კავკასიის საერთაშორისო უნივერსიტეტი
Caucasus International University

CBRN
ცბრნ საფრთხეების სტრატეგიული კვლევების ინსტიტუტი
STRATEGIC STUDIES INSTITUTE FOR RESEARCH CBRN THREATS

ციფრული ტექნოლოგიების საუკუნე და კიბერუსაფრთხოების თანამედროვე საერთაშორისო პოლიტიკური გამოწვევები

ორნიკე ხელაშვილი

ციფრული ტექნოლოგიების საუკუნე და ქიბერუსაფრთხოების თანამედროვე საერთაშორისო პოლიტიკური გამოწვევები

თბილისი - 2022

რედაქტორი:

ვახტანგ მაისაია

პოლიტიკის მეცნიერების დოქტორი, კავკასიის საერთაშორისო უნივერსიტეტის პროფესორი, პოლონეთის პოლიტიკური მეცნიერების ასოციაციის წევრი

რეცენზენტები:

ანდრო გოცირიძე

კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის - CYSEC-ის დამფუძნებელი და თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს ყოფილი დირექტორი (2014 -2016 წწ).

ალიკა გუჩუა

პოლიტიკის მეცნიერების დოქტორი, კავკასიის საერთაშორისო უნივერსიტეტის ასოცირებული პროფესორი, საერთაშორისო ურთიერთობებისა და საერთაშორისო უსაფრთხოების ანალიტიკოსი.

დაიბეჭდა გამომცემლობა «თბილისელები პრინტში»

წიგნი გახლავთ გზამკვლევი კიბერუსაფრთხოების სპეციალისტებისთვის, ჰიბრიდული ომების ანალიტიკოსებისთვის, კიბერტერორიზმის წინააღმდეგ მებრძოლი ორგანიზაციებისთვის და დაინტერესებული პირებისთვის. წიგნის გამოყენება შესაძლებელია შემდგომი კვლევებისთვის. ასევე, უმაღლესი სასწავლებლების საბაკალავრო და სამაგისტრო პროგრამებში. კვლევები და რეკომენდაციები გამოსადეგია საქართველოს მთავრობის მიერ ქვეყნის უსაფრთხოების სტრატეგიის ძირითადი მიმართულებების განსაზღვრისთვის. შესაძლოა, კვლევის შედეგები განზოგადდეს პოსტსაბჭოთა ქვეყნებისა და აღმოსავლეთ ევროპის სახელმწიფოებისთვის.

ISBN 978-9941-8-2277-3

სარჩევი

გამოყენებული აბრევიატურა

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

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

IBM - International Business Machines, საერთაშორისო ბიზნეს მანქანები

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

WWW - World Wide Web, მსოფლიო მასშტაბის ქსელი

WIFI - Workforce Investment Field Instructions

DoS - Denial-of-Service, მომსახურების უარყოფა

RBN - Russian Business Network, რუსეთის ბიზნეს ქსელი

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

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

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

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

ICT - Information and Communications Technology, ინფორმაციისა და საკომუნიკაციო ტექნოლოგია

ITU - International Telecommunication Union, საერთაშორისო სატელეკომუნიკაციო კავშირი

ICANN - The Internet Corporation for Assigned Names and Numbers,

მინიჭებული სახელების და ციფრების ინტერნეტკორპორაცია

NDI - National Democratic Institute, ეროვნული დემოკრატიული ინსტიტუტი

HTB - რუსეთის ტელევიზია „ენტევე“

ORT - რუსეთის „პირველი არხი“

RTR - Russia 1, რუსეთის ტელევიზია “რუსეთი 1“

URL - Uniform Resource Locator, რესურსების ერთიანი ლოკატორი

IP - Internet Protocol, ინტერნეტ პროტოკოლი

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

RAP - Readiness Action Plan - მზადყოფნის სამოქმედო გეგმა

KSN - Kaspersky Security Network - კასპერსკის უსაფრთხოების ქსელი

CtfTool - Computerized Transmission Function Tool, გადაცემის კომპიუტერიზებული ფუნქციის ინსტრუმენტი

GEOIP – Geographical Internet Protocol, გეოგრაფიული ინტერნეტ-ადგილმდებარეობა.

VMWARE (Virtual Machine) Workstation - ვირტუალური მანქანის სამუშაო სადგური

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

ZDNet - Ziff Davis Network, ზიფ დევისის ქსელი

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

BTC - Bitcoin, ბიტკოინი (ციფრული ვალუტის ერთეული)

ICA - Iran’s Cyber Army, ირანის კიბერ არმია

Yandex - Yet Another Indexer, კიდევ ერთი ინდექსერი

ID - Identity Document, პირადობის დამადასტურებელი დოკუმენტი

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

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

HMR - Hammersmith Medical Research Clinic, ჰამერსმიტის სამედიცინო კვლევების კლინიკა

GHC - GEORGIAN HACKERS COMMUNITY, საქართველოს ჰაკერების საზოგადოება

რედაქტორისაგან

თორნიკე ზედელაშვილის მონოგრაფიის თემაა - „ციფრული ტექნოლოგიების საუკუნე და კიბერუსაფრთხოების თანამედროვე საერთაშორისო პოლიტიკური გამოწვევები“, რომელიც ძალიან აქტუალური და ინოვაციური საკითხია არა მარტო საქართველოსთვის, საერთაშორისო საზოგადოებისთვისაც. საკვლევი თემა განხილულია კიბერუსაფრთხოებისა და კიბერომის თეორიის მიხედვით, გაანალიზებულია მისი გეოპოლიტიკური მნიშვნელობა, ნაჩვენებია, თუ როგორ ხორციელდება აღნიშნული მოდელი რეალურ ცხოვრებაში, კონკრეტული აქტორების მაგალითებზე (ევროკავშირი, ირანის ისლამური რესპუბლიკა, ჯიჰადისტური ორიენტაციის ტერორისტული ჯგუფები და ა.შ.), რომლის საშუალებითაც ნათლად წარმოჩინდება არასახელმწიფოებრივ და სახელმწიფოებრივ აქტორებს შორის კიბერუსაფრთხოების კუთხით დაპირისპირების და კონკურენციის საკითხი.

ბოლო დროინდელი კონფლიქტების ანალიზი გვიჩვენებს, რომ კიბერუსაფრთხოება ყველა ომისა თუ კონფლიქტის განუყოფელი ნაწილია. აღნიშნული თემა თავის მხრივ დაკავშირებულია ინფორმაციული ტიპის კონფლიქტებთან, რომელიც სწორედ კიბერევშეტევის მიზეზით შეიძლება იყოს გამოწვეული და ახალი კონფლიქტის კერა წარმოშვას ან არსებულის ესკალაცია გამოიწვიოს.

მონოგრაფიაში განხილულია კიბერუსაფრთხოებისა და საინფორმაციო უსაფრთხოების არსი, მისი განმსაზღვრელი ფაქტორები, საინფორმაციო უსაფრთხოების ფენომენი, რუსეთ-საქართველოს ომის მაგალითი, რეალური კიბერშეტევები. საუბარია იმაზე, თუ რა როლი უჭირავს კიბერუსაფრთხოებას დღევანდელ გეოპოლიტიკურ სივრცეში, რამდენად გადამწყვეტ მოვლენას წარმოადგენს სახელმწი-

ფოებისთვის. კიბერუსაფრთხოება მიზნად ისახავს ორგანიზაციის უსაფრთხოების მიღწევას და მისი შენარჩუნების უზრუნველყოფას. ასევე, მომხმარებლების აქტივობების შესაბამის დაცვას რისკებისგან.

კიბერუსაფრთხოება გლობალური ინტერესების საგნად იქცა. სახარო სამსახურები დღითი-დღე სულ უფრო მეტად ხდებიან დამოკიდებული ტექნოლოგიების საშუალებით ინფორმაციისა და კომუნიკაციის გამოყენებაზე (ICT-Information and communications technology). რაც უფრო დამოკიდებულნი ვხდებით ICT-ზე, მით ღრმაა კავშირი კიბერუსაფრთხოებასთან. ამ მიზეზებიდან გამომდინარე, კიბერუსაფრთხოება წარმოადგენს თანამედროვე სამყაროს ნამდვილ გამოწვევას, რომელთან გამკლავებაც მხოლოდ სამართალმცოდნეების, უსაფრთხოების ექსპერტებისა და საზოგადოების აქტიური მონაწილეობით არის შესაძლებელი.

ბატონ ზედელაშვილის ფუნდამენტური კვლევა ნათლად დაგვანახებს, თუ რა მოხდა 2008 წელს, როცა რუსეთმა არაერთხელ მოაწყო მასშტაბური კიბერთავდასხმა საქართველოს წინააღმდეგ, როგორ ხორციელდებოდა კიბერომი ევროკავშირის წინააღმდეგ და რა პრინციპებზე ხორციელდება კიბერჯიჰადიზმის სტრატეგია.

იქიდან გამომდინარე, რომ კიბერუსაფრთხოების როლი უმნიშვნელოვანესია კონფლიქტებში და გადამწყვეტი როლიც კი უკავია რიგ შემთხვევებში, აუცილებელია ამ ფენომენის სიღრმისეულად შესწავლა.

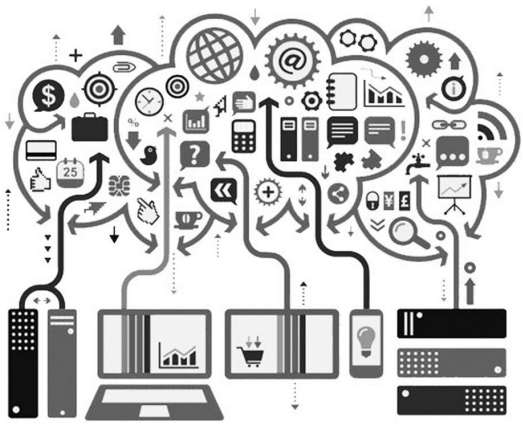
ნაშრომი საშუალებას გვაძლევს, დავინახოთ კიბერუსაფრთხოების დადებითი და უარყოფითი მხარეები. ასევე დავინახავთ იმასაც, თუ რამდენად გახდა იგი საერთაშორისო უსაფრთხოების განმსაზღვრელი ფაქტორი და შეცვალა თუ არა მან ბოლო ათწლეულის განმავლობაში მსოფლიო.

ვახტანგ მაისაია,
პოლიტიკის მეცნიერების დოქტორი, კავკასიის
საერთაშორისო უნივერსიტეტის პროფესორი

ავტორისაგან

ინტერნეტი და ტექნოლოგიური მიღწევები. კიბერომისგან, კიბერშეტევებისგან მომდინარე საფრთხეები, სხვადასხვა ქვეყნების თავდაცვითი კიბერშესაძლებლობები, ვირუსები, მავნე პროგრამები და ჰაკერული თავდასხმები, საინფორმაციო ომი, პორპაგანდა, დეზინფორმაცია, ფეიკ-ნიუსი, უსაფრთხოების კონცეფციები და არსებული გამოწვევები. ეს არის წიგნის ძირითადი არსი და საფუძველი. გაანალიზებულია გლობალური უსაფრთხოება, ამერიკის შეერთებული შტატების, დასავლეთ ევროპის, აღმოსავლეთ ევროპის, ევროკავშირისა და ნატოს როლი. საქართველოს გეოსტრატეგიული მდგომარეობა, უსაფრთხოება და რუსეთის მიერ განხორციელებული კიბერთავდასხმები. კვლევის საფუძველზე ნაშრომში გამიჯნული და განმარტებულია სხვადასხვა ტერმინები, ყურადღება ეთმობა ირანის ისლამური რესპუბლიკის, ჩინეთისა და რუსეთის მიერ წარმოებულ ჰიბრიდულ ომებს, ჰაკერულ თავდასხმებს, საინფორმაციო ომის წარმოებას, არასახელმწიფო აქტორებს, ტერორისტებს, რომლებიც სწრაფად ითვისებენ და იყენებენ ახალ ტექნოლოგიებს. პანდემია, კრიზისი, უამრავი საფრთხე როგორც რეალურ, ასევე ირეალურ სამყაროში, კიბერსივრცეში. ნაშრომში განხილულია სტანდარტები და მექანიზმები, თუ როგორ უნდა იფუნქციონირონ სახელმწიფო უწყებებმა, საერთაშორისო თუ ადგილობრივმა ორგანიზაციებმა, რათა ნაკლები ზარალი მიიღონ კიბერთავდასხმებისგან. განხილულია ევროკავშირისა და ნატოს კიბერუსაფრთხოების პოლიტიკა და სტანდარტები. ასევე საუბარია უკრაინა-საქართველოს კიბერუსაფრთხოების გარემოსა და პოლიტიკაზე.

შესავალი



თითოეული მოქალაქის სოციალური და ეკონომიკური კეთილდღეობა, ჯანმრთელობა და სიცოცხლე მნიშვნელოვნად არის დამოკიდებული ინფორმაციული სისტემებისა და ელექტრონული მომსახურების უსაფრთხოების უზრუნველყოფაზე. კიბერშეტევები დიდ გავლენას ახდენს ეკონომიკის ყველა სექტორზე, აფერხებს ფინანსური სივრცეების ფუნქციონირებას, ამცირებს ელექტრონული სერვისების მიმართ საზოგადოების ნდობას და საფრთხეს უქმნის ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების გამოყენებით ეკონომიკის განვითარებას. გლობალური მასშტაბით კიბერსაფრთხეების ფონზე, როდესაც ყოველდღიურ რეჟიმში ხორციელდება ასეულობით შეტევა - ხორციელდება კიბერჯაშუშობა, კიბერტერორიზმი, ვრცელდება დეზინფორმაცია, ახალი თავდაცვითი მექანიზმების შემუშავება, დანერგვა და განვითარება მნიშვნელოვან საკითხს წარმოადგენს. ამ მიმართულებით მნიშვნელოვანი როლი ენიჭება ჩრდილო-ატლანტიკურ ალიანსს ევროკავშირთან ერთად და წარმოადგენს

უსაფრთხოების ერთგვარ ქოლგას, როგორც წევრი, ასევე პარტნიორი ქვეყნებისთვის.

21-ე საუკუნეში ყველაზე საშიშ მოვლენად იქცა კიბერსივრცეში მიმდინარე მოვლენები - ყოველდღიურად ზარალდება უამრავი ადამიანი, კერძო კომპანია და სახელმწიფო დაწესებულება. თავდაცვის მიზნით უკვე იხარჯება მილიარდობით დოლარი. ნატოს ყველა კონცეფციასა თუ დოქტრინაში ხაზგასმითაა აღნიშნული, რომ ძირითადი პრინციპებიდან გამომდინარე, მისი არც ერთი წევრი ქვეყანა არ უნდა იყოს იძულებული, დაეყრდნოს მხოლოდ საკუთარ ძალებს. ალიანსის სტრატეგია საშუალებას აძლევს თითოეულ სახელმწიფოს, კოლექტიური მეთოდებით მოახდინონ ეროვნული უსაფრთხოების მიზნების რეალიზება.

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

მიუხედავად იმისა, რომ საქართველო ამ ეტაპზე არ იმყოფება მოწინავე პოზიციაზე (ამას ადასტურებს არაერთი კვლევა), არსებობს თავდაცვის ეფექტური სისტემა - ფუნქციონირებს **კიბერუსაფრთხოების ბიურო** და ციფრული მმართველობის სააგენტო. როგორც საქართველოს **ეროვნული უსაფრთხოების სტრატეგიაშია** აღნიშნული, საქართველოს მიზანია, გახდეს კიბერუსაფრთხოების სერვისების რეგიონული პროვაიდერი და განავითაროს საკუთარ ტერიტორიაზე განლაგებული სხვა ქვეყნების საკომუნიკაციო სისტემების მუშაობისთვის საჭირო ინფრასტრუქტურა. ამის გაკეთება შეუძლებელია პარტნიორების დახმარების გარეშე. საქართველოს **უსაფრთხოების სამსახურის ანგარიშებში** ნათქვამია, რომ ჩვენი ქვეყნისთვის მნიშვნელოვან რისკს წარმოადგენენ უცხო ქვეყნების სპეცსამსახურების

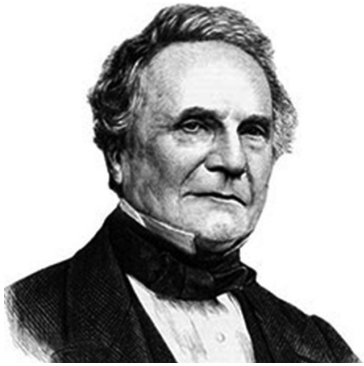
მიერ კონტროლირებადი ჰაკერული დაჯგუფებები, სამთავრობო ინფრასტრუქტურაზე კიბერშეტევებისა და კიბერსადაზვერვო ოპერაციების განხორციელება.

საფრთხეების თავიდან აცილება შეუძლებელია თანამედროვე ტექნოლოგიების, პროფესიონალი კადრებისა და წამყვან სახელმწიფოებთან თანამშრომლობის გარეშე. შესაბამისად, ერთადერთ გზას წარმოადგენს საერთაშორისო თანამშრომლობა. საქართველოსთვის, უსაფრთხოების თვალსაზრისით, გასაძლიერებელია ნატოსთან და წამყვანი სახელმწიფოების უსაფრთხოების სამსახურებთან თანამშრომლობა, რათა დროულად მოხერხდეს პრევენციული ზომების გატარება. ასევე საჭიროა უფრო მჭიდრო თანამშრომლობა მეზობელი სახელმწიფოების უსაფრთხოების სამსახურებთან. ნატო ერთადერთი ორგანიზაციაა, რომელსაც ტექნიკურად, ფინანსურად თუ ადამიანური რესურსების მხრივ შესწევს ძალა, წინააღმდეგობა გაუწიოს კიბერსივრციდან მომდინარე საფრთხეებს. ამიტომ მნიშვნელოვანია დღევანდელი მდგომარეობისა და სამომავლო გეგმების შესწავლა, გაანალიზება, კვლევა, პრაქტიკული კუთხით წარმოჩენა. მკვლევართა მტკიცებით, თუ იქნება სწორი მეცნიერული მიდგომა, კიბერომის შედეგები არ გახდება ისეთი დამანგრეველი, როგორიც იყო წინა წლების განმავლობაში.

თავი პირველი
კიბერუსაფრთხოების არსი და ისტორიული მიმოხილვა

ვითარდება ტექნოლოგიები და რა თქმა უნდა, მატულობს მავნე საქმიანობის საფრთხეც. ეპოქა, რომელშიც ვცხოვრობთ, ტექნოლოგიური რევოლუციების ყოველდღიურ რეჟიმს წარმოადგენს. ახალი ტექნოლოგიებით კი იბადება მძლავრი, უფრო მოქნილი, როგორც თავდაცვითი, ასევე თავდასხმითი მექანიზმები. სამწუხაროდ, უკვე იქამდე მივედით, რომ კიბერშეტევა ყველა სამხედრო ომის თანმდევი გახდა, ომები მიმდინარეობს ჰიბრიდული კომპონენტების გამოყენებით. კიბერომი, როგორც მოვლენა, დაიწყო კომპიუტერისა და ინტერნეტის გამოგონებისთანავე.

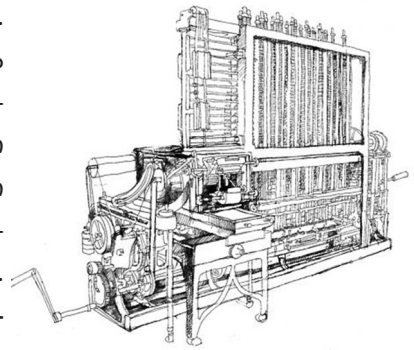
როგორ შეიქმნა კომპიუტერი? ეს არ მომხდარა ხელის ერთი დარტყმით - ამ მოვლენას საფუძვლად უდევს გამოთვლითი ტექნოლოგიების განვითარება. XX საუკუნეში მეცნიერების ეფექტურმა მუშაობამ გამოიწვია ტექნოლოგიური რევოლუცია. მაგალითად, ქაღალდი, ჟურნალი, გაზეთი, წიგნი, კინო, ტელევიზია ისეთი ხელმისაწვდომი გახდა, როგორც არასდროს. ამას მოჰყვა კომპიუტერი და ინტერნეტი. შეიძლება დაუჯერებლად მოგეჩვენოთ, პირველი კომპიუტერი იკავებდა ერთ მოზრდილ ოთახს და მხოლოდ რიცხვების გამოანგარიშება შეეძლო. ეს ის პერიოდია, როცა კალკულატორიც კი არ არსებობს. XX საუკუნის დასაწყისში მეცნიერებმა გამოიგონეს ელექტრონული ლამპა, რომელსაც იყენებდნენ რადიომიმღების სიგნალის გასაძლიერებლად. 1940-იან წლებში გაჩნდა იდეა, რომ ელექტრონული ლამპები გამოეყენებინათ კომპიუტერებშიც. მეორე მსოფლიო ომის პერიოდში მეცნიერები ცდილობდნენ, ინტენსიურად ემუშა-



ჩარლზ ბებიჯი (1791-1871)

ვათ ტექნოლოგიების განვითარებაზე - დადგა საკითხი, შეექმნათ ისეთი მოწყობილობა, რომელიც არა მხოლოდ გამოთვლიდა რიცხვებს, არამედ ამოხსნიდა მათემატიკურ ამოცანასაც. პირველი მცდელობა ჰქონდა კემბრიჯის უნივერსიტეტის პროფესორს **ჩარლზ ბებიჯს** (1791-1871). მცდელობა უშედეგოდ დამთავრდა.

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



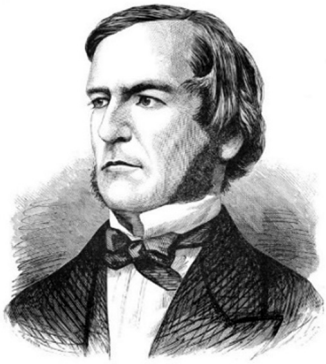
„ანალიტიკური ძრავი'' (1834)

ჯოზეფ მარი ჟაკარტი (1752-1834)

1 Freiberger A. P., Swaine R. M., Analytical Engine, Encyclopedia Britanica, 2020, p 1. https://www.britannica.com

ადა აუგასტა (1815-1852)

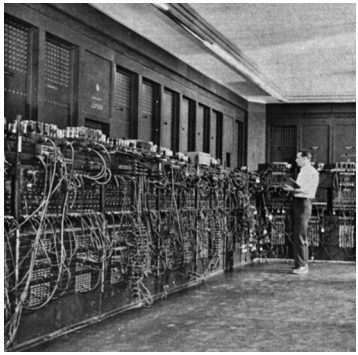
მეცნიერების წინაშე დადგა ახალი ამოცანა - პროგრამირების შექმნა და განვითარება. 1843 წლის 19 ივლისი პირველი პროგრამის შექმნის თარიღად არის აღიარებული. მის შექმნაში დიდი წვლილი მიუძღვის ცნობილი ინგლისელი პოეტის, **ჯორჯ გორდონ ბაირონის** ქალიშვილს - **ადა აუგასტას**, რომელიც გახლდათ **გრად ლავლეისის** მეუღლე. 1843 წლის 19 ივლისს **აუგასტამ** შექმნა პირველი ბერძნული რიცხვების გამოსათვლელი პროგრამა. ამ დროს მანქანას შეეძლო შეესრულებინა არა მხოლოდ არითმეტიკული გამოთვლა, არამედ ლოგიკური ოპერაციებიც. ეს მას შემდეგ გახდა შესაძლებელი, რაც (1847 წელს) ინგლისელმა მათემატიკოსმა **ჯორჯ ბულმა** შექმნა ლოგიკურ გამონათქვამთა თეორია და ეწოდა **„ბულის ალგებრა“**[2]. აქვე აღსანიშნავია, ქართველი მეცნიერის, **გიორგი ნიკოლაძის** წვლილი (1888-1931). ნიკოლაძის გამოგონებამდე რაც კი არითმომეტრები არსებობდა, იყო მექანიკური, საფრანგეთში ყოფნისას მან შეისწავლა არსებული არითმომეტრები და გამოიგონა ახალი ელექტრონული გამომთვლელი, რომელსაც ეწოდა **„პირდაპირი გამრავლების ელექტრონული არითმომეტრი“**. იგი სხვა გამომ-



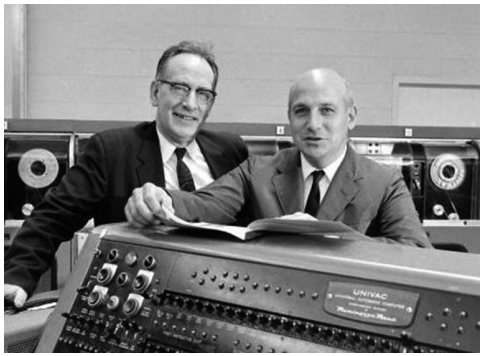
ჯორჯ ბული (1815-1864)

გიორგი ნიკოლაძე (1888-1931)

2 Loritz M. Who was Ada Lovelace? The life of the woman who envisioned the modern day computer, Media Website “EU-Startup”, 2019, p 1. https://www.eu-startups.com

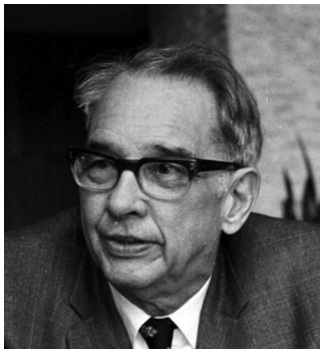


ENIAC – Electronic Numerical Integrator and Computer (1945)



ჯონ მოუჩი და ჯონ ეკრტი (1945 წელი)

თვლელებისაგან განსხვავდებოდა ელექტრონული გამანაწილებლით. ამ გამოგონებით მაშინვე დაინტერესდნენ ამერიკული და ევროპული კომპანიები, თუმცა მან უარი თქვა მათთან თანამშრომლობაზე, გამოემგზავრა სამშობლოში, საქართველოში შექმნა არითმომეტრის მოდელი, რომელიც შემდეგ გაიგზავნა გამოფენაზე მოსკოვში. სამწუხაროდ, **გიორგი ნიკოლაძეს** არ დასცალდა, დაეზუსტებინა არითმომეტრის სრული კონსტრუქციის დოკუმენტაცია, 1931 წელს მოულოდნელად გარდაიცვალა[3]. დიდი ხნის განმავლობაში აღიარებული იყო, რომ პირველი კომპიუტერი შეიქმნა 1945 წელს, ამერიკელი ფიზიკოსების - **ჯონ ეკრტის** და **ჯონ მოუჩის** მიერ, რომლის სახელწოდებაც იყო **„ენიაკი“ (ENIAC – Electronic Numerical Integrator and Computer)**. თუმცა ეს ისტორია მცდარი აღმოჩნდა. მართალია, **„ენიაკი“** მსოფლიოში პირველი კომპიუტერია, რომლის კონსტრუქტორებიც **ეკერტი** და **მოუჩი** არიან, დიდი წვლილი მიუძღვით გამოთვლითი ტექნიკის განვითარებაში, მაგრამ პირველი კომპიუტე-



ჯონ ატანასოვი (1903-1995)

3 აბულაშვილი ი. “პირველი ელექტროგამომთვლელი მანქანის გამომგონებელი ქართველი”, გაზეთი „რეზონანსი“, 2017, გვ. 1. http://www.resonancedaily.com

რის მუშაობის პრინციპები მათ არ მოუფიქრებიათ. ეს პრინციპები ჩამოყალიბდა 1937 წელს და პირველი კომპიუტერის შექმნის მცდელობაც იყო აიოვას შტატის ქალაქ ეიმსში მომუშავე ბულგარელი ფიზიკოსის **ჯონ ატანასოვის** და მისი დამხმარის, **კლიფორდ ბეტისის** მიერ, რომელსაც უწოდეს **„ABC"**, მისი შექმნა 1942 წელს დამთავრდა. ამ დროს მხოლოდ დარჩენილი იყო პერიფერიული ნაწილის აწყობა. თუმცა II მსოფლიო ომის გამო ექსპულატაციაში ვერ ჩაეშვა. 1973 წელს დაიწყო დავა ორი დიდ კომპანიას შორის, პირველი კომპიუტერის აწყობის საავტორო უფლებების თაობაზე. გაიმართა 135 სასამართლო სხდომა. საბოლოოდ დამტკიცდა, რომ 1940 წელს **ატანასოვს** მიუწვევია **მოუჩი**, მისთვის უჩვენებია ხელნაწერები, განუმარტავს და აუხსნია გამოთვლითი მოწყობილობის მუშაობის პრინციპები. შემდეგ კი **მოუჩიმ** შეძლო, შეექმნა ის, რასაც პირველი კომპიუტერი ეწოდა. თუმცა დადასტურებულად შეგვიძლია ვთქვათ, რომ პირველი კომპიუტერის შემქმნელი **ატანასოვია**[4]. კომპიუტერი - ეს არის პროგრამის მიხედვით ავტომატურად მართვადი სწრაფი მოქმედების სისტემა. ელექტრონული მანქანა, რომლის ძირითადი დანიშნულებაა დიდი მოცულობის ინფორმაციის შენახვა, დამუშავება და გადაცემა. დღეს ეს ყველაფერი უფრო მრავალფეროვნად გვეჩვენება, მაგრამ კომპიუტერს ძირითადი ფუნქციები არ შეუცვლია. გადის წლები, მატულობს კომპიუტერების რაოდენობა და იხვეწება. ტექნოლოგიური მიღწევების წყალობით შესაძლებლობები ყველა ტექნიკურ სისტემაში გაიზარდა - მობილურ ტელეფონებში, ავტომობილებში, სხვადასხვა საოჯახო თუ სამეწარმეო დანადგარებში.

კლიფორდ ბეტსი (1918-1963)

4 Levy S. The Brief History of the ENIAC Computer, Smithsonian Magazine, 2013, p 1. https://www.smithsonianmag.com

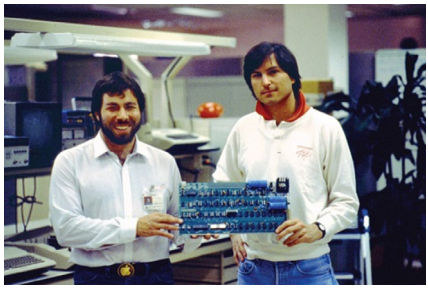
კომპიუტერი ,,ალტაირი" (1975)

1974 წელს შეიქმნა პირველი პერსონალური მიკროკომპიუტერი **„Altair”**. მისი მწარმოებელი იყო, **ედ რობერტსონის** დაარსებული კომპანია **MITS**. მიკროკომპიუტერი **„Altair”** წარმოადგენდა ასაწყობ კომპლექტს, არ ჰქონდა კლავიატურა და მონიტორი. მონაცემების შეყვანა ხორციელდებოდა წინა პანელზე მოთავსებული გადამრთველების საშუალებით. ამ კომპიუტერის ინტერპრეტატორი ბეისიქი შექმნა **ბილ გეიტსის** მიერ დაარსებულმა კომპანია **„Microsoft”**-მა. 1977 წელს გამოვიდა კიდევ

ედ რობერტსონი (1941-2010)

რამდენიმე პერსონალური კომპიუტერი - **Tandy, Commodore, Apple II**.

ამათგან გამოსარჩევია **Apple**, რომელიც შექმნა ორმა ახალგაზრდა მეგობარმა - **სტივ ჯობსმა** და **სტივ ვოზნეაკმა**. კომპიუტერის შექმნამდე (1976 წელს) მათ დაარსეს კომპანია **Apple Computer**, რომლის სამუშაო ოფისადაც გამოიყენეს ჯობსის მშობლების ბინის ერთ-ერთი საძინებელი ოთახი.



სტივ ჯობსი და სტივ ვოზნეაკი (1976 წელი)

მათი შექმნილი კომპიუტერი გამოირჩეოდა კარგი დიზაინით და საიმედოობით. ეს იყო პირველი ფერადი გრაფიკით. ამ მოდელის შექმნა იმდენად წარმატებული აღმოჩნდა, 1980 წელს **Apple Computer**-ის შემოსავალმა

კომპიუტერი Apple II plus

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

ალან ტიურინგი (1912-1954)

კომპიუტერი იყოფა თაობებად:

პირველი თაობა - კომპიუტერები აწყობილი იყო ლამპებით, ასევე ელექტრონულ-სხივური მილაკებით. ასეთმა მანქანებმა იარსება 1950-1957 წლებში. „ენიაკი“ იწონიდა 27 ტონას, იგი შედგებოდა 18000 ლამპისგან, იკავებდა 200 კვადრატულ მეტრ ფართობს. კომპიუტერის სამუშაოდ საჭირო იყო უამრავი პროგრამისტი და ინჟინერი. მუშაობის სიმძლავრე წამში 10-15 ათასი არითმეტიკული ოპერაციის შესრულება იყო, რაც დღევანდელ კომპიუტერთან შედარებით ძალიან მცირეა. მეხსიერება მაგნიტურ დონეზე იყო წარმოდგენილი. ეს ფაქტობრივად გახლდათ ექსპერიმენტული მოწყობილობები და იქმნებოდა სხვადასხვა თეორიული მოსაზრებების შესამოწმებლად. მნიშვნელოვანია ის ფაქტი, რომ **„ენიაკის“** პარალელურად, **დიდ ბრიტანეთში**

მაქს ნიუმენი (1897-1984)

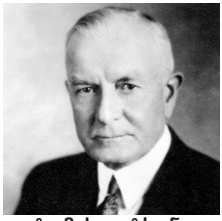
ტომი ფლაუერი (1905-1998)

5 Levy S. Steve Jobs American businessman, Encyclopedia Britanica, 2020, p 1. https://www.britannica.com

საიდუმლოდ იწარმოებოდა კომპიუტერი **IBM**, რომელსაც შეეძლო კოდების გაშიფრვა.


ჰოვარდ ეიკენი (1900-1973)

ამის გამო იყო გასაიდუმლოებული. უკვე ცნობილი ფაქტია, მას იყენებდნენ გერმანიაში პირველი და მეორე მსოფლიო ომების დროს. კოდების გაშიფრვის მათემატიკური მეთოდი შექმნილი იყო პროფესიონალ მათემატიკოსთა ჯგუფის მიერ, რომელშიც შედიოდა **ალან ტიურინგი**. 1943 წელს ლონდონში **მ. ნიუმენმა** და **ტ. ფლაუერიმ** გამოიგონეს მანქანა **„Colossus“**, რომელიც შედგებოდა 1500 ელექტრონული ლამპისგან. 1937 წელს მათემატიკოსმა **ჰოვარდ**


ტომას ვოტსონი
(1874-1956)


mark 1
(1939)

კომპიუტერი
IBM (1939)

ეიკენმა შეიმუშავა დიდი გამომთვლელი მანქანის შექმნის პროექტი. ამ საქმეში 500 ათასი დოლარი ჩადო **IBM**-ის პრეზიდენტმა **ტომას ვატსონმა**. ამით დაიწყო **Mark-1**-ის დაპროექტება. პროდუქცია 1939 წელს **IBM**-ის სახელით გამოვიდა.


Ferrant Pegasus Computer
(1955)

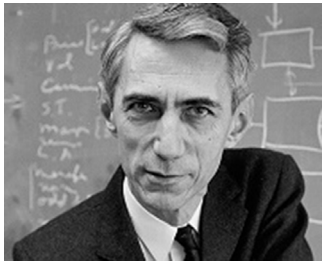
1955 წელს ფირმა **Ferrant**-მა გამოუშვა კომპიუტერი **Pegasus**, ამ კომპიუტერში გამოიყენეს საერთო დანიშნულების რეგისტრების კონცეფცია. შემდგომში კომპიუტერისთვის აშშ-ის საზღვაო ფლოტის ოფიცერმა (ადმირალმა), პროგრამისტმა, **გრეის ხოპერმა** შექმა პირველი კომპილატორი - პროგრამა, რომელიც ადამიანისთვის გასაგებ ენაზე დაწერილ პროგრამას თარგმნიდა მანქანის ენაზე. ამან

საგრძნობლად გააადვილა პროგრამირების პროცესი. ისტორიულად, პირველი კომპიუტერის ფუძემდებლებად ითვლებიან, ინფორმაციის თეორიის შემქმნელი - **კლოდ შენონი**, პროგრამირების და ალგორითმების თეორიის შემქმნელი, მათემატიკოსი - ალან ტიურინგი და გამომთვლელი მოწყობილობების კონსტრუქციის ავტორი - **ჯონ ფონ ნეიმანი**. **პირველი თაობის კომპიუტერებია**: „ENIAC“, „Ural-2“, „Strela“, M-20 და ა.შ.


გრეის ხოპერი (1906-1992)

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


ჯონ ფონ ნეიმანი (1903-1957)

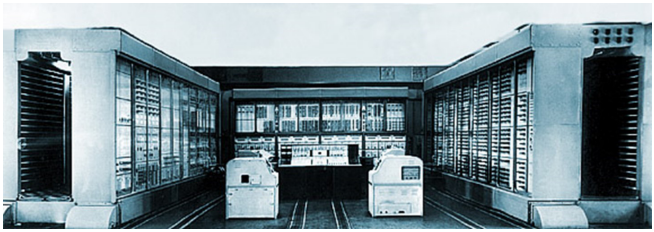

კლოდ შენონი (1916-2001)

მეორე თაობის კომპიუტერებია:

ENIAC

Ural-2

M-20



Strela

M-220

M-220, BESM-4, URAL-14, MINSK-2, MINSK-4 და ა.შ.

მესამე თაობა - 1964 წელს ფირმა IBM-მა ექვსმოდულიანი მოწყობილობა წარადგინა. კომპიუტერები ერთმანეთს უკავშირდებოდნენ ოპერატიული სისტემით და ჰქონდათ ბრძანების ერთიანი სისტემა. 1957 წელს **რობერტ ნოისმა**, რომელმაც შემდეგ ფირმა **Intel** დაარსა, გამოიგონა სრულყოფილი მეთოდი, რომლის საშუალებით ერთ ფირფიტაზე თავსდებოდა რამდენიმე ათეული ტანზისტორი და ყველა შემაერთებელი საშუალება. ამ სქემას ეწოდა **„ჩიპი“**. 1968 წელს პირველი ჩიპიანი კომპიუტერი გამოვიდა, 1970

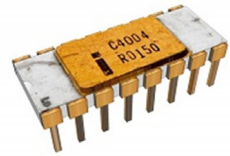
BESM-4

URAL-14

MINSK-2

MINSK-4

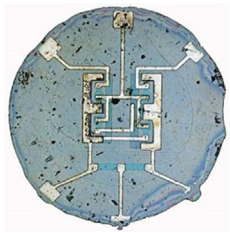
რობერტ ნოისი
(1927-1990)



Intel-4004

წელს კი **Intel**-მა ჩიპის გაყიდვა დაიწყო. **Intel**-მა ამავე წელს დაიწყო ცენტრალური პროცესორის აწყობა ანალოგიური ჩიპით. ეს იყო პირველი მიკრო-პროცესორის გაჩენის პერიოდი - **Intel-4004**. ჩიპების გამოყენებამ მესამე თაობის კომპიუტერების მოქმედების სისწრაფე საგრძნობლად გაზარდა, რაც გულისხმობდა 80-100 ათას არითმეტიკულ ოპერაციას წამში. ამავე პერიოდში შეიქმნა დისკი, ანუ დისკური ტიპის მეხსიერება და ინფორმაციის შემტან-გამომტანი მოწყობილობა, რომელსაც უწოდეს **„დისფლეი“**. დისკი, ანუ გარე მეხსიერება განკუთვნილია იმ ინფორმაციის დასამახსოვრებლად, რომელიც შეიძლება მრავალჯერ იქნას გამოყენებული. სწორედ ამ წლებში **IBM**-მა დაიწყო კომპიუტერების გამოშვება, როგორც პატარა, ასევე დიდი და იმ დროისთვის ყველაზე მძლავრი, ძვირადღირებული კომპიუტერებისა.

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



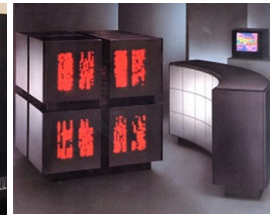
პირველი „ჩიპი"

მეოთხე თაობა - 1975-1985 წლებში გამოშვე-


EC-1022


EC-1035


CM-2


CM-4

ბული კომპიუტერები ეკუთვნის მეოთხე თაობას. არსებობს სხვა მოსაზრებებიც, რადგან იმ პერიოდისთვის კომპიუტერის განვითარების დონე არც ისე მაღალი იყო. მნიშვნელოვანი მაინც ის არის, რომ 1980-იანი წლების დასაწყისიდან, პერსონალური კომპიუტერების გამოჩენის წყალობით, კომპიუტერული ტექნიკა საზოგადოებისთვის ხელმისაწვდომი გახდა.


EC-1055

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

ინტერნეტის შექმნა

1957 წელს საბჭოთა კავშირმა შექმნა ხელოვნური თანამგზავრი, რომელიც დედამიწის ორბიტაზე გაუშვა. ეს ფაქტი შეერთებული შტატების თავდაცვის უწყებამ მიიჩნია საბჭოთა კავშირის ტექნოლოგიური მიღწევების მაღალ ნიშნულად. იფიქრეს, ფართომასშტაბიანი ომის შემთხვევაში ამერიკელებს ინფორმაციის გადაცემის საიმედო სისტემა დასჭირდებოდათ. სხვა არსებული სისტემების ერთ-ერთი

6 Burns D. The five generations of computers, Business to Business Company, 2016, p 1. https://btob.co.nz

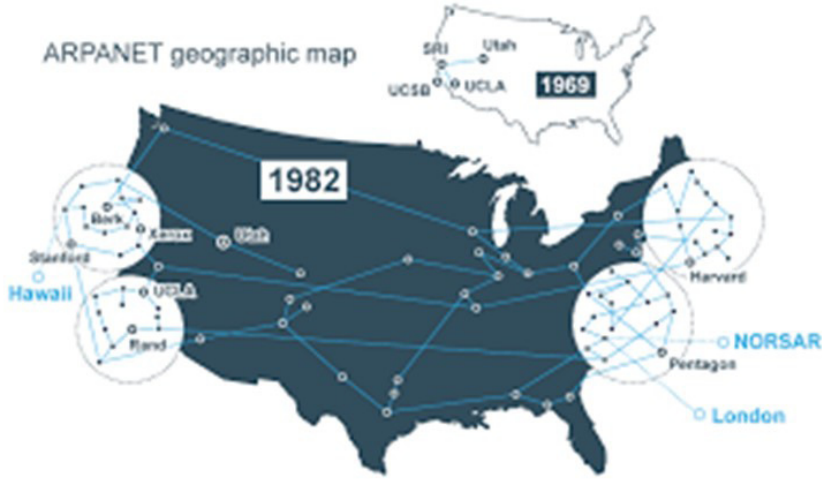
ნაკლი იყო სამართავი ცენტრი, ადგილი, რომლის გათიშვის შემთხვევაში მთელი სისტემა გამოვიდოდა მწყობრიდან. ამიტომ საჭირო იყო ისეთი ქსელის შექმნა, რომელსაც არ ექნებოდა მართვის ერთიანი ცენტრი და რომელიმე სეგმენტის გათიშვის დროს სისტემა შეუფერხებლად იმუშავებდა. ამ მიზანს ისახავდა მოწინავე პროექტების კვლევის სააგენტოს დაარსება - **Advanced Research Projects Agency**, იგი ცნობილია როგორც **ARPA**. ეს იყო ადგილი, სადაც შეიმუშავეს ინტერნეტის საწყისი კონცეფცია. ინტერნეტის შექმნის იდეა ამერიკელ სამხედროებს ეკუთვნით, ხოლო იდეის განხორციელება ამერიკულმა უნივერსიტეტებმა შეძლეს. ამის შემდეგ შეიქმნა ინტერნეტის შემდეგი ვერსია - **ARPANET**[7].

პირველი ინტერნეტკავშირი

1969 წლის 29 ოქტომბერს **ARPANET**-ში ჩართულ ორ კომპიუტერს შორის პირველი კავშირი შედგა. ისინი ერთმანეთს 640 კილომეტრით დააშორეს. პირველი კომპიუტერი სტენფორდის კვლევათა ინსტიტუტში, ხოლო მეორე კალიფორნიის უნივერსიტეტში, ქალაქ ლოსანჯელესში მდებარეობდა. სტენფორდის კვლევითი ინსტიტუტის კომპიუტერთან დაკავშირებას და მონაცემების გადაგზავნას ჩარლი კლაინი ცდილობდა, ხოლო მონაცემების გადაგზავნის პროცესს სტენფორდში ბილ დიუვალი ადევნებდა თვალ-ყურს. პირველი ჩართვისას მხოლოდ სამი სიმბოლოს გაგზავნა მოხერხდა, სიმბოლო იყო-**LOG**, მთლიანი გადასაგზავნი სიტყვა **LOGON**, ანუ სისტემაში შესვლის ბრძანება, თუმცა ქსელი გაითიშა, მისი აღდგენა კი მხოლოდ საათნახევრის შემდეგ მოხერხდა. მომდევნო ცდა წარმატებული გა-

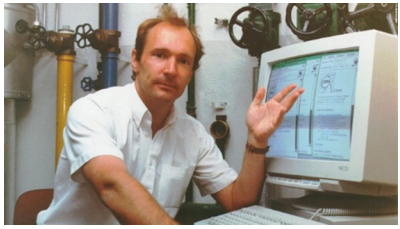
7 Andrews E. The Invention of the Internet, Internet publisher History, 2019, p 1. https://www.history.com

მოდგა. ამას მოყვა აშშ-ის მსგავსად ევროპის სხვადასხვა ქვეყნებში ინტერნეტის ქსელების განვითარება. ამ საქმეში 1973 წელს ტრანსატლანტიკური კაბელის საშუალებით პირველი არაამერიკული ორგანიზაციები, დიდი ბრიტანეთი და ნორვეგია ჩაერთვნენ, რითაც ქსელი საერთაშორისო გახდა. 1983 წელს არსებულ გლობალურ ქსელს „ინტერნეტი“ უწოდეს და მის დიდ ნაწილს **ARPANET**-ი წარმო-



ადგენდა. თავიდან ინტერეტით მხოლოდ ინფორმაციის გაგზავნა და მიღება იყო შესაძლებელი. ეს, რა თქმა უნდა, წინ გადადგმული ნაბიჯი გამოდგა. მანამდე დიდი მოცულობის ინფორმაციის გადაგზავნა და მიღება მხოლოდ ფაქსის მეშვეობით იყო შესაძლებელი. ფაქსით მრავალგვერდიანი ტექსიტს გაგზავნა და მიღება ბევრ სირთულესთან არის დაკავშირებული. ინტერნეტით ეს იოლად ხერხდება. ასევე, ინტერნეტით შესაძლებელია ერთი დოკუმენტის ერთდროულად რამდენიმე ადგილას გადაგზავნა, ფაქსით ეს გამორიცხულია. პირვანდელი ინტერნეტი დღევანდელი ინტერნეტისგან ძალიან განსხვავდება, იმ დროისთვის ადამიანები მხოლოდ ინფორმაციას უცვლიდნენ ერთმანეთს[8].

8 Weber M. october 29, 1969: Happy 40TH Birthday to a Radical Idea!, Computer



ტიმ ბერნერს ლი (1955)

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

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

History Museum, 2009, p 1. https://computerhistory.org

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

Dialup access

საერთაშორისო კოსმოსური სადგურიდანაც გახდა შესაძლებელი[10]. ეს გახლავთ მცირე ისტორია იმ პროცესების შესახებ, რასაც ტექნოლოგიური რევოლუცია ჰქვია და რამაც მიგვიყვანა, როგორც ბევრ სიკეთემდე, ასევე ბევრ საფრთხის შემცველ მოვლენამდე - მასობრივი სოციალური ქსელების განვითარება, მავნე ვებ-გვერდების შექმნა, ვირუსებისა და მასოვრივი თაღლითობის უწყვეტი რეჟიმი, კიბერტერორიზმი, კიბერდანაშაული, კიბეროში.

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

კიბერდელიკი (Cyberdelic) - ეხება ხელოვნებას, გაჯანსაღებას ან იმპრესიულ გამოცდილებას, რომელიც ინტერნეტის აქტიური მოხმარების ხარჯზე ხორციელდება.

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

რიჩარდ სკრენტა (1967)

კიბორგი (Cyborg) - ტექნიკურად გულისხმობს კიბერნეტიკისა და ორგანიზმის შერწყმას. ეს ეხება, რაც შედგება რობოტული ნაწილებისგან.

კიბრაული (Cybrarian) - კიბერბიბლიოთეკარი, უფრო მოკლედ - კიბრალეული, არის მკვლევარი, რომელიც ინფორმაციისთვის ძირითადად ინტერნეტს იყენებს.

კიბერნავტები (Cybernauts) - კიბერნაუტი არის ადამიანი, რომელიც ქმნის სენსორული და ვირტუალური რეალობის მოწყობილობებს. კიბერდანაშაული, კიბეროომი, კიბერტერორიზმი, კიბერშეტევები და მსგავსი მოვლენები დღევანდელი ყოფის თანმდევია[11].

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

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

12 Deffere S. 1st computer virus is written, January 30, 1982, Electronics Design Network, 2019, p 1. https://www.edn.com

საძიებო სისტემა Blekko

უმრავლესობას კომპიუტერი ექნებოდა. პირველი ჰაკერული თავდასხმა 1971 წელს განხორციელდა და სრულიად უწყინარი იყო - ექსპერიმენტს უფრო წარმოადგენდა, ვიდრე დამაზიანებელ კიბერშეტევას. **რობერტ (ბობ) თომასი** თავისი შექმნილი პროგრამით ისტორიაში შევიდა, რომელიც მიჩნეულია როგორც „კომპიუტერული ჭია“. იგი საერთოდ არ იყო მავნე და ყველა ინფიცირებულ ეკრანზე აჩვენებდა შეტყობინებას: „მე ვარ მცოცავი, დამიჭირე, თუ შეგიძლია“[13].

რობერტ (ბობ) თომასი (1945-2014)

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

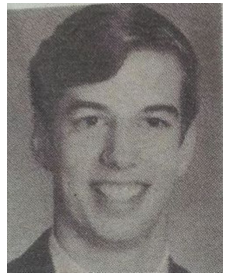
ამავე წელს ისტორიაში ,,საშინელი'' დღე აღინიშნა - **ჯოსეფ პოპმა** შექმნა პირველი **გამოსასყიდი შეტევა**. მან გამოიყენა მავნე პროგრამა სახელწოდებით - **AIDS Trojan**, რომელიც გადაიგზავნა მისი ელფოსტის მეშვეობით. **პოპი** იმედოვნებდა, რომ ამ

13 Uhde A. A short history of computer viruses, Sentrian Pty Ltd, 2017, p 1. https://www.sentrian.com.au

14 Long T. “July 26, 1989: First Indictment Under Computer Fraud Act”, Media News Company - Wired, 2011, p 1. https://www.wired.com


რობერტ მორისი (1965)

პროგრამით ხალხს გამოსძალავდა ფულს[15]. რაც შეეხება ყველაზე დიდ კიბერშეტევას, იგი 1982 წელს, როდესაც ჯერ კიდევ **ცივი ომის** პერიოდი იყო, მაშინ განხორციელდა, **აშშ-ის ცენტრალურმა სადაზვერვო სააგენტომ** როგორღაც იპოვა გზა ციმბირის (რუსეთი) გაზსადენის მუშაობის ჩაშლისთვის - ბომბების, რაკეტებისა და სხვა ასაფეთქებელი მოწყობილობების გარეშე. ამერიკის ცენტრალურმა სადაზვერვო სამსახურმა გაზსადენის აფეთქება გამოიწვია კომპიუტერული სისტემის კოდის გამოყენებით. აფეთქება ისეთი მასშტაბის იყო, კოსმოსიდანაც ჩანდა[16].


ჯოსედ პოპი (1950-2006)

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

რა ვითარებაა დღეს და რა პრობლემების წინაშე დააყენა მსოფლიო ტექნოლოგიურმა რევოლუციამ? კაცობრიობას თავის დამშვიდების უფლება არ აქვს - ფაქტია, რაც უფრო მეტ სიმაღლეებზე ავა კომპიუტერული მიღწევები, მით მეტი საშიშროება შეიქმნება **კიბერდამნაშავეების** მხრიდან. თემის კვლევისას კიბერომი, როგორც

15 Rubens P. Common Types of Ransomware, Internet Website e Security Planet, 2017, p 1. https://www.esecurityplanet.com

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

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

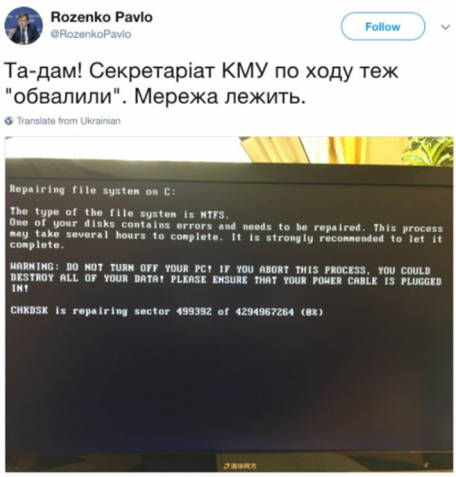
მოვლენა, აუცილებლად უნდა დავყოთ რამდენიმე მიმართულებად: **პირველი** - ტექნოლოგიური მიღწევების ათვისება-გამოყენება; **მეორე** - პროპაგანდისტული მეთოდების დამუშავება-გამოყენება.

კიბერშეტევები ყოველწლიურად იზრდება, აქტიურდება და იხვეწება. ჯერ კიდევ 2006 წელს **რუსეთის ბიზნესქსელმა (RBN)** დაიწყო მავნე პროგრამების გამოყენება პირადობის მოწმობების ქურდობისთვის, 2007 წლიდან **RBN**-ი მთლიანად ,,მონოპოლიზირდა'' ონლაინ ქურდობაში. 2007 წლისთვის მათი ვირუსი სახელწოდებით - **„შტორმი ჭია“**, მუშაობდა დაახლოებით ერთ მილიონ კომპიუტერზე და ყოველდღე გზავნიდა მილიონობით ინფიცირებულ ელ-წერილს. 2008 წელს კიბერშეტევები პერსონალური კომპიუტერიდან სამთავრობო ინსტიტუტების სისტემებზე გადავიდა. 2008 წლის 27 აგვისტოს **NASA**-მ დაადასტურა, რომ საერთაშორისო კოსმოსურ სადგურში ლეპტოპებზე **„შტორმ ჭია“** იყო ნაპოვნი.

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

რუსეთი ახორციელებდა და დღესაც ახორციელებს როგორც საქართველოს, ასევე უკრაინის წინააღმდეგ სამხედრო და კიბერომის შერწყმულ თავდასხმებს, იყენებს ჰიბრიდული ომის სხვადასხვა კომპონენტებს. კრემლს საბჭოთა მეთოდოლოგია არ შეუცვლია, შეცვალა მხოლოდ ტექნოლოგიები. თუ საკითხს განვიხილავთ რუსეთის მიერ ჩადენილი და ჯერ კიდევ «ჩაუდენელ» დანაშაულთა ჭრილში, ალბათ, ყველა აღიარებს, რომ ამ მხრივ საქმე გვაქვს არაპროგნოზირებად სა-

18 Sciarrone M. Cyber Warfare: The New Front, George W. Bush Institute, 2017, p 1. https://www.bushcenter.org



პაველ როზენკოს პოსტი "ტვიტერზე" (2017)

ხელმწიფოსთან. მიუხედავად ამისა, მსოფლიოს წამყვანი ქვეყნები ვალდებულნი არიან, ამ არაპროგნოზირებადი ქვეყნის ქმედება ერთიან სისტემაში მოაქციონ და წინააღმდეგობა გაუწიონ.

ჩვენი მსჯელობა რუსეთთან მიმართებაში უფრო საფუძვლიანი, რომ იყოს, მაგალითად შეგვიძლია მოვიყვანოთ - 2008 წლის რუსეთ-საქართველოს ომი, როდესაც ყველაზე მასშტაბური კიბერშეტევა განხორციელდა რუსეთის მხრიდან საქართველოს სახელმწიფო, სატელევიზიო და საინფორმაციო სააგენტოების ვებ-გვერდებზე. ასეთი მაგალითი 2014 წელს რუსეთ-უკარინის ომთან მიმართებაშიც შეგვიძლია მოვიყვანოთ, სადაც სამხედრო ომს თან სდევდა ჰიბრიდული ომის სხვადასხვა კომპონენტები, ე.წ. ამოუცნობი ტიტუშკების გამოყენება და კიბერშეტევები სამთავრობო უწყებებზე.

რამდენიმე წლის შემდეგ, კერძოდ 2017 წელს, უკრაინის მინისტრთა კაბინეტის შიდა სისტემა ჰაკერების თავდასხმის მსხვერპლი აღმოჩნდა, ამის შესახებ უკრაინის ვიცე-პრემიერმა, **პაველ როზენკომ „ტვიტერზე“** დაწერა და სურათიც გამოაქვეყნა:

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

ამ დროს არა მხოლოდ უკრაინის მინისტრთა კაბინეტი იყო ჰაკერების თავდასხმის ობიექტი, არამედ შეფერხებით მუშაობდა ენერგოკომპანიები და ეროვნული ბანკი. კიბერშეტევის მსხვერპლი იყო

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

მედიაჰოლდინგი **„ლუქსი“**, კიევის მეტროპოლიტენი, უკრაინის ფოსტა, ახალი ფოსტა და სხვა. სამიზნეებს შორის იყო ბორისპოლის აეროპორტის სისტემაც, რის მეშვეობითაც შესაძლებელია ავიარეისების შეყოვნება.

უკრაინა დიდიხანია საცდელ პოლიგონად იქცა რუსეთისთვის, ფაქტობრივად დაწყებულია ევროპაში ერთ-ერთი უდიდესი სახელმწიფოს დაშლა-დანაწევრება. 2022 წლის დასაწყისიდან, თითქმის ორთვიანმა ალყამ და საომარმა მდგომარეობამ მსოფლიოს ბევრი რამ დაანახა. თუმცა რუსეთის სტილი, ხელწერა და მეთოდი არ იცვლება. მას შემდეგ, რაც ვლადიმერ პუტინმა უკრაინის საზღვრებთან 150 ათასი ჯარისკაცი და სამხედრო ტექნიკა განალაგა, არაერთხელ განხორციელდა კიბერთავდასხმა სამთავრობო სტრუქტურების სისტემებზე. მათ შორის ყველაზე მასშტაბური თავდასხმა გახლდათ 16 თებერვალს, როცა დაიბლოკა თითქმის ყველა სტრუქტურის ვებ-საიტი. იყო თუ არა ეს ფაქტი სამხედრო ომის დასაწყისი, ანუ სიგნალი, ამის განსაზღვრა რთულია, მაგრამ რაც საქართველოში მოხდა 2008 წლის აგვისტოში, ამის გათვალისწინებით, ნამდვილად იყო.

რუსეთს აქვს ღია მოთხოვნა: ნატო არ უნდა გაფართოვდეს აღმოსავლეტ ევროპისკენ, ამ ორგანიზაციის წევრები ვერ გახდებიან უკრაინა და საქართველო. ვლადიმერ პუტინის განცხადებით, ამერიკის შეერთებულმა შტატებმა და ჩრდილო ატლანტიკური ალიანსის ხელმძღვანელებმა ჯერ კიდევ 30 წლის წინათ დადეს პირობა, რომ ერთ ნაბიჯსაც არ გადმოადგამდნენ აღმოსავლეთ ევროპისკენ. სინამდვილეში კი რა ხდება? რუსეთს ნელ-ნელა აქცევენ ალყაში. ამ ქვეყანას ყოველთვის აქვს თავისი სამართალი, თავისი მიდგომები, თავისი სპეციფიკა, თავისი პროგრამები, გეგმები და ამოცანები. რაც მთავარია, ამ უკიდეგანო სახელმწიფოდან დაუსრულებლად მოედინება შოვინიზმი და სხვისი ტერიტორიების დაბყრობის სურვილი. გასაგებია, რომ უკრაინელები და რუსები მონათესავე ერები არიან, მაგრამ ეს სულაც არ უშლის ხელს კეთილმეზობლურ ურთიერთობას და დამოუკიდებელი ინტერესებით ცხოვრებას. რუსეთმა კატეგორი-

ულად მოითხოვა, ამერიკის შეერთებულმა შტატებმა და ევროპამ გადახედონ ბრიუსელის სამიტზე მიღებულ გადაწყვეტილებას და უკან წაიღონ აღმოსავლეთ ევროპის მიმართულებით გაფართოების სტრატეგია.

ბრიუსელის სამიტი

ბრიუსელში ნატოს სამიტი 2021 წლის 14 ივნისს გაიმართა. გენერალურმა მდივანმა იენს სტონტელბერგმა ისაუბრა რუსეთის აგრესიულ პოლიტიკაზე. მისი თქმით, ისინი რუსეთის მხრიდან ხედავენ მხოლოდ საფრთხეს მრავალი წლის განმავლობაში: ,,ნატომ გაზარდა თავდაცვითი ხარჯები ბალტიის ქვეყნების აღმოსავლეთ ნაწილში, ევროპაში, კანადასა და ასევე უკრაინაში. ახლა უფრო შესაძლებელია მეტი საჰაერო პატრულირება, საზღვაო ძალების გამოყენება და ასე შემდეგ. **ეს ძალიან მკაცრი გზავნილია რუსეთისთვის, ჩვენ აქ ვართ მოკავშირეების დასაცავად, არა იმისთვის, რომ მოხდეს კონფლიქტის პროვოცირება, არამედ მისი თავიდან აცილება. მშვიდობის შენარჩუნება აუცილებელია, რათა აღარ განმეორდეს ის, რაც უკრაინისა და საქართველოს წინააღმდეგ განხორციელდა''.**

იენს სტონტელბერგმა ყურადღება გაამახვილა იმ ერთ-ერთ

ყველაზე საფრთხის შემცველ სივრცეზე, რაც ამ წიგნის მთავარ თემას წარმოადგენს - ეს გახლავთ კიბერსივრცე და ჰიბრიდული თავდასხმები»

იენს სტოლტენბერგი (1959)

„ჩვენთვის ეს ახალი გამოწვევაა, უკვე დავდექით აგრესიის სხვადასხვა ფორმის წინაშე. ახლა საჭიროა ჩვენ ერთობლივი მუშაობის შეცვლილი ფორმირება და ადაპტაცია. ჩვენ ინ ტენსიურად ვმუშაობთ კიბერუსაფრთხოების გაძლიერებაზე''.

სტონტელბერგმა ასევე ისაუბრა რუსეთის მოქმედებებზე შავი ზღვის აუზსა და ბალკანეთში. მისი პოზიცია ამაზე საკმაოდ მკაფიო იყო - ნატო უკვე არის ბალკანეთში, ალიანსს ჰყავს ახალი პარტნიორები ამ რეგიონში და ახალი წევრების მიღება არის მნიშვნელოვანი. ნატოს ჰყავს სამი წევრი სახელმწიფო შავ ზღვაში - თურქეთი, ბულგარეთი, რუმინეთი. ამავე რეგიონში ჰყავს ორი მნიშვნელოვანი პარტნიორი საქართველოსა და უკრაინის სახით.

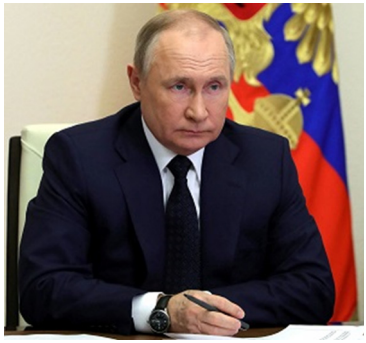
„ნატომ არა ერთხელ დააფიქსირა პოზიცია, რომ საქართველოსთვის ნატოს კარი ღიაა. ჩვენ მკაფიოდ ვაფიქსირებთ, რომ საქართველო გახდება ალიანსის წევრი, მაგრამ ჩვენ არ ვაკონკრეტებთ ზუსტ თარიღს“.

იენს სტოლტენბერგი ამბობს, რომ დღეს ნატო არის კონცენტრირებული რეფორმებზე. მათი მიზანია, ალიანსმა გააგრძელოს საქართველოს მხარდაჭერა. მოხდეს თავდაცვისა და უსაფრთხოების ძალების სისტემის მოდერნიზება. რუსეთს არ აქვს ჩარევის უფლება ამ პროცესში. ეს არის ნებმისმიერი სუვერენული ქვეყნის უფლება აირჩიოს საკუთარი განვითარების გზა[20].

20 ბოჭოიძე ნ. საქართველოს ატლანტიკური ხელშეკრულების ახალგაზრდული ასოციაცია, “2021 წლის ნატოს სამიტის გენერალური მდივნის გახსნითი სიტყვა”, ბრიუსელი, გვ. 1. 2021 წ. http://yata.ge/ge/?p=1883

ნატომ გამოაქვეყნა კომუნიკე, სადაც ჩაიწერა, რომ ბუქარესტის 2008 წლის გადაწყვეტილება ძალაში რჩება. კომუნიკეში ხაზგასმით არის აღნიშნული, რომ საქართველო ალიანსის წევრი აუცილებლად გახდება, ამ პროცესის შემადგენელი იქნება გაწევრიანების სამოქმედო გეგმის, ანუ მაპის მიღებაც. კომუნიკეში მნიშვნელოვანი გზავნილებია რუსეთის მისამართითაც. ნატო რუსეთს მოუწოდებს, აფხაზეთიდან და ე.წ. სამხრეთ ოსეთიდან გაიყვანოს ჯარები. აღსანიშნავია, რომ ბრიუსელის სამიტის პარალელურად მოეწყო ფორუმი, სადაც სპიკერებს შორის მსოფლიოს რამდენიმე ქვეყნის ლიდერთან ერთად საქართველოს პრემიერ-მინისტრი ირაკლი ღარიბაშვილიც იყო[21].

საქართველოსთან დაკავშირებული ჩანაწერები აღნიშნულ კომუნიკეში ძალიან მნიშვნელოვანი და დამაკმაყოფილებელია. ჩვენს ქვეყანას ნატოში გაწევრიანებისთვის ყველა პრაქტიკული ინსტრუქცია და ინსტრუმენტი გააჩნია.



ვლადიმერ პუტინი (1952)

სწორედ ბუქარესტის სამიტზე მიღებული გადაწყვეტილება ვერ მოინელა რუსეთმა, სადაც ოფიციალურად გაფორმდა, რომ უკრაინა და საქართველო აუცილებლად გახდებიან ნატოს წევრები. 2022 წლის 21 თებერვალს რუსეთის პრეზიდენტმა **ვლადიმერ პუტინმა** ხელი მოაწერა უკრაინის ორი სეპარატისტული რეგიონის - დონეცკისა და ლუგანსკის დამოუკიდებელ რესპუბლიკებად აღიარებას, შემდეგ კი ამ **,,რესპუბლიკებთან“** სამშვიდობო, ანუ სამხედრო ხელშეკრულებები გააფორმა. ზუსტად იგივე სცენარი, რაც დატრიალდა საქართველოს თავზე 2008 წლის აგვისტოში. თუმცა აქ არის ერთი ,,ცდომილება“, უკ-

21 ახალაია ლ., საქართველოს საზოგადოებრივი მაუწყებელი, “ბრიუსელის სამიტი და ნატოს კომუნიკე”, ბრიუსელი, გვ. 1. 2021 წ. https://1tv.ge/video/briuselis-samiti-da-natos-komunike/

რაინის ხელისუფლება არ წამოეგო რუსეთის მიერ დაგებულ პროვოკაციაზე, არ გაიმეორა მიხეილ სააკაშვილის შეცდომა. თუმცა ამით დიდად არაფერი იცვლება, შედეგი იგივეა, ოღონდ უფრო ფართო მასშტაბით. აქვე უნდა აღინიშნოს, რომ პროვოკაციის მომზადებას და ე.წ. აღიარების პროცესს წინ უძღვოდა უწყვეტი საინფორმაციო ომი არა მხოლოდ უკრაინის, არამედ მთელი მსოფლიოს წინააღმდეგ. რუსული ტელეარხები, საინფორმაციო სააგენტოები ავრცელებდნენ დეზინფორმაციას, რომ პროვოკაციას აწყობდა არა რუსეთი, არამედ უკრაინა, ანუ კიევში მოკალათებული ჯგუფი, რომელმაც მიიტაცა ძალაუფლება. ამ ყველაფერს ასევე წინ უძღვოდა კიბერთავდასხმები სამთავრობო სტრუქტურების სისტემებზე.

როგორც რეალურ სივრცეში, ასევე ვირტუალურ სივრცეში მნიშვნელოვანი ზარალი განიცადა რუსეთმაც. ექსპერტების მტკიცებით, ომმა, რომელიც 2022 წლის 24 თებერვალს დაიწყო, დაანგრია არა მხოლოდ რუსეთის უძლეველობის მითი სამხედრო თვალსაზრისით, ასევე კიბერომის თვალსაზრისითაც. ომის დაწყებისთანავე რუსეთში ჰაკერებმა გატეხეს ვიდეოპლატფორმები **Wink** და **IVI**, რუსეთის რამდენიმე არხზე სერიალების ნაცვლად ეთერში გაუშვეს უკრაინაში დაბომბვების შესახებ „ნასტოიაშჩეე ვრემიასა“ და “დოჟდის” ვიდეოები.

ომის კადრების რუსულ არხებზე გაშვების შესახებ **„ანონიმუსმა“ „ტვიტერზე“** დაწერა და ვიდეოც გაავრცელა. მართალია, რუსული არხების მაუწყებლობა მალევე აღდგა, მაგრამ ეს მაინც დარჩა მძლავრ სიგნალად, რომ რუსეთი არც ამ სფეროშია უძლეველი.

„ანონიმუსმა“, რომელიც თავი-

სუფალი, არაცენტრალიზებული ჰაკერული ორგანიზაციაა და აერთიანებს ე.წ. **ჰაკტივისტებს** სხვადასხვა ქვეყნებიდან, გამოაქვეყნა განცხადება, თითქოს მათ შეაღწიეს რუსეთის უსაფრთხოების სისტემებში და გამოიტანეს რუსეთის აგენტების სიები, რასაც ეტაპობრივად გამოაქვეყნებდნენ სახელმწიფოების მიხედვით. ამ განცხადებას თავიდანვე ეტყობოდა, რომ შესაძლოა **„ფეიკი“**, ანუ პროპაგანდის ყალბი ნაწილი ყოფილიყო, მსგავსი „ამბების“ გავრცელება გახლავთ ჩვეულებრივი მეთოდი. ყოველ შემთხვევაში, **„ანონიმუსის“** დაპირება არ შესრულდა, არავითარი აგენტების სია არ გამოქვეყნებულა. საერთოდ, ეს ძალიან სენსიტიური თემაა, შეიძლება რამე მსგავსი სია გამოქვეყნდეს, მაგრამ მერე იქ ვინ რას ჩაამატებს და როგორ დაამახინჯებს, ვეღარავინ გაიგებს. თუ **„ანონიმუსის“** ჰაკერებმა მართლაც შეაღწიეს რუსეთის უსაფრთხოების სისტემებში, იქიდან რაიმე ღირებული გამოიტანეს და გამოქვეყნებაზე უარი თქვეს, მაშინ გამოდის, ეს ,,ჭკვიანური›› ორგანიზაცია ყოფილა. რაკი სიტყვამ მოიტანა, კარგი იქნება, დეტალურად გაგაცნოთ, რას წარმოადგენს **,,ანონიმუსი’’**. იგი შეიქმნა 2003 წელს. როგორც თავად ხელმძღვანელები ამბობენ, ეს არ არის ჰაკერული დაჯგუფება.

„თუ თქვენ იზიარებთ **„ანონიმოუსის“** იდეებს, შეგიძლიათ დაუძახოთ თქვენს თავს **ანონიმი**, იმიტომ, რომ თქვენ **ანონიმი ხართ!**“ - აცხადებენ ისინი თავიანთ მიმართვებში, რომლებსაც ვიდეოჩანაწერების სახით ავრცელებენ.

2008 წლის პროექტი **Chanology!** თავდასხმა ეკლესია **Scientology**-ს ვებ გვერდზე. გათიშვის შემდეგ ინტერნეტში გავრცელდა ვიდეო, სადაც **ანონიმები** სრულად იღებენ პასუხისმგებლობას საიტის გათიშვაზე. რამდენიმე რელიგიური და მსხვილი კორპორატიული საიტისა თუ სერვერის შემდეგ სამიზნე გახდა ისეთი ქვეყნების სამთავრობო ვებ-გვერდები და სერვერები, როგორებიცაა აშშ, ისრაელი, ტუნისი, უგანდა, თურქეთი და სხვა. **ანონიმებმა** ასევე გაილაშქრეს ბავშვთა პორნოგრაფიის წინააღმდეგ. **,,ანონიმოუსს’’** საჯაროდ დაუჭირა მხარი **LulzSec-მა, AntiSec-მა (ჰაკერულმა დაჯგუფებებმა)** და

შემდეგ გაერთიანებული ძალებით დაესხნენ თავს აშშ -ის სამთავრობო სააგენტოებს, მედიას, ვიდეოთამაშების კომპანიებს, სამხედრო კონტრაქტორებს, სამხედრო პერსონალის დახურული ინფორმაციის შემცველ სერვერებს.

,,ჩვენ, **ანონიმები**, ვართ ის ადამიანები, რომელბმაც ვიპოვეთ საშუალება, გავაკეთოთ ის, რაც გვინდა. ამის შესაძლებლობა ჩვენ არასდროს გვქონია ჩვეულებრივ საზოგადოებაში. აკეთეთ ის, რაც გინდათ, სულ ესაა!» - ვკითხულობთ **„ანონიმუსის“** განცხადებაში.

მას შემდეგ, რაც მათ გააკეთეს ის, რაც სურდათ, ინტერპოლმა რამდენიმე ათეული ადამიანი დააკავა განსაკუთრებით მძიმე კიბერ დანაშაულის ბრალდებით. პირველი პირი, რომელიც დააკავეს **DDoS** შეტევის გამო, იყო ვინმე **Guzner**, ცხრამეტი წლის ამერიკელი ჰაკერი. მან დანაშაული აღიარა და 2009 წელს 1 წლით თავისუფლების აღკვეთა ამერიკის ფედერალური ციხეში. ანონიმები დააკავეს დიდ ბრიტანეთშიც, ავსტრალიაშიც, ნიდერლანდებშიც, ესპანეთსა და თურქეთშიც. ანონიმებმა უპასუხოდ არ დატოვებს ეს ქმდებები და სათითაოდ ჩაატარეს ყველა ქვეყანაში ე.წ. სპეცოპერაცია **,,takedown“**, რაც ამ ქვეყნების სამთავრობო საიტების განადგურებას ითვალისწინებდა. 2011 წელს თურქეთში დააკავეს 32 პირი **DDoS** თავდასხმების გამო. ისინი თავს დაესხნენ თურქულ სამხედრო სერვერებს[22].

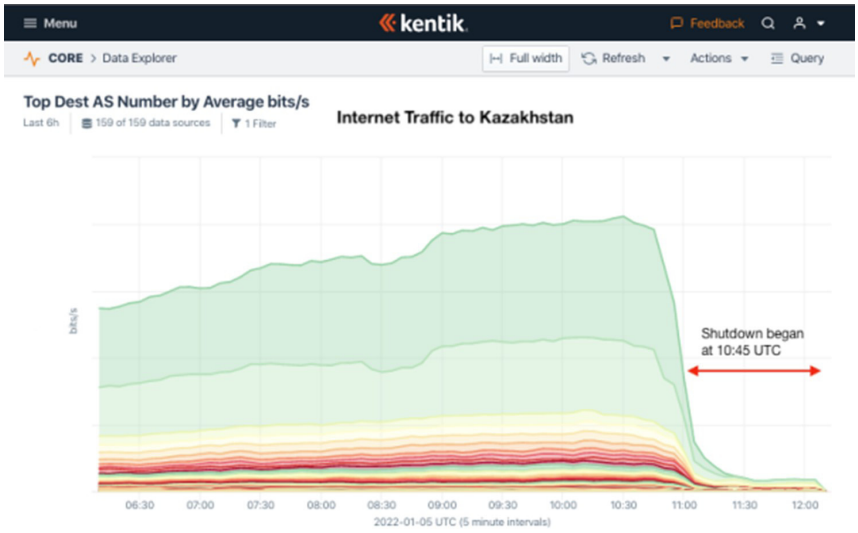
ჯერ კიდევ ბოლომდე გაურკვეველია, რა სახის თავდასხმები განხორციელდა უკრაინულ და რუსულ სამთავრობო ვებ-გვერდებზე ან სამხედრო სისტემებზე, რა სახის ზარალი განიცადა ან ერთმა, ან მეორე მხარემ. ალბათ ამის ზუსტს აღრიცხვას და გაანალიზებას წლები დასჭირდება.

ჩვენ ყურადღების გარეშე არ უნდა დავტოვოთ ყაზახეთში რუსეთ-უკრაინის ომამდე განვითარებული მოვლენები, რაც თითქოს მოულოდნელი იყო მთელი მსოფლიოსთვის, მსგავსი ვანდალიზმი, სახელმწიფო დონეზე აყვანილი განუკითხაობა იშვიათად თუ უნა-

22 ქართული „ვიკიპედია“, „ანონიმუსი“ (ჰაკერული დაჯგუფება), 2004 წ. გვ. 1, https://ka.wikipedia.org/

ხავს მსოფლიოს. კი, ბატონო, ყაზახეთის მოსახლეობის პროტესტი გასაკვირი ნამდვილად არ არის, ნურსულთან ნაზარბაევის ფეოდალიზმი ალბათ ყველას ყელში ამოუვიდა, მაგრამ საკუთარი ქვეყნის გადაბუგვა და ე.წ. სამშვიდობოების მიწვევა რუსეთის მეთაურობით, უარეს მომავალს ნიშნავს. საკითხავია, დასრულდა კი ყაზახეთში ნურსულთანიზაცია? ყველაფერი კი დაიწყო საწვავის ფასების ზრდით და შემდეგ პროტესტით, ხელისუფლების სისასტიკით.

ყაზახეთის პრეზიდენტმა **ყასიმ-ჟომარტ ტოყაევმა (Kassym-Jomart Tokayev)** კოლექტიური თავდაცვის ხელშეკრულების ორგანიზაციას მიმართა დახმარებისთვის. მშვიდობა დამყარდა სისხლის ფასად, დაკავებულთა რაოდენობამ 8000-ს ადამიანს გადააჭარბა. საყურადღებოა ის ფაქტი, რომ ყაზახეთში ინტერნეტ-სატელეკომუნიკაციო კავშირი ერთ კვირაზე მეტ ხანს გათიშული იყო. ეს მოხდა ხელისუფლების ბრძანებით. როდესაც პრეზიდენტი აკეთებდა განცხადებას, მხოლოდ იმ შემთხვევაში ხორციელდებოდა ინტერნეტის ჩართვა. ყაზახეთში კიბერსივრცე ჩაახშეს იმ მოტივით, რომ პროტე-



დიაგრამა – სატელეკომუნიკაციო ქსელების მონიტორინგის სააგენტო "kentik"-ის მონაცემები

წყარო: https://www.kentik.com/analysis/internet-blackout-in-kazakhstan-as-crisis-continues/

სტანტებს ვერ მოეხერხებინათ მობილიზაცია. ამან შედეგი გამოიღო.

სატელეკომუნიკაციო ქსელების მონიტორინგის სააგენტო **„Kentik"**-ის ინფორმაციით, ინტერნეტის პირველი გამორთვა 5 იანვარს, ადგილობრივი დროით 16:45 საათზე დაიწყო. რასაკვირველია, ამან გამოიწვია ქვეყნის **,,დადუმება"** ყველა დონეზე - პოლიტიკური, ეკონომიკური თუ დანარჩენ მსოფლიოსთან ურთიერთობის მიმართულებით. თუ ყაზახეთში დამანგრეველი აქციების ლოკალიზება მალე მოხერხდა, უკრაინის პრობლემა ალბათ წლების განმავლობაში გაიწელება. სამწუხაროდ, მსგავსი მწარე გაკვეთილი საქართველომ უკვე გაიარა, ტერიტორიების 20% დაკარგულია[23].

კიბერომის თეორია და მისი ადგილი თანამედროვე მსოფლიო პოლიტიკაში

როდესაც ვსაუბრობთ კიბერომზე, პირველ რიგში უნდა ავხსნათ, რა მოვლენასთან გვაქვს საქმე. ეს არის ერთი ქვეყნის მიერ მეორე ქვეყანაზე ციფრული შეტევები (კომპიუტერული ვირუსები ან ჰაკერული კიბერშეტევები) კომპიუტერული ინფრასტრუქტურის დაზიანების, ლიკვიდაციისა და განადგურების მიზნით.

ტერმინ **„კიბერომთან"** დაკავშირებით ექსპერტებს შორის განსხვავებული მოსაზრებები არსებობს. ერთნი ამბობენ, რომ ეს ტერმინი არასწორია, რადგან დღემდე არცერთი კიბერშეტევა არ შეიძლება შეფასდეს, როგორც **,,ომი"**. ექსპერტების მეორე ნაწილი მიიჩნევს, რომ ეს შესაბამისი სახელწოდებაა, რადგან კიბერშეტევა ფიზიკურად აზიანებს ადამიანებს და საგნებს რეალურ სამყაროში.

განიხილება თუ არა კიბერშეტევა ომის წარმოებად? ეს დამოკიდებულია მრავალ ფაქტორზე - რას აკეთებენ, როგორ აკეთებენ და რა ზიანს აყენებენ სამიზნე ობიექტს. შეტევების კვალიფიკაცია უნდა

23 "Support the Guardian" Available for everyone, funded by readers, "Kazakhstan protests: Moscow-led alliance sends 'peacekeeping forces' ", 2022, p. 1, https://www.theguardian.com/world/2022/jan/05/kazakhstan-protests-president-threatens-ruthless-crackdown

იყოს მნიშვნელოვანი მასშტაბისა და სიმძიმის. ინდივიდი ჰაკერების, ან ჰაკერთა ჯგუფის თავდასხმები არ ითვლება კიბერომად, თუ სახელმწიფო არ ეხმარება ან არ ხელმძღვანელობს. მიუხედავად ამისა, ვირტუალური სამყარო კიბერშეტევების მიმართულებით მაინც ბუნდოვნად არის წარმოდგენილი. არსებობენ სახელმწიფოები, რომლებიც მხარს უჭერენ ჰაკერებს დამაზიანებელი შეტევების განხორციელებაში, ეს საშიში, მაგრამ ჩვეულებრივი ტენდენციაა.

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

ასევე არის განსხვავება სამიზნე ობიექტსა და მასშტაბს შორის: ინდივიდუალური კომპანიის ვებ-გვერდის გაფუჭება კიბერომად არ მიიჩნევა, მაგრამ საჰაერო ბაზაზე სარაკეტო თავდაცვის სისტემების მწყობრიდან გამოყვანა აღიქმება კიბერომად. ამ შემთხვევაში მნიშვნელოვანია, თუ რა იარაღს იყენებს თავდამსხმელი. მაგალითად, მონაცემთა ცენტრისთვის რაკეტის სროლა კიბერომად არ ჩაითვლება, თუნდაც მონაცემთა ცენტრი შეიცავდეს მთავრობის საიდუმლო ჩანაწერებს. ჰაკერების გამოყენება ჯაშუშობისთვის ან მონაცემების მოპარვის მიზნით, კიბერომს არ გულისხმობს და ეს კიბერჯაშუშობის კვალიფიკაციით განისაზღვრება. კიბერომთან მიმართებაში ბევრი ბნელი ხვრელია, მაგრამ ყველა შეტევის კიბერომად მიჩნევა შეუძლებელია[24].

მიუხედავად იმისა, რომ ამ მიმართულებით არსებობს განსხვავებული მოსაზრებები, თუ როგორ უნდა განისაზღვროს **„კიბერომი“**, როგორც ტერმინი, დღეს ბევრ ქვეყანას, მაგალითად, ამერიკის შეერთებულ შტატებს, რუსეთს, ბრიტანეთს, ინდოეთს, პაკისტანს, ჩინეთს, ისრაელს, ირანის ისლამურ რესპუბლიკას და ჩრდილოეთ

24 Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict, Information Technology Company ZDnet, 2018, p 1. https://www.zdnet.com

კორეას უკვე გააჩნიათ კიბერშესაძლებლობები როგორც შეტევითი, ასევე თავდაცვითი ოპერაციებისთვის.

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

კიბერომის უამრავი სცენარი არსებობს. უკვე ისეთ ეპოქაში ვცხოვრობთ, შეიძლება ერთ დღესაც გაიღვიძოთ და საბანკო ანგარიშები განულებული დაგხვდეთ, რადგან ვიღაც ჰაკერმა მოინდომა ასე. ან სულაც, დაიძინოთ მშვიდად და გაიღვიძოთ ქაოსში.

არსებობს კიბერომის სამი ძირითადი მეთოდი: დივერსია, ელექტრონული ჯაშუშობა, ანუ კომპიუტერებიდან ინფორმაციის მოპარვა ვირუსების საშუალებით და კრიტიკულ ინფრასტრუქტურაზე

კიბერშეტევა. მესამე, ალბათ, ყველაზე საგანგაშოა, რადგან აღნიშნულმა კიბერშეტევამ შესაძლოა ქვეყნის პარალიზება გამოიწვიოს[25].

წამყვანი სახელმწიფოების მთავრობები აცნობიერებენ, რომ თანამედროვე საზოგადოება დამოკიდებულია კომპიუტერულ სისტემებზე - დაწყებული ფინანსური მომსახურებით, დამთავრებული სატრანსპორტო ქსელებით. ამ სისტემების გაჩერება ვირუსებით ან სხვა საშუალებებით შეიძლება ისეთივე საზიანო და დამანგრეველი იყოს, როგორც ტრადიციული

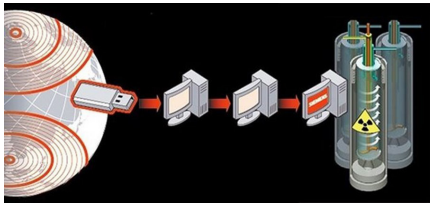
25 Gartzke E. Making Sense of Cyberwar, Harvard Kennedy School Belfer Center for Science and International Affairs, 2014, p 1. https://www.belfercenter.org

სამხედრო შეტევა შეიარაღებული ძალების გამოყენებით.

მეტიც, ტრადიციული სამხედრო თავდასხმებისგან განსხვავებით, კიბერშეტევა შეიძლება განხორციელდეს ნებისმიერი მანძილიდან. ისიც შესაძლებელია, არავითარი კვალი არ დარჩეს და მტკიცებულება საერთოდ გაქრეს.

სახელმწიფოთა მესვეურები და სადაზვერვო სააგენტოები შიშობენ, რომ ციფრული შეტევები კრიტიკული ინფრასტრუქტურის წინააღმდეგ - საბანკო სისტემებზე ან ენერგეტიკულ ქსელებზე, თავდამსხმელებს საშუალებას მისცემს, გვერდი აუარონ ქვეყნის ტრადიციულ თავდაცვას. ამიტომ ყველა ქვეყანა ისწრაფვის კომპიუტერული უსაფრთხოების გაუმჯობესებისკენ.

2012 წელს ირანის ისლამური რესპუბლიკის ხელისუფლების მიერ დაქირავებულმა ჰაკერებმა ნიუ-იორკში ბოუმენის ავენიუს კაშხალზე



სრული კონტროლი მოიპოვეს. კრიტიკულ ინფრასტრუქტურაზე კიბერშეტევის ყველაზე გახმაურებული მაგალითია **“Stuxnet”** კომპიუტერული ვირუსით თავდასხმა, რომელმაც ირანის ბირთვული პროგრამა შეაჩერა და ბირთვული მასალის გამოყოფისთვის გამოყენებული ცენტრიფუგები გაანეიტრალა. ამ ინციდენტმა დიდი შეშფოთება გამოიწვია, რადგან **“Stuxnet”**-ზე ეჭვობდნენ, რომ შეიძლება ადაპტირებული ყოფილიყო **“SCADA”** სისტემებზე თავდასხმისთვისაც. **“SCADA”** სისტემებს იყენებს მრავალი კრიტიკული ინფრასტრუქტურა და ინდუსტრია ევროპასა და აშშ-ში.

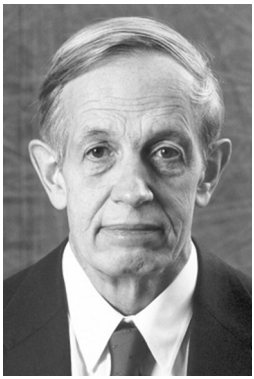
ასეთი თავდასხმა 2014 წელს გერმანიაში დაფიქსირდა, რომელმაც ფოლადის ქარხანა დააზარალა - კიბერშეტევამ გამოიწვია ღუმელების გათიშვა. თავდამსხმელებმა გამოიყენეს სოციალური ინჟინერიის ტექნიკა[26].

26 Lohrmann D. How Vulnerable Is Critical Infrastructure to a Cyberattack?, Governament Technology, 2020, p 1. https://www.govtech.com

კიბერომის ტრანსფორმაციის ისტორიული ასპექტები - სამხედრო კონფლიქტების სივრცული მახასიათებლები

ჰაკერთა ტიპები:

აუცილებელია განვიხილოთ ჰაკერთა ტიპები და ტიპოლოგია. ტერმინი ,,ჰაკერი'' ნობელის პრემიის ლაურეატს, ცნობილ მათემატიკოსს, **ჯონ ნეშს** ეკუთვნის.



სურათი 1 ჯონ ნეში (1928-2015)

არსებობს **ჰაკერთა** რამდენიმე ტიპი იმის მიხედვით, თუ რა განზრახვა აქვს ამ პროფესიის ადამიანს. სიტყვა ,,ჰაკერი'' ხშირად აღიქმება ნეგატიურად, თუმცა არსებობენ **ეთიკური ჰაკერებიც**, რომლებიც ნეგატიური და მავნებლური საქმიანობებისგან შორს არიან.

ავხსნათ ტერმინი **,,ეთიკური ჰაკერი''** - ჰაკინგი უმეტესად აღიქმება, როგორც უკანონო ან მავნე კიბერ აქტივობა, რომელსაც ახორციელებენ კიბერთავდამსხმელები, კიბერჯაშუშები, კიბერტერორისტები და ა.შ. მიუხედავად ამისა, შეიძლება ჰაკერსა და ჰაკინგს ხშირად არ ჰქონდეს მავნე განზრახვა. ჰაკინგის ორი ვარიანტი არსებობს - არის კანონიერი და უკანონო. როგორც წესი, ჰაკერი ცდილობს, გამოიყენოს კომპიუტერი ან ქსელი მონაცემების მოსაპარად, ფაილების გასანადგურებლად, უსაფრთხოების დარღვევისთვის და ა.შ.

მაგრამ არსებობს მეორე ვარიანტიც - შესაძლებელია, ჰაკერი ემსახურებოდეს კეთილ მიზნებს, იგი ცდილობდეს აღმოაჩინოს უსაფრთხოების ხარვეზები აპლიკაციებში, ქსელებში ან სისტემებში. ეს უკვე

წარმოადგენს ლეგიტიმურ, ანუ კანონიერ შეჭრას და ჰქვია **ეთიკური ჰაკინგი**. მსოფლიო მასშტაბით ბევრ ორგანიზაციას და წამყვან სახელმწიფოს ჰყავს დაქირავებული

ეთიკური ჰაკერები, რათა აღმოაჩნინონ პოტენციური დაუცველობის ელემენტები ან კიბერსაფრთხეები, რათა აღმოფხვრან. ასევე, თავი დაიცვან მავნე ჰაკერების მხრიდან განხორციელებული კიბერთავდასხმებისგან.

სიტყვები **„ჰაკერი“** და **„ჰაკინგი“** საიდან გაჩნდა, რას ნიშნავს? ჰაკერი არის ადამიანი, რომელიც სწავლობს სისტემებს, რათა გაარ-

კვიოს, თუ როგორ მუშაობს. შესაძლოა, გაუმჯობესების განზრახვით ან უბრალოდ მანიპულირებდეს სისტემაში გართობის მიზნით. 1980-იან წლებში ჰაკერებმა შეისწავლეს, თუ როგორ მუშაობდა სატელეფონო ქსელები და დაიწყეს ჯიხურებიდან უფასო მანიპულაციები. ამის შემდეგ მედიაში უფრო გააქტიურდა ჰაკერების აუგად ხსენება.

კიბერუსაფრთხოების ექსპერტები ჰაკერების სხვადასხვანაირ კლასიფიკაციას აყალიბებენ, ჩვენ გამოვყოფთ ძირითად 6 ტიპს, რომელიც კიბერუსაფრთხოებით დაინტერესებულმა ადამიანებმა აუცილებლად უნდა იცოდნენ:

შავქუდიანი ჰაკერები (ცუდი ბიჭები) Black Hat Hackers (the bad guys)

ისინი გამოცდილი ჰაკერები არიან, სისტემაში ავტორიზაციის გარეშე იჭრებიან. იყენებენ სისტემის უსაფრთხოებას მავნე განზრახვით ან ფინანსური სარგებლისთვის. შავქუდიანი ჰაკერები მუშაობენ ორგანიზაციულ-დანაშაულებრივ ჯგუფებთან. მათ შეიძლება დააინფიცირონ სისტემა მავნე პროგრამით, რათა მოიპარონ პერსონალური მონაცე-

მები, ინფორმაცია საკრედიტო ბარათების შესახებ, დააზიანონ ფაილები და მწყობრიდან გამოიყვანონ უსაფრთხოების ქსელი.

თეთრქუდიანი ჰაკერები (ეთიკური ჰაკერები) White Hat Hackers (Ethical Hackers)

შავქუდიანთაგან განსხვავებით თეთრქუდიანები ითვლებიან კარგ ჰაკერებად. ისინი მუშაობენ საწარმოებისთვის, საერთაშორისო თუ ადგილობრივი ორგანიზაციებისთვის, მთავრობებისთვის ქსელებისა და სისტემების უსაფრთხოების გასაუმჯობესებლად. ეხმარებიან სამართალდამცავ ორგანოებს გამოძიებაში. ისინი ცნობილნი არიან ეთიკური ჰაკერების სახელითაც, აქვთ უნარ-ჩვევები, რაც საჭიროა უსაფრთხოების სისტემების შესამოწმებლად. თეთრქუდიანი ჰაკერები იცავენ კომპანიის საინფორმაციო და უსაფრთხოების ქსელებს, იდენტიფიკაციას ახდენენ და პოულობენ სისტემაში არსებულ სუსტ რგოლებს ან შესაძლო საფრთხეებს, რათა მოხდეს კიბერ შეტევების თავიდან აცილება.

რუხქუდიანი ჰაკერები Grey Hat Hackers

რუხქუდიანი ჰაკერები ორივე ტიპის ჰაკერებს წარმოადგენენ - შავქუდიანებსა და თეთრქუდიანებს. ისინი ეძებენ სისუსტეებს უსაფრთხოების ქსელებში, თუმცა ხშირად მავნე განზრახვის გარეშე. მათ პერიოდულად უწევთ ინკოგნიტოდ მუშაობა და კანონის დარღვევა, რათა არასანქცირებული წვდომა მიიღონ სისტემებზე. ეს შეიძლება იყოს გამოძიების დახმარების მიზნით, მაგრამ არა მავნე განზრახვით. ისინი თეთრქუდიანები არიან, მაგრამ ხანდახან სჭირდებათ შავი ქუდის ტარება.

ლურჯქუდიანი ჰაკერები Blue Hat Hackers

ლურჯქუდიანი ჰაკერები ცნობილნი არიან ორი სახით - პირველი განმარტებით, ლურჯქუდიანი ჰა-

კერები არიან შურისმაძიებლები, ხოლო მეორე განმარტებით, ისინი არიან უსაფრთხოების ექსპერტები. მათ იწვევენ ორგანიზაციები ახალი სისტემებისა და აპლიკაციების შესამოწმებლად, სუსტი ბმულების გამოსასწორებლად.

წითელქუდიანი ჰაკერები Red Hat Hackers

წითელქუდიანი ჰაკერები - ისინი ნადირობენ შავქუდიანებზე იმ მიზნით, რომ რისკები შეამცირონ. მათ სურთ თეთრქუდიანების მსგავსად გადაარჩინონ სამყარო ბოროტი ჰაკერებისგან. ისინი ირჩევენ ექსტრემალურ, ზოგჯერ უკანონო გზებს თავიანთი მიზნების მისაღწევად. წითელქუდიან ჰაკერებს კიბერუსაფრთხოების სფეროში ფსევდო რობინ ჰუდებსაც უწოდებენ. შეიძლება ვთქვათ, ისინი არასწორ გზას მიჰყვებიან სწორი საქმის საკეთებლად. როდესაც აღმოაჩენენ შავქუდიან ჰაკერებს, ისინი ახორციელებენ სახიფათო კიბერშეტევებს მათ წინააღმდეგ.

მწვანექუდიანი ჰაკერები Green Hat Hackers

ესენი ჰაკერების სამყაროში ცნობილნი არიან როგორც „ახალშობილები“. მწვანექუდიანებმა არ იციან უსაფრთხოების მექანიზმები და ქსელის შიდა ფუნქციონირება. თუმცა არიან მონდომებული მოსწავლეები და გადაწყვეტილი აქვთ, აიმაღლონ თავიანთი პოზიციები ჰაკერების საზოგადოებაში. მიუხედავად იმისა, რომ მათი განზრახვა სულაც არ წარმოადგენს ზიანის მიყენებას, შეიძლება გამოიყენონ სხვადასხვა მავნე პროგრამები ტექნიკის დასახვეწად. მწვანექუდიანი ჰაკერები შესაძლოა დამაზიანებელნი აღმოჩდნენ უნებლიედ, მათ ხშირად არ იციან, რა შედეგები მოჰყვება მათ საქმიანობას[27].

27 Cyber Security, ,,Different Types of Hackers: The 6 Hats Explained'', InfoSec Insights, 2020. p. 1, https://sectigostore.com/blog/different-types-of-hackers-hats-explained/

კიბერსივრცეში ასევე არსებობენ სხვადასხვა ტიპის ჰაკერები:

- **სკრიპტის ბავშვები (Script Kiddie)**
- **ქვეყნების მიერ დაფინანსებული ჰაკერები (State/Nation Sponsored Hackers)**
- **მავნე ინსაიდერები: მამხილებელი ჰაკერები (Malicious Insider: Whistleblower Hackers)**
- **ჰაკტივისტები (Hacktivists)**
- **ელიტარული ჰაკერები (Elite Hackers)**
- **კრიპტოჯეკერები (Cryptojackers)**
- **თამაშის ჰაკერები (Gaming Hackers)**

სკრიპტის ბავშვები (Script Kiddie)

აღნიშნული ტერმინი ნიშნავს მოზარდებს, რომლებიც არ არიან საკმარისად გამოცდილები იმისათვის, რომ შექმნან და განახორციელონ კომპიუტერის მავნე თავდასხმები. შეიძლება პარალელები გავავლოთ მწვანექუდიან ჰაკერებთან, თუმცა განსხვავებები არსებობს. მაგალითად Script Kiddie-ბი ხშირად ეყრდნობიან სხვების მიერ შექმნილ სკრიპტებს ან მავნე პროგრამებს კიბერშეტევების განხორციელებისთვის. მათ არ აინტერესებთ ჰაკერების საზოგადოება. კიბერუსაფრთხოების ზოგიერთი ექსპერტი აღნიშნავს, რომ შეიძლება Script Kiddie-ბი მომავალში გახდნენ შავქუდიანი ჰაკერები. ისინი ხშირად წარმატებით იყენებენ ინტერნეტში მოპოვებულ სხვადასხვა პროგრამებს, მავნე ჰაკერული თავდასხმებისთვის.

ქვეყნების მიერ დაფინანსებული ჰაკერები (State/Nation Sponsored Hackers)

ჰარეკები, რომლებიც დაქი-

რავებულნი არიან რომელიმე ქვეყნის მთავრობის მიერ, მეორე ქვეყნის კომპიუტერულ სისტემებზე წვდომის მისაღწევად. მათი ნიჭი გამოიყენება სენსიტიური ინფორმაციის მოსაპოვებლად, პოტენციური საფრთხის ან თავდასხმის წინ. ისინი უფრო მეტად არიან საერთაშროისო საფრთხეების მონიტორინგზე და პრევენციაზე ორიენტირებულნი.

მავნე ინსაიდერები: მამხილებელი ჰაკერები (Malicious Insider: Whistleblower Hackers)

მავნე ინსაიდერები არიან ის ჰაკერები, რომლებიც იწყებენ კიბერშეტევას იმ კომპანიის შიგნიდან, რომელშიც მუშაობენ. მამხილებლები თავდასხმებს აწყობენ პირადი შურისძიების მიზნით, ვისთანაც მუშაობენ. მათი ძირითადი მიზანია ორგანიზაციის კონფიდენციალური ინფორმაციის გამჟღავნება.

ჰაკტივისტები (Hacktivists)

ჰაქტივისტები არიან ის ჰაკერები, რომლებიც კიბერშეტევებს ანხორციელებენ პოლიტიკური მიზნით, თავს ესხმიან და არღვევენ სამთავრობო ქსელებს, სისტემებს, რათა ყურადღება მიიპყრონ პოლიტიკური ან სოციალური მიმართულებით. ტერმინი ,,ჰაქტივისტი›› ნაწარმოებია სიტყვა „აქტივისტისგან“. ისინი იყენებენ ჰაკერულ შეტევებს, როგორც პროტესტის ერთგვარ მეთოდს, იღებენ სენსიტიურ სამთავრობო მონაცემებს, პოლიტიკური ან სოციალური მიზეზების გამო.

ელიტარული ჰაკერები (Elite Hackers)

ელიტარული ჰაკერები არიან

საუკეთესოთა შორის კიბერდანაშაულის სფეროში. ისინი აღიარეს საუკეთესო სპეციალისტებად კიბერსფეროში და ხშირად აკეთებენ კიბერტაქტიკურ აღმოჩენებს.

კრიპტოჯეკერები (Cryptojackers)

კრიპტოჯეკერები სარგებლობენ ქსელების ხარვეზებით და იპარავენ კომპიუტერულ რესურსებს ბიტკოინების მოპოვების მიზნით. ისინი ავრცელებენ მავნე პროგრამებს სხვადასხვა მეთოდებით, მათ შორის კომპიუტერების დაინფიცირების გზით.

მოთამაშე ჰაკერები (Gaming Hackers)

მოთამაშე ჰაკერებად იწოდებიან ისინი, რომლებიც ძალისხმევას ხარჯავენ კონკურენტების დაჰაკვაზე. სათამაშო ინდუსტრიის ზრდასთან ერთად, გასაკვირი არ არის, რომ გაჩნდა მოთამაშე ჰაკერების კატეგორია. პროფესიონალ გეიმერებს შეუძლიათ დახარჯონ ათიათასობით დოლარი მაღალი ხარისხის სათამაშო ხელსაწყოებზე და კრედიტებზე, ხოლო მოთამაშე ჰაკერები, როგორც წესი, მიზნად ისახავენ კონკურენტების საკრედიტო ქეშების დაჰაკვას ან კიბერშეტევებს ახორციელებენ, რათა გამოყარონ ისინი თამაშიდან[28].

ტექნოლოგიების განვითარებამ არ შეცვალა პრიორიტეტები სახელმწიფო დაცვის საკითხებში, როგორც მეორე მსოფლიო ომის დროს - ძირითადი ტაქტიკური დარტყმები ენერგეტიკული ობიექტებისკენ არის მიმართული. ამჟამად სერიოზული კიბერთავდასხმების უმეტე-

28 Private & Security digital life - SICCURA, ,,Top Hackers to Watch Out For", 2021. p. 1, https://siccura.com/top-hackers-to-watch-out-for/

სობა ხდება ენერგეტიკულ კომპლექსებზე, შემდეგ მოდის ფინანსური სექტორი.

ციფრულმა სამყარომ ახალი ტიპის საფრთხეების წარმოშობას შეუწყო ხელი. როგორც უკვე აღვნიშნეთ, ყველა სახის კიბერშეტევას ვერ განვიხილავთ კიბერომის ჭრილში. მიუხედავად იმისა, რომ განვსაზღვრეთ, რა არის კიბერომი და რა კიბერშეტევა, მაინც რთულია კიბერომის კვალიფიკაციის მინიჭება, უმეტესი ფაქტი ემყარება ვარაუდს. კვალს ხშირად მივყავართ რომელიმე აგრესორ სახემწიფომდე, მაგრამ ხშირად მტკიცებულებები არ არსებობს. კიბერომებსა და ტექნიკურ მახასიათებლებს განვიხილავთ სხვადასხვა კვლევებზე დაყრდნობით, ვაკეთებთ ანალიზს - როდიდან იწყება, როგორ ტრანსფორმირდა, რა როლი აქვს მიმდინარე კონფლიქტებისას და ასე შემდეგ. მნიშვნელოვანი ფაქტია, რომ მრავალი სახელმწიფო არა მხოლოდ ახორციელებს კიბერჯაშუშურ საქმიანობას, დაზვერვას და კვლევას, არამედ თვითონვე ქმნიან კიბერომის შესაძლებლობებს. მე-20 საუკუნის ბოლოს ვერავინ წარმოიდგენდა, რომ რეალური ომი იქცეოდა განყენებულ განზომილებაში შექმნილი ომის დანამატად, ან პირიქით, ირეალური სივრცე შეერწყმებოდა რეალურს. ალბათ, ვერც იმას წარმოიდგენდა ვინმე, რომ გაჩნდებოდა განზომილება, რომლის გაკონტროლება იქნებოდა თითქმის შეუძლებელი, კაცობრიობა დადგებოდა უხილავი საფრთხის წინაშე. როდესაც კიბერომის ტრანსფორმაციის ახსნას ვცდილობთ, აუცილებლად უნდა გამოვყოთ, თუ რა ცვლის ამ ყველაფერს. ეს უმეტესად კიბერთავდასხმების ტექნოლოგიების დახვეწას და მავნებლური ჰაკერული სტრატეგიების, პროგრამებისა თუ ვირუსების შექმნას უკავშირდება. აქედან გამომდინარე, უნდა გამოვყოთ შეტევის ტიპები: **არსებობს პასიური და აქტიური კიბერშეტევები, პასიური შეტევა** გულისხმობს ტრაფიკის ანალიზსა და დაუცველი კომუნიკაციების მონიტორინგს. **აქტიური შეტევის** დროს ჰაკერი დაცულ სისტემებს უტევს. ეს უმეტესწილად ვირუსებით ხორციელდება[29].

29 Digiacomo J. Active vs Passive Cyber Attacks Explained, Intellectual Property

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

ცხრილი 1 - კიბერშეტევების ტიპები

Denial-of-service (DoS)	ამ შეტევის დროს დიდი რაოდენობის გამოუსადეგარი ტრაფიკი იგზავნება და ქსელი მწყობრიდან გამოდის. მომხმარება იმ დროს ფერხდება, ანუ წყდება, როდესაც ვებ-სერვერი ივსება და ლეგიტიმურ მოთხოვნებს აღარ პასუხობს.
distributed denial-of-service (DDoS)	შეტევის დროს რამდენიმე ჰაკერი ან გატეხილი სისტემა აკეთებს ბევრ მოთხოვნას ვებ-სერვერზე და გამოუსადეგარი ტრაფიკით ბლოკავს სერვისს. კოორდინირებულ შეტევას დიდი ზიანის მოტანა შეუძლია.
Man-in-the-middle (MitM)	როდესაც ვიღაც ერევა და აკონტროლებს თქვენი კომუნიკაციის პროცესს, თქვენ გგონიათ, ესაუბრებით ნაცნობ ადამიანს, ან გაქვთ სერვერთან უშუალო წვდომა, მაგრამ ამ დროს, ყველა თქვენს პირად ინფორმაციას ხედავს ჰაკერი.
Phishing	თავდამსხმელი ქმნის რეალური ვებ-გვერდის კლონს, მიზანში ამოღებულ მომხმარებელს ელ-ფოსტაზე უგზავნის ყალბი ვებ-გვერდის ბმულს, თუ მომხმარებელი გადავა ამ ბმულზე და შეიყვანს პირად მონაცემებს, ჰაკერი მიიღებს წვდომას ამ მონაცემებზე.
War Drive	უკაბელო კომპიუტერულ ქსელებში შესვლის მოპოვების მეთოდი, მაგალითად, ლეპტოპი, ანტენები და უკაბელო ქსელის ადაპტერი, რომელიც გულისხმობს უნებართვო წვდომის მიღებას.
Password	პაროლების მოპოვება ჩვეულებრივი და ეფექტური შეტევის მეთოდია. ეს შეიძლება გაკეთდეს შემთხვევითი ან სისტემატური გზით.

Malware attack - მავნე კოდის შეტევა:

არასასურველი პროგრამა, რომელიც თქვენი თანხმობის გარეშე სისტემაში არის გაშვებული, მას შეუძლია, ლეგიტიმურ კოდს დაერთოს და გამრავლდეს. ასევე შეუძლია, სხვადასხვა პროგრამებში გამრავლება, ან ინტერნეტთან ინტერპრეტაცია. აღსანიშნავია, რომ

Lawyer Revision Legal, 2017, p 1. https://revisionlegal.com

ყველა ვირუსი არის **Malware**. თუმცა ყველა **Malware** არ არის ვირუსი, შეიძლება იყოს პროგრამა, აპლიკაცია და ასე შემდეგ, რომელიც ჰაკერს აძლევს უფლებას, ჰქონდეს უნებართვო წვდომა პირად მონაცემებზე[30].

გამოვყოფთ მავნე კოდის შეტევის რამდენიმე აქტუალურ ფორმას:

ცხრილი 2 - მავნე კოდის შეტევების ტიპები

Ransomware	**სისტემაში არსებულ ფაილებს შიფრავს და დროებით მიუწვდომელს ხდის, ამ თავდასხმის შემთხვევაში ჰაკერები ინფორმაციის დაბრუნების სანაცვლოდ გამოსასყიდს ითხოვენ.**
Logic bombs	**ის შეიძლება იყოს პროგრამული უზრუნველყოფის ნაწილი, რომელიც გარკვეული თარიღის დადგომის შემდეგ იქცევა ზიანის შემცველ პროგრამად.**
Trojan horse	**იმალება სასარგებლო პროგრამაში. მას ჩვეულებრივ აქვს დამაზიანებელი ფუნქცია. ჰაკერს შეუძლია, ვირუსი გამოიყენოს მოსასმენად და თავდასხმების განსახორციელებლად.**
Worm	**დამოუკიდებელი კომპიუტერული პროგრამა, რომელიც ქსელში თავად მრავლდება ერთი სისტემიდან მეორეზე.**

კვლევის საფუძველზე შეგვიძლია, კიბერშეტევების სამიზნე ჯგუფიდან 3 კატეგორია გამოვყოთ:

ცხრილი 3 - კიბერშეტევების სამიზნე ჯგუფების კატეგორიები

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

30 Zamora W. 10 easy ways to prevent malware infection, Software Company Malwarebytes, 2016, p 1. https://blog.malwarebytes.com

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

მსოფლიოში წამყვანი სამეცნიერო-საკონსულტაციო კომპანია **„Gartner"**-ი ასაჯაროებს მონაცემებს კიბერუსაფრთხოების ხარჯებთან დაკავშირებით, ამ მონაცემებში შედარებული და განხილულია 2017-2019 წლების მსოფლიო კიბერუსაფრთხოების დანახარჯი სეგმენტის მიხედვით.

ცხრილში ვხედავთ **(ცხრ. 4)**, რომ კიბერუსაფრთხოების კუთხით მსოფლიოში 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[31]. **"Gartner"**-ის ინფორმაციით, 2022 წელს მსოფლიო კიბერუსაფრთხოების ხარჯებმა 133.7 მილიარდ აშშ დოლარს მიაღწია[32].

თუმცა საყურადღებოა, რომ მსოფლიოსთვის მიყენებული ზარალი ბევრად აღემატება უსაფრთხოებისთვის დახარჯულ თანხებს, **„Cybersecurity Ventures"**-ის ანგარიშში ნავარაუდებია, კიბერშეტევებისგან მიყენებული ზარალი 6 ტრილიონი აშშ დოლარია. **"Cybersecurity Ventures"**-ი ელოდება, რომ გლობალური კიბერდანაშაულის ხარჯები გაიზრდება ყოველწლიურად 15 პროცენტით მომდევნო წლების განმავლობაში,

31 Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, Consulting Agency Gartner, 2018, p 1. https://www.gartner.com

32 Sobers R. 110 Must-Know Cybersecurity Statistics for 2020, Software Company Varonis, 2020, p 1. https://www.varonis.com

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

ცხრილი 4 - მსოფლიოს წამყვანი სამეცნიერო-საკონსულტაციო კომპანია „Gartner“-ის 2017-2018-2019 წლის მონაცემები კიბერუსაფრთხოების ხარჯებთან დაკავშირებით წყარო: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

რაც მიაღწევს **10,5 ტრილიონ აშშ დოლარს** 2025 წლისთვის[33]. ეს კი იძლევა პასუხს იმაზე, რომ კიბერომებისა და კიბერშეტევების ტენდენცია მასშტაბურ სახეს იძენს და ასევე განიცდის ტრანსფორმაციას.

რუსეთს აქვს დიდი შესაძლებლობები კიბერომის თვალსაზრისით და არაერთი მოვლენა ადასტურებს ამას. რუსეთმა გამოიყენა კიბერიარაღი საქართველოზე 2008 წლის ომის დროს. 2019 წელს იგივე მეთოდით კიბერშეტევები განახორციელა საქართველოს სამთა-

33 Morgan S. “Cybercrime To Cost The World $10.5 Trillion Annually By 2025”, 2022. p. 1, https://cybersecurityventures.com/

ვრობო უწყებების ვებ-გვერდებსა და სატელევიზიო ინფრასტრუქტურაზე. უცხოური მედიის ცნობით, 2020 წლის გაეროს უშიშროების საბჭოს დახურულ სხდომაზე ამერიკის შეერთებულმა შტატებმა, ბრიტანეთმა და ესტონეთმა აღნიშნული ფაქტი შეაფასეს რუსეთის მხრიდან წარმოებულ კიბერშეტევად. იგივე ხელწერა შეინიშნება 2014 წლის დასაწყისში უკრაინაზე თავდასხმისას[34].

კიბერომის კონცეფცია - 21-ე საუკუნის საერთაშორისო უსაფრთხოების სისტემა

ჩვენ ვხედავთ ფიზიკურ ინსტრუმენტებს, როგორებიცაა - კომპიუტერები, კაბელები, მობილურები. ინსტრუმენტები ურთიერთქმედებენ ვირტუალურ და არარეალურ სფეროში. ეს ხელს უწყობს დედამიწის ერთი წერტილიდან ომის წარმოებას დედამიწის მეორე წერტილში. დამნაშავის ამოცნობა ყოველთვის ვერ ხერხდება. კიბერომი ხშირად წარმოადგენს კონცეპტუალურ ჩარჩოს, რომელიც დაკავშირებულია ომის ტრადიციულ წარმოებასთან - მოიცავს ძალის დემონსტრირებას, ფიზიკურ ზიანს და ძალადობას. რაც დრო გადის, მით მნიშვნელოვანი ხდება იმის დაზუსტება, თუ რა ტიპის კიბერშეტევას უნდა ეწოდოს კიბერომი. ამ ტიპის განსაზღვრება მნიშვნელოვანია კიბერომთან დაკავშირებული საკითხების მოგვარებისას, რაც ხან კინეტიკურ, ხან არაკინეტიკურ თავდასხმებს გულისხმობს. ჩვენ უკვე განვიხილეთ კიბერშეტევისა და კიბერომის განსხვავებაზე - მსოფლიო მასშტაბით მრავალი მცდელობა იყო, ზუსტად განესაზღვრათ კიბერომის არსი კონცეპტუალურ დონეზე, მაგალითად, ნატოს „კიბერთავდაცვის სფეროში თანამშრომლობის უნარების ცენტრის“ ხელმძღვანელობით შეიქმნა **„ტალინის სახელმძღვანელო“**, სადაც საერთაშორისო სამართლის კანონების მიხედვით არის განხილული კიბერომებში გამოყენებული კანონდარღვევები. თუმცა იგი

34 Evansky B. US, UK and Estonia call out Russia over cyber attacks against Georgia in UN Security Council first, Fox News Channel, 2020, p 1. https://www.foxnews.com

არ წარმოადგენს ნატოს პოლიტიკურ, ოფიციალურ დოკუმენტს. ამ შემთხვევაში სირთულე ის არის, რომ ნაციონალური სახელმწიფოები და არასახელმწიფო აქტორები ყოველთვის არ იცავენ კანონებს. ვფიქრობთ, **„ტალინის სახელმძღვანელოში“** ზოგიერთი თემა ზოგადი, ზედაპირული და კიბერსივრცის თეორიულ განმარტებებთან შეუთავსებელია, საჭიროებს დახვეწას. მაგალითად, ამ სახელმძღვანელოში კიბერომი გაიგივებულია კიბერშეტევასთან - ნათქვამია, რომ ის წარმოადგენს შეტევით ან თავდაცვით ოპერაციას, რომელმაც შეიძლება გამოიწვიოს ადამიანის სიკვდილი, დაზიანება ან ობიექტების განადგურება[35].

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

როდესაც კიბერომის კონცეფციაზე ვსაუბრობთ და უსაფრთხოების საკითხს ვეხებით, აუცილებლად უნდა განვიხილოთ ჩრდილოატლანტიკური ალიანსის კონტექსტში - უსაფრთხოება და კიბერთავდაცვა უშუალოდ უკავშირდება ნატოს. კიბერთავდასხმებისგან თავდაცვის განმტკიცების აუცილებლობა ნატოში გაწევრიანებულმა ქვეყნებმა პირველად 2002 წელს პრაღაში გამართულ სამიტზე განიხილეს. მას შემდეგ კიბერუსაფრთხოება გახდა ნატოს

35 Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict, Information Technology Company ZDnet, 2018, p 1. https://www.zdnet.com

დღის წესრიგის მნიშვნელოვანი კომპონენტი. 2008 წელს მიიღეს პირველი კიბერთავდაცვის პოლიტიკური დოკუმენტი. 2012 წლიდან დღემდე აქტიურად მიმდინარეობს ნატოს თავდაცვის სისტემაში კიბერუსაფრთხოების ინტეგრაციის პროცესი. 2014 წელს **უელსის სამიტზე** მოკავშირეებმა კიბერთავდაცვა კოლექტიური თავდაცვის ძირითადი ნაწილი გახადეს და განაცხადეს, რომ კიბერშეტევამ შეიძლება გამოიწვიოს ნატოს ხელშეკრულებაში განსაზღვრული კოლექტიური თავდაცვის მე-5 მუხლის გამოყენება.

2016 წელს **ვარშავის სამიტზე** ალიანსის წევრმა ქვეყნებმა ინფორმაციული და საკომუნიკაციო ქსელის უსაფრთხოება ერთ-ერთ ძირითად თავდაცვით სფეროდ აღიარეს და შეთანხმდნენ, რომ კიბერსივრცეში **ნატომ** ისევე ეფექტურად უნდა დაიცვას თავი, როგორც ხმელეთზე, ზღვასა და ჰაერში. კიბერუსაფრთხოების სფეროში **ნატოს** ძირითადი პარტნიორია **ევროკავშირი**, რომელთანაც ალიანსმა 2016 წლის თებერვალში **ურთიერთდახმარებისა და თანამშრომლობის ტექნიკური ხელშეკრულება გააფორმა[36].**

მთავარი საკითხები, რაც **ვარშავის სამიტზე** განიხილეს, ეს იყო, როგორ უნდა გამოყოფილიყო კიბერუსაფრთხოებასთან დაკავშირებით რესურსები საუკეთესო ეფექტის მისაღწევად - აღიარეს, რომ ამ პრობლემის მოსაგვარებლად დიდი რესურსები იყო საჭირო. ასევე, კითხვები იყო იმასთან დაკავშირებით, თუ რა თანხა უნდა დახარჯულიყო, რა იქნებოდა ინვესტიციის მინიმალური დონე? მაგალითად, 2014 წლიდან, საფრანგეთში **“Pacte Défense Cyber”**-ის ბიუჯეტი მოიცავდა 1 მილიარდ ევროს კიბერთავდაცვისთვის. 2016 წელს დიდმა ბრიტანეთმა გამოაცხადა, რომ კიბერუსაფრთხოების პროგრამის გასამყარებლად 1,9 მილიარდი გირვანქა სტერლინგი გამოყო[37].

36 Karasev P. NATO’s Cyber Defense Evolution - NATO’s New Digital Wall, Russian Council RIAC, 2016, p 1. https://russiancouncil.ru

37 Pennetier M. France to invest 1 billion euros to update cyber defences, Media News Reuters, 2014, p 1. https://www.reuters.com

2018 წელს **ბრიუსელის სამიტზე** მოკავშირეები შეთანხმდნენ ახალი კიბერსივრცის ოპერაციების ცენტრის შექმნაზე. საერთო გამოწვევების გათვალისწინებით, ნატო და ევროკავშირი აძლიერებენ თანამშრომლობას კიბერთავდაცვის სფეროში, განსაკუთრებით ინფორმაციის გაცვლაში. ტარდება ერთობლივი ტრენინგები და კვლევები[38]. ცალკე აღსანიშნავია ამერიკის შეერთებული შტატების დამსახურება,

ბარაკ ობამა (1961)

რომელიც არ იშურებს ძალისხმევას, რათა შეიმუშაოს კიბერუსაფრთხოებასთან დაკავშირებით ახალი რეგულაციები და ასევე არ იშურებს თანხებს. აშშ-ის ბიუჯეტში კიბერუსაფრთხოებასთან დაკავშირებით ხარჯები ყოველწლიურად იზრდება, 2015 წელს **ბარაკ ობამას** ადმინისტრაციამ გამოყო 14 მილიარდი დოლარი ოფიციალურად, შემდეგ კი გაჩნდა ინფორმაცია, რომ დაიხარჯებოდა გაცილებით მეტი[39].

მსოფლიო მასშტაბით თავდაცვითი ხარჯები დღითი-დღე მატულობს, მაგრამ აშშ-ის ფინანსები შთამბეჭდავია. ცნობილია, რომ 2021 წლისთვის აღნიშნულმა სფერომ 18,8 მილიარდი დოლარით დაფინანსდებას მიაღწია[40].

2022 წლის 30 მარტს **ბაიდენის** ადმინისტრაციამ 2023 წლის ფისკალური ბიუჯეტი გამოაქვეყნა, რომელშიც 11 მილიარდი აშშ დოლარია გამოყოფილი სამოქალაქო კიბერუსაფრთხოების ხარჯებისთვის, ეს 11%-ით მეტია წინა წელთან შედარებით.

შემოთავაზებული ბიუჯეტი ითვალისწინებს 175 მილიონ აშშ დოლარს კერძო საკუთრებაში არსებული კრიტიკული ინფრასტრუქ-

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

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

40 Department of Homeland Security Statement on the President's Fiscal Year 2021 Budget, Homeland Security, 2020, p 1. https://www.dhs.gov

ჯო ბაიდენი (1942)

ტურის მდგრადობის გაუმჯობესებისთვის. ასევე გაწერილია ხარჯები, კიბერუსაფრთხოების მრჩეველთა კომიტეტისთვის **(CISA)**, კიბერუსაფრთხოების საბჭოსთვის და საბჭოს პროგრამის მართვის ოფისის შექმნისთვის[41]. ჯერ კიდევ 2007 წელს შეერთებული შტატების სამხედრო-საჰაერო ძალებში შეიქმნა კიბერსარდლობა, რომელმაც 2008 წლის ბოლომდე იარსება, შემდეგ კი ეს ფუნქციები გადაეცა სამხედრო-საჰაერო ძალების კოსმოსურ სარდლობას[42].

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

1. **ეკონომიკა** - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ღია და ლიბერალური ბაზარი;
2. **ეროვნული ქსელის დაცვა** - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა;
3. **სამართალებრივი მხარე** - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება;
4. **სამხედრო სფერო** - უსაფრთხოების თანამედროვე გამოწვევებზე მზადყოფნა;
5. **სამთავრობო ინტერნეტის ქსელი** - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება;

41 Jones D., ,,Biden administration's FY 2023 budget includes 11% increase for cyber", Cybersecurity Dive, 2022. p. 1. https://www.cybersecuritydive.com/news/biden-2023-budget-cybersecurity/621264/#:~:text=The%20budget%20earmarks%20%242.5%20billion,after%20Congress%20appropriated%20additional%20funding.

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

6. **საერთაშორისო განვითარება** - უსაფრთხოების ორგანიზება, საერთაშორისო კომპეტენციების განვითარება და ეკონომიკური აყვავება;
7. **თავისუფლება ინტერნეტში** - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა[43].

რამდენი სახის კონცეფცია შეიძლება არსებობდეს დღევანდელ მსოფლიოში? გარდა იმისა, რომ მნიშვნელოვანი კონცეფციები გააჩნიათ აშშ-ს, ევროკავშირს, ნატოს, ყველა ქვეყანას აქვს საკუთარი სამოქმედო ეროვნული გეგმა, ყველაზე საყურადღებოდ მაინც 2010 წელს **ლისაბონის სამიტზე** დამტკიცებული ახალი სტრატეგიული კონცეფცია[44]. ითვლება, რომლის თანახმადაც ამერიკის შეერთებულმა შტატებმა ჩამოაყალიბა კიბერსარდლობა. ეს იყო პასუხი რუსეთის ქმედებებზე. **ვლადიმერ პუტინი** მოვიდა თუ არა ხელისუფლებაში, დაამტკიცა საინფორმაციო უსაფრთხოების ახალი დოქტრინა[45], რომლის სტრატეგია იყო ის, რომ ხელისუფლებას მიანიჭა საინფორმაციო და მედიაქსელებზე კონტროლის უფლებები. **პუტინმა** ასევე ხელი მოაწერა საკანონმდებლო ცვლილებას - საგადასახადო პოლიციას, შინაგან საქმეთა სამინისტროს, კრემლის საპარლამენტო და საპრეზიდენტო დაცვის სამსახურებს, საზღვრის დაცვას და საბაჟო სამსახურს იგივე უფლებები მიენიჭა, რაც მხოლოდ უსაფრთხოების ფედერალურ სამსახურს ჰქონდა.

2017 წლის 18 დეკემბერს გამოქვეყნდა აშშ-ის პრეზიდენტის, დონალდ ტრამპის პირველი **„ეროვნული უსაფრთხოების სტრატეგია“**[46], რომელიც საფუძვლად დაედო სტრატეგიულ დოკუმენტებს, როგორიცაა აშშ-ის თავდაცვის დეპარტამენტის **„ეროვნული თავდაცვის**

43 Inter National Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, The White House, 2011, pp 3-24. https://www.hsdl.org

44 Edited by Jens Ringsmose and Sten Rynning, NATO’s New Strategic Concept: a Comprehensive Assessment, DIIS. Danish Institute for International Studies, Copenhagen, NATO, 2011, pp 23-43.

45 Information Security Doctrine of The Russian Federation, Moscow: Russian Federation, 2000, pp 1-32.

46 National Security Strategy, Washington: United States governments, 2017, pp 1-2.

სტრატეგია“. სტრატეგია ეფუძნება ოთხ მნიშვნელოვან ეროვნულ ინტერესს:

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

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

„ამერიკის შეერთებული შტატებისათვის რუსეთი ეგზისტენციალურ საფრთხედ აღიქმება. რუსეთი ცდილობს, აღიდგინოს დიდი სახელმწიფოს 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“.[47]

დეკანი ჩენგი

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 მასშტა-

47 “ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია”, ამერიკის შეერთებული შტატების საელჩო საქართველოში, 2017, გვ. 1. https://ge.usembassy.gov

ბით პოზიციების გაუმჯობესებას. მათ გააცნობიერეს ინფორმაციის კონტროლის მნიშვნელობა, როგორც ძალაუფლების შენარჩუნების ერთ-ერთი ძლიერი ელემენტი. **ჩენგი** ასევე ყურადღებას ამახვილებს ომის სახეობების განვითარებაზე:

„ტექნოლოგიების განვითარებამ, როგორც ეკონომიკასა და საზოგადოებაზე, ასევე ომის ბუნებაზე მოახდინა გავლენა. ისტორიულად ომი ვითარდებოდა, კაცობრიობამ ხმლები, შუბები და სხვა სახის „ცივი იარაღი“ განავითარა, ანუ შეცვალა თოფებით, ყუმბარებით, ავტომატებით და ა.შ. დღეს კი კაცობრიობა, ტექნოლოგიების განვითარების ხარჯზე „ცხელი იარაღიდან“ „რბილ ძალამდე“ მივიდა“[48]. 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[49].

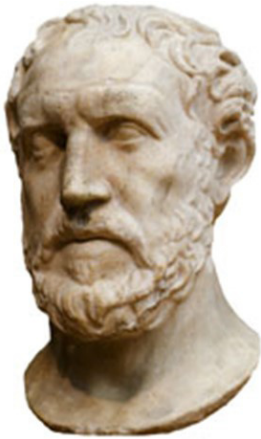
როდესაც აშშ-ის სტრატეგიაში საუბარია ამერიკის გავლენის გაზრდაზე, აქვე თვალშისაცემია, თუ როგორ ფაქიზად უდგება თეთრი სახლი საერთაშორისო ურთიერთობებს, თუმცა ძნელი სათქმელია, რამდენად იქნება რეალური, როცა საქმე გვაქვს რუსეთთან, რომლისთვისაც პოლიტიკა და ეთიკა, პირობის შესრულება და სამართალი ძალიან შორსაა.

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

49 “ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია”, ამერიკის შეერთებული შტატების საელჩო საქართველოში, 2017, გვ. 1. https://ge.usembassy.gov

თავი მეორე
კონფლიქტების ტრანსფორმაცია ახალი გეოპოლიტიკური წესრიგის პირობებში

თემას განვიხილავთ **პოლიტიკური რეალიზმის თეორიაზე** დაყრდნობით. რეალიზმი დიდი ხანია დომინირებს პარადიგმად საერთაშორისო ურთიერთობების სფეროში და ემყარება ზოგად ვარაუდებს საერთაშორისო პოლიტიკის შესახებ. მაგალითად, იმას, რომ სახელმწიფოები არიან ყველაზე მნიშვნელოვანი მოქმედი პირები, როგორც დამოუკიდებელი ერთეულები საერთაშორისო სისტემაში, არ გააჩნიათ ცენტრალიზებული ავტორიტეტი და აქვთ საკუთარი ინტერესები, რათა უზრუნველყონ ძალა და უსაფრთხოება. ამ მეთოდოლოგიის არსი არის მნიშვნელოვანი კიბერუსაფრთხოების სფეროში. **პოლიტიკური რეალიზმის თეორიის** მნიშვნელობა დიდია **საერთაშორისო კიბერპოლიტიკაში**. ამ შემთხვევაში ის ცალსახად უკავშირდება კიბერუსაფრთხოებას. ისტორიულად, **პოლიტიკური რეალიზმის თეორიის საფუძვლები** შეიძლება მოვიძიოთ **თუკიდიდეს** მიერ **პელოპონესის ომის** აღწერილობაში (ძვ.წ. V საუკუნე), სადაც მან ხაზი გაუსვა საერთაშორისო პოლიტიკის ამორალურ ხასიათს და ძალაუფლების მნიშვნელობას გადარჩენისთვის.



თუკიდიდე (დაახლოებით დ. ძვ. წ. 465/460/455 - გ. ძვ. წ. 400/395)

საერთაშორისო ურთიერთობებში ამ თეორიის ჩამოყალიბება

ჰანს მორგენთაუ (1904-1980)

შეიძლება ძირითადად **ჰანს მორგენთაუს** (1948) დამსახურება იყოს, რომელიც ყურადებას ამახვილებს ძალაუფლებისთვის ბრძოლაზე დამოუკიდებელ სახელმწიფოებს შორის[50].

პოლიტიკური რეალიზმის თეორიის მიმდევრების **პაულ დ. სენეზის** და **ჯონ ა. ვასქეზის (Paul D. Senese and John A. Vasquez)** მტკიცებით, არსებობს ფაქტორები, რაც ზრდის საფრთხეებს - მაგალითად სამხედრო შენაერთები, კავშირები, გაერთიანებები, ალიანსები, ხშირად არაპროდუქტიულია და ზრდის კონფლიქტის ალბათობას[51].

ამის მიუხედავად, უსაფრთხოების და კონფლიქტის საკითხებზე ფოკუსირებით, **რეალიზმი**, როგორც ჩანს, არის ბუნებრივი თეორია კიბერუსაფრთხოების მწვავე საკითხების გარკვევაში. ზოგადად, კიბერკონფლიქტის შესწავლა მაშინ დაიწყო, როდესაც **ჯონ არკილამ** და **დევიდ რონფელდტმა (John Arquilla, David Ronfeldt)** განავითარეს **"კიბერომის"** და **"ინტომის"** კონცეფციები და იწინასწარმეტყველეს ომის ტრანსფორმაცია **ICT**– ის სწრაფი წინსვლის შესაბამისად[52].

რეალიზმის მიმდევრები, **ბრენდონ ვალერიანო** და **რაიან კ, მანესი (Brandon Valeriano and Ryan C. Maness)** საკითხს ასე განიხილავენ, კონფლიქტის ეს ფორმა ხდება **კიბერსივრცეში** და გულისხმობს "კიბერსივრცეში გამოთვლითი ტექნოლოგიების გამოყენებას ბოროტი ან/და დესტრუქციული მიზნებისთვის, სუბიექტებს შორის დიპლომატიური და სამხედრო ურთიერთქმედების გავლენის შეცვლის მიზნით"[53].

50 Karpowicz W. Political Realism in International Relations, Stanford Encyclopedia of Philosophy, 2017, p 1, https://plato.stanford.edu

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

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

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

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

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

პოლიტიკური რეალიზმის კლასიკური გაგებით, შეიარაღების გაუმჯობესება ზრდის ომის ალბათობას. **ბარნი გლეიზერის** აზრით, სამხედრო დანაზოგი რევიზიონისტული ძალაუფლების შეკავების აუცილებელი საშუალებაა[54], ამ შემთხვევაში ისმება კითხვა: გადაიზ-

54 Glaser B. Grounded Theory: The Philosophy, Method, and Work, Florida:

რდება თუ არა უსაფრთხოების კონკურენცია რეალურ კონფლიქტში? გამოიწვევს თუ არა კიბერშეიარაღების გაზრდა ახალ კონფლიქტებს?

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

არსებობს მოსაზრება, რომ კიბერსივრცესთან მიმართებაში, სუსტი სახელმწიფოები კიდევ უფრო აძლიერებენ ძლიერ სახელმწიფოებს და ახდენენ სისტემაში განაწილების კონფიგურაციას. მაგალითად, დიდი სკანდალი გამოიწვია ჩრდილოეთ კორეაში ათასობით ჰაკერის მომზადებამ, ასევე ჩინეთის აქტიურობამ, რომელიც ბრალდებულია **აშშ**-ის წინააღმდეგ მუდმივ კიბერჯაშუშურ კამპანიასა და **ირანის ისლამური სახალიფოს** კიბერომის ტაქტიკის დახვეწაში. ბუნებრივია, მოწინავე ქვეყნები ყველაზე მეტად არიან დამოკიდებულნი ციფრულ ინფრასტრუქტურაზე და შესაბამისად, ასევე არიან დაუცველები[55]. თუმცა **ჯონ ლინდსი** ამტკიცებს, რომ მხოლოდ ტექნოლოგიურ ზესახელმწიფოს აქვს ყველაზე დახვეწილი კიბერშეიარაღების განვითარების შესაძლებლობა[56].

კიბერსივრცე გახდა ახალი საერთაშორისო ბრძოლის ველი. ინტერნეტი შესანიშნავად ერგება უსაფრთხოების რეალისტურ მო-

---

BrownWalker Press, 2011, pp 175-187.

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

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

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

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

ბოლო დროის დაკვირვებები და მაგალითები გვიჩვენებს, რომ ნებისმიერ ქვეყანაზე ეკონომიკური ზეწოლა უფრო ადვილია, ვიდრე სამხედრო ლაშქრობა. ამის ნათელი მაგალითია აშშ-ისა და დიდი ბრიტანეთის მიერ სანქციების დაწესება კუბისთვის, სერბეთისა და ბელორუსისთვის, თუნდაც რუსეთისთვის სანქციების დაწესება ევროკავშირის მიერ. პოლიტიკური მიზნების მისაღწევად აღარ არის აუცილებელი საომარი მოქმედებების წარმოება. თუმცა მიზანსაც გააჩნია, თუ მიზანი ტერიტორიის ოკუპაცია ან ბუფერული ზონის შექმნაა, მაშინ შეიარაღებული ძალების გამოყენების გარეშე ეს ვერ მოხდება. ამ მხრივ გვაქვს მაგალითები უკრაინასა და საქართველოში., სადაც რუსეთმა სამხედრო ძალებით და კიბერომის დახმარებით მოახდინა ტერიტორიების ანექსია.

ვირტუალური საფრთხე და ასიმეტრიული სამხედრო გამოწვევები

მსოფლიოში არსებობს ომის საწარმოებელი ხუთი სივრცე - **ჰაერი, ხმელეთი, ზღვა, კოსმოსური სივრცე** და **კიბერსივრცე**. ვირტუალურ საფრთხეებში მხოლოდ კიბერომები, ფსიქოლოგიური ტერორი, ციფრული ვირუსები და ჰაკერული თავდასხმები არ შედის, ვირტუალური საფრთხე მოიცავს საინფორმაციო და დეზინფორმაციულ მანიპულაციებსაც, ასევე გლობალურ ინტერნეტ ბაზარს, რომელიც შავი ბაზრის სახელით არის ცნობილი **(Darknet)**. პირველ რიგში გამოვყოთ **საინფორმაციო ომი**, რომელიც მოიცავს საინფორმაციო ტექნოლოგიების გამოყენებას და მენეჯმენტს მოწინააღმდეგეზე უპირატესობის მოსაპოვებლად. იგი შეიძლება გამოყენებულ იქნას ტაქტიკური ინფორმაციის მოსაპოვებლად, დეზინფორმაციისა და პროპაგანდის გავრცელებაში, რათა მოხდეს საზოგადოების ან მოწინააღმდეგის დემორალიზება. შეიძლება იქნას გამოყენებული მანიპულაციისთვის, ასევე შეუშალოს ხელი რეალური ინფორმაციის გავრცელებას.

საინფორმაციო-პროპაგანდისტული ომის ფენომენი ახალი არ გახლავთ, ის ძველი მეთოდია. უბრალოდ იცვლებოდა და ალბათ მომავალშიც შეიცვლება (პროგრესირდება) ტექნოლოგიების განვითარებასთან ერთად. **პროპაგანდა** - გულისხმობს ნებისმიერი სა-

კომუნიკაციო ფორმის გეგმაზომიერ გამოყენებას, ადამიანთა გონებაზე, ქცევასა და ემოციებზე ზემოქმედების მიზნით. ეს საშუალება ბევრი ადამიანის რამეში დარწმუნებისთვის ყველაზე ეფექტურ და გავრცელებულ საშუალებად მიიჩნევა, რომელსაც პოლიტიკურ საქმიანობას უკავშირებენ. სადაზვერვო სამსახურები პროპაგანდას ისტორიულად დიდიხანია იყენებენ. **პროპაგანდისტული მიმართულების** მთელი სიძლიერე გამოვლინდა **მეორე მსოფლიო ომის** პერიოდში და აქტუალურია დღემდე. ძნელი დასაჯერებელია, მაგრამ ფაქტია, როდესაც მეორე მსოფლიო ომი დასრულდა, გერმანიაში ბევრი რიგითი მოქალაქე აცხადებდა: **„დიახ, ადოლფ ჰიტლერი დამნაშავეა, ცოტა გადააჭარბა, მაგრამ კარგი უფრო მეტი გააკეთა, აღგვიდგინა ღირსება და დაგვიგო ავტობანები“.**[57]


პოლ ჯოზეფ გებელსი (1897-1945)

მეტიც, პოსტჰიტლერულ გერმანიაში იმდენად ძლიერი იყო **გებელსის** იდეოლოგიისა და პროპაგანდის გავლენა, რომ 1948 წელს **ნიურნბერგის** სასამართლო პროცესებზე მოწმეები არ გამოდიოდნენ.[58] 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, პრესა, იყო იდეოლოგია, იყო მოსახლეობაში გაჩაღებული აგიტაცია-პროპაგანდა, იყო ზეწოლა იარაღის ქვეშ. ამ მხრივ შეგვიძლია ვთქვათ, რომ რუსეთს დიდი საინფორმაციო, პროპაგა-

57 Jaffe E. How Highway Construction Helped Hitler Rise to Power, Bloomberg City Lab, 2014, p 1. https://www.bloomberg.com

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

ნდისტულ-დეზინფორმაციული ისტორია აქვს. ტექნოლოგიური რევოლუციების ეპოქაში ამ საქმიანობამ უფრო ეფექტური ხასიათი მიიღო. **რუსული პროპაგანდა** არ არის სიმართლეზე ორიენტირებული, თუმცა ეს არ ნიშნავს იმას, რომ ყველაფერი ტყუილია. აქ გვაქვს შერეული მეთოდი, როდესაც სიმართლეში შერეული დეზინფორმაცია ვრცელდება.

არის შემთხვევები, როდესაც მთლიანად დეზინფორმაციასთან და **„ფეიკ-ნიუსთან“** გვაქვს საქმე. 2014 წლის 11 სექტემბერს გავრცელებული **ფეიკ-ინფორმაცია**, რომელიც გვამცნობდა, რომ **ლუიზიანაში** არსებული **ქიმიკატების** საწარმო აფეთქდა.[59]

იმ დროისთვის ეს ინფორმაცია სარწმუნო ჩანდა, თითქმის ყველა სოციალური ქსელი მოიცვა. საერთოდ, ყალბი ახალი ამბავი სწრაფად ვრცელდება და იოლად დასაჯერებელი ხდება. მით უმეტეს, როცა ინფორმაციას ავრცელებს არა ერთი, არამედ რამდენიმე მედიასაშუალება. ამ შემთხვევაში მნიშვნელოვანია საზოგადოების გაფრთხილება მოსალოდნელი დეზინფორმაციის თაობაზე. ზოგადად მოგვიწოდებენ, რომ გადავამოწმოთ ფაქტები, ვნახოთ რამდენიმე წყარო, მაგრამ მასასთან მიმართებაში ეს არაეფექტურია - ფაქტების გადამოწმება მოითხოვს დროსა და ცოდნას. როდესაც დასტურდება, რომ ინფორმაცია იყო ყალბი, უკვე ჩავლილი ამბავია, თავის მართლება და უარყოფა შედარებით არაეფექტურია, უსარგებლოა. თუმცა სხვა გზაც არ არსებობს. საქართველოში კრემლის პროპაგანდის ძირითადი საყრდენი მედიასაშუალებები და სოციალური ქსელებია. მინიმუმ, ერთი ტელევიზია, რამდენიმე ინტერნეტ-ტელევიზია, ბეჭდური გამოცემა და ვებ-გვერდი გამოირჩევა ანტიდასავლური **„მესიჯ-ბოქსით“**, ისინი ინფორმაციის გავრცელებისას ძირითადად ეყრდნობიან რუსულ წყაროებს. თვალშისაცემია რუსული პროპაგა-

59 Szal A. Report: Russian 'Internet Trolls' Behind Louisiana Chemical Explosion Hoax, Industrial Media - Manufacturing, 2015, p 1. https://www.manufacturing.net

ნდის გამავრცელებლების მიერ სოციალური ქსელების აქტიური გამოყენებაც, როდესაც ხდება დეზინფორმაციის ან ანტიდასავლური ნარატივის შემცველი ინტერნეტმასალების ვირუსული გავრცელება. საზოგადოებრივი აზრის არაერთი გამოკითხვა აჩვენებს, რომ საქართველოში ინფორმაციის მიღების ძირითადი წყარო ტელევიზიაა. **ეროვნულ-დემოკრატიული ინსტიტუტის (NDI)** 2016 წლის გამოკითხვის თანახმად, საქართველოს მოსახლეობის 77% პოლიტიკისა და მიმდინარე მოვლენების შესახებ ინფორმაციის მიღების პირველწყაროდ ტელევიზიას ასახელებს. გამოკითხვები ასევე აჩვენებს, რომ ქართველი ტელემაყურებლების თითქმის ნახევარი (47%) ქართული არხების გარდა უცხოურ არხებსაც უყურებს. ყველაზე პოპულარული უცხოური არხები კი რუსულია **(HTB, ORT და RTR)**.[60] აღსანიშნავია, რომ არის ქვეყნები, სადაც აქტიურად აკონტროლებენ ინტერნეტსივრცესა და საკომუნიკაციო ქსელებს. მაგალითად, **ჩინეთი**, რომელიც ასევე აკონტროლებს ტელევიზიებს და სოციალურ მედიას. ცნობილია, რომ **ჩინეთის** მთავრობას დაქირავებული ჰყავს ორ მილიონამდე ადამიანი, ისინი ინსტრუქციის მიხედვით წერენ კომენტარებს და ზეგავლენას ახდენენ, მართავენ საზოგადოებრივ აზრს. ამასთან დაკავშირებით **კარი კინგის, მარგარეტ რობერტსისა** და **ჯენიფერ პანის** კვლევაც გამოქვეყნდა, რომელსაც საფუძვლად უდევს ინტერნეტში გაჟონილი სამთავრობო იმეილები. აღნიშნულ კვლევაში ნათქვამია, რომ ჩინეთის მთავრობა წელიწადში **448 მილიონი** კომენტარის ფაბრიკაციას ახდენს. სოციალურ ქსელებში დაქირავებულები ხშირად განადიდებენ **ჩინეთს** და **ჩინეთის კომუნისტურ პარტიას**, ისინი ცდილობენ, ხალხს ყურადღება სხვა, ნაკლებად მნიშვნელოვან საკითხებზე გადაატანინონ.[61]

60 ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., "კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016, გვ. 5-23.

61 Waddell K. 'Look, a Bird!' Trolling by Distraction, The Atlantic Magazine, 2017, p 1.

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

1. **Surface Web** - ნიშნავს ზედაპირულ ქსელს. ასევე მოიხსენიებენ **Clear Web**-ის სახელითაც **(სუფთა ვები)**. ეს ქსელი იძებნება სტანდარტული ვებსაძიებო სისტემებით. ქსელი არის ინდექსირებული საძიებო სისტემების მიერ. ამ ქსელში შედის **„Google“**-ი, **„Facebook“**-ი, **„Yahoo“**, **„Wikipedia“**, **„Instagram”**-ი და ა.შ.
2. **Deep Web** - ღრმა ქსელი, მისი **შინაარსი შეიძლება იქნას ნაპოვნი პირდაპირ URL-ს ან IP მისამართით**. თუმცა შესაძლოა, ვებ-საიტების სანახავად საჭირო გახდეს პაროლის ან უსაფრთხოების სხვა რეჟიმის გავლა. თუმცა გულისხმობს ჩვეულებრივ გამოყენებას. მაგალითად, როდესაც მომხმარებელს აქვს შეზღუდული წვდომა სხვადასხვა ვებ-გვერდებზე, სადაც საჭიროებს რეგისტრაციას შინაარსის სანახავად. ისეთ საიტებზე, სადაც საჭიროა თანხის გადახდა ელჟურნალის ან ელგაზეთის გადმოსატვირთად. **ამ სივრცეს მიეკუთნება, „Paypal“-ი, „Facebook”-ი, “Twitter”-ი, “Wathsapp”-ი, “Gmail”-ი და ა.შ.**
3. **Dark Web** - ბნელი ქსელი. ასევე ცნობილია, **Darknet**-ის სახელით, როგორც **„დაფარული ქსელი“**. ეს არის სისტემა, რომელიც ხელმისაწვდომია არასტანდარტული პორტების გამოყენებით. **დარქნეტი** განსხვავდება სხვა ქსელებისგან იმით, რომ ფაილის გაზიარება ხდება ანონიმურად, ანუ **IP** მისამა-

https://www.theatlantic.com

რთები საჯაროდ არ არის ხელმისაწვდომი. ამ სივრცეში კომუნიკაცია უკონტროლოა და შეიცავს სხვადასხვა საფრთხეებს. შეგვიძლია პარალელი გავავლოთ იატაკქვეშა არალეგალურ საქმიანობასთან, რაც რეალურ სივრცეში ხორციელდება და **დარქნეტს** შორის, რომელიც ვირტუალურ სივრცეში ხორციელდება. ამ სისტემაში მოხვედრა არ არის იოლი, საჭიროა კონკრეტული პროგრამული უზრუნველყოფა და ავტორიზაცია. **დარქნეტი** შეიძლება ასევე განხილულ იქნას როგორც ალტერნატიური ინტერნეტი, ან ინტერნეტის ბნელი მხარე, ეს უზარმაზარი ქსელია, რომელიც ათასობით არალიცენზირებულ და უკანონო ვებ-გვერდებს აერთიანებს. აქ ხელმისაწვდომია უამრავი რამ - არალეგალურად იარაღის ყიდვა, კლონირებული კარტების შეძენა, ყალბი პასპორტების ყიდვა, მონის გამოწერა, ნარკოტიკების ყიდვა, ქილერის დაქირავება და ა.შ. **დარქნეტში** უამრავი არალეგალური ფორუმი, სოციალური ქსელი და არასტანდარტული ვებ-გვერდებია. ნაშრომში შეგ-

Surface web, Deep web, Dark web-Dark net


კნაფ კენეტი

ნებულად არ განვიხილავთ ამ სისტემაში შესვლის ინსტრუქციას, შეიძლება გაგებული იყოს წახალისებად.

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

„უსაფრთხოების კომპანიები, როგორებიცაა **IBM ISS X-Force, PandaLabs** და **Symantec** აღნიშნავენ კიბერშეტევების ზრდას, მაგალითად, **Symantec**-ის მოხსენების თანახმად, იგი აკვირდება შავი ბაზრის სხვადასხვა ფორუმებს და აღნიშნავს, რომ სავარაუდოდ ფორუმებს უმეტესწილად იყენებენ ჰაკერები, კრიმინალები და კრიმინალური ორგანიზაციები, ისინი ვაჭრობენ სხვადასხვა სახის პროდუქციით. მათ მიზანი კი საბოლოო ჯამში პირადი მონაცემების ქურდობაა. **Symantec**-ის მოხსენებაში მკაფიოდ არის აღნიშნული, რომ შავი ბაზრები წარმოადგენენ სერიოზულ საფრთხეს, როგორც პერსო-

ნალურ, ასევე გლობალურ დონეზე. შავი ბაზრის გამოყენებით სერიოზული საფრთხე ექმნება პერსონალური ინფორმაციის დაცულობას. ჰაკერები ასევე იყენებენ კონკრეტული მომხმარებლებისა და კონკრეტული საიტების წინააღმდეგ, ბრაუზერებზე და ვებ-გვერდებზე კიბერშეტევების განსახორციელებლად“. [62]

თანამედროვე მაღალი ტექნოლოგიების გავლენა

საერთაშორისო უსაფრთხოების პროცესებზე

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

ძალთა ბალანსი, ანუ ძალთა წონასწორობა საერთაშორისო

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

ურთიერთობათა თეორიაში ერთ-ერთი უძველესი და უმთავრესი საკითხია. ამ კონცეფციის თანახმად, სახელმწიფოების ძირითად ამოცანას თვითგადარჩენისა და თვითდამკვიდრებისთვის ბრძოლა წარმოადგენს, ისინი ზრუნავენ უსაფრთხოებასა და დამოუკიდებლობაზე. ხშირად სახელმწიფოები ერთიანდებიან, რათა დაუპირისპირდნენ იმ სახელმწიფოს, ან სახელმწიფოთა ჯგუფს, რომელიც საფრთხეს წარმოადგენს. გამოდის, საერთაშორისო სისტემა, ვუწოდოთ თანამშრომლობა, დაყოფილია სახელმწიფოთა რამდენიმე ჯგუფად, რაც განსაზღვრავს მათთვის მშვიდობას. თანამედროვე ეპოქაში კიბერშესაძლებლობების ასიმეტრიული გამოყენების მაღალმა შესაძლებლობამ დასაშვები გახადა პატარა ქვეყნების მიერ ზეგავლენის მოხდენა მსოფლიოში მიმდინარე პროლიტიკურ პროცესებზე. მიუხედავად ამისა, საერთო ტენდენცია აჩვენებს, რომ ძალაუფლება მაინც დიდი და ძლიერი ქვეყნების ხელთაა. მას შემდეგ, რაც კიბერომი საერთაშორისო პოლიტიკის სტანდარტულ იარაღად იქცა, შეგვიძლია ვთქვათ, თანამედროვე ტექნოლოგიებმა გარკვეულწილად შეცვალა გლობალური უსაფრთხოების მიდგომები. ამ საკითხთან დაკავშირებით მნიშველოვანია, **განვსაზღვროთ ძალთა ბალანსის კონცეფცია** და კიბერტექნოლოგიების გაძლიერების პირობები, რაც გულისხმობს სახელმწიფოთა კიბერშესაძლებლობებს, განვითარებას და დაბალანსებას. აქ იგულისხმება არა მხოლოდ ერთი სახელმწიფოს გაძლიერება თუ გაბატონება კიბერტექნოლოგიების თვალსაზრისით, არამედ თანამშრომლობის სხვადასხვა ეტაპები. ძალთა ბალანსის კონცეფცია გულისხმობს: თუ ერთი სახელმწიფო გაძლიერდება, ისარგებლებს სხვა სახელმწიფოების სისუსტით, რაც გამოიწვევს სუსტი სახელმწიფოების გაერთიანებას თავდაცვის მიზნით. ეს არის ჯაჭვური რეაქცია, რომელიც განვითარდა ტექნოლოგიების განვითარების ფონზე და ხელი შეუწყო კიბერომების წარმოებას. ამან კი ზოგიერთი ქვეყნის უსაფრთხოების საკითხი კითხვის ნიშნის

ქვეშ დააყენა. როგორც წინა თავებში აღვნიშნეთ, **ამერიკის შეერთებული შტატები** განაგრძობს ლამის გაათმაგებული ფინანსების დახარჯვას კიბერშესაძლებლობების გასაძლიერებლად. ეს არც არის გასაკვირი, რადგან **აშშ-ი შეიქმნა ინტერნეტი** და ამ ქვეყანაშივე დაინერგა მრავალი ახალი ტექნოლოგია. საერთოდ, კიბერინსტრუმენტების ფართო სპექტრი პოლიტიკაშიც უზრუნველყოფს სტრატეგიული მოქნილობის სხვადასხვა ვარიანტებს, რაც ადრე თითქმის წარმოუდგენელი იყო. აქვე აღსანიშნავია **რუსეთის** ფაქტორი, რომელიც კიბერშესაძლებლობების თვალსაზრისით ასევე მოწინავე პოზიციებზეა. რას წარმოადგენს რუსული კიბერძალა და რა როლს ასრულებს **ძალთა ბალანსის** თვალსაზრისით? რუსეთი ნამდვილად მუშაობს ინოვაციურად სხვადასხვა კონფლიქტებში. სპეციფიკური გეოპოლიტიკური გარემოდან გამომდინარე, რუსეთმა წარმატებით მოახერხა კიბერშეტევების ადაპტირება საკუთარი ინტერესების გასაფართოებლად. ნაშრომში უამრავი მაგალითი გვაქვს განხილული რუსეთთან მიმართებაში. ერთ-ერთი 2007 წლის კიბერშეტევებია ესტონეთის წინააღმდეგ. ეს იყო მარტივი **DDoS** შეტევა, რომელსაც მნიშვნელოვანი ზარალი არ მოჰყოლია, მაგრამ დადებითად იმოქმედა **ესტონეთისა და ნატოს ურთიერთობის გაძლიერებაზე უსაფრთხოების თვალსაზრისით.** იგივე განმეორდა 2008 წელს **რუსეთ-საქართველოს ომის პერიოდში**, რაც უკვე არაერთხელ აღვნიშნეთ. ასევე - **უკრაინასთან** მიმართებაში, სადაც კიბერშეტევები უფრო „დახვეწილი“ და დამაზიანებელი აღმოჩნდა. მაგალითები

მრავლად გვაქვს, რაც **რუსეთის** გაძლიერებულ კიბერშესაძლებლობებზე მიანიშნებს. **რუსეთის** მიერ განხორციელებული კიბერთავდასხმები უმეტესად გამოყენებულია ასიმეტრიული კონფლიქტის პირობებში. თუმცა 2016 წელს **აშშ**-ის საპრეზიდენტო არჩევნებში ჰაკერების ჩარევა განსხვავებული იყო იმ გაგებით, რომ რუსეთმა არ გამოიყენა კიბერშეტევა, ეს არ იყო სადამსჯელო ღონისძიება, აღნიშნული მიზნად ისახავდა კიბერშესაძლებლობების მოსინჯვას არჩევნებზე ზეგავლენის მოსახდენად. ბუნებრივია, **რუსეთის** შესაძლებლობებსაც აქვს ზღვარი. როდესაც ანხორციელებს კიბერშეტევას

გარკვეული სტრატეგიით, პოტენციურ მოწინააღმდეგეებს შესაძლებლობა აქვთ, მოემზადონ თავდაცვითი მიმართულებით. შეიძლება **რუსეთის** მიერ განხორციელებული კიბერშეტევები **საქართველოსა** და **უკრაინაზე** ჩაითვალოს ექსპერიმენტებად, მაგრამ სწორედ ეს აძლევს **საშუალებას წამყვან ქვეყნებს**, სრულყოფილად შეისწავლონ ე.წ. **რუსული** მეთოდები ტექნოლოგიური თვალსაზრისით. შემდეგ კი უფრო იოლად ხდება თავდაცვითი მექანიზმების გაუმჯობესება. მაგალითად, **საფრანგეთის, იტალიის, ჰოლანდიისა** და **გერმანიის** არჩევნებში **რუსი** ჰაკერების ჩარევა იმდენად ეფექტური არ იყო, როგორც ეს შეიძლება ყოფილიყო წინა შემთხვევებში. აქვე აღსანიშნავია **ჩინეთის** როლი კიბერშესაძლებლობების მიმართულებით. **ჩინეთის** კიბერჯაშუშობის ინტენსიურმა გამოყენებამ თეთრი სახლის ადმინისტრაცია უკიდურესად გააღიზიანა. სწორედ ამ თავდასხმების ხარჯზე მოხდა საიდუმლო მასალების გატანა **ჩინეთის** დაზვერვის მიერ. ერთ-ერთი ყველაზე დამაზიანებელი იყო, როცა აშშ-ის ადმინისტრაციის პერსონალის მართვის ოფისის სისტემაზე მიიტანეს იერიში - 20 მილიონზე მეტი ადამიანის პერსონალური მონაცემი მოიპოვეს.[63]

63 Zengerle P., Megan Cassella M., Millions more Americans hit by government personnel data hack", Media Company Reuters, 2015, p 1. https://uk.reuters.com

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

ამ სახელმწიფოებს ემატება **ჩრდილოატლანტიკური ალიანსი**, რომელიც კიბერუსაფრთხოების თვალსაზრისით, მნიშვნელოვან როლს თამაშობს მსოფლიო მასშტაბით და თანამშრომლობს წევრ თუ არაწევრ ქვეყნებთან. **ნატო ევროკავშირის** დახმარებით ცდილობს ვირტუალურ სივრცეში წარმოქმნილ საფრთხეებთან გამკლავებას, რაც უფრო მეტად აბალანსებს მდგომარეობას, ამცირებს რისკებს და საფრთხეებს. ნათელია, რომ დღეს, კიბერტექნოლოგიების თვალსაზრისით, სისტემა არ გახლავთ ერთპოლუსიანი. ამ შემთხვევაში პოტენციური მოკავშირეების რიცხვი მეტია და უფრო მარტივია პოლიტიკის წარმოებაც. დღევანდელი საერთაშორისო გარემო მრავალპოლარულია სხვადასხვა განზომილებით. შეიძლება იმდენ ფინანსებს არავინ ხარჯავს, რამდენსაც **ამერიკის შეერთებული შტატები**, არც სამხედრო ალიანსს ქმნის არავინ, თუნდაც **ჩინეთი** და **რუსეთი**, მაგრამ ისინი მაინც აძლიერებენ სამხედრო თანამშრომლობას და კოორდინაციას უწევენ საგარეო პოლიტიკას. გასათვალისწინებელია ის ფაქტიც, რომ **აშშ-მ** გააორმაგა ძალისხმევა **ჩინეთის** საპირწონედ მთელ მსოფლიოში, განსაკუთრებით **აღმოსავლეთ აზიაში**. საერთოდ, ჩინეთი განიხილება ნომერ პირველი საფრთხედ **აშშ-ისთვის**. საქმე ეხება გლობალურ პოლიტიკაში **ამერიკის** პირველობას.

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

კიბერომის ფენომენის ასახვა ეროვნული უსაფრთხოების სტრატეგიებში - მითი და რეალობა

ეროვნული უსაფრთხოების სტრატეგია უმნიშვნელოვანეს დოკუმენტს წარმოადგენს ნებისმიერ სახელმწიფოში უსაფრთხო გარემოს შექმნის თვალსაზრისით. წამყვანი ქვეყნების (აშშ-ის, დიდი ბრიტანეთის, რუსეთის, ჩინეთის, ირანის, საფრანგეთის, ესპანეთის) სტრატეგიულ დოქტრინაში კიბერომს მნიშვნელოვანი ადგილი უკავია. საქართველომ კიბერუსაფრთხოების ახალი სტრატეგია 2021 წლის 30 სექტემბერს დაამტკიცა. პროგრამა 2021-2024 წლების პერიოდს მოიცავს. ახალ სტრატეგიაში ყურადღება გამახვილებულია კიბერომებზე, საინფორმაციო ომებზე, კიბერჯაშუშობასა და სახელმწიფო აქტორების მიერ მართულ კიბერშეტევებზე. ასევე დიდი ყურადღება ეთმობა კრიტიკული ინფრასტრუქტურების წინააღმდეგ მიმართულ კიბერშეტევებს. შესაძლოა, კრიტიკული ინფრასტრუქტურის დაზიანებამ მნიშვნელოვანი ზარალი გამოიწვიოს.

საქართველოს ახალ სტრატეგიაში პრიორიტეტულ საკითხებს წარმოადგენს საზოგადოების ცნობიერების ამაღლება და საჯარო თუ კერძო სექტორის კიბერუსაფრთხოების გაძლიერება.

მიზნები და ამოცანები:

მიზანი 1: ინფორმაციული საზოგადოებისა და ორგანიზაციების

კიბერკულტურის განვითარება და შესაძლებლობების გაძლიერება კიბერსივრცეში საფრთხეებსა და ინციდენტებთან გამკლავების მიზნით.

ამოცანა 1.1: კიბერსივრცეში უსაფრთხოდ და დაცულად ფუნქციონირებისთვის სკოლის მოსწავლეებისა და სტუდენტებისთვის საჭირო უნარ-ჩვევების განვითარება და განათლების დონის ამაღლება.

ამოცანა 1.2: კიბერსივრცეში უსაფრთხოდ და დაცულად ფუნქციონირებისთვის კიბერსაფრთხეებისა და რისკების შესახებ ინფორმაციული საზოგადოებისა და ორგანიზაციების ცნობიერების ამაღლება.

მიზანი 2: კიბერუსაფრთხოების მმართველობითი სისტემის მდგრადობა და საჯარო-კერძო თანამშრომლობის გაძლიერება.

ამოცანა 2.1: ეროვნულ დონეზე კიბერინციდენტებისა და კიბერსაფრთხეების დროული გამოვლენის, რეპორტინგისა და მათთან ეფექტიანი გამკლავების სისტემის შექმნა და განვითარება.

ამოცანა 2.2: კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანი სისტემის განვითარება.

ამოცანა 2.3: ჩამოყალიბებული საკომუნიკაციო პლატფორმების გამოყენებით თანამედროვე ტენდენციების, საუკეთესო პრაქტიკისა და კიბერსაფრთხეების შესახებ ინფორმაციის გაცვლა, საერთაშორისო სტანდარტების დანერგვის ხელშეწყობა.

ამოცანა 2.4: ეროვნული კიბერუსაფრთხოების მიზნების განსაზღვრა.

ამოცანა 2.5: კიბერუსაფრთხოების სფეროში კვლევითი საქმიანობის მხარდაჭერა და გაძლიერება.

მიზანი 3: კიბერშესაძლებლობების განვითარება ძლიერი ადამიანური რესურსით და სათანადო ტექნიკური უზრუნველყოფის საშუალებებით.

ამოცანა 3.1: დარგის სპეციალისტების ცოდნისა და კვალიფიკაციის ამაღლება.

ამოცანა 3.2: ეროვნული კიბერშესაძლებლობების გაძლიერება

ტექნიკური უზრუნველყოფის საშუალებებით.

მიზანი 4: კიბერუსაფრთხოების საერთაშორისო ასპარეზზე საქართველოს, როგორც უსაფრთხო და დაცული ქვეყნის როლის გაძლიერება.

ამოცანა 4.1 კიბერსაფრთხეებსა და ინციდენტებთან დაკავშირებულ ინფორმაციაზე წვდომის ზრდა და საერთაშორისო მხარდაჭერის/თანამშრომლობის გაძლიერება.


ჰილარი კლინტონი (1947)

ამოცანა 4.2 საერთაშორისო კიბერსწავლებებსა და კიბერსავარჯიშოებში ჩართულობის უზრუნველყოფა, ცოდნისა და გამოცდილების გაზიარება კიბერუსაფრთხოების გლობალურ დღის წესრიგში წვლილის შეტანისთვის.

ამოცანა 4.3 საერთაშორისო ორმხრივი და მრავალმხრივი ფორმატის პარტნიორობის გაძლიერება.

ასევე ყურადღება უნდა გავამახვილოთ **ნატო-ევროკავშირის** უსაფრთხოების სტრატეგიებზეც. თუმცა მნიშვნელოვანია, განვიხილოთ აგრესორი ქვეყნის უსაფრთხოების სტრატეგია. საინტერესოა, როგორია რუსეთის ხელისუფლების ხედვა გლობალური საფრთხეების კუთხით. რუსეთის ეროვნული უსაფრთხოების დოქტრინის **2015 წლის** ვარიანტში **მე-16** და **მე-17** პარაგრაფებში მთავარ მოწინააღმდეგეებად მოიაზრებიან **აშშ** და **ნატო**, ხოლო **მე-7** პარაგრაფში პირდაპირ არის დაფიქსირებული რუსეთის ფედერაციის როლის ამაღლება მსოფლიო წესრიგის მოწყობის საქმეში.[64]

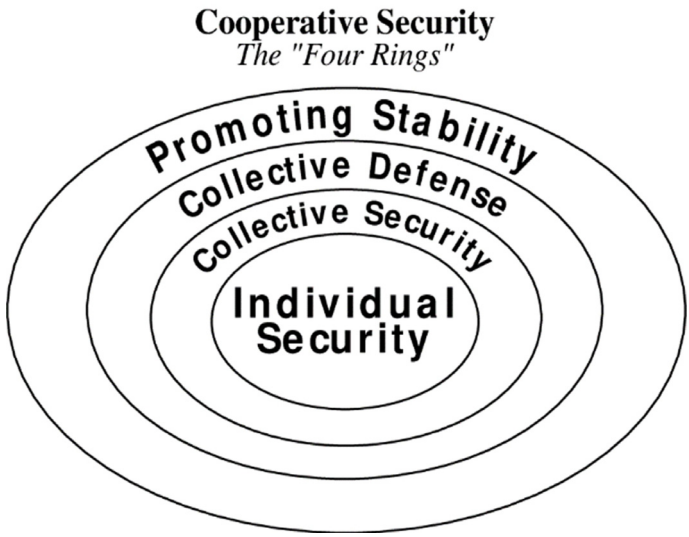

სერგეი ლავროვი (1950)

რუსეთის ფედერაცია ამბობს, რომ ის კი არ წარმოადგენს სხვა ქვეყნებისთვის საფრთხეს, არამედ თავად არის მსხვერპლი

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

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

კონკრეტულად რა წერია აშშ-ის ეროვნული უსაფრთხოების სტრატეგიაში, რომელიც 2017 წლის დეკემბერში გამოქვეყნდა? სტრატეგიის შესავალშივე აღნიშნულია, რომ ამერიკის კეთილდღეობა და



უსაფრთხოება დამოკიდებულია იმაზე, თუ როგორ უპასუხებს **კიბერსივრცეში** არსებულ შესაძლებლობებსა და გამოწვევებს. აქვე აღნიშნულია, რომ კრიტიკული ინფრასტრუქტურა, ეროვნული თავდაცვა და ამერიკელების ყოველდღიური ცხოვრება ეყრდნობა კომპიუტერულ და ინფორმაციულ ტექნოლოგიებს.[65]

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

„კოლექტიური თავდაცვითი“ მოდელი ეკუთვნის ამერიკელ პოლიტოლოგს **რიჩარდ კოენს**, მან შეიმუშავა **„თანამშრომლობითი უსაფრთხოების“** კონცეფცია, რომელიც იყოფა ოთხ ნაწილად - **ინდივიდუალური უსაფრთხოება, კოლექტიური უსაფრთხოება,**

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

კოლექტიური თავდაცვა და **სტაბილურობის შენარჩუნება**. ინდივიდუალური უსაფრთხოება გულისხმობს ქვეყნის უნარს, დამოუკიდებლად დაიცვას საკუთარი ტერიტორია, გაეროს წესდების 51-ე მუხლის თანახმად, მათ შორის სამხედრო გზით. **კოლექტიური უსაფრთხოება** გულისხმობს ქვეყნების გაერთიანებას საერთო სახის სამხედრო რისკების და გამოწვევების წინააღმდეგ. **კოლექტიური თავდაცვა** ნიშნავს ქვეყნების გაერთიანებას სხვა ქვეყნებისგან თავდაცვის მიზნით, რაც დღეს ნატოს მოდელს უდევს საფუძვლად - ტრანსატლანტიკური სოლიდარობის პრინციპი. **სტაბილურობის მიღწევა** საერთო ძალისხმევით, ეს ნიშნავს და უფრო მეტად არის იდალური ვარიანტი მაღალი დონის კოლექტიური უსაფრთხოების გლობალური სცენარის დროს - მაგალითად, **„ისლამური სახალიფოს“** წინააღმდეგ.[66]

რეალობა გვიჩვენებს, რომ ეს კონცეფცია საკმაოდ აქტუალურია XI საუკუნეშიც. უფრო მეტად მნიშვნელოვანი გახადა კიბერტექნოლოგიების განვითარებამ. **„კოლექტიური თავდაცვა“** ნატოს წესდე-

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

ბაში მკაფიოდ არის გაწერილი და წევრ ქვეყნებს ავალდებულებს, დაიცვან ერთმანეთი. კოლექტიური თავდაცვა ნიშნავს, რომ თავდასხმა რომელიმე ერთ მოკავშირეზე ითვლება თავდასხმად ყველაზე - ეს პრინციპი გათვალისწინებულია ვაშინგტონის ხელშეკრულების მე-5 მუხლითაც. **ნატომ** პირველად მე-5 მუხლი აამოქმედა **აშშ-ზე** 11 სექტემბერს ტერორისტული თავდასხმის შემდეგ. კოლექტიური თავდაცვის პრინციპის საკითხი ასევე წამოიჭრა, როდესაც რუსეთმა უკრაინის წინააღმდეგ წამოიწყო სამხედრო აგრესია. 2014 წლის 1-ელ აპრილს ნატოს საგარეო საქმეთა მინისტრმა ალიანსის სამხედრო ხელმძღვანელობას მიმართა, რათა შეემუშავებინათ დამატებითი ზომები კოლექტიური თავდაცვის გასაძლიერებლად.

[67]საერთაშორისო სამართლის თანახმად, სახელმწიფოებს უფლება აქვთ, გამოიყენონ ძალა შეიარაღებული თავდასხმისგან თავის დასაცავად. კიბერშეტევის შედეგად დაზარალებულ სახელმწიფოს უფლება აქვს, კიბერომის კვალიფიკაციის მქონე თავდასხმებს უპასუხოს სამხედრო ძალის გამოყენებით. მიუხედავად იმისა, რომ მსგავსი ფაქტი ჯერ არ მომხდარა, მთავრობები მაინც აქტიურად განიხილავენ ასეთი შესაძლებლობების დარეგულირების საკითხს. მაგალითად, 2014 წელს ნატომ გამოაქვეყნა დეკლარაცია, რომელშიც ნათქვამია, რომ კიბერშეტევების გავლენა შეიძლება ისეთივე მავნე იყოს თანამედროვე საზოგადოებისთვის, როგორც ჩვეულებრივი სამხედრო თავდასხმა. ამავე დეკლარაციაშივე აღნიშნულია, რომ ნატოს წევრ ქვეყანაზე კიბერშეტევამ შეიძლება გამოიწვიოს ჩრდილოატლანტიკური ალიანსის მე-5 მუხლის გამოყენება. ალიანსის სტრატეგიულ კონცეფციაში დიდი ყურადღება ეთმობა პარტნიორობის, თანამშრომლობისა და დიალოგის ფაქტორს. ალიანსი ცდილობს, ევროატლანტიკურ პარტნიორობის საბჭოს წევრებს შორის ყველა საკითხში იყოს ნდობა და გამჭვირვალობა. ეს კი ევროკავშირისა თუ ნატოს არაწევრ ქვეყნებსაც ავალდებულებს, აქტიურად იყვნენ ჩაბმულნი საერთაშორისო უსაფრთხოების პროცესებში. 2016

67 Collective defence - Article 5, NATO, 2019, p 1. https://www.nato.int

წელს ნატოს წევრმა ქვეყნებმა კიბერსივრცე აღიარეს როგორც საომარი მოქმედებების სფერო.[68]

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

ჯააკ ტარიენი (1974)

„ჩვენი სასწავლო პროცესი მოიცავს წელიწადში 17 კურსს. კურსებზე განიხილება და ისწავლება, მაგალითად, კრიტიკული ინფრასტრუქტურის დაცვა, საერთაშორისო სამართალი და კიბერთავდაცვითი ოპერაციების დაგეგმვა“.[69]

კიბერთემის შესწავლის თვალსაზრისით მნიშვნელოვან ობიექტს წარმოადგენს საქართველო, რომელიც გლობალური პოლიტიკური პროცესების შემადგენელ ნაწილს წარმოადგენს. შესაბამისად, საქართველოს ეროვნული კონცეფციის განხილვაც და ქვეყნის კიბერტექნოლოგიური უსაფრთხოების შეფასება-განსაზღვრაც მნიშვნელოვანია. საქართველოს ეროვნული უსაფრთხოების კონცეფცია არის დოკუმენტი, რომლითაც ხელისუფლებამ უნდა იხელმძღვანელოს არა მხოლოდ ექსტრემალურ სიტუაციაში, არამედ დასახოს პრიორიტეტები.

რა არის ქვეყნის პრიორიტეტები? უსაფრთხოება, კეთილდღეობა,

68 Brent L. NATO’s role in cyberspace, NATO, 2019, p 1. https://www.nato.int

69 Riazi T. Know The CCDCOE: Interview with Director Col. Jaak Tarien, NATO Assotiation of Canada - NAOC, 2020, p 1. http://natoassociation.ca

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

"რუსეთის ფედერაციის მიერ საქართველოს ტერიტორიების ოკუპაცია და ოკუპირებული ტერიტორიებიდან რუსეთის ფედერაციის მიერ ორგანიზებული ტერორისტული აქტები, რუსეთის ფედერაციის მხრიდან ახალი სამხედრო აგრესიის რისკი».[70]

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

70 "საქართველოს ეროვნული უსაფრთხოების კონცეფცია", თბილისი: საქართველოს მთავრობა, 2018, გვ. 3-30.

ლისათვის. 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.

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. 5 კომპონენტიდან, რა თქმა უნდა, ყველა მნიშვნელოვანია, მაგრამ მთავარი მაინც ტექნიკური ბაზაა. თუ კვლევის საგანია მხოლოდ მზაობა, მაშინ საქართველოსთვის მიკუთვნებული რეიტინგი დამაჯერებელი იყო. როგორც ჩანს, ამ შემთხვევაში საქმე გვაქვს მხოლოდ ორგანიზაციულ მოწყობასთან, თანამშრომლობის ღიაობასთან და არა დღევანდელ შესაძლებლობასთან. 2017 წელს იუსტიციის სამინისტროში აცხადებდნენ, რომ ამის მიღწევა-შენარჩუნება-განვითა-

რება კომპლექსური საკითხი იყო და სხვადასხვა უწყებები დაუღალავად იშრომებდნენ. ეს უწყებები იყო: **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 არსებობამ და წარმატებულმა მუშაობამ როგორც ადგილობრივ, ისე საერთაშორისო ასპარეზზე. ეს ჯგუფი იუსტიციის სამინისტროს **მონაცემთა გაცვლის სააგენტოს** სტრუქტურის ნაწილი იყო, შემდგომში კი სააგენტო **სმარტ ლოჯიკთან** გაერთიანდა და დაერქვა **ციფრული მმართველობის სააგენტო**, რომელიც პასუხისმგებელია კიბერუსაფრთხოების, ინფორმაციული უსაფრთხოების განვითარება-შენარჩუნებაზე, კიბერინციდენტების წინააღმდეგ მიმართული ღონისძიებების გატარებაზე და ასე შემდეგ.[71]

რა მოხდა ამ კუთხით ბოლო წლებში? კიბერუსაფრთხოების ინდექსით საქართველო მსოფლიოში მე-19 ადგილზე იყო. ინდექსში საქართველოს 100 სარეიტინგო ქულიდან 64.94 ქონდა. ციფრული განვითარების დონით კი საქართველოს სარეიტინგო ქულა 59.66-ია. რეიტინგში პირველ ადგილზე საფრანგეთი - 83.12 ქულით. მას მოსდევდა გერმანია 83.12 ქულით და ესტონეთი 81.82 ქულით. რომელ ქვეყნებს ვუსწრებდით? იტალიას, რუსეთს, ნორვეგიას, ლუქსემბურგს, შეერთებულ შტატებს. თუ საქართველო 2017 წელს იყო მე-8 ადგილზე და შემდეგ ჩამოქვეითდა მე-17 ადგილამდე, ამ შემთხვე-

71 "კიბერუსაფრთხოების ინდექსში საქართველო მე-8 ადგილზეა". ტელეკომპანია "იმედი", 2017, გვ. 1. https://imedinews.ge

დიაგრამა 2 – NCSI დიაგრამა, სადაც გამოსახულია საქართველოს სარეიტინგო ქულა და ადგილი. წყარო: https://ncsi.ega.ee/country/ge/?allData=1/

ვაში არსებობს ორი ვერსია: პირველი - საქართველოში გაუარესდა მდგომარეობა; მეორე - სხვა ქვეყნებმა გააუმჯობესეს სიტუაცია.[72]

2022 წელს კი ასეთი სურათი გვაქვს ამ მხრივ, „National Cyber Security intex"-ის მონაცემებით საქართველო 51.95 ქულით 61-ე ადგილზეა, ამ შემთხვევაში მონაცემებს თუ შევადარებთ იმის თქმა, რომ საქართველოში კიბერუსაფრთხოების მდგომარეობა გაუარესდა გაგვიჭირდება, მეტიც, საქართველომ კიბერუსაფრთხოების სხვადასხვა კომპონენტები, მაგრამ სხვა ქვეყნებმაც შეძლეს უფრო მეტად თავიანთი კიბერუსაფრთხოების გაუმჯობესება.[73]

72 "კიბერუსაფრთხოების ინდექსით, საქართველო მსოფლიოში მე-19 ადგილზეა". ტელეკომპანია "იმედი", 2018, გვ. 1. https://imedinews.ge

73 "National Cyber Security intex", "61. Georgia 51.95", 2022. pp. 1-2, https://ncsi.ega.ee/country/ge/?allData=1

კიბერომი ევროკავშირის სივრცეში

დღეს მთელი ევროპა ლაპარაკობს რუსეთიდან მომდინარე საფრთხეებზე. ეს უფრო ხელშესახები გახდა უკრაინასთან ომის წამოწყების შემდეგ. ვარშავაში მიღებული გადაწყვეტილების საფუძველზე, ნატომ 2017 წლის დასაწყისში ბალტიისპირეთის ქვეყნებში (ლიტვა, ლატვია, ესტონეთი) და პოლონეთში განათავსა ბატალიონის ტიპის 4 სამხედრო ქვედანაყოფი, რომლებიც ადგილობრივ სამხედრო ქვედანაყოფებთან შეთანხმებულად მოქმედებენ. ამ გადაწყვეტილებას წინ უძღვოდა ნატო-ს 2014 წლის უელსის სამიტზე მზადყოფნის სამოქმედო გეგმის **RAP**-ის დამტკიცება, რომელიც ძირითადად სწორედ რუსეთიდან მომდინარე საფრთხეებისა და მათი სტრატეგიული გავლენის საპასუხოდ იქნა მიღებული. ვარშავის სამიტის დეკლარაციაში ისიც აღინიშნა, რომ 2014 წლის შემდეგ საფრთხე დაემუქრა ბალტიის ზღვის რეგიონის უსაფრთხოებას. კერძოდ, ხაზი გაესვა რუსეთის გააქტიურებულ სამხედრო აქტივობებს და ახალი სამხედრო ტექნოლოგიების განლაგებას, რაც დამატებით გამოწვევებს უქმნის რეგიონის უსაფრთხოებას. რასაკვირველია, ახალი სამხედრო ტექნოლოგიები თავისთავად გულისხმობს კიბერსივრცის გაკონტროლებასაც და კიბერთავდასხმებსაც.[74]

ევროკავშირმა ასევე დაიწყო ყალბ ახალ ამბებთან ბრძოლის გაძლიერება და ევროკომისიამ დეზინფორმაციის გავრცელების წი-

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

ნააღმდეგ სამოქმედო გეგმაც კი წარადგინა. ამ გეგმის პრეამბულაში ნათქვამია, რომ უნდა შევინარჩუნოთ ერთიანობა, რათა ჩვენი დემოკრატია უკეთ დავიცვათ დეზინფორმაციისგან. ვიხილეთ არჩევნებსა და რეფერენდუმებში ჩარევის არაერთი შემთხვევა, ყველა მტკიცებულება მიუთითებს, რომ დამნაშავე უმრავლეს შემთხვევაში რუსეთია.

სამოქმედო გეგმის თანახმად, უკვე გაიზარდა ევროკავშირის საგარეო პოლიტიკური უწყების ბიუჯეტი - კერძოდ, სტრატეგიულ კომუნიკაციებზე 5 მილიონი ევრო იხარჯება. დაგეგმილია იმ უწყების თანამშრომელთა გაზრდა, რომელსაც დეზინფორმაციის გამოვლენა ევალება.

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

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

რულ სამყაროსთან. მაგალითად - ბიზნესი, არაკომერციული სააგენტოები, მთავრობები და კრიმინალური საწარმოები.

„კომუნიკაციების საშუალებამ მკვეთრად შეცვალა გლობალური კიბერსაფრთხის განტოლება. ICT სისტემა შეიძლება გამოყენებულ იქნეს ბოროტი საქმიანობისთვის, როგორც ინსტრუმეტი სახელმწიფო დონის აგრესიაში. ამის გაკეთება შესაძლებელია ინდივიდუალურადაც - მაგალითად ჰაკინგი სხვადასხვა დაჯგუფებების, კრიმინალების, ტერორისტების, მთავრობების მიერ ორკესტრირებული გეგმის განხორციელებით“.[75]

როდესაც საქმე ეხება ჰიბრიდულ ომს, კიბერ-თავდასხმებს, ჰაკერულ თავდასხმებს, ფეიკ-ნიუსების, ანუ ყალბი ახალი ამბების გავრცელებას, დასავლეთში მუდმივად რატომ მიუთითებენ რუსეთზე? მაგალითად, 2019 წლის შემდეგ სოციალურ ქსელ **«ფეისბუქიდან»** და **“ინსტაგრამიდან”** ასობით გვერდი, ჯგუფი და ანგარიში იშლება. ყველა ეს გვერდი, ჯგუფი და ანგარიში იმართება რუსეთიდან, კოორდინირებულად მოქმედებს და სხვადასხვა ქვეყნების აუდიტორიაზე გათვლილ ინფორმაციას ავრცელებს. მათ შორის იყო რამდენიმე, რომლის სამიზნე ქართველი მომხმარებლები იყვნენ. როგორც **“ფეისბუქის”** ადმინისტრაციაში განმარტეს, ანგარიშებისა და გვე-

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

ვიტაუტას კერსანსკასი

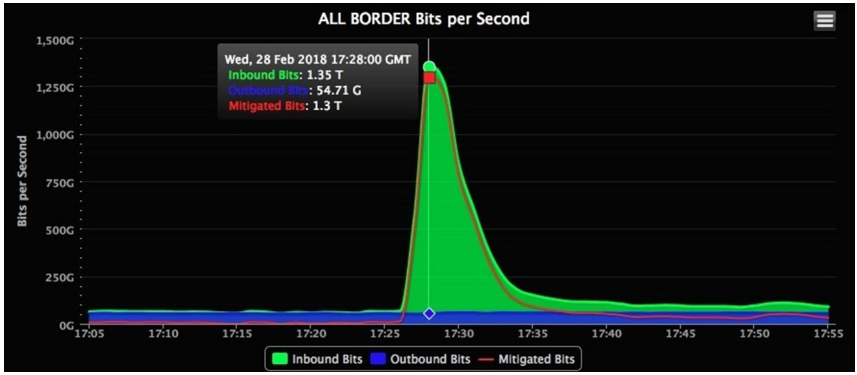
რდების უმრავლესობა რუსული საინფორმაციო სააგენტო **„სპუტნიკის“** თანამშრომლებს ეკუთვნოდათ.

ეს არ არის პირველი შემთხვევა, როდესაც საქართველო რუსეთიდან მომავალი ყალბი ინფორმაციისა და კოორდინირებული საინფორმაციო კამპანიის მსხვერპლი ხდება. როგორც ჰელსინკში მდებარე ჰიბრიდული საფრთხეების საწინააღმდეგო ევროპული ცენტრის თანამშრომელი **ვიტაუტას კერსანსკასი** აცხადებს, რუსეთის ამოცანაა, საზოგადოების სხვადასხვა ჯგუფებს შორის უთანხმოების გამოწვევა, დაძაბულობის ესკალაცია საზოგადოებასა და მთავრობას შორის, ასევე მოკავშირე ქვეყნების დაპირისპირება. უნდა ვებრძოლოთ დეზინფორმაციას და ყალბ ამბებს, რადგან ის ნეგატიურ ზემოქმედებას ახდენს მოქალაქეთა აზროვნებაზე. მეტიც, არსებობს შესაძლებლობა, რომ მოქალაქეებმა სხვა სახელმწიფოების კარნახით დაიწყონ მოქმედება. მაგალითად, არჩევნებში ხმა მისცენ უცხო ქვეყნის მიერ მხარდაჭერილ კანდიდატს ან მიიღონ მონაწილეობა ისეთ საპროტესტო აქციაში, რომელიც უცხო ქვეყნის ინტერესებშია.[76]

რეკორდული სიძლიერის კიბერთავდასხმა

ჩვენ შეგვიძლია უამრავი მაგალითის მოყვანა გახმაურებულ კიბერთავდასხმებზე. ყველაზე მასშტაბური თავდასხმა მსოფლიოში ერთ-ერთ წარმატებულ კომპანიაზე - **„Github”**-ზე მოხდა. აღნიშნული ორგანიზაცია წარმოადგენს დეველოპერების ინტერესის სფე-

76 ერსანსკასი ვ. “დეზინფორმაციასთან და ყალბ ამბებთან საბრძოლველად მარტივი და სწრაფი გზა არ არსებობს, ეს გრძელვადიანი სტრატეგიაა”. საქართველოს საზოგადოებრივი მაუწყებელი, 2019, გვ. 1. https://1tv.ge



დიაგრამა 3 - DDos რეკორდული კიბერთავდასხმა „Github"-ზე
წყარო: https://www.wired.com/story/github-ddos-memcached/

როს. **„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-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 ვებუსაფრთხოების ვიცე-პრეზიდენტმა **ჯოშ შულმა** განაცხადა, რომ მათ თავიანთი შესაძლებლობები გაზარდეს

ჯოშ შული

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“.[77]

კიბერჰიგიენა

კიბერჰიგიენა ძალიან ჰგავს პირად ჰიგიენას. როგორც ადამიანები ეწევიან გარკვეული სახის პირადი ჰიგიენის დაცვას, ასევეა კიბერჰიგიენაც - ადამიანებმა უნდა დაიცვან, რათა შეძლონ მონაცემთა უსაფრთხოდ შენარცუნება. ეს უპირველესად ხელს უწყობს მოწყობილობების სწორ ფუნქციონირებას, იცავს გარე შეტევებისგან და მავნე პროგრამებისგან. კიბერჰიგიენა დამოკიდებულია პრაქტიკასა და სიფრთხილის ზომებზე, რომლებიც მომხმარებლებმა უნდა დაიცვან და გამოიყენონ, რათა შეინარჩუნონ მნიშვნელოვანი მონაცემების უსაფრთხოება ქურდობისა და გარე თავდასხმებისგან.

კიბერჰიგიენის დეფინიცია - კიბერჰიგიენა არის მითითება იმ ნაბიჯებზე, რომლებსაც კომპიუტერებისა და სხვა მოწყობილობების მომხმარებლები იყენებენ სისტემების უსაფრთხოდ შესანარჩუნებლად, ასევე ონლაინ უსაფრთხოების გასაუმჯობესებლად. აღნიშნული პრაქტიკა ხშირად რუტინის ნაწილია.

კიბერჰიგიენის პროცედურების დანერგვა სასარგებლოა ორი მიმართულებით. ესენია: მოვლა და უსაფრთხოება. ტექნიკური მომსახურება აუცილებელია კომპიუტერებისა და პროგრამული უზრუნველყოფის მაქსიმალური ეფექტურობისთვის.

როდესაც ფაილები ფრაგმენტირებული ხდება, ამ დროს თქვენი

77 Newman H. L. GitHub Survived the Biggest DDoS Attack Ever Recorded, Media Company Wired, 2018, p 1. https://www.wired.com

პროგრამები მოძველებულია? რა თქმა უნდა, ეს ზრდის დაუცველობის რისკს. თუ იქნებით მზად, რომ დაიცვათ კიბერჰიგიენა და მოუაროთ თქვენს კომპიუტერულ მოწყობილობებს, შესაბამისად, ადრეულ ეტაპზე აღმოაჩენთ ბევრ პრობლემას და თავიდან აიცილებთ. მიუხედავად იმისა, რომ საფრთხეების პროგნოზირება შეიძლება იყოს რთული, ხშირ შემთხვევაში თავიდან აცილება ხდება კიბერჰიგიენის დაცვით.

მონაცემთა დაკარგვა Loss of Data

(მყარი დისკები და ონლაინ მეხსიერების საცავები, რომელიც არ წარმოადგენს სარეზერვო მეხსიერებას და არ არის შენახული, დაუცველია ჰაკერული თავდასხმებისგან, რამაც შეიძლება გამოიწვიოს ინფორმაციის დაკარგვა)

არასწორად განთავსებული მონაცემები Misplaced Data

(კიბერჰიგიენის ცუდმა დაცვამ შეიძლება გამოიწვიოს მონაცემების დაკარგვა სხვადასხვა გზებით. მაგალითად, ინფორმაცია შეიძლება არ იყოს დაზიანებული ან წაშლილი, მაგრამ ბევრი მონაცემების შენახვა და ფაილების არასწორმა განთავსებამ შეიძლება მიგვიყვანოს პრობლემებამდე, აღნიშნული ხშირად ხდება ორგანიზაციებში).

უსაფრთხოების დარღვევა Security Breach

(არსებობს მუდმივი საფრთხეები კომპანიების მონაცემებზე. ფიშინგი, ჰაკერები, მავნე პროგრამები, სპამი, ვირუსები და სხვა. აღნიშნული საკითხები მუდმივ პროცესშია).

ვადაგასული პროგრამული უზრუნველყოფა Out of Date Software

(აუცილებელია, პროგრამული აპლიკაციები დროულად განახლდეს, რაც უზრუნველყოფს უსაფრთხოების უახლეს დამატებებს და უახლესი ვერსიების გამოყენებას ორგანიზაციებში. მოძველებული პროგრამული უზრუნველყოფა უფრო დაუცველია თავდასხმებისა და მავნე პროგრამების მიმართ).

ძველი უსაფრთხოების პროგრამული უზრუნველყოფა Older Security Software

(ანტივირუსული პროგრამული უზრუნველყოფა და უსაფრთხოების

სხვა პროგრამული უზრუნველყოფა მუდმივად უნდა განახლდეს, რათა მოხდეს კიბერსაფრთხეების თავიდან აცილება).

კიბერჰიგიენის დაცვა - პრაქტიკული რჩევები

მიუხედავად იმისა, რომ ციფრული სისტემების დაცვა 21-ე საუკუნეში პრობლემას წარმოადგენს, კიბერჰიგიენის რუტინის შექმნა არც ისე რთულია. რეგულარულად შესრულებულმა რამდენიმე საკვანძო პრაქტიკამ შეიძლება მკვეთრად გააუმჯობესოს ნებისმიერი სისტემის უსაფრთხოება.

გაითვალისწინეთ, აუცილებელია ყველა მიმდინარე აღჭურვილობისა და პროგრამის დოკუმენტირება, აპარატურა, პროგრამული უზრუნველყოფა და აპლიკაცია უნდა იყოს დოკუმენტირებული.

შექმენით სამი ძირითადი კომპონენტი:

1. აპარატურა Hardware

კომპიუტერები, დაკავშირებული მოწყობილობები (მაგ. პრინტერები) და მობილური მოწყობილობები (მაგ. სმარტფონები, ტაბლეტები).

2. პროგრამული უზრუნველყოფა Software

ყველა პროგრამა, რომელსაც იყენებთ ქსელში, რომელიც დაინსტალირებულია პირდაპირ კომპიუტერზე.

3. აპლიკაციები Applications

ვებ-აპლიკაციები (მაგ. Dropbox, Google Drive), აპლიკაციები ტელეფონებზე, რომელიც პირდაპირ არ არის დაინსტალირებული მოწყობილობებზე.

კიბერჰიგიენის პოლიტიკა და სხვა ელემენტები:

პაროლების ცვლილება Password Changes

კომპლექსური პაროლების რეგულარულად შეცვლამ შეიძლება თავიდან აგვაცილოს მრავალი მავნე მოქმედება და დაიცვას კიბერუსაფრთხოება.

პროგრამული უზრუნველყოფნის განახლებები Software Updates

თქვენ მიერ გამოყენებული პროგრამული უზრუნველყოფის განახლება უნდა იყოს რეგულარული მიმოხილვის ნაწილი.

აპარატურის განახლება Hardware Updates

ძველი კომპიუტერებისა და სმარტფონების განახლება შეიძლება საჭირო გახდეს მუშაობის გამართული რეჟიმის შესანარჩუნებლად და პრობლემების თავიდან ასაცილებლად.

ახალი ინსტალაციების მართვა Manage New Installs

ყოველი ახალი ინსტალაცია უნდა განხორციელდეს სწორად და დოკუმენტირებულად, რათა შეინახოს ტექნიკისა და პროგრამული უზრუნველყოფის განახლებული ინვენტარი.

მომხმარებლის შეზღუდვა Limit Users

მხოლოდ მათ, ვისაც სჭირდება ადმინისტრატორის დონის წვდომა პროგრამებზე, უნდა ჰქონდეს წვდომა. სხვა მომხმარებლებს უნდა ჰქონდეთ შეზღუდული შესაძლებლობები.

მონაცემთა სარეზერვო ასლის შექმნა Back Up Data

ყველა მონაცემის სარეზერვო ასლი უნდა იყოს მეორად წყაროზე (მაგ. მყარ დისკზე, ღრუბლოვან საცავში). ეს უზრუნველყოფს მის უსაფრთხოებას.

კიბერუსაფრთხოების ჩარჩო Cyber Security Framework

შესაძლოა, ბიზნესს სურდეს გადახედოს და დანერგოს უფრო მოწინავე სისტემა (მაგ. NIST Framework) უსაფრთხოების უზრუნველსაყოფად.

ეს ყველაფერი უნდა შესრულდეს რუტინულად, დაიგეგმოს განახლება, გადახედვა. მაგალითად, პაროლების შეცვლა ყოველ 30 დღეში, ან განახლების შემოწმება კვირაში ერთხელ. ამით უზრუნველყოფილი იქნება თქვენი ტექნიკისა და პროგრამული უზრუნველყოფის მთელი ქსელის კიბერჰიგიენა.[78]

78 Brook Ch., ,,What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More'', DATAINSIDER - Digital Guardian's Blog, 2020. p. 1, https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more?fbclid=IwAR0iFAutj9eyTLKRJmJ94HUnSyKtWC50d1Y1PyOg07C56pkQBx3AC4OZOAQ

ანტივირუსი როგორც ერთ-ერთი თავდაცვითი მექანიზმი

ვირუსების და კიბერთავდასხმების ფონზე აქტიურად ხდება მათი შემაკავებელი მექანიზმების გამოგონება, პირველი ანტივირუსი **1984 წელს ჰოპკინზმა შექმნა**[79], დღეს კი არსებობს უამრავი ანტივირუსული კომპანია, რომლებიც მუშაობენ ანტივირუსების შექმნაზე, ისინი გვთავაზობენ გარკვეულ ფასად ჩვეულებრივ ანტივირუსულ პროგრამებს, თუმცა ასევე დიდი კომპანიებისთვის შემუშავებული აქვთ ბიზნეს-ანტივირუსებიც, რომელიც ანტივირუსის სრულ პაკეტს მოიცავს. რთული სათქმელია, რომელ ანტივირუსზე შეიძლება ვთქვათ, რომ სრულიად უზრუნველყოფს დაცვას, რადგან ყველა ანტივირუსს აქვს რაღაც პლიუსი და რაღაც მინუსი, მაგრამ ჩვენ შეგვიძლია განვიხილოთ მონაცემები, თუ როგორ მუშაობენ ისინი. ამ მხრივ ერთ-ერთ ყველაზე დიდ კორპორაციას წარმოადგენს **„კასპერსკი“**.

„კასპერსკი“ წარმოადგენს რუსულ კომპანიას, რომელსაც ოფიციალურად იყენებენ სხვადასხვა ქვეყნებში, მათ შორის აშშ-ის სახელმწიფო სააგენტოებში. არსებობს ეჭვი, რომ ის არის მოქცეული რუსეთის მთავრობის გავლენის ქვეშ და შესაძლოა, წარმოებულ პროდუქციაში დამატებულია ჰაკერული სისტემა ინფორმაციის გადმოსაქაჩად. თუმცა **„კასპერსკი“** ყველა წაყენებულ ბრალდებას თუ მსგავს მოსაზრებას უარყოფს. გავეცნოთ **Kaspersky Security Network**-ის სტატისტიკას, რომელიც გამოქვეყნებულია ელექტრონულად და მოპოვებულია **KSN**-ის განაწილებული ანტივირუსული ქსელების გამოყენებით, რომელიც მუშაობს ანტიმავნე დამცავი კომპონენტებით. მონაცემები შეგროვდა **KSN**-ის მომხმარებლებისგან, რომლებიც დათანხმდნენ ინფორმაციის მიწოდებაზე. **Kaspersky Lab**-ის მილიონობით მომხმარებელი მონაწილეობს მავნე საქმიანობის შესახებ ინფორმაციის გლობალურ გაცვლაში. მისი უსაფრთხოების ქსელის თანახმად: **Kaspersky Lab**-ის გადაწყვეტილებებმა დაბლოკა **989 432**

79 Leiden J. The 30-year-old prank that became the first computer virus, Information Technology Company The Register, 2012, p 1. https://www.theregister.com

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.

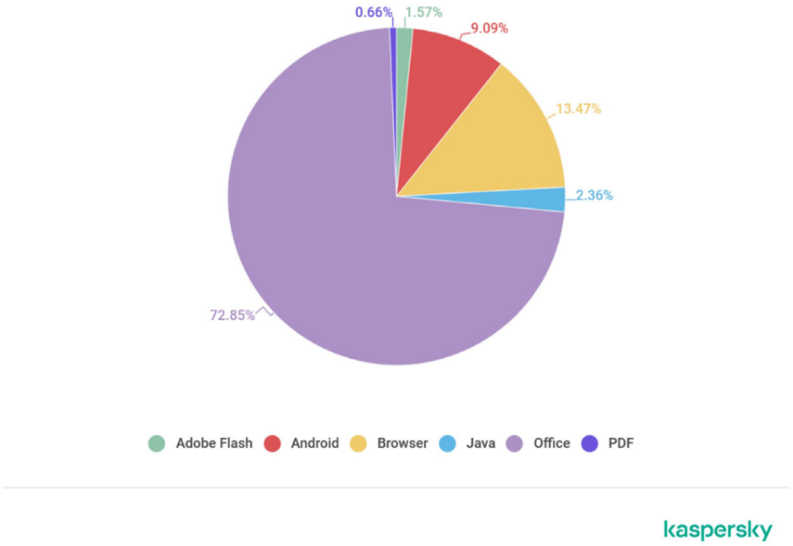
კიბერდანაშაულების მიერ გამოყენებული ექსპლუატაციების განაწილების შესახებ სტატისტიკის თანახმად, **Microsoft Office**-ის აპლიკაციების ნაკრებში დიდი ნაწილი დაუცველია **(73%)**. ყველაზე გავრცელებული შეცდომები ბოლო კვარტალში იყო **(CVE-2017-11882, CVE-2018-0802)** Equation Editor პროგრამაში, რომელიც ადრე **Microsoft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

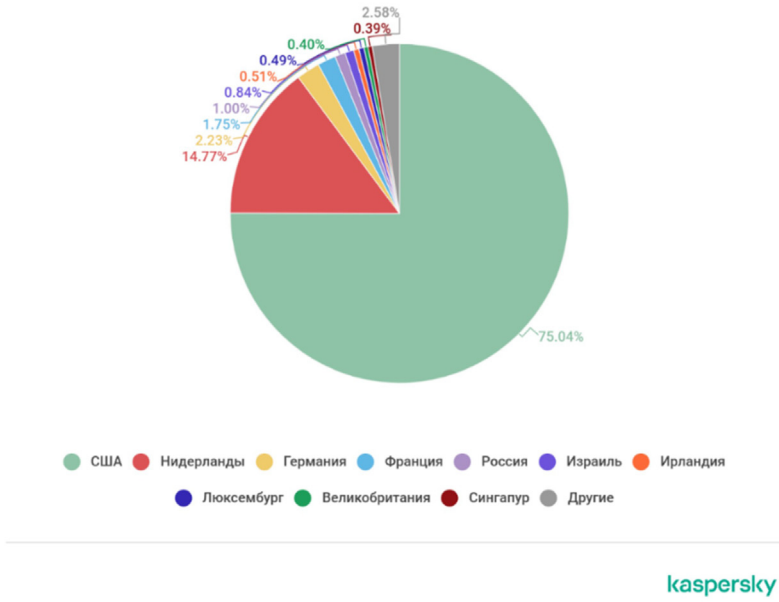
Google-ის მკვლევარმა გამოაქვეყნა ინსტრუმენტი ამ პრობლემის დემონსტრირებისთვის - **CtfTool**, რომელიც საშუალებას გაძლევთ, დაიწყოთ პროცესები სისტემის პრივილეგიებით, ასევე შეიტანოთ ცვლილებები სხვა პროცესების მეხსიერებაში და შეიყვანოთ თვითნებური კოდი.



დიაგრამა 4 - 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:



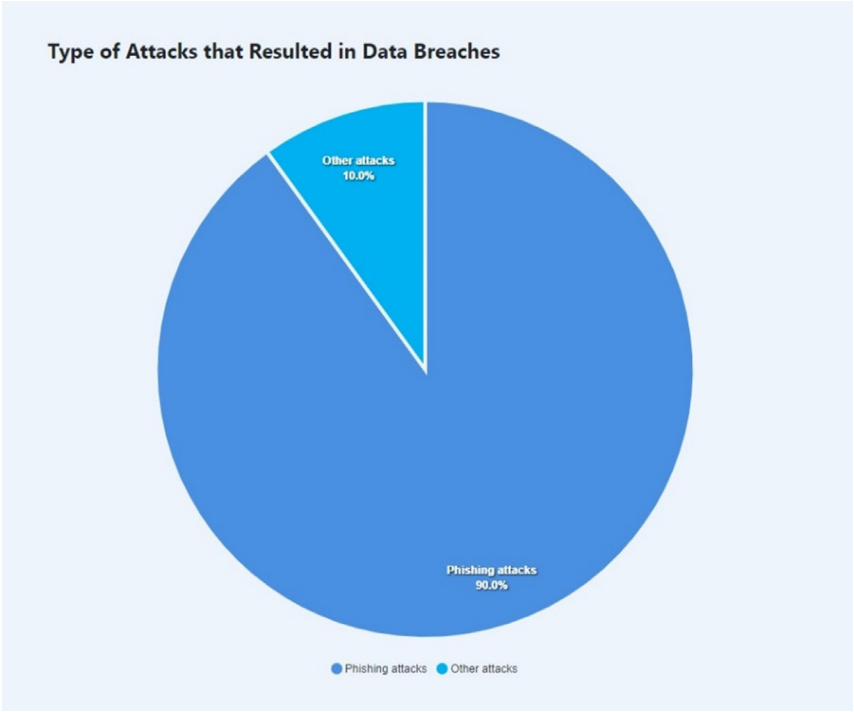
დიაგრამა 5 - კომპანია კასპერსკის დიაგრამა, სადაც გამოსახულია ვებ-თავდასხმების ტოპ-ათი ქვეყანა
წყარო: https://securelist.ru/it-threat-evolution-q3-2019-statistics/95163/

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%).

რამდენი მონაცემების დარღვევა მოხდა ,,ფიშინგის" შეტევების შედეგად?

საერთაშორისო ორგანიზაციის **„Cisco“**-ს 2021 წლის **კიბერუსაფრთხოების საფრთხის ტენდენციების ანგარიშის** მიხედვით **„ფიშინგის“** შეტევები 90%-ს შეადგენს.[80]

მათი სტატისტიკური მონაცემების მიხედვით ირკვევა, რომ კიბერკრიმინალები უფრო ხშირად სარგებლობენ ადამიანების ემოციებით ან დაუდევრობით, ვიდრე სისტემის დაუცველობით.



დიაგრამა 6 - საერთაშორისო ორგანიზაცია „Cisco”-ს დიაგრამა, სადაც გამოსახულია „ფიშინგ“ შეტევების მონაცემები
წყარო: https://www.cloudwards.net/cyber-security-statistics/

როგორ უნდა დავიცვათ თავი კომპიუტერულ ქსელებზე კიბერთავდასხმებისგან? ამის შესახებ თეორიულ მეთოდებს შეგვიძლია გავეცნოთ სახელმძღვანელოში - **„კიბერ ოპერაციები, მშენებლობა,**

80 Pitchkites M., “Top Cyber Security Statistics, Facts & Trends in 2022”, 2022. p. 1, https://www.cloudwards.net/cyber-security-statistics/

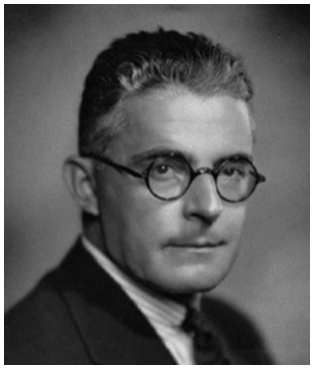
დაცვა და თავდასხმა, თანამედროვე კომპიუტერული ქსელები“, რომლის ავტორიც გახლავთ **მაიკ ოლილე**. ის თავის წიგნში კომპიუტერულ ოპერაციებს განიხილავს სისტემურ დონეზე:

„კიბერდაცვა, ეს ვერ აიხსნება, თუ არ ავხსნით **“windows”**-ის და **Linux**-ის მთელი სამუშაო პროცესის. მათ შორის **Centos, Mint, OpenSuSE** და **Ubuntu** სისტემები. ეს შეიძლება იყოს ფიზიკური ან ვირტუალური სისტემები, რომლებიც აშენებულია **VMWARE Workstation**-ით ან **VirtualBox**-ით. კიბერშეტევისას თავდამსხმელს, რომელიც იმყოფება სისტემაში, სურს შეინარჩუნოს ე.წ. დაშვება, ამიტომ ის მუდმივად ახორციელებს თავდასხმას. ჩვენ შეგვიძლია ვაჩვენოთ შეტევების სპექტრი, მათ შორის, **internet Exprorer**-ის, **Firefox**-ის, **Java**-ს და **Adobe Flash**-ის წინააღმდეგ გამოყენებული. ასეთი კიბერშეტევები ქსელში ტოვებს კვალს და თუ ჩვენ გვაქვს პროგრამულად ჭკვიანური დაცვა, მაშინ შეგვიძლია ამის ნახვა“.[81]

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

თავი მესამე

პოლიტიკური კონფლიქტის ახალი იდენტიფიკაცია და ასიმეტრიული საფრთხის ფენომენი კიბერომის მაგალითზე



ჯონ უოტსონი (1978-1958)

ტექნოლოგიების განვითარება ყოველთვის აისახება და გავლენას ახდენს საზოგადოებაზე. ჩვენ ვერ გაუმკლავდებით ტექნოლოგიურ გამოწვევებს ადამიანის ბუნების გათვალისწინების გარეშე, ხოლო ადამიანის ბუნების ექსპერტები არიან ქცევითი მეცნიერები ანუ ბიჰევიორისტები. ბიჰევიორიზმის თეორიის გაჩენა უკავშირდება (1913 წ.) **ჯონ უოტსონის** დეკლარაციებს, რომელიც თავმოყრილი იყო მის სტატიაში - **"ფსიქოლოგია ბიჰევიორისტის თვალსაზრისით"**.[82]

ბიჰევიორისტები სწავლობენ ადამიანის ინდივიდუალურ და საზოგადოებრივ ქცევას. ჩვენ ამ თეორიას განვიხილავთ კიბერუსაფრთხოების ჭრილში. მეთოდოლოგია დამკვიდრებულია სხვადასხვა წამყვან ქვეყნებში. შეიძლება უცნაური იყოს, ასეთ ტექნიკურ მხარეს, როგორიც კიბერსამყაროა, როგორ უნდა უკავშირდებოდეს ბიჰევიორიზმი? კიბერუსაფრთხოების სპეციალისტი **ბრიუს შნაიერი** ამ საკითხს ასე განმარტავს: **"მხოლოდ მოყვარულები უტევენ მანქა-**

82 Cherry K. History and Key Concepts of Behavioral Psychology, publisher very well mind company, 2019, p 1. https://www.verywellmind.com/

ნებს, პროფესიონალები მიზანში იღებენ ადამიანებს".[83]

მაგალითისთვის ავიღოთ ჰაკერების ერთ-ერთი თავდასხმის ტექნიკა, რომელსაც ჰქვია **"ფიშინგი"**. ფიშინგის შეტევისას თავდამსხმელი, რომელიც ცდილობს, კომპიუტერულ სისტემაში შეაღწიოს, უპირველეს სამიზნეს წარმოადგენს მომხმარებელი და არა ავტომატიზებული დაცვის მექანიზმის გატეხვა. თავდამსხმელი მომხმარებლებს უგზავნის შეტყობინებას ელფოსტით, სადაც ყალბი ვებ-გვერდია მითითებული, თუმცა ის ორიგინალს ჰგავს. მაგალითად, ეს შეიძლება იყოს ბანკის შეტყობინება, რომელიც თითქოს სანდოობის გარანტია, მაგრამ თუ ადრესატი ყალბ ბმულს გახსნის, ამან შეიძლება უნებლიედ გამოიწვიოს თავდამსხმელის წვდომა პირად ინფორმაციაზე.

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

კიბერშეტევების წინააღმდეგ ბრძოლისთვის ამერიკის შეერთებული შტატების არმია აქტიურად იყენებს ბიჰევიორიზმის თეორიას. კიბერბიჰევიორიზმის მოდელის ანალიზი, ანუ თანამედროვე კომერციული მეთოდი, გაჩნდა აშშ-ის არმიის მიერ ჩატარებული **(Cyber Quest 2017)**[84] ღონისძიების შემდეგ, როგორც კიბერ საფრთხეზე ერთ-ერთი პასუხი. **პოლკოვნიკ სტივენ რენის** აზრით, მთავარია კი-

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

84 Schmidt R. Cyber Quest, Action Impact LLC, 2017, p 1. https://www.actionimpact.com

ბერქსელში ტრეფიკის და მომხმარებლის ქცევის ნორმალური მონიტორინგი, ამის შემდეგ შეიძლება განისაზღვროს სიტუაცია და ქმედება, რომელიც მიუთითებს ჰაკერის მხრიდან კიბერთავდასხმაზე ან კიბერშეჭრაზე სისტემაში.[85]

კომერციული დეველოპერების მტკიცებით, კიბერსივრცეში არსებობს ოთხი ფენა - **ფიზიკური, ქსელური, სოციალური და პერსონალური**. საფრთხეების მონიტორინგი მოიცავს **ბიჰევიორისტული** მონაცემების შეგროვებას თითოეულ ფენაზე, შემდეგ ამ მონაცემების კორელაციასა და კომბინირებას. ამერიკელი სამხედრო პოლკოვნიკის, **რენის** აზრით, ბიჰევიორიზმის თეორია არ იხილავს წესებს, არამედ ამ თეორიის საშუალებით ჩვენ ვუყურებთ კიბერქსელში ცხოვრების წესს. ეს სისტემა კი ასე მუშაობს: მონიტორინგის დროს, მაგალითად, ერთი სერვერი ყოველთვის ამყარებს კონტაქტს მეორე სერვერთან, მაგრამ რაღაც დროის გასვლის შემდეგ იგი როუტერთან შედის კავშირში ან სხვა სერვერთან. ამ შემთხვევაში ხდება დეტალური დაკვირვება და ანალიზი. სერვისების შიდა ქსელებზე გამოყენების შემთხვევაში, ქცევითი ანალიზის მეთოდი მნიშვნელოვანი ინსტრუმენტი იქნება იმისთვის, რომ შეამცირონ კიბერშეტევებისა და უსაფრთხოების დარღვევის რისკები.[86]


გენერალი ჯონ მორისონი

გასაკვირი არ არის, რომ ამ მეთოდოლოგიის გამოყენება ქმნის ფართო მონაცემების პრობლემას. თუმცა **გენერალ მორისონის** თქმით: «გამოსავალი ხელოვნური ინტელექტისა და მანქანიდან მანქანაში სწავლის ტექნოლოგიის შექმნაა, ხელოვნური ინტელექტი საშუალებას მოგვცემს, გაცილებით სწრაფი რეაგირება მოვახდინოთ კიბერსივრცეში მიმდინარე მოვლე-

85 Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, p 1. https://www.mitre.org

86 Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, p 1. https://www.mitre.org

ნებზე. უნდა იყოს თითოეული ბიტის და ბაიტის მონაცემების ანალიზი, მანქანა კი ამბობს, რომ ხდება რაღაც, რაც ჩვეულებრივ არ ხდება ხოლმე ქსელში, შემდეგ კი იქმნება სიტუაცია, რომ ყველაფერი შემოწმებას დაექვემდებაროს».[87]

ბიჰევიორიზმის თეორიის შესწავლა, გარჩევა, გაანალიზება და ათვისება საჭიროა როგორც კერძო სექტორში მომუშავე პროგრამისტებისთვის, ასევე სახელმწიფო უწყებებში დასაქმებულთათვის. ჩვენ ელფოსტის საშუალებით თითქმის ყოველდღიურად ვიღებთ უამრავ შეტყობინებას სხვადასხვა ქვეყნებიდან თუ ორგანიზაციებიდან, ამ დროს არ ვიცით, რა არის ყალბი და რა არის ნამდვილი. თუ გვინდა, თავი დავაღწიოთ სერიოზულ საფრთხეებს, ჰაკერებს არ ჰქონდეთ წვდომა ჩვენს პირად ინფორმაციაზე, ადგილი არ ჰქონდეს ეფექტურ კიბერთავდასხმებს, მაშინ უნდა გავიაზროთ და ვისწავლოთ ასევე ეფექტური წინააღმდეგობის გაწევა.

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

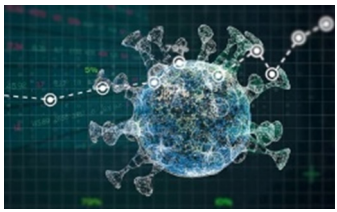
87 Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, p 1. https://www.mitre.org

ბისთვის იყენებენ.

მაგალითად, ამ მხრივ **(„ფიშინგით“)** თაღლითობა აქტიურად დაიწყო ვირუსის გავრცელების დღიდან. მავანნი ცდილობენ, უფრო მეტი შიში და დაბნეულობა დანერგონ ინტერნეტმომხმარებლებში. გახშირდა ჰაკერული თავდასხმები სამედიცინო კლინიკებზე გამოსასყიდის სანაცვლოდ. თავდასხმებმა შეაჩერა ოპერაციები და გამოიწვია გადადება. ასეთი შეტევები უდიდეს საფრთხეს უქმნის პაციენტების ჯანმრთელობას. მოვლენების კვალდაკვალ, **„ვაშინგტონ პოსტმა“** გამოაქვეყნა სტატია სათაურით: **„ჰაკერები კორონავირუსთან დაკავშირებულ შიშებს იყენებენ პირადი მონაცემების მოსაპარად“**. აღნიშნულ სტატიაში განხილულია კორონავირუსის შემდეგ ჰაკერული თავდასხმების ნაკადის მზარდი მატება. ისრაელში მომუშავე კიბერუსაფრთხოების ორგანიზაციამ **„Check Point“**-მა გამოაქვეყნა ანგარიში, სადაც გამოკვეთილია ყველაზე ეფექტურად მომუშავე ჰაკერული ჯგუფის მიერ წამოწყებული კამპანია, რომელსაც უწოდეს **“Vicious Panda”** („მოწინავე საფრთხე“). ანგარიშში ნათქვამია, რომ **“Vicious Panda”**-მ, ანუ ჰაკერულმა ორგანიზაციამ, გამოიყენა ყალბი დოკუმენტები, გაავრცელა ფეიკ-ინფორმაციები მონღოლეთის ჯანდაცვის მინისტრის სახელით. თითქოს ის საშინელ მდგომარეობას ამცნობდა მსოფლიოს. ჰაკერების მიზანი იყო, რაც შეიძლება ბევრ ადამიანს უნდა გაეხსნა ეს ინფორმაცია, შემდეგ კი მათ წვდომა ექნებოდათ მომხმარებელთა პირად მონაცემებზე. ეს იქნებოდა სმარტოფნებისა თუ კომპიუტერების საშუალებით. ანგარიშში **“Check Point”**-ის თავდაცვის დაზვერვის უფროსის, **ლატე ფინკლინტინის** განცხადებაცაა მოცემული, ის აფრთხილებს საჯარო სექტორს, სატელეკომუნიკაციო კომპანიებს: „**Covid-19** წარმოადგენს არა მხოლოდ ფიზიკურ საფრთხეს, არამედ კიბერსაფრთხესაც, ყველა საჯარო სექტორის სუბიექტი და სატელეკომუნიკაციო კომპანია უნდა იყოს ფრთხილად კორონავირუსის გარ-

შემო არსებულ დოკუმენტაციასთან და ვებსაიტებთან“.[88]

კიბერუსაფრთხოების დამოუკიდებელი ექსპერტის, **ლუკას ოლეჯნიკის** თქმით, დღეს ამ მასშტაბური გლობალური კრიზისის დროს მსოფლიო სრულიად არის დაუცველი და შესაძლოა, ვითარება უფრო გაუარესდეს.[89]



ამ შემთხვევაში არც საქართველოა გამონაკლისი, აქ უფრო მცირე დოზით, მაგრამ მაინც ხდება მსგავსი თავდასხმები, როგორც ჰაკერულ, ასევე ინფორმაციულ დონეზე. მაგალითად, ჰაკერებმა საქართველოს **4 934 863** მოქალაქის (მათ შორის გარდაცვლილი პირების) პერსონალური ინფორმაცია გამოაქვეყნეს. ამ საკითხს ამერიკულმა გამოცემამ - **ZDNet**-მა ვრცელი სტატია მიუძღვნა.[90]

რა საჭირო იყო პირადი მონაცემების მოპოვება-გავრცელება? ეს ადამიანების დაუცველობის სინდრომის გაღვივებას და პანიკის დათესვას ემსახურება. მით უმეტეს, როდესაც ქვეყანაში დეზინფორმაციული სააგენტოები და ტელეკომპანიები სჭარბობს, რომლებიც ამ მასალას უფრო მეტად მძაფრად აწვდიან მოსახლეობას, ვიდრე ეს რეალურადაა. აღნიშნული ბაზების ლინკებზე მითითებული იყო, რომ ინფორმაციის წყაროს ცენტრალური საარჩევნო კომისიის სისტემა წარმოადგენდა. თუმცა ეს ინფორმაცია არ დადასტურდა. ცენტრალურმა საარჩევნო კომისიამ გააკეთა განცხადება, სადაც ხაზგასმით წერია, რომ მონაცემთა ბაზა

88 Timberg C., Romm T., Hackers are seizing on coronavirus fears to steal data, researchers and U.S. regulators warn”, The washingtonpost, 2020, p 1. https://washingtonpost.com

89 Newman H. L. Coronavirus Sets the Stage for Hacking Mayhem, Media Company Wired, 2020, p 1. https://www.wired.com

90 Catalin C. Personal details for the entire country of Georgia published online, 2020, p 1. https://www.zdnet.com

რადიკალურად განსხვავდება იმისგან, რაც მათ სისტემაში ინახება. ფაქტობრივად, ეს ბაზა არ შეიცავს ისეთ პირად მონაცემებს, რაც ჩვენს მოსახლეობას შეუქმნის საფრთხეს, მაგრამ ამ მონაცემების გავრცელება მაინც დანაშაულია. ისეთ ადამიანებზე, ვინც ტექნოლოგიებში ვერ ერკვევა, უჩნდება შიში და დაუცველობის განცდა, მიზანიც ზუსტად ეს იყო.

საქართველოს მოსახლეობას საგანგებო მდგომარეობის პერიოდში უგზავნიდნენ შეტყობინებებს, რომლებიც შეიცავდა დეზინფორმაციას: **“UCKEBA”**, რომლის შინაარსია: ,,თქვენ დაჯარიმდით კომენდანტის საათის დარღვევის გამო, ჯარიმის ოდენობა 3000 ლარი. **R.M. police.g**e”.[91]

ეს კიდევ უფრო ამყარებს ეჭვებს, რომ მიზანმიმართულად ხდებოდა მოსახლეობაში პანიკის დათესვა. შინაგან საქმეთა სამინისტრომ განაცხადა, რომ აღნიშნული მოკლე ტექსტური შეტყობინებები არ შეესაბამებოდა სინამდვილეს და ეს არ იყო გაგზავნილი მათ მიერ. ინტერნეტსივრცეში გაჩნდა უამრავი ვებ-გვერდები და სტატისტიკური მონაცემები, რომლებიც რეალობას სცდებოდა, ჰაკერები სხვადასხვა ვებ-გვერდების საშუალებით მანიპულირებდნენ კორონავირუსის სტატისტიკით. რიცხვებით თამაშმა კი საზოგადოებაში პანიკა გამოიწვია. ინტერნეტმომხმარებლები უნებურად ხდებიან ინტერნეტვირუსების მსხვერპლნი, ინფორმაციის მოძიებისას ავტომატურად გადადიან ისეთ ვებ-გვერდებზე, სადაც ხდება დავირუსებული პროგრამის ჩამოტვირთვა. ჰაკერები უნებართვო წვდომას იღებენ სხვადასხვა მანიპულაციების საშუალებით. ერთ-ერთი ასეთი ვიდეო გამოაქვეყნა **GEORGIAN HACKERS COMMUNITY – GHC**-მა. ვიდეოში ნაჩვენებია, **Corona-virus-map.com.**

91 “შსს-ს სახელით მოქალაქეებს მესიჯები მიუვიდათ - რა განცხადებას ავრცელებს სამინისტრო”, საქართველოს შინაგან საქმეთა სამინისტრო 2020, გვ. 1. https://www.ambebi.ge

exe, რომლის ფაილიც შეიცავს თავისი შიგთავსით **AZORult malware**-ის, რომელიც წლების წინ შეიქმნა ინფორმაციის მოპარვისთვის. **AZORult** თქვენი ბრაუზერის **cooki**-ებიდან იპარავს მონაცემებს, ყველაფერი, რაც კი დამახსოვრებული აქვს ბრაუზერს თქვენს კომპიუტერში - პაროლები, პირადობის ნომერი და ა.შ. აძლევს ჰაკერს წვდომას თქვენს მონაცემებზე, რაც ძალიან დიდ საფრთხეს უქმნის პირადი მონაცემების დაცვას და მათ გამოყენებას უნებართვოდ.[92]

ირანის ისლამური რესპუბლიკის შემთხვევის გარჩევა

ყასემ სოლეიმანი (1957-2020)

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

„აშშ-ის პრეზიდენტის, **დონალდ ტრამპის** ბრძანებით, ჩვენმა სამხედროებმა უცხოეთში მყოფი ამერიკელების დასაცავად ქმედითი თავდაცვითი ზომები მიიღეს და გენერალი ყასემ სოლეიმანი მოკლეს. დაჯგუფება **„ალ-კუდსი“**, რომელსაც ის ხელმძღვანელობდა, აშშ-ში ტერორისტული ორგანიზაციების სიაში იყო შეყვანილი. გენერალი **სოლეიმანი** ამერიკელ დიპლომატებზე ერაყსა და მთელ რეგიონში მყოფ სამხედროებზე თავდასხმებს გეგმავდა. **„ალ-კუდსი“** პასუხისმგებელია ასობით ამერიკელი და კოალიციური ჯარის სამხედროთა სიკვდილზე“.[93]

92 ზედელაშვილი თ. „ჰაკერები კორონავირუსთან დაკავშირებულ შიშებს იყენებენ პირადი მონაცემების მოსაპარად“ - უნდა ველოდოთ მასშტაბურ კიბერშეტევებს”, მედიაჰოლდინგი “ჯორჯიან ტაიმსი”, 2020, გვ. 1. http://geotimes.com.ge

93 US Dept of Defense, Statement by the Department of Defense”, U.S. Department

რა იყო მიზეზი, რამაც ასე ფეთქებადსაშიში გახადა ახლო აღმოსავლეთი და რამაც გადააწყვეტინა **ირანის ისლამური რესპუბლიკა**, გამოეცხადებინა **„ჯიჰადი“** მოწოდებით: **„სიკვდილი ამერიკას“**? 2019 წლის 31 დეკემბერს ბაღდადში აშშ-ის მიერ ერაყში **„კატაიბ ჰეზბოლას“** ობიექტებზე მიტანილი იერიშის გამო დაწყებული საპროტესტო აქციის მონაწილეებმა აშშ-ის საელჩოზე თავდასხმა განახორციელეს. მანამდე აშშ-ის ქმედებები ერაყის საგარეო საქმეთა სამინისტრომ დაგმო, ირანმა კი, რომელიც **„კატაიბ ჰეზბოლას“** უჭერს მხარს, თავდასხმას **„ტერორიზმის ნათელი მაგალითი“** უწოდა. აშშ-ის საჰაერო ძალებმა სირიასა და ერაყში დაჯგუფება **„კატაიბ ჰეზბოლას“** ობიექტებზე იერიში 29 დეკემბერს მიიტანეს.


დონალდ ტრამპი (1946)

სოლეიმანის სიკვდილიდან მეორე დღესვე ამერიკის შეერთებული შტატების უსაფრთხოების უწყებამ გაავრცელა განცხადება, რომ შესაძლოა, შეერთებულ შტატებზე ირანის ისლამური რესპუბლიკის მხრიდან კიბერთავდასხმა განხორციელდეს: „**ირანის ისლამურ რესპუბლიკას** საკმაოდ ძლიერი კიბერპროგრამა აქვს და თეირანი ცნობილია პოლიტიკურად მოტივირებული კიბერთავდასხმების განხორციელებით“.[94]

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 იყენებდნენ სოცია-

of Defense (DoD), 2020, p 1. https://www.defense.gov

94 რუხაძე თ. “ირანის მხრიდან შესაძლოა, აშშ-ზე კიბერთავდასხმა განხორციელდეს”, საქართველოს საზოგადოებრივი მაუწყებელი, 2020, გვ. 1. https://1tv.ge

ჰასან რუჰანი (1948)

ლურ ქსელებს, კერძოდ - **„ტვიტერს“**.ამავე ხერხს მიმართეს ირანელმა მოხელეებმაც. **აშშ-ირანის ისლამური რესპუბლიკის** სამხედრო დაპირისპირება მიმდინარეობდა საინფორმაციო ომის ფონზე. ფაქტია, სოციალურ ქსელებში **დონალდ ტრამპის** მხრიდან არაერთხელ დაფიქსირდა მუქარა, თუ **ირანის ისლამური რესპუბლიკა** ჩვენს ქვეყანაზე თავდასხმებს განახორციელებს, 52 ირანულ ობიექტს დავბომბავთ, დარტყმა სწრაფი და ძლიერი იქნებაო. **„ირანელ ხალხს არასოდეს დაემუქრო“**, - ამ სიტყვებით მიმართა ქვეყნის პრეზიდენტმა **ჰასან რუჰანმა** დონალდ ტრამპს.[95]

ირანის ისლამურმა რესპუბლიკამ უყურადღებოდ არ დატოვა სოლეიმანთან დაკავშირებული „შეურაცხყოფა“ და ***ერაყში აშშ-ის სამხედრო ბაზების მიმართულებით 35 ბალისტიკური რაკეტა გაუშვა***. მოგვიანებით გაჩნდა ინფორმაცია, რომ ერაყის ხელისუფლებამ ამერიკელები გააფრთხილა და სამხედროებმა ბუნკერებში ჩასვლა მოასწრეს.[96]

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

ირანს ასევე თავის ტკივილად ექცა თეირანის აეროპორტში ჩამოვარდნილი უკრაინული თვითმფრინავი, სადაც 178 მგზავრი და

95 Rouhani H. Never threaten the Iranian nation: Rouhani tells Trump, Alarabiya, 2020, p 1. https://english.alarabiya.net

96 Trump D. Trump says ‘Iran appears to be standing down’ following its retaliatory attacks against Iraqi bases housing US troops, CNN, 2020, p 1. https://edition.cnn.com

ალი რაბიეი (1955)

ეკიპაჟის 9 წევრი დაიღუპა. ამერიკელების მტკიცებით, სამგზავრო თვითმფრინავი ირანელებმა ააფეთქეს რუსული რაკეტის გასროლით. **ირანის ისლამური რესპუბლიკა ამერიკის შეერთებულ შტატებს** დიდ ტყუილში ადანაშაულებს. მთავრობის პრესსპიკერმა, **ალი რაბიეიმ** განაცხადა, რომ ასეთი დიდი სიცრუისთვის პასუხისმგებლობას არავინ აიღებს. მისივე თქმით, ეს არის ფსიქოლოგიური სპეცოპერაცია **ირანის ისლამური რესპუბლიკის** წინააღმდეგ. თუმცა ამ მხრივ საინფორმაციო ომი დიდხანს არ გაგრძელებულა, 11 იანვარს ირანის ისლამური რესპუბლიკის ხელისუფლებამ აღიარა, რომ თვითმფრინავი შეცდომით ჩამოაგდეს და ამას „ადამიანური შეცდომა“ უწოდეს.[97]

ვაღიაროთ, ამ სამხედრო დაპირისპირებასა და საინფორმაციო ომში **ირანის ისლამური რესპუბლიკა** პირწმინდად დამარცხდა. თუმცა რას მოიმოქმედებს შემდგომში ეს არაპროგნოზირებადი 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 ისლამური რესპუბლიკის** პარლამენტმა ერთხმად დაამტკიცა და „ის ყველა ამერიკელ სახმედროზე, პენტაგონის თანამშრომელზე და იმ პირებზე ვრცელდება, ვინც ირანელ გენერალ **სოლეიმანის** მკვლელობაზეა პასუხისმგებელი. **ირანის ისლამური რესპუბლიკის** პარლამენტმა ასევე მხარი დაუჭირა **„ისლამური რევოლუციის გუშაგთა კორპუსის“** ელიტური ქვედანაყოფის **„ალ-კუდსის“** დაფინანსების 200 მილიონი ევროთი გაზრდას. აღნიშნული

97 კუპრეიშვილი თ. “ყველაფერი, რაც ვიცით უკრაინული თვითმფრინავის კატასტროფაზე”. საინფორმაციო სააგენტო “ნეტგაზეთი”, 2020, გვ. 1. https://netgazeti.ge

ქვედანაყოფი **ირანის ისლამური რესპუბლიკის** ფარგლებს გარეთ სპეცოპერაციების ჩატარებაზეა პასუხისმგებელი.[98]

ირანის ისლამური სახალიფოს შესაძლებლობები და კიბერუსაფრთხოების სისტემები

ამერიკის შეერთებული შტატები დათმობას არ აპირებს. ჯერ კიდევ სათავეში მყოფმა უკმაყოფილო **დონალდ ტრამპმა** ბევრჯერ 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:

დონალდ ტრამპი (1946)

„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".[99]

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

98 ახალაია ლ. "ირანმა აშშ-ის სამხედრო ძალები „ტერორისტულ ორგანიზაციად" გამოაცხადა", საქართველოს საზოგადოებრივი მაუწყებელი, 2020, გვ. 1. https://1tv.ge,

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

კიბერუსაფრთხოების ბიურომ 2015 წელს შეიმუშავა სტრატეგია, სადაც (თავი 35) საუბარია **ირანის ისლამური რესპუბლიკის** კიბერშესაძლებლობებსა და ამ სახელმწიფოს ინტერესებზე. დღეს ყველა ექსპერტი აღნიშნავს, რომ საქართველოსა და ირანს შორის კი არის ნორმალური ურთიერთობა ეკონომიკური და კულტურული ურთიერთობის თვალსაზრისით, მაგრამ ის მაინც ითვლება საფრთხედ, რადგან რუსეთთან ერთად წარმოადგენს ძლიერ კიბერმოთამაშეს არა მხოლოდ რეგიონში, არამედ მსოფლიოში. ირანის ისლამურ რესპუბლიკაში შექმნილია ასეულობით კიბერორგანიზაცია, რომლებიც მუშაობენ სხვადასხვა საკითხებზე - მაგალითად, პოლიტიკურ კულტურულ და რელიგიურ თემებზე. ამათგან ყველაზე ძლიერ დანაყოფს წარმოადგენს **ICA**, რომელიც შეიქმნა **"ისლამური რევოლუციის მცველების"** მიერ 2005 წელს და კავშირშია ქვეყნის შეიარაღებულ ძალებთან. ეს ორგანიზაცია კიბერთავდასხმებს ანხორციელებს ირანის საზღვრებს გარედან, დიდი ბრიტანეთიდან, ჩინეთიდან, პაკისტანიდან და საუდის არაბეთიდან.

როგორ უნდა გაუმკლავდეს საქართველო ასეთ დიდ საფრთხეს, რომელიც შეიძლება ერთ დღესაც მთელი ძალებით ამუშავდეს? რასაკვირველია, გამოსავალი მხოლოდ ერთია - მჭიდრო თანამშრომლობა უსაფრთხოების კუთხით ამერიკის შეერთებულ შტატებთან, ევროპის წამყვან სახელმწიფოებთან და ნატოსთან, რასაც შედეგად უნდა მოჰყვეს კვალიფიციური კადრების მომზადება და ახალი ტექნოლოგიების ათვისება. ასევე, დაზვერვისა და კონტრდაზვერვის გაძლიერება მთელი რეგიონის მასშტაბით.


ჯავად ზარიფი (1960)

2019 წლის სექტემბერში ირანის ისლამური რესპუბლიკის საგარეო საქმეთა მინისტრმა **ჯავად ზარიფმა** კომპიუტერული ვირუსი **Stuxnet**-ი ახსენა და აშშ-ის 2020 წლის საპრეზიდენტო არჩევნებში ჩარევის ბრალდებებიც უარყო. მისი თქმით, თეირანი

არჩევნებზე უპირატესობას არცერთ მხარეს არ ანიჭებს და არც სხვა სახელმწიფოების შიდა საქმეებში ერევა.

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

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

როდესაც ვსაუბრობთ ირანზე, უნდა გავიხსენოთ ისიც, რომ ამ ქვეყანას 2012 წლიდან მოყოლებული, კიბერკონფლიქტი აქვს მეზობელ აზერბაიჯანთანაც, რასაც ასეულობით ვებგვერდის „დაბომბვა“ მოჰყვა. 2012 წლის იანვარში აზერბაიჯანელ ჰაკერთა ჯგუფმა, რომელიც საკუთარ თავს **„ნამდვილი აზერბაიჯანის კიბერარმიას“** უწოდებს, შეტევა განახორციელა ირანის ვებსაიტებზე, რაც გახლდათ პასუხი წინა დღეს განხორციელებულ იერიშებზე. აზერბაიჯანის ათამდე ოფიციალური - მათ შორის, პრეზიდენტ **ალიევის**, მმართველი პარტიის, საკონსტიტუციო სასამართლოს, შინაგან და კომუნიკაციების

სამინისტროების საიტები გახდა მიუღწეველი. თუკი ვინმე ამ საიტებზე შესვლას შეეცდებოდა, პირველ გვერდზე ხვდებოდა ინფორმაცია, რომ ამაში პასუხისმგებელი აზერბაიჯანას კიბერარმიაა და ბაქო „ებრაელებს ემსახურება“. იმავე დღეს მოხდა თავდასხმა ისრაელის ვებსაიტებზე. მათ შორის იყო საავიაციო კომპანია **„ელ ალის“** და თელ-ავივის ბირჟის საიტები. ირანსა და აზერბაიჯანს შორის იმ პერიოდში ურთიერთობა დაიძაბა იმის გამო, რომ თეირანმა ბაქო ისრაელთან თანამშრომლობაში დაადანაშაულა. ისრაელი ნავთობის მნიშვნელოვან ნაწილს აზერბაიჯანისგან იღებს. იმავე წლის დეკემბერში აზერბაიჯანის საგარეო საქმეთა მინისტრი ვაშინგტონში სიტყვით გამოვიდა და ირანი სომხეთთან თანამშრომლობაში ამხილა, ამ ქვეყანას მთიანი ყარაბახის ოკუპაციაში ეხმარებაო. მოკლედ, პერიოდულად იქმნება შთაბეჭდილება, რომ ირანსა და აზერბაიჯანს შორის თბილი ურთიერთობაა (თუნდაც ერთმორწმუნეობის გამო), მაგრამ სინამდვილეში საქმე სხვანაირადაა - ირანისთვის ყველა მტერია, ვინც საქმეს დაიჭერს ამერიკის შეერთებულ შტატებთან და ისრაელთან, თუნდაც ეკონომიკური თვალსაზრისით.

ჩრდილო ატლანტიკური ალიანსის სტრატეგიის ყველა კონცეფცია ითვალისწინებს კიბერთავდაცვის საკითხებს და ყოველწლიურად იხარჯება მილიარდობით დოლარი. მით უმეტეს, მეტი იქნება საჭირო, თუკი ჩრდილო-ატლანტიკური ალიანსი ახლო აღმოსავლეთშიც დაფუძნდება და შემდეგ დაიწყებს გაფართოებას. ბუნებრივია, ეს ყველაფერი ვერ განხორციელდება კიბერთავდაცვის სისტემების შექმნისა და არსებული სისტემების გაძლიერების გარეშე.

ციფრული ვალუტა

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

მაგალითისთვის ავიღოთ ერთ-ერთი პირველი და პოპულარული **კრიპტო-ვალუტა - ბიტკოინი**, რომელიც ქსელში 2008 წელს გამოჩნდა. მისი შექმნა **სატოში ნაკამოტოს** სახელით ცნობილ პროგრამისტს უკავშირდება. კრიპტო-ვალუტა სტანდარტული ვალუტისგან განსხვავებით არ იბეჭდება. იგი წარმოიქმნება, ინახება და იხარჯება ელექტრონულად. ის არ კონტროლდება არც ერთი სახელმწიფოს და არც ერთი ბანკის მიერ. **ბიტკოინის** წარმოშობა ხდება რთული მათემატიკური ფორმულირების შედეგად კომპიუტერული ქსელების საშუალებით. ტრადიციული ვალუტა ეფუძნება ოქროს ღირებულებას, ხოლო ციფრული ვალუტა ეფუძნება მათემატიკას. ბიტკოინის შექმნის პროცესს მაინინგი ეწოდება.[100]

ციფრული ვალუტის მაინინგისთვის აუცილებელია კომპიუტერებისა და სერვერების სისტემა. ბოლო დროს აქტიურად ჩნდება სპეციალური აპლიკაციები, რომლებიც ციფრული ვალუტის გენერირებას სმარტფონიდან ხდის შესაძლებელს. რაც შეეხება ბიტკოინს, მისი რაოდენობა მსოფლიო მასშტაბით ვერ იქნება **21 000 000**-ზე მეტი. ზოგადად, ციფრულ ვალუტაზე უამრავი ინფორმაცია და დეზინფორმაცია ვრცელდება, მაგრამ უშუალოდ ბიტკოინით განხორციელებული ტრანზაქციის გაყალბება თითქმის შეუძლებელია. ცნობილია, რომ ტრანზაციის მონაცემები ინახება ფრაგმენტულად და არა ერთ სერვერზე. მნიშვნელოვანია, რომ ბიტკოინით ანგარიშსწორება დიდი ხანია დაშვებულია ისეთ ონლაინ-მაღაზიებში, როგორიცაა **eBay**, **Amazon** და ა.შ.[101]

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

101 Hayes A. What Happens to Bitcoin After All 21 Million Are Mined?, Business & Economy Website Investopedia, 2020, p 1. https://www.investopedia.com

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

ელექტრონული ფული „P2P“ ტექნოლოგიაზეა აგებული, ის სრულიად დამოუკიდებელი და დეცენტრალიზირებული ქსელია. სწორედ ეს ქმნის შესაძლებლობას, ნებისმიერმა მომხმარებელმა პირდაპირ გადაიხადოს ან გადასცეს. გადარიცხვას, გადაცემას ამ შემთხვევაში ადასტურებენ ქსელის სხვა მომხმარებლები, რომლებსაც მაინერები ეწოდებათ. დასტური ხერხდება კრიპტოგრაფიული ხელმოწერით და ყოველი ხელმოწერის 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.[102] რა თქმა უნდა, აქ არ არის მხოლოდ ბიტკოინი, დღეს უამრავი მსგავსი ვალუტა არსებობს.

საქართველოში **ციფრული ვალუტა** არც თუ პოპულარობით სარგებლობს. თუმცა შეგვიძლია, ისეთი ქვეყნებიც მოვიყვანოთ მაგალითად, სადაც ბიტკოინი ოფიციალურ ღირებულებადაა დაშვებული - აშშ-ში ბიტკოინით დაშვებულია სავაჭრო საქმიანობის წარმოება. თუმცა იმ ქვეყნების რაოდენობა ბევრად სჭარბობს მსოფლიოში, სადაც ცდილობენ, ელექტრონული ვალუტა სამართლებრივად შეზღუდონ და აკრძალონ კიდეც, რადგან ვირტუალური ფული არ არის არც ერთი ეკონომიკური სისტემით ან ფიზიკური ღირებულებებით გამაგრებული. საყურადღებოა

102 გოგუაძე მ. “მომავლის ვალუტა ბიტკოინი – კრიპტოვალუტა”, სესხების შემდარეებელი კომპანია „ფინანსერი“, 2017, გვ. 1. https://financer.com

ის ფაქტიც, რომ 2015 წელს ევროპის უმაღლესი სასამართლოს დადგენილებით ბიტკოინის ყიდვა ფიზიკური ფულით შესაძლებელი იქნება დღგ-ს გარეშე.[103]

ამ ყველაფრის გათვალისწინებით, კრიპტო-ვალუტის მომავალი მაინც გაურკვეველია. თუმცა ის საკმაოდ მომხიბლავად გამოიყურება, როგორც მსხვილი კომპანიებისთვის, ასევე ცალკეული ადამიანებისთვის. აქვე აღსანიშნავია, რომ ჰაკერები კრიპტოვალუტასაც ძალიან კარგად იყენებენ თაღლითობისთვის, Ransomware - ის, ანუ გამოსასყიდის მოთხოვნით ჰაკერები შიფრავენ თქვენს მონაცემებს კომპიუტერში, შემდეგ კი ითხოვენ დიდ ანაზღაურებას მონაცემებზე წვდომის აღდგენის მიზნით. თუმცა გადახდის შემთხვევაშიც თქვენს მონაცემებზე წვდომა არ აღდგება. ამ ტიპის თაღლითობა მეტწილად ხდება ანონიმური კრიპტოვალუტების წყალობით - მაგალითად, ბიტკოინით.

კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების პოლიტიკა და სტანდარტები

ჩვენ ხშირად გვესმის და ვხედავთ, რომ ნატო და ევროკავშირი ერთობლივი თანამშრომლობით ცდილობენ, გაუმკლავდნენ სხვადასხვა გამოწვევებს, მათ შორის კიბერ და საინფორმაციო შეტევებს. თუმცა სხვადასხვა ქვეყნები ტექნოლოგიების ხარჯზე ინდივიდუალურადაც ცდილობენ თავდაცვას. მაინც ხშირად ისმება შეკითხვა: სად არის გამოსავალი? რა უნდა დაუპირისპიროს მსოფლიომ, სახელმწიფომ, ნატომ, ევროკავშირმა, საერთაშორისო თუ ადგილობრივმა ორგანიზაციებმა? ამაზეც არსებობს არაერთგვაროვანი პასუხები. მაგალითად, გასაგებია, რომ ნატო და ევროკავშირი კიბერ და საინფორმაციო ომის მიმართულებით წლების განმავლობაში აქტიურად მუშაობენ, ავითარებენ ამ სფეროს და ხარჯავენ მეტ ფინანსებს, ვიდრე აქამდე ხარჯავდნენ, მაგრამ ეს საკმარისი ნამდვილად არ არის.

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

რა თქმა უნდა, ბევრი შეგვიძლია ვისაუბროთ ნატოს, ევროკავშირის, აშშ-ის და თუნდაც საფრანგეთის ან გერმანიის მიღწევებზე, უამრავი მაგალითი შეგვიძლია მოვიყვანოთ კიბერშეტევებისა და საინფორმაციო ომის შესახებ, მაგრამ ჩვენ ვსვამთ კითხვას: სად არის გამოსავალი, როგორ უნდა დაამარცხოს განვითარებულმა კაცობრიობამ კიბერტერორიზმი? შევეცდებით, არსებული რეალობიდან გამომდინარე, ამ კითხვას ვუპასუხოთ.

კიბერუსაფრთხოების თემა იმდენად მრავალმხრივია, რომ რთულია, ერთი მიმართულებით განვიხილოთ. კიბერუსაფრთხოების სტანდარტები ფაქტობრივად მუშაობს როგორც პოლიტიკის ერთობლიობა, რომელიც განსაზღვრავს მეთოდებს ან/და მიდგომებს, სისტემების დაცვას სახელმწიფო უწყებებსა თუ კერძო ორგანიზაციებში. 21-ე საუკუნეში ბაზარზე უკვე არსებობს კიბერუსაფრთხოების რამდენიმე სტანდარტი - თითქმის ყველა ორგანიზაცია, რომელიც მუშაობს მაღალ დონეზე, ვალდებულია, დაიცვას ეს სტანდარტები, რადგან სრულად განსაზღვრავს უსაფრთხოებას.

უპირველესად უნდა ვახსენოთ ნატო და ევროკავშირი, ასევე წამყვანი ქვეყნები, რომლებიც მილიარდობით დოლარს ხარჯავენ კიბერუსაფრთხოების მიმართულებით. ყველაზე მეტი იხარჯება აშშ-ის, საფრანგეთისა და გერმანიის მხრიდან.

აქედან გამომდინარე, უნდა ვისაუბროთ **ნატოს სტანდარტიზაციის ოფისზეც (NSO - NATO Standardization Office)**, რომელსაც კიბერუსაფრთხოების საკითხი მოწინავე პოზიციებზე აქვს დაყენებული. აღნიშნული ორგანიზაცია კოორდინაციას უწევს, მხარს უჭერს და მართავს ნატოს სტანდარტიზაციის საქმიანობას, რომელიც ტარდება სპეციალური კომიტეტის **(CS)** უფლებამოსილებით. ასევე, **NSO** ეხმარება ნატოს სამხედრო კომიტეტს სამხედრო ოპერატიული სტანდარტების შემუშავებაში, რაც ხელს უწყობს ალიანსის სამხედრო ძალე-

ბის ეფექტურობის ზრდას.

მოგეხსენებათ, 2021 წლის ივნისში, ბრიუსელში ჩატარდა სამიტი, სადაც ნატოს ხელმძღვანელებმა გამოაქვეყნეს განცხადება. ეს კიდევ ერთხელ ადასტურებს კოლექტიური უსაფრთხოების ვალდებულებას. განცხადებაში განხილულია მიმდინარე სტრატეგიული საკითხები წარმოჩენილია ნატოს თავდაცვითი როლი კიბერსივრცეში. ნატოს პოლიტიკა იძლევა მე-5 მუხლის გამოყენების საშუალებას - ცალკეულ შემთხვევებში ალიანსი ამბობს, რომ ზოგიერთი კიბერშეტევა შეიძლება გავათანაბროთ შეიარაღებულ თავდასხმასთან, რამაც შეიძლება ავტომატურად გამოიწვიოს ნატოს მე-5 მუხლის ამოქმედება.

თუმცა, აქვე გასათვალისწინებელია, რომ კიბერშეტევების უმრავლესობა ძალის გამოყენების ზღვარს ქვემოთაა. როგორ რეაგირებს ნატო პროპორციულად **„დაბალი ხარისხის“** კიბერშეტევებზე? შეიძლება ზოგიერთმა ექსპერტმა კიბერსივრცეში ნატოს თავდაცვითი პორციზია გააკრიტკოს, მაგრამ მაინც უნდა აღინიშნოს - ე.წ. დაბალი ხარისხის კიბერშეტევებზე რეაგირება ალიანსს ყველაზე ნაკლებ რისკებს უქმნის. მაგალითად, დაბალი ხარისხის კიბერშეტევებში შეიძლება განვიხილოთ ისეთი შეტევა, რომელიც იპარავს ინფორმაციას ან ფინანსურ რესურსებს, აღნიშნული შეიძლება იყოს სახელმწიფო ან სანქცირებული, ხოლო თავდასხმის უკან, როგორც ცნობილია, ხშირად დგას რუსეთი, ჩინეთი ან ირანი. ნატოში განმარტავენ, რომ ასეთი კიბერშეტევები არ იწვევს ხანგრძლივ ეკონომიკურ ზარალს. შესაბამისად, მათზე საპასუხო კოლექტიური რეაგირება მიზანშეწონილად ვერ ჩაითვლება. **დაბალი ხარისხის** კიბერშეტევების დროს ძირითადად კმაყოფილდებიან დიპლომატიური კორპუსის გაძევებით და ეკონომიკური გავლენის გამოყენებით, ანუ სანქციებით. რეაგირების მოცულობა უნდა განისაზღვროს თავდასხმის ღირებულებით - თუ ზარალი შეფასდა 10 მილიონი აშშ დოლარით, სანქციაც უნდა იყოს პროპორციული - 10 მილიონი აშშ დოლარის. ამ განცხადებას არაერთგვაროვანი შეფასებები მოჰყვა, რადგან ძნელია ზუსტი

განსაზღვრა, თუ რა შედეგები მოჰყვება სანქციებს და დიპლომატიური ურთიერთობების გართულებას. მით უმეტეს, შესაძლებელია, სახელმწიფოს მიერ სანქცირებული თავდამსხმელები არ იყვნენ მთავრობის სრული კონტროლის ქვეშ.[104]

ოცდაათმა ქვეყანამ, რომლებიც ბრიუსელის სამიტზე იყვნენ წარმოდგენილნი, ერთობლივი განცხადება გამოაქვეყნეს:

„ჩვენ უფრო მეტად გამოვიყენებთ ნატოს, როგორც მოკავშირეებს შორის პოლიტიკური კონსულტაციების პლატფორმას, კიბერშეტევების მიმართულებით გამოცდილების გაზიარების და ეროვნული მიდგომების კუთხით, ასევე განვიხილავთ კოლექტიური საპასუხო შეტევის განხორციელებას და ასევე დავაკისრებთ ხარჯებს მათ, ვინც გვაზიანებს ჩვენ. ნატოს თავდაცვითი მანდატის დადასტურებით, ალიანსში გადაწყვეტილია, გამოიყენოს შესაძლებლობების სრული სპექტრი ნებისმიერ დროს, რათა აქტიურად შეაკავოს, დაიცვას და გაუმკლავდეს კიბერსაფრთხეების მთელ სპექტრს, მათ შორის ჰიბრიდული კამპანიების ფარგლებში განხორციელებულ საერთაშორისო სამართლის შესაბამისად“.

განცხადებაში ასევე აღნიშნულია, რომ ნატო, როგორც ორგანიზაცია, გააგრძელებს ადაპტირებას და გააუმჯობესებს კიბერთავდაცვით პოლიტიკას, კიდევ უფრო განავითარებს თავის შესაძლებლობებს.

ცხადია, აგრესორი სახელმწიფოები და მათ შორის ყველაზე აქტიური რუსეთი მრავალი მიმართულებით ახორციელებს კიბერშეტევებს, როგორც საქართველოზე, უკრაინაზე, ასევე ამერიკის შეერთებულ შტატებზე, აღარაფერს ვამბობთ დანარჩენ პოსტსაბჭოთა სივრცეზე.

ზემოთ უკვე აღვნიშნეთ, მიუხედავად დიდი მონდომებისა და დაუღალავი მუშაობისა, კიბერშეტევების გასანეიტრალებლად ნატოს ბრძოლა არ არის საკმარისი და დრო გადის, უფრო მეტი რესურსია

104 International Centre for Defence and Security - Eesti Estonia, “A Defence of Defence. NATO’s Response to Low-Grade Cyber-Attacks”, 2021, p. 1, https://icds.ee/en/a-defence-of-defence-natos-response-to-low-grade-cyber-attacks/

საჭირო. დღეს ყველა სპეციალისტი აღიარებს, ყველაზე ეფექტური გამოსავალი, როგორც საერთაშორისო, ასევე ინდივიდუალურ დონეზე, არის სტანდარტების დაცვა. რაც უფრო მეტი ადამიანი იქნება გათვითცნობიერებული, თუ როგორ დაიცვას თავი კიბერშეტევისგან, მით ნაკლები ზარალი მიადგება სახელმწიფო სტრუქტურებს, კერძო თუ საერთაშორისო ორგანიზაციებს.

მოდით, გავშალოთ თემა, თუ რას ნიშნავს საერთაშორისო სტანდარტები და რა გვაქვს ამ მიმართულებით კიბერუსაფრთხოების

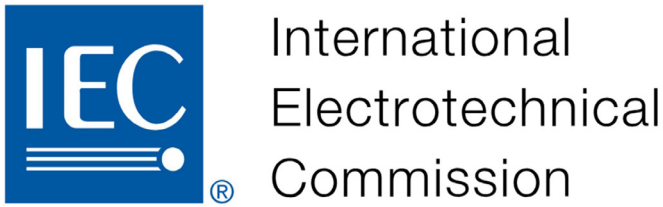
მხრივ: უკვე აღვნიშნეთ, გლობალური სტანდარტების ქვაკუთხეთი **სტანდარტების საერთაშორიოს ორგანიზაცია (ISO)** გახლავთ, რომელიც გვთავაზობს ერთგვარ თეორიულ და პრაქტიკულ მექანიზმებს, თუ როგორ შეიძლება ავირიდოთ ზარალი, როგორც სახელმწიფო, ასევე საერთაშორისო ან კერძო ორგანიზაციის დონეზე, იმ სტანდარტების, რეკომენდაციების გამოყენებით და დაცვით, რასაც ეს საერთაშორისო ორგანიზაცია იძლევა.

სტანდარტიზაციის საერთაშორისო ორგანიზაცია **ISO (International Organization for Standardization)** დაარსდა **1947** წელს. მისი წევრია **160** - ზე მეტი ქვეყნის შესაბამისი სტრუქტურა.

ISO აკონტროლებს მის ტექნიკურ კომიტეტებში მიმდინარე მუშაობას. საერთაშორისო ტექნიკური კომიტეტების საერთო რაოდენობა ამჟამად დაახლოებით **250**-ია. ყველა ორგანოს აქვს უფლება, კომიტეტებში დანიშნოს წევრები.

ISO (International Organization for Standardization) - ეს არის გლობალური ორგანო, რომელიც აგროვებს და მართავს სტანდარტებს სხვადასხვა დისციპლინისთვის მსოფლიო მასშტაბით. როდესაც ინდუსტრია დამოკიდებულია ინტერნეტსა და ციფრულ ქსელებზე, უფრო მეტი აქცენტი კეთება აღნიშნულ სტანდარტებზე, ტექნოლოგიურ მიდგომებზე. **ISO**-ს მიდგომები არის საუკეთესო იმის უზრუნველსაყოფად, რომ სამთავრობო თუ კერძო კომპანიების შიდა პროცესი მიზნად ისახავდეს მომხმარებლის მოთხოვნის დაკმაყოფილებას უმაღლეს დონეზე. როდესაც ცნობილია, რომ სახელმწიფო სტრუქტურა ან სხვა კომპანია იცავს და სერთიფიცირებულია **ISO**-ით განსაზღვრული ყველა ნორმით, ეს ხელს უწყობს ორ მხარეს შორის ნდობის ამაღლებას. დღეს საერთაშორისო დონეზე უკვე მთავარი მოთხოვნაა, თანამშრომლობის შემთხვევაში, ყველა დაინტერესებულ მხარეს უნდა გააჩნდეს **ISO**-ის სერთიფიკატი.[105]

ISO-სთვის სტანდარტიზაციის ყველაზე მნიშვნელოვანი პარტნიორია საერთაშორისო ელექტროტექნიკური კომისია **IEC. ISO**-სა და **IEC**



(International Electrotechnical Commission) – ს აქვთ ერთობლივი ტექნიკური კომიტეტები. მაგალითად, **ინფორმაციული ტექნოლოგიების სტანდარტიზაცია** არის ერთობლივი ძალისხმევით შექმნილი, რომელიც დაარსდა 1906 წელს. **IEC** შეიძლება ჩაითვალოს პირველ საერთაშორისო სტანდარტიზაციის ორგანიზაციად.

ელექტროტექნოლოგია იყო პირველი ინდუსტრია, სადაც აღია-

105 Watson T., "benefits of ISO 9001 and 27001 for companies and Their Clients", 2019, p. 1, https://skywell.software/blog/benefits-of-iso-9001-and-27001/

რეს საერთო ტერმინოლოგიის საჭიროება. საერთაშორისო სატელეკომუნიკაციო კავშირი **ITU** არის გაეროს სპეციალური ორგანიზაცია. სატელეკომუნიკაციო სტანდარტიზაციის მიზანია, საკომუნიკაციო ქსელების, ტერმინალური მოწყობილობებისა და საკომუნიკაციო სერვისების თავსებადობა. **ინფორმაციის უსაფრთხოების მენეჯმენტი ISMS (Information Security Management Systems)** მოიცავს შემოწმებას და გადახედვას - ამ შემთხვევაში აუდიტორები ეძებენ, თუ როგორ ხდება თქვენი პროცედურების დოკუმენტირება და გადახედვა რეგულარულად. აღნიშნულ პროცედურებში შედის:

ადამიანური რესურსების უსაფრთხოება, აქტივების მენეჯმენტი, წვდომის კონტროლი, კრიპტოგრაფია, ფიზიკური და გარემოსდაცვითი უსაფრთხოება, ოპერაციების უსაფრთხოება, კომუნიკაციების უსაფრთხოება, სისტემის შეძენა, განვითარება და მოვლა, მომწოდებლებთან ურთიერთობა, ინფორმაციული უსაფრთხოების ინციდენტების მენეჯმენტი, ბიზნესის უწყვეტობის მენეჯმენტის საინფორმაციო უსაფრთხოების ასპექტები შესაბამისობა.

ერთ-ერთი შეცდომა, რომელსაც ბევრი ორგანიზაცია უშვებს, არის ის, რომ **ISO**-ს სერტიფიკაციის ყველა პასუხისმგებლობა აკისრია ადგილობრივ **IT** გუნდს. მიუხედავად იმისა, რომ ინფორმაციული ტექნოლოგია არის **ISO 27001** ბირთვი, პროცესები და პროცედურები მაინც უნდა გაიზიაროს ორგანიზაციის ყველა ნაწილმა.

სტანდარტების საერთაშორისო ორგანიზაციის (ISO) ერთ-ერთ მიმართულებას წარმოადგენს კიბერუსაფრთხოების სტანდარტები. თანამედროვე დინამიურ ეპოქაში ყველაფერი ძველ დროსთან შედარებით სხვაგვარად მუშაობს. კიბერუსაფრთხოების თვალსაზრისით,

ყველა რეგიონში სხვადასხვა სტანდარტი შემოიღეს. როგორც აღვნიშნეთ, ამ მიმართულებით არაერთი საერთაშორისო თუ ადგილობრივი ორგანიზაცია ცდილობს სიახლეების დანერგვას. მათ შორის ნატო. თუმცა, იქიდან გამომდინარე, რომ მსოფლიოს ინტერნეტი აერთიანებს და გამოიყენება ყველგან, არსებობს სტანდარტები, რომლებიც ყველასთვის ერთი უნდა იყოს და უცვლელი დარჩეს.

უფრო კონკრეტულად, რა არის კიბერუსაფრთხოების სტანდარტი? იგი შეგვიძლია განვსაზღვროთ, როგორც წესების ერთობლიობა, რომელსაც სახელმწიფო სტრუქტურა ან/და ორგანიზაცია უნდა აკმაყოფილებდეს იმისათვის, რომ ზოგიერთ საკითხთან დაკავშირებით მოიპოვოს უფლება. მაგალითად, ონლაინ გადახდა, პაციენტის მონაცემების შენახვა და ა.შ. აღნიშნული სტანდარტები მოიცავს ძირითად წესებს, რომელსაც უწყება უნდა ემორჩილებოდეს.

კიბერუსაფრთხოების სტანდარტებში შედის რამდენიმე საერთო ძირითადი პუნქტი:

1. ISO 27001

სტანდარტი, რომელიც იცავს ორგანიზაციას ინფორმაციის უსაფრთხოების თვალსაზრისით. ამ სტანდარტის თანახმად, ორგანიზაციამ უნდა დანერგოს ახალი ტექნოლოგიები, სერვერები უნდა შეამოწმონ გარკვეული ინტერვალით, პერიოდულად.

2. PCI DSS (Payment Card Industry Data Security Standard)

აღნიშნული წარმოადგენს ინდუსტრიის მონაცემთა უსაფრთხოების სტანდარტს, რომელიც ბარათით გადახდის შემთხვევაშია საჭირო. ეს შეიძლება ჩაითვალოს ისეთ სტანდარტად, რომელიც უნდა აირჩიოს ორგანიზაციამ. ბიზნესსტრუქტურა, რომელიც ინახავს მომხმარებლის მონაცემებს (სახელი, გვარი, დაბადების თარიღი, ბარათთან დაკავშირებული ინფორმაცია), ვალდებულია, დაემორცილოს ამ სტანდარტს და შესაბამისობა უნდა მოხდეს განახლებული ტექნოლოგიით. სისტემა განუწყვეტლივ უნდა გადიოდეს უსაფრთხოების შემოწმებას, შეფასებას. აღნიშნული სტანდარტი შემუშავებულია ბარათების მწარმოებელთა მსოფლიო ბრენდების მიერ:

American Express, Visa, MasterCard, JCB, Discover.

3. HIPAA (ealth Insurance Portability and Accountability Act)

არის ჯანმრთელობის დაზღვევის პორტაბელურობისა და ანგარიშვალდებულების აქტი. ეს არის სტანდარტი, რომელმაც უნდა დაიცვას ჯანდაცვის კლინიკები. ამ შემთხვევაში დასაცავია პაციენტების მონაცემები. ნებისმიერ საავადმყოფოს უნდა ჰყავდეს ქსელის უსაფრთხოების ძლიერი ჯგუფი, რომელიც რეაგირებას მოახდენს ყველა ინციდენტზე. უსაფრთხოების კვარტალური ანგარიშები უნდა იყოს გამჭვირვალე, ყველა გარიგება უნდა განხორციელდეს დაშიფრულ რეჟიმში. სტანდარტი უზრუნველყოფს პაციენტის ჯანმრთელობასთან დაკავშირებული კრიტიკული ინფორმაციის დაცვას, რათა ადამიანმა თავი იგრძნოს უსაფრთხოდ.

4. Finra (Financial Industry Regulatory Authority)

წარმოადგენს ფინანსური ინდუსტრიის მარეგულირებელ ორგანოს. ეს სტანდარტი მიზნად ისახავს ფინანსური ორგანოების უსაფრთხოებას, რომლებიც ახორციელებენ დაფინანსებებს ან არიან აქტიურად ჩართულნი ფინანსურ ოპერაციებში. ამ სტანდარტში სისტემა უნდა იყოს უაღრესად დაცული - აუცილებელია მონაცემთა უსაფრთხოებისა და მომხმარებლის მონაცემების სრული დაცვა. ეს არის ერთ-ერთი უმნიშვნელოვანესი სტანდარტი, რომელსაც ყველა ფინანსური ორგანიზაცია უნდა აკმაყოფილებდეს.

5. GDPR (General Data Protection Regulation)

ეს არის მონაცემთა დაცვის ზოგადი რეგულაცია. განსაზღვრულია ევროკავშირის მიერ. ამ შემთხვევაშიც მთავარია მომხმარებელთა მონაცემების დაცვა და უსაფრთხოება.[106]

ევროპული სტანდარტიზაციის კომიტეტი

აღსანიშნავია, რომ 1961 წელს დაარსდა ევროპული სტანდარტიზაციის კომიტეტი **CEN** - ასოციაცია, რომელიც აერთიანებს სახელმწიფოების სტანდარტიზაციის ეროვნულ ორგანიზაციებს. იგივე

106 Pedamkar P., "Cyber Security Standards", 2020, p. 1, https://www.educba.com/cyber-security-standards/

ევროპული სტანდარტები მოქმედებს **CEN** – ის ყველა წევრ ქვეყანაში. ისინი ვალდებულნი არიან, დაამტკიცონ ევროპული და გააუქმონ ნებისმიერი წინააღმდეგობრივი სტანდარტი. **CEN**-ის მიერ დამტკიცებულ სტანდარტებს აქვთ აღნიშვნა **„EN“**, დაახლოებით 30 პროცენტი ემყარება გლობალურ **ISO**-ს სტანდარტებს.

CEN-ს აქვს 300-ზე მეტი ტექნიკური კომიტეტი, ანუ ევროპული სტანდარტიზაციის ჯგუფები. ყველა წევრს აქვს უფლება, მონაწილეობდეს ტექნიკურ კომიტეტებში. სამდივნოს მენეჯმენტი იძლევა შესაძლებლობას, დააკვირდეს სტანდარტების შემუშავებას, კერძოდ, გავლენა მოახდინოს მომავალი სტანდარტების შინაარსზე.

ელექტროტექნიკური სტანდარტიზაციის კომიტეტი **CENELEC (European Committee for Electrotechnical Standardization)** მართავს ევროპული ელექტროტექნიკური სტანდარტების შემუშავებას. მისი წევრია ევროკავშირის ყველა ქვეყანა და აღმოსავლეთ ევროპის სახე-

ლმწიფოები. **CENELEC** სტანდარტების 75 პროცენტი ემყარება გლობალური **IEC (International Electrotechnical Commission)** სტანდარტებს. ფინეთში ელექტროტექნიკურ სტანდარტიზაციაზე პასუხისმგებელი ორგანიზაცია არის **SESKO (Electrotechnical Standardization in Finland)**.

ევროპის სატელეკომუნიკაციო სტანდარტების ინსტიტუტი **ETSI**

(European Telecommunications Standards Institute) ავითარებს საერთაშორისო სატელეკომუნიკაციო სტანდარტებს. მისი წევრები არიან მმართველი ორგანოები საინფორმაციო ტექნოლოგიების სფეროში. ფინეთში სატელეკომუნიკაციო სტანდარტიზაციაზე პასუხისმგებელი ორგანიზაციაა **Traficom (Finnish Transport and Communications Agency). CEN, CENELEC** და **ETSI** შეიმუშავებენ სტანდარტებს ევროკომისიის მოთხოვნითაც. საბოლოო ჯამში ჰარმონიზებული სტანდარტები იძლევა უფრო დეტალურ მითითებებს და კონკრეტულ დირექტივებს.

ასიმეტრიული საფრთხეები და ჯიჰადისტების კიბერომი

ჩვენ ვსაუბრობთ კიბერომებზე, კიბერშეტევებზე, საინფორმაციო ომზე, პროპაგანდაზე, დეზინფორმაციაზე, ფეიკნიუსებზე და ზოგადად ჰიბრიდულ ომებზე, ტექნოლოგიების დადებით და უარყოფით მხარეებზე. რეალურად უნდა განვმარტოთ თუ ვის ხელში წარმოადგენს ტექნოლოგიური წინსვლა იარაღს და საფრთხეს. აქ მხოლოდ აგრესორ ქვეყნებზე კი არა, საუბარია არასახელმწიფოებრივ აქტორებზეც, რომლებიც კარგად ითვისებენ ახალ ტექნოლოგიებს. ტერორიზმს გააჩნია დიდი ისტორია და მისი უამრავი დეფინიცია არსებობს, ასევეა კიბერტერორიზმთან დაკავშირებით და ეს განმარტება უფრო სარწმუნოა: კიბერტერორიზმი ნიშნავს კომპიუტერული და სატელეკომუნიკაციო ტექნოლოგიების, მათ შორის ინტერნეტის გა-

მოყენებას ძალადობრივი ქმედებების შესასრულებლად, რომელიც საფრთხეს უქმნის სიცოცხლეს ან იწვევს სიკვდილს. კიბერტერორისტული აქტები მიზნად ისახავს პოლიტიკური ან იდეოლოგიური უპირატესობების მიღწევას დაშინებისა და მუქარის საშუალებით. ტერმინი „კიბერტერორიზმი“ პირველად გამოიყენეს 1980-იან წლებში. ზოგჯერ კიბერტერორიზმში მოიაზრებენ, როგორც კომპიუტერული ქსელების განძრახ დაზიანებას სხვადასხვა საშუალებებით, მაგალითად, ვირუსების, ფიშინგის წარმოებით და სხვა მავნე პროგრამებით.

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

საქართველოსთვის, ისევე როგორც მსოფლიოს მრავალი ქვეყნისთვის, ძირითად გამოწვევას ტერორისტული ორგანიზაცია **„ისლამური სახალიფოს“ („დაეში“)** და მასთან დაკავშირებული დაჯგუფებები წარმოადგენენ. **„დაეში“** მოქმედებას აგრძელებდა დასუსტებისა და ტერიტორიული დანაკარგების შემდეგ შემუშავებული ახალი სტრატეგიით. აღნიშნულის ფარგლებში **„დაეშისთვის“** პრიორიტეტული აღარ იყო მხარდამჭერების სირიასა და ერაყში მობილიზება. ტერორისტული ორგანიზაციის მოქმედების მთავარ იარაღად იქცა კონფლიქტის ზონის მიღმა ტერორისტული აქტების განხორციელება. **„დაეში“** მსოფლიოს სხვადასხვა ქვეყნებში მცხოვრებ რადიკალიზებულ პირებს ნებისმიერი საშუალებით ტერორისტული თავდასხმების განხორციელებისკენ მოუწოდებდა. ეს ორგანიზაცია თანამედროვე ტექნოლოგიების, მათ შორის, ინტერნეტსივრცისა და სოციალური ქსელების გამოყენებით, კვლავ აქტიურად ავრცელებდა საკუთარ იდეოლოგიას, ახდენდა ადამიანების გადაბირებას. როგორც ანგარიშში ვკითხულობთ:

„ალ-კაიდა“ აქტივობებს, ძირითადად ახლო აღმოსავლეთსა და აფრიკის კონტინენტზე მოქმედი რეგიონული დაჯგუფებების მეშვეო-

ბით ახორციელებდა. „თალიბანი“ განაგრძობდა ავღანეთის სამთავრობო ძალებსა და ქვეყანაში საერთაშორისო მისიით მყოფ სამხედროებზე თავდასხმებს».[107]

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.[108]

ინტერნეტსივრცეში ყოველდღიურად ჩნდება **ჯიჰადისტური** ქსელები მრავალნაირი ფორმით. ამ მხრივ მიდის სელექციური მუშაობა ახალი თაობის **ჯიჰადისტების** აღსაზრდელად. როგორც **ვახტანგ მაისაია** აღნიშნავს, ესენი არიან მეორე და მესამე თაობის **ჯიჰადისტები**, რომლებმაც უნდა იმუშაონ “მტრის ზურგში”.

ვახტანგ მაისაია (1972)

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 სამიზნეს, რომელსაც ასევე სჭირდება უფრო მეტი სიმძლავრეებით წინააღმდეგობის გაწევა. თანამედროვე მსოფლიოსთვის ერთ-ერთი უმთავრესი გამოწვევა ისეთი ტიპის ასიმეტრიული საფრთხეებია, როგორიცაა საერთაშორისო ტერორიზმი და ტრანსნაციონალური

107 “საქართველოში მცხოვრებ „დაეშის“ შესაძლო მხარდამჭერთა რაოდენობა და გავლენა შემცირდა”. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, 2019, გვ. 1. https://imedinews.ge

108 მაისაია ვ. „ისლამური ხალიფატის“ საინფორმაციო-პროპაგანდისტული/კიბერ-ვირტუალური ომის სპეციფიკა - „რბილი ძალის“ კონცეფტი”, მედიაჰოლდინგი “ჯორჯიან-თაიმსი”, 2017, გვ. 1. http://geotimes.com.ge

ორგანიზებული დანაშაული.

რას წარმოადგენს **ჯიჰადი** და რა საფრთხე შეიძლება იყოს საქართველოსთვის? სიტყვა **„ჯიჰადი“** არაბული წარმოშობისაა, სწრაფვასა და ძალისხმევას ნიშნავს. იგი კლასიკურ ტექსტებში მეტწილად ბრძოლისა და ომის მნიშვნელობით გამოიყენება. ხშირად იმოწმებენ ფრაზას ყურანიდან - **„ღვთის გზაზე ბრძოლა“**, რასაც მრავალი ინტერპრეტაცია მოეძებნა ზნეობრივი სწრაფვიდან დაწყებული, შეიარაღებული ბრძოლით დამთავრებული. მუსლიმური სამართლის მიხედვით, ომის წარმოება 4 ტიპის მტრის წინააღმდეგ არის გამართლებული: ურწმუნონი, განდგომილნი, ამბოხებულნი და ყაჩაღები. მართალია, ოთხივე ტიპის ბრძოლა ლეგიტიმურია, მაგრამ მხოლოდ პირველი 2 ითვლება **ჯიჰადად**. ამრიგად, **ჯიჰადი** რელიგიური ვალდებულებაა. წმინდა ომის ფენომენის განხილვისას, მუსლიმი სამართალმცოდნენი შემტევ და თავდაცვით **ჯიჰადს** განასხვავებენ. იერიშის დროს **ჯიჰადი** ზოგადად მუსლიმური საზოგადოების მოვალეობაა და იგი მოხალისეთა და პროფესიონალთა მიერ იწარმოება. თავდაცვით ომში ეს თითოეული მუსლიმის მოვალეობა ხდება. **ბინ ლადენმა** სწორედ ეს პრინციპი წამოსწია წინ თავის საომარ დეკლარაციაში შეერთებული შტატების წინააღმდეგ. მუსლიმური ტრადიციის მიხედვით მსოფლიო იყოფა ორ ნაწილად: **ისლამის სახლი (დარ ალ-ისლამი)**, სადაც მუსლიმური მმართველობაა და **ომის სახლი (დარ ალ-ჰარბი)** - დანარჩენი მსოფლიო, სადაც ურწმუნონი სახლობენ. **ჯიჰადი** უნდა გაგრძელდეს მანამ, სანამ მთელი მსოფლიო ან ისლამურ რჯულზე არ მოექცევა, ან მუსლიმურ სამართალს არ დაემორჩილება. ის, ვინც **ჯიჰადს** აწარმოებს, დაჯილდოვებულ იქნება ორივე ცხოვრებაში. მას ექნება ქონება მიწიერ ცხოვრებაში და სამოთხე - შემდგომში. ზოგჯერ **ჯიჰადს** ჯვაროსნული ბრძოლის მუსლიმურ სინონიმად მოიაზრებენ და ეს ორი ფენომენი მეტ-ნაკლებად ერთნაირად აღიქმება.[109]

109 ქაზუმოვი ო. “ძალადობა რელიგიის სახელით და ინტერპრეტაციის მნიშვნელობა”. ტოლერანტობისა და მრავალფეროვნების ინსტიტუტი (TDI), 2018, გვ. 1.

2013 წლის 6 ივნისს “იუთუბზე” შოკისმომგვრელი ვიდეო გავრცელდა სახელწოდებით: **“ჯიჰადი ავღანეთში საქართველოს ჯარების წინააღმდეგ”**[110], რომელიც შეიცავდა მუქარას ავღანეთის მისიაში მონაწილე საქართველოს შეიარაღებული ძალების წინააღმდეგ. მუქარისშემცველი ვიდეოს გავრცელებას მოჰყვა მსხვერპლი. სანამ ქართველი ჯარისკაცების დაღუპვის შესახებ გახდებოდა ცნობილი, ამ ვიდეოს საქართველოს ხელისუფლებაში სერიოზულად არ აღიქვამდნენ. მისი წარმომავლობის დადგენაზე მოკვლევა დაიწყო თავდაცვის სამინისტრომაც. გავრცელებული ტექსტი კი ასეთი გახლდათ:

“ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!”[111]

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


გიორგი თავდგირიძე

“საქართველოს ბიუჯეტიდან საკმაოდ მნიშვნელოვანი სახსრებია გამოყოფილი ასეთი საქმიანობისთვის, საზღვრებისა და აეროპორტების გაკონტროლებისთვის, ამიტომ შესაბამისი სამსახურები უნდა მოიქცნენ ისე, როგორც მსგავსი მუქარის შემთხვევის დროს იქცევიან”.[112]

მართალია, ტერორისტების მთავარ სამიზნედ საფრანგეთი, ზო-

---

https://www.tdi.ge

110 ზამან ჰ. “Youtub-ზე გავრცელებული ვიდეოს წარმომავლობა გაურკვეველია”, საინფორმაციო “ფორ.ჯი”, 2013, გვ. 1. https://for.ge

111 ზამან ჰ. “თალიბანი საქართველოს შურისძიებით ემუქრება? - შოკისმომგვრელი ვიდეო YouTube-იდან”. მედიაჰოლდინგი “პალიტრა”, 2013, გვ. 1. https://www.palitravideo.ge

112 “ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!”. ტერორისტული ორგანიზაცია „ჯიჰადი“, 2013, გვ. 1. https://for.ge

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

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

"ტერორისტული საქმიანობისთვის ქვეყნიდან გამგზავრებისა და შემოსვლის პრევენციის მიზნით, შსს-სთან თანამშრომლობით სათანადოდ ხორციელდება სასაზღვრო კონტროლი (საზღვრის მწვანე ზოლის, ასევე სასაზღვრო გამტარი პუნქტების). ხდება ვიზიტორებთან გასაუბრება. ყველა სასაზღვრო-გამტარი პუნქტი აღჭურვილია ბირთვული და რადიოაქტიური მასალების, ნივთიერებების დეტექტორებით".[113]

აღსანიშნავია, რომ ზუსტად ტერორიზმითა და ორგანიზებული

113 "ტერორიზმთან ბრძოლა". საქართველოს სახელმწიფო უსაფრთხოების სამსახური, 2015, გვ. 1. https://ssg.gov.ge

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

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

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

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

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

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

“კიბერშეტევა ხდებოდა იმ ვებპლატფორმებიდან, რომლებიც მანამდე კრიმინალს ემსახურებოდა. კონკრეტულად, ეს იყო დარქვები, რომლებიც რუსული ორგანიზებული დანაშაულის პლატფორმაა. დიფეისებში, რომელბსაც შეტევისას იყენებდნენ, კონკრეტული ქივორდები იყო: ნატო, საქართველო და ამერიკა, სამხედრო თანამშრომ-

ანდრია გოცირიძე

ლობა. გარდა ამისა, რამდენიმე დიფეისი, გაკეთებული იყო ომამდე 2 წლით ადრე, უბრალოდ, 2008-ში აამოქმედეს".[114]

კიბერუსაფრთხოების ექსპერტის, **ანდრია გოცირიძის** თქმით, 2007-2008 წლებში ესტონეთისა და ლიეტუვას წინააღმდეგ განხორციელებული **DDoS** კიბერშეტევები სადამსჯელო ოპერაციას და ერთგვარ პოლიტიკურ გზავნილს წარმოადგენდა, რომლის მიზანიც სამოქალაქო მღელვარებისა და მასობრივი არეულობის გამოწვევა იყო, თუმცა არ უკავშირდებოდა ამა თუ იმ სამხედრო ამოცანის შესრულებას და არც საომარი მოქმედებების ინფორმაციულ უზრუნველყოფას ემსახურებოდა. რაც შეეხება რუსეთ-საქართველოს ომს, აქ კიბერელემენტის გამოყენება უშუალოდ კონვენციური მოქმედებების ორგანიზებულ თანმხლებ პროცესს წარმოადგენდა, რომლის მიზანიც რუსეთის შეიარაღებული ძალებისათვის სამხედრო მიზნების შესრულების გაიოლება, საინფორმაციო ვაკუუმის შექმნა, ინფორმაციული უპირატესობის მოპოვება და კონფლიქტის შესახებ რუსული ნარატივის დამკვიდრება იყო.[115]

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

114 გეგიძე თ. "როგორ მოვიგერიეთ კიბერთავდასხმა და პროპაგანდა 2008 წელს", სააგენტო "ონ.ჯი", 2019, გვ. 1. https://on.ge/

115 გოცირიძე ა. "რუსეთ-საქართველოს 2008 წლის ომის კიბერგანზომილება", საქართველოს სტრატეგიისა და საერთაშორისო უსაფრთხოებების კვლევის ფონდი, 2019, გვ. 1. https://www.gfsis.org

დასავლური არასამთავრობო ორგანიზაციები თავიანთ ანგარიშებში ასევე 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“**.[116] მათი მტკიცებით, ეს ორგანიზაციები გამოირჩევიან ანტიდასავლური რიტორიკით და ანალიტიკური ნაშრომებისა თუ სტატიების გამოქვეყნებისას ეფუძნებიან რუსულ წყაროებს. საჯარო რეესტრის მონაცემების მიხედვით, პრორუსული არასამთავრობო ორგანიზაციების დამფუძნებელთა და ხელმძღვანელთა სიაში ხშირად ერთი და იგივე პირები ფიქსირდებიან. ორგანიზაციებს შორის კავშირი მათ ვებ-გვერდებზეც არის მითითებული. გარდა ამისა, პრორუსული არასამთავრობო ორგანიზაციების ქსელს კავშირი აქვს ანტიდასავლური რიტორიკით გამორჩეულ საინფორმაციო საშუალებებთან. შესაძლოა, პროდასავლური არასამთავრობო ორგანიზაციები ნაწილობრივ არც ტყუიან, მაგრამ მათ მიერ დასახელებული ორგანიზაციები ამტკიცებენ, რომ საქმე პირიქითაა - დასავლურ კურსს ხელს უშლიან ის ორგანიზაციები, რომლებიც ყალბი პროდასავლური შეფუთვით არიან წარმოდგენილნი. თუ ე.წ. **“ევრაზიული”** დასახელების ორგანიზაციები თავიანთ ორიენტაციას არ მალავენ და ხშირად ამბობენ, რომ ისინი რუსულ კი არა, ქართულ საქმეს აკეთებენ, პროდასავლურად შეფუთულ ორგანიზაციებში ხშირად მართლაც ჭირს გარკვევა - არის შემთხვევები, როცა ამა თუ იმ საკითხის კვლევისას აშკარად შეინიშნება პირადი ინტერესები.

არასამთავრობო ორგანიზაციების ნაწილი იმაზეც წერს, რომ საქართველოში მომრავლდა პრორუსული ორიენტაციის პოლიტიკური პარტიები. ხშირად კეთდება განცხადებები, თითქოს რიგი პოლიტი-

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

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

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

რუსეთი რომ საქართველოსთვის მრავალი პრობლემის სათავეა, ეს ცხადია, მაგრამ საზოგადოებაში არსებობს კიდევ ერთი სახის ილუზია, რომელიც მეზღაპრეთა მიერ გახლავთ მოგონილი: ბევრი

ქადაგებს იმის თაობაზე, თითქოს რუსეთი დღე-დღეზე დაიშლება, გაცამტვერდება და გვეშველება; მეორე - რუსეთში მოვა დემოკრატიული ხელისუფლება და ტერიტორიებს უპრობლემოდ შემოვიერთებთ; მესამე - რუსეთს მალე ნავთობი შემოაკლდება, გაკოტრდება და ასევე გვეშველება. შესაძლოა, ოდესღაც ყველაფერი მოხდეს, მაგრამ ასეთი მოსაზრებებით შორს ვერ წავალთ. რა მოჰყვება რუსეთის დაშლას კაცობრიობისთვის და ასევე რა მოჰყვება რუსეთში დემოკრატიული ხელისუფლების მოსვლას, ეს ჯერ არავინ იცის.

ამ ფონზე არსებობს ვირტუალური საფრთხე - კიბერომი და საინფორმაციო ფრონტი, რომელიც გახსნილია რამდენიმე მიმართულებით. ერთია ღია პროპაგანდა, მეორეა - შენიღბული პროპაგანდა, ანუ პროდასავლური შირმით რუსეთის ინტერესების გატარება. რუსეთი ამერიკის შეერთებულ შტატებს, ბალტიის ქვეყნებს, უკრაინას, საქართველოს, ევროპასა და დანარჩენ სამყაროს უტევს კიბერმეთოდებით, წინასწარ დამუშავებული ჰიბრიდული ხერხებით და დეზინფორმაციით. მაგალითად, რუსები სლოვაკეთსა და ჩეხეთში ამერიკის ენერგეტიკული პოლიტიკის კრიტიკაზე არიან ორიენტირებულნი და ცდილობენ წარმოაჩინონ, თითქოს აშშ მხოლოდ საკუთარი ინტერესებიდან გამომდინარე მოქმედებს, მსოფლიოს სხვადასხვა კუთხეში კონფლიქტების პროვოცირებას უწყობს ხელს. რუმინეთში რუსეთიდან დაფინანსებული მედიასაშუალებები ცდილობენ, ევროკავშირში გაწევრიანება შეცდომად წარმოაჩინონ და დემოკრატიული ინსტიტუტები დააკნინონ. შვედეთში მთავრობა სექსუალური გარყვნილების მიმდევრად არის წარმოჩენილი. უკრაინაში მიდის პროპაგანდა კორუფციაზე, სიღარიბეზე, უწესრიგობასა და დასავლეთის მიერ მართულ „მარიონეტულ“ რეჟიმზე. ლიტვაში, ლატვიასა და ესტონეთში პროპაგანდისტული მანქანა მუშაობს იმაზე, თუ როგორი დისკრიმინაციის ქვეშ არიან ამ ქვეყნებში რუსები მათი ეთნიკური თუ ენობრივი მახასიათებლების გამო.[117]

117 ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., “კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტი-

მიუხედავად რუსული აგრესიისა, ყველა პოსტსაბჭოთა ქვეყნის სასახელოდ უნდა ითქვას, რომ საბჭოთა კავშირის დაშლის შემდეგ არსად დაწყებულა რუსებისა და რუსულენოვანი მოსახლეობის მასობრივი დევნა-შევიწროება, ადგილი არ ჰქონია სისხლისღვრასა და სისასტიკეს. ალბათ ამ შემთხვევაში გადამწყვეტი როლი შეასრულა იმ ფაქტორმა, რომ 70 წლის განმავლობაში მაინც ჩამოყალიბდა ნათესაური კავშირები და სხვა სახის კულტურული თუ სოციალური ურთიერთობები. იმის ნაცვლად, რომ რუსეთი გაფრთხილებოდა ამ ურთიერთობებს, დაიწყო საბჭოთა კავშირის მსგავსი სივრცის შექმნა, სადაც მუდმივად ანხორციელებს სამხედრო აგრესიას და ეწევა ჰიბრიდულ ომს. ცნობილია, რომ ბალტიისპირეთში რუსეთის პროპაგანდის მთავარი მამოძრავებელი ძალაა **„Первый Балтийский канал“**, ასევე ონლიაინსაიტი **Regnum.ru**, რომელიც 10 წელზე მეტია ფუნქციონირებს. ბოლო დროს რუსებმა აამუშავეს საიტი **Baltnews**, სადაც ანონიმურად თავსდება ინფორმაცია და ახალი ამბები ესტონურ, ლიეტუვურ და ლატვიურ ენებზე.[118]

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

კის აუცილებლობა”, თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016, გვ. 5-25.

118 ვაჩარაძე ა. “რუსეთის საინფორმაციო ომი - სტრატეგიები და მიზნები”, საგენტო “დამოუკიდებლობა”, 2015, გვ. 1. http://www.damoukidebloba.ge

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

“იმ შემთხვევაში, თუ ომი რეალურად იქნება, მათი მიზანი კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურა გახდება, მათ შორის აეროპორტები, ნავსადგურები, სადგურები და სხვა ინფრასტრუქტურა, რათა ამ ქვეყნებში შოკი გამოიწვიოს და ადგილობრივმა მოსახლეობამ ხელისუფლებისგან ზავი ითხოვოს”.[119]

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


სერგეი ლავროვი (1950)

2018 წლის ივნისში პენტაგონმა აღიარა, რომ რუსეთის შეჭრის შემთხვევაში, ბალტიისპირეთის ქვეყნების და პოლონეთის დაცვას ვერ მოასწრებს. **“ვაშინგტონ პოსტის”** ცნობით, ამ დასკვნამდე პენტაგონში ევროკავშირის ქვეყნებისა და რუსეთის სამხედრო წინააღმდეგობის სიმულაციის შედეგად მივიდნენ. როგორც გამოცემა იტყობინება: „სანამ აშშ-ის არ-

119 ბასილაია ე. “გერმანული მედია: რუსები 2008 წელს ბირთვული იარაღის გამოყენებას აპირებდნენ”. გაზეთი “რეზონანსი”, 2017, გვ. 1. http://www.resonancedaily.com

მიის 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, ხიდებიც კი ისეთი სუსტია, ამერიკული ტექნიკის წონას ვერ გაუძლებს. საზღვრებზე პრობლემებს ქმნის ევროპული ბიუროკრატიაც.[120] რუსეთს პოსტსაბჭოთა სივრცეში გახსნილი აქვს რამდენიმე ფრონტი, სადაც ჩართულნი არიან ხელისუფლების მაღალჩინოსნები. მაგალითად, 2019 წლის სექტემბერში საგარეო საქმეთა მინისტრმა **სერგეი ლავროვმა** აღნიშნა, რომ ბალტიისპირეთის ქვეყნები დღემდე ევროკავშირის დოტაციაზე ცხოვრობენ და მათ დახმარება მალე შეუწყდებათ.[121]

ვიაჩესლავ მოლოტოვი (1890-1986)

რასაკვირველია, ეს არის გამიზნული დეზინფორმაცია, რომლის მეშვეობითაც რუსები ცდილობენ, ბალტიის ქვეყნების მოსახლეობას გაუჩინონ ნიჰილიზმი და უიმედობის შეგრძნება - აგერ, დღეს ევროკავშირი გეხმარებათ, დასავლეთის კმაყოფაზე ხართ, მაგრამ ხვალ ეს დახმარება შეგიწყდებათო. რუსეთი ანხორციელებს მუდმივ იდეოლოგიურ ზეწოლას - მაგალითად, კრემლი დაუსრულებლად ამტკიცებს, რომ ბალტიის სახელმწიფოების გასაბჭოება საერთაშორისო სამართლის ნორმების შესაბამისად მოხდა და ტერმინი **”ოკუპაცია”** აქ არ შეიძლება იქნას გამოყენებული. კრემლი მალავს ფაქტს, როცა ამ ქვეყნების საგარეო საქმეთა მინისტრებს ე.წ. შეთანხმებაზე ხელის მო-

120 Person R. 6 reasons not to worry about Russia invading the Baltics, The Washington Post, 2015, p 1. https://www.washingtonpost.com

121 იაგორაშვილი ი. “რუსეთის 2 მითი ბალტიისპირეთის ქვეყნების შესახებ”. ვებ-გვერდი “My the Detector”, 2019, გვ. 1. https://www.mythdetector.ge

წერა არ სურდათ, ისინი შიშობდნენ, რომ ეს მათ ნეიტრალიტეტს დაარღვევდა. უარის შემდეგ კი **მოლოტოვმა** ესტონეთის წარმომადგენელს ასე მიმართა:

“ჩვენ დიდხანს ლოდინი არ შეგვიძლია. გირჩევთ, დაეთანხმოთ საბჭოთა კავშირის სურვილს, რათა თავიდან აიცილოთ უარესი. ნუ აიძულებთ საბჭოთა კავშირს ძალის გამოყენებას.”.[122]

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.

საინფორმაციო ომი გაცილებით ადრე დაიწყო, ჯერ კიდევ მაშინ, როცა არ არსებობდა ამდენი მედიასაშუალება და სოციალური ქსელი. ეს არის ერთ-ერთი მძლავრი იარაღი, რომლის საშუალებითაც შესაძლებელია არეულობის შეტანა მოწინააღმდეგის ბანაკში. ამის საუკეთესო მაგალითი გახლავთ ფაშისტური გერმანიის მიერ წარმოებული პროპაგანდა მეორე მსოფლიო ომის პერიოდში. იღებდნენ ე.წ. დოკუმენტურ ფილმებს სხვა ქვეყნების ლიდერებზე, მდგომარეობაზე, მოსახლეობაზე და ავრცელებდნენ სხვადასხვა ფორმებით. ეს, რა თქმა უნდა, იწვევდა გარკვეულ დემორალიზაციას და ნერგავდა შიშს, იმედგაცრუებას. იგივე მეთოდს იყენებდა საბჭოთა კავშირიც. ომის დასრულების შემდეგ დაიწყო ახალი ერა, სამმა ზესახელმწიფომ - საბჭოთა კავშირმა, დიდმა ბრიტანეთმა და ამერიკის შეერთებულმა შტატებმა გადაინაწილეს მსოფლიო. ბუნებრივია, ამავე დროს დაიწყო კიბერომების ახალი ეტაპი. თითქოს ქვეყნებს შორის დაპირისპირება აღარ არსებობდა, მაგრამ ბოლოს საქმე იქამდე მივიდა, რომ საბჭოთა კავშირიც დაინგრა და ვარშავის პაქტიც გაუქმდა. ეს კი გამოიწვია დიდძალმა ფინანსებმა და საინფორმაციო ომმა.

რამდენად დიდი საფრთხეა დღევანდელი მსოფლიოსთვის

122 იაგორაშვილი ი. «მარია ზახაროვა სსრკ-ის მიერ ესტონეთის ოკუპაციას უარყოფს». ვებ-გვერდი «My the Detector», 2020, გვ. 1. https://www.mythdetector.ge

კიბერთავდასხმები, საინფორმაციო ომი და ე.წ. ფეიკ-ნიუსი, როგორც მოვლენა? ჩვენი საზოგადოება არის მუდმივად დაძაბულ მდგომარეობაში, მუდმივად მიდის საინფორმაციო ომი, ანუ ფეიკ-ნიუსებით ბრძოლა.

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? ვფიქრობთ, აქ უკვე დაკვეთასთან გვაქვს საქმე. შეიძლება სადღაც რაღაცა მოხდა, ჟურნალისტმა ფაქტი დაიჭირა, დაინტერესებული პირებისგან აიღო ფული და რუსებს მიაწება საქართველოც, შექმნა ყალბი სკანდალი, მაგრამ ყველა ხომ ვერ მიხვდა, რომ ყალბია? გარდა ამისა, ჩვენს ქვეყანაშია ცოტა უცნაური მიდგომა - თუ უცხოურმა გაზეთმა დაბეჭდა, სრული სიმართეა, თუ უცხოელმა პოლიტიკოსმა რამე თქვა, აუცილებლად ჭკვიანურია და ასე შემდეგ. ამ სტატიაში მითითებულია, რომ საქართველოს ხელისუფლება ჩართულია რუსულ თამაშში, ის ვერ აკონტროლებს პანდემიას. ფაქტობრივად, ბრიტანულმა გამოცემამ თქვა ის, რასაც ლაპარაკობს ოპოზიცია, რა სიცრუესაც

ავრცელებს ოპოზიცია. არადა, ეს ის ადამიანები არიან, რომლებსაც სურდათ არეულობა და მეტი მსხვერპლი თავიანთი პოლიტიკური მიზნებისთვის“.

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

რუსეთი არ ებრძვის მხოლოდ საქართველოს, ის ებრძვის თითქმის მთელ მსოფლიოს. როდესაც ნატო-ს ეგიდით გამართულ კონფერენციებს ვესწრებოდი წლების წინ, იქ იყო ხოლმე საუბარი ჩინეთიდან მომდინარე საფრთხეებზე. მაშინ მეცინებოდა, ჩინეთიდან რა საფრთხეები უნდა წამოვიდეს-მეთქი? თუმცა აღმოჩნდა, რომ ყველაფერი წინასწარ იყო შესწავლილი და გათვლილი. ჩვენ რუსეთის მხრიდან დღეს წავაწყდით პრობლემებს, თორემ ასეთი გეგმები არ მუშავდება სპონტანურად, ამას სჭირდება ათეული წლები. რუსეთის მთავარი მიზანი არის გავლენის აღდგენა პოსტსაბჭოთა სივრცეში და აღმოსავლეთ ევროპაში, მას სჭირდება სიძლიერის აღიარება დასავლეთისა და აშშ-ის მხრიდან.

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 წვრილმანი საკითხებია, ჩვენ უფრო დიდი საფრთხეების წინაშე ვდგავართ, უფრო დიდი გეგმები გვაქვს, ტერიტორიების 20 პროცენტი ოკუპირებულია. უფრო დიდი საფრთხის წინაშე დავდექით უკრაინაში (აღმოსავლეთ

ევროპაში) მიმდინარე მოვლენების შემდეგ. ვხედავთ, როგორ ამუშავდა საქართველოში ე.წ. მე-5 კოლონა, რომელიც ცდილობს, ქვეყანა ჩაითრიოს რუსეთთან ომში, რუსეთს გაუხსნას მეორე ფრონტი. ხელისუფლება სწორად მოიქცა, როცა ღიად განაცხადა, რომ საქართველო არ შეუერთდებოდა რუსეთის წინააღმდეგ დაგეგმილ სანქციებს. შეიძლება პრემიერ-მინისტრ ირაკლი ღარიბაშვილის განცხადება თავდაპირველად ხისტად გამოიყურებოდა, მაგრამ მას შემდეგ, როცა გერმანიამ, საფრანგეთმა და ევროპის სხვა ქვეყნებმა შერბილებული მიდგომა არჩიეს, აღმოჩნდა, რომ ის მართალი ყოფილა. სჯობს, თავიდანვე მწარე სიმართლე თქვა, ვიდრე ტკბილი ტყუილი - ამ შემთხვევაში არსებობს ორი მიმართულება, ჯერ ერთი, 2008 წლის აგვისტოს შემდეგ არც ევროპას, არც აშშ-ს რუსეთისთვის არანაირი სანქციები არ დაუწესებია და მეორეც - საქართველოს მხრიდან რუსეთის მიმართ დაწესებული სანქციები დააზარალებს მხოლოს საქართველოს. აქვე სათქმელია ისიც, რომ 2008 წლის აგვისტოში სახელმწიფო მინისტრმა თემურ იაკობაშვილმა ევროსაბჭოს მიმართა განცხადებით, სადაც შავით თეთრზე გარკვევით ეწერა, რომ არც ერთ ქვეყანას რუსეთისთვის, ანუ მოსახლეობისთვის სანქცია არ უნდა დაეწესებინა. რუსეთ-უკრაინის ომის ფონზე ე.წ. ოპოზიციამ (,,ნაციონალურმა მოძრაობამ››) რიტორიკა შეცვალა და მოღალატეობრივი ნაბიჯები გადადგა - მათ ერთმანეთის მიყოლებით გააკეთეს განცხადებები, რომ საქართველოს ხელისუფლებამ ითანამშრომლა რუსეთთან, ვლადიმერ პუტინთან და არ დაეხმარა უკრაინას. ეს გახლავთ მტკნარი სიცრუე, გარდა იმისა, რომ საქართველო შეუერთდა ყველა რეზოლუციას საერთაშორისო დონეზე, უკრაინაში გაიგზავნა ასეულობით ტონა ჰუმანიტარული ტვირთი.

დავუბრუნდეთ ნაშრომის ძირითად თემას: შესაძლებელია თუ არა კიბერომის შეჩერება და ლიკვიდაცია ტექნოლოგიური მიღწევებით? - როგორი მდგომარეობაა ამ მხრივ საქართველოში? გასაგებია, რომ გვეხმარებიან, არსებობს საერთაშორისო სტანდარტები, რეკომენდაციები, თანამშრომლობის მემორანდუმები,

მაგრამ ჩვენ თვითონ რა შეგვიძლია? დღეს ტექნოლოგიები ისეთი სისწრაფით ვითარდება, ოდნავი მოდუნება და მორჩა, შეიძლება კატასტროფის წინაშე აღმოჩნდე. ვინაიდან, ეს არის ომის ერთ-ერთი სახეობა და შეიარაღების თანმდევი ინსტრუმენტი, ამის შეჩერება შესაძლებელია მხოლოდ მოლაპარაკებით, სხვანაირად მშვიდობა არ იქნება. თუ არ დაისახა ერთობლივი გეგმა, წინააღმდეგობის 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.

დასკვნა

კიბერუსაფრთხოების უზრუნველყოფა შედარებით ახალი დარგია თანამედროვე სამყაროში. გლობალური თვალსაზრისით, მსოფლიოში არსებობს სამართლებრივი ბაზისა და საერთაშორისო სტანდარტების ნაკლებობის პრობლემა, რაც გლობალიზაციისა და თანამედროვე მსოფლიო წესრიგის გათვალისწინებით, ართულებს რეგიონული და ეროვნული კიბერუსაფრთხოების სტრატეგიის ჩამოყალიბების პროცესს. ამის მიუხედავად, კიბერუსაფრთხოების უზრუნველყოფის მექანიზმები დიდწილად დამოკიდებულია ცალკეული ქვეყნის გამოცდილებაზე, ყოველ შემთხვევაში, ამ საკითხთე კავკასიის რეგიონული უსაფრთხოების, პოსტსაბჭოთა სივრცისა და საქართველოს მაგალითები ასეთ სურათს გვიჩვენებს. რაც შეეხება ნატოსა და ევროკავშირში გაწევრიანებულ სახელმწიფოებს, ასევე ცალკეულ ქვეყნებს, რომელთაც გააჩნიათ და ხარჯავენ დიდ ფინანსებს ამ მიმართულებით, არაერთი ფაქტი ადასტურებს, რომ არც ეს ზონაა ბოლომდე დაცული. კიბერომი ნამდვილად არის პოლიტიკური კონფლიქტების ახალი რეალობა. ეს რომ ასეა, მსოფლიოში მიმდინარე პოლიტიკურმა მოვლენებმაც აჩვენა - უკვე არაერთი სახელმწიფოს საშინაო საქმეებში ჩაერივნენ დაინტერესებული სახელმწიფოები, მეტწილად საარჩევნო პროცესებში. რუსეთი კიბერსივრცეში გააქტიურებით ცდილობს, პოლიტიკური გავლენა მოიპოვოს როგორც აღმოსავლეთ ევროპის სახელმწიფოებზე, ისე პოსტსაბჭოთა ქვეყნებზე. ირანის ისლამური სახალიფოც კი, რომელიც არ არის მსოფლიოში მნიშვნელოვანი პოლიტიკური მოთამაშე, ცდილობს, ჩაერიოს ამერიკის შეერთებული შტატების საპრეზიტენტო არჩევნებში. ამის თაობაზე არაერთხელ განაცხადეს თეთრ სახლში.

შესაძლებელია, საერთაშორისო საზოგადოებაზე კიბერომმა იქო-

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

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

კიბერუსაფრთხოების უზრუნველყოფის საკითხებში საქართველოს სტრატეგიულ პარტნიორებს - ევროკავშირს, ნატოს, ამერიკის შეერთებულ შტატებს დიდი მნიშვნელობა ენიჭებათ. ვინაიდან, კიბერინციდენტები არის ტრანსნაციონალური ხასიათის, კიბერუსაფრთხოების დაცვა და უზრუნველყოფა შეუძლებელია მხოლოდ საკუთარი ძალებით. საფრთხეების აღკვეთა-შემცირების პროცესში აუცილებელია თანამშრომლობა საერთაშორისო დონეზე. კიბერინციდენტებზე ეფექტური რეაგირების მიზნით, შესაძლოა, მონაცემები ინახებოდეს სხვადასხვა სახელმწიფოების ტერიტორიაზე, რაც წარმოადგენს მოწყვლად ინფორმაციას. ინფორმაციის დროული მოპოვება შეუძლებელია ეფექტიანი საერთაშორისო თანამშრომლობის გარეშე. მიუხედავად იმისა, რომ საქართველოს კიბერუსაფრთხოების სფეროში აქვს პროგრესი, მაინც დიდი მნიშვნელობა ენიჭება ნატოსა და ევროკავშირის კიბერუსაფრთხოების სტრატეგიას, ასევე გამოცდილებას. 2014 წლის შეთანხმების თანახმად, კიბერთა-

ვდაცვა იქცა კოლექტიური თანამშრომლობის განუყოფელ ნაწილად, საქართველოს მხრიდან კი ამ სისტებაში ჩართვა მიზნად ისახავს ალიანსის ოპერაციების მხარდაჭერას.

გლობალურ უსაფრთხოებაში პოლიტიკური კონფლიქტების ახალი განზომილება ერთ-ერთი მნიშვნელოვანი და საკვანძო საკითხია. კიბერომი მნიშვნელოვან გავლენას ახდენს საერთაშორისო უსაფრთხოების პროცესების მიმდინარეობასა და შედეგებზე. ტექნოლოგიების განვითარებამ ისეთ მნიშვნელოვან სივრცეს, როგორიც არის ინტერნეტი, ხელი შეუწყო კიბერომებისა და კიბერშეტევების წარმოებას, რამაც საფრთხე შეუქმნა როგორც ეროვნულ, ასევე საერთაშორისო უსაფრთხოებას. ნაშრომში უამრავი მაგალითია, თუ რატომ და როგორ განსაზღვრავს კიბერტექნოლოგიები საერთაშორისო უსაფრთხოების პროცესების მიმდინარეობას, რა ზეგავლენას ახდენს ამ პროცესების შედეგებზე. საფუძველზე განვსაზღვრავთ, რომ რაც უფრო დიდი კიბერტექნოლოგიური შესაძლებლობები აქვს ამა თუ იმ ქვეყანას, მით უფრო მძლავრ მოთამაშეს წარმოადგენს საერთაშორისო პოლიტიკაში. კიბერომი შესაძლოა უფრო საშიში აღმოჩნდეს კაცობრიობისთვის, ვიდრე იყო მე-20 საუკუნის მეორე ნახევარში გაჩაღებული „ცივი ომი“ და დაპირისპირება ორ ბანაკს შორის. ვინაიდან, კიბერომი ყველა კონვენციური ომის თანმდევი პროცესია, უნდა დავასკვნათ, რომ მსოფლიო დგას დიდი საშიშროების წინაშე.

ბიბლიოგრაფია

1. ჯიაკუმოპულოს კ., ბუტარელი ჯ., ო'ფლერთი მ., "მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო", ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018.
2. Edited by Jens Ringsmose and Sten Rynning, NATO's New Strategic Concept: a Comprehensive Assessment, DIIS. Danish Institute for International Studies, Copenhagen, NATO, 2011, pp 23-43.
3. Information Security Doctrine of The Russian Federation, Moscow: Russian Federation, 2000, pp 1-32.
4. National Security Strategy, Washington: United States governments, 2017, pp 1-2.
5. Cheng D. Cyber dragon, inside China s information warfare and cyber operations, United States: Publishing House Praeger, 2017, pp 79-82.
6. Senese D. P., Vasquez A. J., The Steps to War: An Empirical Study, United States: Princeton University Press, 2018, pp 11-20.
7. Arquilla J., Ronfeldt D., Swarming and the Future of Conflic, Santa Monica: RAND National Defense Research Institute, 2000, pp 7-25.
8. Valeriano B., Maness C. R., Cyber War versus Cyber Realities, New York: Oxford University Press, 2015, pp 2-31.
9. Glaser B. Grounded Theory: The Philosophy, Method, and Work, Florida: BrownWalker Press, 2011, pp 175-187.
10. Popescu N., Secrieru S., Hacks, leaks and disruptions Russian cyber strategies, Paris: European Union Institute for Security Studies, 2018, Chaillot paper №148, pp 53-75.
11. Lindsay R. J. The Impact of China on Cybersecurity, United States: the President and Fellows of Harvard College and the Massachusetts

Institute of Technology, 2015, pp 1-3.
12. Bazyler J. M., Tuerkheimer M. F., Forgotten Trials of the Holocaust, United States: NYU Press, 2014, p 384.
13. ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., «კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა», თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016, გვ. 5-23.
14. Kenneth J. K. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions, Colorado: U.S. Air Force Academy, 2009, pp 26-27.
15. Russian National Security Strategy, Moscow: Russian Federation, 2015, No. 683, pp 1-4.
16. National Security Strategy of the United States of America, Washington: The White House, 2017, pp 1-2.
17. Cohen R., Mihalka M., Cooperative Security: New Horizons for International Order, London: European Center for Security Studies, The Marshall Center Papers, 2001 No. 3. pp 3-15.
18. "საქართველოს ეროვნული უსაფრთხოების კონცეფცია", თბილისი: საქართველოს მთავრობა, 2018, გვ. 3-30.
19. "ნატო-ს ვარშავის სამიტის დეკლარაციის მოკლე მიმოხილვა (გავლენა საქართველოზე)", თბილისი: საქართველოს უსაფრთხოების და განვითარების ცენტრი, 2014, გვ. 2-3.
20. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks, London: Publisher European Parliament, 2009, pp 8-9.
21. Mike O. Cyber Operations Building, Defending, and Attacking Modern Computer Networks, Marilend: Publishing House Apress, Department of Mathematics, Towson University, 2015, pp 237-265.
22. Schneier B. Psychology and Usability - Only amateurs attack machines; professionals target people, London: University of

Cambridge, Department of Computer Science and Technology The Computer Laboratory, 2017, Chapter 3, pp 1-2.
23. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, America: Bitcoin Organization, 2009, pp 1-9.
24. ჭყოიძე ნ., ტომარაძე გ., «ვირტუალური/კრიპტოგრაფიული ვალუტა და მისი თავისებურებები ვირტუალური ვალუტების რეგულირება (bitcoin-ის მაგალითზე)», თბილისი: გამოცემა "ეკონომიკა და საბანკო საქმე", 2014, გვ. 41-55.
25. ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., «კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა», თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016, გვ. 1.
26. ავალიშვილი ლ., ლომთაძე გ., ქევხიშვილი ს., "კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", თბილისი: IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2016, გვ. 5-25.

ინტერნეტ წყაროები:

1. Freiberger A. P., Swaine R. M., Analytical Engine, Encyclopedia Britanica, 2020, p 1. https://www.britannica.com
2. Loritz M. Who was Ada Lovelace? The life of the woman who envisioned the modern day computer, Media Website "EU-Startup", 2019, p 1. https://www.eu-startups.com
3. აბულაშვილი ი. "პირველი ელექტროგამომთვლელი მანქანის გამომგონებელი ქართველი", გაზეთი „რეზონანსი", 2017, http://www.resonancedaily.com
4. Levy S. The Brief History of the ENIAC Computer, Smithsonian Magazine, 2013, p 1. https://www.smithsonianmag.com

5. Burns D. The five generations of computers, Business to Business Company, 2016, p 1. https://btob.co.nz
6. Andrews E. The Invention of the Internet, Internet publisher History, 2019, p 1. https://www.history.com
7. Weber M. october 29, 1969: Happy 40TH Birthday to a Radical Idea!, Computer History Museum, 2009, p 1. https://computerhistory.org
8. Berners-Lee T. A short history of the Web - Where the Web was born, CERN Accelerating science, 2013, p 1. https://home.cern
9. Ambersariya D. Types of Internet Connections- Wireless, Dial-up, DSL, Fiber, Cable, ISDN, Technology Website Invention Sky, 2019, p 1. https://inventionsky.com
10. Coe T, Where does the word cyber come from?, Oxford University Press's Academic Insights for the Thinking World, 2015, p 1. https://blog.oup.com
11. Deffere S. 1st computer virus is written, January 30, 1982, Electronics Design Network, 2019, p 1. https://www.edn.com
12. Uhde A. A short history of computer viruses, Sentrian Pty Ltd, 2017, p 1. https://www.sentrian.com.au
13. Long T. "July 26, 1989: First Indictment Under Computer Fraud Act", Media News Company - Wired, 2011, p 1. https://www.wired.com
14. Rubens P. Common Types of Ransomware, Internet Website e Security Planet, 2017, p 1. https://www.esecurityplanet.com
15. Vidisha J. America's Hidden Stories' tackles CIA's alleged involvement in the Trans-Siberian Pipeline explosion of 1982, Media Entertainment Arts WorldWide, 2019, p 1. https://meaww.com
16. Thurrott P. Windows 98 rockets to 1998 sales of 25 million, News Media IT Pro Today, 1999, p 1. https://www.itprotoday.com
17. Sciarrone M. Cyber Warfare: The New Front, George W. Bush Institute, 2017, p 1. https://www.bushcenter.org
18. Perlroth N., Scott M., Frenkel S., Cyberattack Hits Ukraine Then Spreads Internationally, The New York Times, 2017, p 1. https://

www.nytimes.com
19. ბოჭოიძე ნ. საქართველოს ატლანტიკური ხელშეკრულების ახალგაზრდული ასოციაცია, «2021 წლის ნატოს სამიტის გენერალური მდივნის გახსნითი სიტყვა», ბრიუსელი, გვ. 1. 2021 წ. http://yata.ge/ge/?p=1883
20. ახალაია ლ., საქართველოს საზოგადოებრივი მაუწყებელი, «ბრიუსელის სამიტი და ნატოს კომუნიკე», ბრიუსელი, გვ. 1. 2021 წ. https://1tv.ge/video/briuselis-samiti-da-natos-komunike/
21. ქართული „ვიკიპედია“, „ანონიმუსი“ (ჰაკერული დაჯგუფება), 2004 წ. გვ. 1, https://ka.wikipedia.org/
22. “Support the Guardian” Available for everyone, funded by readers, “Kazakhstan protests: Moscow-led alliance sends ‘peacekeeping forces’ ”, 2022, p. 1, https://www.theguardian.com/
23. Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict, Information Technology Company ZDnet, 2018, p 1. https://www.zdnet.com
24. Gartzke E. Making Sense of Cyberwar, Harvard Kennedy School Belfer Center for Science and International Affairs, 2014, p 1. https://www.belfercenter.org
25. Lohrmann D. How Vulnerable Is Critical Infrastructure to a Cyberattack?, Governament Technology, 2020, p 1. https://www.govtech.com
26. Private & Security digital life - SICCURA, ,,Top Hackers to Watch Out For”, 2021. p. 1, https://siccura.com/top-hackers-to-watch-out-for/
27. Digiacomo J. Active vs Passive Cyber Attacks Explained, Intellectual Property Lawyer Revision Legal, 2017, p 1. https://revisionlegal.com
28. Zamora W. 10 easy ways to prevent malware infection, Software Company Malwarebytes, 2016, p 1. https://blog.malwarebytes.com
29. Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, Consulting Agency Gartner, 2018, p 1. https://www.gartner.com

30. Sobers R. 110 Must-Know Cybersecurity Statistics for 2020, Software Company Varonis, 2020, p 1. https://www.varonis.com
31. Morgan S. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", 2022. p. 1, https://cybersecurityventures.com/
32. Evansky B. US, UK and Estonia call out Russia over cyber attacks against Georgia in UN Security Council first, Fox News Channel, 2020, p 1. https://www.foxnews.com
33. Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict, Information Technology Company ZDnet, 2018, p 1. https://www.zdnet.com
34. Karasev P. NATO's Cyber Defense Evolution - NATO's New Digital Wall, Russian Council RIAC, 2016, p 1. https://russiancouncil.ru
35. Pennetier M. France to invest 1 billion euros to update cyber defences, Media News Reuters, 2014, p 1. https://www.reuters.com
36. Brussels Summit Declaration - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, NATO, 2018, p 1. https://www.nato.int
37. Kerr D. Obama asks for $14 billion to step up cybersecurity - The president urges Congress to pass legislation that would strengthen the country's hacking detection system and counterintelligence capabilities, Media News CNet, 2015, p 1. https://www.cnet.com
38. Department of Homeland Security Statement on the President's Fiscal Year 2021 Budget, Homeland Security, 2020, p 1. https://www.dhs.gov
39. Jones D., ,,Biden administration's FY 2023 budget includes 11% increase for cyber", Cybersecurity Dive, 2022. p. 1. https://www.cybersecuritydive.com/
40. Inter National Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, The White House, 2011, pp 3-24.

https://www.hsdl.org

41. ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია», ამერიკის შეერთებული შტატების საელჩო საქართველოში, 2017, გვ. 1. https://ge.usembassy.gov
42. "ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", ამერიკის შეერთებული შტატების საელჩო საქართველოში, 2017, გვ. 1. https://ge.usembassy.gov
43. Karpowicz W. Political Realism in International Relations, Stanford Encyclopedia of Philosophy, 2017, p 1, https://plato.stanford.edu
44. Jaffe E. How Highway Construction Helped Hitler Rise to Power, Bloomberg City Lab, 2014, p 1. https://www.bloomberg.com
45. Szal A. Report: Russian 'Internet Trolls' Behind Louisiana Chemical Explosion Hoax, Industrial Media - Manufacturing, 2015, p 1. https://www.manufacturing.net
46. Waddell K. 'Look, a Bird!' Trolling by Distraction, The Atlantic Magazine, 2017, p 1. https://www.theatlantic.com
47. Zengerle P., Megan Cassella M., Millions more Americans hit by government personnel data hack", Media Company Reuters, 2015, p 1. https://uk.reuters.com
48. Collective defence - Article 5, NATO, 2019, p 1. https://www.nato.int
49. Brent L. NATO's role in cyberspace, NATO, 2019, p 1. https://www.nato.int
50. Riazi T. Know The CCDCOE: Interview with Director Col. Jaak Tarien, NATO Assotiation of Canada - NAOC, 2020, p 1. http://natoassociation.ca
51. "კიბერუსაფრთხოების ინდექსში საქართველო მე-8 ადგილზეა". ტელეკომპანია "იმედი", 2017, გვ. 1. https://imedinews.ge
52. კიბერუსაფრთხოების ინდექსით, საქართველო მსოფლიოში მე-19 ადგილზეა». ტელეკომპანია «იმედი», 2018, გვ. 1. https://imedinews.ge

53. “National Cyber Security intex”, “61. Georgia 51.95”, 2022. pp. 1-2, https://ncsi.ega.ee/country/ge/?allData=1
54. კერსანსკასი ვ. «დეზინფორმაციასთან და ყალბ ამბებთან საბრძოლველად მარტივი და სწრაფი გზა არ არსებობს, ეს გრძელვადიანი სტრატეგიაა». საქართველოს საზოგადოებრივი მაუწყებელი, 2019, გვ. 1. https://1tv.ge
55. Newman H. L. GitHub Survived the Biggest DDoS Attack Ever Recorded, Media Company Wired, 2018, p 1. https://www.wired.com
56. Brook Ch., ,,What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More’’, DATAINSIDER - Digital Guardian’s Blog, 2020. p. 1, https://digitalguardian.com/
57. Leiden J. The 30-year-old prank that became the first computer virus, Information Technology Company The Register, 2012, p 1. https://www.theregister.com
58. Pitchkites M., “Top Cyber Security Statistics, Facts & Trends in 2022”, 2022. p. 1, https://www.cloudwards.net/cyber-security-statistics/
59. Cherry K. History and Key Concepts of Behavioral Psychology, publisher very well mind company, 2019, p 1. https://www.verywellmind.com/
60. Schmidt R. Cyber Quest, Action Impact LLC, 2017, p 1. https://www.actionimpact.com
61. Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, p 1. https://www.mitre.org
62. Caputo D. Applying Behavioral Science to the Challenges of Cybersecurity, MITRE solve problems for a safer world, 2012, p 1. https://www.mitre.org
63. Timberg C., Romm T., Hackers are seizing on coronavirus fears to steal data, researchers and U.S. regulators warn”, The washingtonpost, 2020, p 1. https://washingtonpost.com

64. Newman H. L. Coronavirus Sets the Stage for Hacking Mayhem, Media Company Wired, 2020, p 1. https://www.wired.com
65. Catalin C. Personal details for the entire country of Georgia published online, 2020, p 1. https://www.zdnet.com
66. "შსს-ს სახელით მოქალაქეებს მესიჯები მიუვიდათ - რა განცხადებას ავრცელებს სამინისტრო", საქართველოს შინაგან საქმეთა სამინისტრო 2020, გვ. 1. https://www.ambebi.ge
67. ზედელაშვილი თ. „ჰაკერები კორონავირუსთან დაკავშირებულ შიშებს იყენებენ პირადი მონაცემების მოსაპარად" - უნდა ველოდოთ მასშტაბურ კიბერშეტევებს», მედიაჰოლდინგი «ჯორჯიან ტაიმსი», 2020, გვ. 1. http://geotimes.com.ge
68. US Dept of Defense, Statement by the Department of Defense", U.S. Department of Defense (DoD), 2020, p 1. https://www.defense.gov
69. რუხაძე თ. «ირანის მხრიდან შესაძლოა, აშშ-ზე კიბერთავდასხმა განხორციელდეს», საქართველოს საზოგადოებრივი მაუწყებელი, 2020, გვ. 1. https://1tv.ge
70. Rouhani H. Never threaten the Iranian nation: Rouhani tells Trump, Alarabiya, 2020, p 1. https://english.alarabiya.net
71. Trump D. Trump says 'Iran appears to be standing down' following its retaliatory attacks against Iraqi bases housing US troops, CNN, 2020, p 1. https://edition.cnn.com
72. კუპრეიშვილი თ. «ყველაფერი, რაც ვიცით უკრაინული თვითმფრინავის კატასტროფაზე». საინფორმაციო სააგენტო «ნეტგაზეთი», 2020, გვ. 1. https://netgazeti.ge
73. ახალაია ლ. «ირანმა აშშ-ის სამხედრო ძალები „ტერორისტულ ორგანიზაციად" გამოაცხადა», საქართველოს საზოგადოებრივი მაუწყებელი, 2020, გვ. 1. https://1tv.ge,
74. ტრამპი დ. «ნატო-მ ახლო აღმოსავლეთიც უნდა მოიცვას და ახალ ალიანსს დავარქვათ „ნატო+ახლო აღმოსავლეთი" – რა მშვენიერი სახელწოდებაა, სახელებს კარგად ვიგონებ». საინფორმაციო «ინტერპრესნიუსი», 2020, გვ. 1. https://www.

interpressnews.ge

75. Hayes A. What Happens to Bitcoin After All 21 Million Are Mined?, Business & Economy Website Investopedia, 2020, p 1. https://www.investopedia.com
76. გოგუაძე მ. «მომავლის ვალუტა ბიტკოინი – კრიპტოვალუტა», სესხების შემდარეებელი კომპანია „ფინანსერი“, 2017, გვ. 1. https://financer.com
77. International Centre for Defence and Security - Eesti Estonia, “A Defence of Defence. NATO’s Response to Low-Grade Cyber-Attacks”, 2021, p. 1, https://icds.ee/en/a-defence-of-defence-natos-response-to-low-grade-cyber-attacks/
78. Watson T., “benefits of ISO 9001 and 27001 for companies and Their Clients”, 2019, p. 1, https://skywell.software/blog/benefits-of-iso-9001-and-27001/
79. Pedamkar P., “Cyber Security Standards”, 2020, p. 1, https://www.educba.com/cyber-security-standards/
80. “საქართველოში მცხოვრებ „დაეშის“ შესაძლო მხარდამჭერთა რაოდენობა და გავლენა შემცირდა”. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში, 2019, გვ. 1. https://imedinews.ge
81. მაისაია ვ. „ისლამური ხალიფატის“ საინფორმაციო-პროპაგანდისტული/კიბერ-ვირტუალური ომის სპეცეფიკა - „რბილი ძალის“ კონცეფტი», მედიაჰოლდინგი «ჯორჯიან-თაიმსი», 2017, გვ. 1. http://geotimes.com.ge
82. ქაზუმოვი ო. «ძალადობა რელიგიის სახელით და ინტერპრეტაციის მნიშვნელობა». ტოლერანტობისა და მრავალფეროვნების ინსტიტუტი (TDI), 2018, გვ. 1. https://www.tdi.ge
83. ზამან ჰ. «Youtub-ზე გავრცელებული ვიდეოს წარმომავლობა გაურკვეველია», საინფორმაციო «ფორ.ჯი», 2013, გვ. 1. https://for.ge
84. ზამან ჰ. «თალიბანი საქართველოს შურისძიებით ემუქრება?

- შოკისმომგვრელი ვიდეო YouTube-იდან». მედიაჰოლდინგი «პალიტრა», 2013, გვ. 1. https://www.palitravideo.ge
85. “ჩვენ ვიცით თქვენი სახელები, მისამართები, ნათესავები და მალე საქართველოში ჩამოვალთ! ჩვენ შურს ვიძიებთ!”. ტერორისტული ორგანიზაცია „ჯიჰადი“, 2013, გვ. 1. https://for.ge
86. ტერორიზმთან ბრძოლა». საქართველოს სახელმწიფო უსაფრთხოების სამსახური, 2015, გვ. 1. https://ssg.gov.ge
87. გეგიძე თ. «როგორ მოვიგერიეთ კიბერთავდასხმა და პროპაგანდა 2008 წელს», სააგენტო «ონ.ჯი», 2019, გვ. 1. https://on.ge/
88. გოცირიძე ა. «რუსეთ-საქართველოს 2008 წლის ომის კიბერგანზომილება», საქართველოს სტრატეგიისა და საერთაშორისო უსაფრთხოებების კვლევის ფონდი, 2019, გვ. 1. https://www.gfsis.org
89. ვაჩარაძე ა. «რუსეთის საინფორმაციო ომი - სტრატეგიები და მიზნები», სააგენტო «დამოუკიდებლობა», 2015, გვ. 1. http://www.damoukidebloba.ge
90. ბასილაია ე. «გერმანული მედია: რუსები 2008 წელს ბირთვული იარაღის გამოყენებას აპირებდნენ». გაზეთი «რეზონანსი», 2017, გვ. 1. http://www.resonancedaily.com
91. Person R. 6 reasons not to worry about Russia invading the Baltics, The Washington Post, 2015, p 1. https://www.washingtonpost.com
92. იაგორაშვილი ი. «რუსეთის 2 მითი ბალტიისპირეთის ქვეყნების შესახებ». ვებ-გვერდი «My the Detector», 2019, გვ. 1. https://www.mythdetector.ge
93. იაგორაშვილი ი. «მარია ზახაროვა სსრკ-ის მიერ ესტონეთის ოკუპაციას უარყოფს». ვებ-გვერდი «My the Detector», 2020, გვ. 1. https://www.mythdetector.ge

თორნიკე ზედელაშვილის (პოლიტიკის მეცნიერების დოქტორის) გამოქვეყნებული პუბლიკაციები

სტატიები:

1. „თანამედროვე საინფორმაციო ომის გეოპოლიტიკური კონტურები რუსეთ-აშშ-ის კონფრონტაციის ხაზი ბალტიის ზღვიდან შავ ზღვაში“, რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - ,,ANTE PORTAS Security Studies”, № 13. ნომერი 1. 2019 წ. (ინგლისურ ენაზე)
2. “კიბერომის ფენომენის ასახვა ეროვნული უსაფრთხოების სტრატეგიებში - მითი და რეალობა ამერიკის შეერთებული შტატების მაგალითზე”, რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - ,,American Studies Periodical“, შავი ზღვის საერთაშორისო უნივერსიტეტი, №12. 2019 წ. (ინგლისურ ენაზე)
3. ,,კიბერ ომი, როგორც ასიმეტრიული საფრთხის ფენომენი და კიბერბირთვული უსაფრთხოების საფრთხეები“, რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - ,,Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi“, ჩერნოვეცის ეროვნული უნივერსიტეტი, N 40. 2019 წ. (ინგლისურ ენაზე)
4. „კიბერომის კონცეფცია და 21-ე საუკუნის საერთაშორისო უსაფრთხოების სისტემა“, კავკასიის საერთაშორისო უნივერსიტეტი. რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - „პოლიტო/ლოგოს“. II გამოცემა. 2020 წ.
5. “კიბერ საფრთხეები და ასიმეტრიული სამხედრო გამოწვევები ბირთვული უსაფრთხოების კონტექსტში: უკრაინის და საერთაშორისო შემთხვევების ანალიზი”, უკრაინული რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - “Ukrainian Policymaker”, ტომი 7. 2020 წ. (ინგლისურ ენაზე)

6. “ნატოსა და ევროკავშირის კიბერუსაფრთხოების გარემო და სტანდარტები”, უკრაინული რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - “Ukrainian Policymaker”, ტომი 9. 2021 წ. (ინგლისურ ენაზე)
7. „საქართველოს კიბერუსაფრთხოება და საფრთხეები რუსეთის მხრიდან“, პოლონეთის ლოძის უნივერსიტეტის რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - „Eastern Review“, ტომი 9. 2020 წ. (ინგლისურ ენაზე)
8. „ევროკავშირის კიბერუსაფრთხოების სტრატეგია და ეკონომიკური საფრთხეები“, რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - ,,ANTE PORTAS Security Studies”, № 15. ნაწილი 1. 2020 წ. (ინგლისურ ენაზე)
9. ,,შავი ზღვის რეგიონის უსაფრთხოება, კიბერ ომი და ახალი ტექნოლოგიები», რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - ,,ANTE PORTAS Security Studies”, № 15. ნაწილი 2. 2020 წ. (ინგლისურ ენაზე)
10. ,,ევროკავშირის კიბერუსაფრთხოების სტრატეგია და ეკონომიკური საფრთხეები”, რეფერირებადი საერთაშორისო სამეცნიერო ჟურნალი - ,,ANTE PORTAS Security Studies”, № 16. ნაწილი 1. 2021 წ. (ინგლისურ ენაზე)

საერთაშორისო კონფერენციები:

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

კონფერენცია, კავკასიის საერთაშორისო უნივერსიტეტი. 2019 წ.

4. “21-ე საუკუნის გამოწვევა - კიბერუსაფრთხოება და საინფორმაციო ომი”, სტუდენტთა XI საერთაშორისო სამეცნიერო კონფერენცია. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2019 წ.
5. სამეცნიერო კონფერენცია - „ეროვნული და კორპორაციული უსაფრთხოება“, ეროვნული და კორპორაციული უსაფრთხოების სასწავლო კვლევითი ცენტრი. 2019 წ.
6. “კიბერ ომი - როგორც ომის ახალი სახეობა და ევროკავშირის უსაფრთხოების სტრატეგია”, სამეცნიერო კონფერენცია: „ევროკავშირის გაერთიანება - პრობლემები და პერსპექტივები“, საქართველოს საპატრიარქოს წმინდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტი. 2019 წ.
7. “კიბერომის ფენომენის ასახვა ეროვნული უსაფრთხოების სტრატეგიებში - მითი და რეალობა ამერიკის შეერთებული შტატების მაგალითზე”, საერთაშორისო სამეცნიერო კონფერენცია - ,,American Studies International Conference“, შავი ზღვის საერთაშორისო უნივერსიტეტი, №12. 2019 წ.
8. “სამხრეთ კავკასიის რეგიონში მიმდინარე პროცესები, 21-ე საუკუნის საინფორმაციო ომი და კიბერ შეტევები“, ახალგაზრდული კონფერენცია „შიდა და გარე ფაქტორების კავშირი სამხრეთ კავკასიის უსაფრთხოების კონტექსტში“, საქართველოს უნივერსიტეტი. 2019 წ.
9. “21-საუკუნის საერთაშორისო უსაფრთხოების სტრატეგიული თავდაცვითი მექანიზმები და კიბერშეტევების ტაქტიკა”, მერვე საერთაშორისო კონფერენცია, კავკასიის საერთაშორისო უნივერსიტეტი. 2020 წ.
10. “სამხრეთ კავკასიის რეგიონი და კიბერუსაფრთხოება“, კონფერენცია - კონფლიქტები სამხერთ კავკასიაში, საქართველოს საპატრიარქოს წმინდა ანდრია პირველწოდებულის სა-

ხელობის ქართული უნივერსიტეტი. 2020 წ.

11. „ბიოლოგიური ვირუსი, რომელმაც კიბერსამყარო უფრო მაღალ დონეზე აიყვანა“ - საქართველოს საპატრიარქოს წმინდა ანდრია პირველწოდებულის სახელობის ქართული უნივერსიტეტი. 2021 წ.

ორნიკე ზელაშვილი

2015 წელს დაამთავრა გორის სახელმწიფო უნივერსიტეტის სოციალურ მეცნიერებათა ბიზნესისა და სამართალ-მცოდნეობის ფაკულტეტი ჟურნალისტიკის სპეციალობით (დამატებითი სპეციალობა - ტურიზმი). მიენიჭა სოციალური მეცნიერებების ბაკალავრის აკადემიური ხარისხი. 2017 წელს კავკასიის საერთაშორისო უნივერსიტეტში დაასრულა სოციალურ მეცნიერებათა ფაკულტეტი, მიენიჭა საერთაშორისო ურთიერთობების მაგისტრის აკადემიური ხარისხი. 2021 წელს ამავე უნივერსიტეტში დაიცვა დისერტაცია კიბერუსაფრთხოების თემაზე და გახდა პოლიტიკის მეცნიერების დოქტორი.

2016 წლიდან არის ინტერნეტგამოცემა „ლიდერის“ დამფუძნებელი. 2021 წლიდან მუშაობს იუსტიციის სამინისტროში, ციფრული მმართველობის სააგენტოს ინფორმაციული უსაფრთხოების დეპარტამენტში.

9789941844522