამ საქმეში ჩართულია ნატო-ს სამეკავშირეო ოფისი საქართველოში და აშშ-ის საელჩო, რომელთა მიზანი გახლავთ კიბერდანაშაულის წინააღმდეგ ბრძოლის საკითხებში ქართველი სამართალდამცველების პროფესიული გაძლიერება და წარმატებული საერთაშორისო პრაქტიკის გაცნობა. გამოძიება, როგორც ასეთი, თანამედროვე ტექნოლოგიების განვითარებისა და ინტერნეტსივრცეზე დამოკიდებულების ზრდის პარალელურად, ეს საკითხი კიდევ უფრო მეტ აქტუალობას იძენს. რა კუთხით მიმდინარეობს სამართალდამცავთა გადამზადება? ტრენინგებსს აშშ-დან მოწვეული პრაქტიკოსი ექსპერტები ატარებენ და მოიცავს შემდეგ საკითხებს: ყველაზე

[53] საქართველოს პრეზიდენტის ადმინისტრაცია. *საქართველოს პრეზიდენტის ბრძანებულება №321, საქართველოს კიბერუსაფრთხოების.* 2013.17.05. გვ. 1-9. მოპოვებული matsne.gov.ge: https://matsne.gov.ge/ka/document/download/1923932/0/ge/pdf-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

[54] http://csbd.gov.ge/, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

გავრცელებული კიბერდანაშაულის სახეები, ქსელური გამოძიების ტექნიკა, ჩხრეკისა და ამოღების ჩატარების პრაქტიკა, სასამართლოში ბრალდების დასადასტურებლად მობილურის, კომპიუტერის ექსპერტიზის გამოყენება, სასამართლოში ციფრული მტკიცებულებების გამოყენების სტრატეგია, მტკიცებულებათა დასაშვებობა, ვირტუალური ვალუტის, ციფრული ტექნოლოგიებით ფულის გათეთრების გამოძიების საფუძვლები და ასე შემდეგ.

იუსტიციის სამინისტროში **შეიქმნა მონაცემთა გაცვლის სააგენტო კიბერუსაფრთხოების კუთხით**, **(კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE)** რომელიც ემსახურება როგორც საჯარო, ასევე კერძო სექტორს. ამ საკითხში ჩართულია შინაგან საქმეთა სამინისტროც, რომელიც იძიებს საქართველოში გავრცელებულ კიბერდანაშაულის ტიპებს. სამინისტროში აცხადებენ, რომ დღეს ინტენსიურად ხდება კვალიფიციური კადრების კერძო სექტორში გადინება, რაც უკვე პრობლემას წარმოადგენს. იგივე სამინისტრო ადასტურებს, რომ ბოლო ორი წლის განმავლობაში კიბერინციდენტების რაოდენობა გაიზარდა.

„ბოლო პერიოდში მნიშვნელოვნად გაიზარდა კიბერშეტევები და ამ მიმართულებით დამატებითი ნაბიჯები არ გადაიდგა და არ მოხდა ადექვატური რეაგირება, ამას შეიძლება მძიმე შედეგები მოყვეს",– აღნიშნულია შსს-ს 2018 წლის ანგარიშში.[55]

რამდენად ორგანიზებულია სახელმწიფო უწყებებს შორის კოორდინაცია და როგორ ხდება ინფორმაციის კლასიფიკაცია, რამდენად ეფექტურია მოქმედი კონტროლის მექანიზმები, რამდენად საკმარისია დღეს არსებული ტექნიკური ბაზა და რამდენად აკმაყოფილებენ კვალიფიციური კადრები თანამედროვე მოთხოვნებს, როცა უკვე ოფიციალურადაა გაცხადებული,

[55] საქართველოს შინაგან საქმეთა სამინისტრო. *საქართველოს შინაგან საქმეთა სამინისტროს 2018 წლის საქმიანობის ანგარიში.* 2019 წ. გვ. 16-23, მოპოვებული info.police.ge: https://info.police.ge/uploads/5cf7e783a0c6d.pdf-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

რომ კადრები მიდიან კერძო სექტორში, ანუ იქ, სადაც უფრო მეტი ანაზღაურებაა? საქართველოს პარლამენტში იმაზეც იყო საუბარი, რომ პრობლემის აქტუალურობიდან გამომდინარე, როგორც ახალგაზრდებისთვის, ასევე სხვადასხვა სფეროში დასაქმებული პირებისთვის და მათ შორის დეპუტატებისთვის სპეციალური ტრენინგები უნდა გაიმართოს. "საზოგადოებრივი მაუწყებლის" ეთერში ყოველკვირეულად გავიდა გადაცემა კიბერდანაშაულისა და პრევენციის თემაზე. თუმცა დეპუტატებისთვის ტრენინგები არ ჩატარებულა.

რა მხრიდანაც არ უნდა შევხედოთ საკითხს, პრობლემას, საკვლევ თემას, მაინც მივდივართ საერთაშორისო გამოცდილებამდე და სტანდარტებამდე. ნატოში ამოქმედებულია გეგმა, რომლის თანახმადაც დაგეგმილია ერთობლივი საქმიანობა პარტნიორ ქვეყნებთან და ორგანიზაციებთან, რაც საქართველოს უსაფრთხო გარემოს გაუმჯობესებასთანაც ასოცირდება. როგორც ნატოს ყოფილი მრჩეველი უსაფრთხოების საკითხებში, გენერალი **ფრანკ ვან კაპენი** აღნიშნავს:

„საერთაშორისო საფრთხეების შეკავების და დაძლევისთვის აუცილებელია სახელმწიფოთა მიერ მრავალი მიმართულებით ერთიანი სტრატეგიული მიდგომის შექმნა და, რა თქმა უნდა, კოორდინებული მოქმედებების განხორციელება".[56]

ამ მხრივ ძალიან საინტერესოა პოლიტოლოგ **სოსო ცინცაძის** განმარტება, იგი ჩვენთან საუბრისას ამბობს, რომ საინფორმაციო ომის ერა გაძლიერებული მეთოდებით დაიწყო „ცივი ომის" დამთავრების შემდეგ, რომელიც მოინათლა როგორც „ჰიბრიდული ომი":

„სოციალური ქსელების განვითარებასთან ერთად ჩნდება თითქმის შეუზღუდავი რესურსი საინფორმაციო ომის მწარმოებლებისთვის. საინფორმაციო ომის „ეშხი" იმაშია, რომ აქ ძალიან ძნელია თავდაცვა.

[56] კაპენი, ფ. *"კონფლიქტის ახალი ფორმა – ჰიბრიდული ომი"*. 2016.02.03. გვ. 1. მოპოვებული http://yata.ge/ge/?p=691: http://yata.ge/ge/?p=691-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

ჰაკერები უკვე არჩევნებშიც ერევიან, მაგრამ კონკრეტულად დამტკიცება ჭირს. რასაც დღეს ვხედავთ, ჩვენი აზრით, ეს დასაწყისია, მომავალი უფრო მძაფრსიუჟეტიანი იქნება, რადგან ამ საქმეში უკვე იხარჯება ძალიან დიდი ფული. მაგალითად, რუსეთი ხარჯავს მილიარდებს, რათა მოიპოვოს გავლენა ყველა სფეროში, განსაკუთრებით - პოლიტიკური თვალსაზრისით“.[57]

2.3. ასიმეტრიული საფრთხეები და ჯიჰადისტების კიბერომი

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 სახელმწიფო“** (**„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. აღნიშნული ტერორისტული ორგანიზაცია თანამედროვე ტექნოლოგიების, მათ შორის, ინტერნეტსივრცისა და სოციალური ქსელების გამოყენებით, კვლავ აქტიურად ავრცელებდა საკუთარ იდეოლოგიას,

[57] ცინცაძე, ს. "სოციალური ქსელების განვითარებასთან ერთად ჩნდება თითქმის შეუზღუდავი რესურსი საინფორმაციო ომის მწარმოებლებისთვის". (ინტერვიუერი თ. ზედელაშვილი,), 2017.03.06.

ახდენდა პირების რადიკალიზაციასა და გადაბირებას. როგორც ანგარიშში ვკითხულობთ:

„ალ-ქაიდა“ აქტივობებს, ძირითადად, ახლო აღმოსავლეთსა და აფრიკის კონტინენტზე მოქმედი რეგიონული დაჯგუფებების მეშვეობით ახორციელებდა. „თალიბანი“ განაგრძობდა ავღანეთის სამთავრობო ძალებსა და ქვეყანაში საერთაშორისო მისიით მყოფ სამხედროებზე თავდასხმებს".[58] 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.[59]

ინტერნეტსივრცეში ყოველდღიურად ჩნდება **ჯიჰადისტური** ქსელები მრავალნაირი ფორმით. ამ მხრივ მიდის სელექციური მუშაობა ახალი თაობის **ჯიჰადისტების** აღსაზრდელად. როგორც **ვახტანგ მაისაია** ამბობს, 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 მსოფლიო უსაფრთხოებისთვის ერთ-ერთი უმთავრესი

---

[58] საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში. *"საქართველოში მცხოვრებ „დაეშის“ შესაძლო მხარდამჭერთა რაოდენობა და გავლენა შემცირდა".* 2019.28.03. მოპოვებული imedinews.ge: https://imedinews.ge/ge/samartali/100997/susi-saqartveloshi-mtskhovreb-daeshis-shesadzlo-mkhardamcherta-raodenoba-da-gavlena-shemtsirda-dan, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

[59] მაისაია, ვ. *„ისლამური ხალიფატის“ საინფორმაციო-პროპაგანდისტული/კიბერ-ვირტუალური ომის სპეციფიკა - „რბილი ძალის“ კონცეფტი.* 2017.07.06. მოპოვებული: http://geotimes.com.ge/blogi/?m=82&post_id=18&lng=geo-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020

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 იმოწმებან 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, 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.[60]

2013 წლის 6 ივნისს "იუთუბზე" შოკისმომგვრელი ვიდეო გავრცელდა სახელწოდებით: **"ჯიჰადი ავღანეთში საქართველოს ჯარების წინააღმდეგ"**,[61] რომელიც შეიცავდა მუქარას ავღანეთის მისიაში მონაწილე საქართველოს შეიარაღებული ძალების წინააღმდეგ. მუქარისშემცველი ვიდეოს გავრცელებას მოჰყვა მსხვერპლი. სანამ ქართველი ჯარისკაცების დაღუპვის შესახებ გახდებოდა ცნობილი, გავრცელებულ ვიდეოს საქართველოს ხელისუფლებაში სერიოზულად არ აღიქვამდნენ. ვიდეორგოლის წარმომავლობის დადგენაზე მოკვლევა დაიწყო თავდაცვის სამინისტრომაც. გავრცელებული ტექსტი კი ასეთი გახლდათ:

"ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!"[62]

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 იქნეს მიღებული:

"საქართველოს ბიუჯეტიდან საკმაოდ მნიშვნელოვანი სახსრებია გამოყოფილი ასეთი საქმიანობისთვის, საზღვრებისა და აეროპორტების

---

[60] ტოლერანტობისა და მრავალფეროვნების ინსტიტუტის (TDI). *"ძალადობა რელიგიის სახელით და ინტერპრეტაციის მნიშვნელობა"*. 2018.07.05. მოპოვებული tdi.ge: https://www.tdi.ge/ge/page/zaladoba-religiis-saxelit-da-interpretaciis-mnishvneloba-0-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020

[61] https://www.myvideo.ge/v/2058973, უკანასკნელად იქნა გადამოწმებული: 15.06.2020

[62] Zaman, H. *"თალიბანი საქართველოს შურისძიებით ემუქრება? - შოკისმომგვრელი ვიდეო YouTube-იდან"*. 2013.06.06. გვ. 1. მოპოვებული palitravideo.ge: https://www.palitravideo.ge/garthoba/skhvadaskhva/32044-gaiziare-bednie reba-erthi-qilidan-sayvareli-sasmeli-akhali-shefuthvith.html?start=140&fullComments=1-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020

გაკონტროლებისთვის, ამიტომ შესაბამისი სამსახურები უნდა მოიქცნენ ისე, როგორც მსგავსი მუქარის შემთხვევის დროს იქცევიან ხოლმე".[63]

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 სახელმწიფოში"** 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:

"ტერორისტული საქმიანობისთვის ქვეყნიდან გამგზავრებისა და შემოსვლის პრევენციის მიზნით, შსს-სთან თანამშრომლობით სათანადოდ ხორციელდება სასაზღვრო კონტროლი (საზღვრის მწვანე ზოლის, ასევე

[63] ჯიჰადი. *"ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!"*. 2013.07.06. მოპოვებული for.ge: https://for.ge/view/23153/jihadi-Cven-viciT-Tqveni-saxelebi-misamarTebi-naTesavebi-da-male-saqarTveloSi-CamovalT-Cven-Surs-viZiebT.html-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020

სასაზღვრო გამტარი პუნქტების). ხდება ვიზიტორებთან გასაუბრება. ყველა სასაზღვრო-გამტარი პუნქტი აღჭურვილია ბირთვული და რადიოაქტიური მასალების, ნივთიერებების დეტექტორებით".[64]

[64] საქართველოს სახელმწიფო უსაფრთხოების სამსახური. *"ტერორიზმთან ბრძოლა"*. 2015.01.11. გვ. 1. მოპოვებული ssg.gov.ge: https://ssg.gov.ge/page/counter-terrorism-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020

თავი III. კიბერომის კონცეფცია და 21-ე საუკუნის საერთაშორისო უსაფრთხოების სისტემა

თანამედროვე ჰიბრიდულ ომებში გამოიკვეთა ახალი ელემენტები – ეკონომიკური, კიბერ შეტევები, ბირთვული მუქარები, საინფორმაციო ომები. რა გამოწვევები არსებობს, რა ეტაპზეა „ახალი ცივი ომის აჩრდილი“, მსოფლიო წესრიგის რა ფუნდამენტური ცვლილებებია მოსალოდნელი? ამ მხრივ საინტერესო ანალიზს იძლევა ბატონი **ვახტანგ მაისაია** თავის ნაშრომში: **„ახალი ცივი ომის“** აჩრდილი და მსოფლიო წესრიგის ფუნდამენტური ცვლილება - საქართველო სად არის”? მისი თქმით, მიმდინარე საერთაშორისო პოლიტიკური მოვლენების ფონზე, საქართველოში ყველაფრეზე მსჯელობენ და არა იმ ძირითად ტენდენციებზე, რომლებმაც უკვე შეცვალა მსოფლიო წესრიგის მოწყობა და ის გახადა მულტიპოლარული.

“1999 წლიდან აშშ-მ შეძლო გლობალური მართვის სადავეების ხელში ჩაგდება, განსაკუთრებით ჯორჯ ბუშ-უმცროსის ადმინისტრაციის მიერ გამოცხადებული „ტერორიზმთან გლობალური ომის“ სტრატეგიის განხორციელებისთანავე. ასეთი მოდელი, ანუ აშშ-ის გლობალური ჰეგემონობა და მონოპოლარული მსოფლიოს წესრიგის მოდელი გაგრძელდა 2014 წლამდე, მას შემდეგ, რაც რუსეთის ფედერაციამ განახორციელა უკრაინის სუვერენული ტერიტორიის ყირიმის ნახევრაკუნძულის ოკუპირება ე.წ. „ჰიბრიუდლი ომის“ მეშვეობით და საერთაშორისო სამართლის ყველა ნორმისა და პრინციპის უგულებელყოფით მოახდინა მისი ანექსია, რამაც, შემდეგ გამოავლინა საკუთარი ამბიცია უკვე მსოფლიო ჰეგემონობისკენ“.[65]

[65] მაისაია, ვ. „ახალი ცივი ომის“ აჩრდილი და მსოფლიო წესრიგის ფუნდამენტური ცვლილება - საქართველო სად არის? 2017.15.05. გვ. 1. მოპოვებული geotimes.com.ge: http://geotimes.com.ge/blogi/?m=82&post_id=16-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020

ამ შემთხვევაში შეუძლებელია, არ დავეთანხმოთ **ძალთა ბალანსის თეორიას,** ძალიან ახლოსაა პოლიტიკურ რეალიზმს და გამომდინარეობს საერთაშორისო სისტემის ანარქიული სტრუქტურიდან. თუ კარგად დავაკვირდებით რუსეთის პოლიტიკას უკრაინისა და საქართველოს მიმართულებით, აშკარად დავინახავთ, რომ საერთაშორისო სისტემა გადადის ანარქიულ მდგომარეობაში, სადაც ამ სახელმწიფოს ძირითადი ამოცანაა ბრძოლა თვითგადარჩენისა და თვითდამკვიდრებისათვის. თუმცა რუსეთის შემთხვევაში საქმე არ გვაქვს უსაფრთხოების მოპოვება-შენარჩუნებასთან, პირიქით, ის საფრთხეს უქმნის სხვა სახელმწიფოებს. ვინ უნდა ითამაშოს მთავარი როლი, ვინ უნდა დაიცვას ძალთა თანასწორობა და ძალთა ბალანსი თანამედროვე მსოფლიოში? რა თქმა უნდა, ამერიკის შეერთებულმა შტატებმა, ევროკავშირმა და ნატომ. ამ თეორიის თანახმად, სახელმწიფოები ერთად მოქმედებენ, რათა დაუპირისპირდნენ რუსეთს, რომელიც საფრთხეს უქმნის მათ უსაფრთხოებასა და სუვერენიტეტს. რა თქმა უნდა, ძალთა ბალანსის დაცვა ხდება ვირტუალურ სივრცეშიც, სადაც მიდის უხილავი, მაგრამ დაუნდობელი ბრძოლა.

რამდენი სახის კონცეფცია შეიძლება არსებობდეს დღევანდელ მსოფლიოში? გარდა იმისა, რომ მნიშვნელოვანი კონცეფციები გააჩნიათ აშშ-ს, ევროკავშირს, ნატოს, ყველა ქვეყანას აქვს საკუთარი სამოქმედო ეროვნული გეგმა. თუმცა ყველაზე საყურადღებოდ მაინც 2010 წელს ლისაბონის სამიტზე დამტკიცებულ ახალ სტრატეგიულ კონცეფცია ითვლება, რომლის თანახმადაც ამერიკის შეერთებულმა შტატებმა ჩამოაყალიბა კიბერსარდლობა. ეს იყო პასუხი რუსეთის ქმედებებზე კიბერუსაფრთხოების თვალსაზრისით. ვლადიმერ პუტინი მოვიდა თუ არა ხელისუფლებაში, 2000 წელს დაამტკიცა საინფორმაციო უსაფრთხოების ახალი დოქტრინა, რომლის სტრატეგია იყო ის, რომ ხელისუფლებას მიანიჭა საინფორმაციო და მედიაქსელებზე კონტროლის უფლებები. პუტინმა ასევე ხელი მოაწერა საკანონმდებლო ცვლილებას - საგადასახადო პოლიციას, შინაგან საქმეთა სამინისტოს, კრემლის საპარლამენტო და საპრეზიდენტო დაცვის

სამსახურებს, საზღვრის დაცვას და საბაჟო სამსახურს იგივე უფლებები მიენიჭა, რაც მხოლოდ უსაფრთხოების ფედერალური სამსახურს ჰქონდა.

2017 წლის 18 დეკემბერს გამოქვეყნდა აშშ-ის პრეზიდენტის, დონალდ ტრამპის პირველი **„ეროვნული უსაფრთხოების სტრატეგია“,** რომელიც საფუძვლად დაედო სტრატეგიულ დოკუმენტებს, როგორიცაა აშშ-ის თავდაცვის დეპარტამენტის **„ეროვნული თავდაცვის სტრატეგია“.** „ეროვნული უსაფრთხოების სტრატეგია“ ეფუძნება ოთხ მნიშვნელოვან ეროვნულ ინტერესს: **1) ამერიკელი ხალხისა და ამერიკული ცხოვრების წესის დაცვა; 2) ამერიკის კეთილდღეობის ზრდა; 3) სიმტკიცით მშვიდობის შენარჩუნება; 4) ამერიკის გავლენის გაზრდა. ამ სტრატეგიაში საუბარია საქართველოზეც:**

„მიუხედავად იმისა, რომ საბჭოთა კომუნიზმის საშიშროება წარსულს ჩაბარდა, ჩვენი სიმტკიცე ახალი საფრთხეების წინაშე დგას. რუსეთი მიმართავს მავნებლურ ზომებს, რათა ეჭვქვეშ დააყენოს ამერიკის ერთგულება ევროპის მიმართ, ძირი გამოუთხაროს ტრანსატლანტიკურ ერთიანობას და შეასუსტოს ევროპული ინსტიტუტები და მთავრობები. საქართველოსა და უკრაინაში შეჭრით რუსეთმა აჩვენა, რომ სურს დაარღვიოს ამ რეგიონის ქვეყნების სუვერენიტეტი. რუსეთი აგრძელებს მეზობელი ქვეყნების დაშინებას ისეთი საფრთხის შემცველი ქმედებებით, როგორიც არის ბირთვული იარაღით პოზიცირება და შეტევითი ხასიათის შეიარაღების განთავსება.“[66]

როგორც ხედავთ, აქ ყველაფერია ნათქვამი და სტრატეგიის ზოგადი მიზნებიც კი ნათლად ასახავს აშშ-საქართველოს ურთიერთობას. სტრატეგიაში ძალზე საინტერესოა მე-3 თავი, რომლის სათაურია: „ძალის

[66] აშშ-ის საელჩო საქართველო, "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", 19 დეკემბერი, 2017, გვ. 1. მოპოვებული: https://ge.usembassy.gov/ka/2017-national-security-strategy-united-states-america-president-ka/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

მეშვეობით მშვიდობის შენარჩუნება“, სადაც ორი სახელმწიფოს – რუსეთისა და ჩინეთის მიმართ პრეტენზიებია გამოთქმული:

„ამერიკის შეერთებული შტატებისათვის რუსეთი ეგზისტენციალურ საფრთხედ აღიქმება. რუსეთი ცდილობს, აღიდგინოს დიდი სახელმწიფოს 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“.[67]

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,

[67] აშშ-ის საელჩო საქართველო, "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", 19 დეკემბერი, 2017, გვ. 1. მოპოვებული: https://ge.usembassy.gov/ka/2017-national-security-strategy-united-states-america-president-ka/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

ტექნოლოგიების განვითარების ხარჯზე „ცხელი იარაღიდან“ „რბილ ძალამდე“ მივიდა“.[68]

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

„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.[69]

როდესაც 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. ამ შემთხვევაში აშშ ანვითარებს **ნეოკლასიკური რეალიზმის თეორიას,** რომლის თანახმადაც, პოლიტიკური ძალა და ძლიერება არის მშვიდობის ერთადერთი გარანტი.

3.1. თანამედროვე მაღალი ტექნოლოგიების გავლენა საერთაშორისო უსაფრთხოების პროცესებზე

კიბერომი, კიბერთავდასხმები და მოგერიება, ეს უწყვეტი პროცესია. ალბათ, ვერასოდეს ვიტყვით, რომ საბოლოო შედეგი მიღწეულია და დროა, ამ შედეგით კმაყოფილი უნდა ვიყოთ. რაც უფრო განვითარდება ინტერნეტსივრცე და დაინერგება ახალი მეთოდები, მით მეტად

[68] Cheng Dean, „Cyber dragon, inside China s information warfare and cyber operations“, The Changing Face of War James Jay Carafano, Series Editor, Publishing House “Praeger”, USA, 2017 Y. P. 79-82.

[69] აშშ-ის საელჩო საქართველო, "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", 19 დეკემბერი, 2017, გვ. 1. მოპოვებული: https://ge.usembassy.gov/ka/2017-national-security-strategy-united-states-america-president-ka/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

გაძლიერდება საფრთხეებიც. სწორედ ამაზე მიანიშნებს დაფინანსების ზრდა ყოველწლიურად და როგორც ნახეთ, ეს არის უკვე ასეულობით მილიარდი დოლარი. რაც შეეხება ზარალს, უკვე ადის ტრილიონობით დოლარზე. ნუ გამოვრიცხავთ იმასაც, რომ შესაძლოა, ხვალ ისეთ თემებზე მოგვიწიოს კვლევების ჩატარება, რაზეც დღეს ბუნდოვანი წარმოდგენა გვაქვს, ან საერთოდ არ გვაქვს წარმოდგენა - ახალი ტექნოლოგიები აუცილებლად მოიტანს ახალ საფრთხეებს. რასაკვირველია, მსოფლიო მზად უნდა იყოს უპრეცედენტო კვლევებისა და უპრეცედენტო მიმართულებების დანერგვისთვის. ნატო-ს, ამერიკის შეერთებულ შტატებსა და ევროკავშირს ამის გაკეთება ნამდვილად შეუძლიათ.

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 1

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) 1.*** 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.[70] ასევე **"Gartner"**-ის ინფორმაციით, 2022 წელს მსოფლიო კიბერუსაფრთხოების ხარჯები 133.7 მილიარდ აშშ დოლარს მიაღწევს.[71] თუმცა აქ საყურადღებოა შემდეგი ფაქტი, რომ მსოფლიოსთვის მიყენებული ზარალი ბევრად აღემატება უსაფრთხოებისთვის დახარჯულ თანხებს. სპეციალისტების ვარაუდით, 2021 წელს კიბერშეტევებისგან გამოწვეული ზარალი 6 ტრილიონი დოლარი იქნება.[72]

ჩვენ განვიხილავთ ჰიბრიდული ომის სხვადასხვა კომპონენტებს, საფრთხის შემცველ მოვლენებს, რაც სრულიად უკავშირდება მეცნიერულ მიღწევებს და ახალ ტექნოლოგიებს. აქვე არ უნდა გამოგვრჩეს ერთი მინშვნელოვანი საკითხი - **კრიპტო-ვალუტა.** ბოლო წლებში საბანკო-საფინანსო სფერომ ძალიან დიდი განვითარება ჰპოვა. სწორედ ამას უკავშირდება ელექტროვალუტის შექმნა. რა არის ციფრული ფული? რით განსხვავდება სტანდარტული 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 განსხვავდბეით არ იბეჭდება. იგი წარმოიქმნება, ინახება და იხარჯება ელექტრონულად. ის არ კონტროლდება არც ერთი სახელმწიფოს და არც ერთი ბანკის მიერ.

---

[70] Gartner. *"Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019".* 2018,08,15. P. 1. Retrieved from Gartner: https://www.gartner.com, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

[71] Varonis. *"110 Must-Know Cybersecurity Statistics for 2020".* 2020,01,09. P. 1. Retrieved from Varonis: https://www.varonis.com, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

[72] კეკენაძე, დ. *"კიბერდანაშაული, როგორც 21-ე საუკუნის მნიშვნელოვანი პრობლემა".* 2019.12.08. გვ. 1. მოპოვებული ON: https://on.ge-დან, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

ბიტკოინის წარმოშობა ხდება რთული მათემატიკური ფორმულების შედეგად და ასევე კომპიუტერული ქსელების საშუალებით. ტრადიციული ვალუტა ეფუძნება ოქროს ღირებულებას, ხოლო ციფრული ვალუტა ეფუძნება მათემატიკას. ბიტკოინის შექმნის პროცესს მაინინგი ეწოდება.[73]

ციფრული ვალუტის მაინინგისთვის აუცილებელია კომპიუტერების და სერვერების არსებობა, მაგრამ რადგან ისეთ ეპოქაში ვცხოვრობთ სადაც ტექნოლოგიები დღითი-დღე უფრო და უფრო ვითარდება, ამ პერიოდში 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 უამრავ ინფორმაციას და დეზინფორმაციას მოისმენთ თუ წაიკითხავთ, 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.[74]

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

საინტერესოა ისიც, რომ **ელექტრონული ფული „P2P“** ტექნოლოგიაზეა აგებული, ის სრულიად დამოუკიდებელი და დეცენტრაციზირებული ქსელია. სწორედ ეს ქმნის შესაძლებლობას, ნებისმიერმა მომხმარებელმა

[73] Nakamoto Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", გვ. 1-9. Extracted: https://bitcoin.org/bitcoin.pdf, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

[74] paxful, "What Happens When All the Bitcoin in the World Has Been Mined?", March 2, 2020, P. 1. Extracted: https://paxful.com/blog/what-happens-when-all-21-million-bitcoins-mined/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

პირდაპირ გადაიხადოს ან გადასცეს. გადარიცხვას, გადაცემას ამ შემთხვევაში ადასტურებენ ქსელის სხვა მომხმარებლები, რომლებსაც მაინერები ეწოდებათ. დასტური ხერხდება კრიპტოგრაფიული ხელმოწერით და ყოველი ხელმოწერის 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.[75]

რა თქმა უნდა, აქ არ არის მხოლოდ ბიტკოინი, დღეს უამრავი მსგავსი ვალუტა არსებობს, მაგალითად: **365Coin (365), Aiden (ADN), Adzcoin (ADZ), Ambercoin (AMBER), Amsterdamcoin (AMS), Argentum-SHA (ARG), Argentum-Scrypt (ARG), Aricoin (ARI), AUR-Scrypt (AUR), Bytecoin (BCN), Belacoin (BELA), Bipcoin (BIP), Dobbscoin (BOB), GlobalBoosti-Y (BSTY), Bata (BTA), Bitcoin (BTC), Bitmark (BTM), Burnercoin (BURN), Cachecoin (CACH), BottleCaps (CAP), Cryptobullion (CBX), X-Children (CHILD), Checkcoin (CKC), Cloakcoin (CLOAK) და სხვა.**[76]

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

[75] გოგუაძე მამუკა, "მომავლის ვალუტა ბიტკოინი – კრიპტოვალუტა", ნოემბერი 21, 2017, გვ. 1. მოპოვებული: https://financer.com/ge/kriptovaluta-bitcoin/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

[76] https://steemit.com/cryptocurrency/@qanon1111/list-of-all-coin-cryptocurrency-a-to-z, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

კიდეც, რადგან ვირტუალური ფული არ არის არც ერთი ეკონომიკური სისტებით ან ფიზიკური ღირებულებებით გამაგრებული. საყურადღებოა ის ფაქტიც, რომ 2015 წელს, ევროპის უმაღლესი სასამართლოს დადგენილებით ბიტკოინის ყიდვა ფიზიკური ფულით შესაძლებელი იქნება დღგ-ის გარეშე.[77]

ამ ყველაფრის გათვალისწინებით, კრიპტო-ვალუტის მომავალი მაინც გაურკვევლად რჩება, მაგრამ ის საკმაოდ მომხიბლავად გამოიყურება, როგორც მსხვილი კომპანიებისთვის, ასევე ცალკეული ადამიანებისთვის, შესაბამისად დასაშვებია უახლოეს მომავალში, რომ ეს მოვლენა ეკონომიკის უსაფრთხოების ერთ-ერთ მნიშვნელოვან გამოწვევადაც იქცეს. აქვე აღსანიშნავია, რომ ჰაკერები კრიპტოვალუტასაც ძალიან კარგად იყენებენ თაღლითობისთვის, **Ransomware** - ის, ანუ გამოსასყიდის მოთხოვნით ჰაკერები შიფრავენ თქვენს მონაცემებს კომპიუტერში, შემდეგ კი ითხოვენ დიდ ანაზღაურებას მონაცემებზე წვდომის აღდგენის მიზნით. თუმცა გადახდის შემთხვევაშიც თქვენს მონაცემებზე წვდომა არ აღდგება. ამ ტიპის თაღლითობა კი მეტწილად ხდება ანონიმური კრიპტოვალუტების წყალობით, მაგალითად, ბიტკოინით.

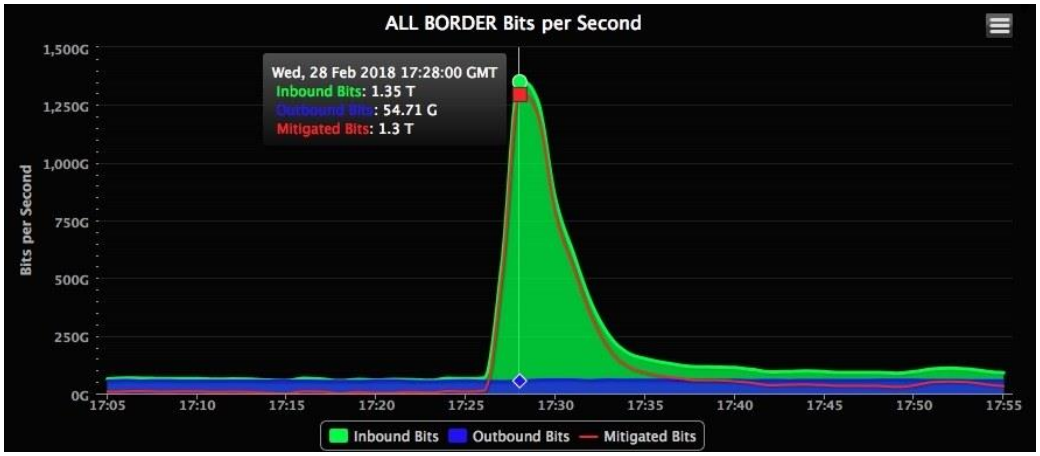
ვინაიდან, **კრიპტო-ვალუტით** თაღლითობა კიბერშეტევით ხორციელდება, გადავიდეთ იმის განხილვაზე, თუ კიბერშეტევის რა მეთოდები არსებობს მსოფლიოში - მაგალითად, ძალიან გავრცელებულია **DDos** შეტევები (**Distributed Denial-of-Service).** ასეთი შეტევები უმეტესწილად ხდება ვებ-საიტებზე. **Dos**-ზე არის აწყობილი **Windows**-ი. ამ შეტევის დროს ხდება გარედან, ანუ სხვა ადგილიდან თავდასხმა. ნებისმიერი წერტილიდან შეიძლება მოხდეს სერვერზე შეტევა. შეიძლება განხორციელდეს ერთდროულად რამდენიმე ქვეყნიდან-ქალაქიდან. ისეთი შთაბეჭდილება იქმნება, ვებ-გვერდზე თითქოს ერთ დროულად უამრავი ადამიანია შესული, ამ დროს სერვერი სუსტდება, სხვადასხვა მექანიზმები მწყობრიდან გამოდის,

[77] ჭყოიძე ნატალია & ტომარაძე გიორგი, "ვირტუალური/კრიპტოგრაფიული ვალუტა და მისი თავისებურებები ვირტუალური ვალუტების რეგულირება (bitcoin-ის მაგალითზე)", 2014 წ. გვ. 41-55. მოპოვებული: https://www.nbg.gov.ge/uploads/journal/2014/2014_3/4.pdf, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

მინიმუმამდე ნელდება სისწრაფე და ადვილი "დასაჰაკი" ხდება. არსებობს უამრავი ვირუსი, ეს არის ფაილი, რომელიც დასავირუსებლად აუცილებლად უნდა მოხვდეს კომპიუტერში, „ფლეშკის" დისკის, ინტერნეტის ან სხვა საშუალებით. არსებობს ვირუსები, რომლებიც ყველა ფაილს კომპიუტერში „შორდქათად" აქცევს. ყველა ვირუსს თავისი დანიშნულება აქვს და სხვადასხვანაირად მუშაობს, თუმცა მიზანია ფაილების და კომპიუტერული ინფრასტრუქტურის სისტემური დაზიანება. მაგალითად, არსებობს „სახელგანთქმული" ვირუსი **„ტროიანი"**. ის სხვა ვიურსებისგან განსხვავდება, რადგან **„ტროიანი"** ჰაკერს აძლევს საშუალებას, ჰქონდეს წვდომა ფაილებთან და ინფორმაციასთან, რაც კომპიუტერში ინახება. ერთ-ერთი ყველაზე ცნობილი ვირუსი, რომელიც ბოლო წლებში არსებობდა, დაწერა **კევინ მიტნიკმა.** ეს ვირუსი **„ჭიის"** სახელით არის ცნობილი. მიტნიკმა ვირუსი ბანკის სისტემაში გაუშვა და ყველა ანგარიშიდან ერთ ცენტს აჭრიდა. მას ვერ დაუმტკიცეს დანაშაული. არსებობს ისეთი დაცული სისტემები, როგორიც არის **„მაკინტოში",** რადგან მასზე მხოლოდ ერთი ვირუსი არსებობს. ხოლო **„ანდროიდის"** სისტემაზე თითქმის ვირუსები არ არსებობს და უმეტეს წილად აპლიკაციებს მოყოლებული რეკლამები ჰგონიათ ხოლმე.

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 3

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 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".[78]

[78] the developer platform GitHub. *"GitHub Survived the Biggest DDoS Attack Ever Recorded"*. 2018,03.01. P. 1. Retrieved from Wired: https://www.wired.com, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

კიბერომი, რომელიც მსოფლიო მასშტაბით მძვინვარებს, ხორციელდება საქართველოზე, უკრაინასა და ისეთ ქვეყნებზე, რომლებსაც არ შესწევთ ძალა, თავი დაიცვან აგრესიისგან. მაგალითისთვის შეგვიძლია მოვიყვანოთ ბოლო პერიოდში 2019 წლის 28 ოქტომბერს განხორციელებული კიბერთავდასხმა საქართველოზე. როდესაც მაშტაბური შეტევა განხორციელდეა სახელმწიფო უწყებების ვებ-გვერდებზე, ასევე საქართველოს სხვადასხვა წამყვან ტელეარხებზე, შედეგიც იყო, უამრავი მასალის დაკარგვა და შეფერხებული მუშაობა რამდენიმე დღის განმავლობაში. ამასთან დაკავშირებით 2020 წლის 28 თებერვალს ეუთო-ში აშშ-ის მისიის ხელმძღვანელის მოადგილემ, **ჰარი კამიანმა** ვენაში, მუდმივი საბჭოს შეხვედრაზე განაცხადა, რომ აშშ გმობს რუსეთის მიერ საქართველოზე კიბერშეტევას, ეს ოპერაციები მიზნად ისახავს დანაწევრებას, დაუცველობის შექმნას და დემოკრატიული ინსტიტუტების შელახვას. **კამიანმა** ასევე აღნიშნა, რომ 2019 წლის 28 ოქტომბერს, საქართველოს წინააღმდეგ ფართომასშტაბიანი გამანადგურებელი თავდასხმა, რუსეთის არმიის გენერალური შტაბის მთავარი სადაზვერვო სამმართველოს სპეციალური ტექნოლოგიების მთავარმა ცენტრმა განახორციელა:

„ჩვენ, საერთაშორისო თანამეგობრობასთან ერთად, გავაგრძელებთ მუშაობას, რათა დავიცვათ კიბერსივრცეში პასუხისმგებლიანი სახელმწიფოს ქცევის საერთაშორისო ჩარჩო. ჩვენ საქართველოს გავუწევთ ტექნიკურ დახმარებას.“.[79]

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

[79] კამიანი, ჰ. *"აშშ მოუწოდებს რუსეთს, შეაჩეროს უგუნური კიბერთავდასხმები საქართველოსა და სხვა ქვეყნებზე".* 2020.28.02. გვ. 1. მოპოვებული საზოგადოებრივი მაუწყებელი: https://1tv.ge-დან, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

არაწევრ ქვეყნებსაც ავალდებულებს, აქტიურად იყვნენ ჩაბმულნი საერთაშორისო უსაფრთხოების პროცესებში.

2016 წელს ნატოს წევრმა ქვეყნებმა კიბერსივრცე აღიარეს, როგორც საომარი მოქმედებების სფერო.[80] ჩამოყალიბებულია არაერთი თავდაცვითი საერთაშორისო ორგანიზაცია. ერთ-ერთი ასეთი ცენტრი გახლავთ, **CCDCOE - ნატოს „კოოპერატიული კიბერ თავდაცვის 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 კიბერ თავდაცვითი ოპერაციების დაგეგმვა“.[81]

იმის თქმა, რომ თანამედროვე ტექნოლოგიები გავლენას არ ახდენს, ან უმნიშვნელოდ ახდენს უსაფრთხოების საკითხებზე, იქნება დიდი გულუბრყვილობა. უსაფრთხოების პროცესები ძირითადად ეყრდნობა ტექნოლოგიებს და სწორედ მასზეა დამოკიდებული წარმატება თუ წარუმატებლობა. როგორც აშშ-ის სტრატეგიაში, ასევე ალიანსის კონცეფციაში დიდი ყურადღება ეთმობა პარტნიორობის, თანამშრომლობისა და დიალოგის ფაქტორს. კერძოდ, ალიანსი ცდილობს, პარტნიორობის საბჭოს წევრებს შორის ყველა საკითხში იყოს ნდობა, და გამჭვირვალობა.

[80] Brent, L. *"NATO's role in cyberspace"*. 2019,02.12. P. 1. Retrieved from NATO: https://www.nato.int, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
[81] Riazi, T. "Know The CCDCOE: Interview with Director Col. Jaak Tarien". (J. Tarien, Interviewer) 2020,01.29. P. 1. Retrieved from http://natoassociation.ca, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

3.2. კიბერომის ტრანსფორმაციის ისტორიული ასპექტები: სამხედრო კონფლიქტების სივრცული მახასიათებლები

როდის გაჩნდა კიბერომის შესაძლებლობა, როდიდან შეიძლება დავიწყოთ ისტორიული ათვლა? ეს არის 21-ე საუკუნის ეპიდემია. გამოიგონეს კომპიუტერი, შექმნეს ინტერნეტი და ამას მოჰყვა მთელი სივრცის ეტაპობრივი ათვისება. ალბათ მე-20 საუკუნის ბოლოს ვერავინ წარმოიდგენდა, რომ რეალური ომი იქცეოდა განყენებულ განზომილებაში შექმნილი ომის დანამატად, ან პირიქით, ირეალური სივრცე შეერწყმებოდა რეალურ სივრცეს. ალბათ ვერც იმას წარმოიდგენდა ვინმე, რომ გაჩნდებოდა განზომილება, რომლის გაკონტროლება იქნებოდა თითქმის შეუძლებელი და უსაზღვრო, კაცობრიობა დადგებოდა უხილავი საფრთხის წინაშე. სხვათა შორის, იგივე კაცობრიობა კიბერომის შესაძლებლობის გაჩენას არ შეხვედრია მოუმზადებელი და ამაში დიდი როლი ითამაშა მეორე მსოფლიო ომმა, რომლის დამთავრებისთანავე გაჩნდა საერთაშორისო უსაფრთხოებისადმი მიძღვნილი კვლევების საჭიროება. გაეროს ეგიდით თავდაპირველად ის ჩამოყალიბდა, როგორც დამოუკიდებელი კვლევითი დარგი. აღნიშნული სფერო მოიცავს ისეთ საკითხებს, როგორიცაა "უსაფრთხოების კვლევები", "სტრატეგიული კვლევები", "სამშვიდობო კვლევები" და სხვა. თუ საერთაშორისო უსაფრთხოებაში თავიდან იგულისხმებოდა ჩვეულებრივი სამხედრო ძალის რეჟიმი, ამას უკვე დაემატა კიბერრეჟიმი, რომელსაც პირობითად "ბაბილონის გოდოლსაც“ კი უწოდებენ. ზემოთაც აღვნიშნეთ და კიდევ გავიმეორებთ: ეროვნული უსაფრთხოება, რომელიც მოიცავს სახელმწიფო მონოპოლიის საკითხებს და განიხილავს ძალის გამოყენებას მოცემულ ტერიტორიაზე, ხაზს უსვამს სამხედრო და პოლიციური კომპონენტების უსაფრთხოებას, ნელ-ნელა ტრანსფორმირდა და გადავიდა ტრანსნაციონალური უსაფრთხოების სივრცეში, ანუ ერთობლივ ღონისძიებებში. მეცნიერები აღნიშნავენ, რომ იყო ტრადიციული უსაფრთხოება და შემდეგ გაჩნდა უსაფრთხოება საზღვრების გარეშე. ტრადიციული უსაფრთხოება ეყრდნობოდა ორ ზესახელმწიფოს - საბჭოთა კავშირს და აშშს შორის არსებულ სამხედრო პოტენციალს, ეროვნულ

ინტერესებს და აბსოლუტურ სუვერენიტეტს. ამ თვალსაზრისით, საერთაშორისო სტაბილურობა ეყრდნობოდა გზავნილს, რომ თუ სახელმწიფოთა შორის უშიშროება შენარჩუნებულია, მაშინ მოქალაქეების უსაფრთხოებაც დაცულია. უსაფრთხოება განიხილებოდა, როგორც ქვეყანაში შეჭრისაგან თავდაცვა. როგორც კი დასრულდა "ცივი ომი", აშკარა გახდა, რომ მოქალაქეთა უსაფრთხოებას ემუქრება არა მხოლოდ აგრესორთაგან მომდინარე მუქარა, არამედ სახელმწიფოთა შიდასაქმიანობისას წარმოქმნილი სირთულეები. 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 წყალობით მყისიერად ვრცელდება დოკუმენტები, ფილმები, ფოტოები მთელი მსოფლიოს მასშტაბით.

საერთოდ, საინფორმაციო ომის ტაქტიკა და მეთოდოლოგია განსხვავებულია ქვეყნების მიხედვით, ყველა რეგიონს გააჩნია თავისებურება - ისტორია, კულტურა, პოლიტიკური აზროვნებისა და ანალიზის უნარი, განათლების დონე და ასე შემდეგ. თუმცა თუ საბჭოთა კავშირის მემკვიდრის, რუსეთის ქმედებებს დავაკვირდებით, ამ სახელმწიფოს ყველა მიმართულებით გააჩნია თითქმის ერთფეროვანი მეთოდი - რასაც ვერ აკეთებს ჰიბრიდული ომით, საინფორმაციო საშუალებებით, კიბერთავდასხმებით, საკითხს აგვარებს სამხედრო აგრესიით. აღნიშნული მიდგომა კი უკვე ასწლეულებს ითვლის. **„საქართველოს 100-წლიანი ბრძოლა კრემლის დეზინფორმაციასთან“,** – ამ სათაურით სტატიას ევროკავშირის მიერ დაფინანსებულ ვებგვერდი **„ეუ ვიეს დეზინფო“ (euvsdesinfo.eu)** აქვეყნებს. სტატიაში ნათქვამია, რომ საბჭოთა რუსეთმა საქართველოსთან და მის ევროპულ საგარეო კურსთან ბრძოლა 100 წლის წინ, დამოუკიდებლობის გამოცხადების დღიდან, წამოიწყო.

„საქართველო იყო რუსეთის სამხედრო ინტერვენციისა და აგრესიული დეზინფორმაციული კამპანიის მსხვერპლი. „მოსკოვის პრავდაში“ გამოქვეყნებულ სტატიაში ბოლშევიკებმა საქართველოს პირველი რესპუბლიკის ლიდერ ნოე ჟორდანიას საქართველოს ინგლისისთვის მიყიდვაში დასდეს ბრალი“.[82]

ვებგვერდზე გამოქვეყნებულია ამ ბრალდების შემცველი წერილიც. ამავე დროს გამოცემა აღნიშნავს, რომ „საქართველო დღესაც რჩება რუსეთის დეზინფორმაციული კამპანიის სამიზნედ“ და ევროკავშირის სპეციალურმა დანაყოფმა „ასობით მსგავსი შემთხვევა გამოავლინა“.[83]

როგორც პუბლიკაციის ავტორები აღნიშნავენ, რუსეთის დეზინფორმაციული კამპანიის მთავარი გზავნილებია – „საქართველომ დამოუკიდებლობა დაკარგა“, „საქართველო აშშ-ის პროტექტორატია“, „საქართველო ფეოდალური წარმონაქმნია, რომელსაც დასავლეთი მართავს“, „საქართველო თურქეთის მონაა“.[84]

სტატიაში ნათქვამია, რომ კრემლის დეზინფორმაცია აგებულია ერთი და იმავე გზავნილზე – დამოუკიდებლობის შელახვის საკითხზე, რომლის მორგებაც ნებისმიერ ეპოქაზე, პოლიტიკურ სიტუაციასა თუ ქვეყანაზეა შესაძლებელი. რასაკვირველია, როდესაც ჩვენში მიდის პროპაგანდა, რომ ვართ ამერიკის შეერთებული შტატების მონები, თურქეთის ვასალები, რუსეთს იგივე მიდგომა აქვს ბალტიისპირეთის ქვეყნების მიმართაც - როგორც ზემოთ აღვნიშნეთ, კრემლის მაღალჩინოსანი **სერგეი ლავროვი** პირდაპირ უმიზნებს ევროკავშირს, ანუ ცდილობს, განხეთქილება შეიტანოს ევროკავშირისა და ბალტიისპირელების ურთიერთობაში, თუ ვერ დაანგრევს

[82] Euvsdisinfo. "*FIGURE OF THE WEEK: 100, ALMOST"*. 2019,11.19. P. 1. Retrieved from euvsdisinfo.eu: https://euvsdisinfo.eu/figure-of-the-week-100-almost/, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

[83] Euvsdisinfo. "*FIGURE OF THE WEEK: 100, ALMOST"*. 2019,11.19. P. 1. Retrieved from euvsdisinfo.eu: https://euvsdisinfo.eu/figure-of-the-week-100-almost/, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

[84] Euvsdisinfo. "*FIGURE OF THE WEEK: 100, ALMOST"*. 2019,11.19. P. 1. Retrieved from euvsdisinfo.eu: https://euvsdisinfo.eu/figure-of-the-week-100-almost/, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

ამ ურთიერთობას, ოდნავ ბზარს მაინც შეიტანს, რადგან ხშირად ამ რეგიონის და არა მხოლოდ ამ რეგიონის მოსახლეობა იჯერებს იმას, რაც სრულიად დაუჯერებელია და სისულელემდეც კი მიდის. რუსეთს, რა თქმა უნდა, 70-წლიანი "ძმობის" პერიოდში ძალიან კარგად აქვს შესწავლილი პოსტსაბჭოთა ერების ფსიქოლოგია, განათლების დონე, აღქმის უნარი და ასე შემდეგ. რუსეთს ცივილიზებულ სამყაროსთან ომი არ დაუწყია გუშინ და არც იმის იმედი უნდა გვქონდეს, რომ დაამთავრებს ხვალ, ან როდესმე და რა თქმა უნდა, დანარჩენი სამყარო უნდა იყოს მზად ყველაფრისთვის - გაძლიერებული ჰიბრიდული ომისთვის, სამხედრო აგრესიისთვის და კიდევ ისეთი წინააღმდეგობებისთვის, რაც შეიძლება ვერ წარმოიდგინოს ნორმალურმა დემოკრატიულმა საზოგადოებამ.

ზემოთ ვახსენეთ 2019 წლის ნოემბერში საქართველოს წინააღმდეგ განხორციელებული კიბერთავდასხმა, რომელსაც თავისი მასშტაბებით და შედეგებით ერთ-ერთ ძლიერ თავდასხმად თვლიან. **სურეის** უნივერსიტეტის პროფესორმა, კიბერუსაფრთხოების ექსპერტმა, **ალან ვუდვორდმა BBC**-ისთან ინტერვიუში განაცხადა, რომ საქართველოში განხორციელებული მასშტაბური კიბერთავდასხმის მსგავსი შეტევა აქამდე არ უნახავს.[85] **კიბერუსაფრთხოების საგანმანათლებლო-კვლევითი ცენტრის, CYSEC** -ის დამფუძნებელი, კიბერუსაფრთხოების ექსპერტი **ანდრო გოცირიძე** ამბობს, რომ დიდი რაოდენობით ვებგვერდი კი დაზიანდა, მაგრამ ამ საიტების კომპრომეტაცია ცალ-ცალკე არ მოხდა, რამდენიმე ჰოსტინგი გატეხეს და შეტევა გავრცელდა მათ კლიენტებზე. ჰაკერების მთავარი უპირატესობა ასეთ დროს პროგრამულ უზრუნველყოფასა თუ სერვერებზე არსებული სისუსტეა. სამწუხაროდ, ქართული კიბერსივრცე არ აღმოჩნდა საკმარისად დაცული ამ არცთუ მაღალტექნოლოგიური შეტევისგან, რომელიც, შედეგებით თუ ვიმსჯელებთ, საკმაოდ ფართომასშტაბიანი აღმოჩნდა. ეს კიდევ ერთხელ ადასტურებს ხშირად ნათქვამს, რომ სუსტად დაცული

[85] British Broadcasting Corporation. *"UK says Russia's GRU behind massive Georgia cyber-attack"*. 2020,02.20. P. 1. Retrieved from bbc.com: https://www.bbc.com/news/technology-51576445, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

ინფრასტრუქტურის პირობებში, დაბალტექნოლოგიური შეტევაც კი არაპროპორციული ზარალის მიზეზი შეიძლება გახდეს. როგორც **გოცირიძე** აღნიშნავს, თუ ქვეყანას კიბერუსაფრთხოების თვალსაზრისით შესაბამისი ზომები არ იქნა გატარებული, ეს ინვესტორშიც უნდობლობას გააჩენს და ქვეყნის ეკონომიკაზეც უარყოფითად აისახება. აღნიშნულის მოგვარების ერთადერთ გზად კი **ანდრია გოცირიძე** მთავრობასა და ბიზნესს შორის მუდმივ თანამშრომლობასა და შესაბამისი ნორმატიული ბაზის შექმნაში ხედავს:

„ტექნიკურად მეტი უზრუნველყოფა გვჭირდება. კიბერომი ისეთი რამეა, ბიზნესის საშუალებით ქვეყანას რომ აყენებ ზარალს, ამიტომ აუცილებელია ამ ორ სექტორს შორის იყოს სისტემატური კომუნიკაცია და შეიქმნას გარკვეული ნორმატიული ბაზაც“.[86]

კიბერომი ყველა მიმართულებით, - ასეთია დღევანდელი მდგომარეობა. თუ 2008 წელს რუსეთმა ჩაგვიტარა კიბერომის პირველი გაკვეთილი, ანუ სპეცოპერაცია, 2019 წლის ნოემბრის გამოხტომა უნდა ჩავთვალოთ მეორე გაკვეთილად. თუმცა არის მაშინდელსა და დღევანდელს შორის განსხვავებაც - თუ 2008 წელს კიბერომი მოჰყვა ნამდვილ ომს, ეს უკვე იყო მხოლოდ კიბერომი. აშშ-ის თავდაცვის მინისტრის მოადგილე (დაზვერვის სფეროში) **დევიდ ჰოლისი** ამბობს, ეს იყო წინასწარი დემონსტრაცია, თუ როგორ გამოიყენებენ შეიარაღებული ძალები საინფორმაციო ომებს და კიბეროპერაციებს მომავალში, რისთვის უნდა მოემზადონ მეთაურები და პოლიტიკური კურსის გამტარებლები. **ჰოლისის** ცნობით, 2008 წელს რუსეთის შეტევითი ოპერაციები კიბერსივრცეში უშუალოდ ტიპური სამხედრო მოქმედებების გაჩაღებამდე რამდენიმე კვირით ადრე დაიწყო. რუსეთის კიბერდაზვერვის ქვედანაყოფებმა მნიშვნელოვან ადგილებში

[86] გოცირიძე ა. "თუ ქვეყანა არ ფლობს კიბერუსაფრთხოების საჭირო ელემენტებს, ის ვერ ჩაითვლება სანდო პარტნიორად, მათ შორის, ვერც ეკონომიკის ჭრილში". (ინტერვიუერი ს. ლემონჯავა) commersant. თბილისი. 2018.28.05. გვ. 1. მოპოვებული https://commersant.ge/ge/post/ra-dartymas-ayenebs-kiberomi-saqartvelos-ekonomikas-დან, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

ამოცნობის პროცედურები ჩაატარეს და შეესივნენ ქართულ სამხედრო და სამთავრობო ქსელებს იმ მონაცემთა მოსაძიებლად, რომელიც მათ დაწყებული კამპანიის დროს გამოადგებოდათ. ამ ხნის განმავლობაში, რუსეთის მთავრობამ მოხალისეთა კიბერრაზმების, არასამთავრობო უშტატო ჰაკერების ორგანიზებაც დაიწყო, რომლებიც კამპანიას მხარს დაუჭერდნენ და ამავდროულად სამთავრობო ოპერაციებისთვის ერთგვარი ფარის ფუნქციას შეასრულებდნენ. ამ პერიოდში ხელისუფლება და კიბერრაზმები ქართულ სამიზნეებზე თავდასხმის რეპეტიციებს გადიოდნენ. **ჰოლისი** აღნიშნავს, რომ 2008 წლის აგვისტოში რუსმა სტრატეგებმა მოახდინეს კიბერსივრცის ოპერაციების მყარი ინტეგრაცია თავიანთ სამხედრო, დიპლომატიურ და სტრატეგიულ ოპერაციებთან და კომპიუტერული სისტემები დააზიანეს თავისთვის საჭირო მომენტებში. ქართული ეპიზოდი საუკეთესო მასალაა კიბერსივრცის მებრძოლთათვის შესასწავლად, რომლებიც მსგავსი ახალი კონფლიქტისთვის მოემზადებიან.[87]

თუ **ჰოლისის** მოსაზრებას დავუჯერებთ, ქართული ეპიზოდი სამხედრო აგრესიის წინაპირობაა და უნდა ვემზადოთ ახალი კონფლიქტებისთვის. კიბერომში მთავარი „კოზირი“ ის არის, რომ შეიძლება აგრესორი ისე შეინიღბოს, ვერავინ გაიგოს, საიდან, დედამიწის რომელი წერტილიდან ხორციელდება თავდასხმა, შეიძლება ჰაკერთა ბანდა იჯდეს კრემლში და თავდასხმა ხორციელდებოდეს აფრიკის რომელიღაც უდაბნოდან. კიბერთავდასხმის ტექნიკური წარმომავლობის დადგენა ძალიან რთულია, მაგრამ ამავე დროს იოლად ამოსაცნობია ხელწერა. რუსეთი ცდილობს, ამ კუთხით გაეროც გამოიყენოს, სადაც არაერთხელ წარადგინა წინადადებები, ინიციატივები და ბოლოს იქამდეც კი მივიდა, რომ არ შეუერთდა ევროპის საბჭოს კონვენციას კიბერდანაშაულის შესახებ, დოკუმენტს, რომელიც

[87] ჰოლისი, დ. "კიბერომის პირველი გაკვეთილი". kvirispalitra.ge. (ინტერვიუერი ფ. პოლისი,) აშშ. 2011.07.02. გვ. 1. მოპოვებული https://www.kvirispalitra.ge/ras-weren-chvenze/6616-kiberomis-pirveli-gakvethili.html-დან, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

ხელმოწერისთვის 2001 წლიდან ღიაა. სპეციალისტების მტკიცებით, რუსეთს სურს, რომ მხოლოდ მას ჰქონდეს უფლება, საგამოძიებო მოქმედებები აწარმოოს საკუთარი კანონებით. კრემლი ცდილობს, ცივილიზებულ სამყაროს თავზე მოახვიოს თავისი ინიციატივები და ხელშეკრულებები, სიტუაცია ისე დახატოს, თითქოს ის უპირველესი წინააღმდეგია კიბერთავდასხმებისა თუ საინფორმაციო ომებისა. მეტიც, მიუნხენის 47-ე უსაფრთხოების კონფერენციაზე რუსეთი შეეცადა მიეღოთ კონვენცია, რომლის თანახმადაც სამართლებრივი წესებით შეიზღუდებოდა კიბერთავდამსხმელთა საქმიანობა. რუსეთი ითხოვს იმის სამართლებრივ აკრძალვას, ან რეგულაციას, რაც სამართლებრივად უკვე შეზღუდულია, რაც თავისთავად უკვე წარმოადგენს დანაშაულს.

3.3. კიბერომის ფენომენის ასახვა ეროვნული უსაფრთხოების სტრატეგიებში - მითი და რეალობა

რუსეთის ეროვნული უსაფრთხოების დოქტრინის 2015 წლის ვარიანტში მე-16 და მე-17 პარაგრაფებში მთავარ მოწინააღმდეგებად მოიაზრებიან აშშ და ნატო, ხოლო მეშვიდე პარაგრაფში პირდაპირ არის დაფიქსირებული რუსეთის ფედერაციის როლის ამაღლება მსოფლიო წესრიგის მოწყობის საქმეში. ოფიციალურმა მოსკოვმა სწორედ „ჰიბრიდული ომის“ ელემენტების გამოყენებით შეძლო სერიოზული დარტყმის მიყენება აშშ-სთვის, საპრეზიდენტო არჩევნების დროს შეიტანა პოლიტიკური არასტაბილურობის ნიშნები აშშ-ს მონოლითურ პოლიტიკურ სისტემაში.[88] იმის მიუხედავად, რომ **დონალდ ტარმპი** არ არის კრემლის ფავორიტი, ქვეყანაში მაინც გაჩნდა ეჭვი. საპრეზიდენტო არჩევნებში ჰაკერული ჩარევის ამბავი სრული სიცრუეც რომ იყოს, მაინც წყალს ასხამს პუტინისტური რუსეთის გუნება-განწყობაზე, ანუ ყოვლისშემძლეობის განცდაზე და აჩენს ნიჰილიზმს ამერიკის შეერთებული შტატების მოსახლეობაში. თუმცა რატომ

[88] მაისაია, ვ. *„ახალი ცივი ომის“ აჩრდილი და მსოფლიო წესრიგის ფუნდამენტური ცვლილება - საქართველო სად არის?* 2017.15.05. გვ. 1. მოპოვებული geotimes.com.ge: http://geotimes.com.ge/blogi/?m=82&post_id=16-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

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 2001 წლის 11 სექტემბრის მოვლენებიც გამოდგება,[89] როცა ტერორისტებმა ლამის თავზე დაიმხეს ამერიკის შეერთებული შტატები, როცა ააფეთქეს შენობები და სამგზავრო თვითმფრინავები. აი, აქ გაჩნდა პირველად არა მხოლოდ "ამერიკული ნიჰილიზმი", არამედ "მსოფლიო ნიჰილიზმი". ამერიკის შეერთებულ შტატებს სწორედ მაგ პერიოდში ჰქონდა ე.წ. მოფერება-გადატვირთვის პოლიტიკა, რითაც ასერიგად ისარგებლეს მტრებმა. სახელმწიფო მდივანი **ჰილარი კლინტონი** მოსკოვში ჩაბრძანდა და რუსეთის საგარეო საქმეთა მინისტრს, **სერგეი ლავროვს** გადატვირთვის „ღილაკი“ შესთავაზა, ხოლო იმჟამინდელ დოქტრინაში პირდაპირ ჩაწერეს, რომ რუსეთთან აუცილებელია კონსტრუქციული თანამშრომლობა, ნატო-რუსეთის უსაფრთხოება გადაჯაჭვულია და ასე შემდეგ. როგორც შემდგომში ვნახეთ, ასეთმა მიდგომამ არ გაამართლა. 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 და მსოფლიოს სხვადასხვა კუთხეში კონფლიქტების პროვოცირებას უწყობს ხელს. რუმინეთში რუსეთიდან დაფინანსებული მედიასაშუალებები ცდილობენ, ევროკავშირში გაწევრიანება შეცდომად წარმოაჩინონ და დემოკრატიული ინსტიტუტები დააკნინ. შვედეთში მთავრობა სექსუალური გარყვნილების მიმდევრად არის წარმოჩენილი. უკრაინაში დეზინფორმაციული ბრძოლა ხორციელდება - კორუფციაზე, სიღარიბეზე, უწესრიგობაზე და დასავლეთის

[89] https://www.history.com/topics/21st-century/9-11-attacks, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

მიერ მართულ „მარიონეტულ“ რეჟიმზე. ლიტვაში, ლატვიასა და ესტონეთში პროპაგანდისტული მანქანა მუშაობს მიმართულებით, თუ როგორი დისკრიმინაციის ქვეშ არიან ამ ქვეყნებში რუსები მათი ეთნიკური თუ ენობრივი მახასიათებლების გამო.[90]

ფინეთში რუსული მედიაპროპაგანდა ხელისუფლებას რუსულ-ფინური წყვილების განქორწინების დროს ბავშვების მეურვეობასთან დაკავშირებული სასამართლო გადაწყვეტილებების არაკეთილსინდისიერებაში სდებს ბრალს.[91]

პრინციპში, ყველა პოსტსაბჭოთა ქვეყნის სასახელოდ უნდა ითქვას, რომ საბჭოთა კავშირის დაშლის შემდეგ არსად არ 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 ნათესავური 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. ინტერნეტგამოცემა **damoukidebloba.ge** - ის, ინფორმაციაზე დაყრდნობით - ბალტიისპირეთში რუსეთის პროპაგანდის მამოძრავებელი ძალაა - **„Первый Балтийский канал“.** ასევე ონლიაინ საიტი **Regnum.ru**, რომელიც უკვე 10 წელზე მეტია ფუნქციონირებს. უკანასკნელ დროს რუსეთის მიერ ამოქმედდა საიტი **Baltnews**, სადაც ანონიმურად

[90] "ინფორმაციის თავისუფლების განვითარების ინსტიტუტის" (IDFI). *"კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", პოლიტიკის დოკუმენტი.* 2016.22.08. გვ. 5-23, მოპოვებული idfi.ge: https://idfi.ge/public/upload/Meri/Russian%20Propaganda%20in%20Georgia%20-%20Policy%20Paper.PDF-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

[91] https://www.mythdetector.ge/ka/myth/dezinpormatsia-titkos-pinetshi-rusul-ojakhebs-bavshvebs-artmeven, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

თავსდება ინფორმაცია და ახალი ამბები ესტონურ, ლიტვურ და ლატვიურ ენებზე.[92]

როგორც გერმანული გამოცემა **"ბილდი"** საკუთარ წყაროებზე დაყრდნობით წერს, თუკი 2008 წლის საქართველო-რუსეთის ომში ამერიკის შეერთებული შტატები ღიად ჩაერეოდა, რუსებს ბალტიის ქვეყნებზე თავდასხმა ჰქონდათ გადაწყვეტილი, ხოლო თუ ამერიკელები ბალტიის ქვეყნებსაც გაუწევდნენ დახმარებას, მაშინ უკვე ბირთვული იარაღის გამოყენებასაც ფიქრობდნენ.

"ბილდის" მიმომხილველი ასევე წერს, რომ ფართომასშტაბიანი სამხედრო სწავლების - "დასავლეთ 2017"-ის ფარგლებში რუსეთი რეპეტიციობდა არა "ტერორიზმის წინააღმდეგ ბრძოლაში", არამედ "ნატო-ს 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 "შოკურ კამპანიას" ნატოს ქვეყნების წინააღმდეგ, მათ შორის იყო გერმანია, ნიდერლანდები, პოლონეთი, ნორვეგია, ასევე, ნეიტრალური შვედეთი და ფინეთი. გამოცემის წყაროს თქმით, 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".[93]

---

[92] http://damoukidebloba.ge/c/news/sainformacio_omi, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

[93] გერმანული გაზეთი "ბილდი". *"გერმანული მედია: რუსები 2008 წელს ბირთვული იარაღის გამოყენებას აპირებდნენ"*. 2017.23.12. გვ. 1. მოპოვებული resonancedaily.com: http://www.resonancedaily.com/index.php?id_rub=2&id_artc=42590-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

გამოცემის ცნობით, ნორვეგიის თავდაცვის სამინისტროს წყაროების ინფორმაციით, სწავლების ფარგლებში რუსეთმა დატესტა ქალაქ შპიცბერგენის დაბომბვა და ხელში ჩაგდება. როგორც ვნახეთ, ეს გეგმა პრაქტიკულად არ განხორციელდა, 2008 წლის მოვლენებში ამერიკის შეერთებული შტატები არ წამოეგო რუსეთის პროვოკაციაზე, მაგრამ რაკიღა არსებობს მსგავსი მოდელირებული გეგმა, ანუ 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 ქვეყნების 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 სატრანსპორტო ინფრასტრუქტურაა. საქმე მეტისმეტად სუსტ ხიდებს შეეხება, რომლებიც ამერიკული ტექნიკის წონას ვერ გაუძლებენ. საზღვრებზე პრობლემებს ქმნის ევროპული ბიუროკრატიაც.[94]

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

[94] The Washington Post. *"პენტაგონმა აღიარა, რომ რუსეთის შეჭრის შემთხვევაში, ბალტიისპირეთის ქვეყნების და პოლონეთის დაცვას ვერ მოასწრებს"*. 2018.25.06. გვ. 1. მოპოვებული imedinews.ge: https://imedinews.ge/ge/msoflio/67383/pentagonma-agiara-rom-rusetis-shechris-shemtkhvevashi-baltiispiretis-qveknebis-da-polonetis-datsvas-ver-moastsrebs- დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

და მათ დახმარება მალე შეუწყდებათ.[95] 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. როგორც ჩანს, კრემლში საგულდაგულოდ მალავენ ფაქტს, როცა ბალტიის ქვეყნების საგარეო საქმეთა მინისტრებს ე.წ. შეთანხმებაზე ხელის მოწერა არ სურდათ, რადგან 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.".[96]

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.

დისკუსიის ანალიზი

ტელეკომპანია „იმედი". გადაცემა „არენა". 2019 წლის 24 დეკემბერი.

---

[95] იაგორაშვილმა, ი. *(სერგეი ლავროვის განცხადება) "რუსეთის 2 მითი ბალტიისპირეთის ქვეყნების შესახებ".* 2019.27.09. გვ. 1. მოპოვებული mythdetector.ge: https://www.mythdetector.ge/ka/myth/rusetis-2-miti-baltiispiretis-kveqnebis-shesakheb-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

[96] იაგორაშვილი, ი. *(ვიაჩესლავ მოლოტოვის განცხადება) "მარია ზახაროვა სსრკ-ის მიერ ესტონეთის ოკუპაციას უარყოფს".* 2020.13.02. გვ. 1. მოპოვებული mythdetector.ge: https://www.mythdetector.ge/ka/myth/maria-zakharova-ssrk-mier-estonetis-okupatsias-uarqops-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

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 ვაშაზე 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, კიბერ ომს, საინფორმაციო ომს, ტერორიზმს, 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 ფაშისტური 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.

სიღრმისეული ინტერვიუები ექსპერტებთან

ამირან სალუქვაძე (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 (KOVID 9) აფეთქებამ ბევრი რამ შეცვალა დედამიწაზე და არნახული დოზით „ააყვავა“ საინფორმაციო სივრცე, სადაც მთელი ძალებით ამუშავდნენ ყალბი ამბების გამავრცელებლები. პირველი შეკითხვა ამირან სალუქვაძეს დავუსვით ამერიკელი ბიზნესმენის, ილონ მასკის (2002 წელს მასკმა დააფუძნა SpaceX, კოსმოსური ხომალდების მწარმოებელი და კოსმოსური სატრანსპორტო მომსახურებების ამერიკული კომპანია) სატელიტური ანტენების დამონტაჟებასთან და 5G-სთან დაკავშირებულ სალითხზე. მაშინ, როცა მსოფლიო მასშტაბით პანდემია მძვინვარებდა, სოციალურ ქსელებსა თუ მედიაში ვრცელდებოდა დაუჯერებელი ინფორმაცია, თითქოს ყველაფერი გამოწვეული იყო 5G-ის (უსწრაფესი ინტერნეტის) გამოგონების გამო. მეტიც, ასევე ვრცელდებოდა ზღაპრები, თითქოს უახლოეს ხანში ყველას სახლებში მოგვაკითხავდნენ, ძალის გამოყენებით აგვცრიდნენ და სხეულში ჩიპებს ჩაგვიმონტაჟებდნენ. აი, რას ამბობს ამ თემაზე ბატონო ამირან სალუქვაძე:

„საკმაოდ ძლიერი საინფორმაციო მანქანაა ამუშავებული, რომლის მიზანიც ხალხის დაზაფვრა და დაფეთებაა. ეს კამპანია დღეს არ დაწყებულა, უკვე წელიწადია მიმდინარეობს, ჩემი დაკვირვებით, მთელს მსოფლიოში, საქართველოში კი სადღაც მარტიდან ამოიქოქა. ჩათვალეთ, რომ სულ 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.

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.

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“.

როგორც ამირან სალუქვაძე ამბობს, დღეს მსოფლიოში ორი პანდემია მძვინვარებს, ერთი COVID-19-ს, მეორე - შეთქმულების თეორიების. მისი მტკიცებით, საკითხები ასე ლაგდება: კონსპიროლოგია, COVID-19-ის, ანუ ეპიდემიის უარყოფა, ე.წ. ჩიპიზაცია/ვაქცინაცია და გლობალური კონტროლი, ტექნოლოგიები.

რას ნიშნავს კონსპიროლოგია?

„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 1828-29 წლების შემდეგ დაიწყო და მთელ რუსეთს მოედო. ქოლერის პირველი შემთხვევები 1930 წელს თბილისსა და ასტრახანში აღმოაჩინეს. ეპიდემიამ მოსკოვსა და სანქტ-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.

ჩვენს სივრცეში გავრცელებული ჭორების, ინფორმაციების ლომის წილი რუსულენოვანია. თუმცა, შეთქმულების თეორიები სხვა ქვეყნებშიც ფართოდ ვრცელდება. მაგალითად, ამერიკის მოსახლეობის 29%-ს სჯერა კოვიდ-19-ს ხელოვნური წარმომავლობა. ლევადა-ცენტრის მიერ მარტში ჩატარებული გამოკითხვის თანახმად, რუსეთში მოსახლეობის მხოლოდ 24%-ს არ სჯერა კორონავირუსის შესახებ მასმედიის მეშვეობით გავრცელებული ოფიციალური ინფორმაციის. აპრილში ამ განწყობებმა იმატა და 59% შეადგინა. თებერვალში დაინფიცირების შიში მხოლოდ 30%-ს ჰქონდა. მარტის ბოლოს კი მათი რიცხვი 44%-მდე გაიზარდა.

თებერვალში "ფრანს პრესმა" გამოაქვეყნა სტატია, რომელშიც, სახელმწიფო დეპარტამენტის წარმომადგენლების ინფორმაციაზე დაყრდნობით წერდა, რომ სოციალურ ქსელში, რუსეთთან დაკავშირებული ათასობით ანგარიში აქვეყნებდა ინფორმაციებს კოვიდ-19-ის გავრცელებაში აშშ-ს სპეცსამსახურების ბრალეულობის შესახებ. რუსეთმა ეს ბრალდება, როგორც მოსალოდნელი იყო, უარყო“.

რა ხასიათის ინფორმაციას ავრცელებენ ყველაზე მეტად? ამირან სალუქვაძის თქმით, ეს არის ოფიციალური ვერსიების, განცხადებების კითხვის ნიშნის ქვეშ დაყენება ან გაყალბება, სახალხო რეცეპტები, ლოცვები, ფსევდოექიმების რჩევები, ისტორიები პირველწყაროს მითითებით. მაგალუთად, "ჩემი ახლობელი მუშაობდა უხანში და ყვება, რომ..." "ან ჩემმა ნათესავმა იტალიიდან მომიყვა, რომ იქ არაფერი ხდება". პანიკური, გადაუმოწმებელი ინფორმაცია - მაგალითად, "ამაღამ თვითმფრინავებით მოხდება ქალაქის დეზინფექცია. შეხვდით ღია ფანჯრებით" და ა.შ.

რატომ სჯერათ ადამიანებს შეთქმულების თეორისების, განსაკუთრებით ეპიდემიების და სხვა განსაცდელის დროს?

„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, "გამყარებული" აქ ამირან სალუქვაძე ვირუსის შესახებ გავრცელებულ აბსურდულ ვერსიას ასახელებს:

"ვირუსი მოიგონეს, რათა შეეწყვიტათ საჰაერო მოძრაობა და კოსმოსური აპარატები განეთავსებინათ". ამ ტექსტის დამწერს, ან მის გამავრცელებელს ვინმე დააჯერებს რა სიმაღლეზე დაფრინავენ თვითმფრინავები და რა სიმაღლეზეა ორბიტალური სადგურები? ან სკოლაში თუ არა, ინტერნეტში წაუკითხავთ რა არის ტროპოსფერო, სტრატოსფერო, მეზასფერა და ა.შ.? ან გააგებინებთ, რომ თანამგზავრების გაყვანა კოსმოსური რაკეტებით ხდება და საჰაერო მოძრაობას ხელი არასდროს შეუშლია მათ გასაშვებად? ალბათ არ დაიჯერებენ. კიდევ ასეთი პოსტი გამოქვეყნდა. ერთმა გადაიღო fligtjradar24-ის საიტზე დროის რეალურ მომენტში ევროპის საჰაერო სივრცეში არსებული საჰაერო ვითარების ფოტოასლი და გამოაქვეყნა ტექსტით: "ნახეთ რამდენი თვითმფრინავი დაფრინავს. არანაირი შეზღუდვები არ არსებობს". რეალურად, ფოტოზე ბევრი თვითმფრინავია, რამდენიმე ასეული. მაგრამ რამდენი დაფიქრდება იმაზე, რომ 1-2 თვის წინ, შეზღუდვებამდე, იყო 2-3-ჯერ მეტი? ადამიანები დაფიქრდებიან, რომ ყველა ქვეყანას არ დაუწესებია შეზღუდვები, ან ის, რომ არსებობს ჩარტერული რეისები, ან ის რომ საჰაერო ტვირთების გადაზიდვა გრძელდება და, შესაბამისად, გარკვეული რეისები სრულდება? კონსპიროლოგიურ ინფორმაციებს აქვს გარკვეული მახასიათებლები, სიტყვათა წყობა, ლოგიკა. მის გამავრცელებლებს კი ახასიათებთ შემდეგი ტიპის ფრაზები: "რაღაც არ მჯერა", "კი მჯერა, მაგრამ", "ნახე რა ვიპოვე დღეს ქსელში" და ა.შ.

ამირან სალუქვაძის თქმით, შიში დეზინფორმაციის მთავარი მამოძრავებელი ძალაა. ამჟამინდელ 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" ფოტო ასლებს. ამ ვერსიებზე მსჯელობას არ შევუდგები. მერწმუნეთ, ზემოთ ჩამოთვლილ, ასევე სხვა სახელმწიფოებს, უზარმაზარი პოტენციალი აქვთ სიმართლის დასადგენად. თუმცა, ამ სიახლის დადგენაში, ურთიერთბრალდებების, ხანგრძლივი საინფორმაციო ომის მომსწრენი ვიქნებით. ჩინეთთან და ნოვოსიბირკთან მიმართებაში ბევრი ბუნდოვანია. ყველაზე მავნე, რაც ამ თვეების მანძილზე 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.

ბოლნისის შემთხვევა, სხვა ინციდენტები, ამის ნათელი მაგალითია. შესაბამისად, მსგავსი ვერსიების ტირაჟირება, ოფიციალური ვერსიებისადმი უნდობლობის გაღვივება, უკვე აღარაა ცალკეული პირების პირადი საქმე“.

რას ნიშნავს ე.წ. ჩიპიზაცია, ვაქცინაცია და გლობალური კონტროლი? ამ კითხვაზე ექსპერტი ასეთ პასუხს იძლევა:

„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 შესძლებს 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. თავად კაფსულის ზომაა 2 მმx12 მმ-ზე. ასეთი ზომის ჩიპს, თქვენი კანის ქვეშ, თქვენი ნების გარეშე, ვერავინ შეიყვანს. 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 ვაქცინებს, ვაქცინაციას, ჯერ-ჯერობით არც ისეთი ვაქცინა არსებობს, რომელსაც შეუძლია გარკვეულ რასებზე, ან გარკვეული ასაკის ან სქესის ადამიანებზე გამორჩეულად ზემოქმედება. ოდესმე, შესაძლოა, მივიდნენ აქამდე, იღონდ დღეს საუბარი ნაადრევია. როგორ შეიძლება ჩვენი "ასტროლოგის" და აქაური თუ უცხოელი მისნაირების ბოდვა ვინმემ დაიჯეროს, რომ 6,5 მილიარდი ადამიანის მასობრივი დახოცვა იგეგმება“.

რატომ გამოიწვია პანიკა 5G ტექნოლოგიამ?

რა თქმა უნდა, მოთხოვნა იწვევს ქსელის გაფართოების, მისი გამტარუნარიანობის და სისწრაფის გაზრდის საჭიროებას. მობილური ტელეფონები, კომპიუტერები, ინტერნეტ ტელევიზია, სიგნალიზაციები,

საგზაო კამერები და ა.შ. ყველაფერს ინტერნეტი სჭირდება. როგორც ამირან სალუქვაძე ამბობს, 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. ზოგიერთი სპეციალისტიც კი, რომლებიც პუბლიკაციებს აქვეყნებენ, ერევათ რომელ გამოსხივებას ეწოდება რადიაცია:

„მოკლედ, 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. რადარი, რომელზეც მე ვმსახურობდი, სანტიმეტრულ დიაპაზონში, ახლოს მობილური კავშირის სიხშირესთან, მაგრამ სიმძლავრე იმპულსში ჰქონდა 750კვტ, ხოლო მობილური 4G ტელეფონის სიმძლავრე არის 0,2ვტ. არ მოვყვები ახსნას რა არის რადარების ფონური გამისხივება და ა.შ. რა პირობებშიც წლები გავატარე. განა ვამბობ, რომ სასარგებლოა? ან რა, სასარგებლოა მაღალი ძაბვის ელექტრო გადამცემი ხაზები? სასარგებლოა ტელევიზორი, wi-fi როუტერი, სხვა ხელსაწყოები? Wi-fi სახლში ყველას გვაქვს. ასევე ჩვენს ბინებში აღწევს მეზობლად დამონტაჟებული "როუტერები". რა თქმა უნდა არსებობს დაწესებული ნორმები, რომელთა შესაბამისად ღია და დახურული სივრცეებისთვის სხვადასხვა სიმძლავრის "როუტერები" იწარმოება. სასაეგებლო არც ეს ველია, მაგრამ ჩვენ ამ გარემოს უკვე ვეღარ გავექცევით. სხვათაშორის, სახლში ჩართული ნოუთბუქები, მობილურები, ისინიც წარმიქმნიან ველს. სიგნალის გაცვლა ორმხრივია.ზოგადად, უნდა ვიცოდეთ, რომ 5G-სგან განსხვავებით, 4G ანტენები გაცილებით მძლავრია, სიგნალს ასხივებენ ყველა მიმართულებით, ხშირად ფუჭად ხარჯავენ ენერგიას. მანძილი ანტენებს შორის კილომეტრებია. 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 დააჯეროო კონსპიროლოგიით შეპყრობილი და ფიზიკის მასწავლებელზე გაბრაზებული ადამიანი, რომ გრძელი ტალღებისგან გაბსხვავებით, მილიმეტრულ ტალღებს გააჩნია ცუდი შეღწევადობის უნარი, შესაბამისად, უკვე დავწერე, უკეთ აირეკლება ნებისმიერი ზედაპირისგან. ვინც კონსპიროლოგიას წერს, მათ აქვთ უნარი, უფრო დამაჯერებლად წეროონ, ვიდრე მე. ასევე, ვისაც კონსპიროლოგია უყვართ, მათთვის მნიშვნელოვანია არა ფიზიკა, ან ზოგადად მეცნიერება, არამედ უნდობლობა ნებისმიერი ოფიციალური ვერსიისადმი“.

და ბოლოს, მთავარი კითხვა: როგორ დავიცვათ თავი დეზინფორმაციისგან?

ამირან სალუქვაძის აზრით, შეთქმულების თეორიების ანალიზისას პირველი მეთოდი უნდა გამოიყენოთ, მაქსიმალურად უნდა დავანაწევროთ, დავშალოთ ცალკეულ ფაქტებად, ცალკეულ ფრაგმენტებად და დავინახავთ, არსებობს თუ არა მათ შორის კავშირები:

„ანალიზისას ბევრ კითხვას უნდა გავცეთ პასუხი. ერთ-ერთი მთავარი კითხვაა, - "ვის აწყობს?" როცა ანალიტიკური წერილი იწერება, პირიქით ვიქცევით, ჯერ ფაქტობრივი მასალები გროვდება, შემდეგ უნდა წამოაყენო ჰიპოტეზა. როცა სტატიას ვკითხულობთ, ან ვიდეო რგოლს ვუსმენთ, თუ კარგად გავაანალიზებთ, ამოვიცნობთ, ფაქტობრივ მასალაზე წამოაყენეს ჰიპოტეზა, თუ პირიქით, ჰიპოტეზა შეაკოწიწეს ფაქტებით. ზუსტად ეს ახასიათებს კონსპიროლოგიას. იგრძნობა ფაქტების სიუხვე ერთი, უფრო სწორად, ერთადერთი ჰიპოტეზის განსამტკიცებლად. ფაქტები, რომლებიც კონსპიროლოგის ჰიპოტეზაში არ ჯდება, მით მეტი, შეიძლება ჰიპოტეზას კითხვის ნიშნის ქვეშ აყენებდეს, არ განიხილება. შეთქმულების თეორიებისგან 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, რომელიც არის კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის - **CYSEC**-ის დამფუძნებელი და თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს ყოფილი დირექტორი (2014 -2016 წწ), რომლის 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:

„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 პროპაგანდის გავრცელებას, მოსახლეობის - სამიზნე აუდიტორიის აღქმის შეცვლას, სამიზნე აუდიტორიის შეხედულებების შეცვლას“.

რა არის საჭირო სახელმწიფოსთვის, რათა ამ მხრივ უფრო დაცული იყოს? ამ შეკითხვაზე ანდრო გოცირიძე პასუხობს, რომ 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 არის 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. თუ არ არსებობს კერძო საჯარო თავისუფლება, ნიშნავს იმას, რომ ჩვენ ვიცავთ სახელმწიფო სერვერებს, ეს კარგია, მაგრამ ყურადღების მიღმა გვრჩება ძალიან დიდი და მნიშვნელოვანი მასივი, სადაც უამრავი პროექტია თავმოყრილი“.

ანდრო გოცირიძის განმარტებით, კიბერუსაფრთხოების კუთხით, საქართველო არ არის ჩამორჩენილი ქვეყანა, გვაქვს საკმაოდ გამართული ინფრასტრუქტურა:

„რა თქმა უნდა, ეს ყველაფერი ჩვენი პარტნიორების დახმარებით გაკეთდა, მაგრამ რაც გვაქვს, რატომ უნდა უარვყოთ? თუმცა არის პატარ-პატარა ხარვეზები, განსაკუთრებით ბოლო ორი წლის განმავლობაში. 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. მიუხედავად ამისა, მაინც ვერ ვიტყვით, რომ ამ მხრივ ჩამოვრჩებით, გრანდებში არ შევდივართ, მაგრამ დაახლოებით ევროპულ დონეზე ვთამაშობთ.

რუსეთი არის ერთ-ერთი ყველაზე ძლიერი კიპერ-აქტორი, რომელიც მიდის ყველაფერზე. გოცირიძის თქმით, მსოფლიოში დესტრუქციულ კიბერ-აქტორებად მოიაზრებენ რუსეთს, ჩინეთს, ირანსა და ჩრდილოეთ კორეას:

„ზოგადად, რუსული ჰიბრიდული ომისგან სრული თავდაცვა არ არსებობს, ეს დიდი პრობლემაა აშშ-ისთვისაც, გერმანიისთვისაც, საფრანგეთისთვისაც და მთელი ევროპისთვისაც, მაგრამ თუ ჩვენ კონტრნაბიჯებს გადავდგამთ, ეფექტური თავდაცვის სასუალება ნამდვილად გვაქვს. ჩვენ 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 კერზო 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 უნდა ჩაერიოს კერძო სექტორის საქმიანობაში, უნდა არსებობდეს სტანდარტი, თუ ხარ კრიტიკული ინფრასტრუქტურის წარმომადგენელი, მაშინ შენი სისტემა უნდა იყოს დაცული. 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 იღუპზია, 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. 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“.

რა უნდა გააკეთოს ცივილიზებულმა სამყარომ? აქაც თავდაცვის ჩვეულებრივი მეთოდები მოქმედებს. დღეს კიბერ-ტერორისტები კარგად იყენებენ სოციალურ ქსელებს, მათთვის ხელმისაწვდომია ინფორმაცია თითქმის ყველა ადამიანზე. გოცირიძე ხაზგასმით აღნიშნავს ინტერვიუში, რომ 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 (სახელმწიფო უშიშროების მინისტრის ყოფილი მოადგილე (2004), გენერალური შტაბის ყოფილი უფროსი (2005-2006), პოლკოვნიკი:

„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 თუნდაც სოციალური ქსელები. 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 სახისა: 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 ახალი საინფორმაციო ომი. 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“.

ქართული რეალობა - როგორ დავიცვათ თავი ყალბი ამბებისგან? ლევან ნიკოლეიშვილის თქმით, 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 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? ნიკოლეიშვილის აზრით, 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? მე ვფიქრობ, აქ უკვე დაკვეთასთან გვაქვს საქმე. შეიძლება სადღაც რაღაცა მოხდა, ჟურნალისტმა ფაქტი დაიჭირა, დაინტერესებული პირებისგან აიღო ფული და რუსებს წააკლა საქართველოც, ასწია 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“.

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. ნიკოლეიშვილი ინტერვიუში აღნიშნავს, რომ რუსეთი საამისოდ იყენებს ყველა ხერხს, მათ შორის კიბერომს, კიბერთავდასხმებს, ჰაკერულ ჯგუფებს, საინფორმაციო ომს და ასე შემდეგ:

„რუსეთი არ ებრძვის მხოლოდ საქართველოს, ის ებრძვის თითქმის მთელ მსოფლიოს. როდესაც ნატო-ს ეგიდით გამართულ კონფერენციებს ვესწრებოდი წლების წინ, იქ იყო ხოლმე 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, ხოლო მისი 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. 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 ოკუპირებული გვაქვს, ტერორიზმის საკითხები მისახედი გვაქვს, უსაფრთხოების თემა მოსაგვარებელი გვაქვს. რა თქმა უნდა, ამაზე კი 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. 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.

როგორც საკვლევ-საკონსულტაციო ცენტრ „ფსიქოპროექტის“ დამფუძნებელი და დირექტორი, ფსიქოლოგიის მეცნიერებათა დოქტორი, სოციოლოგი **ზურაბ ბიგვავა** ამბობს:

„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“.

რა მოაქვს სოციოლოგიური კვლევებისას ყალბი შედეგების გავრცელებას და არის თუ არა ეს საინფორმაციო ომის ერთ-ერთი შემადგენელი ნაწილი? ზურაბ ბიგვავას თქმით, სოციოლოგიური კვლევებისას ხშირად ვაწყდებით ყალბ შედეგებს:

„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. მაგალითად, ავხსნათ, რა აზრი აქვს „ევროპული საქართველოს“ ერთ-ერთი ლიდერის, დავით ბაქრაძის მუდმივ პირველობას გამოკითხვების თანახმად, თუკი რეალობა

სხვანაირია? 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“.

ზურაბ ბიგვავას აზრით, 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.

იყო ინიციატივა, რომ საქართველოში გაერთიანებულიყო ძლიერი კვლევითი ორგანიზაციები, რომლებიც ობიექტუროზით 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“.

ისტორიის მეცნიერებათა დოქტორის, ასოცირებული პროფესორის, თადარიგის პოლკოვნიკის, სახელმწიფო და კორპორაციული უშიშროების სპეციალისტ-ანალიტიკოსის **დავით კუხალაშვილის** აზრით, დღეს კიბერომების მხრივ მსოფლიოში არის უმძიმესი მდგომარეობა, მით უმეტეს, ისეთი სახელმწიფოებისთვის, რომლებსაც არ გააჩნიათ მყარი დაცვის სისტემები:

„ამ მხრივ მოისუსტებენ ისეთი ქვეყნები, სადაც ხშირად ხდება გადატრიალებები და პოლიტიკური სიტუაცია არის მყიფე. დღეს უმთავრესი საკითხია, თუ როგორ უნდა დაიცვან ადამიანებმა თავი

კიბერთავდასხმებისგან, საინფორმაციო ომისგან, ფსიქოლოგიური შემოტევებისგან და ასე შემდეგ. ყველაზე კარგი თავდაცვა გახლავთ განათლება - ეს თემა უნდა ისწავლებოდეს დაწყებითი კლასებიდან და გრძელდებოდეს ეტაპებად შემდეგ საფეხურებზე. 2016 წლის შემოდგომაზე შეიქმნა აიპ „ეროვნული და კორპორაციული უსაფრთხოების სასწავლო კვლევითი ცენტრი“, რომლის ძირითად მიზანს ეროვნული უსაფრთხოების კუთხით ქვეყნის მოსახლეობის ცნობიერების დონის ამაღლება, ხოლო სასწავლო პროცესის ამოცანას ეროვნული უსაფრთხოების უზრუნველყოფის პროცესში თითოეული მოქალაქის როლის გათვითცნობიერება წარმოადგენს. ცენტრის მიერ მომზადებულია პროგრამები, რომლებიც როგორც სახელმწიფო მოხელეების, ისე კორპორაციულ სექტორში დასაქმებული პირების, ზოგადად საზოგადოების ყველა ფენის ცნობიერების დონის ამაღლებას ემსახურება, სახელმწიფოთა მიერ განხორციელებული ისეთი ქმედებების მიმართ, როგორიცაა: სადაზვერვო და კონტრსადაზვერვო საქმიანობა, კორპორაციული ჯაშუშობა, პირადი უსაფრთხოება და სხვა“.

თუმცა, როგორც დავით კუხალაშვილი ამბობს, რაც დღეს კეთდება, არ არის საკმარისი, სახელმწიფოსთვის უპირველესად გასაძლიერებელია სადაზვერვო საქმიანობა და უცხო ქვეყნების პროპაგანდის მოგერიება:

„სპეცსამსახურები და პოლიციური სტრუქტურები, ასე ვთქვათ, უნდა გადაბარგდნენ ამ სფეროში, რათა დროულად მოხდეს ყველა ორგანიზებული დანაშაულის გამოვლენა. ვიმეორებ, უნდა შეივსოს საგანმანათლებლო სივრცე, ყურადღება მიექცეს სამეცნიერო მიმართულებას. ჩვენ გვჭირდება კვლევითი ლაბორატორიები. კიბერომები არასოდეს არ შეწყდება, პირიქით, უფრო გაფართოვდება, სანამ არსებობს კიბერსივრცე, იარსებებს კიბერომებიც“.

შესაძლებელია თუ არა, დღეს რამდენიმე სახელმწიფოს ვუწოდოთ „აგრესორი“ კიბერ-აქტიურობის მიმართულებით? დავით კუხალაშვილი ამბობს, რომ საკითხი უნდა დავაყენოთ ასე:

„ყველა სახელმწიფოს გააჩნია თავისი ინტერესები, ნებისმიერ ქვეყანას თავის შეიარაღებაში აქვს კიბერომის ელემენტები და გააჩნია სტრატეგია, თუ როგორ უნდა იბრძოლოს ვირტუალურ სივრცეში. ჩვენ გვყვანან სტრატეგიული პარტნიორები, ისინი გვეხმარებიან, მაგრამ ყოველთვის უნდა გვახსოვდეს, პარტნიორობა და დახმარება არის ცვალებადი ცნებები, ხოლო სახელმწიფო ინტერესები არის მუდმივი. საქართველომ თუ არ აითვისა ახალი ტექნოლოგიები, თუ არ განავითარა და არ მოარგო საკუთარ ინტერესებს, მხოლოდ დახმარების იმედით შორს ვერ წავალთ. რაც შეეხება კონკრეტულად რუსეთის ქმედებებს, ამ სახელმწიფოს მიზანი ყველასთვის ნათელია - კიბერთავდასხმებით, საინფორმაციო ომით, გამალებული პროპაგანდით აღმოსავლეთ ევროპასა და პოსტსაბჭოთა სივრცეში უნდა მოახდინოს ზეგავლენა მოსახლეობაზე. ეს შეიძლება იყოს ცრუპროპაგანდით კეთილგანწყობის მოპოვება, შიშის ინსპირირება და ასე შემდეგ. რუსეთს აქვს მუდმივი სურვილი, ნებისმიერი ქვეყნის ხელისუფლება მართოს თავის სასარგებლოდ, კონტროლი დაუწესოს ეკონომიკური და პოლიტიკური კუთხით. ასეა რუსეთი და ასე არიან სხვა სახელმწიფოებიც, მათ შორის, ჩვენთან მიმართებაში. თუ ხელისუფლება ფიქრობს საკუთარი ქვეყნის კეთილდღეობაზე, მუდმივად უნდა იზრუნოს უსაფრთხოებაზე, დაზვერვაზე და ასე შემდეგ“.

დავით კუხალაშვილის თქმით, სამწუხაროდ, დღეს ტერორიზმის შემოქმედებად უკვე გვევლინებიან სახელმწიფოები და არა ერთეული ჯგუფები:

„აქედან გამომდინარე, აუცილებელია სრული მზადყოფნა დაზვერვის მხრივ. სამწუხაროდ, ჩვენ ორი ძირძველი ტერიტორია გვაქვს დაკარგული, სადაც ჩამოყალიბებულია სეპარატისტული რეჟიმები და არსებობს ყველა პირობა, რომ ტერორიზმი და კიბერთავდასხმები ამ ტერიტორიების გამოყენებით განხორციელდეს. გვაქვს ისეთი ზონებიც, სადაც რუსეთს და სხვა მტრულად განწყობილ სახელმწიფოებს შეუძლიათ, განახორციელონ ეთნიკური და რელიგიური ტერორიზმი.

რუსეთის მიერ შემუშავებული მეთოდები თითქმის მუდმივია, ხელწერა არ იცვლება - სახელმწიფო, სამხედრო გადატრიალება, გადაბირება¬ და სხვა. ამას დაემატა სოცქსელები და მასმედია¬. სპეცსამსახურები პოლიტიკურ თუ საზოგადოებრივ ჯგუფებს იყენებენ გავლენის აგენტებად. დიდი ხანია შედგენილია ჩვენი, როგორც ერის ფსიქოლოგიური პორტრეტი და ძალზე ადვილია მანიპულირება“.

პოლიტოლოგისა და ექსპერტის, საერთაშორისო და უსაფრთხოების საკითხებში, **ნიკა ჩიტაძის** განმარტებით, კიბერომი არის ერთ-ერთი სერიოზული საფრთხე კაცობრიობისთვის. საქმე იქამდეც კი მივიდა, რომ უკვე სახელმწიფოები აწარმოებენ ერთმანეთის წინააღმდეგ ე.წ. საინფორმაციო ომს და კიბერთავდასხმებს:

„აქვე მაგალითებიც შეგვიძლია მოვიყვანოთ, რომელიც უკავშირდება კორონავირუსს: 2020 წლის მარტში, როდესაც მსოფლიოში დაავადებულთა 90 პროცენტი მოდიოდა ჩინეთზე, ამავე სახელმწიფოს საგარეო საქმეთა სამინისტროს წარმომადგენლებმა გაავრცელეს განცხადება, თითქოს ჩინეთის ტერიტორიაზე ვირუსი ამერიკელმა ჯარისკაცებმა შეიტანეს. ამის შემდეგ მსგავსი პროპაგანდა წამოიწყო რუსეთმა, აშშ საეჭვო ლაბორატორიებს აფინანსებსო და მათ შორის საუბარი იყო ლუგარის ლაბორატორიაზე. ეს პროპაგანდა გრძელდება“.

კიბერთავდასხმები და საინფორმაციო ომი მიმდინარეობს სახელმწიფოების დონეზე, თუმცა რამდენად არიან ჩართულნი ამ საქმეში კერძო პირები, ანუ ავტორიტეტები? ამაზე ჩიტაძე პასუხობს, რომ საინფორმაციო ომში მხოლოდ სახელმწიფოები არ მონაწილეობენ, გამოჩნდებიან ხოლმე ავტორიტეტები, რომლებიც ამტკიცებენ, თითქოს კორონავირუსი ხელოვნურია:

„მაგალითად, არის ლუკ მონტანიე, ფრანგი ვირუსოლოგი, ნობელის პრემიის ლაურეატი, რომელმაც განაცხადა, ამ ვირუსს ხელოვნული წარმომავლობა აქვს და უხანის ლაბორატორიიდან გავრცელდაო“.

როგორც ყველა შემთხვევაში, აქაც გვერდს ვერ ავუვლით რუსეთის ფაქტორს, რომელიც საქართველოსთვის კარგადაა ცნობილი. ნიკა ჩიტაძის თქმით, რუსეთის მიერ წარმოებულ კიბერთავდასხმებს საქართველოზე, ამას საკმაო ისტორია აქვს:

„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“.

ინტერნეტსივრცის ბოლომდე გაკონტროლება შეუძლებელია. თუმცა არსებობს მეთოდები, რომლის გამოყენებისას, შესაძლებელია, შედარებით განეიტრალდეს მსოფლიო დონის მავნებლობა:

„ინტერნეტსივრცე რომ შედარებით უსაფრთხო 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, ყველამ უნდა დაიცვას. ეს 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. აქედან გამომდინარე, შესაძლებელია, შეიქმნას რამდენიმე საერთაშორისო ორგანიზაცია, რომლებიც პირდაპირ იმუშავაბენ 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“.

როგორც ნიკა ჩიტაძე ამბობს, 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“.

ფოკუს ჯგუფი - 2008 წლის რუსეთ-საქართველოს ომი და კიბერთავდასხმა

2008 წლის აგვისტოში საქართველო გახდა რუსული აგრესიის მსხვერპლი, რასაც წინ უძღვოდა კიბერომი. შეიარაღებულ თავდასხმამდე რამდენიმე დღით ადრე და თავდასხმის პერიოდშიც სახელმწიფო სტრუქტურების ვებ-გვერდებზე განხორციელდა არნახული შეტევა. კიბერთავდასხმა მოხდა 60-მდე სამთავრობო ვებ-გვერდზე.

კვლევისთვის შევარჩიეთ კსუ-ის საერთაშორისო ურთიერთობისა და საერთაშორისო უსაფრთხოების ფაკულტეტის სტუდენტები - 2 მაგისტრანტი, 2 ბაკალავრი, სტუდენტების ასაკი განისაზღვრებოდა 18-დან 30 წლამდე. **განვიხილეთ 2008 წლის რუსეთ-საქართველოს ომი და კიბერთავდასხმა.** მათ გააჩნიათ ურთიერთსაწინააღმდეგო მოსაზრებები აღნიშნულ საკითხთან დაკავშირებით. მიზანი იყო, გაგვერკვია ტენდენცია, ბაკალავრის და მაგისტრატურის სტუდენტები რამდენად ერკვეოდნენ აღნიშნულ საკითხში და რამდენად რეალურად აღიქვამდნენ რუსეთის მხრიდან კიბერთავდასხმის საფრთხეს.

1) იქონია თუ არა გადამწყვეტი გავლენა კიბერთავდასხმამ და მისცა თუ არა რუსეთს უპირატესობა, რათა უფრო „ეფექტურად“ განეხორციელებინა სამხედრო, ანუ ფიზიკური აგრესია?
2) რა მიზანს ისახავდა რუსეთის მხრიდან წამოსული კიბერთავდასხმა, ეს იყო ფანდი, რათა საქართველოს ხელისუფლებას ყურადღება სხვა რამეზე გადაეტანა და მორალურად განადგურებულიყო, თუ ეს იყო ფიზიკური თავდასხმის ერთ-ერთი შემადგენელი ნაწილი?

3) რუსი ჰაკერები აცხადებდნენ, რომ საინფორმაციო ომი საქართველომ დაიწყო და ამიტომაც მოუწიათ ჩართვა. რამდენად სარწმუნოა მათი ვერსია?
4) სპეციალისტების თქმით, იმ პერიოდში საქართველოს არ ჰქონდა შესაბამისი ტექნოლოგიები და აპარატურა, რომ წინააღმდეგობა გაეწია რუსული აგრესიისთვის, როგორ ფიქრობთ, დღეს შესაძლებელია თუ არა პასუხის გაცემა?
5) დღეს წარმოადგენს თუ არა საფრთხეს რუსეთიდან მოსალოდნელი კიბერთავდასხმები? რა არის საჭირო იმისთვის, რომ ანალოგიურ თავდასხმებს წინააღმდეგობა გავუწიოთ?

პირველი მაგისტრანტის აზრით, საქართველოს იმ პერიოდში კიბერთავდასხმასა და პროპაგანდასთან ბრძოლის გამოცდილება არ ჰქონდა. ქვეყანა სამ ფრონტზე საერთაშორისო პარტნიორების იმედად იბრძოდა.

მეორე მაგისტრანტი აღნიშნავს, რომ გამოცდილება არაფერ შუაშია, რადგან თითქმის იგივე სახის კიბერთავდასხმა განხორციელდა 2019 წელს, როცა ქართული მედიასაშუალებების სერვერები „დაიბომბა“. შესაძლებელი იყო, ასეთივე თავდასხმა განხორციელებულიყო სამთავრობო საიტებზეც და შედეგი იქნებოდა იგივე, რაც იყო 2008 წლის აგვისტოს ომის დროს.

პირველი ბაკალავრის თქმით, ეს იყო თავდასხმა სამი მიმართულებით - სამხედრო თავდასხმა, საჰაერო თავდასხმა და ინტერნეტთავდასხმა. ვერ ვიტყვით, რომ რუსეთის ხელისუფლებამ ეს გააკეთა მხოლოდ ყურადღების გადატანის მიზნით, აგრესორმა სახელმწიფომ გამოიყენა სამი გამანადგურებელი კომპონენტი და სამწუხაროდ, გამოიყენა წარმატებით.

მეორე ბაკალავრის შეფასებით, ეს იყო თავდასხმა ყურადღების გადატანის მიზნით, ანუ დაბნეულობისა და შიშის დანერგვის მიზნით:

„ლოგიკურად ვიმსჯელოთ, რაში სჭირდებოდა რუსეთს კიბერთავდასხმა, ამის გარეშე ომს ვერ მოიგებდა? მე თუ მკითხავთ, ავიაციის გამოყენებაც კი ზედმეტი იყო, ესეც დაბნეულობის მიზნით გაკეთდა“.

პირველი მაგისტრანტი: „მე არ ვიზიარებ აზრს, თითქოს კიბერთავდასხმა საქართველომ დაიწყო. როგორც ვიცი, ცრუ-ფაქტიც დადეს, ქართული ონლაინგამოცემის Civil.ge-ს ვებგვერდის სქრინშოტი, რომელზეც ჩანს, რომ შეტევის შემდეგ გამოცემა მკითხველს სიახლეების ელ.ფოსტით გაგზავნას სთავაზობდა. დავუშვათ, სთავაზობდა, მერე რა, ეს ხომ არაფერს ამტკიცებს“?

მეორე მაგისტრანტი: „რუსეთი რომ ოკუპანტია, ორი აზრი არ არსებობს, მაგრამ ეს ქვეყანა მაგონებს მიძინებულ დათვს, რომლის გაღვიძებაც სახიფათოა. 2008 წლის აგვისტოში საქართველოს პროვოკაციულმა ხელისუფლებამ დათვი გააღვიძა და მივიღეთ ის, რაც მივიღეთ - ცეცხლი მიწაზე, ცეცხლი ჰაერიდან და ცეცხლი ინტერნეტსივრცეში. არადა, ყველამ კარგად იცოდა, რომ ასე მოხდებოდა. როდესაც შედეგი წინასწარ არის ცნობილი, რატომ უნდა წახვიდე ავანტიურაზე“?

პირველი ბაკალავრი თვლის, რომ საქართველოს, თავისი გეოპოლიტიკური მდგომარეობიდან გამომდინარე, სჭირდება უფრო ძლიერი სპეცსამსახურები, აგენტურული ქსელი და რა თქმა უნდა, შესაბამისი ტექნიკა. შეიძლება ეს შორეული პერსპექტივაა, მაგრამ ინტერნეტსივრცეში აუცილებელია თანამედროვე ტიპის ტექნოლოგიები და უაღრესად განსწავლული კადრები.

მეორე ბაკალავრი სვამს შეკითხვას: რატომ არის შორეული პერსპექტივა? აქვე თვითონ პასუხობს, რომ თანამედროვე ტექნოლოგიების ათვისებას, ეფექტური აგენტურული ქსელის შექმნას და კადრების მომზადებას კი სჭირდება დრო, მაგრამ ეს სულაც არ არის შორეული პერსპექტივა, ეს არის დღესვე გასაკეთებელი საქმე.

პირველი ბაკალავრის თქმით, ამას სჭირდება პოლიტიკური ნება ხელისუფლების მხრიდან: „მე არ ვამტკიცებ, რომ საქართველოს ხელისუფლება ბოლომდე კრემლის დავალებებს ასრულებს, მაგრამ აშკარად ჩანს დათმობაზე წასვლის ნიშნები. ამბობენ, რომ 2008 წლის აგვისტოს ომის შემდეგ კიბერთავდასხმების მხრივ მდგომარეობა გამოსწორდა, ანუ

საქართველოს უკვე გააჩნია ეფექტური თავდაცვითი სისტემები, თუმცა რა გვაჩვენა 2019 წელს რუსეთის მხრიდან განხორციელებულმა მორიგმა თავდასხმამ? ფაქტობრივად, იგივე. როგორც ჩანს, კვლავ დაუცველები ვართ“.

პირველი მაგისტრანტი თვლის, რომ 2008 წლის შემდეგ მდგომარეობა ალბათ ცოტა გამოსწორდა, ტექნოლოგიებიც უფრო მეტად განვითარდა, მაგრამ ვერ ხედავს ეფექტურ ნაბიჯებს ხელისუფლების მხრიდან: ჩვენ ყოველწლიურად გვიგდებენ ანგარიშებს, სადაც წერია, რომ რუსეთი ტრადიციულად გვებრძვის კიბერთავდასხმებით, რბილი ძალით, ცრუ პროპაგანდით, გაჩაღებული აქვს საინფორმაციო ომი. მერე რა, რა კეთდება იმისთვის, რომ ეს ყველაფერი აილაგმოს? სხვათა შორის, წინა ხელისუფლების დროს ამ მხრივ უფრო მეტი აქტიურობა შეინიშნებოდა“.

მეორე მაგისტრანტი სვამს შეკითხვას: რაში გამოიხატებოდა წინა ხელისუფლების აქტიურობა და თუ ასე იყო, რას მიაღწია?

პირველი მაგისტრანტის აზრით, წინა ხელისუფლების დროს დააკავეს არაერთი რუსი ჯაშუში. თუმცა არა მხოლოდ რუსი: „2012 წლის შემდეგ ამ მხრივ თითი თითზე არ დაუკარებიათ. არადა, ხომ ვკითხულობთ სახელმწიფო უსაფრთხოების ანგარიშებში, რომ დღეს რუსეთი გვებრძვის იგივე მეთოდებით“?

მეორე ბაკალავრი: „წინა ხელისუფლების დროს ჯაშუშებზე ნადირობა მართლაც იყო გაჩაღებული, მაგრამ სიტუაცია იყო კომიკური. გავიხსენოთ თუნდაც ფოტორეპორტიორების საქმე, იმჟამინდელი პროკურატურა თავდაპირველად აცხადებდა, რომ დაკავებულები თანამშრომლობდნენ კაგებესთან. ამ საქმეს ისეთი უვიცები იძიებდნენ, არც კი იცოდნენ, რომ 1990-იანი ელების შემდეგ, რაც საბჭოთა კავშირი დაიშალა, კაგებე აღარ არსებობს“.

პირველი მაგისტრანტის აზრით, ეს შეიძლება ყოფილიყო მექანიკური შეცდომა. მეორე ბაკალავრი ამბობს, რომ იურისპრუდენციაში მექანიკური შეცდომები არ არსებობს, ყოველ შემთხვევაში, არ უნდა არსებობდეს, რადგან

შესაძლოა, ერთმა მცირე შეცდომამაც კი ადამიანი ციხეში გამოკეტოს წლების განმავლობაში.

მეორე ბაკალავრი ამბობს, რომ ამის საუკეთესო მაგალითად ვახტანგ მაისაიას საქმეც გამოდგება. მას სამი ქვეყნის ჯაშუშობის ბრალდება წაუყენეს. პირველი მაგისტრანტი ამბობს, რომ ამ საქმის შესახებ გაუგია, მაგრამ დეტალურად არ იცნობს. მეორე ბაკალავრის თქმით, საჭიროა, ამ და სხვა საქმეებს დეტალურად გაეცნონ სტუდენტები. მაგალითად, არსებობს კილაძის, კიღურაძის, „ენვერისა“ და სხვათა საქმეებიც. პირველი და მეორე მაგისტრანტის აზრით, ეს საქმეები მართლაც უნდა იყოს განხილვის საგანი. პირველი ბაკალავრის თქმით, თუ იყო გადაცდომები, მაშინ ეს საქმეები ხელახლა უნდა გამოიძიონ.

შეჯამება: სტუდენტების მიერ შემთხვევის განხილვამ გვაჩვენა, რომ ისინი კი ერკვევიან საერთო სიტიაციაში, მაგრამ კონკრეტულ საკითხებზე საუბრისას ვეღარ მიდიან თემის სიღრმეებში, რადგან დეტალურად არ აქვთ შესწავლილი საქმეები. ისინი სწორ აქცენტებს სვამენ რუსულ შოვინისტურ პოლიტიკაზე საუბრისას. მათი აზრით, დღეს საჭიროა ახალი ტექნოლოგიების დანერგვა, განათლება და კადრების შერჩევა.

დასკვნა და რეკომენდაციები

<u>კვლევის შედეგი:</u>

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

მიუხედავად, კიბერუსაფრთხოების უზრუნველყოფის მექანიზმები დიდწილად დამოკიდებულია ცალკეული ქვეყნის გამოცდილებაზე ამ საკითხის, რასაც კავკასიის რეგიონული უსაფრთხოების შემთხვევაში, პოსტსაბჭოთა სივრცისა და საქართველოს მაგალითები გვიჩვენებს. რაც შეეხება ევროკავშირში გაწევრიანებულ სახელმწიფოებს, არაერთი ფაქტი ადასტურებს და ექსპერტებიც აღიარებენ, რომ არც ეს ზონაა ბოლომდე დაცული. კიბერომი, ასიმეტრიული საფრთხე, ინტერნეტსივრცის გამოყენება ტერორიზმის თვალსაზრისით. ეს გახლდათ ნაშრომის ძირითადი წითელი ხაზი და შინაარსი. ასევე, კვლევის საგანი იყო, თუ რა სერიოზული პრობლემების, ანუ საფრთხის წინაშე დგას ცივილიზებული სამყარო, რა სიკეთე მოაქვს ტექნოლოგიების განვითარებას და ამავე დროს, რა გამოწვევები ჩნდება ყოველდღიურად. სად არის საქართველო, როგორ უნდა ჩავერთოთ საერთაშორისო თავდაცვის სისტემაში? სტაბილურობის ერთადერთი გარანტი არის დასავლური კურსი და ყველა იმ გამოწვევის გათავისება, რომელიც აწუხებს თანამედროვე სამყაროს. საქართველო ამ კუთხით სწორ გზას ადგას. თუმცა ჯერ კიდევ ბევრი მუშაობაა საჭირო, რათა გავხდეთ ამ სამყაროს სრულფასოვანი წევრი.

საჭიროა პრევენციული ზომები. ვინაიდან, საქართველო მდებარეობს ევროპა-აზიის გასაყარზე და ტერორისტებისთვის თუ ნარკომოვაჭრეებისთვის სატრანზიტო დერეფანსაც წარმოადგენს, ბუნებრივია, არსებობს უდიდესი ინტერესი. სახელმწიფო სტრუქტურების მიერ უკვე აღიარებულია, რომ ქვეყანაში არსებობს ექსტრემისტული შეხედულებების მქონე პირთა ჯგუფები. გამორიცხული არ არის, მათ საკუთარი კავშირები და ფინანსური შესაძლებლობები სხვადასხვა ექსტრემისტული ან ტერორისტული ჯგუფებისა თუ ორგანიზაციების სასარგებლოდ გამოიყენონ. ექსტრემიზმი ხშირად იცვლის ფორმას და გადადის ტერორიზმში, რაც დაკავშირებულია ასევე ჰიბრიდულ ომთან, რაც თავისთავად გულისხმობს საინფორმაციო თუ იდეოლოგიურ ომს.

ერთადერთი, რაც ამ ყველაფერს დაუპირისპირდება, ეს არის პრევენციული ზომები სახელმწიფოს მხრიდან.

საქართველოს ეროვნული უსაფრთხოების კონცეფცია არის დოკუმენტი, რომლითაც ხელისუფლებამ უნდა იხელმძღვანელოს არა მხოლოდ ექსტრემალურ სიტუაციებში, არამედ დასახოს პრიორიტეტები. რას გვეუბნება კონცეფცია, რა არის ქვეყნის პრიორიტეტები? ესენია: საქართველოს უსაფრთხო გარემო, უსაფრთხოება, კეთილდღეობა, მშვიდობა. რაში გამოიხატება, 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".[97]

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,

[97] საქართველოს ეროვნული უსაფრთხოების კონცეფცია, 2018 წ. გვ. 3-30. მოპოვებული: https://mod.gov.ge/uploads/2018/pdf/NSC-GEO.pdf, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

საფრთხეებსა და რისკებზე, კვლავ გვეუბნებიან, რომ საშიშროება გვემუქრება მხოლოდ რუსეთიდან. თუმცა გაკვრით მაინც არის 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.

ბერი სალოსის ქუჩაზე ჩატარებული სპეცოპერაციისას მედიამფლობელები აცხადებდნენ, რომ საქართველოში სიტყვისა და გამოხატვის თავისუფლებაა და არავის აქვს უფლება, რაიმე ფორმით შეზღუდოს საინფორმაციო საშუალებები. თუმცა როდესაც საქმე ეხება სახელმწიფოებრიობას, უნდა არსებობდეს რაიმე სახის სახელმძღვანელო, რეკომენდაციები და კანონი. რასაკვირველია, სიტყვისა და გამოხატვის თავისუფლების შეზღუდვა დაუშვებელია, მაგრამ მსგავსი ექსტრემალური სიტუაციებისთვის აუცილებლად უნდა არსებობდეს სტანდარტები, რათა მედიის მხრიდან არ მივიღოთ გაურკვეველი ახსნა-განმარტებები.

რა არის ტერორისტული აქტი? ეს არის დანაშაული, რომელიც მიზნად ისახავს საზოგადოების დაშინებას. ამ დანაშაულის განსახორციელებლად კი ძირითადად გამოიყენება მედია და სოციალური ქსელები. ტერორისტული დაჯგუფებები არა მარტო ფლობენ საჭირო ტექნიკას, ვიდეოკამერებს, ხმის ჩამწერებსა თუ ინტერნეტს, არამედ ასევე კარგად იციან თუ როგორ მიიპყრან საზოგადოების ყურადღება. ისინი ერკვევიან მედიის მუშაობის

სპეციფიკაში, ინფორმაციის მიწოდების ფორმებსა და ეფექტებში. იციან, რა სახის ინფორმაციის მიწოდება როდის ახდენს ეფექტს მოსახლეობაზე. ფაქტია, ტრაგედია და შოკისმომგვრელი ამბები მედიაში კარგად იყიდება, ეს კი ძალიან დიდი ცდუნებაა თავად ჟურნალისტებისთვის, მედიის რეიტინგისა და ტირაჟირებისთვის.

როგორ უნდა მოიქცეს მედია, საერთოდ აღარ გააშუქოს ტერორისტული აქტები ძირეულად და შემოიფარგლოს მხოლოდ მშრალი ინფორმაციით? ამ შემთხვევაში არსებობს მხოლოდ ერთი გამოსავალი, ანუ ე.წ. ოქროს შუალედი - ხელისუფლებამ უნდა ითანამშრომლოს თავისუფალ მედიასთან, ხოლო თავისუფალმა მედიამ უნდა გაითვალისწინოს არა მხოლოდ საერთაშორისო სტანდარტები და რეკომენდაციები, არამედ ვალდებულიცაა, გვერდზე გადადოს პოლიტიკური ინტერესები და მოვლენები გააშუქოს სახელმწიფო ინტერესებიდან გამომდინარე. გადასახედია, ანუ ცვლილებებია შესატანი როგორც "ეროვნული უსაფრთხოების კონცეფციაში", ასევე მაუწყებელთა შესახებ კანონში. შესაბამის კანონმდებლობაშიც ზუსტად უნდა გაიწეროს საკითხები, თუ რის უფლება აქვს მსგავს სიტუაციებში მედიას და რა უფლება-მოვალეობა აკისრია ხელისუფლებას. რასაკვირველია, მედიის ძირეული გაკონტროლება შეუძლებელია, არავინ იცის, რომელი ჟურნალისტი სად, რა ვითარებაში აღმოჩნდება კრიტიკულ მომენტში, მაგრამ აქ საუბარია ინფორმაციის გავრცელების არეალზე, შინაარსზე, დროსა და სიტუაციაზე. სამწუხაროდ, მედიასაშუალების ზოგიერთ ხელმძღვანელს თუ წარმომადგენელს ჰგონია, რომ თუ გარკვეული თავშეკავებისკენ მოუწოდებენ, ან დაავალდებულებენ, ეს არის ზეწოლა ხელისუფლების მხრიდან. სწორედ აქ არის საჭირო ძალიან ფაქიზი მიდგომა, რათა სიფრთხილე და მოვალეობა მართლაც არ გადაიქცეს ზეწოლად, ან არ ჩათვალონ ზეწოლის მცდელობად. ერთმანეთისგან უნდა გაიმიჯნოს საზოგადოების ინფორმირება და საინფორმაციო ომი ვიღაცის წინააღმდეგ.

სადისერტაციო ნაშრომში, ფაქტებზე დაყრდნობით, განვიხილეთ, გამოვიკვლიეთ და გავაანალიზეთ კიბერომის ფენომენი, როგორც თანამედროვე „ცივი ომის“ ერთგვარი სახეობა, რომელიც შესაძლოა, უფრო საშიში აღმოჩნდეს კაცობრიობისთვის, ვიდრე იყო მე-20 საუკუნის მეორე ნახევარში გაჩაღებული „ცივი ომი“ და დაპირისპირება ორ ბანაკს შორის. არაერთი კვლევისა და ექსპერტების მოსაზრებების საფუძველზე თვალნათელი გავხადეთ 3 წლის (2017-2020) განმავლობაში შექმნილი მდგომარეობა მსოფლიო მასშტაბით, შევიმუშავეთ რეკომენდაციები: 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 თავისან იქნას აცილებული.

დანართები

კითხვარი 1

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

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

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

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?

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

როგორ დავიცვათ თავი რუსული ჰიბრიდული ომისგან და ჰაკერული თავდასხმებისგან?

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

ტერორიზმისა და კიბერტერორიზმის წინააღმდეგ რა ერთობლივი გეგმა უნდა შეიმუშავონ ევროკავშირმა, ამერიკის შეერთებულმა შტატებმა და ნატომ, რათა ბრძოლა უფრო ეფექტური იყოს?

ჩინეთი, რუსეთი, ირანი - არის თუ არა ეს სამი სახელმწიფო კიბერთავდასხმების მხრივ დანარჩენი მსოფლიოსთვის საშიში?

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

რა შეიცვლება მსოფლიოში და მათ შორის საქართველოში პანდემიის შემდეგ?

რას შეცვლის რეალურ ცხოვრებაში "5G"-ის სისტემის დანერგვა?

საქართველოში, წლების განმავლობაში მიმდინარეობს თუ არა სოციოლოგიური ომი?

რას ემსახურება გამოკითხვები, რომლის შედეგებიც ყალბია?

სოციოლოგიური მანიპულაცია გასაგებია, გულუბრყვილო ადამიანებზე გათვლილი ინფორმაციაც, მაგრამ 2011 წლიდან მოყოლებული, მიზანს მაინც ვერ აღწევენ. რატომ ფლანგავენ ამდენ დროს, ფულსა და ნერვებს თუნდაც ცნობილი „აირაი" და „ენდიაი"?

დავუშვათ, რა აზრი აქვს დავით ბაქრაძის „პირველობას" , როცა რეალობა სხვანაირია?

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?

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?

რამდენად არის დახვეწილი ჩვენი კანონმდებლობა ამ კუთხით?

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

კითხვარი 2

ფოკუს ჯგუფისთვის შევარჩიეთ კსუ-ის საერთაშორისო ურთიერთობისა და საერთაშორისო უსაფრთხოების ფაკულტეტის სტუდენტები - 2 მაგისტრანტი, 2 ბაკალავრი, სტუდენტების ასაკი განისაზღვრებოდა 18-დან 30 წლამდე. განვიხილეთ **2008 წლის რუსეთ-საქართველოს ომი და კიბერთავდასხმა.** ფოკუს ჯგუფის ჩატარებისას იყო შემდეგი კითხვები დასმული:

1. იქონია თუ არა გადამწყვეტი გავლენა კიბერთავდასხმამ და მისცა თუ არა რუსეთს უპირატესობა, რათა უფრო „ეფექტურად“ განეხორციელებინა სამხედრო, ანუ ფიზიკური აგრესია?
2. რა მიზანს ისახავდა რუსეთის მხრიდან წამოსული კიბერთავდასხმა, ეს იყო ფანდი, რათა საქართველოს ხელისუფლებას ყურადღება სხვა რამეზე გადაეტანა და მორალურად განადგურებულიყო, თუ ეს იყო ფიზიკური თავდასხმის ერთ-ერთი შემადგენელი ნაწილი?
3. რუსი ჰაკერები აცხადებდნენ, რომ საინფორმაციო ომი საქართველომ დაიწყო და ამიტომაც მოუწიათ ჩართვა. რამდენად სარწმუნოა მათი ვერსია?
4. სპეციალისტების თქმით, იმ პერიოდში საქართველოს არ ჰქონდა შესაბამისი ტექნოლოგიები და აპარატურა, რომ წინააღმდეგობა გაეწია რუსული აგრესიისთვის, როგორ ფიქრობთ, დღეს შესაძლებელია თუ არა პასუხის გაცემა?

5. დღეს წარმოადგენს თუ არა საფრთხეს რუსეთიდან მოსალოდნელი კიბერთავდასხმები? რა არის საჭირო იმისთვის, რომ ანალოგიურ თავდასხმებს წინააღმდეგობა გავუწიოთ?

ბიბლიოგრაფია

1. https://1tv.ge/news/sus-saqartveloshi-gavlenis-gadzlierebit-dainteresebuli-qveynebi-hibriduli-omis-metodebs-iyenebdnen-romlis-mnishvnelovan-instruments-dezinformaciuli-kampania-warmoadgenda/, უკანასკნელად იქნა გადამოწმებული: 10.06.2020
2. https://1tv.ge/news/sus-saqartveloshi-gavlenis-gadzlierebit-dainteresebuli-qveynebi-hibriduli-omis-metodebs-iyenebdnen-romlis-mnishvnelovan-instruments-dezinformaciuli-kampania-warmoadgenda/, უკანასკნელად იქნა გადამოწმებული: 10.06.2020
3. http://studinfo.edu.aris.ge/2013/11/12/nato-%E1%83%99%E1%83%98%E1%83%91%E1%83%94%E1%83%A0-%E1%83%A2%E1%83%94%E1%83%A0%E1%83%9D%E1%83%A0%E1%83%98%E1%83%96%E1%83%9B%E1%83%98%E1%83%A1-%E1%83%AC%E1%83%98%E1%83%9C%E1%83%90%E1%83%90/, უკანასკნელად იქნა გადამოწმებული: 11.06.2020
4. https://mod.gov.ge/ge/news/read/4266/hibriduli-omi-da-misi-gavlena-natos-cevr-da-partnior-qveknebze, უკანასკნელად იქნა გადამოწმებული: 11.06.2020
5. მგალობლიშვილი, გ., ქუთელია, ბ., გურული, ი., & ევგენიძე, ნ. (2016). *"ჰიბრიდული ომი და ევრო-ატლანტიკური სივრცის უსაფრთხოების ლანდშაფტის ცვლილება პოლიტიკური და ეკონომიკური შედეგები".* ეკონომიკური პოლიტიკის კვლევის ცენტრი (EPRC), 2016, დოკუმენტი №1, გვ. 9, მოპოვებული: http://old.infocenter.gov.ge/uploads/files/2016-08/1471530452_hybrid-warfare-report-geo_web.pdf-დან, უკანასკნელად იქნა გადამოწმებული: 11.06.2020
6. მაისაია, ვ., & მაღრაძე, გ. *„21-ე საუკუნის საერთაშორისო პოლიტიკა და „თანამშრომლობითი უსაფრთხოების თეორია“: მითი და რეალობა - რეგიონული და გლობალური ასპექტები“.* თბილისი, საქართველო: უნივერსალი, 2017, გვ. 14-193.
7. მაისაია, ვ. „ჰიბრიდული ომის“ რაობა და მისი გეოსტრატეგიული ასპექტები (მეოთხე თაობის ომი) - კიბერომის მაგალითზე". *The Georgian Times*, 2017 წლის 30, 03. გვ 1. მოპოვებული http://geotimes.com.ge/blogi/?m=82&post_id=10-დან, უკანასკნელად იქნა გადამოწმებული: 11.06.2020

8. ანთაძე, გ. "*ჰიბრიდული ომის თეორია და რუსული პრაქტიკა".* 2019.07.12. გვ. 1, მოპოვებული "საზოგადოებრივი მაუწყებელი": https://1tv.ge/video/hibriduli-omis-teoria-da-rusuli-praqtika/-დან, უკანასკნელად იქნა გადამოწმებული: 11.06.2020
9. ჯონსი, ს. *"საინფორმაციო ომის გაკვეთილები საქართველოსა და დასავლეთისთვის".* 2018.15.06. გვ. 1. მოპოვებული amerikiskhma.com: https://www.amerikiskhma.com/a/georgia-is-a-laboratory-of-how-russian-active-measures-work/4440995.html-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020
10. Melnick Jeff. (Director, Global Solutions Engineering), „Top 10 Most Common Types of Cyber Attacks“, March 10, 2020 Y. P. 1. Extracted: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/, უკანასკნელად იქნა გადამოწმებული: 24.06.2020
11. იაგორაშვილი, ი. *(ვიაჩესლავ მოლოტოვის განცხადება) "მარია ზახაროვა სსრკ-ის მიერ ესტონეთის ოკუპაციას უარყოფს".* 2020.13.02. გვ. 1. მოპოვებული mythdetector.ge: https://www.mythdetector.ge/ka/myth/maria-zakharova-ssrk-mier-estonetis-okupatsias-uarqops-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020
12. გობრონიძე, გ.. *(იოზეფ გებელსის დოქტრინა) "გებელსი, პროპაგანდა, გეორგიევსკის ბაფთა და უკრაინა".* 2014.16.06. გვ. 1. მოპოვებული iveria.biz: http://iveria.biz/559-gebelsi-propaganda-georgievsks-bafta-da-ukraina.html-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020
13. ჩივისის, კ. *"რუსეთის ჰიბრიდული ომის დამახასიათებელი ნიშნები".* 2017.19.04. გვ. 1. მოპოვებული gmas.ge: https://gmas.ge/2017/%E1%83%A1%E1%83%98%E1%83%90%E1%83%AE%E1%83%9A%E1%83%94%E1%83%94%E1%83%91%E1%83%98/%E1%83%A0%E1%83%A3%E1%83%A1%E1%83%94%E1%83%97%E1%83%98%E1%83%A1-%E1%83%B0%E1%83%98%E1%83%91%E1%83%A0%E1%83%98%E1%83%93%E1%83%A3%E1%83%9A%E1%83%98-%E1%83-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020
14. საქართველოს მთავრობის დადგენილება №14. *"საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი*

სამოქმედო გეგმის დამტკიცების შესახებ". 2017.13.01. გვ. 1-38, მოპოვებული gov.ge: http://gov.ge/files/469_59439_212523_14.pdf-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020

15. ლიკლიკაძე, კ. *როგორი წესებით უნდა ვიომოთ კიბერომში?* 2013.07.04. გვ. 1. მოპოვებული radiotavisupleba.ge: https://www.radiotavisupleba.ge/a/military-programm/24950058.html-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020
16. ლიკლიკაძე, კ. *როგორი წესებით უნდა ვიომოთ კიბერომში?* 2013.07.04. გვ. 1. მოპოვებული radiotavisupleba.ge: https://www.radiotavisupleba.ge/a/military-programm/24950058.html-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020
17. ლიკლიკაძე, კ. *როგორი წესებით უნდა ვიომოთ კიბერომში?* 2013.07.04. გვ. 1. მოპოვებული radiotavisupleba.ge: https://www.radiotavisupleba.ge/a/military-programm/24950058.html-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020
18. მაისაია, ვ. „ჰიბრიდული ომის“ რაობა და მისი გეოსტრატეგიული ასპექტები (მეოთხე თაობის ომი) - კიბერომის მაგალითზე". The Georgian Times, 2017 წლის 30, 03. გვ 1. მოპოვებული http://geotimes.com.ge/blogi/?m=82&post_id=10-დან, უკანასკნელად იქნა გადამოწმებული: 11.06.2020
19. გერასიმოვი, ვ. *"ჰიბრიდული ომი რუსულ სამხედრო თეორიაში".* 2017.10.07. გვ. 1. მოპოვებული eugeorgia.info: http://eugeorgia.info/ka/article/637/hibriduli-omi-rusul-samxedro-teoriashi/-დან, უკანასკნელად იქნა გადამოწმებული: 19.06.2020
20. Stoltenberg Jens, "Nato: Cyber-attack on one nation is attack on all", 2019, 27 August, P. 1. https://www.bbc.com/news/technology-49488614, უკანასკნელად იქნა გადამოწმებული: 19.06.2020
21. მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო. 2018. მოპოვებული https://rm.coe.int-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020
22. Williams Mike, "The best antivirus software for 2020", techradar - THE SOURCE FOR TECH BUYING ADVICE, 2020 Y. P. 1. Extracted: https://www.techradar.com/best/best-antivirus/, უკანასკნელად იქნა გადამოწმებული: 23.06.2020
23. O'Leary Mike. "Cyber Operations Building, Defending, and Attacking Modern Computer Networks", Publishing House "Apress", Department of Mathematics, Towson University Towson, MD, US, 2015 Y. P. 237-265.

24. J. Knapp Kenneth, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", U.S. Air Force Academy, Colorado, USA, 2009 Y. P. 26-27
25. Dr Paul Cornish, "CYBER SECURITY AND POLITICALLY, SOCIALLY AND RELIGIOUSLY MOTIVATED CYBER ATTACKS", (Policy Department External Policies), FOREIGN AFFAIRS, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION DIRECTORATE B, POLICY DEPARTMENT, (Study carried out within the framework agreement between ISIS Europe and the European Parliament), Publisher European Parliament, Chatham House, London, February 2009, P. 8-9.
26. Dr Paul Cornish, "CYBER SECURITY AND POLITICALLY, SOCIALLY AND RELIGIOUSLY MOTIVATED CYBER ATTACKS", Publisher European Parliament, Chatham House, London, February 2009, P. 24.
27. http://studinfo.edu.aris.ge/2013/11/12/nato-%E1%83%99%E1%83%98%E1%83%91%E1%83%94%E1%83%A0-%E1%83%A2%E1%83%94%E1%83%A0%E1%83%9D%E1%83%A0%E1%83%98%E1%83%96%E1%83%9B%E1%83%98%E1%83%A1-%E1%83%AC%E1%83%98%E1%83%9C%E1%83%90%E1%83%90/, უკანასკნელად იქნა გადამოწმებული: 11.06.2020
28. მნუჩინი, ს. *"საინფორმაციო ომის გაკვეთილები საქართველოსა და დასავლეთისთვის"*. 2018.15.06. გვ. 1. მოპოვებული amerikiskhma.com: https://www.amerikiskhma.com/a/georgia-is-a-laboratory-of-how-russian-active-measures-work/4440995.html-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020
29. ჰეიდენი, მ. *"საინფორმაციო ომის გაკვეთილები საქართველოსა და დასავლეთისთვის"*. 2018.15.06. გვ. 1. მოპოვებული amerikiskhma.com: https://www.amerikiskhma.com/a/georgia-is-a-laboratory-of-how-russian-active-measures-work/4440995.html-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020
30. ჰეთერ, კ.. *"საინფორმაციო ომის გაკვეთილები საქართველოსა და დასავლეთისთვის"*. 2018.15.06. გვ. 1. მოპოვებული amerikiskhma.com: https://www.amerikiskhma.com/a/georgia-is-a-laboratory-of-how-russian-active-

measures-work/4440995.html-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020

31. "ინფორმაციის თავისუფლების განვითარების ინსტიტუტის" (IDFI)."კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", პოლიტიკის დოკუმენტი. 2016.22.08. გვ. 5-23. მოპოვებული idfi.ge: https://idfi.ge/public/upload/Meri/Russian%20Propaganda%20in%20Georgia%20-%20Policy%20Paper.PDF-დან, უკანასკნელად იქნა გადამოწმებული: 12.06.2020
32. ლოლაძე, გ. *"დეზინფორმაცია, თითქოს რუსეთის კიბერშეტევებს მხოლოდ ერთი წყარო ადასტურებს"*. 2019.26.03. გვ. 1. მოპოვებული mythdetector.ge: http://www.mythdetector.ge/ka/myth/dezinpormatsia-titkos-rusetis-kibershetevebs-mkholod-erti-cqaro-adasturebs-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020
33. Timberg Craig & Romm Tony, "Hackers are seizing on coronavirus fears to steal data, researchers and U.S. regulators warn", March 12, 2020. P. 1. Extracted https://www.washingtonpost.com/technology/2020/03/12/hackers-are-using-coronavirus-fears-target-people-looking-information-infection-maps/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
34. Lily Hay Newman, "Coronavirus Sets the Stage for Hacking Mayhem", 03.19.2020, P. 1. Extracted: https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
35. Cimpanu Catalin, "Personal details for the entire country of Georgia published online", March 30, 2020. P. 1. Extracted: https://www.zdnet.com/article/personal-details-for-the-entire-country-of-georgia-published-online/?fbclid=IwAR0Jp5j_NCrdw9Et4k80WGwhWW3r2l2FV6COSv7MYWTqj6Qd9YpV_50jcA8, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
36. საქართველოს შინაგან საქმეთა სამინისტრო, "შსს-ს სახელით მოქალაქეებს მესიჯები მიუვიდათ - რა განცხადებას ავრცელებს სამინისტრო", 02.04.2020, გვ. 1. მოპოვებულია: https://www.ambebi.ge/article/243012-shss-s-saxelit-mokalakeebs-mesijebi-miuvidat-ra-g/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

37. კიბერმედია, "კორონა ვირუსით ჰაკერები მანიპულირებენ", მარტი, 14, 2020. გვ. 1. მოპოვებულია: https://seclab.ge/post/CoronaCovid19, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
38. https://imedinews.ge/ge/msoflio/124873/amerikelma-samkhedroebma-iraneli-generali-kasem-suleimani-mokles, უკანასკნელად იქნა გადამოწმებული: 27.05.2020
39. https://1tv.ge/news/ashsh-is-usafrtkhoebis-uwyeba-iranis-mkhridan-shesadzloa-ashsh-ze-%E2%80%8Bkibertavdaskhma-gankhorcieldes/, უკანასკნელად იქნა გადამოწმებული: 05.01.2020.
40. https://imedinews.ge/ge/msoflio/125067/rouhani-52-iranuli-obieqtis-shesakheb-trampis-gantskhadebas-pasukhobs, უკანასკნელად იქნა გადამოწმებული: 06.01.2020.
41. CNN. *"Trump says 'Iran appears to be standing down' following its retaliatory attacks against Iraqi bases housing US troops"*. 2020.08.01. გვ. 1. მოპოვებული edition.cnn.com: https://edition.cnn.com/2020/01/07/politics/rockets-us-airbase-iraq/index.html-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020
42. კუპრეიშვილი, თ. *"ყველაფერი, რაც ვიცით უკრაინული თვითმფრინავის კატასტროფაზე"*. 2020.08.01. გვ. 1. მოპოვებული netgazeti.ge: https://netgazeti.ge/news/418935/-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020
43. საზოგადოებრივი მაუწყებელი. *"ირანმა აშშ-ის სამხედრო ძალები „ტერორისტულ ორგანიზაციად“ გამოაცხადა"*. 2020.07.01. გვ. 1. მოპოვებული 1tv.ge: https://1tv.ge/news/iranma-ashsh-is-samkhedro-dzalebi-teroristul-organizaciad-gamoackhada/-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020
44. http://www.tabula.ge/ge/story/162804-iranshi-kasem-soleimanis-dakrdzalvaze-chkletashi-sul-mcire-35-adamiani-daighupa, უკანასკნელად იქნა გადამოწმებული: 13.06.2020
45. რუჰანი, ჰ. *"ირანის პრეზიდენტი უკრაინული თვითმფრინავის შეცდომით ჩამოგდებას აშშ-ს ქმედებებს უკავშირებს"*. 2020.11.01. გვ. 1. მოპოვებული 1tv.ge: https://1tv.ge/news/iranis-prezidenti-ukrainuli-tvitmfrinavis-shecdomit-chamogdebas-ashsh-s-qmedebebs-ukavshirebs/-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020

46. ტრამპი, დ. *"ნატო-მ ახლო აღმოსავლეთიც უნდა მოიცვას და ახალ ალიანსს დავარქვათ „ნატო+ახლო აღმოსავლეთი“ – რა მშვენიერი სახელწოდებაა, სახელებს კარგად ვიგონებ"*. 2020.10.01. გვ. 1. მოპოვებული interpressnews.ge: https://www.interpressnews.ge/ka/article/580527-donald-trampi-nato-m-axlo-agmosavletic-unda-moicvas-da-axal-alianss-davarkvat-natoaxlo-agmosavleti-ra-mshvenieri-saxelcodebaa-saxelebs-kargad-vigoneb/-დან, უკანასკნელად იქნა გადამოწმებული: 13.06.2020
47. იუსტიციის სამინისტრო. *"კიბერუსაფრთხოების ინდექსში საქართველო მე-8 ადგილზეა"*. 2017.19.06. გვ. 1. მოპოვებული: https://imedinews.ge/ge/politika/16724/kiberusaprtkhoebis-indeqsshi-saqartvelo-me8-adgilzea-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
48. Forbes Georgia. *"კიბერუსაფრთხოების ინდექსით, საქართველო მსოფლიოში მე-19 ადგილზეა"*. 2018.02.08. გვ. 1. მოპოვებული imedinews.ge: https://imedinews.ge/ge/teqnologiebi/72543/kiberusaprtkhoebis-indeqsit-saqartvelo-msoplioshi-me19-adgilzea-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
49. საქართველოს უსაფრთხოების და განვითარების ცენტრი. *ნატო-ს ვარშავის სამიტის დეკლარაციის მოკლე მიმოხილვა (გავლენა საქართველოზე).* 2014 წ. გვ. 2-3. მოპოვებული gcsd.org.ge: http://gcsd.org.ge/storage/files/doc/NATO-Warsaw-Summit-FINAL.pdf-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
50. იუნკერი, ჟ.-კ. *"ჟან-კლოდ იუნკერი აცხადებს, რომ ყალბი ამბები არა მხოლოდ მედიით, არამედ ევროკავშირის წევრი ქვეყნების პრემიერებისგანაც ვრცელდება"*. 2018.14.12. მოპოვებული 1tv.ge: https://1tv.ge/news/djan-klod-iunkeri-ackhadebs-rom-yalbi-ambebi-ara-mkholod-mediit-aramed-evrokavshiris-wevri-qveynebis-premierebisganac-vrceldeba/-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
51. კერსანსკასი, ვ. *"დეზინფორმაციასთან და ყალბ ამბებთან საბრძოლველად მარტივი და სწრაფი გზა არ არსებობს, ეს გრძელვადიანი სტრატეგიაა"*. 2019.24.01. გვ. 1. მოპოვებული 1tv.ge: https://1tv.ge/video/vitautas-kersanskasi-dezinformaciastan-da-yalb-ambebtan-sabrdzolvelad-martivi-da-swrafi-gza-ar-arsebobs-es-grdzelvadiani-strategiaa/-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020

52. https://globalcase.org/page/about-case/, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
53. https://www.emis.ge/news/708/, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
54. საქართველოს პრეზიდენტის ადმინისტრაცია. *საქართველოს პრეზიდენტის ბრძანებულება №321, საქართველოს კიბერუსაფრთხოების.* 2013.17.05. გვ. 1-9. მოპოვებული matsne.gov.ge: https://matsne.gov.ge/ka/document/download/1923932/0/ge/pdf-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
55. http://csbd.gov.ge/, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
56. საქართველოს შინაგან საქმეთა სამინისტრო. *საქართველოს შინაგან საქმეთა სამინისტროს 2018 წლის საქმიანობის ანგარიში.* 2019 წ. გვ. 16-23, მოპოვებული info.police.ge: https://info.police.ge/uploads/5cf7e783a0c6d.pdf-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
57. კაპენი, ფ. *"კონფლიქტის ახალი ფორმა – ჰიბრიდული ომი".* 2016.02.03. გვ. 1. მოპოვებული http://yata.ge/ge/?p=691: http://yata.ge/ge/?p=691-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
58. ცინცაძე, ს. "სოციალური ქსელების განვითარებასთან ერთად ჩნდება თითქმის შეუზღუდავი რესურსი საინფორმაციო ომის მწარმოებლებისთვის". (ინტერვიუერი თ. ზედელაშვილი,), 2017.03.06.
59. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში. *"საქართველოში მცხოვრებ „დაეშის" შესაძლო მხარდამჭერთა რაოდენობა და გავლენა შემცირდა".* 2019.28.03. მოპოვებული imedinews.ge: https://imedinews.ge/ge/samartali/100997/susi-saqartveloshi-mtskhovreb-daeshis-shesadzlo-mkhardamcherta-raodenoba-da-gavlena-shemtsirda-დან, უკანასკნელად იქნა გადამოწმებული: 14.06.2020
60. მაისაია, ვ. *„ისლამური ხალიფატის" საინფორმაციო-პროპაგანდისტული/კიბერ-ვირტუალური ომის სპეციფიკა - „რბილი ძალის" კონცეფტი.* 2017.07.06. მოპოვებული: http://geotimes.com.ge/blogi/?m=82&post_id=18&lng=geo-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020
61. ტოლერანტობისა და მრავალფეროვნების ინსტიტუტის (TDI). *"ძალადობა რელიგიის სახელით და ინტერპრეტაციის მნიშვნელობა".* 2018.07.05. მოპოვებული tdi.ge: https://www.tdi.ge/ge/page/zaladoba-religiis-saxelit-da-

interpretaciis-mnishvneloba-0-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020

62. https://www.myvideo.ge/v/2058973, უკანასკნელად იქნა გადამოწმებული: 15.06.2020
63. Zaman, H. *"თალიბანი საქართველოს შურისძიებით ემუქრება? - შოკისმომგვრელი ვიდეო YouTube-იდან"*. 2013.06.06. გვ. 1. მოპოვებული palitravideo.ge: https://www.palitravideo.ge/garthoba/skhvadaskhva/32044-gaiziare-bedniereba-erthi-qilidan-sayvareli-sasmeli-akhali-shefuthvith.html?start=140&fullComments=1-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020
64. ჯიჰადი. *"ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!"*. 2013.07.06. მოპოვებული for.ge: https://for.ge/view/23153/jihadi-Cven-viciT-Tqveni-saxelebi-misamarTebi-naTesavebi-da-male-saqarTveloSi-CamovalT-Cven-Surs-viZiebT.html-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020
65. საქართველოს სახელმწიფო უსაფრთხოების სამსახური. *"ტერორიზმთან ბრძოლა"*. 2015.01.11. გვ. 1. მოპოვებული ssg.gov.ge: https://ssg.gov.ge/page/counter-terrorism-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020
66. მაისაია, ვ. „ახალი ცივი ომის“ აჩრდილი და მსოფლიო წესრიგის ფუნდამენტური ცვლილება - საქართველო სად არის? 2017.15.05. გვ. 1. მოპოვებული geotimes.com.ge: http://geotimes.com.ge/blogi/?m=82&post_id=16-დან, უკანასკნელად იქნა გადამოწმებული: 15.06.2020
67. აშშ-ის საელჩო საქართველო, "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", 19 დეკემბერი, 2017, გვ. 1. მოპოვებული: https://ge.usembassy.gov/ka/2017-national-security-strategy-united-states-america-president-ka/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
68. აშშ-ის საელჩო საქართველო, "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", 19 დეკემბერი, 2017, გვ. 1. მოპოვებული: https://ge.usembassy.gov/ka/2017-national-security-strategy-united-states-america-president-ka/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

69. Cheng Dean, „Cyber dragon, inside China s information warfare and cyber operations“, The Changing Face of War James Jay Carafano, Series Editor, Publishing House “Praeger”, USA, 2017 Y. P. 79-82.
70. აშშ-ის საელჩო საქართველო, "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", 19 დეკემბერი, 2017, გვ. 1. მოპოვებული: https://ge.usembassy.gov/ka/2017-national-security-strategy-united-states-america-president-ka/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
71. Gartner. *"Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019".* 2018,08,15. P. 1. Retrieved from Gartner: https://www.gartner.com, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
72. Varonis. *"110 Must-Know Cybersecurity Statistics for 2020".* 2020,01,09. P. 1. Retrieved from Varonis: https://www.varonis.com, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
73. კეკენაძე, დ. *"კიბერდანაშაული, როგორც 21-ე საუკუნის მნიშვნელოვანი პრობლემა".* 2019.12.08. გვ. 1. მოპოვებული ON: https://on.ge-დან, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
74. Nakamoto Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", გვ. 1-9. Extracted: https://bitcoin.org/bitcoin.pdf, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
75. paxful, "What Happens When All the Bitcoin in the World Has Been Mined?", March 2, 2020, P. 1. Extracted: https://paxful.com/blog/what-happens-when-all-21-million-bitcoins-mined/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
76. გოგუაძე მამუკა, "მომავლის ვალუტა ბიტკოინი – კრიპტოვალუტა", ნოემბერი 21, 2017, გვ. 1. მოპოვებული: https://financer.com/ge/kriptovaluta-bitcoin/, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
77. https://steemit.com/cryptocurrency/@qanon1111/list-of-all-coin-cryptocurrency-a-to-z, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
78. ჭყოიძე ნატალია & ტომარაძე გიორგი, "ვირტუალური/კრიპტოგრაფიული ვალუტა და მისი თავისებურებები ვირტუალური ვალუტების რეგულირება (bitcoin-ის მაგალითზე)", 2014 წ. გვ. 41-55. მოპოვებული: https://www.nbg.gov.ge/uploads/journal/2014/2014_3/4.pdf, უკანასკნელად იქნა გადამოწმებული: 25.06.2020

79. the developer platform GitHub. *"GitHub Survived the Biggest DDoS Attack Ever Recorded"*. 2018,03.01. P. 1. Retrieved from Wired: https://www.wired.com, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
80. კამიანი, ჰ. *"აშშ მოუწოდებს რუსეთს, შეაჩეროს უგუნური კიბერთავდასხმები საქართველოსა და სხვა ქვეყნებზე"*. 2020.28.02. გვ. 1. მოპოვებული საზოგადოებრივი მაუწყებელი: https://1tv.ge-დან, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
81. Brent, L. *"NATO's role in cyberspace"*. 2019,02.12. P. 1. Retrieved from NATO: https://www.nato.int, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
82. Riazi, T. "Know The CCDCOE: Interview with Director Col. Jaak Tarien". (J. Tarien, Interviewer) 2020,01.29. P. 1. Retrieved from http://natoassociation.ca, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
83. Euvsdisinfo. "*FIGURE OF THE WEEK: 100, ALMOST"*. 2019,11.19. P. 1. Retrieved from euvsdisinfo.eu: https://euvsdisinfo.eu/figure-of-the-week-100-almost/, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
84. Euvsdisinfo. "*FIGURE OF THE WEEK: 100, ALMOST"*. 2019,11.19. P. 1. Retrieved from euvsdisinfo.eu: https://euvsdisinfo.eu/figure-of-the-week-100-almost/, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
85. Euvsdisinfo. "*FIGURE OF THE WEEK: 100, ALMOST"*. 2019,11.19. P. 1. Retrieved from euvsdisinfo.eu: https://euvsdisinfo.eu/figure-of-the-week-100-almost/, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
86. British Broadcasting Corporation. *"UK says Russia's GRU behind massive Georgia cyber-attack"*. 2020,02.20. P. 1. Retrieved from bbc.com: https://www.bbc.com/news/technology-51576445, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
87. გოცირიძე ა. "თუ ქვეყანა არ ფლობს კიბერუსაფრთხოების საჭირო ელემენტებს, ის ვერ ჩაითვლება სანდო პარტნიორად, მათ შორის, ვერც ეკონომიკის ჭრილში". (ინტერვიუერი ს. ლემონჯავა) commersant. თბილისი. 2018.28.05. გვ. 1. მოპოვებული https://commersant.ge/ge/post/ra-dartymas-ayenebs-kiberomi-saqartvelos-ekonomikas-დან, უკანასკნელად იქნა გადამოწმებული: 16.06.2020
88. ჰოლისი, დ. "კიბერომის პირველი გაკვეთილი". kvirispalitra.ge. (ინტერვიუერი ფ. პოლისი,) აშშ. 2011.07.02. გვ. 1. მოპოვებული https://www.kvirispalitra.ge/ras-

weren-chvenze/6616-kiberomis-pirveli-gakvethili.html-დან, უკანასკნელად იქნა გადამოწმებული: 16.06.2020

89. მაისაია, ვ. *„ახალი ცივი ომის“ აჩრდილი და მსოფლიო წესრიგის ფუნდამენტური ცვლილება - საქართველო სად არის?* 2017.15.05. გვ. 1. მოპოვებული geotimes.com.ge: http://geotimes.com.ge/blogi/?m=82&post_id=16-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020
90. https://www.history.com/topics/21st-century/9-11-attacks, უკანასკნელად იქნა გადამოწმებული: 18.06.2020
91. "ინფორმაციის თავისუფლების განვითარების ინსტიტუტის" (IDFI). *"კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", პოლიტიკის დოკუმენტი.* 2016.22.08. გვ. 5-23, მოპოვებული idfi.ge: https://idfi.ge/public/upload/Meri/Russian%20Propaganda%20in%20Georgia%20-%20Policy%20Paper.PDF-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020
92. https://www.mythdetector.ge/ka/myth/dezinpormatsia-titkos-pinetshi-rusul-ojakhebs-bavshvebs-artmeven, უკანასკნელად იქნა გადამოწმებული: 18.06.2020
93. http://damoukidebloba.ge/c/news/sainformacio_omi, უკანასკნელად იქნა გადამოწმებული: 18.06.2020
94. გერმანული გაზეთი "ბილდი". *"გერმანული მედია: რუსები 2008 წელს ბირთვული იარაღის გამოყენებას აპირებდნენ".* 2017.23.12. გვ. 1. მოპოვებული resonancedaily.com: http://www.resonancedaily.com/index.php?id_rub=2&id_artc=42590-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020
95. The Washington Post. *"პენტაგონმა აღიარა, რომ რუსეთის შეჭრის შემთხვევაში, ბალტიისპირეთის ქვეყნების და პოლონეთის დაცვას ვერ მოასწრებს".* 2018.25.06. გვ. 1. მოპოვებული imedinews.ge: https://imedinews.ge/ge/msoflio/67383/pentagonma-agiara-rom-rusetis-shechris-shemtkhvevashi-baltiispiretis-qveknebis-da-polonetis-datsvas-ver-moastsrebs-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020
96. იაგორაშვილმა, ი. *(სერგეი ლავროვის განცხადება) "რუსეთის 2 მითი ბალტიისპირეთის ქვეყნების შესახებ".* 2019.27.09. გვ. 1. მოპოვებული

mythdetector.ge: https://www.mythdetector.ge/ka/myth/rusetis-2-miti-baltiispiretis-kveqnebis-shesakheb-დან, უკანასკნელად იქნა გადამოწმებული: 18.06.2020

97. საქართველოს ეროვნული უსაფრთხოების კონცეფცია, 2018 წ. გვ. 3-30. მოპოვებული: https://mod.gov.ge/uploads/2018/pdf/NSC-GEO.pdf, უკანასკნელად იქნა გადამოწმებული: 19.06.2020
98. Perry Brandon, "Gray Hat C# A Hacker's Guide to Creating and Au t o m a t i n g Security Tools", Publishing House "no sach press", San Francisco, 2017 Y. P. 15-264.
99. Springer Nature Singapore Pte Ltd. "Cyber-Physical System Design from an Architecture Analysis Viewpoint, Communications of NII Shonan Meetings", Publishing House "Springer", Editors Shin Nakajima, Jean-Pierre Talpin Masumi Toyoshima, Huafeng Yu 2017 Y. P. 12-164.
100. "CyberROAD - D 6.2 - Cyber Terrorism Preliminary Best Practices Analysis", (Development of the Cybercrime and Cyber-terrorism Research Roadmap), Funded by the European CommissionSeventh Framework Programme, Version: 1.1, 2015 Y. P. 5-14.
101. Cleary Frances, Felici Massimo (Eds.), "Cyber Security and Privacy" (Communications in Computer and Information Science 530), 4th Cyber Security and Privacy Innovation Forum, CSP Innovation Forum 2015 Brussels, Belgium, April 28–29, 2015 Revised Selected Papers, Publisher "Springer", Commenced Publication in 2007 Founding and Former Series Editors: Alfredo Cuzzocrea, Dominik ęlęzak, and Xiaokang Yang. P. 18-159.
102. Cleary Frances, Felici Massimo (Eds.)"Cyber Security and Privacy", (Communications in Computer and Information Science 470), Third Cyber Security and Privacy EU Forum, CSP Forum 2014 Athens, Greece, May 21–22, 2014 Revised Selected Papers, Publishing House: Springer. P. 16-179.
103. Dunn Cavelty Myriam, "Cyber-Security and Threat Politics", CSS Studies in security and international relations, Publishing House: routledge, London and New York, 2008 Y. P. 12-155.
104. M. Uma and G. Padmavathi (Corresponding author: M. Uma), "A Survey on Various Cyber Attacks and Their Classification", Department of Computer Science, Avinashilingam Deemed University for Women, Coimbatore, Received May 9, 2011; revised and accepted Dec. 12, 2011, P. 392-395.
105. https://issuu.com/sandrasopian/docs/296043650-the-hackers-manual-2016, უკანასკნელად იქნა გადამოწმებული: 25.06.2020
106. Myriam Dunn Cavelty, "Cyber-Security and Threat Politics", CSS Studies in security and international relations, US efforts to secure the information age, Publishing House: Routlendge, London and New York, 2008 Y. P. 12-144.
107. Willson David, "Cyber Security Awareness for CEOs and Management", Contributing Editor Henry Dalziel, USA, Publishing House: Elsevier, 2016 Y, P. 5-46.

108. John G. Voller, "CYBER SECURITY", Canada, Publishing House: Wiley, 2014 Y. P. 9-118.
109. Klipper Sebastian, "Cyber Security", Ein Einblick für Wirtschaftswissenschaftler, Deutschland, Publishing House: Springer, 2015 Y. P. 10-52.
110. James Graham & Richard Howard & Ryan Olson, "CYBER SECURITY ESSENTIALS", Auerbach Publications Taylor & Francis Group, London and New York, Publishing House: CRC Press, 2011 Y. P. 18-287
111. Gregory J. Touhill & C. Joseph Touhill, "Cybersecurity for Executives" (A Practical Guide), the American Institute of Chemical Engineers, Inc. Canada, Publishing House: Wiley, 2014 Y. P. 30-386.
112. Jennifer L. Bayuk & Jason Healey & Paul Rohmeyer & Marcus H. Sachs & Jeffrey Schmidt & Joseph Weiss, "Cyber Security Policy Guidebook", Canada, 2012 Y. Publishing House: Wiley, 19-259.
113. Ferri Abolhassan, "Cyber Security. Simply. Make it Happen". (Leveraging Digitization Through IT Security), Publishing House: Springer, 2017 Y. P. 6-132.
114. Junaid Ahmed Zubairi & Athar Mahboob, "Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies", Published in the United States of America by Information Science Reference (an imprint of IGI Global), 2012 Y. P. 13-295.
115. Alexis Moore & Laurie J. Edward, "Cyber Self-Defense" (Expert advice to Avoid Online Predators, Identity Theft, and Cyberbullying), Publishing House: Lyons Press, 2014 Y. P. 10-245.
116. Julian Richards, "Cyber-War: The Anatomy of the Global Security Threat", USA, Publishing House: PALGRAVE MACMILLAN, 2014 Y. P. 8-89.
117. Clarke A. & Robert K. Knake "Cyber War: The Next Threat to National Security and What to Do About It", United Kingdom, 2010 Y. P. 1-189.
118. JASON ANDRESS & STEVE WINTERFELD & LILLIAN ABLON, "CYBER WARFARE" (Techniques, Tactics and Tools for Security Practitioners), USA, Publishing House: Elsevier, 2014 Y. P. 10-288.
119. Mehedy Masud & Latifur Khan & Bhavani Thuraisingham, "Data Mining Tools for Malware Detection", USA, Publishing House: CRC Press, 2012 Y. P. 32-346.
120. NATO CCD COE Publications, "cyber war in perspective: russian aggression against ukraine", Estonia, Tallinn, Published NATO Cooperative Cyber Defence Centre of Excellence, 2015 Y. P. 8-175.