ლევან ნიკოლეიშვილი
თორნიკე ზედელაშვილი

კიბერშესაძლებლობები და გლობალური უსაფრთხოების ახალი გამოწვევები

კიბერშესაძლებლობები და გლობალური უსაფრთხოების ახალი გამოწვევები

2023 თბილისი

რედაქტორი

თამარ კიკნაძე

პოლიტიკის მეცნიერების დოქტორი, პროფესორი, სტუ -ს პოლიტიკისა და საერთაშორისო ურთიერთობების დეპარტამენტის ხელმძღვანელი, კსუ-ს პოლიტიკის მეცნიერების სადოქტორო პროგრამის ხელძღვანელი.

რეცენზენტი

ზურაბ გარაყანიძე

დ. აღმაშენებლის სახ. ეროვნული თავდაცვის აკადემია,

ასოც. პროფესორი, ეკონომიკის დოქტორი, აკად. ჰ. გუგუშვილის

სახ. პრემიის ლაურეატი ეკონომიკურ მეცნიერებებში,

თადარიგის პოლკოვნიკი.

წიგნი საინტერესო იქნება კიბერტექნოლოგიებით და გლობალური პოლიტიკით დაინტერესებული, მომუშავე თუ სწავლის პროცესში მყოფი ადამიანებისათვის, პოლიტიკის მეცნიერებებისა და საერთაშორისო ურთიერთობების სტუდენტებისთვის.

ISBN 978-9941-8-5851-2

სარჩევი

ავტორებისგან

სამწუხაროდ, მე-20 საუკუნისა და 21-ე საუკუნეების გასაყარზე ტექნიკურმა პროგრესმა, ტექნოლოგიურმა რევოლუციამ უამრავ სიკეთესთან ერთად უამრავი პრობლემაც გააჩინა. ალბათ ეს მოსალოდნელიც იყო - სადაც არის სიკეთე, იქვეა ჩასაფრებული ბოროტებაც. ჩვენ შევეცადეთ, ამ წიგნით მოგცეთ ინფორმაცია, თუ როგორ გამოიყენოთ ტექნიკური სიკეთე და როგორ დააღწიოთ თავი ტექნიკურ ბოროტებას, რათა არ გახდეთ კიბერტერორისტების მსხვერპლი.

ძალზედ სამწუხაროა ის ფაქტიც, რომ კიბერ-ტერორიზმი არ დარჩა მხოლოდ კერძო პირების იარაღად და ამ სფეროში ჩართული აღმოჩნდა არაერთი დიდი სახელმწიფო, უპირველესად კი რუსეთი. ყოველდღიურად იქმნება სპეციალური სამსახურები, სამხედრო დანაყოფები, იატაკქვეშა ორგანიზაციები, რათა ერთ თარგზე გამოჭრილმა სახელმწიფოებმა დააზიანონ სხვა სახელმწიფოები და ამყოფონ მუდმივი სტრესის რეჟიმში, გაუხსნან რეალური საბრძოლო ფრონტი და ამასთანავე ეომონ ირეალურ სამყაროში. სხვათა შორის, ირეალური სამყარო ნელ-ნელა უკვე ისე შეერწყა რეალურს, ვეღარ გაიგებთ, სად იწყება ერთი და სად მთავრდება მეორე. ეს დაადასტურა უკრაინაში რუსეთის შეჭრამაც - მოგეხსენებათ, სამხედრო ტექნიკა უმეტესად იმართება კომპიუტერული სისტემებით და ხშირად ისე იბომბება ქალაქები, ცოცხალი ძალა თუ ავიაცია აღარც კი არის საჭირო.

მოგეხსენებათ, მეცნიერულ-ტექნიკური პროგრესი უწყვეტი მოვლენაა, შესაძლოა, დღევანდელი ნახტომი ხვალ უკვე მოძველებული და ყავლგასული აღმოჩნდეს. ამიტომ, ჩვენ ვალდებული ვართ, კვლევების საფუძველზე კვალში ჩავუდგეთ სამეცნიერო მიღწევებს და კვლავაც გამოვიტანოთ სამზეოზე, სად არის სიკეთე და სად არის ბოროტება. მოდით, ჩავთვალოთ, რომ ეს წიგნი მხოლოდ დასაწყისია.

ლევან ნიკოლეიშვილი

ციფრული ეპოქა - შეიძლება ასე ვუწოდოთ დღევანდელი მსოფლიოს მდგომარეობას. ციფრულმა ეპოქამ უამრავ საინტერესო გამოწვევასთან ერთად მოიტანა უამრავი სახიფათო გამოწვევაც. სწორედ აქედან გაჩნდა განმარტება ,,კიბერუსაფრთხოება''. ამ წიგნში წარმოგიდგენთ, როგორ ვმართოთ საკუთარი კომპიუტერული სისტემა, სამსახურებრივი მოწყობილობები, სახელმწიფო დანიშნულების არეალი და როგორ დავიცვათ თავი მავნებლური თავდასხმებისგან.

რა არის კიბერშეტევა? რას ნიშნავს ფიშინგი? რა ტიპის საფრთხეები არსებობს ინტერნეტსივრცეში? რაზე გავამახვილოთ ყურადღება უპირველესად? როგორ ამოვიცნოთ საეჭვო ვებ-გვერდები და როგორ ავარიდოთ თავი პრობლემებს? როგორ დავაღწიოთ თავი მავნე პროგრამებს? რა ტიპის მავნე პროგრამები არსებობს და რის მიღწევას ცდილობენ კიბერტერორისტები, ანუ სხვადასხვა სახის ჰაკერები? როგორ ხვდებიან მავნე პროგრამების საშუალებით ჰაკერები ჩვენს კომპიუტერულ და მობილურ სისტემებში? ჩვენ მოგითხრობთ ამ ყველაფერზე და მოგცემთ რეკომენდაციებს, როგორ განერიდოთ ციფრული ეპოქის თანმდევ პრობლემებს. ეს რომ აზრობრივად ჩამოგვეყალიბებინა და წიგნად გვექცია, დიდი შრომა დაგვჭირდა, მაგრამ საზოგადოების გათვითცნობიერების მცდელობა ნამდვილად ღირს ამად.

<u>თორნიკე ზედელაშვილი</u>

რედაქტორისგან

ციფრული ტექნოლოგიების განვითარებამ ადამიანის ცხოვრების ყველა სფერო მოიცვა და მთლიანად შეცვალა ჩვენი ყოფა. დღეს თანამედროვე ტექნოლოგიების ათვისების გარეშე ადამიანს წარმატების იმედი არ უნდა ჰქონდეს.

ამასთან, ტექნოლოგიურმა რევოლუციამ, რომელმაც კაცობრიობას უდიდესი სარგებელი მოუტანა, გაზარდა კიბერრისკები ვირტუალურ სივრცეში.

კიბერუსაფრთხოება გლობალური გამოწვევაა, რომელიც სცილდება სახელმწიფოს საზღვრებს და გლობალურ კოლექტიურ საერთაშორისო თანამშრომლობას მოითხოვს. დღეისათვის სახელმწიფოს გეოგრაფიული საზღვრები არ წარმაოდგენს ბარიერს კიბერშეტევებისთვის - მავნე კიბერაქტივობები შესაძლებელია განხორციელდეს ფარულად მსოფლიოს ნებისმიერი წერტილიდან ადამიანის ან ადამიანთა ჯგუფების მიერ სახლიდან კომპიუტერის მეშვეობით და არ საჭიროებს განსაკუთრებულ ძვირადღირებულ რესურსებს. მას შეუძლია გამოიწვიოს ისეთვე დამანგრეველი ეფექტი, როგორც კონვენციურმა საომარმა მოქმედებამ.

მსოფლიოში გახმაურებული კომპლექსური კიბერშეტევები ნათელი დასტურია იმისა, თუ რამდენად მნიშვნელოვანია კიბერუსაფრთხოების უზრუნველყოფა ქვეყნებისთვის, განსაკუთრებით კი პატარა (მცირე) ქვეყნებისათვის, რომლებიც მოწყვლადები არიან თანამედროვე კიბერგამოწვევების მიმართ. ეს საფრთხე კიდევ უფრო კომპლექსური და უმართავი გახდება ციფრული ტექნოლოგიების და ხელოვნური ინტელექტის ფაზაში.

წიგნი მკითხველს გაათვითცნობიერებს, სწორ გზაზე დააყენებს და ცოდნას მისცემს, ასწავლის თავდაცვას, კომპიუტერულ ჰიგიენას, ქცევის წესებს, რათა არ გახდეს მსხვერპლი კიბერტერორისტების ხელში. და, რაც მთავარია, ის აგისხნით, თუ რა ხდება კიბერსფეროში მსოფლიო მასშტაბით, რამ გამოიწვია ომი უკრაინაში, რატომ არის ასეთი დაუნდობელი აგრესია რუსეთის მხრიდან, როგორი დამოკიდებულება აქვთ ნატოს წევრ ქვეყნებს ყოველივესთან, რა გეგმები და პროექტები არსებობს ევროკავშირსა თუ ამერიკის შეერთებულ შტატებში, რა სიძლიერის თავდაცვისუნარიანობა გააჩნიათ მსოფლიოს წამყვან ქვეყნებს და როგორია მათი ურთიერთთანამშრომლობა. ასევე, შეიტყობთ, როგორ შევჩეროთ

რუსული აგრესია კიბერსივრცეში და როგორ გავანეიტრალოთ კიბერტერორისტული სახელმწიფოები, რათა ინტერნეტსივრცე არ მოიცვას ქაოსმა.

წინამდებარე წიგნი სახელმძღვანელოდ გამოადგებათ როგორც სტუდენტებს, ასევე სკოლის მოსწავლეებსა და საზოგადოების სხვა წარმომადგენლებს.

მადლობა ავტორებს გაწეული შრომისთვის.

თამარ კიკნაძე

პოლიტიკის მეცნიერების დოქტორი, პროფესორი, სტუ-ს პოლიტიკისა და საერთაშორისო ურთიერთობების დეპარტამენტის ხელმძღვანელი, კსუ-ს პოლიტიკის მეცნიერების სადოქტორო პროგრამის ხელმძღვანელი.

შესავალი

დღეს მთელი მსოფლიო დგას მნიშვნელოვანი საფრთხეების წინაშე - არჩევანის საშუალება, რომელიც საზოგადოებას გააჩნია, მრავალწახნაგოვანია, ეს ყველაფერი კი ტექნოლოგიების განვითარებამ მოიტანა. ადამიანები მოიხმარენ ელექტროენერგიას, გაზს, წყალს, საკვებს, საფასურს იხდიან ახალი ტექნოლოგიების საშუალებით - ვაჭრობენ კიბერსივრცეში, ცვლიან ინფორმაციას, ანვითარებენ ბიზნესს, ნერგავენ სოციალურ და ეკონომიკურ იდეებს. სოციალური კიბერსივრცის მიმართულებით ბევრად გამარტივდა გადარიცხვები, ურთიერთობები, იზოგება დრო, ენერგია, თანხები. თუმცა ეს უდიდესი სიამოვნება დიდ საფრთხეებსაც უკავშირდება. ამ კუთხით საჭირო და აუცილებელია პერსონალური მონაცემების დაცვა, ფინანსების მართვა, ჰაკერული თავდასხმებისგან თავის დაღწევა და ასე შემდეგ. მსოფლიო მასშტაბით კიბერსივრციდან მიღებული ზარალი კოლოსალურ თანხებს აღწევს - არსებობენ ინდივიდუალრ დონეზე ,,მოღვაწე'' კრიმინალები, რომლებიც ახალ ტექნოლოგიებს მავნებლური მიზნებისთვის იყენებენ. ასევე, არსებობენ აგრესორი სახელმწიფოები, რომლებიც ძველი, კონვენციური ომის წარმოებასთან ერთად, ითვისებენ ახალ ტექნოლოგიებს და იყენებენ სხვა ქვეყნების დასაზიანებლად. ასეთი ,,მოუხელთებელი'' სახელმწიფო გახლავთ რუსეთის ფედერაცია, რომელსაც საქართველოს ტერიტორიები აქვს ოკუპირებული, ომი აქვს გაჩაღებული უკრაინაში და პერიოდულად ახორციელებს კიბერთავდასხმებს როგორც საქართველოს კრიტიკულ ინფრასტრუქტურაზე, ასევე აწარმოებს კიბერომს უკრაინაში და გავლენის გაძლიერებას ცდილობს სხვა მეზობელ სახელმწიფოებზეც.

მსოფლიო სამწუხარო რეალობის წინაშე აღმოჩნდა, როდესაც 2022 წლის 24 თებერვალს, რუსეთის არმია უკრაინის ტერიტორიაზე შეიჭრა, ამან საფუძველი გააჩინა 21-ე საუკუნეში, ომის სახით მსოფლიოს დიდი ზარალი მიეღო როგორც რეალურ, ასევე ვირტუალურ სამყაროში, ინფრასტრუქტურის დაზიანების, განადგურებისა და მათ შორის ადამიანების სიცოცხლის მოსპობით. მანამდე ბევრი მსჯელობა მიდიოდა, დაიწყებოდა თუ არა ომი, ბევრს სჯეროდა, რომ რუსეთი, კერძოდ პრეზიდენტი ***ვლადიმერ პუტინი*** ამას არ ან ვერ გაბედავდა. თუმცა იმ დროისთვის მნიშვნელოვანი ინფორმაცია იყო ამერიკის შეერთებული შტატების დაზვერვიდან და პრეზიდენტმა ***ჯო ბაიდენმა*** თავის გამოსვლებში არაერთხელ ომის დაწყების თარიღიც კი დაასახელა. ამ მხრივ საინტერესო გახლდათ უკრაინის პრეზიდენტის, ***ვოლოდიმირ ზელენსკის*** განცხადებები - თითქოს საპანიკო არაფერი იყო. მეტიც, ის თავის უკრაინულ დაზვერვას უცხადებდა სრულ ნდობას. თუმცა არც იმის დავიწყება შეიძლება - ომის დაწყებიდან რამდენიმე დღეში უკრაინელმა პოლიტიკოსმა, მთავრობის ადმინისტრაციის აწ უკვე ყოფილმა მრჩეველმა ***ოლექს არესტოვიჩმა*** ფაქტობრივად აღიარა, რომ მათ *(უკრაინის ოფიციალურმა პირებმა)* იცოდნენ ომის დაწყების შესახებ და ამას არ ასაჯაროებდნენ, რათა მოსახლეობაში არ გამოეწვიათ შიში, არეულობა და პანიკა - შესაძლოა, საცობებს დიდი პრობლემები შეექმნაო. რა თქმა უნდა, ცალკე საკლვევ საგანს წარმოადგენს, რამდენად გამართლებული იყო აღნიშნული ქმედება, რომელსაც შეიძლება ვუწოდოთ პოლიტიკური და სამხედრო მანევრი. ამ ქმედებას, როგორც ცნობილია, უამრავი ადამიანის დაღუპვა და ინფრასტრუქტურის განადგურება მოჰყვა. იქიდან გამომდინარე, რომ ჩვენი წიგნის მთავარ საკითხს წარმოადგენს ციფრული ეპოქა, კიბერუსაფრთხოება, კიბეშეტევები და კიბერომები, ჰიბრიდული ომი, აუცილებლობად მივიჩნევთ ობიექტურად, პოლიტიკურ, სისტემურ და ციფრულ დონეზე გავაანალიზოთ რეალური მდგომარეობა.

საბედნიეროდ, არსებობენ სახელმწიფოები (აშშ, ინგლისი, საფრანგეთი), რომლებიც ცდილობენ თავდაცვითი და კიბერუსაფრთხოების მექანიზმების შემუშავება-განახლებას, ახალი სტანდარტების დანერგვასა და განვითარებას. ამ საქმეში ისინი მილიარდებს ხარჯავენ.

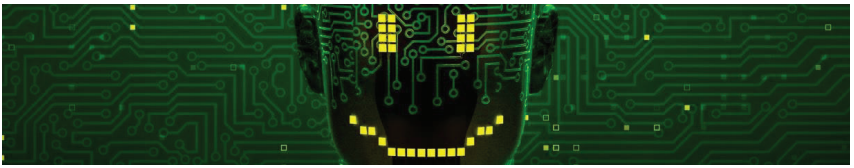
ამ მიმართულებით აქტიურად მუშაობენ ჩრდილოატლანტიკური ალიანსი და ევროკავშირი. ასევე, წამყვანი საერთაშორისო ორგანიზაციები: ***საერთაშორისო სტანდარტების ორგანიზაცია (ISO)*** და ***ევროპის სტანდარტების ორგანიზაცია (EN),*** რომლებიც გარდა სხვა მიმართულებებისა, კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების მიმართულებით აწესებენ გარკვეულ სტანდარტებს, რეგულაციებს.

ტექნოლოგიების რევოლუციურმა განვითარებამ სახელმწიფოებს მისცა საშუალება, თითქმის ყველა სფეროში დანერგონ სასარგებლო მექანიზმები, კიბერსივრცე გახდა რეალური და ვირტუალური სამყაროს სინთეზი. მეტიც, დღეს უკვე აქტიურად მიმდინარეობს და მალე დასრულდება ყველა პროფესიის ციფრული გარდასახვა. არსებობს წინსვლა და სარგებელი? არსებობს განვითარება? რა თქმა უნდა, აქვე არსებობს საფრთხე და უამრავი სახის რისკი. ამ საფრთხეებსა და რისკებზე, თითოეულ ნიუანსზე ადეკვატური პასუხია გასაცემი. უნდა გვესმოდეს, რომ კიბერსივრცეს გააჩნია უამრავი ისეთი ქვესივრცე, რაც საზოგადოებისთვის არანაკლებ საშიშროებას წარმოადგენს. ერთ-ერთი ასეთი გახლავთ ***დარკნეტი.***[1]

დღეს მსოფლიო მასშტაბით ინტერნეტსივრცეში ყველაზე საფრთხისშემცველი მოვლენა კიბერომის წარმოებაა. ამ მოვლენის ზოგადი

[1] *Darknet (Dark Web) - ბნელი ქსელი. ასევე ცნობილია, როგორც დაფარული ქსელი. დარკნეტში მოხვედრა მარტივი არ არის. არსებობს სხვადასხვა პროგრამული საშუალებები, რის შედეგადაც ჩვეულებრივ რიგით ადამიანსაც შეუძლია ისარგებლოს. აქ მხოლოდ ბიტკოინით (ელექტრონული ვალუტა) ხდება გადახდა. შეგვიძლია, შევიძინოთ იარაღი, მოპარული კარტები, სხვადასხვა ქვეყნის მოქალაქეობა, ნარკოტიკი და ა.შ.*

განმარტება ასეთია: „ერთი ქვეყნის მიერ მეორე ქვეყანაზე ციფრული შეტევების გამოყენება (კომპიუტერული ვირუსები ან ჰაკერული კიბერშეტევები) კომპიუტერული ინფრასტრუქტურის დაზიანების, ლიკვიდაციისა და განადგურების მიზნით“.[2]



როგორ აწარმოებენ კიბერშეტევებსა და კიბეროომებს სახელმწიფოები? ამისთვის არსებობენ სპეციალური ჰაკერული ორგანიზაციები. ადამიანებს, რომლებიც მავნებლური საქმიანობით არიან ინტერნეტსივრცეში დაკავებული, ***შავქუდიანი ჰაკერები,***[3] ეწოდებათ. არსებობენ ***სახელმწიფოების მიერ დაფინანსებული ჰაკერები***[4] და ***ჰაკტივისტები,***[5] მათ მიერ განხორციელებული კიბერშეტევები, კიბერთაღლითობები (ფიშინგი), კიბეროომები დიდი ფინანსური ზარალის წინაშე აყენებს თანამედროვე სამყაროს. აღნიშნული საკითხი იმდენად მასშტაბურია, რომ აუცილებლად საჭიროებს სტრუქტურულ და სისტემურ დაგეგმარებას. კიბერუსაფრთხოებისა და კიბერთავდაცვის საკითხებთან ერთად, აქტუალურ საგანს წარმოადგენს ინფორმაციული უსაფრთხოების საკითხი. ინფორმაციული უსაფრთხოება მნიშვნელოვანია სახელმწიფო სტრუქტურებსა თუ კერძო სექტორში მომუშავე ადამიანებისათვის. რასაკვირველია, ამ მიმართულებითაც არსებობს საერთაშორისო გამოცდილება, სტანდარტები და აუცილებელია სერთიფიცირება. კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების მიმართულებით დიდი როლი ენიჭება სტანდარტების დაცვას, რის

---

[2] კიბეროშის წარმოებად ხშირად მიიჩნევენ, როდესაც კიბერტექნოლოგიების საშუალებით ხდება დივერსია, ელექტრონული ჯაშუშობა, ან კრიტიკულ ინფრასტრუქტურაზე თავდასხმა. არსებობს კრიტერიუმები, რითაც კიბეროშის რაობას განსაზღვრავენ - მაგალითად, რა მასშტაბის კიბერშეტევა განხორციელდა, ვინ იყო ობიექტი და რა ზარალის მომტანი აღმოჩნდა აღნიშნული თავდასხმა.

[3] შავქუდიანი ჰაკერები (ცუდი ბიჭები) Black Hat Hackers (the bad guys) - ისინი გამოცდილი ჰაკერები არიან, სისტემაში ავტორიზაციის გარეშე იჭრებიან. იყენებენ სისტემის უსაფრთხოებას შავნე განზრახვით ან ფინანსური სარგებლისთვის. შავქუდიანი ჰაკერები მუშაობენ ორგანიზაციულ-დანაშაულებრივ ჯგუფებთან.

[4] ქვეყნების მიერ დაფინანსებული ჰაკერები (State/Nation Sponsored Hackers), რომლებიც დაქირავებულნი არიან მთავრობების მიერ სხვა ქვეყნების კომპიუტერულ სისტემებზე წვდომის მისაღწევად

[5] ჰაკტივისტები (Hacktivists), რომლებიც კიბერშეტევებს ანხორციელებენ პოლიტიკური მიზნით, თავს ესხმიან და არღვევენ სამთავრობო ქსელებს, სისტემებს, რათა ყურადღება მიიპყრონ პოლიტიკური ან სოციალური მიმართულებით.

შედეგადაც შეიძლება ისეთი საფრთხეები იქნას მინიმუმამდე დაყვანილი, რაც უთუოდ იქნებოდა დაკავშირებული არნახულ ზარალთან.

ხშირად კიბერუსაფრთხოება და ინფორმაციული უსაფრთხოება ერთმანეთთან არის გაიგივებული. თუმცა ინფორმაციული უსაფრთხოება უფრო მასშტაბურ საკითხს წარმოადგენს, ვიდრე კიბერუსაფრთხოება, რადგან ინფორმაციული უსაფრთხოების ერთ-ერთი შემადგენელი ნაწილია კიბერსივრცეში ინფორმაციის დამუშავება, შენახვა და დაცვა. კიბერუსაფრთხოების სტანდარტები ფაქტობრივად მუშაობს როგორც პოლიტიკის ერთობლიობა, რომელიც განსაზღვრავს მეთოდებს ან მიდგომებს, სისტემების დაცვას სახელმწიფო უწყებებსა თუ კერძო ორგანიზაციებში.

კიბერსაფრთხეების იგნორირება, ან არაადეკვატურად შეფასება ნებისმიერ ქვეყანას დააყენებს ისეთი რისკების წინაშე, როგორებიცაა - სახელმწიფო და ეკონომიკური სტრუქტურების მოწყვლადობა, კრიტიკული ინფრასტრუქტურის არასაკმარისი დაცულობა, სამხედრო და ჰიბრიდული საფრთხეებისადმი სისუსტე, თავდაცვისუნარიანობის დაქვეითება და ასე შემდეგ. ამ სფეროში გაჩერება და თავის დამშვიდება უკვე დანაშაულის ტოლია, აქ მუდმივი სიფხიზლეა საჭირო.

Introduction

Presently, the global community confronts formidable challenges, wherein the array of options available to society is manifold, and all of these challenges stem from the advancement of technology. Individuals now engage with novel technologies to fulfill their consumption needs, encompassing electricity, gas, water, and sustenance. Likewise, financial transactions, such as bill payments, are increasingly executed through digital platforms. Additionally, cyberspace facilitates virtual trade, information exchange, entrepreneurial pursuits, and the dissemination of social and economic concepts.

The advent of social cyberspace has significantly streamlined transfers and interpersonal connections, resulting in time, energy, and financial savings. Nevertheless, this newfound convenience is not without its perils. Accordingly, safeguarding personal data, managing financial resources, and averting hacking attacks have become imperative and indispensable. The global landscape is marred by staggering losses incurred within the cyberspace domain, with the existence of highly skilled "master" criminals who exploit emerging technologies for malicious ends at an individual level.

Moreover, in addition to conventional methods of warfare, certain nations assume an aggressive stance by leveraging emerging technologies to inflict harm upon other countries. A prominent example of such an "impervious" state is the Russian Federation, which has not only occupied Georgian territories but also initiated hostilities in Ukraine. Furthermore, the Russian Federation periodically launches cyber-attacks against critical infrastructure in Georgia, engages in cyber warfare within Ukraine, and endeavors to fortify its influence over neighboring states.

The global community was confronted with a somber reality on February 24, 2022, as the Russian military initiated an invasion of Ukrainian territory. This marked the onset of a conflict that would shape the trajectory of the 21st century, inflicting significant losses upon the world across both physical and virtual realms. The consequences manifested in the form of extensive damage to infrastructure, widespread destruction, and loss of human lives.

Preceding the aforementioned events, extensive deliberations ensued regarding the possibility of an impending war, with considerable speculation surrounding whether Russia, particularly President Vladimir Putin, would indeed initiate such actions or possess the

audacity to do so. However, during this period, crucial intelligence from the United States of America emerged, and President Joe Biden repeatedly referred to the commencement date of the war in his public addresses. Notably, the statements made by Ukrainian President Volodymyr Zelensky were intriguing, as he conveyed a sense of composure and downplayed the need for alarm, exhibiting unwavering confidence in the capabilities of Ukrainian intelligence.

Nevertheless, it is crucial to acknowledge that shortly after the onset of the war, Olex Arestovich, a former advisor to the Ukrainian government administration, openly admitted that the Ukrainian officials were indeed aware of the war's commencement but deliberately withheld this information to prevent instilling fear, disorder, and panic among the population. One of the concerns cited was the potential for significant traffic congestion. The justification and implications of this political and military maneuver warrant separate analysis. Regrettably, this course of action resulted in the loss of numerous lives and extensive infrastructure damage. Given that our book focuses on the digital age, cyber security, cyber-attacks, cyber warfare, and hybrid warfare, it is imperative to objectively examine the real situation from political, systemic, and digital perspectives.

Fortunately, certain nations, namely the United States, United Kingdom, and France, actively strive to enhance and modernize their defense and cyber security mechanisms while spearheading the adoption and development of new standards in this realm. These countries allocate substantial financial resources, amounting to billions, towards these endeavors.

The North Atlantic Alliance, along with the European Union, remains actively engaged in concerted efforts to address these challenges. Furthermore, prominent international organizations such as the International Standards Organization (ISO) and the European Standards Organization (EN) play crucial roles in establishing specific standards and regulations pertaining to cyber security and information security, among other domains. These organizations serve as vital catalysts in shaping global frameworks and guidelines in the pursuit of enhanced cyber security measures.

The rapid advancement of technology has paved the way for the implementation of valuable mechanisms across various domains, effectively blending the boundaries between the real and virtual realms. Furthermore, the ongoing digital transformation of all professions

is already well underway and nearing completion. While these developments bring about advancements and benefits, it is crucial to acknowledge the existence of inherent dangers and multiple types of risks. Consequently, it becomes imperative to provide appropriate responses to address the nuances associated with these threats and risks. It is important to recognize that within the vast expanse of cyberspace, there exist numerous subspaces that pose significant dangers to society. One such example is the „Dark net“, which necessitates special attention and countermeasures.

Presently, the production of cyber warfare stands out as the most perilous phenomenon within the global internet domain. Broadly defined, cyber warfare encompasses the deployment of digital attacks, such as computer viruses or hacking cyber-attacks, by one nation against another with the intention to inflict damage, disable, or destroy computer infrastructure. This form of aggression poses significant threats to the stability and security of nations in the interconnected digital landscape.

States employ various means to carry out cyber-attacks and cyber warfare. They often rely on specialized hacking organizations that possess the technical expertise and resources to conduct such operations. Individuals involved in malicious activities within the online realm are commonly referred to as black hat hackers. These actors may include state-sponsored hackers and hacktivists, both of whom engage in cyber-attacks, cyber frauds (such as phishing), and cyber warfare. The repercussions of these activities are substantial, resulting in significant financial losses for the modern world.

The magnitude of the aforementioned issue necessitates comprehensive and systematic planning. In addition to addressing cyber security and cyber defense concerns, the matter of information security assumes significant importance for individuals working in government institutions and the private sector. International experience, standards, and certification play crucial roles in this domain as well. Adherence to established standards holds great significance in the realms of cyber security and information security, as it serves to minimize potential threats that could otherwise result in unprecedented losses. Implementing and following these standards is essential for mitigating risks and safeguarding sensitive information in an

Indeed, while cyber security and information security are related, it is important to recognize that information security encompasses a broader scope than cyber security alone. Information security addresses the comprehensive protection, processing, storage, and management of information, including but not limited to its digital existence within cyberspace. Cyber security, on the other hand, focuses specifically on securing digital systems and networks from cyber threats. Within the framework of information security, cyber security standards play a critical role. These standards serve as a collection of policies, guidelines, and practices that establish methods and approaches for safeguarding systems and data in both government agencies and private organizations.

Neglecting or underestimating the importance of cyber security exposes any nation to significant risks, including vulnerabilities in state and economic structures, inadequate protection of critical infrastructure, susceptibility to military and hybrid threats, compromised defense capabilities, and more. Ceasing efforts or becoming complacent in this field can be equated to a grave oversight, as the consequences can be severe.

მსოფლიო კიბერშესაძლებლობები, საერთაშორისო პოლიტიკური აქტორები და გამოწვევები 21 საუკუნეში

იქიდან გამომდინარე, რომ ჯერ კიდევ აქტიურ თემად რჩება რუსეთ-უკრაინის ომი, მიზანშეწონილად მივიჩნევთ, სიღრმისეულად გავაანალიზოთ აღნიშნული საკითხი, მითუმეტეს, ჩვენი სახელმძღვანელოს მთავარი თემაც ზუსტად ომების რაობას, ზიანის თავიდან აცილების სხვადასხვა სტანდარტებსა და მეთოდებს ეხება, როგორც რეალურ, ასევე ვირტუალურ სამყაროში, რომელიც არაერთხელ აღვნიშნეთ. პირველ რიგში, დავიწყოთ რეალური ომის განხილვით, მასში ჩართული სხვადასხვა აქტორებით და შემდეგ უკვე გავაანალიზოთ, როგორც კიბერსივრცეში წარმოებული კიბერპოლიტიკური აგრესია, ასევე სხვადასხვა ქვეყნების, საერთაშორისო ორგანიზაციების კიბერშესაძლებლობები, სტრატეგიები, სტანდარტდები და ის ძირითადი მიდგომები, რეკომენდაციები, რაც მსოფლიო მასშტაბით არის მიღებული.

ნატო, ევროკავშირი, ამერიკის შეერთებული შტატები, რუსეთის ფედერაცია, ჩინეთი, სამხრეთ კავკასია, უკრაინა, პოლონეთი, ბალტიისპირეთის ქვეყნები, თურქეთი, ისრაელი, ძირითადად ამ ქვეყნების გარშემო იქნება ჩვენი მსჯელობა და ანალიზი, რომლებიც როგორც კიბერსივრცეში არიან აქტიურები, ასევე რეალურ გლობალურ პოლიტიკურ დონეზე, თავიანთი ინტერესებით ზეგავლენას ახდენენ მასზე, აღსანიშნავია, რომ ამა თუ იმ ფორმით ისინი ჩართულებიც არიან რუსეთ-უკრაინის ომის პროცესში, ზოგი იარაღს აწვდის, სანქციებს აწესებს, ზოგი მოლაპარაკების ინიციატივით გამოდის და ასე შემდეგ.

ჩრდილოატლანტიკური ალიანსი (NATO)

რა თქმა უნდა, როდესაც ვახსენებთ პოლიტიკურ აქტორებს, უსაფრთხოებას, სტანდარტდებს, კოლექტიურ თავდაცვას, კიბერუსაფრთხოებას, ინფორმაციულ უსაფრთხოებას და სხვა, პირველი გვახსენდება ჩრდილოატლანტიური ალიანსი, რომელიც ზოგადად უსაფრთხოების გარანტორია მსოფლიო მასშტაბით, თუმცა

ამისდამიუხედავად, რუსეთი მაინც აწარმოებს დაუნდობელ ომს უკრაინაში, ასევე არ უნდა დაგვავიწყდეს, რომ ახორციელებს საქართველოს ტერიტორიის 20 პროცენტის ოკუპაციას და ზეგავლენის მოხდენას ცდილობს ბევრ ქვეყანაზე.

ჩრდილოატლანტიკური ალიანსი წარმოადგენს სამხედრო-პოლიტიკურ ორგანიზაციას, რომელიც 1949 წლის 4 აპრილს შეიქმნა. აღნიშნული ალიანსი ამჟამად აერთიანებს ჩრდილოეთ ამერიკის 2 და ევროპის 28 სახელმწიფოს, რომლის მიზანია ჩრდილოატლანტიკურ სივრცეში მშვიდობის, მისი წევრი ქვეყნების თავისუფლებისა და უსაფრთხოების უზრუნველყოფა, როგორც პოლიტიკური, ისე სამხედრო საშუალებებით. ალიანსი მკაცრად იცავს და პატივს სცემს ისეთ ღირებულებებს, როგორიცაა წევრი ქვეყნების სუვერენიტეტი, ტერიტორიული მთლიანობა, დემოკრატია, ინდივიდუალური თავისუფლება, ადამიანის უფლებები და კანონის უზენაესობა, რაც 360 გრადუსით არ მოდის თანხვედრაში რუსეთის ფედერაციასთან. ომამდე რუსეთის ერთ-ერთი *„ჰრეტენზია“* უკრაინის მიმართ სწორედ ჩრდილოატლანტიკურ ალიანსში გაწევრიანების საკითხი გახლდათ, მიზეზად კი მის საზღვრებთან ალიანსის მიახლოება იყო. რუსეთის ლიდერმა შესანიშნავად იცოდა, რომ უკრაინის ნატოში გაწევრიანება 2022 წელს არარეალისტური გახლდათ, რაზეც მას არაერთხელ მიანიშნეს ნატოს წევრი სახელმწიფოების სხვადასხვა ლიდერებმა, მაგრამ ამ ქვეყნის აგრესიული საგარეო პოლიტიკური ამბიციები, ცხადია, მისი გეოპოლიტიკური ინტერესებიდან გამომდინარეობს და არც ის დავივიწყოთ, რომ ჯერ 2008 წელს საქართველოში შეჭრა და ტერიტორიების 20 პროცენტის ოკუპაცია, ხოლო შემდგომში 2014 წლის ყირიმის ანექსია ერთგვარი წამახალისებელი ფაქტორი შეიქმნა პირადად ვლადიმერ პუტინისთვის. აქვე უნდა აღვნიშნოთ, რომ დაუსჯელობა კიდევ ერთი მნიშვნელოვანი ფაქტორი გახდა პუტინისთვის, რომ ამჯერად დასავლეთისთვისაც მოეწყო გამოცდა, განსაკუთრებით მას ძალის დემონსტრირება ჩრდილოატლანტიკური ალიანსისთვის სურდა, თუმცა უნდა ხაზგასმით ვთქვათ, ნატომ შეძლო და შეინარჩუნა თავისი წევრი ქვეყნების უსაფრთხოება, რომლის გარანტორიც სწორედ მე-5-ე მუხლია - *„ევროპისა და ჩრდილოეთ ამერიკის ტერიტორიაზე ერთ ან ერთზე მეტ მხარეზე განხორციელებული შეიარაღებული თავდასხმა აღიქმება ყველას წინააღმდეგ თავდასხმად“.*[6] რაც, რა თქმა

[6] *Verhelst A., "A comparative analysis of Article 5 Washington Treaty (NATO) and Article 42(7) TEU (EU)", EPRS - European Parliamentary Research Service, p. 1, 2022. www.europarl.europa.eu/RegData/etudes/ATAG/2022/739250/EPRS_ATA(2022)739250_EN.pdf*

უნდა, ალიანსის წევრ-სახელმწიფოებს გულისხმობს, ხოლო არაწევრ სახელმწიფოებს ზედმეტი ილუზიები არ უნდა გაუჩნდეთ. ამის მიუხედავად, რუსეთ-უკრაინის ომმა მაინც დაგვანახა, რომ სამხედრო-პოლიტიკურმა ალიანსმა არა მხოლოდ თავისი ტერიტორიის თავდაცვის შენარჩუნება შესძლო, არამედ საკმაოდ სერიოზულ და ქმედით დახმარებას უწევს უკრაინას. აუცილებლობა ითხოვს, ნატოსთან მიმართებაში სხვა მნიშვნელოვანი დეტალიც გამოვყოთ: მიუხედავად იმისა, რომ გაფართოების პოლიტიკის დეკლარირებით, რომელიც თავის დროზე საქართველოზე და უკრაინაზე ***MAP***-გაწევრიანების სამოქმედო გეგმის არმიცემამ რუსეთის ხელმძღვანელობა საკმაოდ გაათამამა, რაც იმას გულისხმობს, რომ ახალი პრეტენზიები წაუყენა დასავლეთს, მაგრამ შეიძლებოდა გვევარაუდა, რომ შეცვლილი პოლიტიკური ვითარებიდან გამომდინარე, ნატო მიიღებდა ახალ წევრებს შვედეთისა და ფინეთის სახით, შვედეთი ჯერ-ჯერობით არა, თუმცა ფინეთი ცოტა ხნის წინ ნატოს ახალი წევრი გახდა, რაც ამ ქვეყანას სწორედ რუსეთის შესაძლო აგრესიისგან პრევენციამ და სწორედ მისგან უფრო საფუძვლიანმა თავდაცვამ გადაწყვიტა. რაც შეეხება შვედეთს, თუ ის შეძლებს თურქეთის მოთხოვნების დაკმაყოფილებას, ნატოს წევრად ვიხილავთ.

ვლადიმერ პუტინი

ამ საკითხთან დაკავშირებით, საინტერსო განცხადება გააკეთა რუსეთის პრეზიდენტმა ***ვლადიმერ პუტინმა:***

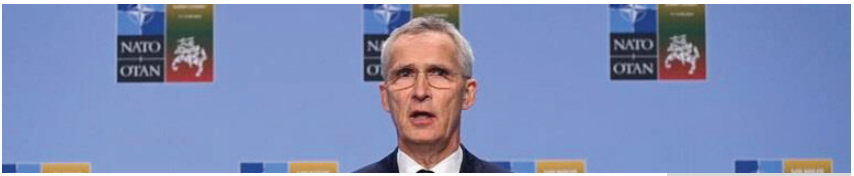
„რუსეთს არ ემუქრება საფრთხე, თუ შვედეთი და ფინეთი გაწევრიანდებიან ნატოში, თუმცა მოსკოვი უპასუხებს, თუ აშშ-ის ხელმძღვანელობით ალიანსი გააძლიერებს სამხედრო ინფრასტრუქტურას ახალ სკანდინავიურ წევრებში.“[7]

[7] *Faulconbridge G., "Putin sees no threat from NATO expansion, warns against military build-up", Reuters, p. 1, 2022, https://www.reuters.com/world/europe/russia-calls-finland-sweden-joining-nato-mistake-with-far-reaching-consequences-2022-05-16/*

აღნიშნული მოვლენების ასეთი განვითარება ცხადყოფს, რომ ევროკავშირს თავისი ტერიტორიის თავდაცვის უზრუნველყოფა ნაკლებად შეუძლია *(ევროკავშირის წევრ ქვეყნებს, რომელთა უმეტესობა ნატოს წევრიცაა, ნამდვილად არა აქვთ სურვილი ორი სამხედრო ბიუჯეტი და ორმაგი სამხედრო დანახარჯი ჰქონდეთ. ასევ კარგად ესმით, სამხედრო ამბიციები, თუ ამერიკის შეერთებული შტატების სამხედრო პოტენციალის მხრიდან არ იქნება უზრუნველყოფილი და მხარდაჭერილი, რეალურ უსაფრთხოებაზე და თავდაცვაზე ლაპარაკი ზედმეტია).* აქედან გამომდინარე, ევროპისთვის ნატო კვლავ ერთადერთია, რომელიც რჩება თავდაცვისა და უსაფრთხოების მთავარ გარანტორად. ხოლო ერთადერთ საფრთხედ რუსეთი რჩება ბირთვული პოტენციალით. თუმცა არ უნდა დაგვავიწყდეს ჩრდილოატლანტიკური ალიანსის, მათ შორის ევროპის ტერიტორიაზე განლაგებული სამი ქვეყნის ბირთვული შეიარაღება. იმედია, საქმე ასეთ დაპირისპირებამდე არ მივა, მიუხედავად იმისა, რომ ხშირია საუბრები ბირთვული იარაღის გამოყენებაზე, თუ მისი გამოყენება განხორციელდა რუსეთის მხრიდან, რა თქმა უნდა, პასუხიც ადეკვატური იქნება, შედეგები კი კატასტროფამდე მიიყვანს მსოფლიოს. რა რეალობაც გვაქვს, შეგვიძლია ვთქვათ, რომ რუსეთ-უკრაინის ომში, ნატოს საკმაოდ მკაცრი პოზიცია უჭირავს და არ აპირებს რუსეთთან რაიმე სახის დათმობაზე წასვლას, თუ, რა თქმა უნდა, ალიანსის ლიდერი სახელმწიფოების პოლიტიკური ხელმძღვანელობის პოლიტიკური ნებაც მტკიცედ იქნება შენარჩუნებული.

გვერდს ვერ ავუვლით ვილნიუსში გამართულ ნატოს სამიტს, სადაც ყველაზე მნიშვნელოვანი განცხადება, რაც გაკეთდა, გახლდათ ის, რომ მოკავშირეები შეთანხმდნენ ნატოს ყველაზე დეტალურ და მტკიცე თავდაცვის გეგმებზე ცივი ომის შემდეგ. ფაქტობრივად, მოხდა ძველი გეგმის ადაპტაცია, ოღონდ იმის გათვალისწინებით, თუ ვინმეს ეჭვი ეპარებოდა იმაში, რომ რუსეთი არ იყო პოტენციური მოწინააღმდეგე, ამ სამიტზე დააკონკრეტეს, ხაზგასმით აღნიშნეს - ნატო

კვლავ გამოთქვამს მზადყოფნას წარმართოს პრაგმატული პოლიტიკა რუსეთთან მიმართებაში. ასევე, სამიტზე მოხდა შეთანხმება უკრაინისა და ნატოსთან უფრო მეტად დაახლოებაზე. მოკავშირეებმა დაადასტურეს, რომ უკრაინა გახდება ნატოს წევრი სამოქმედო გეგმის ***(MAP)*** გარეშე.



იენს სტოლტენბერგი

„ეს შეცვლის უკრაინის წევრობის გზას ორსაფეხურიანი პროცესიდან ერთსაფეხურიან პროცესზე“,[8] - განაცხადა ***იენს სტოლტენბერგმა:*** *„ჩვენ გამოვუგზავნით უკრაინას ნატოში გაწევრიანების მოწვევას, როდესაც მოკავშირეები შეთანხმდებიან, რომ პირობები შესრულდება''.*[9] მან დასძინა, რომ უკრაინა ახლა *"ნატოსთან უფრო ახლოსაა, ვიდრე როდისმე".*[10] მისი თქმით, ომის დასრულების შემდეგ მოკავშირეებმა უნდა უზრუნველყონ ღონისძიებები უკრაინის უსაფრთხოებისთვის. ნიშნავს თუ არა ეს რეალურად ნატოში უკრაინის გაწევრიანების ვადას? ცხადია, არა. ნიშნავს თუ არა უკრაინისთვის დახმარების გაზრდას? დიახ, ნიშნავს, მაგრამ რამდენად დაკმაყოფილდა ამით უკრაინის პოლიტიკური ისტებლიშმენტის, კერძოდ პრეზიდენტ ზელენსკის თვითდაჯერებული ამბიციები, ეს უკვე სხვა საკითხია.

რა მიიღო საქართველო ამ სამიტიდან? იგივე, რაც მანამდე ჰქონდა - ნატოს კარი ჩვენთვის ისევ ღიაა, მაგრამ იქ შესასვლელად დასავლეთის მტკიცე პოლიტიკური ნება კვლავ არ ჩანს. ვილნიუსის სამიტმა დაგვანახა, რომ ნატოს თავდაცვით გეგმებში მაინც და მაინც აქტიური როლი არ გვაქვს, რით არის ეს გამოწვეული, ისევ რუსეთის არგაღიზიანების პოლიტიკით თუ გაუაზრებელი სტრატეგიულ-გეოგრაფიული მდებარეობის მნიშვნელობით? ამას მომავალი გვიჩვენებს.

---

[8] *Nato, "Doorstep statement - by NATO Secretary General Jens Stoltenberg at the start of the 2023 NATO Summit in Vilnius", p. 1, 2023. https://www.nato.int/cps/en/natohq/opinions_217038.htm?selectedLocale=en*

[9] *Nato, "Doorstep statement - by NATO Secretary General Jens Stoltenberg at the start of the 2023 NATO Summit in Vilnius", p. 1, 2023. https://www.nato.int/cps/en/natohq/opinions_217038.htm?selectedLocale=en*

[10] *Nato, "Doorstep statement - by NATO Secretary General Jens Stoltenberg at the start of the 2023 NATO Summit in Vilnius", p. 1, 2023. https://www.nato.int/cps/en/natohq/opinions_217038.htm?selectedLocale=en*

ნატოს შემდეგი სამიტი 2024 წელს ვაშინგტონში გაიმართება ალიანსის დაარსებიდან სამოცდათხუთმეტი წლის აღსანიშნავად, დაველოდოთ, მომავალი სამიტი ან მხოლოდ საიუბილეო თარიღით იქნება ისტორიული, ან რეალური ნაბიჯებიც გადაიდგმება... ვნახოთ ***„ვაშინგტონი - 2024“*** თავს რით დაგვამახსოვრებს.

რეჯეფ ტაიფ ერდოღანი

პოლიტიკური ლიდერების ნება რომ მნიშვნელოვანია, ეს ახალი არ არის. მაგალითად, ჩრდილოატლანტიკური ალიანსის მნიშვნელოვანი წევრი ქვეყნის, თურქეთის შემთხვევაში შეგვიძლია ვისაუბროთ, თუ რამხელა როლი და გავლენა გააჩნია პრეზიდენტ ***რეჯეფ ტაიფ ერდოღანს (Recep Tayyip Erdoğan),*** როგორც ერთ-ერთ სერიოზულ პოლიტიკურ ფიგურას. ხაზი უნდა გავუსვათ იმას, რომ თურქეთის პრეზიდენტი უპირველესად თავისი ქვეყნის ინტერესების სასარგებლოდ მოქმედებს. ამის ნათელი მაგალითია, თუ როგორ შეძლო მან სირიის ომის დროს რუსეთთან დაძაბული ურთიერთობის დარეგულირება. როგორც ვიცით, თურქეთის მიერ რუსული სამხედრო თვითმფრინავს ჩამოგდების შემდეგ ***ერდოღანმა*** ბოდიში მოიხადა, პირადად ჩავიდა რუსეთში, შეხვდა ***ვლადიმერ პუტინს*** და საბოლოოდ ინციდენტიც ამოიწურა. არადა, იმდენად დაძაბული იყო სიტუაცია, სერიოზულადაც კი განიხილებოდა გარკვეულ წრეებში რუსეთ-თურქეთის შესაძლო ომი, მიუხედავად იმისა, რომ თურქეთი ნატოს წევრია. ერდოღანმა, რეალურად გადაარჩინა თურქული ექსპორტ-იმპორტის ბაზარი, ინვესტიციები. ასევ შეინარჩუნა მილიონობით რუსი ტურისტი. რა იყო ეს, თურქეთის პრეზიდენტის სისუსტე თუ სიძლიერე? ცხადია, მან გაიმარჯვა, და მეტიც, რუსეთთან ურთიერთობა კიდევ უფრო გააძლიერა, მით უმეტეს, იმ ფონზე, როცა ცალკე ევროპელებზე და ცალკე ამერიკელებზეც განაწყენებული გახლდათ. ყოველივეს თამამად შეიძლება ვუწოდოთ თურქულ-აღმოსავლური დიპლომატიის სიბრძნეც და მოქნილობაც. დღეს რუსეთ-უკრაინის მოლაპარაკებაში თურქეთის, როგორც შუამავლის როლი, არამარტო ომის დასრულებასა და რაღაც შეთანხმების მიღწევაშია მნიშვნელოვანი, არამედ თვით თურქეთისთვისაც გახლვ

სარფიანი, როგორც რეგიონული მოთამაშის სტატუსის უფრო გაძლიერებისთვის. თუ იმასაც გავითვალისწინებთ, რომ ის ომთან დაკავშირებით საკმაოდ ფრთხილ, მოქნილ და გონიერ საგარეო პოლიტიკის აწარმოებს, უნდა ჩავთვალოთ, რომ საქმე გვაქვს სერიოზულ პოლიტიკასთან. როგორც, არ უნდა დასრულდეს რუსულ-უკრაინული მოლაპარაკებები, სავარაუდოდ, თურქეთის შუამავლის როლს ვერც რუსული და ვერც უკრაინული მხარე ადვილად ვერ დაივიწყებს. ასევე, ეს არის სიგნალი, როგორც ამერიკელებისთვის, ევროპელებისთვისაც, ევროკავშირისთვისაც და ნატოსთვისაც, რომელთა კრიტიკასაც პერიოდულად ამ ომთან დაკავშირებით პრეზიდენტი ***ერდოღანი*** არ ივიწყებს. მათ ვერ შეძლეს თურქეთის, როგორც აქტორის როლის და მნიშვნელობის შეფასება მთელ რიგ საკითხებთან მიმართებაში. ომის დასრულების შემდეგ კი მისი პრეტენზიები, რუსული, უკრაინული თუ ევროპული ბაზრის მიმართ უფრო და უფრო გაიზრდება, რაც შესაძლოა, სავსებით სამართლიანიც გახდეს.

თურქეთში საპრეზიდენტო არჩევნები ცოტა ხნის წინ ჩატარდა, ***რეჯეფ ტაიფ ერდოღანმა*** დამაჯერებლად გაიმარჯვა. ცხადია, საქართველოს მიმართ პოლიტიკა არ შეცვლილა და ეს ასეც იყო მოსალოდნელი. ვვარაუდობთ, ეტაპობრივად შეიძლება გაიზარდოს თურქეთის მხარდაჭერა, უპირობო მხარდაჭერა საქართველოს ევროტლანტიკური მისწრაფებებისადმი. უნდა ველოდოთ, რომ ბატონი ***ერდოღანი,*** როგორც რეგიონული ლიდერი, კიდევ უფრო წაახალისებს რეგიონში საქართველოს როლსა და მნიშვნელობას. იგი, სავარაუდოდ,. მიმართავს ფორმულას - ძლიერი და სტაბილური მეზობელი შენი სიძლიერის ერთგვარი გარანტორია. თურექთის პრეზიდენტი ყოველთვის აფასებდა და დღესაც აფასებს საქართველოს, როგორც დამოუკიდებელი მეზობლის როლს სამხრეთ კავკასიის სტაბილურობის, მშვიდობისა და ეკონომიკური განვითარების საქმეში. რაც შეეხება პრეზიდენტობის კანდიდატს, რომელიც მეორე ტურში დამარცხდა, ქემალ ქილიჩდაროღლუს, იგი აქცენტს აკეთებდა, არა რეგიონულ ლიდერობაზე, არამედ დასავლეთთან მჭიდრო ურთიერთობაზე. შესაბამისად, ბატონი ქილიჩდაროღლუს გამარჯვების შემთხვევაში, შეიძლებოდა გვევარაუდა, რომ საქართველოს მოუწევდა კიდევ ერთი *„პრო-დასავლური“* ლიდერის საშუამავლო *„შეგონების“* მოსმენა. ერდოღანის პოზიცია რუსეთ-უკრაინის ომთან დაკავშირებით ცალსახად ცნობილია, იგი მრავალი ფაქტორის, მათ შორის თურქეთის ეროვნული ინტერესების გათვალისწინებით,

სამშვიდობო ინიციატივას უჭერს მხარს. ფაქტია, თურქეთის რესპუბლიკა, რომელთანაც მჭიდრო სავაჭრო-ეკონომიური ურთიერთობები გვაკავშირებს, ჩვენთვის უმნიშვნელოვანესი სახელმწიფო გახლავთ და იქ განვითარებული მოვლენები პირდაპირ თუ ირიბად ჩვენზეც ახდენს ზეგავლენას.

ნატოს კიბერშესაძლებლობები

მსოფლი მასშტაბით ყველა მოწინავე ქვეყანა, რომელიც კიბერუსაფრთხოების მიმართულებით მუშაობს, თანხმდება იმაზე, რომ კიბერსივრციდან მომდინარე საშიშროებასთან გამკლავება შეუძლებელია, თუ არ იქნება ერთიანი კოორდინირებული მუშაობა, ერთიანი პროგრამა და საერთო სტრატეგია. შესაბამისად, ამ მხრივ ცენტრალურ რგოლს წარმოადგენს ჩრდილო ატლანტიკური ალიანსი, რომელიც თავდაცვითი მიმართულებით ერთი ქოლგის ქვეშ აერთიანებს არა მხოლოდ თავის წევრ ქვეყნებს. ამავე ქოლგაში ერთ-ერთ მნიშვნელოვან რგოლად შედის ევროკავშირიც თავისი სტრუქტურებით და წევრი ქვეყნებით. ამ ორ სტრუქტურას სრულად აქვს იმის შესაძლებლობა, გაუმკლავდეს და თავიდან აიცილოს მძლავრი, ასე ვთქვათ, დამანგრეველი კიბერშეტევები.

“ნატოში პირველად ეს საკითხი 2002 წელს განიხილეს პრაღის სამიტზე, ხოლო 2008 წელს შიიღეს პირველი კიბერთავდაცვითი პოლიტიკური დოკუმენტი. 2012 წლიდან ნატო ახორციელებს კიბერუსაფრთხოების სისტემური ინტეგრაციის პროცესს. მნიშვნელოვანია, რომ 2014 წელს უელსის სამიტზე მოკავშირეებმა კიბერთავდაცვა კოლექტიური თავდაცვის ერთ-ერთი პუნქტი გახადეს. 2016 წელს ვარშავის სამიტზე ალიანსის წევრმა ქვეყნებმა ინფორმაციული და საკომუნიკაციო ქსელების უსაფრთხოება ერთ-ერთ წამყვან სფეროდ აღიარეს და განაცხადეს, რომ ნატო, როგორც ხმელეთზე, ზღვასა და ჰაერში იცავს თავს, ასევე უნდა დაიცვას კიბერსივრცეში“.[11]

[11] *NATO, "Cyber defence", p. 1, 2022, https://www.nato.int*

როგორც აღვნიშნეთ, კიბერუსაფრთხოების და ინფორმაციული უსაფრთხოების მიმართულებით ნატოს ყველაზე მნიშვნელოვან პარტნიორს 2016 წლიდან ევროკავშირი წარმოადგენს.

იენს სტონტელბერგი

2021 წელს ნატოს სამიტი ბრიუსელში გაიმართა. ჩრდილოატლანტიკური ალიანსის გენერალურმა მდივანმა ***იენს სტონტელბერგმა*** ბევრ საკითხზე გაამახვილა ყურადღება და მათ შორის კიბერსივრცეზეც ისაუბრა:

„ჩვენთვის ეს ახალი გამოწვევაა, უკვე ვდგავართ აგრესიული ქვეყნების მხრიდან მომდინარე სხვადასხვა საფრთხის წინაშე. ახლა მთავარია ერთობლივი მუშაობა, ადაპტაცია და ფორმირება. ჩვენ ყოველდღიურად ვმუშაობთ კიბერუსაფრთხოების გაძლიერებაზე“.[12]

ჩრდილო-ატლანტიკურ ალიანსში კიბერუსაფრთხოების საკითხები რამდენიმე მიმართულებად არის დაყოფილი, ესენია: კვლევა, შესაძლებლობების განვითარება და რისკების შემცირება. ამ მხრივ მუშაობს ***ნატოს კომუნიკაციებისა და ინფორმაციის სისტემების მომსახურების სააგენტო (NCSA)***, აქ ძირითადად ყალიბდება თავდაცვით მექანიზმები. ასევე, არსებობს ***ნატოს ინფორმაციის უსაფრთხოების ტექნიკური ცენტრი (NITC),*** რომელიც უზრუნველყოფს კომუნიკაციას, მენეჯმენტს, კრიპტოგრაფიულ აპარატურას, კიბერშეტევებზე რეაგირების კოორდინაციასა და კომპიუტერულ უსაფრთხოებას. ***ნატოს კომპიუტერული ინციდენტების რეაგირების ცენტრი (NCIRC),*** რომელიც პასუხისმგებელია დაშიფრული სისტემების დაცვაზე.

[12] *NATO, "NATO Secretary General addresses the Brussels Forum: "We need a bold strategy for our new security reality", p. 1. 2022. https://www.nato.int*

ნატოს კოოპერატიული კიბერთავდაცვის ცენტრი არის მრავალეროვნული და ინტერდისციპლინარული კიბერთავდაცვის სტრუქტურა (CCDCOE), რომელიც ატარებს კვლევებს, ტრენინგებსა და წვრთნებს ოთხ ძირითად სფეროში: ***ტექნოლოგია, სტრატეგია, ოპერაციები*** და ***სამართალი.*** აღნიშნული ცენტრის მიერ მსოფლიო მასშტაბით ტარდება კონფერენციები, იწერება სამეცნიერო სტატიები, იქმნება სახელმძღვანელოები უსაფრთხოების მიმართულებით. ჩვენ უნდა განვიხილოთ რამდენიმე მეტად საყურადღებო თემა, რათა უფრო სრულად წარმოვიდგინოთ, თუ რას აკეთებს კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების მიმართულებით ნატო, როგორი ხედვა აქვს და რა პერსპექტივები არსებობს. სახელმძღვანელოში ***(NATIONAL CYBER SECURITY FRAMEWORK MANUAL)***, სადაც განსაზღვრულია, თუ რა სტრატეგიული მიმართულებებით მოქმედებს ნატო ინფორმაციული უსაფრთხოებისა და კიბერუსაფრთხოების მიმართულებით, გამოყოფილია ძირითადი თეორიული მიდგომები:

National Cyber Security (NCS) *Defined*	*'The focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security.'*
The 5 Mandates *Different interpretations of NCS & common activities*	- Military Cyber - Counter Cyber Crime - Intelligence and Counter-Intelligence - Critical Infrastructure Protection and National Crisis Management - Cyber Diplomacy and Internet Governance + 3 'Cross Mandates': coordination, information exchange and data protection, research & development and education
The 3 Dimensions *Different stakeholder groups in NCS*	- Governmental (central, state, local) – 'coordination' - National (CIP/contactors, security companies, civil society) – 'co-operation' - International (legal, political and industry frameworks) – 'collaboration'
The 5 Dilemmas *Balancing the cost and benefits of NCS*	- Stimulate the Economy vs. Improve National Security - Infrastructure Modernisation vs. Critical Infrastructure Protection - Private Sector vs. Public Sector - Data Protection vs. Information Sharing - Freedom of Expression vs. Political Stability

ცხრილი 1: ძირითადი თეორიული მიდგომები. *წყარო: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf*

„ეროვნული კიბერუსაფრთხოება (NCS) - *„კონკრეტული სამთავრობო ბერკეტების, ინფორმაციის უზრუნველყოფის, საჯარო, კერძო და შესაბამისი საერთაშორისო* ***ICT***

სისტემების მიზანმიმართული გამოყენება, რომელიც პირდაპირ ეხება ეროვნულ უსაფრთხოებას".

5 მანდატი, განსხვავებული ინტერპრეტაციები და ეროვნული კიბერუსაფრთხოების საერთო საქმიანობა

- სამხედრო კიბერუსაფრთხოება;

- კიბერდანაშაულის წინააღმდეგ მოქმედება;

- დაზვერვა და კონტრდაზვერვა;

- კრიტიკული ინფრასტრუქტურის დაცვა და ეროვნული კრიზისების მართვა;

- კიბერდიპლომატია და ინტერნეტის მართვა, + 3 „ჯვარედინი მანდატები": კოორდინაცია, ინფორმაციის გაცვლა და მონაცემების დაცვა, კვლევა, განვითარება, განათლება.

3 განზომილება, დაინტერესებული მხარეების სხვადასხვა ჯგუფები ეროვნულ კიბერუსაფრთხოებაში

- სამთავრობო (ცენტრალური, სამთავრობო, ადგილობრივი) - ,,კოორდინაცია";

- ეროვნული (CIP/კონტაქტები, უსაფრთხოების კომპანიები, სამოქალაქო საზოგადოება) - ,,თანამშრომლობა";

- საერთაშორისო (სამართლებრივი, პოლიტიკური და ინდუსტრიული ჩარჩოები) - ,,თანამშრომლობა".

5 დილემა, ღირებულების დაბალანსება და ეროვნული კიბერუსაფრთხოების სარგებელი

- ეკონომიკის სტიმულირება ეროვნული უსაფრთხოების გაუმჯობესების წინააღმდეგ;

- ინფრასტრუქტურის მოდერნიზაცია კრიტიკული ინფრასტრუქტურის დაცვის წინააღმდეგ;

- კერძო სექტორი საჯარო სექტორის წინააღმდეგ;

- მონაცემთა დაცვა ინფორმაციის გაზიარების წინააღმდეგ;

- გამოხატვის თავისუფლება პოლიტიკური სტაბილურობის წინააღმდეგ.[13]

აღნიშნული საკითხები მართლაც აქტუალურია დღევანდელი მსოფლიოსთვის, ინტერნეტი ***საინფორმაციო და საკომუნიკაციო ტექნოლოგიებთან (ICT)*** ერთად არის

[13] *Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 16. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf*

კრიტიკული ეროვნული რესურსი, ინფრასტრუქტურისა და სოციალურ-ეკონომიკური ზრდისა, განვითარების მთავარი მამოძრავებელი. ბოლო წლების განმავლობაში ყველა სფერო მოიცვა ინტერნეტმა და საინფორმაციო საკომუნიკაციო ტექნოლოგიებმა.

ფინანსების გამომუშავებამ, დასაქმებამ და ონლაინ სივრცეში მუშაობამ, ბიზნესის მართვამ, ინფორმაციაზე წვდომის უწყვეტობამ და ელექტრონულმა ონლაინ სწავლებამ ხელი შეუწყო ქვეყნების განვითარებას ყველა მიმართულებით. *"ზოგიერთ სახელმწიფოში მთლიანი შიდა პროდუქტის წვლილი ინტერნეტიდან 8 პროცენია".*[14]

უნდა ვაღიაროთ, ინტერნეტი შემთხვევით არავის გამოუგონია, ეს არის მეცნიერთა დაუღალავი შრომის შედეგი. *„პირველი ინტერნეტკავშირი 1969 წელს მოხდა. მას შემდეგ იყო საცდელი პერიპეტიები. სადაც ამჟამად დღეში 284 მილიარდი ელექტრონული ფოსტა იგზავნება, ჯერ კიდევ 1970-იან წლებში ინტერნეტპროტოკოლები შეიქმნა, რათა ფაილების გაზიარება და ინფორმაციის გაცვლა ყოფილიყო შესაძლებელი. დღეს ინფორმაციის შექმნა და გაზიარება ონლაინ სივრცეში პრობლემას საერთოდ აღარ წარმოადგენს. 1983 წელს დომენის სახელების სისტემების წარმატებული დემონსტრირება მოხდა **(DNS)**, რომელმაც საფუძველი ჩაუყარა დიდ გაფართოებას, პოპულარიზაციასა და ინტერნეტის კომერციალიზაციას. 1985 წლიდან უმაღლესი დონის დომენების გამოგონებით **(com, edu, gov და ა.შ.)** შესაძლებელი გახდა ელექტრონული კომერციის, ელექტრონული ეკონომიკის განვითარება. აღნიშნული საკითხი 1990 წელს მსოფლიო ქსელის გამოგონებით, უფრო მასშტაბური გახდა. დღეს ინტერნეტს მოიხმარს დედამიწის ორი მესამედი, რაც ასევე ონლაინ რეჟიმში ბიზნესის წარმოებასაც გულისხმობს - იყენებენ ისეთ საძიებო სისტემებს, როგორებიცაა Google, Yahoo და ა.შ."*[15] სოციალურ ქსელებზე, რომ აღარაფერი ვთქვათ.

აქვე უნდა აღვნიშნოთ, რომ ინტერნეტი და ***საინფორმაციო საკომუნიკაციო ტექნოლოგიები (ICT)***, რომელიც მას უდევს საფუძვლად და ქსელები, რომლებსაც ის

[14] Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 19. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

[15] Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 20. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

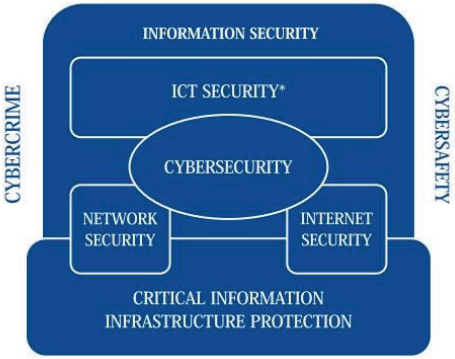
აკავშირებს, მოიხსენიება როგორც „კიბერსივრცის“ ერთობლიობა. ტერმინი „კიბერი“ ხშირ შემთხვევაში განისაზღვრება როგორც კომპიუტერბთან ან კომპიუტერულ ქსელებთან დაკავშირებული ჩართული სისტემა - ინტერნეტი, ვირტუალური სივრცე. თუმცა რეალურად კიბერსივრცე უფრო მეტია, ვიდრე ინტერნეტი, იგულისხმება არა მხოლოდ აპარატურა, პროგრამული უზრუნველყოფა ან საინფორმაციო სისტემები, არამედ ადამიანური რესურსი და სოციალური აქტივობა აღნიშნულ ქსელებში.

ამასთან დაკავშირებით, უნდა ითქვას, რომ ***საერთაშორისო სტანდარტიზაციის ორგანიზაცია (ISO)*** იყენებს ოდნავ განსხვავებულ ტერმინს, რომელიც კიბერს განსაზღვრავს, როგორც კომპლექსურ გარემოს, იგი წარმოიქმნება ურთიერთობების საშუალებით. ადამიანები, პროგრამული უზრუნველყოფა ინტერნეტში ტექნიკური მოწყობილობების საშუალებით, მასთან დაკავშირებული ქსელები, რომლებიც არ არსებობს რაიმე ფიზიკური ფორმით რეალურ სივრცეში.

საინტერესო ის გახლავთ, რომ მთავრობები თვითონ ადგენენ კიბერთან დაკავშირებულ ტერმინებს და ასევე განსაზღვრავენ, თუ რას გულისხმობენ კიბერსივრცეში, კიბერომში, კიბერშეტევებში და ა.შ. მაგალითად, ბრიტანეთის 2009 წლის კიბერუსაფრთხოების ეროვნული სტრატეგიის დოკუმენტში კიბერსივრცეს მოიხსენიებენ, როგორც *„ქსელური, ციფრული აქტივობების ყველა ფორმას. ეს, რა თქმა უნდა, უცნაურ საკითხს წარმოადგენს და ხშირ შემთხვევაში სადაოს ხდის ტერმონოლოგიის შინაარსს”.*[16]

ნატო, როგორც უსაფრთხოების მიმართულებით წამყვანი საერთაშორისო ორგანიზაცია, კიბერუსაფრთხოებას სხვა დომენების უსაფრთხოებათა შორის ასე აღიქვამს ***(იხილეთ ფიგურა 1.)***:

[16] *Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 25. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf*



ფიგურა 1: კავშირი კიბერუსაფრთხოებასა და უსაფრთხოების სხვა დომენებს შორის. *წყარო: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf*

კიბერდანაშაული და კიბერუსაფრთხოება

1. *ინფორმაციული უსაფრთხოება;*
2. *საინფორმაციო და საკომუნიკაციო ტექნოლოგიების უსაფრთხოება;*
3. *კიბერუსაფრთხოება;*
4. *ქსელის უსაფრთხოება;*
5. *ინტერნეტის უსაფრთხოება;*
6. *კრიტიკული ინფორმაციის ინფრასტრუქტურის დაცვა.*[17]

როგორც ყველა ქვეყანა, ნატოც კიბერმიმართულებით ტრემინოლოგიებს თავისებურად აყალიბებს. მსოფლიო მასშტაბით კი ტერმინოლოგიასთან მიმართებაში გარკვეული პრობლემები შეინიშნება. ჩვენ უკვე განვმარტეთ ზოგადად, თუ რას ნიშნავს კიბერშეტევა, კიბერომი, კიბერუსაფრთხოება და ა.შ. ამ შემთხვევაში შეგვიძლია გავიგოთ, თუ რას ამბობს ნატო კიბერომთან დაკავშირებით. მაგალითად, ჩრდილოატლანტიკური ალიანსის დაქვემდებარებული ორგანიზაციის მიერ გამოცემულ წიგნში ვკუთხულობთ:

„კიბეროში ორაზროვან ტერმინს წარმოადგენს, ამაზე ექსპერტები დღემდე კამათობენ და ოფიციალური განმარტება მაინც ვერ დაადგინეს. რაც შეეხება საინფორმაციო ან

[17] *Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 27. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf*

ინფორმაციულ ომს, ეს ტერმინი ხშირად გამოიყენება ოფიციალურ დოკუმენტებში, თუმცა სხვადასხვა გაგებითა და მნიშვნელობით. ამჟამად 30-ზე მეტ ქვეყანას აქვს ჩამოყალიბებული კიბერუსაფრთხოების დოქტრინა, სადაც კიბეროშის განმარტებები კი არის წარმოდგენილი, მაგრამ შინაარსობრივი სხვაობა მაინც აშკარაა".[18]

70 წელზე მეტია, ნატო ავითარებს თავის ტექნოლოგიებს, რათა უზრუნველყოს მოკავშირეებისა და წევრი ქვეყნების დაცვა. *„2021 წლის თებერვალში ნატოს თავდაცვის მინისტრებმა დაამტკიცეს სტრატეგია* ***განვითარებადი და დამაზიანებელი (დამღუპველი) ტექნოლოგიების*** *შესახებ, რომელიც წარმართავს ნატოს* ***EDT*** *პოლიტიკის შემუშავებას კონკრეტულ მიმართულებებში.*

2021 წლის სამიტზე ბრიუსელში, ***„ნატო 2030"*** *დღის ფარგლებში, მოკავშირე ქვეყნების ლიდერები შეთანხმდნენ, რომ აემოქმედებინათ პროგრამა სახელწოდებით -* ***ინოვაციების ამაჩქარებელი ჩრდილო ატლანტიკისთვის (DIANA),*** *რათა შექმნან მრავალეროვნული რისკების კაპიტალის ფონდი, რათა მხარი დაუჭირონ ინოვაციების განვითარებას.*

2022 წელს მადრიდში გამართულ სამიტზე ალიანსის მოკავშირე ქვეყნების ყველა ლიდერმა მხარი დაუჭირა ***DIANA****-ს ქარტიას და გამოაქვეყნა სატესტო ცენტრებისა და ამაჩქარებლების საწყისი ლოკაციები. ნატოს 22 მოკავშირე ქვეყნების ლიდერები ვალდებულნი არიან, თავიანთი წვლილი შეიტანონ ალიანსის ინოვაციების ფონდში, რომელიც 1 მილიარდ ევროს შეადგენს. ინვესტიციების გაცემა 2023 წელს დაიწყება".*[19]

ცნობილია, რომ ნატო განვითარებადი და დამაზიანებელი (დამღუპველი) ტექნოლოგიების მიმართულებით თანამშრომლობს ევროკავშირთანაც და გაეროსთანაც, რათა ამ მხრივ სრულყოფილად მოაგვაროს პრობლემები. ნატო თავის

[18] *Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 28. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf*
[19] *Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 34. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf*

მხრივ გამოყოფს კიბერუსაფრთხოების ხუთ ძირითად საკითხს: ***იდენტიფიცირება, დაცვა, გამოვლენა, პასუხის გაცემა, აღდგენა.***

Identify	Cybersecurity is about cyber risk reduction, Thus, accurate risk identification from a safety and business perspective is essential for efficient allocation of resources. The identify function develops the organisational understanding to manage the cybersecurity risk to systems, assets, data, and capabilities.
Protect	Protection challenges are the introduction of dynamic and distributed networks in cloud environments. This challenge is solved with automation and security orchestration, where fit-for-purpose security policies are automatically set into the network infrastructure. Security policies ensure that the infrastructure has the desired and consistent security level across domains. This means policies enabling holistic security, e.g. identity and access security, data and traffic protection, and valid certificates. Furthermore, the automation ensures solid configurations of the network across domains, making intrusion or lateral movement for an attacker difficult.
Detect	Once the actual protection of the network is established, and under control, the focus moves to detection of threats and vulnerabilities. A vulnerability analysis is performed to verify the security characteristics and security configuration of the product/ solution and identifies new vulnerabilities through both black-box and white-box testing. Multiple tools and techniques can be used, such as vulnerability scanning, fuzzing and dynamic web application testing, and pen testing. Comprehensive security monitoring of both known and unknown threats with varying attacker tactics, techniques, and procedures is essential for keeping the network as secure as possible.
Respond	A successful security strategy must include detection of domain-specific threats and vulnerabilities followed by a response. Resources have the right domain knowledge to analyse threats at a deeper level based on data and insights from security tools, understand what is going on, and decide what actions need to be taken. Breaches and incidents also provide feedback to the security solution for continuous improvements, e.g. leading to new or enhanced security policies. To respond quickly, security automation needs to be integrated closely with network management platforms and network orchestration platforms including user plane monitoring (data monitoring) functions. The organisation also needs to have rehearsed digital forensics and incident response processes suitable for critical infrastructure with safety implications.
Recover	A recovery strategy helps an organisation to maintain or quickly resume its mission-critical functions after a disaster generally caused by a cyberattack. It is used to facilitate preventive planning and execution for catastrophic events that can significantly damage the infrastructure and the network assets. Predictive and automated security conditions recovery can significantly reduce the losses to critical systems that can be caused by cyberattacks and provide the system with the necessary resilience for operational continuity. Recovery processes and systems must be regularly tested especially against ransomware.

ცხრილი 2: კიბერუსაფრთხოების ხუთი ძირითადი საკითხი. *წყარო: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf*

„იდენტიფიცირება: *კიბერუსაფრთხოება წარმოდგენს კიბერრისკების შემცირებას, იდენტიფიცირება გულისხმობს რისკის ზუსტ ანალიზს, რათა მოხდეს უსაფრთხოდ ბიზნესპერსპექტივის განსაზღვრა, აუცილებელი რესურსების ეფექტური განაწილება. იდენტიფიკაცია ხელს უწყობს სისტემების, აქტივების, მონაცემებისა და კიბერუსაფრთოხების რისკების მართვის ნორმალურად ფუნქციონირებას.*

დაცვა: *დაცვის გამოწვევები მრავალმხრივია - თავდაცვითი მექანიზმების დანერგვა, ე.წ. ინფორმაციის შენახვა ვირტუალური მეხსიერების ღრუბლებზე. აღნიშნული გამოწვევა შესაძლოა მნიშვნელოვანწილად მოგვარდეს ავტომატიზაციით, ანუ სადაც უსაფრთხოების პოლიტიკა ავტომატურად არის დაყენებული ქსელის ინფრასტრუქტურაში. უსაფრთხოების პოლიტიკა გულისხმობს, რომ იყოს ინფრასტრუქტურა, რომელსაც ექნება შესაძლებლობა უსაფრთხოების სტანდარტების სრულად დაკმაყოფილებისა.*

უსაფრთხოების პოლიტიკამ უნდა უზრუნველყოს ჰოსტინგის უსაფრთხოება. მაგალითად, უნებართვო წვდომა, მონაცემების დაცვა და ტრაფიკის კონტროლი. ასევე საჭიროა მოქმედი საერთაშორისო სერთიფიკატები, რომ სტანდარტებს აკმაყოფილებს ჩვენი მოწყობილობები და ასევე - ცოცხალი რესურსი. რაც შეეხება ავტომატიზაციას, იგი უზრუნველყოფს მყარ კონფიგურაციას ქსელის დომენებს შორის, რაც ართულებს უნებართვო შეჭრას ქსელში.

გამოვლენა: *ქსელის დაცვის შემდეგ, როდესაც უსაფრთხოების ნორმები სრულად არის დაცული, აქცენტი უნდა გაკეთდეს საფრთხეებისა და დაუცველობის გამოვლენაზე. დაუცველობის ანალიზი და გამოვლენა ხორციელდება უსაფრთხოების შესამოწმებლად, შეიძლება ითქვას, ახალი დაუცველობის იდენტიფიცირებისა და აღმოფხვრის მიზნით. ამ დროს შეიძლება გამოყენებული იქნას მრავალი ინსტრუმენტი და ტექნიკა, როგორიცაა სკანირება, ბუნდოვანი და დინამიური ვებ-აპლიკაციის ტესტირება და ა.შ. ინტენსიური უსაფრთხოების მონიტორინგი, პროცედურების ჩატარება აუცილებელია ქსელის მაქსიმალურად უსაფრთხოების შესანარჩუნებლად.*

პასუხის გაცემა: *წარმატებული უსაფრთხოების სტრატეგია უნდა მოიცავდეს დომენის სპეციფიკური საფრთხეებისა და დაუცველობის გამოვლენას, რასაც უნდა მოჰყვებოდეს აუცილებელი პასუხი. უნდა არსებობდეს რესურსები, რათა უფრო ღრმად გაანალიზონ საფრთხეები ინსტრრუმენტების მონაცემების გამოყენებით და საკუთარ შეხედულებებზე დაყრდნობით. უნდა გავიგოთ, რა ხდება, რა გადაწყვეტილებები მივიღოთ, რა მოქმედებები განვახორციელოთ პასუხის გასაცემად. დარღვევები და ინციდენტები იძლევა უკუკავშირის საშუალებას, უსაფრთხოების გაუმჯობესებას. როდესაც დარღვევა ან ინციდენტი ხდება აღმოფხვრის მიზნით, აუცილებელია უსაფრთხოების ახალი, გაძლიერებული პოლიტიკის შემუშავება. სწრაფი რეაგირებისთვის უსაფრთხოების ავტომატიზაცია მჭიდროდ უნდა იყოს ინტეგრირებული ქსელის მართვის პლატფორმებთან. ორგანიზაციებს უნდა ჰქონდეთ შესაბამისი ციფრული სასამართლო ექსპერტიზისა და ინციდენტებზე რეაგირების საშუალება, კრიტიკული ინფრასტრუქტურის უსაფრთხოების მიზნით.*

აღდგენა: *აღდგენის სტრატეგია ეხმარება ორგანიზაციებს, შეინარჩუნონ ან სწრაფად განაახლონ მათი ფუნქციონირება კიბერშეტევით გამოწვეული ზარალის ან შეფერხების შემდეგ. თუ ორგანიზაცია ხშირად ინახავს მნიშვნელოვან და საჭირო მასალებს, პროგნოზირებადი და ავტომატური მონაცემების აღდგენამ შეიძლება მნიშვნელოვნად*

შეამციროს დანაკარგები. აღდგენის პროცესები და სისტემები რეგულარულად უნდა შემოწმდეს, განსაკუთრებით ფრთხილად უნდა ვიყოთ გამოსასყიდ კიბერთაღლითურ თავდასხმებთან მიმართებაში".[20]

რა პერსპექტივა გააჩნია კიბერუსაფრთხოების მიმართულებით დღეს ჩრდილოატლანტიკურ ალიანსს?

ნატოს ამ მიმართულებით მთელი რიგი გამოწვევები აქვს. კიბერის ინტეგრირება ერთობლივ ფუნქციებში და საბრძოლო საკითხებში წარმატების მისაღწევად ერთ-ერთი მნიშვნელოვანი საკითხია. ნატოს უნდა ჰქონდეს მკაფიო ხედვა იმაზე, თუ საით მიდის და რისი მიღწევა უნდა. რეალურად კიბერტექნოლოგიებს უფრო დიდი როლი უნდა ქონდეს ერთობლივ ვარჯიშებში.

ერთ-ერთ სირთულეს კიბერთავდასხმების შესახებ ტექნიკური მონაცემების მნიშვნელოვანი ინფორმაციის თარგმნა წარმოადგენს. აღნიშნული საკითხი დიდ ძალისხმევას ითხოვს. ალიანსი განმარტავს, რომ მეტი სამუშაოა ჩასატარებელი პასუხისმგებლობის ტაქტიკისა და დისციპლინის დაცვის მხრივ. ჩრდილოატლანტიკური ალიანსი აცხადებს, რომ მას ესაჭიროება მულტიდისციპლინური სპეციალისტები, რომელთაც უფრო ფართო გაგება აქვთ ახალ ტექნოლოგიებზე. კიბერნეტიკის ინტეგრირება ერთობლივ წვრთნებში და ამის ისე გაკეთება, რომ ყველა დონეზე სასწავლო მოთხოვნები დაკმაყოფილდეს, ამ შემთხვევაში ნატომ უნდა შეითვისოს სასწავლო ცენტრის ფუნქცია-მოვალეობებიც.

„წარმოიდგინეთ გაწვრთნილი ადამიანები, რომლებიც ბრუნდებიან ეროვნულ ძალებში, ეს ეფექტურსა და პროდუქტიულს ეროვნულ წვრთნებს. როგორ უნდა გაზარდოს ალიანსმა წარმატება ინდივიდებისა და კოლექტივების მოშზადებაში? ამაზე პასუხი ის არის, რომ ნატომ უნდა უზრუნველყოს სწორი ტრენინგის მიზნები. ნატოსა და ეროვნული წვრთნების უკეთესი ინტეგრაციის ერთ-ერთი გზა იქნება კიბერდიაპზონის უფრო ფართო გამოყენება, რა თქმა უნდა, ეროვნულ კიბერდიაპზონებთან ერთად".[21]

---

[20] *Nato Cooperative Cyber Defence Centre of Excellence, "Research Report Military Movement: Risks from 5G Networks", Tallinn, p. 48. 2022. https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf*

[21] *Ertan A., Kuprys L. C. A., Lillemets P., Nordli L. C. G., "Cyber Exercises: A Vision for NATO CyCon 2021 Workshop Summary Report", the NATO Cooperative Cyber Defence Centre of Excellence, p. 7, 2021. https://ccdcoe.org/uploads/2022/07/Cyber-Exercises-A-Vision-for-NATO-Summary-Doc-August-2021.pdf*

ზემოთ აღვნიშნეთ და ალბათ ხშირად გავიმეორებთ, რომ სტანდარტების დაცვა ერთ-ერთი უმნიშვნელოვანესი საკითხია კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების მიმართულებით. თუ არ იქნა ერთიანი სტანდარტები და მათი დაცვა, რუტინა, სხვაგვარად არაფერი გამოვა, ამის დასკვნის საშუალებას კი მსოფლიო პრაქტიკა იძლევა.

ჩრდილოატლანტიკურ ალიანსში არსებობს ***სტანდარტიზაციის ოფისი (NSO),*** რომელსაც კიბერუსაფრთხოების საკითხი მოწინავე პოზიციებზე აქვს დაყენებული. აღნიშნული ორგანიზაცია კოორდინაციას უწევს, მხარს უჭერს და მართავს ნატოს სტანდარტიზაციის საქმიანობას, რომელიც ტარდება სპეციალური კომიტეტის უფლებამოსილებით. იგი ეხმარება ნატოს სამხედრო კომიტეტს ოპერატიული სტანდარტების შემუშავებაში, რაც ხელს უწყობს სამხედრო ძალების ეფექტურობის ზრდას.

ნატომ განაცხადა, რომ მაღალი ხარისხის კიბერშეტევამ შეიძლება გამოიწვიოს მე-5 მუხლის გააქტიურება, რაც გულისხმობს კოლექტიურ თავდასხმას - „ერთი ყველასათვის, ყველა ერთისათვის“.

ჩრდილოატლანტიკური ალიანსის პოზიცია ასევე ცნობილია დაბალი ხარისხის კიბერშეტევებთან მიმართულებით. ნატოში განმარტავენ, რომ *“დაბალი ხარისხის კიბერშეტევა ყველაზე ნაკლებ რისკებს ქმნის და ამაზე პასუხი შეიძლება იყოს სანქციები. დაბალი ხარისხის კიბერშეტევაში იგულისხმება ფინანსური ან ინფორმაციული ზარალი, რომელიც ხანგრძლივ ეკონომიკურ ან ინფორმაციულ ზარალს არ წარმოადგენს”.*[22]

საყურადღებოა, რომ ალიანსის მოკავშირეებს ირიბი თუ პირდაპირი გზით წვლილი შეაქვთ ამ ორგანიზაციის მართვისა და პოლიტიკის საქმიანობის განხორციელებაში. ნატოს საერთო დაფინანსებული პროგრამები პირდაპირი შენატანებით ხორციელდება, რომელიც ხმარდება სამხედრო ინფრასტრუქტურის

[22] *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/*

მართვას და აქ კიბერინფრასტრუქტურაც შედის, *„რაც წარმოადგენს მოკავშირე ქვეყნების ჯაშური თავდაცვის ხარჯების მხოლოდ 0,3 პროცენტს, დაახლოებით 2,5 მილიარდი ევროს ექვივალენტს“.*[23]

მნიშვნელოვან საკითხს წარმოადგენს ისიც, რომ *„ნატოს ახალი სტრატეგია მოიცავს 1 მილიარდ დოლარს, განვითარებადი ტექნოლოგიების, კვლევების დასაფინანსებლად, მათ შორის კვანტური გამოთვლისა და ხელოვნური ინტელექტის მიმართულებით“.*[24]

ალბათ დაგვეთანხმებით, თანამედროვე ძალას, ისევე, როგორც მაგალითად, ინოვაციურ თავდაცვით ტექნოლოგიურ საერთაშორისო ორგანიზაციას, უნდა შეეძლოს გამოიყენოს, შეინახოს, უზრუნველყოს, გაანალიზოს და გააზიაროს დიდი რაოდენობით მონაცემები ნებისმიერი ადგილიდან.

„ნატოს მასშტაბით ციფრული ტრანსფორმაციაში კრიტიკული ინვესტიციის მცირე მაგალითები მოიცავს დიდი ბრიტანეთის თავდაცვის სამინისტროს 17,75 მილიონი ფუნტის კონტრაქტს Microsoft-ისა და Azure-ის კერძო „ღრუბელოვანი“ სერვისებისათვის. აღნიშნული საკითხი საჭიროა იმისთვის, რომ უფრო ეფექტურად ითანამშრომლონ მოკავშირე ქვეყნებმა“.[25]

ევროკავშირი (EU)

ევროპის სახელმწიფოთა ეკონომიკურ-პოლიტიკური გაერთიანება ***ევროპის კავშირი (ევროკავშირი),*** რომელსაც 1993 წლამდე ***ევროპის თანამეგობრობა (European Community)*** ერქვა. სადაც მოქმედებს ერთიანი შიდა ბაზარი, რომელსაც წევრი ქვეყნების კანონთა ერთობლიობა არეგულირებს. მისი გაცხადებული ძირითადი მიზანია ადამიანების, სერვისების, კაპიტალის, საქონლის თავისუფალი გადაადგილების უზრუნველყოფა, ერთიან შიდა ბაზარზე, ასევე მათ შორის აქტუალურ საკითხს წარმოადგენს ციფრული ბაზრის მნიშვნელობაც. საერთო

[23] *NATO, "Funding NATO", p. 1. 2022. https://www.nato.int*
[24] *Maggie M., "NATO establishes program to coordinate rapid response to cyberattacks", Politico, p. 1. 2022. https://www.politico.com*
[25] *Edwards S. S., Loomis W., Handler S., "Supersize cyber", Atlantic Cuncil, p. 1. 2022. https://www.atlanticcouncil.org*

პოლიტიკის შენარჩუნება ვაჭრობის მიმართულებით - სოფლის მეურნეობა, თევზის რეწვა და სხვა. როგორც ვიცით შენგენის ზონაში გაუქმებულია საპასპორტო კონტროლი, ასევე 1999 წელს წევრი ქვეყნები შეთანხმდნენ, რომ საჭირო იყო ერთიანი ვალუტის შემოღება - ევრო, რომელიც ძალაში 2002 წლის დასაწყისში შევიდა. აღსანიშნავია, ევროზონაში მხოლოდ 19 ქვეყანაა გაერთიანებული, რაც გულისხმობს იმას, რომ ამ ქვეყნების ვალუტა ევროა. ევროკავშირს აქვს თავისი ინსტიტუტები, რითაც იგი სხვა ტრადიციული საერთაშორისო ორგანიზაციებისგან განსხვავდება, მისი ინსტიტუციური სტრუქტურა, შეიძლება ითქვას, უნიკალურია. მათ შექმნილი აქვთ ერთი მეორისგან დამოუკიდებელი ინსტიტუტები, რომლებიც ავსებენ ერთმანეთს და ყოველ მათგანს თავისი როლი აკისრია ამა თუ იმ საკითხის გადაწვეტილების მიღების პროცესში. ასეთებია: ევროკავშირის საბჭო, ევროპის პარლამენტი, ევროკომისია, ევროპულ თანამეგობრობათა სასამართლო, ევროპის აუდიტორთა სასამართლო, ევროპის საფინანსო ორგანიზაციები, ევროპის ცენტრალური ბანკი, ევროპის საინვესტიციო ბანკი და სხვა. აღნიშნული ინსტიტუტები ფუნქციონირებენ სხვადასხვა ქვეყნებსა და ქალაქებში. მაგალითად: ბელგიაში, კერძოდ ბრიუსელში, საფრანგეთში *(სტრასბურგი),* ლუქსენბურგში, გერმანიაში (მაინის ფრანკფურტი) და სხვა. ზოგადად ცნობილია, რომ ევროკავშირს პოლიტიკური ცენტრი არ გააჩნია, მაგრამ მის ერთგვარ დედაქალაქად ბრიუსელს მიიჩნევენ.

რაც შეეხება იმ საკითხს, რომ უკრაინა ევროპის კონტინენტის ქვეყანას წარმოადგენს, რომლის ტერიტორიაზეც რუსეთის ფედერაციას კონვენციური ომი აქვს გაჩაღებული, რა თქმა უნდა, ევროკავშირისთვის აღნიშნული საკითხი დიდ პრობლემას წარმოადგენს. როგორც ცნობილია, ევროკავშირის ქვეყნები უკრაინას ყოველდღიურ რეჟიმში ეხმარებიან და ამ ომში ერთ-ერთ სერიოზულ აქტორს ევროკავშირიც წარმოადგენს. იმის გათვალისწინებით, რომ საომარი მოქმედებები სწორედ ამ ორგანიზაციის საზღვრებთან მიმდინარეობს, ასევე იმისაც თუ რეალურად შევხედავთ, გარდა უსაფრთხოებისა, უკრაინიდან ევროკავშირის წევრ სახელმწიფოებში ლტოლვილთა საკმაოდ დიდი რაოდენობის გადასვლის გარდა, მთავარი საფრთხე და რისკები ეკონომიკური ხასიათისაა. ევროკავშირმა დაძლია ერთგვარი *„ტრადიციული ყოყმანის ჰოლიტიკა“* და საკმაოდ სერიოზული სანქციები დაუწესა რუსეთს. თუმცა, როგორც აღმოჩნდა, საკმარისი არ არის სამხედრო აგრესიის შესაჩერებლად. რუსეთი აღნიშნულ ქმედებას მორალურად, მეტ-ნაკლებად

მომზადებული შეხვდა. გარდა ამისა, მთავარი ფაქტორი, რაც რუსეთმაც და ევროკავშირმაც იციან, ენერგომატარებლებია: ევროპა არ აღმოჩნდა მზად რუსეთის ენერგოდამოკიდებულებისგან გასათავისუფლებლად, მეტიც, ვერსალის შეხვედრაზე პირდაპირ ითქვა, რომ ამისათვის მათ მინიმუმ 5 წელი დასჭირდებოდათ. ამ რეალობამ ვლადიმერ პუტინს ახალი ძალა შთაბერა და ამჟამად რუსული რუბლის გამყარებაზე დაიწყო ფიქრი, საუბარია გაზისა და ნავთობის საფასურის რუბლით გადახდაზე, რაზეც ყველასგან უარყოფითი პასუხი მიიღო, ხელშეკრულებაში არარსებული პუნქტის გამო. თუმცა მთლიანობაში რუსული გაზისა და ნავთობის ექსპორტი ევროპაში კვლავ გრძელდება და რუსეთის ბიუჯეტი დღესაც მილიარდობით ევროთი ივსება. რაც შეეხება ევროკავშირის უსაფრთხოებას და თავდაცვის სისტემის გაძლიერებას, მათ შორის სწრაფი რეაგირების ძალების ჩამოყალიბებას, რომელზეც აგერ უკვე ათეული წლებია საუბარი მიდის, ჯერ-ჯერობით საშველი არ დაადგა. ამის მიზეზი მარტივია - ევროკავშირის წევრ ქვეყნებს, რომელთა უმეტესობა ნატოს წევრიცაა, ნამდვილად არა აქვთ სურვილი, ორი სამხედრო ბიუჯეტი და ორმაგი სამხედრო ხარჯი გაიღონ. ასევე კარგად ესმით, თუ სამხედრო ამბიციები აშშ-ის სამხედრო პოტენციალის მხრიდან არ იქნება უზრუნველყოფილი და მხარდაჭერილი, რეალურ უსაფრთხოებაზე და თავდაცვაზე ლაპარაკი ზედმეტია. ეს ერთგვარი ფუფუნება კი, როგორც ნატოს წევრებს, ისედაც აქვთ. მაშ, რაში სჭირდებათ ახალი ველოსიპედის გამოგონება?! გასაგებია, რომ ევროკავშირი კვლავ გმობს რუსეთის ქმედებებს უკრაინაში, სანქციებს უწესებს, მაგრამ ზემოთ აღნიშნული მიზეზების გამო, რუსეთის წინააღმდეგ სრული გალაშქრება მაინც არ და ვერ გამოსდის.

მიუხედავად იმისა, რომ დიდი ბრიტანეთი გავიდა ევროკავშირიდან, მაინც მოგვიწევს, იგი განვიხილოთ ამ კონტექსტში და გავაანალიზოთ გაერთიანებული სამეფოს პოზიციები და მდგომარეობა. თუ კი ვინმემ ამ ომის დროს პრინციპული და შეუპოვარი პოზიცია დაიკავა, სწორედ ეს ქვეყანა და მისი ლიდერი, იმ დროისთვის პრემიერ-მინისტრი ბორის ჯონსონი იყო. ეს ქვეყანა შეიარაღებით და ტექნიკით ეხმარება უკრაინას და ომის დასრულების შემდეგ რუსეთის მიმართ სანქციების გაგრძელების ინიციატივითაც გამოდის. ცოტა, ძნელი წარმოსადგენია, იქნებოდა თუ არა დიდი ბრიტანეთი ასეთი პრინციპული, ისევ ევროკავშირის წევრად რომ დარჩენილიყო. ამ საკითხში შეიძლება დიდი როლი მის უდიდებულესობა

დედოფალს ჰქონდეს. დიდი ბრიტანეთს, სიძლიერის საწინდარი, დემოკრატის ხარისხი, მდგრადი ეკონომიკა, ამერიკის შეერთებულ შტატებთან განსაკუთრებული ურთიერთობა, ნატოს გარკვეულწილად ლიდერობა და ბირთვული სახელმწიფოს იმიჯიც ეხმარება. მათ ძალიან კარგად ესმით, ნატოს უსაფრთხოებისათვის უკრაინასთან ყველაზე ახლოს მყოფი პოლონეთისა და ბალტიისპირეთის თავდაცვა რამდენად მნიშვნელოვანია, შესაბამისად, უკრაინაში მიმდინარე საომარი მოქმედებების მიმართ გულგრილები ვერ დარჩებოდნენ. ისევე. როგორც საფრანგეთი, რომელიც ევროკავშირის ერთ-ერთ ყველაზე მნიშვნელოვან ქვეყანას წარმოადგენს. თუმცა იგი, შეიძლება ითქვას, განსაკუთრებულად არ გამოირჩევა იმ პოზიციებიდან, რაც ევროპულ ქვეყნებს გააჩნიათ. დიახ, ის შეუერთდა სანქციების დიდ ნაწილს, რომელიც რუსეთის წინააღმდეგ დაწესდა, თუმცა ვერ ვიტყოდით, რომ ამ სანქციებით მან გადამწყვეტი დარტყმა მიაყენა რუსეთს. მეტიც, ემანუელ მაკრონის პოზიცია, ხშირად უფრო გაერო-ს უშიშროების მუდმივი წევრის პოზიციას ჰგავს, ვიდრე ევროკავშირის თავმჯდომარე ქვეყნისას. სამართლიანობა ითხოვს, აღვნიშნოთ, რომ პრეზიდენტ მაკრონს ჰქონდა შესაძლებლობა, ომამდეც და ომის პერიოდშიც პუტინთან როგორც პირადი შეხვედრის, ასევე სატელეფონო საუბრების, მაგრამ ამგვარმა დიპლომატიურმა ნაბიჯებმა არსებითი შედეგები ვერ მოიტანა. სიხისტე და კატეგორიულობა, არის ის, რაც ზოგადად დღევანდელ ევროპელ ლიდერებს აკლიათ. რა თქმა უნდა, საფრანგეთი ემხრობა, რუსეთის მიერ ცეცხლის შეწყვეტასა და ჯარის სრულად გაყვანას უკრაინის ტერიტორიებიდან, მაგრამ ამის გაკეთება მას მხოლოდ დიპლომატიის მეშვეობით წარმოუდგენია. ემანუელ მაკრონის განცხადება, რომ პუტინის მისამართით სიტყვა *,,ჯალათს''* არ გამოიყენებდა, სავარაუდოდ ეჭვს აჩენს, რომ საფრანგეთი იქნება ერთ-ერთი პირველი ქვეყანა, ვინც ომის შემდგომ რუსეთთან ურთიერთობების ნორმალიზაციისთვის გადადგამს ნაბიჯებს. ცხადია, ყველა ლიდერი თავისი ქვეყნის უსაფრთხოებასა და ეკონომიკურ სტაბილურობაზე ფიქრობს, რაც გასაკვირი არ არის, მაგრამ რამდენად დადებითად აღიქვამს საფრანგეთის მოსახლეობა მაკრონის მოღვაწეობას რუსეთ-უკრაინის ომის პერიოდში, ეს მომავალ არჩევნებში გამოჩნდება.

აქვე მნიშვნელოვანი და საინტერესოა ერთ-ერთი ძლიერი ქვეყნის - გერმანიის პოლიტიკური ნება. ისტორიას ჩაბარდა გამორჩეული ლიდერის, ანგელა მერკელის დრო, ახალმა კანცლერმა თითქოს მემკვიდროებით გააგრძელა რუსეთის

არგაღიზიანების პოლიტიკა. პირადად ჩავიდა რუსეთში, და დაუფარავად თქვა ის, რაც ყველამ იცოდა, მაგრამ ხმამაღლა არავინ ამბობდა - უკრაინა არ და ვერ გახდება ნატოს წევრიო. წესით და რიგით, ვლადიმერ პუტინს, *„წერილობითი გარანტია“* უნდა მოეთხოვა, მაგრამ როგორც ჩანს, მისთვის ესეც არ იქნებოდა საკმარისი. ომი დაიწყო და გერმანიამ ამჯერად *(თუ ბრიტანეთს არ ჩავთვლით)* ევროკავშირისა და ნატოს წევრი ქვეყნებიდან ყველაზე მეტი სამხედრო ხასიათის მხარდაჭერა აღმოუჩინა უკრაინას, არც სანქციების დაწესებაში დაუწყია დიდი ყოყმანი. თუმცა მას არ გადაუკვეთავს ის წითელი ხაზები, რომელსაც ნატო-რუსეთის დაპირისპირება შეიძლებოდა გამოეწვია.

რუსეთისგან ენერგოდამოუკიდებლობის მოპოვება ამ დროისთვის არც ევროკავშირის და არც ამერიკის შეერთებული შტატების მხრიდან ჩანს, მაგრამ როგორც უკვე აღვნიშნეთ, ვერსალის სასახლეში შეხვედრისას განიხილეს აღნიშნული საკითხი და ითქვა, რომ 2027 წლისთვის იქნება ამის შესაძლებლობა. ცხადია, ეს საკითხი გერმანიისთვის სასიცოცხლოდ მნიშვნელოვან საგანს წარმოადგენს, მაგრამ მარტივად გადსატანი არ იქნება რუსი ეროვნების იაფი მუშახელის საკმაოდ დიდი რაოდენობის დაკარგვა შიდა ბაზარზე. რაც შეეხება რუსეთის უზარმაზარ ბაზარს, გერმანიის მიერ სანქციების გამო *„ნებაყოფლობით“* გასვლა, სავარუდოდ *„იძულებითი“* დაბრუნებით დასრულდება. გარდა ამისა, გერმანიას ყველაზე მეტად ესმის მშვიდობის ფასი, სხვა ბევრი მიზეზიც არსებობს იმისა, რომ საფრანგეთის შემდგომ ისიც შეეცდება, ომის დასრულების შემდეგ რუსეთთან ურთიერთობების ნორმალიზაციას შეუწყოს ხელი.

ვარშავის პაქტის დაშლის შემდეგ, თუ ვინმემ მოახერხა სწრაფად გონს მოსვლა თავისი ქვეყნის უსაფრთხოებისა და ეკონომიკური მდგრადობის გასაძლიერებლად, ერთ-ერთი პოლონეთი გახლდათ. შესაბამისად, მისი ნატოში და ევროკავშირში წევრობაც ამით იყო განპირობებული. პოლონეთისთვის გეოგრაფიული ფაქტორი და მოსაზღვრე სახელმწიფოებთან ურთიერთობა სერიოზული მნიშვნელობისაა: დასავლეთით გერმანია, სამხრეთ დასავლეთით - ჩეხეთი, ჩრდილოეთის ერთ მონაკვეთზე - ლიეტუვა, აქ არც ეკონომიკური და არც საომარი საფრთხე, ცხადია, არ გამოიკვეთება. სულ სხვა სურათია აღმოსავლეთ საზღვარზე, სადაც მეზობლად ბელორუსი და უკრაინაა. ასევე, არ უნდა დაგვავიწყდეს რუსეთის კალინინგრადის ოლქი, რომელიც პოლონეთის ჩრდილოეთით საკმაოდ სახიფათოდ გამოიყურება

(ბოლო დროს რუსეთმა გერმანია-პოლონეთის, ზოგადად ევროპის შესაშინებლად სწორედ კალინინგრადში გაზარდა სამხედრო ტექნიკის რაოდენობა). რუსეთის მიერ უკრაინაში შეჭრა, პოლონეთისთვის, მიუხედავად ნატოს და ევრიკავშირის წევრობისა, პირდაპირ საფრთხის მომასწავებელი გახდა. ამიტომაც გასაკვირი არ იყო რუსეთისთვის სანქციების დაწესება, ასევე უკრაინისთვის შეიარაღებით დახმარება.

თუმცა აბსოლუტურად გაუგებარი იყო ე.წ. ***MIG-29-ების*** საკითხი: უკრაინის ლიდერების მოულოდნელი *„აღმოჩენა,“* რომ მრავალფუნქციური გამანადგურებლის საჭიროების შესახებ და პოლონეთის ჯერ გადაცემაზე თანხმობა, შემდეგ ამერიკელებისთვის შეთავაზება - *„მე თქვენს ბაზაზე გადმოვიყვან და თქვენ გადაეცით უკრაინელებსო,“* ეს უცნაური თუ პოლიტიკური მანევრით გაჯერებული ისტორია საბოლოდ უკრაინელებისთვის ამ თვითმფრინავების არგადაცემით დასრულდა. არ ვიცით, ვინ გადაწყვიტა, ამერიკელებმა თუ პოლონელებმა ***MIG-29-ებით*** რუსეთის არგაღიზიანება, თუმცა უკრაინამ, რომ ვერ მიიღო, რასაც ითხოვდა, ფაქტია. როგორც არ უნდა დასრულდეს ომი, პოლონეთი რჩება, ცალკე ამერიკის შეერთებული შტატების და ცალკე ევროპის საიმედო მოკავშირედ და ფარად, მით უფრო, ნატოს და ევროკავშირის აღმოსავლეთით გაფართოებას ნამდვილად არ უნდა ველოდოთ. პოლონეთს ასევე მოუწევს ომის შემდგომ უკრაინის ინფრასტრუქტურის, განსაკუთრებით საცხოვრებელი სახლების აშენებაში დიდი წვლილის შეტანა. ცხადია, იმის გათვალისწინებით, რომ ლტოლვილთა ყველაზე დიდი რაოდენობა სწორედ პოლონეთშია. მათი უკრაინაში კვლავ დაბრუნება საჭირბოროტო გახდება. რაც შეეხება უკრაინის ნეიტრალიტეტის შემთხვევაში უსაფრთხოების გარანტორად გამოსვლას, სავარაუდოდ, ეს საკითხი ცალკე ალიანსთან და ცალკე ამერიკელებთან იქნება შეთანხმების საგანი..

მართალია, ევროკავშირზე და მის წევრ ამა თუ იმ ქვეყნებზე ვსაუბრობთ და მათ პოლიტიკურ-სამხედრო პოზიციებსა და მდგომარეობაზე, მათ შორის კიბერ მიმართულებითაც განვიხილავთ, მაგრამ იქიდან გამომდინარე, რომ კონვენციური ომი მიმდინარეობს ევროპის ტერიტორიაზე, აუცილებელია აქვე ყურადღება გავამახვილოთ თვით უკრაინაზეც. როგორც არ უნდა მივუდგეთ ომის

მიმდინარეობას, შეცდომებსა და სხვადასხვა გადადგმულ ან არგადადგმულ ნაბიჯებს, ერთმნიშვნელოვნად იგი თავისი ქვეყნის ტერიტორიულ მთლიანობასა და სუვერენიტეტს იცავს. რუსეთი კი, რაც არ უნდა სპეცოპერაციას არქმევდეს თავის სამხედრო მოქმედებებს, აგრესორ ქვეყნად გვევლინება, რომელიც უცხო ქვეყნის ტერიტორიაზე შეიჭრა. მიუხედავად იმისა, რომ უკრაინას მოუწია მთელი რიგი ტერიტორიების დათმობა, რასაც უამრავი მშვიდობიანი მოსახლეობის დაღუპვა და ქალაქებისა თუ ინფრასტრუქტურის განადგურება მოჰყვა, ამ ქვეყანამ მაინც შეძლო სახმელეთო ჯარების შეტევების მოგერიება, მთელ რიგ რაიონებში ზღუდეების შენარჩუნება და მოწინააღმდეგის ცოცხალი ძალისა თუ საბრძოლო ტექნიკის განადგურება. მისმა შეუპოვარმა თავდაცვამ რუსეთი იძულებული გახადა, მთელ რიგ ადგილებში უკან დაეხია და მოწინააღმდეგისათვის უკვე საჰაერო, სარაკეტო, თუ საარტილერიო დაბომბვებით ეპასუხა. ცხადია, რომ არა სერიოზული თანამედროვე შეიარაღებითა და ტექნიკით დახმარება, რასაც უკრაინა დღესაც იღებს დასავლეთიდან, მას ამ მიზნის მიღწევა ძალიან გაუჭირდებოდა. მთავარი კითხვები კი მაინც რჩება: როდის შეწყდება ცეცხლი და საომარი მოქმედებები? ეს დამოკიდებულია იმაზე, როდის ჩათვლის უკრაინის პოლიტიკური ისტებლიშმენტი, რომ შეჩერება შეიძლება. თუმცა ეს ყველაფერი მარტო მათზე არ არის დამოკიდებული, არამედ, დასავლეთზეც და რუსეთზეც. რუსეთს შესაძლოა დღესვე უნდოდეს შეჩერება, უბრალოდ კარგ მომენტს ელოდება, რათა თავი გამარჯვებულად გამოაცხადოს. გამარჯვებულად თუ არა, განცხადებით მაინც, რომ - *„აგრესორს სათანადო პასუხი გაეცა“* და *„ომი ჯერ არ დასრულებულა“* - წესით უკრაინის ინტერესებშიც უნდა იყოს. ნატომ უკრაინის გაწევრიანების შესახებ უარის თქმით და ასევე უკრაინამ ნატოზე უარის თქმით, პოლიტიკურად ერთი ფაზა სერიოზულად წააგო (ერთმნიშვნელოვნად ამ საკითხში რუსეთმა მოიგო), თუმცა რა სახის ნეიტრალიტეტზე შედგება საუბარი და რამდენად სერიოზულად და მტკიცედ იქნებიან მისი უსაფრთხოების გარანტორები დასავლეთის ქვეყნები, ეს ცალკე საკითხია. ლუგანსკისა და დონბასის რესპუბლიკების დამოუკიდებლობის საკითხი, ანუ უკრაინიდან მათი გამოყოფა, უკრაინისთვის დიდი პრობლემაა, თუ მათ მოახერხეს ამ რეგიონებიდან რუსეთის განდევნა, ეს იდეალური, მაგრამ რთულად შესასრულებელი მისიაა. ამ სიტუაციაში ფართო ავტონომიის მინიჭება, შესაძლოა, უკრაინისთვისაც და რუსეთისთვისაც მისაღები იყოს. თუ ომი გაყინულ კონფლიქტად გამოცხადდება და სამშვიდობო კონტინგენტი ჩადგება, შეიძლება დროებითი

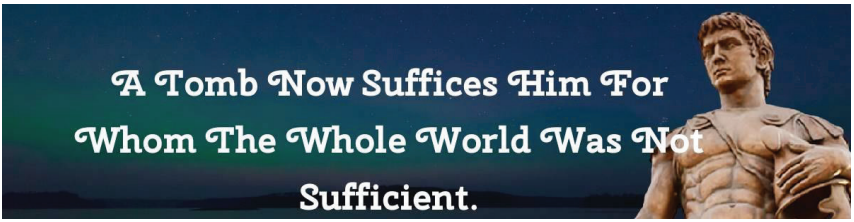
გამოსავალიც აღმოჩნდეს, მაგრამ რთულად სავარაუდოა. მნიშვნელოვან საგანს წარმოადგენს ყირიმი, რისი დათმობაც უკრაინას არაფრით არ შეუძლია (ოფიციალურად მაინც, თორემ აგერ, უკვე 9 წელია, დასავლეთი მხოლოდ შეშფოთება-აღშფოთებით შემოიფარგლება). აი, ყირიმი მარტივად შესაძლოა გადავიდეს გაყინულ საკითხთა ნუსხაში. იგი შეიძლება გაიცვალოს უფრო მნიშვნელოვან და სერიოზულ საკითხზე, რაც თითქმის წარმოუდგენელია, მაგრამ თეორიულად ყველაფერია შესაძლებელი. უკრაინამ ევროკავშირის კანდიდატის სტატუსი მიიღო და ასევე ევროკავშირის კითხვარი, რაც უნდა გამოსწორდეს ამ ქვეყანაში მიუხედავად იმისა, რომ კონვენციური ომი მიმდინარეობს მათ ტერიტორიაზე, ორი აზრი არ არსებობს, ეს მნიშვნილოვანი პოლიტიკური ნაბიჯია უკრაინისათვის, მაგრამ აქვე ისიც უნდა გავიაზროთ, რომ კანდიდატობა, რომლის დადებითი პოლიტიკური ნებაც დასავლეთში შეიძლება არსებობდეს, ჯერ კიდევ არ ნიშნავს წევრობას.

უკრაინა, მიუხედავად მისი პოლიტიკური ისტებლიშმენტის მიერ დაშვებული გარკვეული შეცდომებისა, არ შეჭრილა სხვა სახელმწიფოში და თავის სუვერენიტეტს იცავს. მას აქვს სრული უფლება, ბოლომდე მოითხოვოს თავისი ტერიტორიის სრული გაწმენდა აგრესორისგან, აქვს საერთაშორისო მხარდაჭერაც, მათ შორის თანამედროვე შეიარაღებითაც და ტექნიკითაც. უკრაინა დღეს იგებს საინფორმაციო ომს *(კიბერსივრცეშიც აქტიური ომი აქვს გაჩაღებული, რაც განხილული გვაქვს ამ სახელმძღვანელოში)* რუსეთის წინააღმდეგ. ეს კი წარმატებისთვის საკმაოდ სერიოზული პირობაა. ახლა მთავარია, რამდენად ეყოფა უკრაინის პოლიტიკურ ხელმძღვანელობას სიმტკიცე, ბოლომდე გაუძლოს და რამდენად შეუპოვარი იქნება დასავლეთიც რუსეთთან ბრძოლაში. მათ ხომ რეალურად რუსეთის პრეზიდენტი დამნაშავედ გამოაცხადეს, დამნაშავეს კი დასჯა სჭირდება. თუ რაღაც ეტაპზე გადაწყდა, რომ ომის შეჩერება უფრო მომგებიანი იქნება, მაშინ ჩნდება სავსებით ლეგიტიმური კითხვა, რისთვის მოხდა ამდენი მსხვერპლი, თუ პოლიტიკოსები მაინც მოილაპარაკებენ და რაღაცებს დათმობენ, იქნებ ეს ყოველივე ომამდეც შესაძლებელი ყოფილიყო?!

<u>გამოვყოთ ის შედეგები, რაც დღეს ცნობილია და ჩვენს თვალწინ ხდება:</u>

უამრავი დაღუპული და სხვა ქვეყნებში ლტოლვილებად ქცეული ადამიანები, დანგრეული ქალაქები და ინფრასტრუქტურა, რომლის აღდგენასაც წლებთან ერთად

უზარმაზარი ფინანსური რესურსი დასჭირდება. ფინანსური რესურსების გარდა აუცილებლად მოხდება, ყველა სახის დახმარების (მათ შორის შეიარაღების) სერიოზული კონტროლი დასავლეთის, კერძოდ აშშ-ისა და ბრიტანეთის მხრიდან. პოლიტიკურ ხელმძღვანელობას ბევრ კითხვაზე მოუწევს პასუხის გაცემა, მხარდაჭერა, რაც მათ დღეს გააჩნიათ, საომარი სიტუაციითაა გამოწვეული, თუ სრულ გამარჯვებას მიაღწიეს, ითამაშებს ფორმულა - *„გამარჯვებულებს არ ასამართლებენ“*. კითხვები კი ბევრია - მათ შორის ისეთი, თუ რატომ ცდილობდნენ რუსეთთან ომის პარალელურად საქართველოსთან ურთიერთობის გაფუჭებას, რატომ ითხოვდნენ საქართველოში ხელისუფლების შეცვლას, ან რუსეთთან მეორე ფრონტის გახსნას, რატომ გაიწვიეს ელჩი, როცა ბელორუსიაში, ქვეყანაში, რომლის ტერიტორიდან რუსეთის ჯარები უკრაინაში შეიჭრა, ელჩი არ გაუწვევიათ. რით იყო ეს გამოწვეული, ვიწრო პოლიტიკურ-ფინანსური ინტერესებით თუ უფრო დიდი სცენარით და გეგმის მიხედვით მოქმედებდნენ? როგორც უკვე აღვნიშნეთ, უკრაინა ნატოს წევრი ვერ გახდა, რასაც ასე ეწინააღმდეგებოდა რუსეთი, სხვა სახის უსაფრთხოებისა და თავდაცვის გარანტირებული მოდელი, ჯერ-ჯერობით ბუნდოვანია. იმედია, მეტი სიცხადე ამ საკითხს მეტ დამაჯერებლობას მისცემს. ევროკავშირის მხოლოდ კანდიდატობა და მხოლოდ იმის დაფიქსირება, რომ რუსეთი აგრესორია, შესაძლოა, საკმარისი არ აღმოჩნდეს ან უბრალოდ ვერ გაიგოს უკრაინის მოსახლეობამ, რომელმაც უზარმაზარი მსხვერპლი საკუთარ ოჯახებსა და სახლებზე გადაიტანა. ეს კი იმას ნიშნავს, რომ აუცილებლად დადგება პოლიტიკური ხელმძღვანელობის ცვლილების საკითხი. ახალი ძალა უკრაინის ხელისუფლებაში რა კონფიგურაციით მოვა, იმედია, ამას მხოლოდ უკრაინა გადაწყვეტს.



ჩვენი აზრით, არც ერთ პოლიტიკური თუ გეოპოლიტიკური ინტერესების გამარჯვებისთვის არ ღირს ომის გამართლება, მით უმეტეს, გახანგრძლივება. ომს, რომელსაც მოაქვს უდანაშაულო ადამიანების მსხვერპლი, ქალაქების ნგრევა,

ინფრასტრუქტურის განადგურება, ეროვნებათაშორის შუღლი და შედეგად - ისტორიულ მტრებად ჩამოყალიბება. ეს, ყველაფრი ისევ და ისევ პოლიტიკურ აქტორებზე და მათ ნებაზეა დამოკიდებული. კარგი იქნება, თუ ეყოფათ პოლიტიკური ვაჟკაცობა და ომს შეაჩერებენ. დიდ თუ პატარა, აქტიურ თუ პასიურ პოლიტიკურ აქტორებს უბრალოდ, დიდი ***ალექსანდრე მაკედონელის*** საფლავის ეპიტაფიას შევახსენებდით: *„ეს საფლავი საკმარისი აღმოჩნდა მისთვის, ვისაც არ ჰყოფნიდა მთელი სამყარო“.*[26] ყველანი მოკვდავები ვართ, თუ ერთმანეთს გავუფრთხილდებით და შევძლებთ მშვიდობიან თანაარსებობას, უფალიც შეგვეწევა.

ევროკავშირის კიბერშესაძლებლობები

ევროკავშირი, მისი წევრი სახელმწიფოები კიბერუსაფრთოხებისა და ინფორმაციული უსაფრთხოების მიმართულებით ფინანსებს დღითი-დღე ზრდიან. ევროკავშირი წევრი ქვეყნების გარდა, არაწევრ პარტნიორებთანაც აქტიურად თანამშრომლობს და ეხმარება, იგი ეკონომიკური და პოლიტიკური გაერთიანების მეგა ორგანიზაციას წარმოადგენს. თუმცა ნატოსთან თანამშრომლობით უფრო მეტად გამოიმუშავა სხვადასხვა სტანდარტებისა და პროგრამების განხორციელების უნარი. ევრიკავშირი ჰიბრიდული ომების მიმართულებითაც აქტიურად იბრძვის - დეზინფორმაციის გავრცელების წინააღმდეგ სამოქმედო გეგმაც კი წარადგინეს, რომლის პრეამბულაში ნათქვამია: ჩვენ უკვე ვიხილეთ არჩევნებსა და რეფერენდუმებში ჩარევის არაერთი შემთხვევა, სადაც ხშირად რუსეთის ხელი ურევია. აღნიშნული სამოქმედო გეგმის თანახმად, გაიზარდა ევროკავშირის საგარეო პოლიტიკური უწყების ბიუჯეტი - კერძოდ, სტრატეგიულ კომუნიკაციებზე იხარჯება 5 მილიონი ევრო. დაგეგმილია იმ უწყების თანამშრომელთა რიცხვის გაზრდა, რომელსაც დეზინფორმაციის გამოვლენა ევალება.

[26] *fabbyquotes, "16 Greatest Alexander the Great Quotes", p. 1, https://www.fabbyquotes.com/16-greatest-alexander-the-great-quotes/*

"ევროკავშირის კიბერუსაფრთხოების ბაზარი შეფასებულია 20,1 მილიარდ ევროდ, რაც ნამდვილად აკმაყოფილებს დადგენილ ნორმებს".[27] თუმცა სიტუაციით სარგებლობენ რა კიბერჯაშუშები, ბოროტი ჰაკერები, ისინი ქმნიან საფრთხეს სხვადასხვა თაღლითური საშუალებებით, ცდილობენ მსოფლიო ეკონომიკის ნგრევას. მსხვილი ევროპული კომპანიები უფრო მეტად შეშფოთებულნი არიან კიბერუსაფრთხოებასთან დაკავშირებული რისკებით, ვიდრე დანარჩენ მსოფლიოში. უსაფრთხოების შეფერხება ანელებს ზოგიერთ ტექნოლოგიას, რაც ხელს უშლის ევროკავშირს, მაქსიმალურად გამოიყენოს ინოვაციები ეკონომიკური ეფექტურობის ასამაღლებლად. ევროკავშირის კიბერუსაფრთხოების სტრატეგია, დირექტივები და მონაცემთა დაცვის ზოგადი რეგულაციები დიდ როლს ასრულებს ამ ორგანიზაციის ეკონომიკურ პოლიტიკაში. კიბერუსაფრთხოება, როგორც ეკონომიკური საშუალება, იძლევა ერთიანი ციფრული ბაზრის შექმნის შესაძლებლობას, თუ კიბერუსაფრთხოების რისკები მინიმუმამდე იქნება დაყვანილი.

საზოგადოების დამოკიდებულება წლების განმავლობაში ინტერნეტთან მიმართებაში იზრდება. ასევე იზრდება კიბერსაფრთხეების რიცხვი ახალი, უფრო დახვეწილი ფორმებით. *"ექსპერტების შეფასებით 2030 წლისთვის ინტერნეტში იქნება 125 მილიარდი მოწყობილობა ჩართული, აქედან 90 პროცენტი, 6 წელზე უფროსი ასაკის ადამიანი იქნება".*[28]

ჟან ლოდ იუნკერი

მსოფლიოში აქტიურად ვითარდებიან ქვეყნები კიბერშესაძლებლობების თვალსაზრისით, 21-ე საუკუნეში კიბერიარაღი გეოპოლიტიკური კეთილდღეობისა და მდგომარეობის განმსაზღვრელად იქცა. *"დღეს კიბერდანაშაულის გლობალურ*

[27] *Digital Editor, World Economic Forum, "New European Union cybersecurity proposal takes aim at cybercrime", p. 1, 2022. https://www.weforum.org/agenda/2022/09/new-european-union-cybersecurity-proposal-takes-aim-at-cybercrimes/*

[28] *European Parliament, "Cyber: How big is the threat?", 2019. P. 1. https://www.europarl.europa.eu*

ღირებულებას წარმოადგენს 530 მილიარდი ევრო".[29] ყოველდღიური შეტევები მზარდია, რაც იწვევს დიდ ფინანსურ ზარალს. მაშტაბური თავდასხმებისგან თავის დაცვა მთავრობების თავდაცვით მექანიზმებს აღემატება. 2017 წელს ევროკავშირის პრეზიდენტმა, **ჟან კლოდ იუნკერმა** განაცხადა*: "კიბერშეტევები უფრო მეტ საფრთხეს უქმნის დემოკრატიებსა და ეკონომიკას, ვიდრე იარაღი და ტანკი".*[30]

კიბერშეტევებმა შეიძლება ზიანი მიაყენოს არა მხოლოდ ევროკავშირის ეკონომიკას, არამედ მის დემოკრატიულ საფუძვლებს, რადგან კიბერსივრცე შეიძლება მრავალმხრივ იქნას გამოყენებული, მათ შორის, როგორიც არის დეზინფორმაცია, ეკონომიკური ზეწოლა და ასე შემდეგ. ჩვეულებრივი სამხედრო შეტევის დროსაც კიბერი შეიძლება იყოს ჰიბრიდული ოპერაციის ნაწილი, ციფრული სფეროდან რისკები შეიძლება შეექმნათ მთავრობებსა და პოლიტიკურ სისტემებს, შეეცადონ საზოგადოების დაყოფას და გააღვივონ ქვეყნის გარეთ თუ ქვეყნის შიგნით კონფლიქტი.

კიბერთავდახსმა, როგორც მნიშვნელოვანი საკითხი, მსოფლიო ეკონომიკური ფორუმის 2020 წლის გლობალური რისკების შესახებ შექმნილ დოკუმენტშიც გვხვდება - კიბერსივრციდან მომდინარე საფრთხეები ხუთ ძირითად ეკონომიკურ რისკებში გაიყვანეს. ერთ-ერთი ყველაზე ცნობილი გახლდათ ***"WannaCry"-ის*** *კიბერშეტევა, რომელიც 150 ქვეყანაში 300 000 კომპიუტერზე გავრცელდა. ასევე იყო შეორე -* ***"Petya"*** *და* ***"NotPetya"*** *კიბერთავდასხმები, რამაც გამოიწვია ასობით მილიონის ღირებულების ფინანსური ზარალი, სტრატეგიული სექტორებისა და კრიტიკული ინფრასტრუქტურის მოშლა, ასევე სახელმწიფოთაშორისი დაძაბულობა".*[31]

[29] *European Parliament, "Cyber: How big is the threat?", 2019. P. 1. https://www.europarl.europa.eu*
[30] *Europa Commission, "State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks", 2017. P. 1. https://ec.europa.eu*
[31] *World Economic Forum, "Wild Wide Web - Consequences of Digital Fragmentation", 2020. P. 1. https://reports.weforum.org*

ემანუელ მაკრონი

ხშირად ვისმენთ, რომ კიბერსაფრთხეების წინააღმდეგ გამკლავება ითხოვს კოლექტიურ და ფართო მასშტაბის მიდგომას. უკვე აღვნიშნეთ, როგორც საინფორმაციო ომის, ასევე კიბერომის მიმართულებით ნატო და ევროკავშირი აქტიურად თანამშრომლობენ, ნატო-მ კიბერომი უკვე ერთ-ერთ მთავარ ძირითად გამოწვევად განსაზღვრა და ყოველწლიურად უფრო მეტი თანხები იხარჯება ტექნოლოგიური მიღწევებისთვის, მაგრამ ამ მიმართულებით საყურადღებოა ახალი ინიციატივა, რომელიც 2018 წელს საფრანგეთის პრეზიდენტმა ***ემანუელ მაკრონმა*** გააჟღერა - ეს გახლავთ *„პარიზის მოწოდება ნდობისა და უსაფრთხოების შესახებ კიბერსივრცეში“*,[32] მართალია, აღნიშნული ინიციატივა იურიდიული საფუძველის გარეშეა, მაგრამ მოწოდება კიბერსივრცეში თანამშრომლობის შესახებ მაღალი დონის დეკლარაციაა, რომელსაც მხარი 64-მა ქვეყანამ დაუჭირა, მათ შორის სხვადასხვა საერთაშორისო არასამთავრობო ორგანიზაციებმა, უნივერსიტეტებმა და ასობით კერძო კომპანიამ.

აღსანიშნავია, რომ *“2014 წლიდან, საფრანგეთში **“Pacte Défense Cyber”-ის** ბიუჯეტი მოიცავდა 1 მილიარდ ევროს კიბერთავდაცვისთვის. 2016 წელს დიდმა ბრიტანეთმა კიბერუსაფრთხოების პროგრამის გასამყარებლად 1,9 მილიარდი გირვანქა სტერლინგი*

[32] *Ministère de l'Europe et des Affaires étrangères, "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace", 2018. P. 1. https://www.diplomatie.gouv.fr*

გამოყო".[33] *"2018 წელს ბრიუსელის სამიტზე მოკავშირეები შეთანხმდნენ ახალი კიბერსივრცის ოპერაციების ცენტრის შექმნაზე".*[34] საერთო გამოწვევების გათვალისწინებით, ნატო და ევროკავშირი აძლიერებენ თანამშრომლობას კიბერთავდაცვის სფეროში, განსაკუთრებით ინფორმაციის გაცვლაში. ტარდება ერთობლივი ტრენინგები და კვლევები.

თავდაცვითი ნორმების მიმართულებით არსებობს ***ტალინის სახელმძღვანელო,*** რომელიც ესტონეთმა ნატოსთან თანამშრომლობის საფუძველზე შეიმუშავა. აღნიშნული სახელმძღვანელო იხვეწება და ამ საკითხში ევროკავშირიც აქტიურად მონაწილეობს.

ევროკავშირის სტრატეგიაში ხაზგასმით არის აღნიშნული, რომ კიბერშეტევები დიდ საფრთხეს წარმოადგენს ევროკავშირის წევრი და არაწევრი ქვეყნებისთვის, იგი უნდა გახდეს მთავარი ***„მომავალი კიბერმოთამაშე"*** გლობალურ პოლიტიკაში, რომელიც ჩართული იქნება სრულყოფილად კიბერდიპლომატიაში და შეეცდება პარტნიორობის გაღრმავებას კიბერუსაფრთხოების მიმართულებით.

ევროკავშირისთვის კიბერუსაფრთხოება წარმოადგენს მცდელობებს სტაბილური ციფრული ევროპის შესაქმნელად. *"2020 წელს ევროკავშირმა და მისმა უმაღლესმა*

[33] *Pennetier M. France to invest 1 billion euros to update cyber defences, Media News Reuters, 2014, p 1.* https://www.reuters.com
[34] *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

წარმომადგენლებმა საგარეო საქმეთა უსაფრთხოების პოლიტიკის საკითხებში, წარმოადგინეს ***ევროკავშირის ახალი კიბერუსაფრთხოების სტრატეგია - "EU Cybersecurity Strategy".***[35] ეს დოკუმენტი თავისი შინაარსით ძალიან ამბიციურია, იგი მიზნად ისახავს უსაფრთხო, საიმედო ციფრული ინსტრუმენტებისა და კავშირის უზრუნველყოფას მთელ ევროპაში, რაც გულისხმობს ევროპის ციფრული ეკონომიკის გლობალურ ლიდერად გარდაქმნას. სასიცოცხლო სექტორები, როგორიცაა ელექტრო ენერგია, ტრანსპორტი, ჯანდაცვა, ფინანსები, ტელეკომუნიკაცია, უსაფრთხოება, თავდაცვა, დემოკრატიული პროცესები ყოველდღიურად ურთიერთდამოკიდებულნი ხდებიან ინფორმაციული სისტემების მეშვეობით. ამ ურთიერთდამოკიდებული მოწყობილობებისთვის ევროავშირმა დაიწყო სქემის შექმნა და ინვესტირება ისეთ საკითხებზე, როგორიცაა ხელოვნური ინტელექტი, დაშიფრვა და კვანტური გამოთვლა. მაინც რას წარმოადგენს ევროკავშირის კიბერუსაფრთხოების სტრატეგიის სტრუქტურა, რომელიც პირდაპირ კავშირშია ეკონომიკურ კეთილდღეობასთან?

ევროკავშირის ახალი კიბერუსაფრთხოების სტრატეგია დაყოფილია სამ ნაწილად:

"1. მდგრადობა, ტექნოლოგიური სუვერენიტეტი და ხელმძღვანელობა;

2. ოპერატიული შესაძლებლობების შექმნა, პრევენცია, შეკავება და რეაგირება.

3. გლობალური და ღია კიბერსივრცის წინსვლა".[36]

ევროკავშირის აზრით, როგორც კერძო, ისე საჯარო სექტორს უნდა ჰქონდეს არჩევანის საშუალება ყველაზე უსაფრთხო ინფრასტრუქტურასა და მომსახურებას შორის.

ევროკავშირს აქვს ***დირექტივა ქსელისა და საინფორმაციო სისტემების უსაფრთხოების შესახებ (NIS),*** რომელიც წარმოადგენს კიბერუსაფრთხოების ერთიან

[35] *European Commission, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient", 2020. P. 1. https://ec.europa.eu*
[36] *European Commission, "Jount Communication to the Eorupean Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade", 2020. P. 14. https://eur-lex.europa.eu*

ინტერნეტბაზას. დირექტივის საფუძველზე საჭიროა ყველა შესაბამისი სექტორის, მაგალითად, ენერგეტიკის, ტრანსპორტის, ჯანდაცვის, ფინანსური სექტორის კიბერტექნოლოგიების ამაღლება. ***NIS-ის*** დირექტივის რეფორმირება დაწყებულია, *"იგი ხელს შეუწყობს შიდა ბაზარზე არსებული შეუსაბამობების შემცირებასა და სტრატეგიულად მნიშვნელოვანი სექტორების სპეციფიკურ წესებს. ცნობილია, რომ კიბერტექნოლოგიური კონკურენციის მიმართულებით მნიშვნელოვან როლს შეასრულებენ **ინფორმაციის ანალიზისა და გაზიარების ცენტრები (ISACs) - კომპიუტერული უსაფრთხოების შემთხვევების რეაგირების ჯგუფი (CSIRT) და უსაფრთხოების ოპერაციების ცენტრები (SOC)**".*[37] ამ ცენტრების შექმნის საფუძველია საჯარო და კერძო სექტორის მიერ კიბერსაფრთხეების დაძლევა, რაც გულისმობს შესაბამისი ინფორმაციის გავრცელებას, რეალურ დროში ანომალიების იდენტიფიცირებას ან ჰაკერული, ვირუსული შეტევების გამოვლენას. *"ასეთი ცენტრების შექმნისა და მუშაობისათვის, ევროკავშირი მზად არის, დახარჯოს 300 მილიონი ევრო".*[38] ეს შექმნის კოლექტიურ ცოდნას და საუკეთესო პრაქტიკას კიბერსაფრთხეებთან ბრძოლაში. *"კომისია გეგმავს, რომ ევროკავშირის წევრ ქვეყნებთან ერთად იმუშაოს **ევროპისთვის უსაფრთხო კვანტური კომუნიკაციის ინფრასტრუქტურის შესაქმნელად (QCI)**, რომელიც უზრუნველყოფს სახელმწიფო ხელისუფლების კომუნიკაციების უსაფრთხოებას. **QCI** დაკომპლექტებული იქნება ბოჭკოვანი საკომუნიკაციო ქსელებით, ასევე დაკავშირებული სატელიტებით, რომლებიც მოიცავს ევროკავშირისა და მის გარეთ ტერიტორიებს. 2019 წლის მარტში კომისიამ დაიწყო მუშაობა **5G** ტექნოლოგიაზე და მომავალი თაობის მობილური ქსელების უსაფრთხოებაზე, ევროკავშირმა რეკომენდაცია გამოსცა **5G** ქსელების კიბერუსაფრთხოების შესახებ. რეკომენდაციას 2019 წლის ოქტომბერში მოჰყვა ევროკავშირის **5G** ქსელის კიბერუსაფრთხოების რისკების შეფასება და 2020 წლის იანვარში **5G (EU 5G Toolbox)** ქსელის კიბერუსაფრთხოების რისკის შემამცირებელი ზომების მიღება და შემსუბუქება. 2020 წლის ოქტომბერში ევროსაბჭომ მოუწოდა ევროკავშირის წევრ ქვეყნებს, სრულად გამოიყენონ **5G** კიბერუსაფრთხოების ინსტრუმენტები, ასევე გამოიყენონ შესაბამისი შეზღუდვები მაღალი რისკის*

[37] *NIS Cooperation group, "EU coordinated risk assessment of the cybersecurity of 5G networks", 2019. PP. 4-12. report__eu_risk_assessment_E4583F51-F351-6B15-A1317185D4FB353A_62132.pdf*

[38] *NIS Cooperation group, "EU coordinated risk assessment of the cybersecurity of 5G networks", 2019. PP. 4-12. report__eu_risk_assessment_E4583F51-F351-6B15-A1317185D4FB353A_62132.pdf*

მომწოდებლებზე".[39] აღსანიშნავია, რომ 2020 წლის დეკემბერში ევროკავშირმა გამოაქვეყნა ანგარიში ***„ევროკავშირის რეკომენდაციების გავლენის შესახებ",*** სადაც ნაჩვენებია, თუ როგორი მნიშვნელოვანი პროგრესი განიცადეს ევროკავშირის წევრმა ქვეყნებმა ***EU 5G-ის*** დანერგვასა და განხორციელებაში, მაგრამ გარკვეული ცვლილებებით და რიგ შემთხვევაში დარჩენილი ხარვეზებით. ევროკავშირმა წევრ სახელმწიფოებს მოუწოდა, განაგრძონ **5G** ძირითადი რეკომენდაციების შესრულება. ამრიგად, ნათელია, ევროკავშირი კიბერუსაფრთხოებისა და კიბერტექნოლოგიების მიმართულებით რამდენიმე ფრონტზე იბრძვის, იგი ცდილობს, გაზარდოს კიბერგამძლეობა, ებრძოლოს კიბერდანაშაულს, გაზარდოს კიბერდიპლომატია, გააძლიეროს კიბერთავდაცვითი უნარები, გაზარდოს კვლევები და დანერგოს ინოვაციური ტექნოლოგიები, დაიცვას კრიტიკული ინფრასტრუქტურა.

NCSI
national cyber security index

ეროვნული კიბერუსაფრთხოების ინდექსის (NCSI) ათეული ასე გამოიყურება: *„საბერძნეთი, ლიეტუვა, ბელგია, ესტონეთი, ჩეხეთი, გერმანია, რუმინეთი, პორტუგალია, ესპანეთი, პოლონეთი".*[40] ***(იხილეთ ცხრილი 3.)***

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Greece	96.10	64.47	31.63
2.	Lithuania	93.51	68.61	24.90
3.	Belgium	93.51	75.34	18.17
4.	Estonia	93.51	76.51	17.00
5.	Czech Republic	92.21	69.86	22.35
6.	Germany	90.91	81.43	9.48
7.	Romania	89.61	60.67	28.94
8.	Portugal	89.61	68.25	21.36
9.	Spain	88.31	73.92	14.39
10.	Poland	87.01	66.61	20.40

[39] *NIS Cooperation group, "EU coordinated risk assessment of the cybersecurity of 5G networks", 2019. PP. 4-12. report__eu_risk_assessment_E4583F51-F351-6B15-A1317185D4FB353A_62132.pdf*
[40] *National Cyber Security Index, p.1, 2022. https://ncsi.ega.ee/ncsi-index/*

ცხრილი 3: NCSI-ის პირველი ათეული. *წყარო: https://ncsi.ega.ee/ncsi-index/*

როგორც ხედავთ, აღნიშნული ინდექსის მიხედვით, მოწინავე პოზიციებზე ევროკავშირის ქვეყნები არიან წარმოდგენილები. ამ სტატისტიკაზე დაყრდნობით ჩვენ არ შეგვიძლია, ზუსტად ვთქვათ, მაგალითად, საბერძნეთი კიბერუსაფრთხოების მიმართულებით ამერიკის შეერთებულ შტატებზე უკეთესია თუ უარესი, აღნიშნული სტატისტიკაში უამრავი კომპონენტი არსებობს, თუნდაც კიბერშეტევების სიხშირე ქვეყნის მასშტაბით. თუმცა არსებობს კომპონენტები, რომლის მიხედვითაც შესაძლებელია, მაინც მოვახდინოთ შედარება, რაც დაგვეხმარება სწორად აღვიქვათ, რომელი სახელმწიფო რა დონეზე იმყოფება.

არსებობს ***ევროკავშირის კიბერუსაფრთხოების სააგენტო (ENISA),*** რომელიც ზრუნავს ევროკავშირის მასშტაბით მაღალი დონის მიღწევაზე. ***ENISA*** თანამშრომლობს ევროკავშირის წევრ სახელმწიფოებთან და დახმარებას უწევს მათ, რათა სათანადოდ მოემზადონ მომავალი კიბერგამოწვევებისთვის.

ასევე შეგვიძლია ვისაუბროთ ***EU4Digital Facility-ზე,*** რომელიც ხელს უწყობს ციფრულ ეკონომიკასა და საზოგადოების ძირითად სფეროებს, ევროკავშირის ნორმებს. აღსანიშნავია, რომ ციფრული ბაზრების ჰარმონიზაცია არის ევროკავშირის პოლიტიკის ერთ-ერთი მთავარი მიღწევა. ევროკავშირის მხარდაჭერა ამ სფეროში ხორციელდება ***EU4Digital Initiative-ის*** მეშვეობით. ციფრული ბაზრის ჰარმონიზაცია ***EU4Figital-ის*** საშუალებით ხელს უწყობს ონლაინსერვისების ბარიერების აღმოფხვრას მოქალაქეებისთვის, საჯარო ადმინისტრაციებისა და ბაზრებისთვის, რაც გულისხმობს ონლაინსერვისების გაუმჯობესებას, უკეთეს ფასებს და მეტ არჩევანს. ეს საკითხი ხელს უწყობს ინვესტიციების მოზიდვას, ვაჭრობის გაზრდას, დასაქმებას. არსებული კომპანიები უფრო სწრაფად გაიზრდებიან, სტარტაპ ბიზნესი უფრო ადვილად შეიქმნება, რაც შეაჩერებს ჭკვიანი ტვინების გადინებას ქვეყნებიდან.

EU4Digital არის ერთგვარი ქოლგა, რომელიც ახორციელებს ევროკავშირის მხარდაჭერას. ***EU4Digital Initiative*** აერთიანებს ევროკავშირის სხვადასხვა პრიორიტეტებს, მათ შორის არის კიბერუსაფრთხოება. მაგალითად, ხორციელდება

EAST პროექტი, რომელიც მიზნად ისახავს პარტნიორ ქვეყნებში კიბერუსაფრთხოების გაძლიერებასა და ციფრული სერვისების გამოყენების მიმართულებით ნდობის გაზრდას.

ასევე, ***EA4Digital-ის*** მეშვეობით ხორციელდება პროექტი *„კიბერუსაფრთხოება აღმოსავლეთში“ რომელიც მოიცავს 2019-2022 წლებს. ევრკოავშირის კონტრიბუცია შეადგენს 3,121,600 ევროს. აღნიშნულ პროექტში შედიან ისეთი ქვეყნები, როგორებიცაა: სომხეთი, აზერბაიჯანი, ბელორუსია, საქართველო, მოლდოვა და უკრაინა“.*[41]

ევრკოავშირს, როგორც ნატოს, გააჩნია თავისი სტანდარტიზაციის ასოციაცია. 1961 წელს დაარსდა ევროპული სტანდარტიზაციის კომიტეტი ***CEN***, რომელიც აერთიანებს სახელმწიფოების სტანდარტიზაციის ეროვნულ ორგანიზაციებს. იგივე 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 გააჩნია 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) მართავს ევროპული ელექტროტექნიკური სტანდარტების შემუშავებას. მისი წევრია ევროკავშირის ყველა ქვეყანა და აღმოსავლეთ ევროპის სახელმწიფოები. ***CENELEC*** სტანდარტების 75 პროცენტი ემყარება საერთაშორისო ელექტროტექნიკური კომისიის ***(IEC)*** სტანდარტებს.

[41] *Funded by the European Union, "The EU4Digital Initiative", p. 1, 2022. https://eufordigital.eu/discover-eu/the-eu4digital-initiative/*

ევროპის სატელეკომუნიკაციო სტანდარტების ინსტიტუტი (ETSI) ავითარებს საერთაშორისო სატელეკომუნიკაციო სტანდარტებს. მისი წევრები არიან მმართველი ორგანოები საინფორმაციო ტექნოლოგიების სფეროში. ***CEN, CENELEC*** და ***ETSI*** შეიმუშავებენ სტანდარტებს ევროკომისიის მოთხოვნითაც. საბოლოო ჯამში ჰარმონიზებული სტანდარტები იძლევა უფრო დეტალურ მითითებებს და კონკრეტულ დირექტივებს.

გაერო (UN)

გაერთიანებული ერების ორგანიზაცია, რომელიც 1945 წელს შეიქმნა, ამჟამად 193 წევრს ითვლის, რაც იმას ნიშნავს, რომ წევრი სახელმწიფოები ეთანხმებიან ამ ორგანიზაციის წესდებასა და პრინციპებს. წესდებისა და პრინციპების ქვაკუთხედი კი საყოველთაო მშვიდობის უზრუნველყოფა და სახელმწიფოთა თანამშრომლობაა. აი, აქ კი შევდივართ ერთგვარ ჩიხში: საქმე ის არის, რომ გაერო გმობს ომს, მსხვერპლს, ნგრევას, შიმშილს, ლტოლვილების გაჩენას, ეკოლოგიურ კატასტროფებს, გარემოს დაბინძურებას და ათას უბედურებას (რომელი არ არის ამჟამად უკრაინაში?!), მაგრამ ქმედებებში ან ძალიან ნელია, ან შეშფოთება-აღშფოთება-დაგმობის პროცესშია, ან მხოლოდ რეზოლუციებით შემოიფარგლება. არ გვინდა, დავაკნინოთ ამ ორგანიზაციის ეგიდით წარსულში განხორციელებული სამშვიდობო, ჰუმანიტარული თუ სხვა სახის ოპერაციები, მაგრამ რეალობა ის არის, რომ ეს ღონისძიებები მხოლოდ იმ შემთხვევაში ყოფილა წარმატებული, როცა გაეროს უშიშროების საბჭოს მუდმივი წევრებისგან ან თანხმობა ყოფილა, ან უბრალოდ წინააღმდეგობა არ გაუწევიათ. გაეროს არაეფექტურობის მაგალითად საქართველოს მაგალითების მოშველიებაც სრულიად საკმარისია: უამრავ რეზოლუციას თუ განცხადებას ჩვენი დევნილების შესახებ, ქმედითი ნაბიჯებია არ მოჰყოლია. სამწუხაროდ, გაეროს შეშფოთება-აღშფოთება-დაგმობის რეზოლუციები ვერც უკრაინას ეხმარება და ვერც რუსეთს აჩერებს. ასევეა ციფრულ საფრთხეებთან მიმართებაშიც. თუ რუსეთ-უკრაინას შორის რაიმე სახის სამშვიდობო შეთანხმება შედგება, შეიძლება გაეროსაც დაეკისროს სამშვიდობო მანდატი, რომელსაც ერთი მხრივ სიმბოლური დატვირთვა ექნება,

მეორე მხრივ კი ლეგიტიმურობისთვის მნიშვნელოვანი იქნება. დიდი ხანია დადგა დრო, გაეროს ადაპტირება მოხდეს ისევ და ისევ მისი ეფექტიანობის გასაძლიერებლად. თუ იმასაც გავითვალისწინებთ, ამ ორგანიზაციის ბიუჯეტი 3.1 მილიარდი აშშ დოლარია, მაშინ პრეტენზიები უფრო საფუძვლიანი და ლეგიტიმური ხდება.

ამერიკის შეერთებული შტატები

ზესახელწმიფო - ეს ტერმინი ცივი ომის დასრულებისთანავე არ გამქრალა. ამერიკის შეერთებულმა შტატებმა, ფაქტია, ეს სახელი თავის თავზე უფრო მეტად მოირგო, ვიდრე სხვამ. მსოფლიო ჰეგემონობისთვის, რა თქმა უნდა, გადამწყვეტი მნიშვნელობა ბირთვული სახელმწიფოს, უზარმაზარი შესაძლებლობების სამხედო პოტენციალს აქვს, თორემ განვითარებულ ეკონომიკა და თანამედროვე ტექნოლოგიები სხვა ქვეყნებსაც გააჩნიათ.

ამერიკის შეერთებული შტატები, როგორც ვიცით, მოიცავს ორმოცდაათ შტატსა და ერთ ფედერალურ ოლქს, ხოლო კონტინენტზე მდებარეობს ორმოცდაცხრა შტატი. მას ჩრდილოეთიდან ესაზღვრება კანადა, ხოლო სამხრეთიდან - მექსიკა, მოქცეულია ორ ოკეანეს შორის. საინტერესოა, რომ ამერიკის შეერთებულ შტატებსა და რუსეთს ბერინგის სრუტე აკავშირებთ. იგი ასევე ფლობს ტერიტორიებს წყნარ ოკეანესა და კარიბის ზღვებში, ხოლო ეკონომიკის მაჩვენებლებით მსოფლიოში პირველი ადგილი უკავია.

ასევე საინტერესოა, რომ ამერიკის შეერთებული შტატები დააარსა ცამეტმა ბრიტანულმა კოლონიამ, როდესაც 1776 წლის 4 ივლისს თავი დამოუკიდებლად

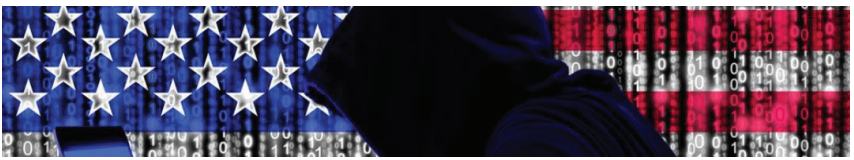
გამოაცხადეს, ხოლო 1787 წლის 17 სექტემბერს მიიღეს ამერიკის შეერთებული შტატების კონსტიტუცია. ამერიკის შეერთებული შტატები მონაწილეობდა როგორც პირველ, ასევე მეორე მსოფლიო ომში. იგი გახდა პირველი სახელმწიფო, რომელმაც ბირთვული იარაღი შექმნა. ქვეყანა არის გაეროს უშიშროების საბჭოს მუდმივი წევრი.

ასეთი ზესახელმწიფოს არსებობა თავისთავად გულისხმობს იმას, რომ დიდი როლი ენიჭება მის პოზიციას რუსეთ-უკრაინის ომში. თუ როგორ განვითარდება რუსეთ-უკრაინის ომი, დიდი წილი მის პოლიტიკურ ნებაზეა დამოკიდებული.

ერთი წუთით წარმოვიდგინოთ, რუსეთის წინააღმდეგ დაწესებულ სანქციებში აშშ რომ არ მონაწილეობდეს, ან შეიარაღეებით არ ეხმარებოდეს უკრაინას, ან რუსი ოლიგარქების ქონებას თუ საბანკო ანგარიშებს არ აყდაღებდეს და არ ყინავდეს, ვინმეს სჯერა, რომ ევროპელები მარტო შეძლებდნენ ამ ეკონომიკურ და ფინანსურ ფრონტზე რუსეთის რეალურ დაზარალებას?! ან წარმოიდგინეთ, რომ ამერიკის შეერთებული შტატები, თავის ბირთვული შეიარაღების პოტენციალით, რომელიც ევროპაშიცაა განთავსებულ-განლაგებული, რომ ნატოს ლიდერი ქვეყანა არ იყოს? არც ერთი ქვეყნის დაკნინებას არ ვცდილობთ, მაგრამ სწორედ ამერიკის შეერთებული შტატებია ის მთავრი შემაკავებელი ფაქტორი ნატოსთან ერთად, რუსეთი უკრაინის მაგივრად სხვა ევროპული ქვეყნის ტერიტორიაზე რომ არ არის შეჭრილი.

რამდენად და რამდენ ხანს შეძლებს რუსეთი ომის წარმოებას უკრაინაში, უამრავ ფაქტორზეა დამოკიდებული, მაგრამ იმ დროს, როცა შეჩერება მოუწევს, მოლაპარაკების პროცესში ამერიკელების სიტყვა გადამწყვეტი იქნება. იმ შემთხვევაში, თუ ეს პირდაპირ არ გამოჩნდება, მაშინ ამ მისიას ანგლო-საქსური ფაქტორი (მაგ. ბრიტანული ან კანადური) აიღებს თავის თავზე, ცხადია, ამერიკელებთან შეთანხმებული და კოორდინირებული ქმედებებით.

ამერიკის შეერთებული შტატების კიბერშესაძლებლობები



მთავრობები იწყებენ იმის გაცნობიერებას, თუ რამდენად მნიშვნელოვანია კიბერუსაფრთხოება რეალურად. ამერიკის შეერთებული შტატები არის ნომერ პირველი ქვეყანა კიბერუსაფრთხოების მიმართულებით, მისი ფინანსები კოლოსალურად მაღალია. იგი ყოველწლიურად ზრდის თანხებს კიბერშესაძლებლობების განვითარებისათვის. *"2022 წლის მარტში პრეზიდენტ ბაიდენის ადმინისტრაციამ 2023 წლის ფისკალური ბიუჯეტი გამოაქვეყნა, რომელშიც სამოქალაქო კიბერუსაფრთხოების ხარჯებისთვის 11 მილიარდი აშშ დოლარია გამოყოფილი - ეს 11%-ით მეტია წინა წელთან შედარებით".*[42]

ამერიკის შეერთებული შტატების კიბერუსაფრთხოების გაძლიერებაში ერთ-ერთ ფაქტორს რუსეთი ფედერაცია, ირანის ისლამური სახელმწიფო და ჩინეთი წარმოადგენენ, მათი ქმედებები სუპერსახელმწიფოს უბიძგებს, უფრო მეტად განავითაროს ტექნოლოგიები და შეიმუშაოს ახალი მექანიზმები. 2016 წელს აშშ-ის საპრეზიდენტო არჩევნებში რუსეთის ფედერაციის მხრიდან დაქირავებული ჰაკერების ჩარევამ გვაჩვენა, რომ ასეთ ქვეყანასაც კი სჭირდება კიბერტექნოლოგიების გაძლიერება, რათა მსგავსი საფრთხეები მინიმუმამდე იქნას დაყვანილი.

დონალდ ტრამპი

2017 წელს გამოქვეყნდა აშშ-ის პრეზიდენტის, ***დონალდ ტრამპის*** პირველი ***„ეროვნული უსაფრთხოების სტრატეგია",*** იგი ეფუძნება ოთხ მნიშვნელოვან ეროვნულ ინტერესს: *"ამერიკული ხალხისა ცხოვრების წესის დაცვა, ამერიკის კეთილდღეობის ზრდა, მშვიდობის შენარჩუნება, ამერიკის გავლენის გაზრდა".*[43] აქ ძალზე საყურადღებოა მესამე თავი: „ძალის მეშვეობით მშვიდობის შენარჩუნება", სადაც ორი სახელმწიფოს - რუსეთისა და ჩინეთის მიმართ პრეტენზიებია

[42] *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.*

[43] *"ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სტრატეგია", ამერიკის შეერთებული შტატების საელჩო საქართველოში, 2017, გვ. 1. https://ge.usembassy.gov*

გამოთქმული. ასევე მნიშვნელოვანია სტრატეგიის მეოთხე თავი: „ამერიკის გავლენის გაზრდა“, რომელიც პირდაპირ გვამცნობს, თუ რა არის ამ სახელმწიფოს მიზანი.

ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სააგენტო *(NSA)* არის კიბერუსაფრთხოების ორგანიზაციების მაკონტროლებელი ორგანო. *,,იგი შეიქმნა 1952 წელს, როგორც საიდუმლო ორგანიზაცია. მისი შექმნის საჭიროება დაზვერვითი პოტენციალის შესაძლებლობების გაზრდამ გამოიწვია, დაზვერვისა **(SIGINT)** და ინფორმაციული უსაფრთხოების **(INFOSEC)** გასაანალიზებლად და დასამუშავებლად“.*[44]

თავიდან ეროვნული უსაფრთხოების სააგენტო დაფარული ბიუჯეტით და ანონიმურობით სარგებლობდა. რაც არ უნდა გასაკვირი იყოს, *,,დიდი ხნის განმავლობაში ამ ორგანიზაციას მოიხსენიებდნენ „არაფრის სააგენტოდ“ – “No Such Agency”. იგი ოფიციალურ სააგენტოდ 1975 წელს გამოცხადდა“.*[45]

ენ ნოიბერგერი

აღნიშნული სააგენტოს მრჩევლის მოადგილე გახლავთ ***ენ ნოიბერგერი (Anne Neuberger)*** და კონსულტაციას უწევს პრეზიდენტს კიბერუსაფრთხოების საკითხებში. ასევე ეხმარება პრეზიდენტის ბრძანებების შესრულებაში სააგენტოებს.

ამერიკის შეერთებულ შტატებს კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების მიმართულებით სხვადასხვა პრობლემები ჰქონდა. მაგალითად, *,,ვიეტნამის ომის დროს საეკლესიო მოსმენებისას გაირკვა, რომ ეროვნული*

[44] Tyson M., "The US federal cybersecurity bureaucracy: A guide", CSO united states, may 16. p. 1, 2022. https://www.csoonline.com/
[45] Tyson M., "The US federal cybersecurity bureaucracy: A guide", CSO united states, may 16. p. 1, 2022. https://www.csoonline.com/

*უსაფრთხოების სააგენტო აკვირდებოდა ომის მოწინააღმდეგე აქტივისტებს, იმ დროისთვის ისეთ ცნობილ ადამიანებს, როგორებიც იყვნენ, **მუჰამედ ალი** და **მარტინ ლუთერ კინგი უმცროსი”**. აღნიშნული ინფორმაციის დადასტურებამ კი 1978 წელს გამოიწვია დაზვერვის ზედამხედველობის აქტის შემუშავება **(FISA),** თუმცა მსგავსი პრობლემები ამით ვერ აღმოიფხვრა. 2010 წელს ეროვნული უსაფრთხოების სააგენტო კვლავ მოექცა ყურადღების ცენტრში - აღმოჩნდა, რომ სააგენტო იყენებდა **Prism (პრიზმა)** პროგრამის კოდს, რომელიც ასევე ცნობილია **SIGAD US-984XN**-ის სახელით.[46]* აღნიშნული პროგრამა აგროვებს ინფორმაციას სხვადასხვა ორგანიზაციებზე, კომპანიებზე ინტერნეტში, სხვადასხვა საძიებო პლატფორმების გამოყენებით, ელფოსტის, ტელეფონისა და სოციალური ქსელების საშუალებით. აღნიშნული პროგრამა ეწინააღმდეგებოდა სამოქალაქო საზოგადოების დაცვას.

ამერიკის შეერთებულ შტატებში 2009 წელს დაარსდა ***კიბერსარდლობა (CYBERCOM),*** რომელიც წარმოადგენს ერთიან საბრძოლო ხელმძღვანელობას, ეს არის უმაღლესი დივიზია ამ ქვეყნის არმიაში. შეიძლება ითქვას, კიბერსარდლობა და ეროვნული უსაფრთხოების სააგენტო ერთი ქოლგის ქვეშ ფუნქციონირებენ. იყო საუბარი მათ გამიჯვნაზე, მაგრამ ამ დროისთვის მაინც ემორჩილებიან ერთიან სარდლობას.

შეიძლება გაგვიჩნდეს ლოგიკური კითხვა: რა განსხვავებაა ამ ორ ორგანიზაციას შორის? ამაზე პასუხი არ არის მარტივი იქიდან გამომდინარე, რომ ისინი საიდუმლო საქმიანობით არიან დაკავებულნი და ინფორმაცია თითქმის არ არსებობს. შეუძლებელია, ზუსტად დადგინდეს, რა განსხვავებაა მათ შორის. ერთი რის თქმაც შეგვიძლია, არის ის, რომ ფუნქციონირებენ სხვადასხვა სამართლებრივი უფლებამოსილებით. თუმცა ამის დეტალურად გაანალიზებაც დიდ სირთულეს წარმოადგენს.

შეიძლება მაგალითისთვის გამოვყოთ კიბერსარდლობის ერთ-ერთი განცხადება, რათა შევეცადოთ განსხვავების პოვნას ამ ორ სააგენტოს შორის:

[46] *Tyson M., "The US federal cybersecurity bureaucracy: A guide", CSO united states, may 16. p. 1, 2022. https://www.csoonline.com/*

„ამერიკის შეერთებული შტატების კიბერსარდლობა ხელმძღვანელობს და ახორციელებს ინტეგრირებულ ელექტრონულ ომს, ასევე ინფორმაციულ და კიბერსივრცის ოპერაციებს“.[47]

ამ განცხადებაში საყურადღებოა სიტყვა „ომი“. თუმცა რთულია იმის განსაზღვრა, რა გაგებით არის ეს სიტყვა ნახსენები კიბერსარდლობის მხრიდან. ვინაიდან, ამ სააგენტოს საქმიანობა დაფარულია, შეიძლება ვივარაუდოთ, რომ მათ წვლილი მიუძღვით ისეთ აქტივობებზე, როგორიცაა საპასუხო კიბერთავდასხმები ირანის ისლამურ სახელმწიფოსა და რუსეთის ფედერაციაზე.

ამერიკის შეერთებულ შტატებში ფუნქციონირებს ***კიბერუსაფრთხოებისა და ინფრასტრუქტურის სააგენტო (CISA).*** აღნიშნული სააგენტოს შექმნა გახლავთ მთავრობის მცდელობა კიბერსაფრთხეებზე სწრაფი რეაგირებისთვის. მისი მთავარი მისიაა, უხელმძღვანელოს და გამოიყენოს კიბერრესურსები კიბერ და ფიზიკური რისკების გასაანალიზებლად, შემდეგაც კი ჩაერთოს მართვაში და დაიცვას კრიტიკული ინფრასტრუქტურა.

კიბერუსაფრთხოებისა და ინფრასტრუქტურის სააგენტო ინფრასტრუქტურის დაცვის ფართო მისიით შეიქმნა 2018 წელს. მას უფრო აქვს თავდაცვითი და მარეგულირებელი პოზიცია, ვიდრე ***ეროვნული უსაფრთხოების სააგენტოსა*** და ***არმიის კიბერსარდლობას.*** *„CISA-ს მთავარი მიზანია არჩევნების უსაფრთხოება“,*[48] ეს მის სტრატეგიულ დოკუმენტშია აღნიშნული. ორგანიზაცია თანამშრომლობს როგორც ამერიკის შეერთებული შტატების მთავარ ხელმძღვანელობასთან, ასევე ფედერალურ მთავრობებთან საარჩევნო ინფრასტრუქტურის გასავითარებლად და გასაძლიერებლად.

[47] *Tyson M., "The US federal cybersecurity bureaucracy: A guide", CSO united states, may 16. p. 1, 2022. https://www.csoonline.com/*
[48] *Tyson M., "The US federal cybersecurity bureaucracy: A guide", CSO united states, may 16. p. 1, 2022. https://www.csoonline.com/*

ამერიკის შეერთებულ შტატებში ფუნქციონირებს ***სტანდარტებისა და ტექნოლოგიების ეროვნული უნივერსიტეტი (NIST).*** მისი მიზანია აშშ-ის ინოვაციებისა და სამრეწველო კონკურენტუნარიანობის ხელშეწყობა, რათა გაზარდოს ეკონომიკური უსაფრთხოება და გააუმჯობესოს ცხოვრების ხარისხი.

კიბერუსაფრთხოების სფეროში სტანდარტებისა და ტექნოლოგიების ეროვნული უნივერსიტეტი ორიენტირებულია კრიპტოგრაფიაზე. მან თავისი როლი შეასრულა თანამედროვე კრიპტოგრაფიის, როგორც ასიმეტრიულ, ასევე სიმეტრიულ განვითარებაში. ინსტიტუტი აგრძელებს მონაწილეობას კრიპტო სტანდარტების განსაზღვრასა და ლიდერობს პოსტ-კვანტური უსაფრთხო ალგორითმების შემუშავებაში.

Office of the National Cyber Director

აშშ კიბერუსაფრთხოების მიმართულებით ავითარებს შესაძლებლობებს, იგი ცდილობს, ყველა საჭირო გამოწვევაზე ადეკვატური პასუხი გასცეს და შესაბამისი ფინანსებიც დახარჯოს. მაგალითად, 2021 წელს შეიქმნა ***ეროვნული კიბერდირექტორის ოფისი (ONCD),*** რომლის ხელმძღვანელიც ***კრის ინგლისი (Chris Inglis)*** გახლავთ.

კრის ინგლისი

აღნიშნული თანამდებობა არის პრეზიდენტის კიდევ ერთი მრჩევლისთვის, რომელიც ძალიან ჰგავს კიბერ და განვითარებადი ტექნოლოგიების მრჩეველს. აღნიშნული ოფისი ჯერ კიდევ თავისი შესაძლებლობების განვითარების პროცესშია და ფოკუსირებულია მთავრობის ერთიანი ქმედებების წარმართვაზე. ოფისს გააჩნია საქმიანობის ოთხი ძირითადი მიზანი: *„ფედერალური თანმიმდევრობის*

უზრუნველყოფა, საჯარო და კერძო თანამშრომლობის გაუმჯობესება, რესურსების მორგება მისწრაფებებთან, აწმყო და მომავალი გამძლეობის გაზრდა".[49]

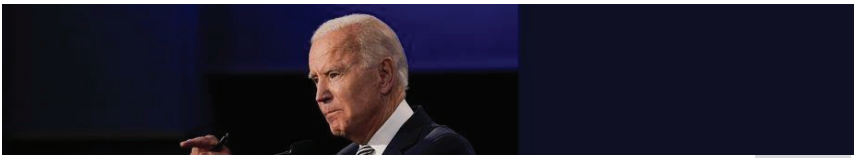
ფედერალური კიბერუსაფრთხოების მიმართულებით დიდი როლი ენიჭება ***FBI - ის.*** იგი წარმოადგენს წამყვან სააგენტოს კიბერშეტევებისა და უნებართვო შეჭრების გამოძიებაში. არადა, ***FBI - ის*** ვებ-გვერდი და მისი კიბერტექნოლოგიები არც ისე თანამედროვედ გამოიყურება. თუმცა დამსახურება მეტად მნიშვნელოვანია - ***FBI - ის*** აქვს ფართო მანდატი კიბერუსაფრთხოების მიმართულებით, რომელიც ახორციელებს გამოძიებას მარტივი თაღლითობიდან დაწყებული, საერთაშორისო გამოსასყიდი ორგანიზაციების პროგრამებით დამთავრებული.

ამერიკის შეერთებული შტატების უახლესი მიდგომები კიბერუსაფრთხოების მიმართულებით არის ყოვლისმომცველი. ჩვენ ასევე შეგვიძლია ვისაუბროთ ***CIA-ზე,*** რომელიც უახლეს ციფრულ, კიბერვაჭრობასა და ***IT*** ინფრასტრუქტურის განვითარებას მოიცავს. ასევე, ***ფედერალური სავაჭრო კომისიის (FTC)*** პასუხისმგებლობაზე ან ***ბავშვთა ონლაინ კონფიცენციალურობის აქტზე (COPPA),*** შემდეგ ***ტრანსპორტის უსაფრთხოების ადმინისტრაციის (TSA)*** ჩართულობაზე კიბერუსაფრთხოების მიმართულებით.

ყველა სფერო თავის მხრივ ჩართულია კიბერუსაფრთხოების მიმართულებით, ისინი ყოველდღიურ რეჟიმში გადართულნი არიან ტექნოლოგიების განვითარებაზე - კერძო თუ საერთაშორისო ორგანიზაცია, ქვეყანა და ა.შ.

[49] *Tyson M., "The US federal cybersecurity bureaucracy: A guide", CSO united states, may 16. p. 1, 2022. https://www.csoonline.com/*

კიბერსაფრთხეების გაზრდასთან ერთად, ბუნებრივია, აშშ-ის ტექნოლოგიური სისტემებისა და ქსელების დაცვა არაავტორიზებული წვდომისგან უფრო რთული ხდება. 2021 წელს ***გენერალური ინსპექტორის ოფისმა (OIG)*** გამოაქვეყნა განცხადება, სადაც აღნიშნულია, რომ *"**შეერთებული შტატების შიდა უსაფრთხოების დეპარტამენტმა (DHS)** გაუმჯობესა კიბერუსაფრთხოების მიმართულებით თანამშრომლობა და კოორდინაცია **თავდაცვის დეპარტამენტთან (DOD),** მაგრამ ხარვეზების ნაწილი მაინც დარჩა".*[50]



ჯო ბაიდენი

2021 წლის მარტში პრეზიდენტმა ***ჯო ბაიდენმა*** ხელისუფლების ყველა დონეზე კიბერუსაფრთხოება ***შიდა უსაფრთხოების დეპარტამენტის*** მთავარ პრიორიტეტად აქცია.[51] ეს განაპირობა გამოსასყიდი პროგრამის მზარდმა საფრთხემ.

ამის შემდეგ ***შიდა უსაფრთხოების დეპარტამენტი, ეროვნული უსაფრთხოების სააგენტო, კიბერსარდლობა*** და ***თავდაცვის დეპარტამენტი*** შეთანხმდნენ, რომ აღნიშნული პრობლემები გადაეჭრათ სამოქმედო გეგმის ***CAP-ის***[52] მემორანდუმის საშუალებით. ***გენერალური ინსპექტორის ოფისმა*** ჩაატარა კვლევა, რათა შეეფასებინა ***შიდა უსაფრთხოების დეპარტამენტისა*** და ***თავდაცვის დეპარტამენტის*** თანამშრომლობა კიბერუსაფრთხოების მიმართულებით, მათი ერთობლივი ძალებით განხორციელებული საქმეები.

დამკვირვებელმა ორგანომ ***(OIG)*** დაადგინა, რომ გასული ექვსი წლის განმავლობაში შიდა უსაფრთხოების დეპარტამენტი მონაწილეობდა კრიტიკული ინფრასტრუქტურის პროგრამებში, აუმჯობესებდა კიბერტექნოლოგიების მიმართულებით ინფორმირებულობას და ატარებდა ტრენინგებს.

---

[50] Bielby K., "OIG: DHS Has Improved Cybersecurity Collaboration With DOD But Gaps Remain", p. 1. 2021, https://www.hstoday.us/

[51] Homland Security, "President Biden has made cybersecurity, a critical element of the Department of Homeland Security's (DHS) mission, a top priority for the Biden-Harris Administration at all levels of government", p. 1. 2022. https://www.dhs.gov/topics/cybersecurity

[52] United States Air Force Auxiliary, "The CAP Guide to Effective Communication", 2021. https://www.gocivilairpatrol.com/media/cms/P_12_1_Oct_2021_E4A84FC1A6F2B.pdf

აშშ-ის მთავრობა და კერძო სექტორი მჭიდროდ თანამშრომლობენ კრიტიკული ინფრასტრუქტურის უსაფრთხოების გაძლიერების მხრივ. თანამშრომლობა შემოიფარგლება ინიციატივებით და უწოდებენ ***Pathfinder (გზამკვლევი)*** პროგრამებს. იგი მორგებულია იმ გამოწვევებსა და საფრთხეებზე, რის წინაშეც კრიტიკული ინფრასტრუქტურის სექტორი დგას. *,,ორი წლის განმავლობაში შიდა უსაფრთხოების დეპარტამენტი მონაწილეობდა **Pathfinder-ის** ორ პროგრამაში, რომელიც მოიცავდა ენერგეტიკისა და ფინანსური სერვისების კრიტიკული ინფრასტრუქტურის უსაფრთხოებას. შიდა უსაფრთხოების დეპარტამენტმა კიბერთავდაცვის უნარების გასაძლიერებლად 46 ერთობლივ ტრენინგებსა და წვრთნებში მიიღო მონაწილეობა, აქედან სამს თავად ხელმძღვანელობდა".*[53]

მიუხედავად ამისა, გენერალური ინსპექტორის ოფისი ამბობს, რომ ,,მათ ზუსტად ვერ დაადგინეს ***შიდა უსაფრთხოების დეპარტამენტმა*** დააკმაყოფილა თუ არა მემორანდუმ ***CAP-ში*** ასახული ყველა მოთხოვნა".[54] ასევე, მათი განმარტებით, ***შიდა უსაფრთხოების დეპარტამენტი*** არ ახორციელებდა ეფექტურ მონიტორინგს. როგორც განცხადებაშია ნათქვამი, იგი ვალდებული იყო ტექნიკური პერსონალი გაეზარდა 50 ადამიანამდე, გამოძიების შედეგად კი დადასტურდა, რომ შიდა ტექნიკური მიმართულებით 10-ზე მეტი ადამიანი არ მუშაობდა. რაც, რა თქმა უნდა, პროგრამების სრულფასოვნად შესრულებას ხელს შეუშლიდა.

ასეა თუ ისე, კიბერუსაფრთხოების მიმართულებით ***შიდა უსაფრთხოების დეპარტამენტისა*** და ***თავდაცვის დეპარტამენტის*** ერთობლივი თანამშრომლობით განხორციელებული პროგრამები ჩატარდა და დასრულებულად ჩაითვალა.

მოვლენების კვალდაკვალ თეთრმა სახლმა გამოაქვეყნა ახალი ზომები კიბერუსაფრთხოების გასაძლიერებლად ფედერალურ სააგენტოებში, აშშ-ის კერძო და საჯარო ინფრასტრუქტურაზე გაზრდილი კიბერშეტევების გამო. განცხადებაში აღნიშნულია, რომ სააგენტოები გადავლენ ***„ნულოვანი ნდობის"*** მოდელზე, რაც გულისხმობს ყველაფრის გადამოწმებასა და თავდასხმების მოგერიებას.

[53] *Bielby K., "OIG: DHS Has Improved Cybersecurity Collaboration With DOD But Gaps Remain", p. 1. 2021, https://www.hstoday.us/*

[54] *Bielby K., "OIG: DHS Has Improved Cybersecurity Collaboration With DOD But Gaps Remain", p. 1. 2021, https://www.hstoday.us/*

ჯო ბაიდენი

აღნიშნული მიდგომა ემთხვევა პრეზიდენტ ***ჯო ბაიდენის*** განკარგულებას ქვეყნის კიბერუსაფრთხოების გაუმჯობესების შესახებ, რომელსაც მან ხელი მოაწერა დიდი კიბერშეტევის შემდეგ. აღნიშნული კიბერშეტევა რუსი ჰაკერების ჯგუფმა განახორციელა, რომელიც ***DarkSide-ის*** სახელით არის ცნობილი. *„მათ განახორციელეს კიბერშეტევა მილსადენზე და გათიშეს ოპერატიული სისტემები, რითაც 4,4 მილიონი დოლარის გამოძალვა შეძლეს. მოგვიანებით იუსტიციის დეპარტამენტმა ფულის უმეტესი ნაწილი დააბრუნა".*[55]

ამერიკის შეერთებული შტატების მართვისა და მენეჯმენტის ოფისმა (OMB) განაცხადა, რომ ***„ნულოვანი ნდობის"*** *სტრატეგია სააგენტოებს მისცემს საფრთხეების აღმოჩენისა და აღმოფხვრის უნარს. კიბერუსაფრთხოების ექსპერტები ვარაუდობენ, რომ* ***„ნულოვანი ნდობის"*** *სტრატეგიამ შეიძლება გაუმჯობესოს კიბერუსაფრთხოება, მაგრამ სხვა საკითხებზე იმოქმედოს უარყოფითად".*[56] აღნიშნული მოდელი გულისხმობს, რომ ყველა მომხმარებელი და ყველა სახის აქტიურობა წარმოადგენს რისკს. რა თქმა უნდა, ეს ეფექტურია კიბერთავდასხმების მინიმუმამდე დასაყვანად, მაგრამ ასევე შეიძლება უარყოფითად ეფექტური იყოს ორგანიზაციებზე ნეგატიური ზემოქმედებისთვის.

[55] *Dress B., "White House moves to boost cybersecurity at federal agencies", p. 1, 2022. https://thehill.com/policy/cybersecurity/591497-white-house-moves-to-boost-cybersecurity-at-federal-agencies/*
[56] *Dress B., "White House moves to boost cybersecurity at federal agencies", p. 1, 2022. https://thehill.com/policy/cybersecurity/591497-white-house-moves-to-boost-cybersecurity-at-federal-agencies/*

ისრაელი

ისრაელს სხვა მიღწევებთან ერთად *(სამეზობლოში თითქმის ყველა ქვეყანასთან აქვს ომი გადატანილი, ყველასთან გამარჯვებული გამოვიდა)* აქვს არნახული გამარჯვებები და ეს ასე უბრალოდ არ ხდებოდა: ებრაელი ხალხი, მიუხედავად უამრავი წინააღდგომებისა, წლების განმავლობაში აშენებდა და ავითარებდა თავის ქვეყანას დემოკრატიულად, პოლიტიკურად, ეკონომიკურად, ფინანსურად. ისრაელი, სამხედრო პოტენციალის თვალსაზრისით ერთ-ერთ ძლიერ სახელმწიფოდ ჩამოყალიბდა - იარაღის გაყიდვის მხრივ წამყვანი ქვეყნების ოთხეულშია *(აშშ, რუსეთი, ჩინეთი, ისრაელი).* ამ ყველაფერს საფუძვლად უარესად პასუხიმგებლიანი დამოკიდებულება, შრომისმოყვარეობა, განათლება, საქვეყნოდ ცნობილი ებრაული ჭკუა დაედო. ვინ, ვინ და ისრაელმა ნამდვილად იცის ომისა და მშვიდობის ფასი. სწორედ ამიტომ რუსეთ-უკრაინის ომში სამშვიდობო ინიციატივითაც გამოდის. საგულისხმოა, ებრაელებს სათანადო გამოცდილებაც გააჩნიათ და ავტორიტეტიც. ნიშანდობლივია, რომ ისრაელის ლიდერებს შეუძლიათ, ნაყოფიერი შუამავლობა გასწიონ როგორც რუსებთან, ასევე უკრაინელებთან, ამერიკელებთან, პოლონელებთან თუ ბრიტანელებთან. გასათვალისწინებელია, რომ ეს ქვეყანა მოწინავეა როგორც სამხედრო თვალსაზრისით, ასევე დიპლომატიური წარმატებებით, მათ შორის ადრე კონფლიქტში თუ საომარ მდგომარეობაში მყოფ ქვეყნებთანაც. ისრაელისა და მისი პოლიტიკური ელიტის, როგორც შუამავლის და მომლაპარაკებლის არგამოყენება შეიძლება დანაშაულის თუ არა, უგუნურობის ტოლფასიც გახდეს. ვფიქრობთ, უნდა ღირდეს მათი გამოცდილების გაზიარებაც და გათვალისწინებაც.

ისრაელის კიბერშესაძლებლობები

ისრაელი, როგორც უკვე აღვნიშნეთ, უამრავი მიმართულებით არის მოწინავე პოზიციებზე და ცდილობს, უფრო მეტად დახვეწას და განვითარებას, ამ მხრივ არც კიბერსივრცეა გამონაკლისი, ეს ქვეყანა მსოფლიო მასშტაბით მოიაზრება ერთ-ერთ ძლიერ კიბერსახელმწიფოდ. მიუხედავად ამისა, თუ კრიტიკულად გავაანალიზებთ მის კიბერთავდაცვით პოტენციალს, მივხვდებით, რომ ამ მხრივ მაინც პრობლემები აქვს. პირველ რიგში უნდა აღვნიშნოთ, რომ ტექნოლოგიური კომპანიები - ***NSO, Argus, Chek Point*** და სხვები ისინი ხელს უწყობენ ისრაელის ტექნოლოგიურ განვითარებას და ეთანხმებიან იმ კამპანიას, რომ ისრაელს შეუძლია სამხედრო სფეროში თავისი ტექნოლოგიური შესაძლებლობების გადაკეთება და აქტივებად გაყიდვა. ისრაელის მხრიდან კიბერთავდასმხების მაგალითები გვიჩვენებს, რომ იგი მართლაც წარმოადგენს საშიშ კიბერძალას. მაგალითად, ცნობილია, ისრაელი სხვადასხვა ტერორისტულ ორგანიზაციებზე ახორციელებს კიბერთავდასხმებს, ასევე ისეთ სახელმწიფოზე, როგორიც ირანის ისლამური რესპუბლიკაა. ერთ-ერთი ყველასათვის ცნობილი კიბერშეტევა ***Stuxnet-ის,***[57] ექსპერტების მოსაზრებით, აღნიშნული კიბეროპერაციების და თავდასხმების უკან ამერიკის შეერთებული შტატები და ისრაელი იყო. შეგვიძლია ვთქვათ, რომ ისრაელის კიბერშესაძლებლობები უკეთესია სხვა წამყვან ქვეყანასთან შედარებით, თუმცა, როგორც უკვე აღვნიშნეთ, იმისთვის, რომ მსოფლიო მასშტაბით ისრაელი იყოს მოწინავე პოზიციაზე, საჭიროა კიბერთავდაცვითი პოტენციალის გაზრდა, კიბერთავდასხმებისგან თავის დაცვა.

[57] *Stuxnet არის მავნე პროგრამა, ბევრი კიბერექსპერტის აზრით იგი წარმოადგენს მავნე პროგრამის ერთ-ერთი ყველაზე რთულ ნაწილს, რომელიც 500 კბ-ზე მეტს შეადგენს. აღნიშნული მავნე პროგრამით თავდასხმის საბოლოო მიზანი იყო პროგრამირებადი ლოგიკური კონტროლერების (PLC) შეცვლა, რომლებიც არეგულირებენ ცენტრიფუგების ბრუნვის სიჩქარეს. თავდამსხმელები ცდილობდნენ მიეყენებინათ დაზიანება და გავლენა მოეხდინათ პროცესზე.*

ნადავ არგამანი

მსოფლიოში მიმდინარე პროცესების ფონზე თუ ვიმსჯელებთ, ისრაელი და მისი მოწინააღმდეგეები აგრძელებენ ბრძოლას ერთმანეთთან, მაგრამ მათ ტრადიციულ შეიარაღებას ემატება კიბერსაშუალებები, ამისი უამრავი მაგალითი მოვიყვანეთ ჩვენს ნაშრომში. მაგალითად, 2019 წლის იანვარში ისრაელის შიდა უსაფრთხოების სამსახურის დირექტორმა ***ნადავ არგამანმა (Nadav Argaman)*** განაცხადა, რომ *"სანდო წყაროებზე დაყრდნობით შეიტყო, ისრაელზე უცხო ქვეყნიდან დაფინანსებული ჰაკერული დაჯგუფებები გეგმავდნენ კიბერთავდასხმებს, რათა ჩარეულიყვნენ იმ დროისთვის უკვე მოახლოებულ არჩევნებში".*[58] უსაფრთხოების სამსახურის დირექტორმა აღნიშნულ განცხადებაში პირდაპირ არ განაცხადა, რომელი ქვეყნებიდან შეიძლებოდა განხორციელებულიყო შეტევები, მაგრამ მოგვიანებით ყველასთვის გახდა ცნობილი, რომ უამრავი ქვეყნიდან (*ირანის ისლამური რესპუბლიკა, ჩინეთი, რუსეთი, თურქეთი, ჰეზბოლა, ჰამასი, ჰაქტივისტური დაჯგუფება „ანონიმუსი" და სხვა.)* და მათ შორის ჰაქტივისტური დაჯგუფებებიდან განხორციელდა კიბერშეტევები ისრაელის სამთავრობო და ბიზნესსერვისებზე. აღნიშნული თავდასხმები უმეტესად შეიცავდა პოპულარულ ***DDoS*** შეტევებს. ამ თავდასხმებმა რა დონეზე მოახდინა ზეგავლენა არჩევნებზე, უცნობია. თუმცა ლოგიკურად რომ ვიმსჯელოთ, თუ ამდენი ქვეყნიდან განხორციელდა კიბერშეტევა, ეს აუცილებლად აისახებოდა არჩევნების შედეგებზეც. როგორც წესი, ასეთი სახის ინფორმაციების გასაჯაროებისგან ყველა ქვეყანა თავს იკავებს ხოლმე. მაგალითად შეგვიძლია მოვიყვანოთ 2016 წლის ამერიკის შეერთებული შტატების საპრეზიდენტო არჩევნები, სადაც რუსეთის ფედერაციის ჰაკერების ჩარევა დადასტურდა, თუმცა მასალების სრული გასაჯაროება არ მომხდარა. ამით იმის თქმა გვინდა, რომ რა დონეზე მოახდინა ჩარევამ ზეგავლენა არჩევნებზე, უცნობია.

[58] *Caspit B., "Ahead of elections, Israel fears foreign cyber meddling", Al-monitor, p. 1, 2019, https://www.al-monitor.com/originals/2019/02/israel-russia-iran-benjamin-netanyahu-cyber-attacks-election.html*

იუვალ სტეინიცი

ასევე შეგვიძლია გავიხსენოთ 2020 წლის დასაწყისში, მაშინდელი ინფრასტრუქტურის, ენერგეტიკისა და წყლის რესურსების მინისტრის, ***იუვალ სტეინიცის (Yuval Steinitz)*** განცხადება, სადაც იგი ამბობს, რომ *"ისრაელმა აღკვეთა მასშტაბური, საფრთხისშემცველი კიბერშეტევები ისრაელის ელექტროსადგურებზე",* [59]მაგრამ პარალელურად იმ დროისთვის ვცრელდებოდა ინფორმაცია, როგორ ნახეს რუსული წყალქვეშა ნავები ისრაელის სანაპირო ზოლთან. უსმენდნენ თუ არა რუსები ისრაელს წყალქვეშა ინტერნეტკაბელების საშუალებით?! 2021 წლის აგვისტოში რამდენიმე დასავლურმა არასამთავრობომ დაადანაშაულა ჩინეთი ისრაელის საჯარო და კერძო სექტორის ჯგუფების წინააღმდეგ დამაზიანებელი კიბერშეტევების განხორციელებაში.

აქედან გამომდინარე, ლოგიკურია, რომ ჩნდება კითხვები: არის თუ არა ისრაელის კიბერსივრცე ისეთივე უსაფრთხო და გამძლე, როგორც ეს ზოგადად მსოფლიო მასშტაბით არის აღიარებული? მნიშვნელოვანია იმ ფაქტის გათვალისწინებაც, რომ ისრაელი ისტორიულად გარშემორტყმულია თავისი მოწინაღმდეგე ქვეყნებით, გეოგრაფიული მდგომარეობა და პოლიტიკური იზოლაცია ამ ქვეყანას არასხელსაყრელ მდგომარებაში აყენებს კიბერსფეროშიც, რადგან მას არ შეუძლია ენდოს თავის მეზობელ ქვეყნებს.

კიბერსივრცე, როგორც ამას ბევრი კიბერექსპერტი განმარტავს, არის საინფორმაციო ტექნოლოგიების, ინფრასტრუქტურისა და რეზიდენტთა მონაცემების ურთიერთდამოკიდებული ქსელი. იგი მოიცავს ინტერნეტს, ასევე სხვა სატელეკომუნიკაციო ქსელებს, კომპიუტერულ სისტემებს და კონტროლის სხვა მექანიზმებს. როგორც ცნობილია, კიბერსივრცე აგებულია ოთხი კომპონენტისგან, თითვეული კი მოიცავს განსხვავებულ საკითხებს:

[59] *Solomon S., "Energy minister says Israel foiled 'serious' attack on power station", The Times of Israel, p. 1, 2020, https://www.timesofisrael.com/energy-minister-says-israel-foiled-serious-attack-on-power-station/*

- *ფიზიკური საფუძვლები (ინფრასტრუქტურა);*
- *ლოგიკა;*
- *ინფორმაცია;*
- *მომხმარებელი.*[60]

ამ საკითხის ახსნით და გაანალიზებით შესაძლებელია მივხვდეთ, ესა თუ ის ქვეყანა რამდენად მოწყვლადია და რამდენად დაუცველია მისი კიბერსივრცე. ამ შემთხვევაში ვიკვლევთ ისრაელის კიბერსივრცის დაუცველობას. ფიზიკური საფუძვლები მოიცავს რეალურ სივრცეში ინფრასტრუქტურას, რომელიც შედგება ოპტიკურ-ბოჭკოვანი კაბელებისგან, კაბელების კვანძებისგან, სერვერებისგან, თანამგზავრებისგან, კომპიუტერებისაგან და ნებისმიერი სხვა დაკავშირებული ტექნიკისგან. გლობალური ინტერნეტკავშირების დიდი პროცენტი წყალქვეშა კაბელებით გადის, რაც შეეხება ისრაელის ინტერნეტკავშირებს, იგი დაუცველი წყალქვეშა ოპტიკურ-ბოჭკოვანი კაბელებით და პრობლემური სატელიტური კვშირებით არის ცნობილი. ამ შემთხვევაში კაბელების დაზიანება, გაჭრა და ასევე მოსმენაც შესაძლებელია, ხოლო დაზიანების გამოსწორება რთულ საკითხს წარმოადგენს *(სპეციალური გემებისა და აღჭურვილობის საშუალებით).* თანამგზავრების გაფუჭების შემთხვევაში, იქიდან გამომდინარე, რომ მათი გარემონტება რთულ და ამავდროულად ძვირ სიამოვნებას წარმოადგენს, ახალი იქნება საჭირო. ასეთი დაზიანებები ქვეყნისთვის მნიშვნელოვანი საკითხია - იგი გათიშული იქნება დანარჩენი სამყაროსგან და ალტერნატიული ვარიანტი, რომელიც არსებობს, ეს მხოლოდ სხვა ტიპის კომუნიკაციაა, ეს არის რადიოსიხშირე.

ცნობილია, რომ ჰაიფასა და თელ-ავივის მახლობლად მხოლოდ ორი ზღვიდან შემოდის სანაპიროს ზოლის გავლით ინტერნეტპორტი, რომელიც მთელი ქვეყნის მასშტაბით ნაწილდება და გაშლილია რამდენიმე სახმელეთო კაბელით. აქ დიდი რისკი არსებობს, მტრულად განწყობილმა უცხო ძალებმა შეიძლება მარტივად მოწყვიტონ ისრაელი ინტერნეტიდან და დახურონ მისი სოციალურ-ეკონომიკური საქმიანობის უმეტესი ნაწილი. კარგად დაგეგმილმა კიბერშეტევებმა შეიძლება დიდი ზეგავლენა მოახდინოს ისრაელის ბაზარზე და საზოგადეობაზე. როგორც უკვე აღვნიშნეთ, ასევე შესაძლებელია, მანიპულაციები და კომუნიკაციების მოსმენაც, მით

[60] *Bigelow J., S., Montgomery J., "ITIL (Information Technology Infrastructure Library)", Techtarget, p. 1, https://www.techtarget.com/searchdatacenter/definition/ITIL*

უმეტეს, ფაქტები, რაც ზევით მოვიყვანეთ, ამყარებს ეჭვებს, რომ უცხო წყალქვეშა ნავები ხშირად იმალებიან წყალქვეშა კაბელების სიახლოვეს. ასეთი სცენარის განხორციელების შემთხვევაში, სამხედრო კიბერსივრცე ნაკლებ ზიანს მიიღებს, რადგან იგი დიდწილად იყენებს სატელიტურ კომუნიკაციებს, ან დახურულ ქსელებს, მაგრამ სამოქალაქო საზოგადოება მნიშვნელოვნად დაზარალდება. შემდეგი არის ლოგიკური, შეიძლება მას ლოგიკური ფენაც ვუწოდოთ, რომელიც ერთგვარად კობერსივრცის ცენტრალურ ნერვულ სისტემას წარმოადგენს. იგი პასუხისმგებელია ინფორმაციის გადამისამართებაზე სხვასასხვა საკომუნიკაციო პროტოკოლების მეშვეობით, მომხმარებლებიდან სერვერებზე და სერვერებიდან მომხმარებლებზე. აღნიშნული ე.წ. ფენის დაუცველობა ძირითადად ირღვევა ***DDoS*** შეტევების გამოყენებით. მაგალითად, 2013 წლიდან დეცენტრალიზირებული ჰაქტივისტური დაჯგუფება ***„ანონიმუსი“*** ხშირად ***DDoS*** შეტევებით ესხმის თავს ისრაელის ვებ-გვერდებს. მათ შორის, ამ წიგნში განხილული გვაქვს ისეთი ჰაქტივისტური დაჯგუფებები, როგორებიც არიან ***„ანონიმური სუდანი“*** და ***Killnet-ი,*** ისინიც ახორციელებენ ისრაელის ვებ-გვერდებზე და სხვადასხვა სახელმწიფო სისტემებზე ჰაკერულ თავდასხმებს სახელწოდებით ***#OpIsrael.*** აღნიშნული თავდასხმები წარმოადგენს ერთგვარ კამპანიას მათი მხრიდან. ასეთი თავდასხმები ბლოკავს და ზიანს აყენებს კიბერსივრცის სამოქალაქო დომენს, ანუ თავდასხმები ხორციელდება საჯაროდ ხელმისაწვდომ სამთავრობო თუ ბიზნესის წარმოების ვებ-გვერდებზე, რომლებსაც ისრაელის მოქალაქეები იყენებენ.

მესამე - ეს გახლავთ ინფორმაცია. შეგვიძლია, მას ინფორმაციის ფენა ვუწოდოთ, რომელიც მოიცავს ისეთ ამბებს, რომელიც არის მაგალითად: აუდიო, ვიდეო, ფოტო და ნებისმიერი სხვა სახის შენახული მონაცემები. ე.წ. ფენის დაუცველობა არის ის, რომ შესაძლებელია ინფორმაციის გაჟონვა, გაყალბება ან მანიპულირება. მსგავსი მაგალითები მსოფლიო მასშტაბით უამრავი გვაქვს. ინფორმაციული ფენა ღრმად არის დაკავშირებული მომხმარებელთან. მომხმარებელი ეს კიდევ ერთი კომპონენტია ამ ოთხი საკითხიდან. იგი აყალიბებს კიბერსივრცის მთელ გამოცდილებას. როგორც კიბერექსპერტები განიხილავენ, მომხმარებლები იყოფიან ორ ჯგუფად - არიან სისტემატიური, მშვიდობიანი, არასახიფათო და არიან კრიმინალი, ტერორისტი ან უცხო სახელმწიფოს აგენტი მომხმარებლები. მანიპულაციური მომხმარებლები, რომლებიც იყენებენ

კიბერსივრცეს დანაშაულის, ტერორის და დეზინფორმაციული კამპანიის საწარმოებლად, არიან საფრთხის შემცველნი, რადგან მათ შეუძლიათ მოიპოვონ ინფორმაცია და გადაიტანონ საზოგადოების ყურადღება, შეეცადონ გარკვეული ნაწილის აზრის შეცვლას, რაც ხშირ შემთხვევაში გამოსდით კიდეც. რაც შეეხება უშუალოდ ისრაელს, ბოლო წლებში ეს ქვეყანა დაქვემდებარებულია ფართო გავლენის კამპანიას, რაც არა მხოლოდ მისი უშუალო მოწინააღმდეგეების მხრიდან მოდის - ირანის ისლამური რესპუბლიკა და სხვადასხვა ტერორისტული ორგანიზაციები, არამედ სხვა გლობალური ძალების მხრიდანაც. მაგალითად, ჩინეთის, რუსეთისა და სხვა დასავლური ქვეყნების მხრიდანაც. ისინი ცდილობენ ებრაული საზოგადოებრივი აზრის შეცვლას თავიანთი მიზნების მისაღწევად. სათანადო რეაგირების არარსებობა და ბიზნესის შესახებ არასაკმარისი რეგულაციები ისრაელის მოქალაქეებს უფრო მეტად დაუცველს ხდის კიბერსაფრთხეების მიმართ. ექსპერტების განმართებით, თუ ისრაელს უნდა, კიბერთავდაცვითი პოტენციალი გაზარდოს, უსაფრთხოების რეგულირება სტანდარტად უნდა აქციოს ბიზნესსა და სხვა ინსტიტუტებს შორის, რომლებიც ყველა ქვეყანაში ამუშავებენ დიდ ინფორმაციას. ისრაელმა უნდა მიბაძოს ისეთ ქვეყნებს, როგორებიც არის ესტონეთი, ფინეთი, დანია და სხვა. ისეთ ქვეყნებს, რომელთაც აქვთ კიბერუსაფრთხოების მხრივ ვრცელი საგანმანათლებლო პროგრამები, რომლებიც მიზნად ისახავენ გაზარდონ ციფრული არეალი, მათ შორის მოზარდებში. მოზარდს შეიძლება არ შეეძლოს ანტივირუსების, თავდაცვითი ან თავდასხმითი სტრატეგიების შექმნა, მაგრამ მარტივად მოახდინოს იდენტიფიცირება ონლაინ თაღლითობის, ფიშინგის სხვადასხვა ფორმების გამოყენების მცდელობები. კიბერუსაფრთხოებისთვის კიდევ უფრო მეტია საჭირო, ისრაელმა უნდა გაზარდოს ინვესტიციები, განაახლოს ინფრასტრუქტურა, რაც ხელს შეუწყობს კაბელების დაზიანების რისკებს, უფრო რთული გახდება მათი დაზიანება.

მიუხედავად იმისა, რომ ისრაელს ბევრი კიბერსისუსტე და პრობლემა აქვს, მაინც მიჩნეულია ტოპ კიბერძალად მსოფლიო მასშტაბით. რა შეიძლება ითქვას ამაზე? როგორ მოახერხა ისრაელმა, რომ იგი მსოფლიომ მიიჩნია ერთ-ერთ მოწინავე კიბერძალად? ამაზე პასუხი მარტივია, თუკი თვალს გადავავლებთ წარსულ მოვლენებსა და მაგალითებს, რაც წლების განმავლობაში ისრაელმა აკეთა კიბერსივრცეში, დავრწმუნდებით, რომ აწარმოა დახვეწილი კიბერკამპანიები

მოწინავე საფრთხისშემცველი ქვეყნის წინააღმდეგ, მოახერხა და ირანის ისლამური რესპუბლიკის ბირთვული პროგრამის შეფერხება გამოიწვია. *"ისრაელი კიბერუსაფრთხოების სიდიდით მსოფლიოში მეორე ადგილს იკავებს, 500 უმსხვილესი გლობალური კიბერუსაფრთხოების კომპანიებიდან 12% ისრაელშია წარმოდგენილი, იგი სან-ფრანცისკოს მეტროპოლიტენის შემდეგ მეორეა (32%). ცნობილია, რომ 2014 წელს ისაელის სამოქალაქო კიბერუსაფრთხოების ექსპორტი საშურ აღემატებოდა გაერთიანებული სამეფოს ექსპორტს".*[61] *"**Google-ი** და **Microsoft-ი** 2014 წლიდან იყვნენ ყველაზე აქტიური კორპორატიული მყიდველები ისრაელში, რომელთაც ოცამდე კომპანია შეიძინეს".*[62] ასევე ისრაელში იქმნება სხვადასხვა სახის აპარატურა, რომლებსაც ქმნიან ისეთი მეგაკომპანიები, როგორებიც არის: ***Google, Nividia, Amazon, Apple, Broadcom*** და სხვა. მათ შორის ***Intel-ი*** ათწლეულების განმავლობაში აპროექტებდა პროცესორებსა და სხვა სახის ჩიპებს ისრაელში.

ისრაელის ტექნიკური სექტორი სპეციალიზებულია მაღალი დონის ინოვაციურ კვლევებში და განვითარებად ციფრულ გლობალურ ეკონომიკაში. ებრაელი მეცნიერები და ექსპერტები მუშაობენ ისრაელში, მაგრამ მათი დამსაქმებლები, პარტნიორები, სამიზნე ბაზრები და ინვესტორები უცხოელები არიან. რთული იქნება მრავალეროვანი კორპორაციის დასახელება, რომელსაც არ აქვს ***R&D***[63] ლაბორატორია ისრაელში. ცნობილია, რომ 2019 წელს ისრაელმა მოიზიდა გლობალური კერძო კიბერუსაფრთხოების ინვესტიციების მეხუთედი.

სტრატეგიული კვლევების საერთაშორისო ინსტიტუტი (IISS) თავის კვლევებში შვიდი კატეგორიის მიხედვით, რომელიც მოიცავს წამყვან უპირატესობებს კიბერტექნოლოგიებში მსოფლიო მასშტაბით, *"ისრაელს მეორე ადგილზე ასახელებს,*

---

[61] *Solomon S., "Israel wins second-largest number of cybersecurity deals globally", p. 1, 2018, https://www.timesofisrael.com/israel-nabs-second-largest-number-of-cybersecurity-deals-globally/*

[62] *Orbach M., Shulman S., "The 50 most promising Israeli startups - 2023", p. 1, 2023, https://www.calcalistech.com/ctechnews/article/hjtwkugx2*

[63] *R&D ლაბორატორია, არის ლაბორატორიული ტიპი, რომელიც გამოიყენება პრაქტიკულად ყველა საწარმოო ინდუსტრიაში. ამ ლაბორატორიებში დიდ ყურადღებას უთმობენ პროტოტიპების შექმნას და ექსპერიმენტების ჩატარებას, შეიძლება ითქვას, რომ არსებობს ისინი ხელს უწყობენ შიდა ინოვაციებსა და გამოგონებებს.*

ზოგიერთ შემთხვევაში კი, ჩინეთის, რუსეთის, დიდი ბრიტანეთისა და საფრანგეთის გვერდით მოიაზრებს".[64] ინსტიტუტი განმარტავს, რომ ისრაელი განსაკუთრებით ძლიერია კიბერდაზვერვითი მიმართულებით, ასევე დახვეწილია შეტევით კიბერშესაძლებლობებში.

ისრაელმა ჩამოაყალიბა ეროვნული კრიტიკული ინფრასტრუქტურის დაცვის ***(CIP)***[65] სისტემა. 2010 წელს წამოიწყო ეროვნული კიბერინიციატივა სახელწოდებით: *,,ისრაელმა უნდა შეინარჩუნოს თავისი პოზიციები მსოფლიო მასშტაბით, იგი უნდა იყოს, როგორც საინფორმაციო-ტექნოლოგიური განვითარების ცენტრი, გაითვალისწინოს ზესახელმწიფოების შესაძლებლობები კიბერსივრცეში. უზრუნველყოს თავისი ტექნოლოგიური, ფინანსური და ეროვნული მდგრადობა, როგორც დემოკრატიულმა ქვეყანამ, ცოდნაზე დაფუძნებულით და საზოგადოების ღია ჩართულობით".* გამოვლენილი რისკები და შესაძლებლობები 2011 წლის მთავრობის რეზოლუციაშია წარმოდგენილი - *No. 3611 „ეროვნული კიბერსივრცის შესაძლებლობების განვითარება"* - ეროვნული სტრატეგია.

CIP-ის გარდა, ისრაელიში ფუნქციონირებს სამოქალაქო, სამთავრობო კიბერუსაფრთხოების ორგანიზაცია: ისრაელის ეროვნული კიბერდირექცია ***(INCD).*** კიბერუსაფრთხოების სააგენტოებისგან განსხვავებით, მას არ აქვს სამართალდამცავი ან სადაზვერვო მისია. მისი არსებობა მიზნად ისახავს, შეამციროს დაძაბულობა ძირითად თავისუფლებებსა და უსაფრთხოებას შორის, რაც იწვევს თავდაცვის დაწესებულების დიდ უკმაყოფილებას. 2013 წლიდან სნოუდენის გაჟონვამ, რომელიც გამოავლინა მრავალი გლობალური სათვალთვალო პროგრამა,

[64] *Topwar, "British experts from IISS named 15 countries with maximum cyber capabilities", p. 1, 2021, https://en.topwar.ru/184530-britanskie-jeksperty-iz-iiss-nazvali-15-stran-s-maksimalnymi-kibervozmozhnostjami.html*

[65] Forcepoint, "What Is Critical Infrastructure Protection (CIP)?", p. 1, https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip

გააძლიერა საქმე მკაცრად სამოქალაქო კიბერუსაფრთხოების სააგენტოსთვის. ცხრა წელიწადში ***INCD-ის*** პასუხისმგებლობა სამოქალაქო კიბერუსაფრთხოებაზე გაიზარდა პოლიტიკისა და შესაძლებლობების ჩამოყალიბებიდან ინფორმაციის გაზიარებამდე, ყოველდღიური კიბერთავდაცვის ოპერაციებით კომპიუტერული სასწრაფო დახმარების ჯგუფის ***(CERT-IL)*** და ***CIP-ის*** მიერ.

რუსეთის ფედერაცია

რუსეთის ფედერაცია ევრაზიული ქვეყანაა. იგი 83 ფედერაციული სუბიექტისგან შედგება. ცნობილია, რომ სახმელეთო საზღვრით რუსეთი ყველაზე დიდია მსოფლიოში. მას დასავლეთით ესაზღვრება ევროპული სახელმწიფოები - ფინეთი, ნორვეგია, ესტონეთი, ლატვია, ლიეტუვა და პოლონეთი. ეს ორი სახელმწიფო რუსეთის მხოლოდ ერთ ადმინისტრაციულ სუბიექტს - კალინინგრადის ოლქს ესაზღვრება, რაც ერთგვარ საშიშროებას წარმოადგენს მათთვის. რუსეთს ასევე ესაზღვრება საქართველო, აზერბაიჯანი, უკრაინა, ბელორუსი, ჩინეთი, ჩრდილოეთ კორეა, მონღოლეთი და ყაზახეთი. რეალურად მას დადგენილი, ოფიციალური საზღვარი არ გააჩნია როგორც ამერიკის შეერთებულ შტატებთან, ასევე იაპონიასთან. ეს ორი ქვეყანა რუსეთს ზღვით *(იაპონიასა და რუსეთს შორის ოხოტის ზღვა, ხოლო რუსეთსა და ამერიკის შეერთებულ შტატებს შორის ბერინგის სრუტე)* ემეზობლება.

რუსეთის იმპერიის დამხობის შემდეგ მის მთელ ტერიტორიაზე ჩამოყალიბდა საბჭოთა კავშირი, რომელშიც შემდგომ 15 რესპუბლიკა გაერთიანდა. მეორე მსოფლიო ომმა რუსეთზე დიდი გავლენა მოახდინა, 1991 წელს სსრკ-ის დაშლის შემდეგ რუსეთი დამოუკიდებელი ქვეყანა გახდა. თავდაპირველად ბევრი პრობლემა ჰქონდა, მაგრამ თანდათანობით ეკონომიკამ განვითარება დაიწყო. თუმცა რუსეთის

შეჭრამ უკრაინაში იგი ეკონომიკური თვალსაზრისით ძალიან დააზიანა *(სანქციები, სამხედრო რესურსი, ფინანსები ომისთვის).*

ვლადიმერ პუტინმა 2007 წლის მიუნხენის უსაფრთხოების კონფერენციაზე კრიტიკული განცხადებები გააკეთა ერთპოლუსიანი სამყაროს იდეის, აშშ-ის საგარეო პოლიტიკისა და აღმოსავლეთ ევროპაში, ჩრდილო-ატლასნტიკური ალიანსის გაფართოების შესახებ, რომელსაც, შეიძლება ვთქვათ, შესაბამისი ყურადღება არ მიექცა დასავლეთის მხრიდან. პუტინის აგრესიული ამბიცია, მას მერე რაც მან *„შეძლო“* ჩეჩნური პრობლემის გადაჭრა, უკვე ევროპის ენერგოდამოკიდებულების ხაფანგში გახვევა გახლდათ, რაც მან საკმაოდ წარმატებულად განახორციელა. შემდეგ მნიშვნელოვანი იყო, არავითარ შემთხვევაში არ დაეშვა ნატო-ს შემდგომი გაფართოება აღმოსავლეთით, რასაც იგი ასევე წარმატებით წარმოაჩენდა, როგორც რუსეთის სასიცოცხლოდ მნიშვნელოვან საფრთხედ. შესაბამისად, მის მთავარ ამოცანად უკვე ძალის დემონსტრირება გახდა, რომელიც რუსეთის ფედერაციის მიერ, როგორც მოსკოვში, წითელ მოედანზე გამართულ პომპეზურ სამხედრო აღლუმებზე, ასევე პერიოდულად უცხო ქვეყნის საჰაერო სივრცის დარღვევით გამოიხატებოდა. პუტინის თავხედობის უფრო მაღალი გამოვლინება ჯერ საქართველოში 2008 წლის აგვისტოში შეჭრა და 2014 წელს ყირიმის ნახევარკუნძულის ანექსია გახლდათ. ეს ერთგვარი ტესტი იყო ევროპისთვის და ამერიკის შეერთებული შტატებისთვის, რომლებიც ამ ფაქტებს, როგორც აღმოჩნდა, საკმაოდ სერიოზულ საფრთხეს მხოლოდ *„ტრადიციული“ „აღშფოთება-შეშფოთებით“* დაუპირისპირდნენ. დღის წესრიგში, რუსეთის მიერ ახალი ავანტიურის საკითხი დადგა: გათამამებული იმით, რომ საერთაშორისო სამართლის დარღვევას რეალურად წინ არაფერი და არავინ უპირსპირდებოდა, რუსეთის ლიდერმა პუტინმა, ამჯერად უკრაიაში შეჭრის გადაწყეტილება მიიღო. მიუხედავად იმისა, მსოფლიოს სხვადასხვა ლიდერები ონლაინ ჩართვით თუ პირადად მასთან ვიზიტის დროს ლამის ემუდარებოდნენ, ეს არ გაეკეთებინა, პუტინმა ეს გადაწყვეტილება მაინც მიიღო. მანამდე გაითამაშა უშიშროების საბჭოს სხდომაზე სპექტაკლი, რითაც თითქოს აჩვენა, რომ რუსეთის უმაღლესი პოლიტიკური თანამდებობის პირები, არათუ ერთსულოვნად ეთანხმებოდნენ მის გადაწყვეტილებას, არამედ, ლამის სთხოვდნენ კიდეც უკრაინაში შეჭრას (ერთადერთი, ვინც ხმისკანკალით ნახევრად შეეწინააღმდეგა, საგარეო დაზვერვის უფროსი ნარიშკინი გახლდათ. თუმცა მალევე დატუქსული იქნა თავად

ვლადიმერ პუტინის მიერ). რა იყო ძირითადი მიზეზი, რამაც რუსეთის ლიდერს უკრაინაში შეჭრა გადააწყვეტინა? სხვდასხვა ვერსიებს შორის უფრო რეალურად, რამდენიმე მიგვაჩნია:

• ვლადიმერ პუტინს სურდა, მოარული მითი რუსეთის არმიის უძლეველობის შესახებ, კიდევ უფრო განემტკიცებინა;

• მან მშვენივრად იცოდა, რომ უკრინა უახლოეს მომავალში ნატო-ს წევრი ვერ გახდებოდა (ამის შესახებ მას საფრანგეთის პრეზიდენტმა ემანუელ მაკრონმა და გერმანიის კანცლერმა ოლაფ შოლცმა პირადად მოსკოვში ვიზიტის დროს განუცხადეს), მაგრამ მას თითქოს სურდა არამარტო უკრაინელების ცნობიერებიდან განედევნა ევროატლატიკური აზრები, არამედ ამით სხვებსაც დააშინებდა;

• რუსეთის იმიჯს და სიძლიერეს კიდევ ერთხელ დაინახავდა მსოფლიო, შესაბამისად დაინახავდა აშშ-ისა და ნატოს სისუსტეს;

• მიუხედავად იმისა, რომ შესაძლო სანქციებს ელოდა რუსეთის წინააღმდეგ, პუტინს არ სჯეროდა, რომ ომი დიდხანს გასტანდა, შესაბამისად, ,,გამარჯვებულებს არ ასამართლებენ'' პრინციპით, ამ სანქციებსა ყველა დაივიწყებდა.

საინტერესოა, რომ ომის საწყის ეტაპზევე წინ წამოიწია რეალური აქტორების თემამ, ზოგიერთმა სახელმწიფომ და ლიდერმა უპირობოდ მხარი დაუჭირა უკრაინას, ზოგიც მერყეობდა, თუმცა ყველაზე საინტერესოდ მაინც ჩრდილოატლანტიკური ალიანსი გამოჩნდა.

მიუხედავად იმისა, რომ ბევრი სხვა მოსაზრება არსებობს, კომპეტენტური თუ არაკომპეტენტური რუსეთთან მიმართებაში უფრო მნიშვნელოვან საკითხებზე უნდა გავამახვილოთ ყურადღება - მაგალითად:

- *რუსეთისა და მისი პრეზიდენტის ქცევა რომ გავიგოთ (და არა გავუგოთ ან ვუთანაგრძნოთ), უნდა გავიხსენოთ, რა არის რუსეთის გეოპოლიტიკური სახელმწიფო და ეროვნული ინტერესები;*
- *რომელი ქვეყნის მთავარი სამართალმემკვიდრეა რუსეთი;*
- *კარგად შევხედოთ, რა მმართველობის სტილია დღეს რუსეთში (აქ დემოკრატიული სახელწიფოს ჩამოყალიბებაზე ბევრს ნუ ვიოცნებებთ!);*
- *როგორც პოლიტიკური ლიდერი, ვინ მართავს და დგას ამ ქვეყნის სათავეში (სისულელები იმის შესახებ, დღეს მოქმედი რუსული ოპოზიციიდან ვინმე უკეთესი*

იქნებოდა, დავივიწყოთ. მათთაც იგივე „ველიკოდერჟავული“ ამბიციები გააჩნიათ, უბრალოდ მასშტაბები არა აქვთ შესაბამისი);

- *როგორია ამ ხალხის მენტალიტეტი და დამოკიდებულება სხვა ქვეყნებისა და ხალხების მიმართ (ისტორიას გავეცნოთ);*
- *რამდენად განვითარებულია ეკონომიკურ-სოციალური თვალსაზრისით ეს ქვეყანა (პოტენციალი უზარმაზარი აქვთ, თუმცა ხელისშემშლელი მიზეზების ჩამოთვლა ძალიან შორს წაგვიყვანს);*
- *თამაშობს თუ არა რეალურად სერიოზულ როლს სახლმწიფოს მართვაში მართლმადიდებული რელიგია (აქაც ერთმორწმუნეობაზე და მსგავს სუსტ არგუმენტებს ვერ მივიღებთ - უკრაინას რომ თავი დავანებოთ, საქართველოში ავტოკეფალიის გაუქმება გავიხსენოთ);*

არ და ვერ ხდება უკრაინა ნატოს წევრი და რუსეთმა ეს იცოდა ომამდეც. ცხადია, ამ ომის გასასამართლებელ საბაბად არ გამოდეგება, მაგრამ ალბათ უფრო იმაზე უნდა ვიფიქროთ, როდის შეიძლება შეჩერდეს პუტინი და შეწყვიტოს ომი. მისთვის მთავარია, არ გამოჩნდეს დამარცხებულად. მეტიც, თავი გამარჯვებულად გამოაცხადოს.

ომის მნიშვნელოვანი საკითხები:

- *ყირიმის საკითხი - რუსეთი ღიად აცხადებს, რომ ყირიმს არ დათმობს, იმავეს ამბობს უკრაინაც.*

• დე ფაქტო, ყირიმი რუსეთის შემადგენლობაშია, დე იურე - უკრაინის. ყოველ შემთხვევაში, რუსეთს შეიძლება ამ საკითხის ასე გაიყინვა კიდეც აწყობს.

• დასავლეთი ყირიმს არ აღიარებს, რუსეთი კი ამის შესახებ ნაკლებად ინერვიულებს, ყოველ შემთხვევაში, იმაზე მეტად არა, ვიდრე მანამდე.

- *ლუგანსკი და დონბასი რუსეთის მიერ აღიარებული რესპუბლიკებია, დე იურე - უკრაინის შემადგენელი ნაწილები:*

• რუსეთისთვის, უკრაინას ტერიტორიები დაუბრუნოს, ჰოლიტიკურად მომაკვდინებელი იქნება, ყოველ შემთხვევაში, დღეს ის ასე ფიქრობს.

• შეიძლება მსჯელობა, ფართო ავტონომიის ფარგლებში უკრაინის შემადგენლობაში დატოვებაზე, ძნელია, მაგრამ შეუძლებელი არაფერია.

• დე ფაქტო, რუსეთის მიერ დამოუკიდებლობა აღიარებულად დარჩნენ, დე იურე - უკრაინის შემადგენლობაში. შეიძლება ეს საკითხი ასე გაიყინოს.

• შესაძლოა, ლუგანსკსა და დონბასში აუცილებელი გახდეს საერთაშორისო სამშვიდობო კონტინგენტის განლაგება, სავარაუდოდ, გაეროს ეგიდით. რომელი ქვეყნების წარმომადგენლები იქნებიან მომავალი მშვიდობისმყოფელები, ძალიან სადაო თემა იქნება.

- *მოლაპარაკებისა და ცეცხლის შეწყვეტის ერთ-ერთ მიბმულ საკითხად დადგება საერთაშორისო სამშვიდობო კონტინგენტის განლაგება უკრაინა-რუსეთის ცეცხლის შეწყვეტის ხაზზე. ისევ და ისევ, სავარაუდოდ, გაეროს ეგიდით. აქაც, თუ რომელი ქვეყნების წარმომადგენლები იქნებიან მომავალი მშვიდობისმყოფელები, ისევ სადაო თემა იქნება.*

• ომი შეიძლება „ჩამოყალიბდეს“ ე.წ. გაყინულ კონფლიქტად, რომლის გადაჭრას შეიძლება წლები დასჭირდეს, დღეს რუსეთისთვის ესეც მომგებიანია.

• რამდენად აწყობს ომის რაღაც შედეგით დასრულება რუსეთს, ეს მეორე თემაა, დამოკიდებულია იმაზე, თუ ვინ უფრო კარგად წარმოაჩენს თავის თავს გამარჯვებულად თავის ქვეყანაში.

- *სანქციების დაწესებამ რუსეთისთვის ამ ეტაპზე მომაკვდინებელი შედეგი ვერ გამოიღო.*
- *სამხედრო (მათ შორის ლოჯისტიკურმა) და სადაზვერვო ხასიათის შეცდომებმა, რუსეთი აიძულა, პირვანდელი გეგმა შეეცვალა. ამჯერად გადაჯგუფების სტადიაშია და გადამწყვეტი ბრძოლებისთვის ემზადება;*

• დასავლეთიც შეიძლება დაინტერესებული იყოს მოვლენების ასეთი განვითარებით, მინიმუმ, ეს დრო მათთვის შესაფერისი იქნება ან რუსეთის ენერგოდამოკიდებულებისაგან გასათვისუფლებად, ან უბრალოდ რუსეთთან ურთიერთობების საბოლოოდ გადასახედად, სულაც დასალაგებლად.[66]

<u>მოლაპარაკების საბოლოო შედეგისთვის დიდი მნიშვნელობა ექნება:</u>

• რამდენად წინ წაწევას შეძლებს რუსეთი საბრძოლო მოქმედებებით უკრაინის ტერიტორიაზე;

[66] *ნიკოლეიშვილი ლ., „რუსეთ-უკრაინის ომის დასრულების შესაძლო სცენარები“, სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემია, გორი, 5-8 გვ. 2022.*

• რამდენი ხანი შეძლებენ უკრაინელები თავდაცვას და მეტიც, შეძლებენ მაქსიმუმ კონტრშეტევაზე გადასვლას, ან მინიმუმ - უკვე დაკარგული ტერიტორიების უკან დაბრუნებას;

- *დასავლეთისთვის მნიშვნელოვანია რუსეთს არ მისცენ გამარჯვების საშუალება, ამისთვის შესაძლებლობის ფარგლებში თითქოს ყველაფერს აკეთებენ.*

• მაგრამ ბევრ საკითხთან მიმართებაში ცალკეული ბზარების გაჩენამ და რუსეთზე კვლავ ენერგოდამოკიდებულებამ, რუსეთს, შეიძლება ითქვას, სითამამე შემატა.

• ასევე, მნიშვნელოვანია, დასავლეთის ერთსულოვნების შენარჩუნება და უკრაინიდან მიღებულ ლტოლვილთა მზარდი ნაკადების პრობლემების დარეგულირება;

• ეკონომიკური პრობლემების და ფასების ზრდა სერიოზულ დარტყმას აყენებს როგორც ევროპის მოსახლეობას, ასევ რუსეთს. რომელი მოსახლეობა აღმოჩნდება უფრო „გამძლე“, ამას დრო გვაჩვენებს.

- *ნატომ (გთხოვთ მის წევრ ქვეყნებს, ცალკე ნუ ავურევთ, ჩვენ ვამბობთ ამ ორგანიზაციაზე) შეძლო კონფლიქტში არჩართვა. ალიანსის საზღვრებიც ხელშეუხებელია, ეს იცის რუსეთმაც და ეს იციან წევრმა სახელმწიფოებმაც, მათ საკმაოდ სერიოზული თავდაცვისა და უსაფრთხოების ფარი გააჩნიათ. ერთადერთი ინსტრუმენტი, რაც მის წინააღმდეგ გამოყენებული შეიძლება იქნას, ეს ბირთვული შეიარაღებაა. ჯერჯერობით რუსეთის მხრიდან მხოლოდ ბირთვული შეიარაღების შესაძლო გამოყენების მუქარას ჰქონდა ადგილი, იმედია, ამის იქით არავინ წავა. მარტო ნატოს ტერიტორიაზე სამი სახელმწიფოს (აშშ, დიდი ბრიტანეთი, საფრანგეთი) ბირთვული შეიარაღებაა, და ეს აღარ იქნება შესაძლო მესამე მსოფლიო ომი, არამედ იქნება მსოფლიო კატასტროფა.*

ბოლოს, ყველაფერი დამოკიდებულია იმაზე, რომელ გეოგრაფიულ ადგილზე შეჩერდებიან ომის აქტიურ ფაზაში მოწინააღმდეგები, ვის ექნება უფრო მეტი ტერიტორიული უპირატესობა, რათა შეთანხმების ხელმოწერისას უფრო მეტი თავისი პირობების კარნახი და ზეწოლა შეძლონ. თუმცა სავსებით შესაძლებელია, ომი უფრო ხანგრლივად გაგრძელდეს. ცხადია, არ უნდა გამოვრიცხოთ სხვა სცენარებიც, რომლებიც სიტუაციისა და გარემოებების მიხდევით იქნება ნაკარნახევი.

- *რუსეთმა მიაღწია იმას, რომ უკრაინა ნატოს წევრი ვერ გახდება, თუმცა სხვა ქვეყნებს, ისეთებს, როგორებიც შვედეთი და ფინეთია, გაუჩინა ჩრდილოატლანტიკური ალიანსის წევრობის სურვილი.*
- *მითი იმის შესახებ, რომ რუსეთის არმია უძლეველია, შეიძლება ითქვას, დაინგრა - რუსეთი საუკეთესო ძალებსა და რესურსს ხარჯავს უკრაინაში წარმატების მისაღწევად. პუტინმა ვერ მიაღწია პირველად ამოცანებს, ერთადერთი, რაც შეუძლია თქვას, რომ ომი არა მის, არამედ სხვის ტერიტორიაზე მიმდინარეობს, ინარჩუნებს ყირიმს, იბრძვის დონეცკისა და ლუგანსკის „დასაკანონებლად.“*
- *რუსეთის დღევანდელ ხელისუფლებას აუცილებლად მოუწევს, გადახედოს თავის როგორც საგარეო, ასევე საშინაო პოლიტიკას. ჩვენ რაიმე სახის ცვლილებებს საგარეო მიმართულებით რუსეთის მხრიდან, არ ველოდებით. რაც შეეხება საშინაო პოლიტიკას, კერძოდ საკადრო პოლიტიკას, პუტინს მოუწევს მთელი რიგი ცვლილებების განხორციელება. რაც არ უნდა ლამაზად შეფუთოს ომის შემდგომი შედეგები, ფაქტია, უზარმაზარმა ხარჯებმა როგორც დაზვერვაში, ასევე სამხედრო სფეროში ვერ გაამართლა, რაც პირადი ერთგულების გამო დაწინაურებული კორუმპირებული ჩინოვნიკების „შროშის“ შედეგია. სავარაუდოდ, ვლადიმერ პუტინი მათ სიამოვნებით ხელსაც შეახოცავს და გაწირავს კიდეც. სხვათა შორის, ეს ნაბიჯი აუცილებლად გაზრდის მის რეიტინგს რუსეთის მოსახლეობაში. ასევე, ნაკლებად მოსალოდნელია, მაგრამ არსებობს მცირე შესაძლებლობა, თვითგადარჩენის მიზნით, ეს ხალხი შეეცადოს ჰირიქით მის გაწირვას.*
- *დროის ამბავია, როგორც კი რუსეთში ხელისუფლება ოდნავ შესუსტდება და დასავლეთი ამით აუცილებლად ისარგებლებს, რუსეთს მოუწევს უკრაინიდან უკან დახევა და ჯარების გაყვანა ისე, როგორც მოუწია თავის დროზე გერმანიიდან თუ ავღანეთიდან;*
- *გასაგებია რუსეთის გეოპოლიტიკური თუ ეროვნული ინტერესები, მაგრამ ამ სახელმწიფომ საბოლოოდ დაიმკვიდრა აგრესორი ქვეყნის სტატუსი, რაც იმას ნიშნავს, რომ მასთან ურთიერთობისას ნდობის საკითხზე მართებს დაფიქრება ნებისმიერ ქვეყანას.*

რუსეთის ფედერაციის კიბერშესაძლებლობები

რუსეთის ფედერაცია კიბერუსაფრთხოების მხრივ წარმოადგენს ერთ-ერთ წამყვან მოთამაშეს მსოფლიო მასშტაბით. შეიძლება ასეც ითქვას - კიბერშეტევებისა და კიმერომების წარმოების მიმართულებით, და არა კიბერუსაფრთხოების. ვერ ვიტყვით, რუსეთს თავდაცვითი მექანიზმები ისე აქვს განვითარებული, იოლად უმკლავდება სხვადასხვა ქვეყნებიდან წარმოებულ კიბერშეტევებს.

ვლადიმერ პუტინი

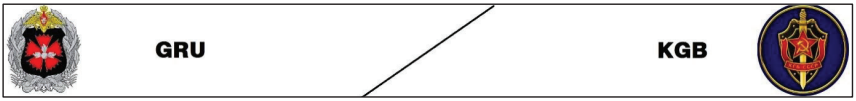
მაგალითისთვის შეგვიძლია მოვიყვანოთ რუსეთ-უკრაინის ომის დაწყების შემდგომ განვითარებული მოვლენები: *"2022 წლის 21 თებერვალს რუსეთის პრეზიდენტმა* ***ვლადიმერ პუტინმა*** *ხელი მოაწერა უკრაინის ორი სეპარატისტული რეგიონის - დონეცკისა და ლუგანსკის დამოუკიდებელ რესპუბლიკებად აღიარებას, შემდეგ კი ამ „რესპუბლიკებთან" სამშვიდობო, ანუ სამხედრო ხელშეკრულებები გააფორმა".*[67]

ამის შემდეგ ჰაკერებმა რუსეთში გატეხეს ვიდეოპლატფორმები ***Wink*** და ***IVI,*** რუსეთის რამდენიმე არხზე სერიალების ნაცვლად ეთერში გაუშვეს უკრაინაში დაბომბვების შესახებ ***„ნასტოიაშჩიე ვრემიასა''*** და ***„დოჟდის''*** ვიდეოები. *"ომის კადრების რუსულ არხებზე გაშვების შესახებ ჰაკტივისტურმა ჯგუფმა* ***„ანონიმუსმა" „ტვიტერზე"*** *დაწერა და ვიდეოც გაავრცელა".*[68] მართალია, რუსული არხების მაუწყებლობა მალევე აღდგა,

[67] *Euronews, "Vladimir Putin recognises Ukrainian separatist regions, in escalation of tensions", p. 1, 2022. https://www.euronews.com/2022/02/21/putin-dangles-donbas-recognition-as-tensions-in-eastern-ukraine-continue-to-rise*

[68] *Vishnu V. V., "Russia-Ukraine War: Anonymous Declares 'cyber War' Against Russia, Targets Govt Websites", Republic World, p. 1. 2022. https://www.republicworld.com/world-news/russia-ukraine-crisis/russia-ukraine-war-anonymous-declares-cyber-war-against-russia-targets-govt-websites-articleshow.html*

მაგრამ ეს მაინც დარჩა მძლავრ სიგნალად, რომ რუსეთი არც ამ სფეროშია უძლეველი. *„ანონიმუსმა“ ასევე დაჰკა „გაზპრომისა“ და რამდენიმე რუსული სამთავრობო უწყების ვებ-გვერდი“,*[69] საიდანაც მოიპოვეს ინფორმაცია რუსეთის აგენტების შესახებ, თუმცა არ გაუვრცელებიათ.



რუსეთის კიბერმართვისა და კონტროლის სისტემების წარმოშობა ჯერ კიდევ საბჭოთა პერიოდიდან დაიწყო. იმ დროს ორი სადაზვერვო უწყება მუშაობდა კოდების დაშიფრვისა და გატეხვის მიმართულებით - ***კგბ*** და ***გრუ.*** ორივე ერთდროულად აწარმოებდა უცხოური კომუნიკაციების თვალთვალს, გაშიფრვასა და ფოკუსირებული იყო რადიოსიგნალების იდენტიფიცირებაზე.

ასევე ცნობილია, რომ ***კგბ*** და ***გრუ*** აქტიურად ეძებდნენ და აგროვებდნენ ნიჭიერ ახალგაზრდებს სამოქალაქო უნივერსიტეტში, სადაც მათემატიკის პროგრამები - ფიზიკისა და მათემატიკის, მექანიკისა და მათემატიკის მიმართულებით ასწავლიდნენ. ეს სისტემა საბჭოთა კავშირის დაშლის შემდეგ გადარჩა. *“**კგბ-ს** რესტრუქტურიზაცია მოხდა 1991 წლის ბოლოს. განყოფილებები, რომლებიც პასუხისმგებელნი იყვნენ პარტიების უფროსებისთვის უსაფრთხო კომუნიკაციის უზრუნველყოფაზე, გადანაწილდნენ სამთავრობო კომუნიკაციის კომიტეტებში და ეწოდათ **FAPSI,** აღნიშნული მოდელი კი **ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სააგენტოს (NSA)** ანალოგი იყო. თუმცა **NSA-გან** განსხვავებით **FAPSI-ს** ასევე დაევალა საზოგადოებრივი აზრის გამოკითხვის ჩატარება, რა თქმა უნდა, მხოლოდ მთავრობისთვის. მოგვიანებით ისინი პასუხისმგებლები გახდნენ რუსეთის ციფრული არჩევნების უსაფრთხოებაზე”.*[70]

[69] *Trinko M., "Anonymous Hacked Gazprom and Leaked 768,000 Emails from Company Employees", Gagadget, p. 1. 2022. https://gagadget.com/en/116384-anonymous-hacked-gazprom-and-leaked-768000-emails-from-company-employees/*

[70] *Borogan I. Soldatov A. "The Dawn of a New Era: The Birth of the FSB," in The New Nobility: the restoration of Russia's security state and the enduring legacy of the KGB, New York, p. 13, 2011.*

ვლადისლავ შერსტიუკი

"FAPSI დაყოფილი იყო ექვს მთავარ განყოფილებად. ყველაზე მნიშვნელოვანი იყო მე-3 განყოფილება, რომელსაც ეწოდებოდა ***კომუნიკაციების ელექტრონული დაზვერვის მთავარი განყოფილება (GURRSS),*** *იგი პასუხისმგებელი იყო უცხოური ტელეკომუნიკაციების ჯაშუშობაზე. მე-3 განყოფილება გახლდათ* ***კგბ-ს*** *მე-16 განყოფილება. მისი ხელმძღვანელი 1995-1998 წლებში იყო* ***ვლადისლავ შერსტიუკი (Vladislav Sherstyk), კგბ-ს*** *ოფიცერი 1966 წლიდან, რომელმაც დაამთავრა მოსკოვის სახელმწიფო უნივერსიტეტის ფიზიკის ფაკულტეტი. მან ფაქტობრივად შეიმუშავა, როგორი უნდა ყოფილიყო რუსეთის კიბერპოლიტიკა. როდესაც* ***შერსტიუკმა*** *დაინახა სამხედრო მოქმედებები ჩეჩნეთის პირველ ომში, მან შეძლო ჩეჩნების კომუნიკაციების თვალთვალი* ***FAPSI-ის*** *სამუშაო ჯგუფის მეშვეობით, რომელსაც მაშინ თვითონ ხელმძღვანელობდა".*[71]

"1998 წელს ***FSB-ის*** *ცენტრალურ აპარატში შეიქმნა ახალი განყოფილება -* ***კომპიუტერული და ინფორმაციული უსაფრთხოების სამსახური (UKIB),*** *რომელიც ექვემდებარებოდა კონტრდაზვერვის უფრო დიდ დეპარტამენტს".*[72] **შეიძლება ითქვას, როგორც *FSB,* ასევე სამხედრო კიბერშესაძლებლობები დიდწილად დაჩრდილა *FAPSI-მ.***

"1990-იანი წლების დასაწყისში შეიქმნა კერძო კიბერკომპანიები - ყველაზე ძლიერი იყო ***Kaspersky Lab,*** *რომელიც დღემდე ფუნქციონირებს".*[73] **ცნობილია, რომ მისი მენეჯმენტი მუშაობდა *კგბ-სთვის.*** **ამ კომპანიის დირექტორმა *ევგენი კასპერსკიმ (Eugene***

[71] Borogran I. Soldatov A., "Putin's Overseas Offensive,", New York", PP. 225-227, 2017.
[72] Borogran I. Soldatov A., "Putin's Overseas Offensive,", New York", PP. 225-227, 2017.
[73] Graham L., "Lonely Ideas: Can Russia Compete?", MIT Press, p. 93, 2013.

Kaspersky) თავად დაამთავრა ***კგბ-ს*** უმაღლესი სკოლის მეოთხე განყოფილება. ალბათ 1998-1999 წლები იყო ყველაზე გავლენიანი პერიოდი ***FAPSI-ის*** ისტორიაში.

ევგენი კასპერსკი

*"1999 წლის მაისში **შერსტიუკი** გადაიყვანეს უშიშროების საბჭოს ხელმძღვანელის პირველ მოადგილედ. დეკემბერში დაინიშნა ინფორმაციული უსაფრთხოების განყოფილების თავმჯდომარედ. ეს გახდა მთავარი განყოფილება, სადაც შეუშავდა კიბერ და ინფორმაციული უსაფრთხოების კონცეფციები".[74]*

ანატოლი სტრელცოვი

ამ პროცესის ერთ-ერთი მონაწილე იყო ***ანატოლი სტრელცოვი, კგბ-ს*** ყოფილი პოლკოვნიკი. ***შერსტიუკსაც*** და ***სტრელცოვსაც*** ესმოდათ, რომ მათ სჭირდებოდათ კვლევითი დაწესებულება კიბერპოლიტიკურ საკითხებზე, რომელიც დაეხმარებოდა პოლიტიკური გადაწყვეტილებების მიღებაში. ამრიგად, *"**მოსკოვის სახელმწიფო უნივერსიტეტში** შეიქმნა განყოფილება **შერსტიუკისა** და **სტრელცოვის** მეთვალყურეობის ქვეშ, რომელიც მალე გახდა **ინფორმაციული უსაფრთხოების საკითხთა ინსტიტუტი.** ეს ინსტიტუტი წარმოიშვა, როგორც ძირითადი ანალიტიკური ცენტრი და განსაზღვრა რუსეთის საგარეო პოლიტიკა ინფორმაციული უსაფრთხოების მიმართულებით. 2000 წელს **შერსტიუკისა** და **სტრელცოვის** გუნდმა შეადგინა **დოქტრინა რუსეთის ფედერაციის ინფორმაციული უსაფრთხოების შესახებ,** რომელიც მოიცავდა საფრთხეების ფართო ჩამონათვალს. 1990-იანი წლებიდან 2000 წლამდე **FAPSI** და მასთან დაკავშირებული ოფიციალური პირები მართავდნენ და აკონტროლებდნენ რუსულ კიბერტექნოლოგიებს".[75]*

---

[74] *Soldatov A. Borogan I., "How Putin Tried to Control the Internet", Vice, p. 1, 2015. https://www.vice.com/en/article/gvyzn4/how-putin-tried-to-control-the-internet*

[75] *Russian Federation, "Information Security Doctrine of the Russian Federation September 2000", Ministry of Foreign Affairs, p. 1, 2000. https://info.publicintelligence.net/RU-InformationSecurity-2000.pdf*

2000 წელს რუსეთის ფედერაციამ მიიღო ***„ინფორმაციული უსაფრთხოების დოქტრინა“,***[76] რომლის მიხედვითაც გაფართოვდა ქვეყნის უმაღლესი საგანმანათლებლო დაწესებულებების სია, სადაც ახორციელებდნენ ტრენინგებსა და გადამზადებას ინფორმაციული უსაფრთხოების მიმართულებით.

*“2003 წელს დაიყო **FAPSI, FSB, SVR** და **FSO. FAPSI-ის** მე-3 განყოფილება, რომელიც პასუხისმგებელი იყო უცხოური ტელეკომუნიკაციების ჯაშუშობაზე, განაგრძომდა მუშაობას, როგორც **FSB-ის** მე-16 განყოფილება. გადანაწილების შემდეგ **SVR-ს** დაევალა, ჩამოეყალიბებინა სამეცნიერო ცენტრი სახელწოდებით **„დელტა“,** რომელის მიზანიც იქნებოდა კვლევების ჩატარება კიბერპოლიტიკაზე. ასეც მოხდა, 2004 წელს - **UKIB-ის** გადაერქვა სახელი და ეწოდა **FSB-ის ინფორმაციული უსაფრთხოების ცენტრი (TSIB).***

*2005 წელს **ქიმიისა და მექანიკის ცენტრალური სამეცნიერო კვლევითი ინსტიტუტი (TSNIIKHM)** გადავიდა **ტექნიკურ და ექსპორტის კონტროლის ფედერალურ სამსახურში“.***[77] ინსტიტუტმა იმ დროისთვის სამუშაო მასშტაბები გაზარდა კიბერტექნოლოგიების მიმართულებით, რათა დაეცვათ სახელმწიფო საიდუმლოება უცხო დაზვერვისგან ტექნიკური საშუალებებით. როგორც უკვე აღვნიშნეთ, ორი წლის შემდეგ ესტონეთი გახდა კიბერშეტევის მსხვერპლი, მიზეზი კი გახლდათ ის, რომ ესტონეთის მთავრობამ ქალაქ ტალინიდან მეორე მსოფლიო ომის მემორიალის აღების გადაწყვეტილება მიიღო. რუსეთის მხრიდან ამ დროს კიბერშეტევები განხორციელდა როგორც საჯარო, ასევე კერძო სექტორზე.

შემდეგ საქართველოს ჯერიც დადგა - 2008 წელს რუსეთმა საქართველოში შეჭრამდე ორი კვირით ადრე დაიწყო კიბერშეტევები. როგორც ესტონეთში, საქართველოშიც ***DDoS*** შეტევები იყო გამოყენებული, რათა დაეზიანებინათ და გამოერთოთ მთავრობის ვებ-გვერდები და ინფრასტრუქტურა. აღნიშნული შეტევები რუსეთ-საქართველოს ომის დროსაც და მის შემდეგაც აქტიურად მიმდინარეობდა. *“2010*

[76] *Российской Федерации, "Доктрина информационной безопасности Российской Федерации", 2000 г. N Пр-1895, https://base.garant.ru/182535/*
[77] *Bennett G., "FPS & FAPSI – RIP," Conflict Studies Research Centre, Occasional Brief No 96, PP. 1-2, 2003, https://www.files.ethz.ch/isn/96240/03_Mar_2.pdf*

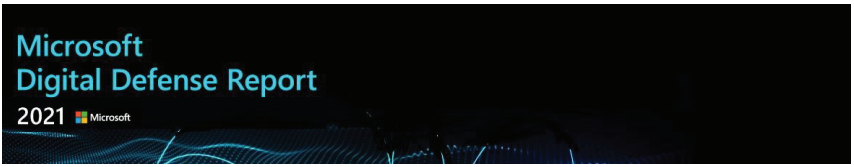
წელს რუსეთის ფედერაციაში ამოქმედდა ***საინფორმციო უსაფრთხოების მთავარ ოფიცერთა ასოციაცია (ARSIB).*** *იგი შექმნის დღიდან ორგანიზებას უწევდა სხვადასხვა შეჯიბრებებს სკოლებსა და უნივერსიტეტებში სადაზვერვო საზოგადოების რეკრუტირების კუთხით. 2011 წელი -* ***Positive Technologies-მა*** *დაიწყო ჰაკერების* ***CTF*** *კონკურსების,* ***Positive Hack Days-ის*** *ორგანიზება, რომელსაც ასევე იყენებენ რუსეთის უშიშროების სამსახურები ნიჭიერი ადამიანების მოსაზიდად. ციფრული უსაფრთხოების კომპანია იმავე წელს იწყებს კონკურსს თეთრქუდიანი, ანუ ეთიკური ჰაკერებისთვის, სახელწოდებით -* ***ZeroNights".***[78]

"2014 წელს რუსეთის უნივერსიტეტების სია, სადაც ასწავლიდნენ ინფორმაციული უსაფრთხოების მიმართულებას, გაიზარდა 170-მდე. შემდეგ ***ვორონეჟის სამხედრო საჰაერო ძალების აკადემიაში*** *ამოქმედდა პირველი სამხედრო ნაწილის კვლევითი ცენტრი, ამ დღიდან იწყება სხვადასხვა კვლევითი ცენტრების ჩამოყალიბება. თავდაცვის სამინისტრომ შექმნა სპეციალური განვითარების ცენტრი, რომელიც ორიენტირებულია კიბერტექნოლოგიებზე. პარალელურად,* ***GRU*** *იწყებს ნიჭიერი ბავშვების შეკრებას რუსულ სკოლებში,* ***FSB-ის*** *და* ***IKSI.XX-თან*** *თანამშრომლობით".*[79] ამავე წელს, უკრაინის საპრეზიდენტო არჩევნებამდე ცოტა ხნით ადრე, რუსმა ბოროტმა ჰაკერებმა, რომლებიც დაკავშირებულნი იყვნენ ***GRU-ს*** მთავარი დაზვერვის განყოფილებასთან, განახორციელეს კიბერშეტევები არჩევნებში ხმის მიცემის მანიპულაციის მიზნით. მათ მოიპოვეს არალიცენზირებული წვდომა ქსელში და წაშალეს ფაილები, რათა შეეცვალათ არჩევნების შედეგები.

ესტონეთის, საქართველოსა და უკრაინის მიმართ რუსეთის მხრიდან კიბერომის წარმოება შეიძლება შევაფასოთ როგორც ერთგვარი ექსპერიმენტი და რუსეთის კიბერტექნოლოგიების გამოცდა. ასეთ მეთოდს რუსეთი ხშირად იყენებს. მაგალითები ბევრი გვაქვს, მათ შორის საფრანგეთის, იტალიის, ჰოლანდიისა და გერმანიის არჩევნებში კიბერჩარევასა და ჩარევის მცდელობებზე. თუმცა ევროპული ქვეყნების არჩევნებში ჩარევა არც ისე ეფექტური აღმოჩნდა.

[78] *Association of Heads of Information Security Services, "Projects of the CTF movement in Russia" p. 1, 2022. http://aciso.ru/aciso-projects/3861/*

[79] *Infoforum, "National Forum on Information Security", p. 1, 2014. https://old.infoforum.ru/conference/conference/view/id/5*



არსებობს კიბერუსაფრთხოებასთან დაკავშირებით სხვადასხვა საერთაშორისო მეგაკომპანიების კვლევები, მოსაზრებები და წლიური ანგარიშები, სადაც რუსეთის ფედერაცია, როგორც აგრესორი კიბერმოთამაშე, ხშირად ფიგურირებს. კომპანია ***Maicrosoft-მა*** გაასაჯაროვა 2021 წლის ანგარიში, სადაც აღნიშნულია, რომ *"გასული წლის განმავლობაში **Maicrosoft-ის** მიერ ეროვნული სახელმწიფოებიდან დაფიქსირებული კიბერშეტევების 58 პროცენტი რუსეთის ფედერაციიდან იყო წარმოებული. განხორციელებული კიბერშეტევებიდან შარშან 21 პროცენტი იყო წარმატებული, ხოლო დღეს იგი 32 პროცენტს შეადგენს",*[80] რაც იმის მანიშნებელია, რომ რუსული ეროვნული სახელმწიფო აქტორების კიბერთავდასხმები სულ უფრო ეფექტური ხდება. რუსეთის ფედერაციიდან მიზანმიმართულად ხდება სხვადასხვა სამთავრობო უწყებების დაზვერვა და ინფორმაციის შეგროვება. სტატისტიკას თუ დავუჯერებთ, *"მათი სამიზნეები ერთი წლის წინ 3 პროცენტიდან 53 პროცენტამდე გაიზარდა. ისინი ძირითადად აკვირდებიან და ინფორმაციას აგროვებენ ისეთ საგენტოებზე, რომლებიც ჩართულები არიან საგარეო პოლიტიკაში, ეროვნულ უსაფრთხოებაში ან თავდაცვაში. რუსეთის ფედერაციის კიბერსამიზნე წლის განმავლობაში იყო სამი ქვეყანა - ამერიკის შეერთებული შტატები, დიდი ბრიტანეთი და უკრაინა".*[81] ***Microsoft-ის*** ფიცრული თავდაცვის ანგარიში მცირეა და იგი მოიცავს 2020 წლის ივლისიდან 2021 წლის ივნისამდე პერიოდს.

ანგარიშში ნათქვამია, რომ რუსეთი არ არის ერთადერთი აქტორი სახელმწიფო, რომელიც კიბერტექნოლოგიებს იყენებს სხვა ქვეყნებზე გავლენისთვის და ზიანის მისაყენებლად. რუსეთის შემდეგ კიბერთავდასხმები ყველაზე ხშირად ხორციელდება ირანიდან, ჩინეთიდან, სამხრეთ კორეიდან და თურქეთიდან. აქვე ნათქვამია, რომ აქტიური კიბერშეტევები ხორციელდება

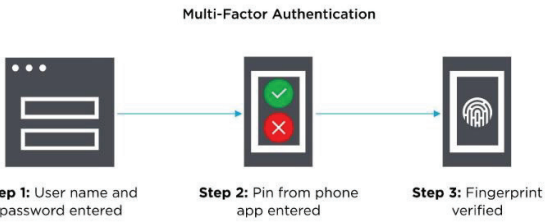
[80] *Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/*

[81] *Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/*

ვიეტნამიდანაც. თუმცა იგი ვერ შეედრება ამ ქვეყნებიდან განხორციელებულ კიბერთავდასხმებს.

საერთო ჯამში, აქტორი ქვეყნების მთავარ მიზანს ჯაშუშობა, სხვა ქვეყნებისთვის კომპიუტერული ტექნოლოგიების დაზიანება და განადგურება წარმოადგენს. იკვეთება სხვა ინტერესებიც - მაგალითად, ირანმა ოთხჯერ გაზარდა ისრაელის წინააღმდეგ კიბერშეტევები იმის გამო, რომ ამ ორ ქვეყანას შორის დაძაბული ურთიერთობაა. ჩრდილოეთ კორეა - მიზნად ისახავდა კრიპტოვალუტის მიმართულებით კიბერთავდასხმებსა და თაღლითობას, რადგან მისი ეკონომიკა სანქციებისა და პანდემიის გამო თითქმის სრულად განადგურდა. ანგარიშში ნათქვამია, რომ *"კიბრშეტევების 21 პროცენტი, რაც **Microsoft-მა** დაფიქსირა, მიმართული იყო მომხმარებლებზე, 79 პროცენტი კი ორგანიზაციებზე, რაშიც 48 პროცენტი მთავრობებზე იყო მიმართული. კიბერთავდასხმების 31 პროცენტი ხდებოდა არასამთავრობო ორგანიზაციებსა და ანალიტიკურ ცენტრებზე. მცირე რაოდენობით ხდება განათლებაზე, მედიასა და **IT** მიმართულებებზე".*[82]

აღსანიშნავია, რომ ***Microsoft-ს*** არ აქვს გლობალურ კიბერშეტევებზე დაკვირვების ფუნქცია და წვდომა. მათ აქვთ შეზღუდული ხილვადობა კიბერთავდასხმებზე. შესაბამისად, ისინი ანგარიშს აქვეყნებენ მხოლოდ საკუთარ ინფორმაციაზე დაყრდნობით, თუმცა აღნიშნული ანგარიშიც, მიუხედავად იმისა, რომ გლობალურ სურათს არ ასახავს, გვაძლევს საერთო სურათის დანახვისა და ანალიზის გაკეთების საშუალებას.



სურათი 1: ორბიჯიანი და სამბიჯიანი ავთენტიფიკაცია. წყარო: *https://www.onelogin.com*

[82] *Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/*

ამ წიგნში განხილული და მოცემული გვაქვს ორბიჯიანი და სამბიჯიანი პაროლების დაყენების ინსტრუქციები და რჩევები ***(MFA),*** ასევე კომპანია ***Microsoft-ი*** თავის ანგარიშში, რომლის სხვადასხვა დეტალები უკვე განვიხილეთ, განმარტავს, რომ *"მომხმარებლების 20 პროცენტზე ნაკლები იყენებს აღნიშნულ მექანიზმებს".*[83] ანგარიშში ნათქვამია, რომ *"თუ მოხდება **MFA-ს** გამოყენება და სისტემების დროულად განახლება, მომხმარებლები დაცულები იქნებიან 99 პროცენტით".*[84] ამ შემთხვევაში მნიშვნელოვანი როლი აკისრიათ ***Microsoft-ის*** მსგავს ტექნოლოგიურ კომპანიებს უსაფრთხო პროგრამული უზრუნველყოფის შემუშავებაში.

ჩვენ ხშირად ვახსენებთ რუსეთ-უკრაინის ომს, ეს ბუნებრივია, მით უმეტეს, როდესაც რუსეთის კიბერშესაძლებლობებზე ვსაუბრობთ. ომის დაწყების შემდეგ *"კიევში დაფუძნებულმა კიბერუსაფრთხოების კომპანია **Unit Technologies-მა** დაიწყო ჰაკერების დაჯილდოება, თუ ისინი წაშლიდნენ და დაზიანებდნენ რუსულ ვებ-გვერდებს. კომპანიამ ამ საქმისთვის 100 000 აშშ დოლარი გამოყო".*[85] იმის მიუხედავად, რომ რუსეთის სამთავრობო უწყებების კომპიუტერულ მოწყობილობებსა და სერვერებზე იმატა სხვადასხვა სახის კიბერშეტევებმა და ყველაზე მეტად ***DDoS*** შეტევებმა, მაინც ვერ მიიღეს ის ეფექტი, რასაც ელოდებოდნენ. მოგეხსენებათ, მსგავსი კიბერშეტევების გამოყენება ბევრ ქვეყანაში კანონით აკრძალულია და ისჯება სისხლის სამართლის კოდექსით, არ აქვს მნიშვნელობა, ვინ არის სამიზნე. შეიძლება იმ ქვეყნებმა, რომლებიც უკრაინას ეხმარებიან და უკრაინის მხარეს დგანან, თვალი დახუჭონ, მაგრამ ამ შემთხვევაში რისკ-ფაქტორს წარმოადგენს კიბერთავდასხმების შედეგები. მაგალითად, ***"რუსეთის კომპიუტერული ინციდენტების ეროვნულმა საკოორდინაციო ცენტრმა (NCCCI)*** *გამოაქვეყნა სია, რომელიც შეიცავდა **17,576 IP** მისამართს და 166 დომენს. უკრაინაში შეჭრის შემდეგ. რუსეთის მიერ*

[83] *Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/*

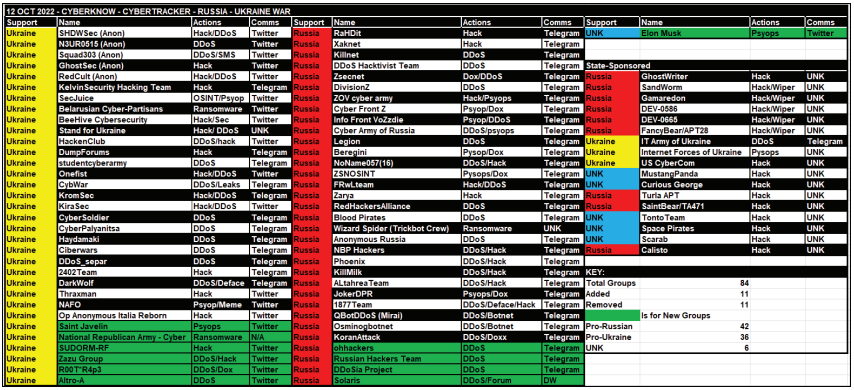
[84] *Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/*

[85] *Janofsky A., "This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites", The Record by Recorded Future, p. 1, 2022. https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/*

*გავრცელებული ინფორმაციის თანახმად, მათ ინფრასტრუქტურაზე **DDoS** თავდასხმების სერიის უკან იდგნენ **FBI, CIA** და რამდენიმე მედიაგამოცემის ვებგვერდი".*[86]

კიბერმკვლევარები აკვირდებიან რუსეთ-უკრაინის კიბერომს. ***Cisco-ს*** ცნობით, *"მასირებული კიბერთავდასხმები განხორციელდა 2022 წლის 15 თებერვალს, მეორე კი 24 თებერვალს. ამის შემდეგ **CISA-მ** და **FBI-მ** 17 მარტს ერთობლივი კიბერუსაფრთხოების რეკომენდაციები გამოაქვეყნეს, მათ მოუწოდეს აშშ-ისა და საერთაშორისო სატელიტური კომუნიკაციის ქსელის პროვაიდერების მომხმარებლებს **(SATCOM),** იყვნენ მზადყოფნაში შესაძლო საფრთხეებთან დაკავშირებით. აღნიშნული გაფრთხილება მოყვა 24 თებერვლის კიბერშეტევებს, როდესაც განხორციელდა თავდასხმები **Viasat-სა** და **KA-SAT-ზე,** რამაც შეაფერხა ფართოზოლიანი თანამგზავრული ინტერნეტი უკრაინასა და ევროპის სხვა ქვეყებში".*[87] რაკი რუსეთი შეიჭრა უკრაინაში, მსოფლიო მასშტაბით ყველა სახელმწიფო უნდა იყოს მზადყოფნაში - სხვადასხვა აქტორები, რომლებიც გამოირჩევიან ჰაკერული თაღლითური და ინფრასტრუქტურის დამაზიანებელი თავდასხმებით, ცდილობენ, რუსეთ-უკრაინის კონფლიქტი გამოიყენონ ერთგვარ ინსტრუმენტად. მაგალითად, ახალი ამბების, დეზინფორმაციის გავრცელება, შემოწირულობების მოთხოვნა მავნე ბმულებით, დახმარების ფონდების სახელებით და ყალბი ვებ-მისამართებით ან ლტოლვილთა მხარდაჭერის ყალბი ვებ-გვერდებით და სხვა. კიბერსაფრთხეების ანალიტიკოსებმა შეადგინეს კიბერჯგუფების ცრილი, რომლებიც რუსეთ-უკრაინის კონფლიქტში არიან ჩართულები, ანალიზის გაკეთების საშუალებას გვაძლევს კიბერსაფრთხეების ლანდშაფტის შესაფასებლად.

[86] *Интернет-портал: Безопасность пользователей в сети интернет,"НКЦКИ: рекомендации по защите информационных ресурсов от компьютерных атак", p. 1, 2022. https://safe-surf.ru/specialists/news/676114/*
[87] *Cisco Annual Report, "Reimagining the future of connectivity", 2022. https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf*



12 OCT 2022 - CYBERKNOW - CYBERTRACKER - RUSSIA - UKRAINE WAR

Support	Name	Actions	Comms	Support	Name	Actions	Comms	Support	Name	Actions	Comms
Ukraine	SHOWSec (Anon)	Hack/DDoS	Twitter	Russia	RaHDit	Hack	Telegram	UNK	Elon Musk	Psyops	Twitter
Ukraine	N3UR0515 (Anon)	DDoS	Twitter	Russia	Xaknet	Hack	Telegram				
Ukraine	Squad303 (Anon)	DDoS/SMS	Twitter	Russia	Killnet	DDoS	Telegram				
Ukraine	GhostSec (Anon)	Hack	Twitter	Russia	DDoS Hacktivist Team	DDoS	Telegram	State-Sponsored			
Ukraine	RedCult (Anon)	Hack/DDoS	Twitter	Russia	Zsecnet	Dox/DDoS	Telegram	Russia	GhostWriter	Hack	UNK
Ukraine	KelvinSecurity Hacking Team	Hack	Telegram	Russia	DivisionZ	DDoS	Telegram	Russia	SandWorm	Hack/Wiper	UNK
Ukraine	SecJuice	OSINT/Psyops	Twitter	Russia	ZOV cyber army	Hack/Psyops	Telegram	Russia	Gamaredon	Hack/Wiper	UNK
Ukraine	Belarusian Cyber-Partisans	Ransomware	Twitter	Russia	Cyber Front Z	Psyop/Dox	Telegram	Russia	DEV-0586	Hack/Wiper	UNK
Ukraine	BeeHive Cybersecurity	Hack/Sec	Twitter	Russia	Into Front VoZdzie	Psyop/DDoS	Telegram	Russia	DEV-0665	Hack/Wiper	UNK
Ukraine	Stand for Ukraine	Hack/ DDoS	UNK	Russia	Cyber Army of Russia	DDoS/psyops	Telegram	Russia	FancyBear/APT28	Hack/Wiper	UNK
Ukraine	HackenClub	DDoS/hack	Twitter	Russia	Legion	DDoS	Telegram	Ukraine	IT Army of Ukraine	DDoS	Telegram
Ukraine	DumpForums	Hack	Telegram	Russia	Beregini	Pysop/Dox	Telegram	Ukraine	Internet Forces of Ukraine	Pysops	UNK
Ukraine	studentcyberarmy	DDoS	Telegram	Russia	NoName057(16)	DDoS/Hack	Telegram	Ukraine	US CyberCom	Hack	UNK
Ukraine	OneFist	Hack/DDoS	Twitter	Russia	ZSNOSINT	Pysops/Dox	Telegram	UNK	Mustang Panda	Hack	UNK
Ukraine	CybWar	DDoS/Leaks	Telegram	Russia	FRwLteam	Hack/DDoS	Telegram	UNK	Curious George	Hack	UNK
Ukraine	KromSec	Hack/DDoS	Telegram	Russia	Zarya	Hack	Telegram	Russia	Turla APT	Hack	UNK
Ukraine	KiraSec	Hack/DDoS	Twitter	Russia	RedHackersAlliance	DDoS	Telegram	Russia	SaintBear/TA471	Hack	UNK
Ukraine	CyberSoldier	DDoS	Telegram	Russia	Blood Pirates	DDoS	Telegram	UNK	TontoTeam	Hack	UNK
Ukraine	CyberPalyanitsa	DDoS	Telegram	Russia	Wizard Spider (Trickbot Crew)	Ransomware	UNK	UNK	Space Pirates	Hack	UNK
Ukraine	Haydamaki	DDoS	Telegram	Russia	Anonymous Russia	DDoS	Telegram	UNK	Scarab	Hack	UNK
Ukraine	Ciberwars	DDoS	Telegram	Russia	NBP Hackers	DDoS/Hack	Telegram	Russia	Calisto	Hack	UNK
Ukraine	DDoS_separ	DDoS	Telegram	Russia	Phoenix	DDoS/Hack	Telegram				
Ukraine	2402Team	Hack	Telegram	Russia	KillMilk	DDoS/Hack	Telegram	KEY:			
Ukraine	DarkWolf	DDoS/Deface	Telegram	Russia	ATathrea Team	DDoS/Hack	Telegram	Total Groups		84	
Ukraine	Thraxman	Hack	Twitter	Russia	JokerDPR	Psyops/Dox	Telegram	Added		11	
Ukraine	NAFO	Psyop/Meme	Twitter	Russia	1877Team	DDoS/Deface/Hack	Telegram	Removed		11	
Ukraine	Op Anonymous Italia Reborn	Hack	Twitter	Russia	QBotDDoS (Mirai)	DDoS/Botnet	Telegram	Is for New Groups			
Ukraine	Saint Javelin	Psyops	Twitter	Russia	Qbmingobotnet	DDoS/Botnet	Telegram	Pro-Russian		42	
Ukraine	National Republican Army - Cyber	Ransomware	N/A	Russia	KoranAttack	DDoS/Doxx	Telegram	Pro-Ukraine		36	
Ukraine	SUDORM-RF	Hack	Twitter	Russia	ohhackers	DDoS	Telegram	UNK		6	
Ukraine	Zazu Group	DDoS/Hack	Twitter	Russia	Russian Hackers Team	DDoS	Telegram				
Ukraine	R00T*R4p3	DDoS/Dox	Twitter	Russia	DDoSia Project	DDoS	Telegram				
Ukraine	Altro-A	DDoS	Twitter	Russia	Solaris	DDoS/Forum	DW				

ცხრილი 4: კიბერ-ჯგუფები ჩართული რუსეთ-უკრაინის ომში. *წყარო: https://cyberknow.medium.com/2022-russia-ukraine-war-cyber-group-tracker-update-3-56f15e83f407*

ცხრილში ნათლად ჩანს, თუ რამდენად მასშტაბურია რუსეთის კიბერშეტევები უკრაინის წინააღმდეგ. რუსეთის მხრიდან დაფინანსებულმა ***მოწინავე საფრთხის ჯგუფებმა (APT)*** გამოავლინეს უნარი, შეინარჩუნონ მუდმივი, ამოუცნობი, გრძელვადიანი წვდომა და უნებართვო წვდომა ქსელებში, ლეგიტიმური სერთიფიკატების გამოყენებით. *„კიბერშეტევების ყველაზე მაღალი რისკი მოდის რუსეთის ფედერაციის მიერ დაქირავებული **APT ჯგუფების** მხრიდან, როგორებიც არიან: **APT28, Turla, Gamaredon, Energetic Bear, APT29, Sandworm** და სხვა“.*[88] უფრო მეტი თვალსაჩინოებისთვის იხილეთ სურათი , რომელიც ასახავს, თუ ვინ მონაწილეობს რუსეთ-უკრაინის კიბერომში და ვის რა პოზიცია უკავია ამ დაპირისპირებაში.

[88] *Curatedintel, "Curated Intelligence Stands With Ukraine", p. 1, 2022. https://www.curatedintel.org/2022/02/curated-intelligence-stands-with-ukraine.html*

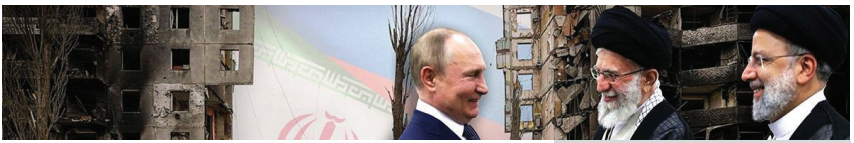
სურათი 2: რუსეთ-უკრაინის "კიბერომის" მონაწილეები. *წყარო: EQUINIX - https://atos.net/en/lp/securitydive/risks-from-the-cyberattacks-ru-ua-conflict*

ირანის ისლამური რესპუბლიკა

ირანის ისლამური რესპუბლიკა წარმოადგენს მსოფლიო მასშტაბით ერთ-ერთ უძველეს სახემწიფოს. ჩრდილო-დასავლეთით ესაზღვრება აზერბაიჯანი, სომხეთი და თურქეთი, დასავლეთით - ერაყი, აღმოსავლეთით - ავღანეთი და პაკისტანი. ცნობილია, რომ *"ირანის ისლამურ რესპუბლიკაში შეიქმნა ზოროასტრიზმი (მაზდეანობა). XVI საუკუნეში კი მათი რელიგია გახდა შიიზმის მიმდინარეობა - მაჰმადიანობა. 1979 წელს ირანში მოხდა ისლამური რევოლუცია აიათოლა ჰომეინის ხელმძღვანელობით, გაუქმდა მონარქია და შეიქმნა ისლამური რესპუბლიკა".*[89]

[89] *BBC, "Iran profile - timeline", p. 1, 2020. https://www.bbc.com/news/world-middle-east-14542438*

ცნობილია, რომ იგი რეგიონის ერთ-ერთი ყველაზე ტექნოლოგიურად განვითარებულ სახელმწიფოს წარმოადგენს.



ვლადიმერ პუტინი და ალი ხამენეი

რაც შეეხება ირანის ისლამური რესპუბლიკის პოციზიასა და როლს რუსეთ-უკრაინის ომთან მიმართებაში, აღნიშნული საკითხი არავისთვის არის დამალული, ომის დაწყებიდან ირანის ისლამური რესპუბლიკის თავდაპირველმა ოფიციალურმა განცხადებამ, რაღაცნაირად გამოიწვია შეგრძნება, რომ ნეიტრალური პოზიცია შეიძლება ჰქონოდა, თუმცა მოგვიანებით, როდესაც ირანის ლიდერმა ***ალი ხამენეიმ (Ali Khamenei)*** განცხადებები გააკეთა, პირდაპირ გაიმეორა ***ვლადიმერ პუტინის (Vladimir Putin)*** რიტორიკა და დაადანაშაულა დასავლეთი. ცნობილია, რომ თეირანმა რუსეთს მიაწოდა ასობით უპილოტო თვითმფირნავები და რუსეთის მიერ ოკუპირებულ ყირიმის ნახევარკუნძულზე გაგზავნა ხალხი ***ისლამური რევოლუციის გვარდიის კორპუსიდან (IRGC).***

ყველა ფაქტისა და მტიკცებულების მიუხედავად, თეირანმა უარყო უპილოტო თვითმფინავების მიწოდება და ჯარისკაცების გაგზავნა ყირიმში. ირანის ისლამური რესპუბლიკის მეთაურმა მხარი არ დაუჭირა კრემლის „რეფერენდუმს“, რომელიც გულისხმობდა უკრაინის ოთხი ოლქის ანექსიას, თუმცა მისი განცხადებები ზუსტად ემთხვევა ვლადიმერ პუტინის განცხადებებს.

ირანის მთავრობა ავრცელებს ნარატივს ორივე ქვეყნის გაწევრიანების შესახებ ეგზისტენციალურ ბრძოლაში მუდმივად გაფართოებული ნატოსა და ზოგადად დასავლეთის წინააღმდეგ. როდესაც პუტინი ეწვია თეირანს *„2022 წლის ივლისში და ხელი მოაწერა 40 მილიარდი დოლარის ფარგლებში* ***ურთიერთთანამშრომლობის***

მემორანდუმს (MOU) *ირანში ენერგეტიკული პროექტების განსავითარებლად,"*[90] ***აიათოლა ალი ხამენეი*** შეეცადა, დაერწმუნებინა რუსი კოლეგა, უკრაინაში ომი არ წამოეწყო. არ შეიძლება უარვყოთ, უკრაინაში დაწყებულმა კონფლიქტმა მნიშვნელოვანი სტიმული მისცა რუსეთსა და ირანს შორის ორმხრივ ურთიერთობას. ამან დიდი შეშფოთება გამოიწვია ამერიკის შეერთებული შტატებსა და ევროკავშირში. დასავლეთი რუსეთ-ირანის პარტნიორობის გაძლიერებას მნიშვნელოვან საფრთხედ თვლის.

ვედანტ პატელი

ამერიკის შეერთებული შტატების სახელმწიფო დეპარტამენტის წარმომადგენლის მოადგილე, ***ვედანტ პატელი (Vedant Patel)*** ირანის მიერ რუსეთისთვის იარაღის მიწოდებას და ურთიერთობების გაღრმავებას გამოეხმაურა, მან განაცხადა, რომ ეს არის დიდი საფრთხე და მთავრობებმა დიდი ყურადღება უნდა მიაქციონ ამ პროცესს.

ირანის ისლამური რესპუბლიკა არ არის მონოლითური ერთეული და მის შიგნით კონკურენტი ფრაქციების შედარებითი ძალა განსაზღვრავს მის საგარეო პოლიტიკას. ისინი ათწლეულების განმავლობაში დასავლეთთან დიპლომატიურ ურთიერთობებს ეწინააღმდეგებოდნენ. მეტიც, როდესაც მიიღეს ***ერთობლივი სამოქმედო გეგმა (JCPOA),***[91] ბევრი მათგანი ეწინააღმდეგებოდა, მაგრამ ემხრობოდნენ დიდი ინვესტიციების განხორციელებას რუსეთთან, ჩინეთთან და სხვა არადასავლურ ქვეყნებთან. პრინციპში, ისიც უნდა აღინიშნოს, რომ ყოფილი პრეზიდენტი ჰასან როჰანი კი ემხრობოდა რუსეთთან, ჩინეთთან და სხვა მსგავს ქვეყნებთან თბილ და გრძელვადიან ურთიერთობებს, მაგრამ ასევე ხაზს უსვამდა დასავლეთთან მოლაპარაკებებისა და ურთიერთობების მნიშვნელობას. 2018 წლის

[90] *independent, "Iran, Russia sign MoU for petroleum investment", p. 1, 2022. https://www.independent.co.ug/iran-russia-sign-mou-for-petroleum-investment/*
[91] *Ajorlo H., "Understanding the threats and barriers to reviving the JCPOA", Aljazeera, p. 1, 2021. https://studies.aljazeera.net/en/analyses/understanding-threats-and-barriers-reviving-jcpoa*

მაისში ამერიკის შეერთებული შტატების ერთობლივი ყოვლისმომცველი სამოქმედო გეგმიდან გამოსვლამ და 2015 წლის შეთანხმების დარღვევამ დააჩქარა ირანის ისლამური რესპუბლიკის საგარეო პოლიიკური ორიენტაციის განვითარება, რომელსაც მოიხსენიებენ სახელწოდებით - *„გახედე აღმოსავლეთს“*,[92] აღნიშნული კი დაემთხვა რუსეთის შეჭრას უკრაინაში და წარმოშვა ის პოლიტიკური მოცემულობა, რასაც დღეს ვუყურებთ მსოფლიო მასშტაბით.

ირანის ისლამური რესპუბლიკის კიბერშესაძლებლობები

ირანის ისლამურმა რესპუბლიკამ კიბერტექნოლოგიების მიმართულებით ბევრი მნიშვნელოვანი ნაბიჯი გადადგა. მართალია, ამ ქვეყნიდან მომდინარე კიბერსაფრთხეები რუსეთიდან მომდინარე კიბერსაფრთხეებს ვერ აჭარბებს, მაგრამ შესაძლებლობებით ბევრს უსწრებს. იგი ამ ეტაპზე ვერ ფლობს კიბერძალაუფლების უმაღლეს რაგნს, თუმცა კარგად აფასებს კიბერიარაღის მნიშვნელობას საერთაშორისო პოლიტიკაში.

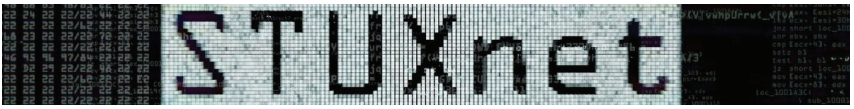
ალი ხამენეი

ირანის ისლამურმა რესპუბლიკამ შექმნა დახვეწილი ორგანიზაციული სტრუქტურა კიბერკონფლიქტების მართვისთვის. კიბერდოქტრინის თითოეულ დეტალს აკონტროლებს ხელისუფლება - უზენაესმა ლიდერმა ***ალი ხამენეიმ (Ali Khamenei)*** შექმნა ***კიბერსივრცის უმაღლესი საბჭო (SCC),***[93] რომელიც დაკომპლექტებულია ამავე ხელისუფლების უმაღლესი წარმომადგენლებით, დაზვერვის მაღალი თანამდებობის პირებით, მინისტრებით. ამავე საბჭოში შედის პრეზიდენტიც.

[92] *Gramer R., Amy Mackinnon A., "Iran and Russia Are Closer Than Ever Before", p. 1, 2022. https://foreignpolicy.com/2023/01/05/iran-russia-drones-ukraine-war-military-cooperation/*
[93] *Connell M., "Deterring Iran's Use of Offensive Cyber: A Case Study", CNA, PP. 2-4, 2014. https://www.cna.org/archive/CNA_Files/pdf/dim-2014-u-008820-final.pdf*

აღნიშნული ორგანოს მიზანია კიბერშეტევებსა და კიბერთავდაცვას შორის კოორდინაციის უზრუნველყოფა.

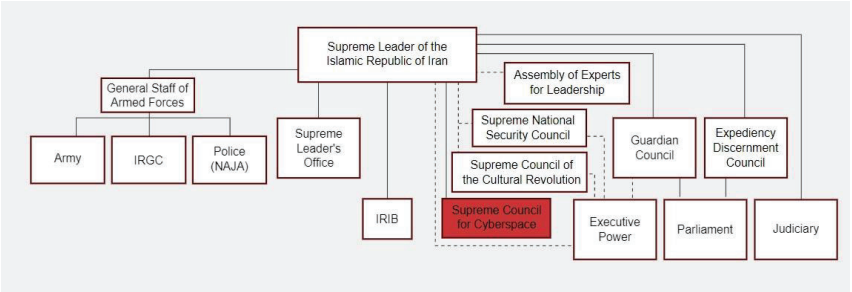
ირანის ისლამური რესპუბლიკა კიბერშეტევებს განიხილავს ასიმეტრიული სამხედრო შესაძლებლობების ნაწილად, რომელიც ეხმარება ამერიკის შეერთებულ შტატებთან მიმართებაში. ასევე ცნობილია, რომ ირანის ისლამური რესპუბლიკა ხშირად არის კიბერდამნაშავეების მასობრივი თავდასხმების ეპიცენტრი. ეს კი მეტწილად ირანის ისლამური რესპუბლიკისა და ისრაელის დაძაბული სიტუაციით არის განპირობებული - მათ ხშირად ღია კიბერკონფლიქტი აქვთ გაჩაღებული.



ირანის ისლამურ რესპუბლიკაზე კიბერთავდასხმის დროს, რომელიც ***Stuxnet-ის***[94] სახელით არის ცნობილი, მოხდა კომპიუტერული ვირუსის - ***Stuxnet-ის*** გამოყენება. თავდასხმა განხორციელდა ბირთვული იარაღის ობიექტებზე. ირანელ ლიდერებს ყველაზე მეტად ეშინიათ იმ რისკებისა, რამაც შეიძლება ,,არაბული გაზაფხულის'' მსგავსი სიტუაცია შექმნას. რაც შეეხება ***Stuxnet-ის*** თავდასხმას, დიდი პანიკა გამოიწვია, გაჩნდა ეჭვი, რომ აღნიშნული ვირუსი შეიძლება ადაპტირებული ყოფილიყო ***SCADA-ს***[95] სისტემებზე, რომელსაც მრავალი ქვეყანა იყენებს კრიტიკული ინფრასტრუქტურისთვის. თუმცა ასე არ აღმოჩნდა.

[94] *Zetter K., "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", Crown Publishers, an imprint of Random House LLC, p. 1, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/*

[95] *SCADA არის სამეთვალყურეო კონტროლისა და მონაცემთა შეგროვების სისტემა, რომელიც შედის სამრეწველო პროცესების კონტროლის პროგრამული აპლიკაციების კატეგორიაში, იგი გულისხმობს დისტანციურად მონაცემთა რეალურ დროში შეგროვებას, აღჭურვილობის კონტროლის მიზნით.*



ფიგურა 2: ირანის ისლამური რესპუბლიკის სამთავრობო სტრუქტურები. *წყარო: https://facesofcrime.org/institution/101/supreme-council-of-cyberspace/*

ირანის ისლამურ რესპუბლიკაში არსებობს სამი სამხედრო ორგანიზაცია, რომელიც წამყვან როლს ასრულებს კიბეროპერაციების წარმოების დროს. ესენია:

- ***ირანის ისლამური რესპუბლიკის რევოლუციური გვარდიის კორპუსი (IRGC);***[96]
- ***ბასიჯი (the Basij);***[97]
- ***ირანის ისლამური რსპუბლიკის პასიური თავდაცვის ორგანიზაცია (NPDO)***[98]

რევოლუციური გვარდიის კორპუსი პირდაპირ არის პასუხისმგებელი ამერიკის შეერთებული შტატებზე, ისრაელის კრიტიკულ ინფრასტრუქტურაზე, საუდის არაბეთსა და სხვა ქვეყნებზე განხორციელებულ კიბერთავდასხმებზე.

ბასიჯის კიბერსაბჭო, როგორც ცნობილია, სამოქალაქო, მაგრამ გასამხედროებული ორგანიზაციაა. აქ 120 000-ზე მეტი კიბერმოხალისე ჰყავთ დასაქმებული. იგი იყენებს შიდა კავშირებს უნივერსიტეტებთან და სკოლებთან, რათა შეკრიბოს მარტივად მართვადი ბოროტ ჰაკერთა ჯგუფები.

რაც შეეხება ***პასიური თავდაცვის ორგანიზაციას,*** იგი პასუხისმგებელია კრიტიკული ინფრასტრუქტურის დაცვაზე. ირანის ისლამურ რესპუბლიკაში ასევე ფუნქციონირებს:

---

[96] *Anderson C. Sadjadpour K., "Iran's Cyber Threat: Espionage, Sabotage, and Revenge", Carnegie Endowment for International Peace, PP. 15-17, 2018. https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf*
[97] *Denning D., "Following the developing Iranian cyber threat", The Conversation, p. 1, 2017. https://theconversation.com/following-the-developing-iranian-cyberthreat-85162*
[98] *Nadimi F., "Iran's Passive Defense Organization: Another Target for Sanctions", p. 1, 2018. https://www.washingtoninstitute.org/policy-analysis/irans-passive-defense-organization-another-target-sanctions*

- ***ეროვნული უშიშროების უმაღლესი საბჭო (SNSC)***[99] **-** არის ეროვნული უსაფრთხოების პოლიტიკის შემუშავების უმაღლესი ორგანო, კოორდინაციას უწევს და ახორციელებს უმაღლესი ლიდერის დირექტივებს.
- ***კიბერსივრცის ეროვნული საბჭო (NCC)***[100] **-** იცავს ისლამურ რესპუბლიკას კიბერომისგან.
- ***ელექტრონული ომისა და კიბერ თავდაცვის ორგანიზაცია (EWCDO)***[101] - ატარებს სასწავლო კურსებს, ცენზურას უწევს შინაარსს და წვდომას.
- ***შეიარაღებული ძალების გენერალური შტაბი (AFGS)***[102] - კოორდინაციას უწევს პოლიტიკასა და ოპერაციებს ***IRGC-სა*** და ჩვეულებრივ ***სამხედროებს (Artesh)*** შორის.
- ***დაზვერვისა და უსაფრთხოების სამინისტრო (MOIS)***[103] **-** პასუხისმგებელია სიგნალების დაზვერვაზე.
- ***ირანის კიბერპოლიცია (aka FATA)*** [104] - ფილტრავს ვებკონტენტს, აკონტროლებს ონლაინ სიტუაციას, წვდომას ახორციელებს პოლიტიკური დისიდენტების ელფოსტის ანგარიშებზე.

ირანის ისლამური რესპუბლიკა ინტენსიურად იკვლევს ამერიკის შეერთებული შტატების კრიტიკულ ინფრასტრუქტურას, როგორც ერთგვარ სამიზნეს კიბერთავდასხმებისთვის. რამდენად წარმატებულია აღნიშნული კვლევები და შემდეგ თავდასხმები ეს სხვა საკითხია. ირანის ისლამურ რესპუბლიკას უკვე აქვს სხვადასხვა სახის კიბერშეტევები განხორციელებული ამერიკის შეერთებულ შტატებზე, მაგრამ მეთოდები დაუძველდა, მსოფლიო ამ კუთხით უფრო შორს წავიდა - დაიხვეწა და განვითარდა კიბერუსაფრთხოების პროგრამები, სტრატეგიები, თავდაცვითი მექანიზმები. კიბერშეტევების მეთოდების მხრივ ირანი რუსეთთანაც კი

---

[99] Katzman K., "Iran: Internal Politics and U.S. Policy and Options," Congressional Research Service, PP. 4-7, 2018. https://sgp.fas.org/crs/mideast/RL32048.pdf

[100] Small Media, "Iranian Internet Infrastructure and Policy Report," smallmedia.org.uk, PP. 3-5, 2014. https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf

[101] U.S. Department of the Treasury, "Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators," Press Release, p. 1, 2018. https://home.treasury.gov/news/press-releases/sm0250

[102] U.S. Navy, "Iranian Naval Forces: A Tale of Two Navies," Office of Naval Intelligence, PP. 13-15, 2017. https://www.oni.navy.mil/Portals/12/Intel%20agencies/iran/Iran%20022217SP.pdf

[103] Library of Congress, "Iran's Ministry of Intelligence and Security: A Profile", Federal Research Division, PP. 2-4, 2012. https://irp.fas.org/world/iran/mois-loc.pdf

[104] U.S. Department of the Treasury, "Treasury Announces Sanctions Against Iran", Press Release, p. 1, 2013. https://home.treasury.gov/news/press-releases

ვერ მიდის ახლოს. რა თქმა უნდა, ეს ამ ქვეყნისთვის პრობლემას წარმოადგენს და ცდილობენ, სიტუაცია გააუმჯობესონ.

ყასემ სოლეიმანი

2020 წელს ირანისთვის დიდი რისკი იყო, როდესაც ერაყში, ბაღდადის აეროპორტის მახლობლად აშშ-ის სარაკეტო დარტყმას ირანის ისლამური რევოლუციის გუშაგთა კორპუსის სპეცდანიშნულების რაზმ ***„ალ-კუდსის“*** ლიდერი, გენერალი ***ყასემ სოლეიმანი (Qasem Soleimani)*** ემსხვერპლა. თითქოს ამის გამო საინფორმაციო ომი და კიბერთავდასხმებისთვის მზადებაც დაიწყო, მაგრამ კიბერსივრცეში ოფიციალური განცხადებებისა და ე.წ. „კუნთების თამაშის“ შემდეგ სიტუაცია განეიტრალდა.

ირანის ისლამურ რესპუბლიკაში კარგად ესმით, რა შეიძლება გამოიწვიოს სერიოზულმა კიბერშეტევებმა ამერიკის შეერთებული შტატების კრიტიკულ ინფრასტრუქტურაზე. ამიტომ ცდილობენ, წითელი ხაზები არ გადაკვეთონ და საპასუხო დარტყმა არ მიიღონ. როგორი იქნება პასუხი კი, ამის ანალიზი რთული ნამდვილად არ არის.

კომპიუტერული უსაფრთხოების ინდუსტრიულმა კომპანიამ ***MalCrawler-მა*** დაკვირვება აწარმოა სხვადასხვა კიბერმავნებელ ქვეყნებზე, მათ შექმნეს დახვეწილი ქსელი, რათა დაედგინათ ქვეყნებს შორის კიბერთავდასხმების მეთოდოლოგია, მიმართულებები და ინტერესები. აღმოჩნდა, რომ რუსეთის ფედერაციას, ჩინეთის და ირანის ისლამური რესპუბლიკის კიბერშეტევებს შორის განსხვავებები არსებობს. მაგალითად, *„რუსმა ბოროტმა ჰაკერებმა მოახდინეს არალიცენზირებული წვდომა სისტემაზე და ჩააშენეს უკანაპორტის წვდომა, შემდგომი მრავალმხრივი გამოყენების მიზნით. ჩინელმა ბოროტმა ჰაკერებმა ასევე შეაღწიეს ქსელში და მოიპარეს ყველაფერი, რაც ახალ ტექნიკურ და საჭირო ინფორმაციას ჰგავდა. ხოლო ირანის ისლამური რესპუბლიკის ბოროტი ჰაკერები როგორც კი მოხვდნენ ქსელში, მაშინვე დაიწყეს რაც*

შეიძლება მეტი ზიანის მიყენება - დაშიფრვა, წაშლა, ქსელის დაზიანება და ასე შემდეგ".[105]

ირანის ისლამურმა რესპუბლიკამ გამოაქვეყნა ***შეიარაღებული ძალების გენერალური შტაბის დეკლარაცია***[106] კიბერსივრცისთვის მოქმედ საერთაშორისო სამართლის შესახებ. დეკლარაციაში ნათქვამია, რომ სამხედროებს აქვთ მანდატი, უზენაესი ლიდერის მეთაურობით შეაჩერონ მტრული კიბეროპერაციები და დაიცვან ერი. დეკლარაციაში ასევე წარმოდგენილია გაფრთხილება, რომ ირანის ისლამური რესპუბლიკის შეიარაღებული ძალები იტოვებს უფლებას, რეაგირება მოახდიონოს ნებისმიერ კიბერსაფრთხეზე, თუ კი რომელიმე სახელმწიფო დაარღვევს წინამდებარე დოკუმენტში წარმოდგენილ რომელიმე პუნქტს. ამ შემთხვევაში მნიშვნელობა არ აქვს, ეს იქნება სახელმწიფო თუ მისგან მხარდაჭერილი კონტროლირებადი კერძო პირი ან ჯგუფი.

ალბათ, საერთო ჯამში ნათელია, რომ აღნიშნული კიბერშეტევები, რომელიც ირანის ისლამურ რესპუბლიკას უკავშირდება, არის მცდელობა მოწინააღმდეგეების გაფრთხილებისა, რომ როგორც სხვებს, მათაც აქვთ უნარი და საშუალება, ზიანი მიაყენონ მტრებს კიბერტექნოლოგიების საშუალებით.

ჩინეთი

ჩინეთი რომ საოცრად გაძლიერდა ეკონომიკური თუ ფინანსური თვალსაზრისით, ამას მთელი მსოფლიო ხედავს. ჩინეთს ვერც სამხედრო

[105] *Cilluffo F., Fixler A., "Monograph - Evolving Menace Iran's Use of Cyber-Enabled Economic Warfare", FDD American Leadership, p. 1, 2018. https://www.fdd.org/analysis/2018/11/06/evolving-menace/*

[106] *Schmitt M. N.,"Noteworthy Releases of International Cyber Law Position - Part II: Iran", p. 1, 2020. https://lieber.westpoint.edu/iran-international-cyber-law-positions/*

პოტენციალს დავუწუნებთ. ამ ქვეყნის მთავარი მიზანი ისტორიულად იყო, არის და იქნება უფრო მეტად გაძლიერება. აშშ-ის მოწოდება, რომ არ დაეხმაროს იარაღით და ტექნიკით რუსეთს, გადაჭარბებული გაფრთხილება გახლდათ. ვინ-ვინ და ჩინეთმა სხვაზე უკეთ იცის, რა და როგორ გააკეთოს - მისთვის მნიშვნელოვანია ომის შედეგად გაღარიბებული რუსეთის ბაზრის მთლიანად თუ არა, მეტწილად ათვისება. ცხადია, არც უკრაინულ, არ ევროპულ და არც ამერიკულ ბაზარზე იტყვის უარს. ასე რომ, ჩინეთის პირდაპირ ჩართვა საომარ მოქმედებებში, უნაყოფო მცდელობაა, საამისო შანსი არც არსებობს. ცხადია, არც პირდაპირ და არც ირიბად, მათ შორის არც იარაღის დახმარებით. უბრალოდ, ჩინეთი მშვიდად ელოდება და აკვირდება, როდის დასრულდება ომი. შემდეგ კი თავის როგორც ეკონომიკურ, ასევე ფინანსურ ფრთებს უფრო გაშლის, განსაკუთრებით რუსეთის ბაზარზე, რათა ზღაპრული ხეირი ნახოს.

ჩინეთის კიბერშესაძლებლობები

ჩინეთთან დაკავშირებით არსებობს ბევრი მოსაზრება, თითქოს იგი წარმოადგენს დიდ პოლიტიკურ აქტორს კიბერტექნოლოგიების მიმართულებით. ხშირად შეიძლება გადააწყდეთ ინფორმაციებს ამ საკითხთან დაკავშირებით, მაგრამ ფაქტებით ეს ვერ დასტურდება. ასევე არსებობს მოსაზრება, რომ ჩინეთი კიბერტექნოლოგიებს იყენებს სხვა ქვეყნების კრიტიკული ინფრასტრუქტურის დასაზიანებლად, მათ შორის ამერიკის შეერთებული შტატების. ასეც რომ იყოს, ნაკლებად სავარაუდოა, ამ საკითხს ჩვეულებრივი სამხედრო კონფლიქტის ფორმა მიეცეს. ერთ-ერთ მიზეზს ჩინეთისა და ამერიკის შეერთებული შტატების ფართო ეკონომიკური თანამშრომლობა წარმოადგენს. ზოგიერთ კიბერექსპერტს აქვს მოსაზრებაც, შეიძლება რაღაც ეტაპზე აშშ-სა და ჩინეთს შორის გაჩნდეს სამხედრო დაპირისპირება, არამედ პირიქით, შეიძლება უახლოეს მომავალში ჩინეთმა და აშშ-მ ერთობლივი ძალებით განავითარონ კიბერშესაძლებლობები.

ჩინეთმა პირველად საუბარი კიბერტექნოლოგიებთან დაკავშირებით 1990 წელს დაიწყო, იმ დროისთვის კიბერომს ინფორმაციული ომი უწოდა. ჩინეთმა დაიწყო იმ საკითხის გაცნობიერებაც, რომ სრულყოფილად თავის დაცვა კიბერომის

წარმოების დროს ფაქტობრივად შეუძლებელია, ხოლო ამ დროს საფრთხეების შემსუბუქება შესაძლებელია მხოლოდ გარკვეული რუტინული ცვლილებებისა და სტანდარტების დაცვის ხარჯზე. 2004 წელს ჩინეთის ეროვნული თავდაცვისთვის ინფორმაცია გახდა მთავარი ფაქტორი შეიარაღებული ძალების საბრძოლო შესაძლებლობების გასაძლიერებლად. პირველად სრულფასოვნად კიბერთან დაკავშირებული საკითხების განხილვა ჩინეთის მიერ მოხდა 2013 წელს, როდესაც ჩინეთის სამხედრო აკადემიამ გამოაქვეყნა კვლევა ***„სამხედრო სტრატეგიის მეცნიერება“,***[107] სადაც აქცენტი იყო გაკეთებული იმაზე, რომ კიბერსივრცე უკვე გახდა სამხედრო ბრძოლის ახალი და აუცილებელი სფერო მსოფლიო მასშტაბით.

ჩინეთში ***„სტრატეგიული მხარდაჭერის ძალები'' (PLASSF)*** არის წამყვანი სტრუქტურა კიბერძალების განვითარებაში, რომელიც აერთიანებს კიბერდაზვერვის, კიბერშეტევისა და კიბერთავდაცვის შესაძლებლობებს. იგი რეალურად უფრო მეტს წარმოადგენს, ვიდრე კიბერგანყოფილებებისა და ელექტრონული ომების კონსოლიდაციაა. ***„სტრატეგიული მხარდაჭერის ძალებში''*** ასევე შედგის კოსმოსური განყოფილება, რომელიც უზრუნველყოფს კოსმოსურ საინფორმაციო მხარდაჭერასა და დაზვერვას. აქვე აღსანიშნავია, რომ ქსელური სისტემების დეპარტამენტი პასუხისმგებელია კიბერ, ელექტრონულ და ფსიქოლოგიური ომების შესაძლებლობების მართვაზე.

ჩვენ ყურადღება უნდა გავამახვილოთ ჩინეთის კიბერმიზნებზე. იქიდან გამომდინარე, ჩინელი ექსპერტები ხშირად აღნიშნავენ, რომ არ არსებობს კიბერომის ერთი მთავარი კონცეფცია. მათი აზრით, კიბერომი არის სტრატეგიული ომი ისევე, როგორიც შეიძლება იყოს ბირთვული ომი. როგორც ჩანს, ჩინეთისთვის კიბერსივრცეს და მათ შორის კიბერომს უფრო დიდი მნიშვნელობა აქვს მათი ეროვნული უსაფრთხოებისთვის და მოიცავს კონკურენციას სამხედრო სფეროს მიღმა, როგორც ეკონომიკური, სოციალური, დიპლომატიური და სხვა მიმართულებებით. ჩინეთის სამხედრო სტრატეგიაში კიბერშესაძლებლობების ძირითადი მიზნებია განსაზღვრული, მაგალითად: კიბერსივრცის სიტუაციის მართვა, კიბერთავდაცვა, კიბერსივრცეში ქვეყნის მიზნებისა და ამოცანების მხარდაჭერა,

[107] *China Aerospace Studies Institute, "PLA's Science of Military Strategy", 2013. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf*

საერთაშორისო კიბერთანამშრომლობაში მონაწილეობა. ჩინეთის მთავრობა ცდილობს, გააკონტროლოს ინტერნეტსივრცეში სოციალური მედიების საქმიანობები და ინფორმაცია. ისინი კარგად აანალიზებენ, რომ 21-ე საუკუნეში ინფორმაცია და კიბერსივრცე წარმოადგენს მნიშვნელოვან იარაღს. აქედან გამომდინარე, შესაძლებელია, ქვეყნის შიგნით მარტივად მოხდეს კიბერჩარევა, ადამიანების ემოციებზე თამაში, მანიპულაცია, პროტესტის გაღვივება, რაც გამოიწვევს არეულბას. ცნობილია, რომ *"ჩინეთის მთავრობას დაქირავებული ჰყავს ორ მილიონამდე ადამიანი, ისინი ინსტრუქციის მიხედვით წერენ კომენტარებს და ზეგავლენას ახდენენ საზოგადოებრივ აზრზე. ამასთან დაკავშირებით არსებობს კვლევა, სადაც ნათქვამია, რომ ჩინეთის მთავრობა წელიწადში 448 მილიონი კომენტარის ფაბრიკაციას ახდენს".*[108]

ჩინეთის უმთავრეს მიზანს ისევე, როგორც ყველა ქვეყნისთვის, წარმოადგენს კრიტიკული ინფრასტრუქტურის დაცვა, ეს ბუნებრივია. საინტერესო ის არის, რომ ჩინეთს აქვს ტექნოლოგიური რესურსი, ამერიკის შეერთებულ შტატებსაც კი გაუწიოს კონკურენცია. რაც არ უნდა გასაკვირი იყოს, ჩინეთის ძირითადი ქსელის ტექნოლოგიები და პროგრამული უზრუნველყოფა, აპარატურა შექმნილია ამერიკული კომპანიების მიერ. მაგალითად, ჩინეთი დამოკიდებულია ისეთი კომპანიების პროდუქტებზე, როგორიცაა: Apple, Google, Intel, Cisco, IBM, Microsoft და სხვა.

ცნობილია, რომ *"ჩინეთმა 2007 წლისთვის არა მხოლოდ ამერიკის შეერთებული შტატებისა და ევროპის ქვეყნების ქსელებში შეღწევა, კოპირება და ექსპორტი დაიწყო წარმატებით, არამედ მოიერიშე თვითმფრინავის - F-35 -ის ქურდობაც, სავარაუდოდ, ჩინეთის კიბერშეტევების დამსახურებაა".*[109]

ჩინეთს უამრავი სახელმწიფო ადანაშაულებს კიბერთავდასხმებში. ამ მხრივ ხშირად ვახსენებთ ამერიკის შეერთებულ შტატებს, ისიც იმ ქვეყნების რიგშია, ვინც ზუსტად იცის, ჩინეთიდან კიბერთავდასხმები რა დროს ხორციელდება. ერთ-ერთი ასეთი კიბერთავდასხმა იყო ბოროტი ჰაკერების მხრიდან, როდესაც ინტელექტუალური საკუთრება და პირადი მონაცემები მოიპარეს. ეს აღმოჩნდა ერთ-

[108] *Farrell H., "The Chinese government fakes nearly 450 million social media comments a year. This is why", washingtonpost, p. 1, 2016. https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/*
[109] *Singh M. C., "China's Cyber Warfare Capabilities", Indian Defence Review, p. 1, 2020. http://www.indiandefencereview.com/news/chinas-cyber-warfare-capabilities/*

ერთი ყველაზე დამაზიანებელი, როდესაც *"ამერიკის შეერთებული შტატების ადმინისტრაციის პერსონალის მართვის ოფისის სისტემაზე განხორციელეს კიბერშეტევა - 20 მილიონზე მეტი ადამიანის პერსონალური მონაცემი მოიპოვეს".*[110]

2017 წელს ინდოეთის საჰაერო ძალების ***(SUKHOI 30) გამანადგურებელი თვითმფრინავი*** ჩამოაგდეს, ეჭვობენ, რომ სავარაუდოდ ეს მოხდა ჩინეთის კიბერშეტევების შედეგად. ინდოეთი წლების განმავლობაში წარმოადგენს ჩინეთის კიბერშეტევების სამიზნეს. ეს ასახულია ***ინდოეთის ეროვნული უშიშროების საბჭოს სამდივნოს (NSCS)*** 2018 წლის მოსხენებაშიც,[111] სადაც ნათქვამია, რომ კიბერშეტევების 35 პროცენტი ჩინეთიდან იყო განხორციელებული.

და მაინც, წარმოდგენს თუ არა ჩინეთი ისეთ კიბერძალას, როგორი სახელიც აქვს? შეგვიძლია დავადასტუროთ და უარვყოთ კიდევაც, რადგან ამ მხრივ უტყუარი მტკიცებულებები არ არსებობს. თუ 2017 წლის ***ICT განვითარების ინდექსს დავუკვირდეთ,*** რომელიც 11 ინდიკატორის საშუალებით იკვლევს, რომელი ქვეყანა რა მდგომარეობაშია კიბერშესაძლებლობების მიმართულებით, ტექნოლოგიური, ინოვაციური თვალსაზრისით, საინფორმაციო-ტექნოლოგიური ინდუსტრიის მხრივ, როგორია კიბერინფრასტრუქტურის დონე, მასშტაბი, ვებ-გვერდები, კიბერდიპლომატია, კიბერსამხედრო ტექნოლოგიები და ასე შემდეგ, ჩინეთმა 2017 წელს 176 ქვეყნიდან 80-ე ადგილი დაიკავა. აღნიშნული კვლევა 2017 წლის შემდეგ აღარ გამოქვეყნებულა. იმ მონაცემებით შეგვიძლია ვივარაუდოთ, რომ ჩინეთის მდგომარეობა კიბერტექნოლოგიების მიმართულებით არც ისე სახარბიელო იყო. ნუ გამოვრიცხავთ, 2022 წლისთვის მდგომარეობა გაუმჯობესებული იყოს. ***(იხილეთ სურათი 3.)***

[110] *Levine M. Date J., "22 Million Affected by OPM Hack, Officials Say", ABC News, p. 1, 2015. https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731*
[111] *Kartha T., "The Rejig of India's National Security Architecture Has Been a Long Time Coming", The Wire, p. 1, 2018. https://thewire.in/security/ajit-doval-national-security-council-secretariat*

სურათი 3: ჩინეთის კიბერშესაძლებლობების ინდექსი. *წყარო: https://www.itu.int/net4/ITU-D/idi/2017/index.html*

სხვათა შორის, ჩინეთთან მიმართებაში არსებობს ენის პრობლემა - სტატისტიკა გვიჩვენებს, რომ ინტერნეტსივრცეში ჩინური ენა ფართო მასშტაბით არ გამოიყენება. მსოფლიოში ჩინურად მოლაპარაკე ადამიანების რაოდენობა ყველაზე მეტია, მაგრამ *„ჩინურ ენას ვებ-გვერდების მხოლოდ 1,7 პროცენტი იყენებს, ინგლისურს - 53,9 პროცენტი“.*[112] ეს, რა თქმა უნდა, ბუნებრივია, ინგლისური ენა საერთაშორისო ენად არის აღიარებული. ჩვენი აზრით, აუცილებელია ახალი კვლევების ჩატარება ჩინეთთან დაკავშირებით, რათა დადგინდეს, ეს ქვეყანა წარმოადგენს საფრთხეს რუსეთის ფედერაციასთან და ირანის ისლამურ რესპუბლიკასთან ერთად.

აღსანიშნავია, რომ ჩინეთში ჰაკერულ და ჰაქტივისტურ დაჯგუფებებს ნაციონალიზაციისა და პატრიორტიზმის სიმბოლოდ აღიქვამენ. შეიძლება ქვეყნებმა ჩაატარონ სამხედრო აღლუმები, სადაც წარმოაჩენენ თავიანთ შესაძლებლობებს, მაგრამ არ არსებობს ისეთი აქცია, სადაც წარმოაჩენენ კიბერშესაძლებლობებს. ამ მხრივ შეიძლება ხშირად საქმე გვქონდეს გაზვიადებასთან, ტრაბახთან და ასე შემდეგ.

ჩინეთის ხელისუფლება აცხადებს, რომ იგი მზად არის, კიბერტექნოლოგიები უფრო მაღალ დონეზე აიყვანოს, 2025 წლისთვის შექმნას ძლიერი არქიტექტურა, როგორც თავდაცვისთვის, ასევე თავდასხმისთვის. ჩინეთისთვის მონაცემების დაცვა კიბერუსაფრთხოების სტრატეგიის განვითარების ძირითადი საკითხია. იქიდან გამომდინარე, რომ 21-ე საუკუნეში უკვე რთულად კონტროლირებადი ხდება

[112] *Jinghua L., "What Are China's Cyber Capabilities and Intentions?", IPI Global Observatory, p. 1, 2019. https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/*

მონაცემების დაცვა, რაც ყოველდღიურ რეჟიმში მიედინება კიბერსივრცეში სხვადასხვა პლატფორმებზე და საზღვრებიც არ გააჩნია, ჩინეთი შეშფოთებულია, არ გამორიცხავენ, განხორციელდეს თვალთვალი სხვადასხვა ქვეყნების მხრიდან, მათ შორის, დიდი დოზით ამერიკის შეერთებული შტატების მხრიდან.

სამხრეთ კავკასია და ბალტიისპირეთის ქვეყნები

რეგიონულ აქტორებს შორის რუსეთის ფედერაცია ერთადერთია, რომელიც დაუფარავად გამოთქვამს თავის უკმაყოფილებას საქართველოს ევროატლანტიკური მისწრაფებების გამო. ერთი მხრივ, ეს გასაგებიცაა, მათი გეოპოლიტიკური ხედვებიდან და ეროვნული ინტერესებიდან გამომდინარე. რუსეთის პოლიტიკურ ლიდერებს მიაჩნიათ, რომ საქართველოს ჩრდილოატლანტიკურ ალიანსში თუ ევროკავშირში გაწევრიანების შემთხვევაში, ის დაკარგავს სერიოზული და გავლენიანი აქტორის როლს არა მარტო კავკასიის რეგიონში, არამედ რუსულ ნაციონალისტურ პოლიტიკურ ელიტაში. მიუხედავად, იმისა, რომ ბალტიისპირეთის რესპუბლიკები და ვარშავის პაქტის ყოფილი წევრები უკვე დიდ ხანია ნატოსა და ევროკავშირის წევრები არიან, რუსეთს ჯერ კიდევ ვერ მოუნელებია ეს ფაქტი და ახლა საქართველოს, მათი ორბიტიდან გაქცევა, სინამდვილეში კი დასავლეთისკენ სწრაფვა, რუსეთისთვის მართლაც მძიმე დარტყმა იქნება. ამ კონტექსტში ცხადია, იმპერიული პოლიტიკური აზროვნებიდან გამომდინარე, მათი მხრიდან მოსალოდნელი იყო და არის კიდეც მთელი რიგი ინსტრუმენტებისა თუ იარაღის გამოყენება, მათ შორის ისეთის, როგორიც რბილი ძალა გახლავთ.

სამხრეთ კავკასიის რეგიონი გამორჩეულია თავის გეოგრაფიით, პოლიტიკური თუ ეკონომიკური, სამხედრო ძალების ბალანსით თუ კულტურული მრავალფეროვნებით. სამ სამხრეთ კავკასიურ სახელმწიფოს - საქართველოს, სომხეთს და აზარბაიჯანს განსხვავებული საგარეო პოლიტიკური კურსი აქვთ, რასაც ცხადია, თავისი როგორც ობიექტური, ასევე სუბექტური მიზეზები გააჩნია. ამავდრულად, თუკი აზერბაიჯანისა და სომხეთის ურთიერთობა კვლავაც დაძაბულობის ხაზზე გადის, საქართველო ორივე ქვეყანასთან კეთილმეზობლურ და

მეგობრულ ურთიერთობას ინარჩუნებს. მეტიც, ცოტა ხნის წინ ოფიცალურმა თბილისმა მათ სამშვიდობო მოლაპარაკების მაგიდაც კი შესთავაზა, ჩვენი პრემიერ-მინისტრის აქტივობისა და ჩართულობის შედეგად კი მოხერხდა სომეხი სამხედრო ტყვეების სამშობლოში დაბრუნება, ხოლო აზერბაიჯანისთვის სომხეთის მიერ დანაღმული ველების რუქების გადაცემა. ეს მართლაც შესანიშნავია, როცა ჩვენი ქვეყანა რეგიონში უკვე სამშვიდობო პროცესების შუამავლად გვევლინება. ის, რომ „საქართველო რეგიონალური თანამშრომლობის გასაღებია!“ - სავსებით სამართლიანად აღნიშნა თურქეთის პრეზიდენტმა რეჯეფ ტაიფ ერდოღანმა. ობიქტურობისთვის უნდა ითქვას, რომ ვინ ვინ და თურქეთი, უკვე წლებია, საქართველოს ჩრდილოატლანტიკურ ალიანში გაწევრინების ერთ-ერთი მხურვალე მხარდამჭერია. თითქოს გასაკვირიც არ უნდა იყოს, მრავალ მიზეზთა შორის, ეს გეოგრაფიული ფაქტორითაც არის განპირობებული: მის სამხრეთ და აღმოსავლეთ სამეზობლოში არის სირია, ერაყი, ირანი და სომხეთი, ცხადია, იმ სასაზღვრო მონაკვეთზე, სადაც საქართველოა, თურქეთს ურჩევნია, ისეთი მეზობელი ჰყავდეს, საიდანაც თუნდაც ნაკლებლად შესაძლო, მაგრამ მაინც საფრთხე არასოდეს დაემუქრება. ნატოს წევრ თურქეთთან მომავალში ნატოს წევრი საქართველოს ურთიერთობა უფრო ძლიერ კავშირში რომ გადავა, ამაში დიდი გათვლების გაკეთება არ არის საჭირო. რაც შეეხება სომხეთსა და აზარბაიჯანს, გამომდინარე ჩვენი ქვეყნის სტრატეგიულ-გეოგრაფიული მდგომარეობიდან, ყოველთვის შეეცდებიან, ჩვენთან არსებული სტატუსქვო შეინარჩუნონ, თუ უფრო მეგობრული თანამშრომლობის გაძლიერებაზე არ იზრუნებენ. ნატოში საქართველოს შესაძლო გაწევრიანება ამ ურთიერთობების დამაბრკოლებელი ფაქტორი არ და ვერ იქნება, ყოველ შემთხვევაში, მათი მხრიდან რაიმე სერიოზულ ხელშეშლას არ ველით.

ამრიგად, რჩება ერთადერთი ქვეყანა, რომელიც ჩვენი ქვეყნის ჩრდილოატლანტიკურ ალიანში გაწევრიანების აბსოლიტურად ღია წინააღმდეგია, რა თქმა უნდა, ეს გახლავთ რუსეთის ფერედრაცია. რუსეთსაც და სხვებსაც, არც თუ იშვიათად ავიწყდებათ, რომ საქართველო დამოუკიდებელი და სუვერენული სახელმწიფოა, რაც იმას ნიშნავს, რომ თვითონ გადაწყვეტს, რა საგარეო პოლიტიკური კურსი აირჩიოს და რომელ საერთაშორისო ორგანიზაციაში გაწევრიანდეს. ამ შემთხვევაში, მთავარი კონტრიარაღი, რომელიც ჩვენ უნდა

დავუპირიპიროთ უმნიშვნელოვანესი მიზნის მისაღწევად, ეს არის ეროვნული გაერთიანება ერთი იდეის გარშემო.

საქართველოს დამუკიდებლობის გამოცხადებიდან 100 წელი და დამოუკიდებლობის აღდგენიდან 30 წელი შესრულდა. ამ პერიოდში ჩვენმა ქვეყანამ უამრავი ქარტეხილი გამოიარა - დამოკიდებლობის დაკარგვა, ისევ აღდგენა-მოპოვება, სამოქალაქო ომები და სახელმწიფო გადატრიალებები. პოლიტიკურ ველზე ათასი ჯურისა თუ ხასიათის პარტიებისა და სუბიექტების შემოსვლა და გასვლა ჩვეულებრივ მოვლენად იქცა. გასაგები მიზეზებიდნ გამომდინარე, ზოგს ამბიცია აქვს, რომ მას შეუძლია სხვაზე მეტი, ზოგს დაავალეს, ზოგს მართლა სჯერა, თუმცა, უფრო და უფრო ნაკლებია იმ ხალხის რაოდენობა, ვინც დროულად მიხვდება და პოლიტიკას თავს დააანებებს. სამწუხაროდ, პოლიტიკური ძალების ნაწილი პრორუსული ორიენტაციისაა და რაც არ უნდა უცნაურად მოგვეჩვენოს, ე.წ. პროდასავლურ ძალებს სულაც არ ეხამუშებათ მათ გვერდით ერთ მაგიდასთან ყოფნა. თავის იმით იმართლებენ, ვითომ „დიადი იდეიისა“ და მიზნის გარშემო არიან თავმოყრილები - ეს მიზანი კი შემდეგია: ნებისმიერ ფასად, თუნდაც რევოლუციით შეცვალონ ხელისუფლება. ასეთი რყევებისა და ქმედებების მთავარი მიზანი მაინც ერთგვარი პოლიტიკური კრიზისისა და დესტაბილიზაციის გამოწვევა გახლავთ. მოგეხსენებათ, პოლიტიკურ კრიზისსა და არასტბილურობას ეკონომიკური კრიზისის გამოწვევა შეუძლია. ამ ფონზე უფრო ნათელი ხდება, თუ რომელი და როგორი ძალების ინტერესშია მსგავსი სცენარი.

როდესაც ვახსენებთ რუსეთს, აქვე აუცილებლად უნდა გავიხსენოთ წარსულიც: 1795 წელს ქართლ-კახეთის მეფე ერეკლე მეორე 5 000 ლაშქრით შეებრძოლა აღა-მაჰმად -ხანის 35 000-იან ჯარს. კრწანისი ბრძოლა სპარსელების მიერ თბილისის აღებით დასრულდა. გეორგიევსკის ტრაქტატის თანახმად კი, რომელიც 1783 წელს იყო ხელმოწერილი, რუსეთის იმპერია ვალდებულებას იღებდა, არ ჩარეულიყო ქართლ-კახეთის საშინაო საქმეებში, უნდა ემართა საგარეო პოლიტიკა და ჯარითაც დახმარებოდა მოკავშირე სამეფოს თუ კი მის წინააღმდეგ საომარი საშიშროება წარმოიქმნებოდა.

რუსეთის იმპერია, სწორედაც, რომ ჯარით უნდა დაგვხმარებოდა, მაგრამ გაგვწირეს. მეტიც, ერეკლეს გარდაცვალებიდან (1798 წწ) სამი წლის თავზე, 1801 წელს რუსეთის იმპერატორ ალექსანდრე I მანფესტით გაუქმდა ქართლ-კახეთის

სამეფო, მოგვიანებით ეტაპობრივად განხორციელდა სხვა სამეფო-სამთავროების გაუქმება და რუსეთის იმპერიაში იძულებით შეყვანა - ფაქტობრივად საქართველოს ანექსია. 1810 წელს ქართულ მართლმადიდებულ ეკლესიას რუსეთის იმპერიის ხელისუფლებამ ავტოკეფალია ჩამოართვა, რომლის აღდგენა მხოლოდ 1917 წელს მოხერხდა.

1918 წლის 26 მაისს ეროვნული საბჭოს მიერ გამოცხადდა საქართველოს დამოკიდებლობა. ორი წლის თავზე - 1920 წლის 7 მაისის ხელშეკრულების თანახმად, ბოლშევიკურმა რუსეთმა დეიურედ ცნო საქართველოს დამოუკიდებლობა, თუმცა ამას ხელი არ შეუშლია მათთვის, რომ 1921 წლის 25 თებერვალს ოკუპაცია განეხორციელებინათ. საბჭოთა კავშირში იძულებით ყოფნა 70 წელი გაგრძელდა. 1991 წლის დამოუკიდებლობის აღდგენის შემდეგ კი იწყება იმ რუსულ-სეპარატისტული ნაღმების ამუშავება, რასაც ქრთულ-ოსური და ქართულ-აფხაზური კონფლიქტი დაარქვეს, სინამდვილეში ეს გახლდათ რუსეთთნ ომი. ამ ყველაფრის დაბოლოება კი 2008 წლის ომი იყო, რასაც ჩვენი ტერიტორიების 20%-ის ოკუპაცია მოჰყვა და აღნიშნულ ტერიტორიებზე რუსული სამხედრო კონტიგენტის უკვე ბაზებად განლაგება. გარდა იმისა, რომ დაიღუპნენ სამხედრო და სამოქალაქო პირები, ჩვენივე ტერიტორიაზე გვყავს იძულებით გადაადგილებულები, რუსეთმა მიწასთან მოასწორა დიდი და პატარა ლიახვის სოფლები, საფუძვლიანად წაშალა ქართული სოფლების გეოგრაფიული ტოპონიმები.

თითქოს ერთი შეხედვით არ ჩანს, მაგრამ უფრო და უფრო მწვავდება დაპირისპირება პრორუსულ და პროდასავლურ ძალებს შორის, განსაკუთრებით კი იმ დროს, როდესაც სახელმწიფოსა და მისი მოსახლეობის საკმაოდ სოლიდურ უმრავლესობას ოფიციალურად აქვს დაფიქსირებული ქვეყნის ევროატლანტიკური მისწრაფებების შესახებ: ნატოსთან თანამშრომლობა, შეიძლება ითქვას, საკმაოდ მაღალ ნიშნულს მიუახლოვდა, გრძელდება რეფორმები და ფართომასშტაბიანი სამხედრო სწავლებები ნატოს ეგიდით. ხელი მოეწერა ევროკავშირთან ასოცირების შეთანხმებას, დაწესდა უვიზო მიმოსვლა შენგენის ზონაში. ყველაფერი გეგმიურად მიდის, თუმცა ხელის შემშლელი ფაქტორებიც ნელ-ნელა იკვეთება - რუსეთის ფედერაცია, გარდა იმისა, რომ ოფიციალურად აცხადებს, არა თუ არ მიესალმება საქართველოს ევროატლანტიკურ ორიენტაციას, ასევე ცდილობს, სხვა დამატებითი ინსტრუმენტები აამუშავოს და არც პირდაპირ მუქარას ერიდება.

სამწუხაროა, ჩვენს ევროატლანტიკურ მისწრაფებებს ფარული თუ ღია მოწინაღმდეგეები ჰყავს, რომლებმაც გადაწყვიტეს არა უხეში მეთოდებით, არამედ რბილი ძალის მეშვეობით მიაღწიონ პროგრამა-მაქსიმუს თუ არა, მინიმუმს მაინც. „რბილი ძალის“ თეორია რეალურად ემიჯნება „უხეში ძალის“ თეორიას. ეს არის მიზიდულობის, ინტერესის გაზრდა ქვეყნისადმი იძულების გარეშე: „ის წარმოიშობა ქვეყნის კულტურის მომხიბვლელობით, პოლიტიკური იდეალებით და ისეთი პოლიტიკით, როცა ჩვენი პოლიტიკა სხვების თვალში ჩანს კანონიერი, ეს აძლიერებს ჩვენს *“რბილ ძალას“*, - წერს ჯ. ნაი. მისი აზრით, კულტურა არის ღირებულებებისა და ინსტრუქციების ნაკრები (ნაზავი), რაც საზოგადოებრივი აზრის ჩამოყალიბებაზე მნიშვნელოვან გავლენას ახდენს. კულტურას ბევრი გამოვლინება აქვს, ის მრავალწახნაგოვანია, მათ შორისაა მაღალი კულტურა - ლიტერატურა, ხელოვნება და განათლება, რომელიც იზიდავს მაღალ საზოგადოებას. ასევეა პოპულარული კულტურა, რომელიც ყურადღებას ამახვილებს მასობრივ გართობაზე. ნატო-ევროკავშირის შესახებ არასაკმარისი ცოდნა ყოველთვის ტოვებს იმ სივრცეს, რასაც ჩვენი ევროატლანტიკური მისწრაფების მოწინაღმდეგეები ადვილად ავსებენ. საქმე ის არის, რომ ერთ-ერთ მთავარ მესიჯად გამოყენებულია ფორმულა, რომ რუსეთი ამას არავითარ შემთხვევაში არ დაუშვებს. მეტიც, ეს შესაძლოა გახდეს მათი მხრიდან ახალი საომარი მოქმედებების დაწყების მიზეზი. აქ ორი მიზანია: პირველი - მოსახლეობის დაზარვა შესაძლო ომის გამო, გაჯერებული იმით, რომ 2008 წლის ომის დროს ნატო საერთოდ არაფერში დაგვეხმარა და მეორე - სახელმწიფოებრიობის იდეის ჩაკვლა, რომ ჩვენ კი არ ვწყვეტთ იმას, თუ რა გვინდა, არამედ სუვერენიტეტი ფორმალური ხასიათისაა და მაინც რუსეთზე ვართ დამოკიდებული. რა თქმა უნდა, ეს ეგრეედ წოდებული ნარატივი ადვილად მოქმედებს ე.წ. საბჭოთა კავშირის ნოსტალგიის მქონე ადამიანებზე, მაგრამ მთავარი ამ სიტუაციაში მაინც ნატოსა და ევროკავშირის შესახებ ინფორმაციის ნაკლებობა გახლავთ.

მეორე სერიოზული გათვლა გახლავთ დეზინფორმაცია იმაზე, რომ ნატოც და ევროკავშირიც მიმართულია ქართული ტრადიციების, კულტურის, ისტორიისა და მართლმადიდებლობის გასანადგურებლად. მოჰყავთ სხვდასხვა მაგალითები, თუ როგორ დაკანონდება ერთსქესიანთა ქორწინება, ან როგორ განთავსდება უცხო ქვეყნის ჯარები საქართველოში, როგორ შემოგვტენიან ათასგვარ „დასავლურ“

რეგულაციებს, მოხდება ადამიანების ათასნაირი *„დაჩიპვა,“* აშენდება სხვდასხვა რელიგიური სახლები, როგორ აიკრძალება ქართული ტრადიცები და ასე შემდეგ. ეს ყოველივე სიცრუე და დეზინფორმაციაა და აქ არამარტო უცოდინრობა არ არის მთავარი. მით უმეტეს, არც ერთი, არც ნატოს ხელშეკრულება, არც ევროკავშირის - მაასტრიხტის ხელშეკრულება მსგავს სისულელეებს (!) არც ასპირანტ და არც მომავალ წევრებს არ ავალდებულებს. სხვათაშორის, ამის ნათელი დადასტურებაა საქართველოს საპატრიარქოს წარმომადგენლების ბრიუსელში ვიზიტი, როდესაც მიტროპოლიტები და ეპისკოპოსები აბსოლუტურად შეცვლილი შთაბეჭდილებებით დაბრუნდნენ, ვგულისხმობთ პოზიტიურს. თუმცა, აღსანიშნავია, რომ ამ მცადარი შეხედულებების გავრცელების საფუძველს ხშირად საქართველოში მოქმედი უამრავი არასამთავრობო იძლევა. თითქოს აქ საგანგაშო არფერია, მაგრამ საზოგადოებისთვის მათ მიერ მოწოდებული ინფორმაცია ხშირად, ცოტა არ იყოს, გადაჭარბებულად ანგაჟერიბულია და ამას ემატება მათ წინააღმდეგ სასწრაფოდ გამოსული გარკვეული და გაურკვეველი „ტრადიციებისა თუ ქართველობის“ დამცველი ფსევდო ჯგუფები. ვინ ვის წისქვილზე ასხამს წყალს, ნებსით თუ უნებლიედ, ეს ცალკე მსჯელობის საგანია, მაგრამ გამომდინარე იქიდან, რომ უბრალო მოქალაქეები ამას არაერთგვაროვნად აღიქვამენ, ცხადია, სწორედ დასავლური ვექტორის წინააღმდეგ მოქმედებს. არადა, სწორედ არასამთავრობო ორგანიზაციებს, ვისაც უშუალოდ ევალება ნატოსა და ევროკავშირის ღირებულებების პროპაგანდა. უშუალოდ მოსახლეობისთვის ინფორმაციის მიწოდება თითქოს მაინც და მაინც არ აღელვებთ.

კიდევ ერთი საინტერესო და აშკარად დამაბნეველი საკითხი: არც თუ ისე დიდხნის წინ ე.წ. მეგობარმა ჯგუფებმა საქართველოში ერთგვარი ტესტი ჩაატარეს, მოაწყვეს კონფერენცია, სადაც ჩრდილოატლანტიკურ ალიანსში გაწევრიანებას შემდეგნაირად განიხილავდნენ - საქართველოს გაწევრიანება ნატოში აფაზეთისა და სამაჩაბლოს გარეშე, მე-5-ე მუხლის ამუშავება, კი მოგვიანებით, როცა ეს მათთვის ე.წ. ტერიტორიები ინტეგრირებული იქნებოდა ჩვენს სახელმწიფოში. თითქოს უბრალო მოსაზრებაა, მაგრამ რა მოჰყვა ამას? საზოგადოების სამართლიანი აღშფოთება. რაც არ უნდა მოხდეს, მიუხედავად იმისა, რომ ჩვენი ტერიტორიების 20% ოკუპირებულია, გამორიცხულია, ვინმე ამ ტერიტორიების ოფიციალურად დაკარგვას შეეგუოს. და აქ რა მოხდა? მცდელობა იმისა, რომ თითქოს ნატო, ამ შემთხვევაში დასავლეთი მოგვიწოდებს ალიანსში გაწევრიანებას აფხაზეთისა და სამაჩაბლოს გარეშე,

ნეგატიური რეაქცია მოჰყვა. არადა, საქმე იქამდე მივიდა, ნატოს გენერალური მდივნის სპეციალურმა წარმომადგენლმა ჯეიმს აპარტურაიმ ოფიციალური განცხადებაც კი გააკეთა - ჩრდილოატლანტიკური ალიანსი არ განიხილავს საქართველოს გაწევრიანების საკითხს მისი ტერიტორიების ნაწილების გარეშე. რაოდენ გასაკვირიც არ უნდ იყოს, ბატონი აპატურაის ამ განცხადებას ძალიან მცირე დრო დაუთმო მასმედიამ, ხოლო მანამდე მავნებლურ ე.წ. ტესტს - *„საქართველო ნატოში-აფხაზეთისა და სამაჩაბლოს გარეშე“,* მთელი დღის ეთერები ჰქონდა მიძღვნილი.

ინფორმაციის ნაკლებობა, ევროატლანტიკური ღირებულებების არასაკმარისი პროპაგანდა სამწუხაროდ არაორაზროვან და ფუჭ შეხედეულებებს ქმნის ევროატლანტიკურ მიზნების შესახებაც. ასეთი მიდგომები კი რუსეთს დამატებით და საკმაოდ მოქნილ პლაცდარმს უქმნის თავის რბილი ძალის გასაძლიერებლად. გასაგებია, რომ რუსეთს ხელს არ აძლევს საქართველოს განვითარება და მით უმეტეს, პროდასვლური კურსი და ევროატლანტიკური ორიენტაცია. ოფიციალურად ომის დაწყება არ შეუძლია, მუდმივად ჩასაფრებულია, რათა რაიმე სახის პოროვოკაციაზე წამოგვიკიდოს. მათთვის საქართველოში არეულობა და პოლიტიკური დესტაბილიზაცია ყველაზე სასურველი სცენარია გავლენის გასაძლიერებლად. სამწუხაროდ, პრორუსული პოლიტიკური პარტიები და მათი მეგობარი ე.წ. პროდასავლურებიც ხშირ შემთხვევაში ხელშემწყობებად გვევლინებიან. ასევე საყურადღებოა, ვითომ დასავლური ღირებულებებით აღჭურვილი არასამთავრობო ორგანიზაციების ნაწილი და მათ წინააღმდეგ მებრძოლი *„ტრადიცულ პატრიოტული“* ჯგუფები ფორმულით - *„ხედავთ, რა ცუდია დასვლეთი?“* ამ ყველაფრის ფონზე კი რუსეთის რბილი ძალა თავის განვითარებას ადვილად პოულობს.[113]

რაც შეეხება პარალელის გავლებას ბალტიისპირეთის ქვეყნებთან, საბჭოთა კავშირის დაშლის შემდეგ მათ თითოეულს ერთმანეთთან და ცალ-ცალკე თავიანთ ქვეყნებში არც პრობლემები აკლდათ, არც გამოწვევები. პრობლემები არ დაივიწყეს, მაგრამ გვერდზე გადადეს, მოხდა კონსოლიდაცია მთავარი იდეის გარშემო და მათ ეს შეძლეს - ისინი ნატოსა და ევროკავშირის წევრები არიან, უსაფრთხოებაც

[113] ნიკოლეიშვილი ლ. "რეგიონალური აქტორის, რუსეთის კიდევ ერთი იარაღი/ინსტრუმენტი საქართველოს წინაღმდეგ", სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემია, გორი, 4-11 გვ. 2021.

გარანტირებული აქვთ და ეკონომიკურად ძლიერები არიან.. საქართველოსთვის ევროატლანტიკურ ოჯახში დამკვიდრება სასიცოცხლოდ მნიშვნელოვანია, ერთი მხრივ ეს არის გზა თავდაცვისა და უსაფრთხოების განმტკიცებისკენ, მეორე მხრივ კი ეკონომიკური განვითარებისკენ. წინააღმდეგობები არის და იქნება - მისი გადალახვა მხოლოდ ეროვნული თანხმობისა და საერთო სამოქალაქო კონსოლიდაციით მიიღწევა.

მიუხედავად იმისა, რომ ბალტიისპირეთის ქვეყნები დიდი სამხედრო პოტენციალით არ გამოირჩევიან, თავიანთი შესაძლებლობის ფარგლებში უკრაინას მაქსიმალური დახმარება აღმოუჩინეს. ასევე, საკმაოდ შეუპოვრები აღმოჩნდნენ რუსეთის წინააღმდეგ სანქციების საკითხში. რა არის ამის მიზეზი? როგორც უკვე აღვნიშნეთ, სამივე ქვეყანამ ფაქტობრივად საბჭოთა კავშირის დაშლისთანავე შეძლო როგორც ნატოში, ასევე ევროკავშირში გაწევრიანება, ჩრდილოატლანტიკური ალიანსი მათთვის, როგორც წევრი ქვეყნებისთვის, თავდაცვისა და უსაფრთხოების გარანტორია. თუმცა რუსეთის მხრიდან მუდმივად საჰაერო სივრცის დარღვევით შანტაჟი და რაც ყველაზე მთავარია, რუსეთთან უშუალო საზღვარი მათ უსაფრთხოებაზე ფიქრი მოსვენებას მაინც არ აძლევდათ. ამიტომაც მუდმივად ითხოვდნენ ალიანსის კონტინგენტის გაზრდას მათ ტერიტორიაზე. რუსეთ-უკრაინის ომმა კი ამ ქვეყნის ლიდერები უფრო დააფიქრა, შემდეგი ნაბიჯი რუსეთმა შესაძლოა მათკენ გადადგას, მით უმეტეს, რუსეთის მხრიდან ომამდეც არაერთხელ გაკეთებულა იმპერიალისტური განცხადებები საბჭოთა კავშირის აღდგენისა თუ ნატოს ძველი საზღვრებისკენ ჩაწევის შესახებ. ბალტიისპირეთს ევროკავშირში გაწევრიანება იმთავითვე მათი ეკონომიკური მდგრადობისა და განვითარების საფუძველი გახდა. შესაბამისად, ამ ქვეყნების რუსეთის ორბიტაზე დაბრუნება ეკონომიკური კოლაფსის ტოლფასია, თუმცა ამის რეალური სურათი ძნელად წარმოსადგენია. საბოლოდ, თუ უკრაინაში რუსეთი დამარცხდება, ბალტიისპირეთის უსაფრთხოება უფრო გამყარდება, ხოლო რუსეთის წარმატების შემთხვევაში, ბალტისპირეთის ქვეყნები სავსებით ლეგიტიმურადაც და ლოგიკურადაც, თავდაცვისა და უსაფრთხოების დამატებით გარანტიებს მოითხოვენ, მით უმეტეს, ნატოს წევრობა, რუსეთის დიდი სურვილის მიუხედავად, მათთვის არავის გაუქმებია.

სამხრეთ კავკასიის და ბალტიისპირეთის ქვეყნების კიბერშესაძლებლობები

როგორც უკვე აღვნიშნეთ, სამხრეთ კავკასიის რეგიონს აქტუალობა ისტორიულად თან სდევს. ამ რეგიონში მიმდინარე პროცესები ყოველდღიურად იცვლება. მისი გეოპოლიტიკური არეალი დიდი ინტერესის სფეროა დიდი ქვეყნებისთვის - რუსეთი, აშშ. ამიერკავკასიის რეგიონში იკვეთება როგორც შავი და კასპიის ზღვების ქვეყნების, ასევე ევროპის, აზიისა და აფრიკის ქვეყნების ეკონომიკურ-პოლიტიკური ინტერესები. სამხრეთ კავკასია ერთგვარი „დერეფანია“ სახმელეთო, საჰაერო და სარკინიგზო კუთხით. აქ არსებული მდგომარეობა გავლენას ახდეს არა მხოლოდ რეგიონის ქვეყნებზე, არამედ მსოფლიო პროცესებზე, ევროატლანტიკურ სივრცეში შექმნილ სიტუაციაზეც. ასეთი ინტერესები იმაზე მიანიშნებს, რომ იგი შეიძლება უახლოეს მომავალში ნატოსთვის ერთგვარი თავდაცვის ტერიტორიადაც იქნას მიჩნეული.

სამხრეთ კავკასიის ქვეყნებში უამრავ გამოწვევასთან ერთად უსაფრთხოების ჭრილში წარმოადგენს საინფორმაციო ომი და კიბერთავდასხმები. ჰიბრიდული ომის ელემენტების გამოყენების დონე რეგიონში ძალიან მაღალია. საინფორმაციო და კიბერომებისგან თავის დაცვა, როგორც უკვე აღვნიშნეთ, მსოფლიოს ყველა ქვეყნისთვის რთული საკითხია, მით უმეტეს ისეთი ქვეყნებისთვის, როგორიც საქართველო, სომხეთი და აზერბაიჯანია. მცირერიცხოვანი სახელმწიფოებისთვის მნიშვნელოვანია, კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების მიმართულებით საერთაშორისო ორგანიზაციების - ნატო-ს, ევროკავშირისა და გაეროს დახმარება, რათა შემუშავდეს ერთიანი სტრატეგიული დოკუმენტი და თავდაცვის მექანიზმები.

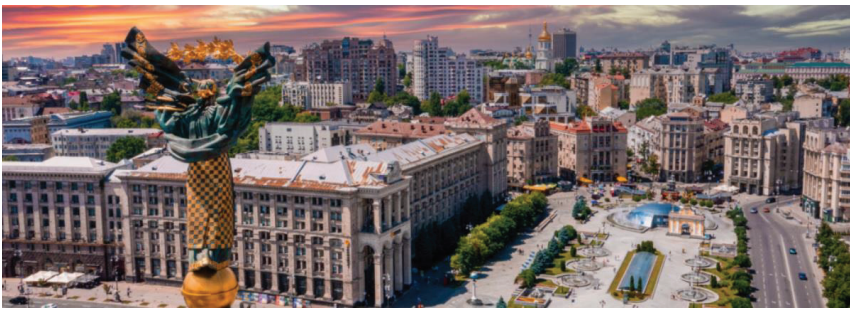
ბევრჯერ ვთქვით და გავიმეორებთ, რომ რუსეთი კონვენციურ ომთან ერთად უკრაინაში აწარმოებს ინტენსიურ საინფორმაციო და კიბერომს. რუსეთის რადარზე ფიქსირდება ასევე საქართველო და რა თქმა უნდა, სამხრეთ კავკასიაც. რუსეთის არაპროგნოზირებად დარტყმებს წინააღმდეგობას ვერც ერთი ნახსენები ქვეყანა

დამოუკიდებლად ვერ უწევს, ჩვენ ერთგვარად მაინც ვიმყოფებით ევროკავშირისა და ნატოს საფარქვეშ. ამ მიმართულებით აქტიურად მონაწილეობს ამერიკის შეერთებული შტატებიც.

კიდევ ერთხელ აღვნიშნავთ, რომ კიბერუსაფრთხოების კონტექსტში უფრო ნათელი გახდეს ჩვენი მსჯდელობა, საბჭოთა კავშირის დაშლის შემდეგ ბალტიისპირეთის სამი ქვეყანა - ესტონეთი, ლატვია და ლიტვა (2004 წელს) ევროკავშირსა და ნატოშიც გაწევრიანდა. თუმცა ამ რეგიონში რუსეთს კვლავ გააჩნია თავისი მავნე ინტერესები და დასავლეთთან დაპირისპირების წყალობით წითელ ხაზად, ანუ ერთგვარ ბუფერულ ზონად აქცია. იყო მოსაზრებები, რომ რუსეთი თავის მიზნების მისაღწევად ვეღარ შეძლებდა სამხედრო შეიარაღების გამოყენებას, იგი მხოლოდ კიბერშეტევებით და საინფორმაციო ომების წარმოებით შეეცდებოდა თავისი მიზნების მიღწევას, ფიზიკურ დაპირისპირებაში არ შევიდოდა, მაგრამ როგორც რეალობა გვიჩვენებს რუსეთი მხოლოდ კიბერ და საინფორმაციო ომით არ კმაყოფილდება.

და მაინც... რა ინტერესები აქვს რუსეთს დამოუკიდებელი სახელმწიფოების მიმართ? უპირველესად ის, რომ დაპყრობაზე ორიენტირებული უზარმაზარი ქვეყანა სამი სახელმწიფოს ნატოში მიღებას საკუთარი საზღვრების ხელყოფად აღიქვამს.

2004 წელს სტამბულის სამიტზე მიღებული გადაწყვეტილება შოკისმომგვრელი აღმოჩნდა კრემლისთვის, აქედან დაიწყო კიდეც მზადება, რათა ნატო მეტად აღარ გაფართოვებულიყო. ფაქტობრივად, აღმოსავლეთ ევროპაში დასავლეთის ასეთი ხისტი ნაბიჯი მოულოდნელი იყო რუსეთისთვის, თორემ ცხადია, კრემლი ბალტიისპირეთშიც შეეცდებოდა, ისეთივე სცენარი გაეთამაშებინა, როგორიც გაათამაშა 2008 წელს საქართველოში და 2014 და 2022 წელს უკრაინაში.



ამასაც დაარქმევდა სპეცოპერაციას. რუსეთის ფედერაცია მზად რომ ყოფილიყო, სამივე ქვეყანაში სიტუაციას არევდა სამხედრო გზით. მით უმეტეს, როცა ბალტიისპირეთში საბჭოთა პერიოდში ჩასახლებული რუსულენოვანი მოსახლეობა არცთუ ცოტაა. ბალტიის ქვეყნებმა რომ "გაასწრეს", ეს განაპირობა რამდენიმე ფაქტორმა: პირველი - 2004 წლამდე თვით რუსეთშიც არ იყო მთლად დალაგებული სიტუაცია, მეორე - როსედაც კრემლმა გამოსცა ე.წ. დეკრეტი საკუთარი მოქალაქეების დაცვის თაობაზე ნებისმიერ ქვეყანაში, ბალტიისპირელებმა თავიდანვე გაითვალისწინეს და როგორც შეძლეს, გაწმინდეს თავიანთი სახელმწიფოები, ანუ რუსულენოვანი მოსახლეობის დიდ ნაწილს არ მისცეს მოქალაქეობა, ამ მხრივ დაწესდა მთელი რიგი შეზღუდვები. მას შემდეგ, რაც სამმა სახელმწიფომ თავი შეაფარა ნატოს ქოლგას, ტექნოლოგიებისა და თავდაცვითი სისტემების წყალობით, შედარებით ეფექტურად შეუძლია კიბერთავდასხმების მოგერიება, რაცამ დონეზე ვერ ხერხდება საქართველოსა და უკრაინის შემთხვევაში.

რუსეთი არ ისვენებს, პერიოდულად ანხორციელებს კიბერთავდასხმებს ბალტიის ქვეყნებზე - 2007-2009 წლებში დიდი შეტევა იყო ესტონეთზე. კრემლის ახალგაზრდული ორგანიზაცია ,,ნაში-''ს ერთ-ერთმა აქტივისტმა აღიარა, რომ ის იყო ბალტიისპირეთის ქვეყნებზე კიბერთავდასხმის სულისჩამდგმელი. ანალიტიკოსების აზრით, ამ შეტევების უკან კრემლი იდგა. ანალოგიური კიბერშეტევა საქართველოზეც განხორციელდა 2008 წლის აგვისტოში რუსეთ-საქართველოს ომის დროს, ასევე 2019 წლის ოქტომბერშიც. პრობლემები შეექმნა ასობით საიტს, გათიშული იყო რამდენიმე ტელევიზია და ვებ-პორტალი. კიბერშეტევა განხორციელდა საქართველოს პრეზიდენტის ადმინისტრაციის ვებ-გვერდზეც - გაჩნდა ექსპრეზიდენტ მიხეილ სააკაშვილის ფოტო წარწერით: „მე დავბრუნდები“. მომდევნო დღეებში საინფორმაციო საშუალებებს დაეგზავნათ წერილები, სადაც ნათქვამი იყო, რომ ,,თავდამსხმელებს" არ აინტერესებდათ არც მიხეილ სააკაშვილი, არც ბიძინა ივანიშვილი, მათ სჭირდებოდათ ფული ბიტკოინების სახით. იმუქრებოდნენ იმუქრებოდნენ იმ მასალების გამოქვეყნებით, რაც თავდასხმის დროს გადატვირთეს სერვერებიდან. ამ ფაქტის თაობაზე არსებობს რამდენიმე ვერსია - შესაძლოა, ეს სულაც არ უკავშირდებოდეს ფულის კეთების ახალ მეთოდს და იყო უბრალოდ რეპეტიცია, შემოწმება; ასევე, შეიძლება ეს ყველაფერი ემსახურებოდა შიშის დანერგვის პროცესს მოსახლეობაში, თითქოს არსებობს რაღაც ძალა, რომელსაც თავისუფლად შეუძლია ნებისმიერი საინფორმაციო საშუალებისა თუ სამთავრობო ვებ-გვერდის დაბლოკვა. საიდან შეიძლება იმართებოდნენ ,,ყოვლისშემძლე" ჰაკერები? დიდი ალბათობით, რუსეთიდან, ხელწერა იგივეა, რაც მოხდა 2008 წლის რუსეთ-საქართველოს ომის დროს.

დღეს მთელი ევროპა და ამერიკა ლაპარაკობს რუსეთიდან მომდინარე საფრთხეებზე. სწორედ ამის გამო, ვარშავაში მიღებული გადაწყვეტილების საფუძველზე ნატო-მ ბალტიისპირეთის ქვეყნებსა 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 რუსეთიდან მომდინარე საფრთხეებისა და მათი სტრატეგიული გავლენის საპასუხოდ მიიღეს. 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. რასაკვირველია, ახალი სამხედრო ტექნოლოგიები გულისხმობს კიბერსივრცის გაკონტროლებასაც და კიბერთავდასხმებსაც.

როდესაც ვსაუბრობთ ბალტიისპირეთის ქვეყნების დღევანდელ მდგომარეობაზე, აქვე პარალელები უნდა გავავლოთ საქართველო-უკრაინის წინააღმდეგ მიმართულ საფრთხეებთან. აქ აშკარად დავინახავთ ერთნაირ ხელწერას. სხვათა შორის, რუსეთს სამხედრო თუ კიბერთავდასხმების მხრივ არ ახასიათებს შემოქმედებითი მიდგომა, არასოდეს ცვლის მეთოდებს, აქვს ერთი სცენარი და ამ სცენარით მოქმედებს ყველა რეგიონში. საქართველოსთან მიმართებაში საინფრმაციო თავდასხმების საფრთხის მაღალ მაჩვენებელს ***სახელმწიფო უსაფრთხოების სამსახურის ბოლო ანგარიშში***[114] მოყვანილი მკაფიო განსაზღვრებებიც ამყარებს. მაგალითად, როგორ ცდილობენ რუსეთის ფედერაცია და სხვა ქვეყნების სპეცსამსახურები საქართველოს ტერიტორიაზე ჰიბრიდული ომის გაჩაღებას. ანგარიშში ნათქვამია, რომ რუსეთი გამალებით ცდილობს, გავლენა მოახდინოს საქართველოს მოსახლეობაზე, შექმნას ილუზია, თითქოს ევროკავშირი, ნატო და ამერიკის შეერთებული შტატები არის მთავარი საფრთხე. ანგარიშის თანახმად, *"რუსეთი საქართველოში ჰიბრიდული ომის ხუთი ძირითადი ინსტრუმენტით მოქმედებს: საოკუპაციო ძალები და დეფაქტო რეჟიმები, საინფორმაციო ომი, ე.წ. რბილი ძალა, ეკონომიკური ექსპანსია, ფარული ოპერაციები".*[115]

2014 წლის შემდეგ, როდესაც რუსეთის ფედერაციამ განახორციელა უკრაინის სუვერენული ტერიტორიის, ყირიმის ნახევრაკუნძულის ოკუპაცია ე.წ. „ჰიბრიუდლი

[114] *ლილუაშვილი გ. „საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში", გვ. 1-27. 2018. http://ssg.gov.ge*
[115] *ლილუაშვილი გ. „რუსეთი საქართველოში ჰიბრიდული ომის ხუთი ძირითადი ინსტრუმენტით მოქმედებს" გვ. 1, 2019. http://parliament.ge*

ომის“ მეშვეობით, საერთაშორისო სამართლის ყველა ნორმისა და პრინციპის უგულებელყოფით, გამოავლინა საკუთარი ამბიცია, იყოს მსოფლიო ბატონი. ერთია სურვილი, მეორეა - რეალობა, ჰეგემონობისკენ ლტოლვას აშშ-ისა და დასავლეთ ევროპის მხრიდან მოჰყვა ეკონომიკური ბლოკადა, რამაც ახალი ცივი ომის სახე მიიღო. აღმოჩნდა თუ არა რუსეთისთვის ეკონომიკური ბლოკადა საკმარისი, რომ მისი შოვინისტური მისწრაფებები ალაგმულიყო? ექსპერტების ნაწილი თვლის, რომ ეს არ იყო ბოლომდე ეფექტური და უფრო მკაცრი სანქციები უნდა განხორციელებულიყო. თუმცა ექსპერტების ნაწილი თვლის, რომ სანქციები საერთოდ უნდა გაუქმდეს. საბოლოო ჯამში, იქმნება შთაბეჭდილება, სანქციები იქნება თუ არა, რუსეთისთვის დიდი მნიშვნელობა არ აქვს, ყოველ შემთხვევაში, კრემლი ხატავს ასეთ სურათს, მით უფრო უკრაინაში შეჭრის შემდეგ. ვფიქრობთ, რუსეთის მოჩვენებითი პოლიტიკა ზედაპირულია - არ შეიძლება, ასეთი აგრესიულმა ქმედებებმა ჩაიაროს უკვალოდ, ანუ ზარალის გარეშე. ერთი პერიოდი ვლადიმერ პუტინს თითქოს გაუმართლა, როცა აშშ-ის პრეზიდენტმა დონალდ ტრამპმა განაცხადა, ჩვენი ქვეყანა აღარ იქნება მსოფლიო პოლიციელის როლშიო. პუტინს, როგორც ჩანს, შექმნა მირაჟი, თითქოს ეს იყო უკანდახევა. პრინციპში, სირია-თურქეთის დაპირისპირებისა და რუსეთ-თურქეთის შეხმატკბილების ფაქტმა გაუჩინა კიდეც ამგვარ შთაბეჭდილებას საფუძველი. მოგეხსენებათ, სირიაში კონტროლის უფლება თურქეთთან ერთად რუსეთმაც მოიპოვა და ერთდროულად ახორციელებენ პატრულირებას. თუმცა ასეთმა ,,წიაღსვლებმა'' არ უნდა შეიყვანოს ექსპერტები შეცდომაში, აშშ და ევროკავშირი მაინც რჩებიან მსოფლიო წესრიგის განმსაზღვრელი ფიგურანტებად.

რა მოხდა შავი ზღვის რეგიონში ყირიმის ანექსიის შემდეგ? ფაქტია, რუსეთის გავლენა უფრო გაიზარდა. პოლიტოლოგების თქმით, თუ ასე გაგრძელდა, აშკარად ჩნდება შავი ზღვის ,,რუსულ ტბად" გადაქცევის პერსპექტივა. რა უნდა გააკეთოს ამერიკის შეერთებულმა შტატებმა, ასე რომ არ მოხდეს? დღის წესრიგში დგება ნატოს გაფართოების საკითხი უკრაინისა და საქართველოს მიმართულებით. სხვათა შორის, ვარშავის სამიტზე ხაზგაზმით აღინიშნა აღმოსავლეთის ფლანგის გაძლიერების აუცილებლობა, ანუ კიდევ უფრო გასაძლიერებელია ბალტიის ქვეყნებისა და პოლონეთის ფლანგი, როგორც სამხედრო თვალსაზრისით, ისე კიბერსივრცის უსაფრთხოების თვალსაზრისით. მართალია, უკრაინაში წამოწყებული ომის

პერიოდში საერთო სურათი შეიცვალა, აშშ-ისა და დასავლეთ ევროპის მიდგომები უფრო გამკაცრდა, მაგრამ რუსული მეთოდები იგივე დარჩა.

როგორ ებრძვიან დღეს რუსულ პროპაგანდას ბალტიისპირეთის ქვეყნებში და რამდენად ეფექტურია ეს ბრძოლა? *"ლატვიამ 2016 წელს რუსული არხი RTR 6 თვით გათიშა. „ნაციონალური ელექტრონული მასმედიის საბჭოს" დადგენილებით, RTR-მა ლატვიის მასმედიის შესახებ კანონი და ევროკავშირის მედიის შესახებ დირექტივა დაარღვია".*[116]

"2015 წელს ლიტვის კომუნიკაციების მარეგულირებელმა კომპანიამ მიიღო გადაწყვეტილება RTR Planet - ის დაბლოკვის შესახებ".[117] ეს ტელევიზია რუსეთის „სახელწიფო რადიო-ტელევიზიის გადამცემი კომპანიის" სერვისის პაკეტში შედის. მიზეზად ვლადიმერ სოლვინის გადაცემა დასახელდა, სადაც წამყვანი პროპაგანდას და სიძულვილის ენას იყენებდა. არხის დაბლოკვა მოხდა ევრკოავშირის მედიადირექტივის თანახმად.

„ევრკოავშირის მარეგულირებელმა ორგანომ გადაწყვიტა, გაეთიშა რუსული არხი, ისტორიას ასეთი რამ არ ახსოვს, ალბათ ბევრი არ ეთანხმდება ამ გადაწყვეტილებას, თუმცა ჩვენ უნდა ვიმოქმედოთ კანონმდებლობის შესაბამისად", - ამის შესახებ მარეგულირებელი სამსახურის პრესპიკერმა ედშუნდას ვაიტიეკუნასმა განაცხადა.[118]

ესტონეთში უნდოდათ, დაებლოკათ ონლაინგამოცემა ***Sputnik-ი.*** თუმცა შემდეგ გადაიფიქრეს, ტელეარხების დროებითი გათიშვა-დაბლოკვა პრობლემას ვერ მოაგვარებდა - მსოფლიო მასშტაბით ხალხი ინტერნეტსივრცის გამოყენებაზეა

[116] *Latvian Public Broadcasting, „Latvia suspends Rossiya RTR channel", p. 1, 2016. https://eng.lsm.lv*
[117] *Lithuanian National Radio and Television, „Lithuanian regulatory agency suspends RTR Planeta", p. 1, 2015. https://www.lrt.lt*
[118] *Baltic News Network, „Lithuanian media regulator has decided to take off air for a three-month period Russian state-owned TV channel RTR Planeta.", p. 1, 2015. https://bnn-news.com*

გადასული. იმ პერიოდში რუსული ტელეარხების გათიშვის თაობაზე საუბარი საქართველოშიც წამოიწყეს, მაგრამ საზოგადოებამ არ მიიღო ეს თემა და არც ხელისუფლება ჩაუღრმავდა საკითხს. ფაქტობრივად, საზოგადოებამ ჩათვალა, რომ დღევანდელი ტექნოლოგიების პირობებში აზრი არ ჰქონდა, ვისაც სურვილი აქვს, სხვადასხვა საშუალებებით რუსულ არხებს ისედაც უყურებს.

დავუბრუნდეთ მთავარ თემას - ახალი ცივი ომისა და უკრაინაში ,,ცხელი ომის'' პირობებში რა სტრატეგიას ირჩევს რუსეთი ბალტიის ქვეყნების, დასავლეთ ევროპისა და ამერიკის შეერთებული შტატების წინააღმდეგ? ვინაიდან, დღეს ძნელად გასარკვევია, სად იწყება თეორიული კიბერომი და სად მთავრდება პრაქტიკული სამხედრო აგრესია, საჭიროა ახალი კვლევები, რეკომენდაციები თუ სამეცნიერო ნაშრომები. ვინაიდან, იმის გარკვევაც კი ჭირს, საიდან იწყება რუსული შოვინიზმი და აქვს თუ არა საერთოდ დასასრული, მსოფლიოს მუდმივად აქვს თავის ტკივილი. სწორედ ამიტომაც აამოქმედა ნატომ ვაშინგტონის ხელშეკრულების მეხუთე მუხლი - „კოლექტიური თავდაცვის“ პრინციპი. მანამდე ჩრდილოატლანტიკური ალიანსი იყენებდა არა მეხუთე მუხლით გათვალისწინებულ ვალდებულებებს, რომლებიც მოიცავენ კრიზისების მართვის ოპერაციებში ჩართულობას. რუსეთმა სამივე დონეზე აამოქმედა თავისი გეოპოლიტიკური და გეოსტრატეგიული ინსტრუმენტები გლობალურ დონეზე: დაპისრისპირება აშშ-სთან და ნატოსთან. ***რუსეთის ეროვნული უსაფრთხოების 2015 წლის ახალ ვარიანტში***[119] მე-16 და მე-17 პარაგრაფებში მთავარ მოწინააღმდეგეებად მოიაზრებიან აშშ და ნატო, ხოლო მეშვიდე პარაგრაფში პირდაპირ არის დაფიქსირებული რუსეთის ფედერაციის როლის ამაღლება მსოფლიო წესრიგის მოწყობის საქმეში. ოფიციალურმა მოსკოვმა სწორედ ჰიბრიდული ომის ელემენტების გამოყენებით შესძლო სერიოზული დარტყმის მიყენება აშშ-სთვის, საპრეზიდენტო არჩევნების დროს, როცა შეიტანა პოლიტიკური არასტაბილურობის ნიშნები აშშ-ს მონოლითურ პოლიტიკურ სისტემაში. იმის მიუხედავად, რომ დონალდ ტარმპი არ იყო კრემლის ფავორიტი, ქვეყანაში მაინც გაჩნდა ეჭვი. საპრეზიდენტო არჩევნებში ჰაკერული ჩარევის ამბავი სრული სიცრუეც რომ იყოს, მაინც წყალს ასხამს პუტინისტური რუსეთის გუნება-განწყობაზე, ანუ ყოვლისშემძლეობის განცდაზე და აჩენს ნიჰილიზმს ამერიკის შეერთებული

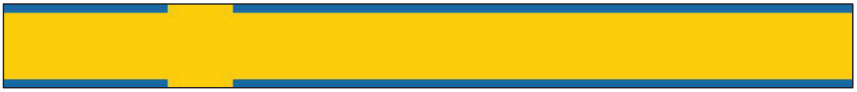
[119] *Russian Federation, "of the 2015 Russian National Security Strategy", Russia Matters, p. 1, 2015. https://www.russiamatters.org/node/21421*

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.

რუსეთი არა მხოლოდ ამერიკის შეერთებულ შტატებს, არამედ მთელ სამყაროს უტევს კიბერმეთოდებით და დეზინფორმაციით. დეზინფორმაცია, რომელიც ვრცელდება დასავლეთ, ცენტრალურ და აღმოსავლეთ ევროპაში, შინაარსობრივად განსხვავებულია, დამოკიდებულია ქვეყნის კულტურულ, პოლიტიკურ და ისტორიულ თავისებურებებზე. ყოველი გზავნილი არის გულდასმით შერჩეული და ძირითადად გათვლილია ამ რეგიონის ქვეყნების რუსულენოვან მოსახლეობაზე.

მაგალითად, ცნობილია, რომ *„სლოვაკეთსა და ჩეხეთში ამერიკის ენერგეტიკული პოლიტიკის კრიტიკაზე არიან ორიენტირებულნი და ცდილობენ, წარმოაჩინონ ისე, თითქოს აშშ მხოლოდ საკუთარი ინტერესებით მოქმედებს და მსოფლიოში კონფლიქტების პროვოცირებას უწყობს ხელს“.*[120]

რუმინეთში სიტუაცია ასეთია: *„რუსეთიდან დაფინანსებული მედიასაშუალებები ცდილობენ, ევროკავშირში გაწევრიანება შეცდომად წარმოაჩინონ და დემოკრატიული ინსტიტუტები დაკნინონ“.*[121]



[120] *Smoleňová I. „The Pro-Russian Disinformation Campaing in The Czech Respublic and Slovakia”, Prague Security Studies Institute, p. 1-18. 2015. http://www.pssi.cz*
[121] *Information Agency „Stop Fake”, „Disinformation and European erosion in Romania“, p. 1, 2019. https://www.stopfake.org*

„შვედეთში მთავრობა სექსუალური გარყვნილების მიმდევრად არის წარმოჩენილი“.[122]

„ფინეთში რუსული მედია-პროპაგანდა ხელისუფლებას რუსულ-ფინური წყვილების განქორწინების დროს ბავშვების მეურვეობასთან დაკავშირებული სასამართლო გადაწყვეტილებების არაკეთილსინდისიერებაში სდებს ბრალს“.[123]

„უკრაინაში დეზინფორმაციული ბრძოლა ხორციელდება - კორუფციაზე, სიღარიბეზე, უწესრიგობაზე, ფაშიზმის აღორძინებასა და დასავლეთის მიერ მართულ „მარიონეტულ“ რეჟიმზე“.[124]

„ლიტვაში, ლატვიასა და ესტონეთში პროპაგანდისტული მანქანა მუშაობს მიმართულებით, თუ როგორი დისკრიმინაციის ქვეშ არიან ამ ქვეყნებში რუსები ეთნიკური თუ ენობრივი მახასიათებლების გამო“.[125]

ბალტიისპირეთში რუსეთის პროპაგანდის მამოძრავებელი ძალაა - ***Первый Балтийский канал.*** ასევე, ონლიაინ საიტი ***Regnum.ru,*** რომელიც 10 წელზე მეტია

[122] *Information Agency “MyTh Detector”, „Geworld Spreads News by Russian Troll Factory on Legalization of Necrophilia and Bestiality in Europe“, p. 1, 2018. https://www.mythdetector.ge*
[123] *Kioski, „Yle Kioski Investigated: This is How Pro-Russia Trolls Manipulate Finns Online – Check the List of Forums Favored by Propagandists“ p. 1. 2015. https://kioski.yle.fi*
[124] *News and View for Ukraine “Euromaidanpress”, „Ukraine remains top target of Russian disinformation“, p. 1, 2019. http://euromaidanpress.com*
[125] *Król A. „Russian Information Warfare in the Baltic States — Resources and Aims“, p. 1, 2017. https://warsawinstitute.org*

ფუნქციონირებს. ბოლო დროს რუსეთმა აამოქმედა საიტი ***Baltnews,*** სადაც ანონიმურად თავსდება ახალი ამბები ესტონურ, ლიტვურ და ლატვიურ ენებზე.

ვერც ბალტიის ქვეყნები, ვერც უკრაინა და ვერც საქართველო ვერ დახარჯავენ ტრილიონობით დოლარს, რათა რუსეთს გაუწიონ წინააღმდეგობა საინფორმაციო ომში. თუ რუსეთს შეუძლია, საქართველოში ფარულადაც და ღიადაც დააფუძნოს რადიოსადგურები, ტელეარხები, სააგენტოები და გაზეთები, ჩვენ არ გვაქვს საშუალება, იგივე გავაკეთოთ რუსეთში. გარკვეული წინააღმდეგობა შეიძლება გასწიო შენივე ქვეყნიდან, მაგრამ ეს არ არის ბოლომდე ეფექტური. მით უმეტეს, როცა ტერიტორიული მთლიანობა მორღვეული გაქვს, როცა 20 პროცენტს საერთოდ ვერ აკონტროლებ. როგორც გერმანული გამოცემა "ბილდი" საკუთარ წყაროებზე დაყრდნობით წერს, თუ 2008 წელს რუსეთ-საქართველოს ომში ამერიკის შეერთებული შტატები ღიად ჩაერეოდა, რუსებს ბალტიის ქყვეყნებზე თავდასხმა ჰქონდათ გადაწყვეტილი. თუ ამერიკელები ბალტიის ქვეყნებსაც დაეხმარებოდნენ, მაშინ ბირთვული იარაღის გამოყენებაზეც ფიქრობდნენ. სანამ რუსეთი უკრაინაში შეიჭრებოდა, ეს ინფორმაცია დაუჯერებლად გვეჩვენებოდა, მაგრამ უკრაინაში გაჩაღებული ომის პერიოდში პუტინის მუქარის შემდეგ, რომ ის გამოიყენებს ბირთვულ იარაღს, ყოველგვარი ეჭვი ქარწყლდება - რუსეთი პალტიისპირეთში აუცილებლად გამოიყენებდა ბირთვულ იარაღს. ,,ბილდის" მიმომხილველი ასევე წერს, რომ ფართომასშტაბიანი სამხედრო სწავლების - "დასავლეთი 2017"-ის ფარგლებში რუსეთი რეპეტიციობდა არა ტერორიზმთან ბრძოლაში, არამედ ნატო-ს წინააღმდეგ ომში და მათ ეს ინფორმაცია დასავლეთის სადაზვერვო მონაცემებზე დაყრდნობით მოიპოვეს. გამოცემა ამტკიცებს, რომ სწავლების სცენარი იყო ბალტიის ქვეყნებისა და ბელორუსის ოკუპაცია რამდენიმე დღეში. ასევე, ე.წ. სწავლება ეხებოდა "შოკურ კამპანიას" ნატოს ქვეყნების წინააღმდეგ - მათ შორის იყო გერმანია, ნიდერლანდები, პოლონეთი, ნორვეგია, ნეიტრალური შვედეთი და ფინეთი. გამოცემის მტკიცებით, რუსეთი ვარჯიშობდა ბალტიის ქვეყნების აეროპორტებისა და პორტების განეიტრალებასა და მათზე კონტროლის დამყარებაზე. მცირე ამონარიდი გამოცემიდან:

,,იმ შემთხვევაში, თუ ომი რეალურად იქნება, მათი მიზანი კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურა გახდება - აეროპორტები, ნავსადგურები, სადგურები და სხვა

ინფრასტრუქტურა, რათა ამ ქვეყნებში შოკი გამოიწვიოს და ადგილობრივმა მოსახლეობამ ხელისუფლებისგან ზავი ითხოვოს". [126]

გამოცემის ცნობით, სწავლების ფარგლებში რუსეთმა დატესტა ქალაქ შპიცბერგენის დაბომბვა და ხელში ჩაგდება. ეს გეგმა პრაქტიკულად არ განხორციელდა, 2008 წლის მოვლენებში ამერიკის შეერთებული შტატები არ წამოეგო რუსეთის პროვოკაციას, მაგრამ რაკი არსებობს მსგავსი მოდელირებული გეგმა, ანუ რუსეთი ჰიბრიდული ომით და კიბერთავდასხმებით მაინც აკეთებს თავის საქმეს, ნუ გამოვრიცხავთ, იგივე სხვა სიტუაციებშიც გამოიყენოს.

სერგეი ლავროვი

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. რუსეთს ბალტიის ქვეყნების წინააღმდეგ გახსნილი აქვს რამდენიმე ფრონტი, სადაც ჩართულნი არიან ხელისუფლების მაღალჩინოსნები. მაგალითად, საგარეო საქმეთა მინისტრმა ***სერგეი ლავროვმა*** ღიად განაცხადა, რომ *"ბალტიისპირეთის ქვეყნები დღემდე ევროკავშირის დოტაციაზე ცხოვრობენ და მათ დახმარება მალე შეუწყდებათ".*[127] რასაკვირველია, ეს არის გამიზნული დეზინფორმაცია, რუსები ცდილობენ, ბალტიის ქვეყნების მოსახლეობას გაუჩინონ ნიჰილიზმი და უიმედობის შეგრძნება - დღეს ევროკავშირი გეხმარებათ, დასავლეთის კმაყოფაზე ხართ, ხვალ ეს დახმარება შეგიწყდებათ და ჩვენ მოგვადგებითო. არადა, სინამდვილეში რა იცის ლავროვმა, რას მოიმოქმედებს ხვალ ევროკავშირი და რატომ უნდა შეუწყვიტოს დახმარება ბალტიისპირელებს? მით უმეტეს, როცა ევროკავშირი განვითარებად სახელმწიფოებს ეხმარება მხოლოდ იმ

[126] *ბასილაია ე. „გერმანული მედია: რუსები 2008 წელს ბირთვული იარაღის გამოყენებას აპირებდნენ", გვ. 1, 2017. http://resonancedaily.com*
[127] *იაგორაშვილი ი. „რუსეთის 2 მითი ბალტიისპირეთის ქვეყნების შესახებ", გვ. 1, 2019. http://www.mythdetector.ge*

მიზნით, რომ ისინი განვითარდნენ. ბალტიის ქვეყნების მიმართ რუსეთი ახორციელებს ასევე იდეოლოგიურ ზეწოლას. ისტორიის გაყალბება - ეს გახლავთ კიდევ ერთი მიმართულება, ანუ დიდი სტრატეგიის ერთ-ერთი ნაწილი, რაც მშვენივრად ჯდება ჰიბრიდული ომის ფარგლებში. ზოგიერთი მკვლევარი ფიქრობს, რომ რუსეთი იმთავითვე მოქმედებდა და დღესაც მოქმედებს მესამე რომის კონცეფციით, სადაც წინა პლანზე წამოწეულია თვითლეგიტიმაცია, ანუ მსოფლიოზე ბატონობის მოპოვება რევოლუციური წიაღსვლებით. ფაქტობრივად, ეს არაფრით განსხვავდება მესამე რაიხის, ანუ იოზიფ გებელსის დოქტრინისგან. ცხადია, თავის დროზე ჰიტლერის ფაშისტურმა რეჟიმმა, იდეოლოგიური თვალსაზრისით, ბევრი რამ წამოიღო მესამე რომის კონცეფციიდან და ასევე ბევრი რამ გადმოიღეს ბოლშევიკებმა. დღეს რუსეთის ურთიერთობას უკრაინასთან და დანარჩენ სამყაროსთან საფუძვლად უდევს გებელსის ბინძური დოქტრინა - კრემლის პროპაგანდას დიდიხანია აღარ გააჩნია საზღვრები. საერთოდ, საინფორმაციო ომის ტაქტიკა და მეთოდოლოგია განსხვავებულია ქვეყნების მიხედვით, ყველა რეგიონს გააჩნია თავისებურება - ისტორია, კულტურა, პოლიტიკური აზროვნებისა და ანალიზის უნარი, განათლების დონე და ასე შემდეგ. თუმცა რუსეთი ამ მხრივ არის სრულიად დაუნდობელი, რასაც ვერ აკეთებს ჰიბრიდული ომით, საინფორმაციო საშუალებებით, კიბერთავდასხმებით, ,,აგვარებს'' სამხედრო აგრესიით.

„საქართველოს 100-წლიანი ბრძოლა კრემლის დეზინფორმაციასთან“, – ამ სათაურით სტატიას ევროკავშირის მიერ დაფინანსებულ ვებგვერდი ***„ევუ ვიეს დეზინფო“ (euvsdesinfo.eu)*** აქვეყნებს. სტატიაში ნათქვამია, რომ საბჭოთა რუსეთმა საქართველოს დამოუკიდებლობასთან და ევროპულ საგარეო კურსთან ბრძოლა 100 წლის წინ, დამოუკიდებლობის გამოცხადების დღიდან, წამოიწყო. გამოცემა აღნიშნავს, რომ საქართველო დღესაც რჩება რუსეთის დეზინფორმაციული კამპანიის სამიზნედ, ევროკავშირის სპეციალურმა დანაყოფმა ასობით მსგავსი შემთხვევა გამოავლინა. რუსეთის დეზინფორმაციული კამპანიის მთავარი გზავნილებია: *„საქართველომ დამოუკიდებლობა დაკარგა“; „საქართველო აშშ-ის პროტექტორატია“;*

„საქართველო ფეოდალური წარმონაქმნია, რომელსაც დასავლეთი მართავს“; „საქართველო თურქეთის მონაა“.[128]

სტატიაში ნათქვამია, რომ კრემლის დეზინფორმაცია აგებულია ერთსა და იმავე გზავნილზე – დამოუკიდებლობის შელახვის საკითხზე, რომლის მორგებაც ნებისმიერ ეპოქაზე, პოლიტიკურ სიტუაციასა თუ ქვეყანაზეა შესაძლებელი. როდესაც ჩვენში მიდის პროპაგანდა, რომ ვართ ამერიკის შეერთებული შტატების მონები, თურქეთის ვასალები, რუსეთს იგივე მიდგომა აქვს ბალტიისპირეთის ქვეყნების მიმართაც - კრემლის მაღალჩინოსნები ლანძღავენ ევროკავშირს იმ მოტივით, რომ როგორმე განხეთქილება შეიტანონ ევროკავშირისა და ბალტიისპირელების ურთიერთობაში. რუსეთს 70-წლიანი ,,ძმობის" პერიოდში კარგად აქვს შესწავლილი პოსტსაბჭოთა ერების ფსიქოლოგია, განათლების დონე, აღქმის უნარი. ამ ქვეყანას ცივილიზებულ სამყაროსთან ომი არ დაუწყია გუშინ და არც იმის იმედი უნდა გვქონდეს, რომ დაამთავრებს ხვალ ან როდისმე, მით უმეტეს, უკრაინაში დატრიალებული ტრაგედიის შემდეგ სამყარო უნდა იყოს მზად ყველაფრისთვის - ჰიბრიდული ომისთვის, სამხედრო აგრესიისთვის და კიდევ ისეთი წინააღმდეგობებისთვის, რაც შეიძლება ვერ წარმოიდგინოს ნორმალურმა დემოკრატიულმა საზოგადოებამ.

გადმოვინაცვლოთ საქართველოში, რა კიბერშესაძლებლობები აქვს ჩვენს სახელმწიფოს? 2013 წელს ახალი კონსტიტუციის ამოქმედების შედეგად, ეროვნულ უსაფრთხოებასთან დაკავშირებული საკითხების დიდი ნაწილი გადავიდა მთავრობის დაქვემდებარებაში. მთავრობის კომპეტენციაში შევიდა ასევე კიბერუსაფრთხოების საკითხი. 2014 წელს უსაფრთხოების მიზნით, თავდაცვის სამინისტროს დაქვემდებარებაში ჩამოყალიბდა კიბერუსაფრთხოების ბიურო. 2015 წელს შინაგან საქმეთა სამინისტროს გამოეყო ეროვნული უსაფრთხოების ბლოკი და ჩამოყალიბდა დამოუკიდებელ უწყებად - უსაფრთხოების სამსახურად. რაც შეეხება

[128] *საქართველოს საზოგადოებრივი მაუწყებელი, „euvsdesinfo.eu აქვეყნებს სტატიას - საქართველოს 100-წლიანი ბრძოლა კრემლის დეზინფორმაციასთან“, გვ. 1, 2019. https://1tv.ge*

სამართალდაცვით საქმიანობას, შინაგან საქმეთა სამინისტროში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო. საქართველოს კიბერუსაფრთხოების ეროვნული სამოქმედო გეგმა ძალაში შევიდა 2017 წელს. საქართველოს იუსტიციის სამინისტროს დაქვემდებარებაშია ციფრული მმართველობის სააგენტო, სადაც ფუნქციონირებს კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების დეპარტამენტი. 2021 წელს ამოქმედდა ***საქართველოს ეროვნული უსაფრთხოების სტრატეგია,***[129] სადაც ყურადღება გამახვილებულია კიბერუსაფრთხოების მიმართულებით საზოგადოების ცნობიერების ამაღლებასა და პროექტებზე, რომლებიც ნატოსთან, ევროკავშირთან, ამერიკის შეერთებულ შტატებთან, ჩეხეთთან, ესტონეთთან და სხვა ქვეყნებთან თანამშრომლობით ხორციელდება.

ფიგურა 3: საქართველოს ეროვნული კიბერუსაფრთხოების ინდექსი. *წყარო: https://ncsi.ega.ee/country/ge/*

„National Cyber Security intex"-ის სტატისტიკის[130] მიხედვით 2019 წელს საქართველო მსოფლიოში მე-19 ადგილზე იყო. ინდექსში საქართველოს 100 სარეიტინგო ქულიდან 64.94 ჰქონდა. ციფრული განვითარების დონით კი საქართველოს სარეიტინგო ქულა

[129] *საქართველოს მთავრობა, "საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგია", საქართველო, თბილისი, 2021. https://matsne.gov.ge/ka/document/view/5263611?publication=0*

[130] *"National Cyber Security intex", "67. Georgia 51.95", 2022. pp. 1-2, https://ncsi.ega.ee/country/ge/?allData=1*

59.66 იყო. 2022 წლის დასაწყისში საქართველომ 51.95 ქულით 61-ე ადგილზე გადაინაცვლა. ხოლო 2022 წლის ბოლოს საქართველოს სარეიტინგო ქულა უცვლელია, მაგრამ პოზიციით 67 ადგილზე გადავიდა. 2023 წელს საქართველო ეროვნული კიბერუსაფრთხოების ინდექსის მონაცემებით 42 ადგილზეა. როგორც უკვე აღვნიშნეთ, როდესაც ევროკავშირის 10 ქვეყნის კიბერუსაფრთხოების ინდექსი განვიხილეთ, ამ შემთხვევაში არსებობს ბევრი კომპონენტი, რომელიც განსაზღვრავს კიბერუსაფრთხოების სარეიტინგო ქულას, მათ შორის არის კიბერშეტევების მომატება, რამაც შეიძლება ქულის დაკლება გამოიწვიოს.

რუსეთ-უკრაინის კიბერომი

როგორც უკვე აღვნიშნეთ, დღეს მსოფლიოში არსებობენ აგრესორი ქვეყნები *(როგორიც არის რუსეთი)* და არსებობენ ჰაკერულ-ტერორისტული დაჯგუფებები, რომლებიც ტექნოლოგიურ მიღწევებს ითვისებენ ავი ზრახვებისთვის. ამჟამად ძალიან სწრაფად იზრდება კიბერსივრციდან მომდინარე საფრთხეები და ამას უფრო ამძაფრებს ის გეოპოლიტიკური ვითარება, რაც მსოფლიო მასშტაბით შეიქმნა. ეს ფაქტობრივად გამოიწვია რუსეთის აგრესიამ უკრაინის წინააღმდეგ. 2022 წლის 24 თებერვლიდან დიდი დრო გავიდა, რუსეთის არმია კვლავაც განაგრძობს სუვერენული სახელმწიფოს მთელ ტერიტორიაზე სახმელეთო, საავიაციო ოპერაციებსა და კიბერთავდასხმებს. რუსეთმა კიბერსივრცეში ომი აქცია ერთგვარ დამატებით იარაღად. კიბერომში ჩართულები არიან როგორც რუსეთის ფედერაციასთან დაკავშირებული ბოროტი ჰაკერული ჯგუფები, ასევე დამოუკიდებელი, ინდივიდუალურად მოქმედი პირები, რომლებიც საკუთარი ინიციატივით ეხმარებიან აგრესორს, თითქოს სიმპატიების გამო. ასევე ცნობილია, რომ გარკვეული ჯგუფები და აქტორები ახორციელებენ კიბერთავდასხმებს, ანუ წინააღმდეგობას უწევენ რუსულ აგრესიას. ერთ-ერთი ასეთი გახლავთ უკრაინის IT არმია, რომელსაც უკრაინის მთავრობა უჭერს მხარს.

როგორც ისტორია გვიჩვენებს, რუსეთი კიბერშეტევებს ყოველთვის ერთი და იგივე ხელწერით ახორციელებს. კიბერექსპერტების თქმით, თავდაპირველად

რუსეთის ფედერაციის მხრიდან მართულმა ჰაქტივისტურმა დაჯგუფებებმა უკრაინის წინააღმდეგ გამოიყენეს მიზანმიმართული კიბერთავდასხმები კრიტიკულ ინფრასტრუქტურაზე, მაგრამ ასევე პარალელურ რეჟიმში საინფორმაციო ოპერაციების წინააღმდეგ აწარმოეს ბრძოლა. ამ უკანასკნელს, როგორც ცნობილია, ორივე მხარე აქტიურად იყენებს. კიბერმკვლევარები განმარტავენ: აღმოსავლეთ უკრაინაში თავდაპირველი შეჭრის ოპერაციები კვალიფიცირდება როგორც კიბერომი, რადგან ყველაფერს თავი რომ დავანებოთ, მათში მონაწილეობდნენ და დღემდე აღნიშნულ პროცესში აქტიურად ჩართულები არიან სახელმწიფოს მიერ დაფინანსებული აქტორები, იყენებენ ერთგვარ კიბერტაქტიკას, რაც რუსეთის მიზნებისა და ამოცანების შესასრულებლად არის საჭირო. ამერიკის შეერთებული შტატები, ნატო, ევროკავშირი და ევროპის წამყვანი ქვეყნები ცდილობენ, უკრაინას დაეხმარონ როგორც რეალურ, ისე კიბერსივრცეში. აღნიშნულ კიბერომს აკვირდებიან საერთაშორისო დონის ექსპერტები, ორგანიზაციები, რათა გაარკვიონ, ვინ ვის მხარეს იბრძვის. არა მხოლოდ ომის დროს, კონვენციური ომის წარმოების გარეშეც ხშირ შემთხვევაში რთულია იმის გამოვლენა, თუ საიდან ხორციელდება კიბერთავდასხმები. თუმცა როგორც აღვნიშნეთ, ამ შემთხვევაში სხვადასხვა ჰაკერული დაჯგუფებები თავიანთ თავზე იღებენ ამა თუ იმ კიბერშეტევას და პირდაპირ გამოხატავენ სიმპატიას რუსეთის ან უკრაინის მიმართ.

უახლოეს წარსულში კიბერსივრცის მკვლევარები ფიქრობდნენ, რომ ამ სფეროში შესაძლებელი იქნებოდა, ბევრი მავნე მიმართულება სასიკეთო საკითხებით შეცვლილიყო - მაგალითად, რეალური კონვენციური ომი სრულად ჩანაცვლებულიყო კიბერომით და ქვეყნებს ვირტუალურ სივრცეში გაეჩაღებინათ ბრძოლა ერთმანეთის წინააღმდეგ. ეს აზრი სრულიად მოწვეტილი აღმოჩნდა რეალობისგან. რეალობა გვიჩვენებს, რომ რუსეთმა და მსგავსმა აგრესორმა სახელმწიფოებმა კონვენციური ომის დროს ერთგვარ დამატებით იარაღად აქციეს კიბერომი. ამ პროცესმა კი გააჩინა უსაფრთხოების მექანიზმების გაძლიერების საჭიროება. თუმცა უნდა ვაღიაროთ, თავდაცვა ძვირი ,,სიამოვნება'' აღმოჩნდა. ცნობილია, რომ მსოფლიო მასშტაბით იხარჯება ასეულობით მილიარდი დოლარი წამყვანი ქვეყნებისა და საერთაშორისო ორგანიზაციების მიერ (ნატო, ევროკავშირი).

რუსეთიდან ციფრული თავდასხმა საქართველომ საკუთარ თავზე არაერთხელ გამოცადა რეალური ომის პარალელურად. ჩვენ ამას ვუყურებთ ბოლო ათწლეულების

განმავლობაში და დღესაც კარგად ვხედავთ უკრაინის მაგალითზე, როგორც ცოცხალი არმიით ომის წარმოებას, ასევე ციფრული ტექნოლოგიების გამოყენებას დრონებით, უპილოტო თვითმფინავებით, თვითმართვადი რაკეტებითა და კიბერთავდასხმებით სხვადასხვა კრიტიკულ ინფრასტრუქტურაზე, მათ შორის დიდი ნაწილი ენერგეტიკულ რესურსებზე. როდესაც ***ვლადიმერ პუტინმა*** მობილიზაციის ბრძანება გასცა, ამან კიბერსივრცეში შავი ბაზრის გააქტიურებაც გამოიწვია. მოგეხსენებათ, კიბერსივრცეში, შავ ბაზარზე (დარკნეტი) იყიდება ბევრი უკანონო საქონელი - იარაღი და ნარკოტიკი. მობილიზაციის გამოცხადების შემდეგ, ომში გაწვევის ასარიდებლად შავ ბაზარზე გაჩნდა ყალბი დასაქმების სერთიფიკატები, ავადმყოფობის დოკუმენტები და ასე შემდეგ. რუსეთი უკრაინასთან ასევე იყენებს ჰიბრიდული ომის ყველა კომპონენტს. ეს არც გუშინ დაწყებულა და არც დღეს, არც ომამდე და არც ომის პერიოდში, რუსული ე.წ. სტრატეგია უკვე ისტორიულ აგრესიად იქცა.

როგორც აღვნიშნეთ, რუსეთ-უკრაინის ომი მეორე წელია მიმდინარეობს. ამ დაპირისპირებაში თითქმის ყველა საომარი იარაღია გამოყენებული, გარდა ბირთვულისა. ამასთანავე, რუსეთი იყენებს ჰიბრიდული ომის ყველა კომპონენტს, ყოველდღიურად ბომბავს უკრაინის ქალაქებს. ამ დროისთვის ცნობილია, რომ ყველაზე მძიმე ბრძოლები ბახმუტში მიმდინარეობს. აქ ერთ-ერთ მნიშვნელოვან საკითხს წარმოადგენს კიბერთავდასხმები. სანამ უშუალოდ დეტალურად ვისაუბრებთ რუსეთ-უკრაინის კიბერომზე, მანამდე უნდა გამოვყოთ რამდენიმე ფაქტი, რომელიც ასახავს, თუ როგორ ახორციელებს რუსეთი კიბერაგრესიას უკრაინის წინააღმდეგ - მაგალითად, 2014 წელს რუსეთ-უკარინის სამხედრო ომს თან სდევდა ჰიბრიდული ომის სხვადასხვა კომპონენტები, ე.წ. ამოუცნობი ტიტუშკების გამოყენება და კიბერშეტევები სამთავრობო უწყებებზე. 2016 წელს ყირიმის ანექსიის შემდეგ, კრიტიკულ ინფრასტრუქტურაზე მოხდა თავდასხმა, სადაც *"გამოიყენეს* ***BlackEnergy*** *ვირუსი, რომელმაც ზამთარში უკრაინის რამდენიმე ქალაქი გათბობის გარეშე დატოვა. 2017 წელს, რუსეთთან დაკავშირებულმა ბოროტმა ჰაკერულმა ჯგუფებმა განახორციელეს კიბერშეტევა -* ***NotPetya,*** *რომელიც გამოსასყიდ კიბერთავდასხმას წარმოადგენს და შიფრავს ფაილებს თანხის სანაცვლოდ. თუმცა ამჯერად აღნიშნული თავდასხმა სხვაგვარად განახორციელეს, რადგან გაანადგურეს ინფორმაცია".*[131]

[131] *CISA Central, "Cyber-Attack Against Ukrainian Critical Infrastructure", p. 1, 2021. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01*

ცნობილია, რომ დაახლოებით 300 000 მდე კომპიუტერი დაინფიცირდა. მსოფლიო მასშტაბით ეს ერთ-ერთ ყველაზე ძლიერ კიბერშეტევად ითვლება.

პაველ როზენკო

ამავე წელს უკრაინის მინისტრთა კაბინეტის შიდა სისტემა ჰაკერების თავდასხმის მსხვერპლი აღმოჩნდა, ამის შესახებ უკრაინის ვიცე-პრემიერმა, ***პაველ როზენკომ (Pavlo Rozenko)*** *„ტვიტერზე“* დაწერა:

„როგორც ჩანს, უკრაინის მინისტრთა კაბინეტის სამდივნო ჰაკერების თავდასხმის ობიექტი გახდა, ქსელი ამჟამად გაჩერებულია“.[132]

2017 წელს არა მხოლოდ უკრაინის მინისტრთა კაბინეტი იყო ჰაკერების თავდასხმის ობიექტი, არამედ შეფერხებით მუშაობდა ენერგოკომპანიები და ეროვნული ბანკი. კიბერშეტევის მსხვერპლი იყო მედიაჰოლდინგი *„ლუქსი“*, კიევის მეტროპოლიტენი, უკრაინის ფოსტა და სხვა. სამიზნეებს შორის იყო ბორისპოლის აეროპორტის სისტემაც, შესაძლებელი გახდა ავიარეისების შეყოვნება.

ყველაზე მასშტაბური თავდასხმა მაინც განხორციელდა 2022 წლის 16 თებერვალს - დაიბლოკა თითქმის ყველა სამთავრობო სტრუქტურის ვებ-საიტი. რუსეთს ღიად ითხოვს: ნატო არ უნდა გაფართოვდეს აღმოსავლეთ ევროპისკენ, ამ ორგანიზაციის წევრები ვერ გახდებიან უკრაინა და საქართველო. რუსეთმა კატეგორიულად მოითხოვა, ამერიკის შეერთებულმა შტატებმა და ევროპამ გადახედონ ბრიუსელის სამიტზე მიღებულ გადაწყვეტილებას და უკან წაიღონ აღმოსავლეთ ევროპის მიმართულებით გაფართოების სტრატეგია. რუსეთს აქვს დიდი შესაძლებლობები კიბერომის თვალსაზრისით და არაერთი მოვლენა ადასტურებს ამას, მაგრამ მის შესაძლებლობებსაც აქვს ზღვარი. ნატომ გამოაქვეყნა

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

კომუნიკე, სადაც ჩაიწერა, ბუქარესტის 2008 წლის გადაწყვეტილება ძალაში რჩება. კომუნიკეში ხაზგასმით არის აღნიშნული, რომ *"საქართველო და უკრაინა ალიანსის წევრები აუცილებლად გახდებიან".*[133] ბუქარესტის სამიტზე მიღებული გადაწყვეტილება ვერ მოინელა რუსეთმა.

არსებობს კიბერუსაფრთხოებასთან დაკავშირებით სხვადასხვა საერთაშორისო მეგაკომპანიების კვლევები, მოსაზრებები და წლიური ანგარიშები, სადაც რუსეთის ფედერაცია, როგორც აგრესორი კიბერმოთამაშე, ხშირად ფიგურირებს. კომპანია ***Maicrosoft-ის*** ანგარიშში, სადაც აღნიშნულია, რომ *"გასული წლის განმავლობაში* ***Maicrosoft-ის*** *მიერ ეროვნული სახემწიფოებიდან დაფიქსირებული კიბერშეტევების 58 პროცენტი რუსეთის ფედერაციიდან იყო წარმოებული. განხორციელებული კიბერშეტევებიდან შარშან 21 პროცენტი იყო წარმატებული, ხოლო დღეს იგი 32 პროცენტს შეადგენს",*[134] რაც იმის მანიშნებელია, რომ რუსული ეროვნული სახელმწიფო აქტორების კიბერთავდასხმები სულ უფრო ეფექტური ხდება. რუსეთის ფედერაციიდან მიზანმიმართულად ხდება სხვადასხვა სამთავრობო უწყებების დაზვერვა და ინფორმაციის შეგროვება. *„ისინი ძირითადად აკვირდებიან და ინფორმაციას აგროვებენ ისეთ სააგენტოებზე, რომლებიც ჩართულები არიან საგარეო პოლიტიკაში, ეროვნულ უსაფრთხოებაში ან თავდაცვაში. რუსეთის ფედერაციის კიბერსამიზნე წლის განმავლობაში იყო სამი ქვეყანა - ამერიკის შეერთებული შტატები, დიდი ბრიტანეთი და უკრაინა".*[135]

[133] *ახალაია ლ., საქართველოს საზოგადოებრივი მაუწყებელი, "ბრიუსელის სამიტი და ნატოს კომუნიკე", ბრიუსელი, გვ. 1. 2021 წ. https://1tv.ge/video/briuselis-samiti-da-natos-komunike/*

[134] *Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/*

[135] *Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/*

კიბერმკვლევარები აკვირდებიან რუსეთ-უკრაინის კიბერომს. ***Cisco-ს*** ცნობით, *"მასირებული კიბერთავდასხმები განხორციელდა 2022 წლის 15 თებერვალს, მეორე კი 24 თებერვალს. ამის შემდეგ **CISA-მ** და **FBI-მ** 17 მარტს ერთობლივი კიბერუსაფრთხოების რეკომენდაციები გამოაქვეყნეს, მათ მოუწოდეს აშშ-ისა და საერთაშორისო სატელიტური კომუნიკაციის ქსელის პროვაიდერების მომხმარებლებს **(SATCOM),** იყვნენ მზადყოფნაში შესაძლო საფრთხეებთან დაკავშირებით. აღნიშნული გაფრთხილება მოყვა 24 თებერვლის კიბერშეტევებს, როდესაც განხორციელდა თავდასხმები **Viasat-სა** და **KA-SAT-ზე,** რამაც შეაფერხა ფართოზოლიანი თანამგზავრული ინტერნეტი უკრაინასა და ევროპის სხვა ქვეყებში".*[136] მსოფლიო მასშტაბით ყველა სახელმწიფო უნდა იყოს მზადყოფნაში - სხვადასხვა აქტორები, რომლებიც გამოირჩევიან ჰაკერული თაღლითური და ინფრასტრუქტურის დამაზიანებელი თავდასხმებით, ცდილობენ, სარგებელი ნახონ - რუსეთ-უკრაინის კონფლიქტი გამოიყენონ ერთგვარ ინსტრუმენტად. მაგალითად, ახალი ამბების, დეზინფორმაციის გავრცელება, შემოწირულობების მოთხოვნა მავნე ბმულებით, დახმარების ფონდების სახელებით და ყალბი ვებ-მისამართებით ან ლტოლვილთა მხარდაჭერის ყალბი ვებ-გვერდებით და სხვა. კიბერსაფრთხეების ანალიტიკოსებმა შეადგინეს კიბერჯგუფების ცრილი, რომლებიც რუსეთ-უკრაინის კონფლიქტში არიან ჩართულები, ანალიზის გაკეთების საშუალებას გვაძლევს კიბერსაფრთხეების ლანდშაფტის შესაფასებლად.

უკრაინის სახელმწიფო სპეციალური კომუნიკაციების სამსახურმა (State Special Communications Service of Ukraine) გამოაქვეყნა ანგარიში ომის დროს რუსეთის კიბერთავდასხმებისა და კიბერსტრატეგიის შესახებ, სადაც ხაზგასმით არის ნათქვამი":

[136] *Cisco Annual Report, "Reimagining the future of connectivity", 2022. https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf*

„24 ნოემბერს რუსეთმა დაიწყო ძლიერი კიბერშეტევები უკრაინის კრიტიკულ ინფრასტრუქტურაზე, კერძოდ, ენერგეტიკულ ობიექტებზე, რათა მომხდარიყო ელექტროენერგიის მიწოდების შეზღუდვა. რუსეთის ფედერაციამ კიბერთავდასხმებთან ერთად პარალელურ რეჟიმში ასევე განახორციელა წერტილოვანი დაბომბვა“.[137]

ამავე ანგარიშში ნათქვამია, საჰაერო დაბომბვასთან ერთად, რომელიც კრიტიკული ინფრასტრუქტურის განადგურებაზე იყო ორიენტირებული, ასევე ხორციელდებოდა საინფორმაციო-ფსიქოლოგიური და პროპაგანდისტული ოპერაციები. ეს მიზნად ისახავდა უკრაინის ხელისუფლებაზე პასუხისმგებლობის დაკისრებას და მოსახლეობაში პროტესტის გაღვივებას.

როგორც აღვნიშნეთ, ამ კიბერშეტევებში ჩართულები არიან სხვადასხვა ჰაკრეული დაჯგუფებები სხვადასხვა დონეზე. როდესაც რუსეთი უკრაინაში შეიჭრა და წამოიწყო კონვენციური ომი, ამას წინ უძღვოდა ტრადიციული კიბერთავდასხმები, რაც დღემდე გრძელდება. არსებობს ჰაკტივისტური დაჯგუფება სახელწოდებით - ***“ანონიმური სუდანი” (Anonymous Sudan).*** ექსპერტების მტკიცებით, იგი არის ბოროტი ჰაკერებით დაკომპლექტებული რუსული ჯგუფი, რომელიც პირდაპირ კავშირშია რუსულ ჰაკტივისტურ დაჯგუფება ***Killnet-თან.*** ამ ჰაკერულ დაჯგუფებას გაცხადებული აქვს, რომ რუსეთ-უკრაინის ომში მხარს რუსეთის ფედერაციას უჭერს, ამიტომ ხშირად უკრაინის საწინააღმდეგოდ მოქმედებს.

„ანონიმური სუდანის“ ისტორიაში ხაზგასმით არის ნათქვამი, რომ დაჯგუფება ახორციელებს კიბერშეტევებს ანტიისლამური აქტივობების გამო. რჩება შთაბეჭდილება, ეს მიზეზი არის გადაფარვა რეალური მიზნებისა, ის გამჟღავნებული პოზიცია, თითქოს ის არის ისლამური ჰაკერული დაჯგუფება, არის გამოგონილი. ეჭვებს ამყარებს ის ფაქტიც, რომ როგორც ***Killnet-ის,*** ასევე ***„ანონიმური სუდანის“***

[137] *CyberScoop, "Ukraine warns of ‘massive cyberattacks’ coming from Russia on critical infrastructure sites", p. 1, 2022, https://cyberscoop.com/ukrainians-warn-of-massive-cyberattacks/*

ყველა სამიზნე იყო ის ქვეყანა, რომელიც ეწინააღმდეგება რუსეთის შეჭრას უკრაინაში.

მიუხედავად იმისა, რომ აღნიშნული ჰაქტივისტური ჯგუფი არ მალავს სიმპათიებს რუსეთის მიმართ, ორ დაჯგუფებას შორის მსგავსება მაინც დიდია. მაგალითად მათი თავდასხმების დიდი წილი მოიცავს ***DDoS*** შეტევებს. 2023 წლის იანვარში ***„ანონიმურმა სუდანმა“*** გამოაქვეყნა განცხადება, რომ იგი დაეხმარა ***Killnet-ს DDoS*** შეტევების წარმოებაში გერმანიის ფედერალური სადაზვერვო სამსახურის წინააღმდეგ. აშკარაა, ***„ანონიმურ სუდანი“*** გახლავთ ჰაკერული დაჯგუფება, რომელიც სუდანშია დაფუძნეული. მას გაცხადებული აქვს, რომ მონაწილეობს კიბერაქტივიზმში და ჰაკერულ პროცესებში მთელი მსოფლიოს მასშტაბით. ეს ორგანიზაცია ითვლება ანონიმური ქსელის ნაწილად, რომელიც წარმოადგენს ჰაქტივისტებისა და აქტივისტების საერთაშორისო გაერთიანებას. აღნიშნული გაერთიანების ფარგლებში ხორციელდება ბევრი გახმაურებული ე.წ. ***#OP*** კიბერთავდასხმა *(#OP არის ერთგვარი შემოკლებული ვარიანტი კიბერსპეცოპერაციის).*[138] ასეთი თავდასხმები ცნობილია, როგორც ***#OPIsrael-ი, #OPAustralia*** და სხვა.

„ანონიმური სუდანი“ ხშირად იყენებს სოციალურ ქსელ ***Telegram-სა*** და ***Twitter-ს*** განცხადებების გასავრცელებლად. თუმცა მისი მიზნები და ამოცანები მაინც ბუნდოვანია. ჩვენ ვეცადეთ, მოგვეპოვებინა სხვადასხვა კვლევები და ამ თემაზე გვემსჯელა.

„ანონიმურმა სუდანმა“ უკრაინაში რუსეთის შეჭრის შემდეგ ბევრ კიბერთავდასხმაზე აიღო პასუხისმგებლობა, მათ შორის საფრანგეთში, გერმაინაში, ჰოლანდიასა და შვედეთში განხორციელებულ ***DDoS*** შეტევებზე. როგორც უკვე აღვნიშნეთ, ერთი მხრივ ცნობილია, რომ ეს კიბერთავდასხმები თითქოს განპირობებულია ანტიისლამური აქტივობების საწინააღმდეგოდ, როდესაც შვედეთში, აქტივისტებმა ყურანი დაწვეს, ამას კიბერთავდასხმები მოჰყვა, დაახლოებით ანალოგიური მიზეზის საფუძველზე განხორციელდა კიბერშეტევები ჰოლანდიის სამთავრობო უწყებების ვებ-გვერდებსა და სისტემებზე, ასევე ***Air France-ზე,*** რა დროსაც მოხდა ავიაკომპანიის საიტიდან მონაცემების მოპარვა. შემდეგ ამას,

[138] *Sigal L., "What You Need to Know About the Anonymous Sudan Hacker Group", CYE Blog, 2023. p. 1. https://cyesec.com/blog/what-you-need-to-know-about-the-anonymous-sudan-hacker-group*

დიდი ალბათობით, გამოიყენებენ შანტაჟისთვის, ფულის გამოძალვისთვის ან გაიყიდება შავ ბაზარზე. ***„ანონიმურმა სუდანმა“*** და ***Killnet-მა*** 2023 წლის მარტში ერთობლივადაც ბევრ კიბერთავდასხმებზე აიღეს პასუხისმგებლობა, მათ შორის ლატვიის სამთავრობო უწყებებზე, ნასას სისტემებზე, უკრაინის სისტემებზე. როგორც ცალ-ცალკე, ასევე ერთობლივად განახორციელეს ***DDoS*** შეტევები საფრანგეთის საავადმყოფოებზე, უნივერსიტეტებზე, აეროპორტებზე, იუსტიციისა და შინაგან საქმეთა სამინისტროების სისტემებზე. სწორედ ასეთი ფაქტების საფუძველზე არსებობს ვარაუდი, რომ ***„ანონიმური სუდანი“*** არის რუსული ჰაქტივისტური დაჯგუფება და ანტიისლამურ კამპანიასთან ბრძოლა უბრალოდ შეფარვისთვის სჭირდებათ.

Killnet-მა რუსეთის მიერ უკრაინაში წამოწყებული ომის შემდეგ რამდენიმე თვეში ***DDoS*** შეტევები განახორციელა სხვადასხვა ორგანიზაციებისა და სახელმწიფო სტრუქტურების სისტემებსა და ვებ-გვერდებზე მთელ მსოფლიოში. ***Killnet-ის*** სამიზნეები აშშ-ის გარდა ყველა ის ქვეყანა აღმოჩნდა, რომელიც ამა თუ იმ ფორმით დახმარებას უწევს უკრაინას. ჰაქტივისტურმა დაჯგუფებამ თებერვალში კიბერთავდასხმები დაიწყო ამერიკის შეერთებული შტატების ათზე მეტ საავადმყოფოზე *„(Stanford Health, Michigan Medicine, Duke Health და Cedar-Sinai და სხვა)“.*[139]

ოქტომბერში ***DDoS*** შეტევები განახორციელა ამერიკის შეერთებული შტატების რამდენიმე აეროპორტზე *„(ლოს-ანჯელესის საერთაშორისო აეროპორტი, ჩიკაგოს ოჰარის საერთაშორისო აეროპორტი, ჰარტსფილდ-ჯექსონ ატლანტას საერთაშორისო აეროპორტი და ა.შ.)“,*[140] რამაც გამოიწვია ფრენების შეჩერება და პარალიზება.

Killnet-მა 2022 წლის აპრილში სრულად გადაიტანა ყურადღება რუსეთის გეოპოლიტიკური ინტერესების მხარდასაჭერად. მისი განცხადებით, *„550-ზე მეტი კიბერთავდასხმა განახორციელეს, აქედან 45 თავდასხმა იყო უკრაინის სისტემებზე, რაც მთლიანი თავდასხმების 10 პროცენტზე ნაკლებია“.*[141]

---

[139] *Check Point Research Team, "The New Era of Hacktivism - State-Mobilized Hacktivism Proliferates to The West and Beyond", p. 1, 2022. https://research.checkpoint.com/2022/the-new-era-of-hacktivism/*
[140] *Check Point Research Team, "The New Era of Hacktivism - State-Mobilized Hacktivism Proliferates to The West and Beyond", p. 1, 2022. https://research.checkpoint.com/2022/the-new-era-of-hacktivism/*
[141] *Check Point Research Team, "The New Era of Hacktivism - State-Mobilized Hacktivism Proliferates to The West and Beyond", p. 1, 2022. https://research.checkpoint.com/2022/the-new-era-of-hacktivism/*

სურათი 4: killnet-ის კიბერთავდასხმები
წყარო: https://www.pinterest.com/pin/464011567858877829/

*„მარტში ჰაკტივისტურმა ჯგუფმა კიბერთავდასხმები განახრციელა ამერიკის შეერთებული შტატების კონექტიკუტის საერთაშორისო აეროპორტზე, აპრილში კიბერშეტევები წამოიწყო რუმინეთის თავდაცვის სამინისტროს, სასაზღვრო პოლიციის, ეროვნული სარკინიგზო ტრანსპორტის კომპანიისა და კომერციული ბანკის ვებ-გვერდებზე, რის შედეგადაც რამდენიმე საათის განმავლობაში აღნიშნული ვებ-გვერდები ხელმისაწვდომი არ იყო. მაისში მასობრივი **DDoS** შეტევები განახორციელეს ევროკავშირის ორ წამყვან ქვეყანაზე - გერმანიასა და იტალიაზე. ხოლო ივნისში კიბერთავდასხმების ორი მნიშვნელოვანი ტალღა განახორციელეს ლიეტუვასა და ნორვეგიის წინააღმდეგ. ივლისში **Killnet-მა** თავისი ძალები მიმართა პოლონეთზე და მოახერხა რამდენიმე სამთავრობო ვებ-გვერდის გათიშვა. აგვისტოში კიბერშეტევები განახორციელეს ლატვიის, ესტონეთისა და ამერიკის შეერთებული შტატების ინსტიტუტებზე. სექტემბერში ჰაქტივისტური დაჯგუფება პირველად დაესხა თავს აზიას და კიბერშეტევები განახორციელა იაპონიაზე, მიზეზი კი იაპონიის მხარდაჭერა იყო უკრაინის მიმართ“.*[142]

Killnet-მა 2022 წლის 8 ივლისს განხორციელებულ ***DDoS*** შეტევებზე, რომელიც აშშ-ის კონგრესის ვებ-გვერდზე მოხდა, გამოაქვეყნა მიმართვა:

[142] *Check Point Research Team, "The New Era of Hacktivism - State-Mobilized Hacktivism Proliferates to The West and Beyond", p. 1, 2022. https://research.checkpoint.com/2022/the-new-era-of-hacktivism/*

„კონგრესს აქვს ფული იარაღის დასაფინანსებლად მთელ მსოფლიოში, მაგრამ ეს არ არის საკმარისი საკუთარი თავდაცვისთვის“.[143]

American Health Associates

დაზარალებული ორგანიზაციები აღნიშნულ კიბერთავდასხმებს განიხილავენ, როგორც საშუალო დონისას, თუმცა უსაფრთხოების ზომების არმიღების შემთხვევაში შესაძლოა დიდი პრობლემები მოჰყვეს. მაგალითად, როდესაც ***Killnet-მა*** ამერიკის შეერთებული შტატების სავადმყოფოებზე განახორციელა კიბერშეტევები, ***ამერიკის ჯანდაცვის ასოციაციამ*** განაცხადა, რომ *„მათი თავდასხმები დიდი ზარალის მომტანი არ არის, მაგრამ შესაძლოა გამოიწვიოს რამდენიმე დღით მომსახურების შეფერხება“.*[144]

მერი მასონი

მიჩიგანის საავადმყოფოს საზოგადოებასთან ურთიერთობის სამსახურის დირექტორი ***მერი მასონი (Mary Mason)*** განმარტავს, რომ ***Killnet-ის*** კიბერშეტევები 2023 წლის 30 იანვარს მოხდა სავადმყოფოს თითქმის ყველა ვებ-გვერდზე *(მაგ. Uofmhealth.org, mottchildren.org და სხვა).* მასონის თქმით:

„არც ერთი ვებ-გვერდი, სადაც მოხდა კიბერშეტევები, არ შეიცავს პაციენტების ინფორმაციას. როდესაც თავდასხმები განხორციელდა, პაციენტებს არანაირი პრობლემა

[143] *Lyngaas S., "Pro-Russia hackers claim disruption of US Congress website", cnn politics, p. 1, 2022. https://edition.cnn.com/2022/07/08/politics/congress-website-disrupted/index.html*

[144] *Vijayan J., "Pro-Islam 'Anonymous Sudan' Hacktivists Likely a Front for Russia's Killnet Operation", Dark Reading, 2023. p. 1, https://www.darkreading.com/attacks-breaches/pro-islam-anonymous-sudan-hacktivists-front-russia-killnet-operation?fbclid=IwAR3RMbRQgQbRcMxmv-iZNGRGsvGEyuMUOK5IRfACYLzZQBPbcPmH6yo5uDA*

არ შექმნიათ თავიანთ ინფორმაციაზე წვდომის, ისინი ჩვეულებრივად იყენებდნენ პორტალ myuofmhealth.org-ს".[145]

ფაქტებს რომ დავაკვირდეთ ***Killnet-ისა*** და ***„ანონიმური სუდანის"*** კიბერთავდასხმები არ არის დიდი ზიანის მომტანი, მაგრამ პროპაგანდა მუშაობს - ისინი ახორციელებენ ძლიერ კიბერშეტევებს. რაც თვალნათლივ ჩანს, მათი მიზანი უბრალოდ ყურადღების მიპყრობა და პრორუსული განცხადებების გავრცელებაა. ისინი თავს ესხმიან მათვრობების, ინსტიტუტების, ორგანიზაციების საჯარო ვებ-გვერდებს, რათა ფართო საზოგადოებას დაანახონ მათი გავლენა და გააჩინონ განცდა, რომ რუსეთი უძლეველია არა მხოლოდ რეალურ სამყაროში, ვირტუალურ სივრცეშიც.

როგორც აღვნიშნეთ, იმის მიუხედავად, რომ ***Killnet-ის*** კიბერთავდასხმები დიდი ზარალის მომტანი არ არის, მაინც არ შეიძლება მისი იგნორირება. ***ამერიკის საავადმყოფოების ასოციაციამ*** განაცხადა, რომ ***Killnet-ი*** არის აქტიური საფრთხე ჯანდაცვის ინდუსტრიისთვისაც:

„ხშირად Killnet-ის კიბერშეტევები არ გვაყენებს დიდ ზარალს, მათ სერვისის შეფერხებით მუშაობა შეუძლიათ გამოიწვიონ, რომელიც როგორც წესი, რამდენიმე საათი, ან ერთი დღე გრძელდება. ამის მიუხედავად, იგი უნდა ჩაითვალოს აქტიურ საფრთხედ მთავრობისა და კრიტიკული ინფრასტრუქტურის თავდაცვითი ორგანიზაციებისთვის, მათ შორის ჯანდაცვის სფეროში".[146]

ბოლო დროს ***Killnet-ის*** განხორციელებული ***DDoS*** შეტევები აშშ-ის, გერმანიის, პოლინეთისა და დიდი ბრიტანეთის სამედიცინო დაწესებულებების სისტემებზე, როგორც ჰაქტივისტურმა დაჯგუფებამ განაცხადა, მთავარი მიზეზი იყო ამერიკის

[145] *Bracken B., "Killnet Gloats About DDoS Attacks Downing Starlink", White House, p. 1, 2022. https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov*
[146] *Bracken B., "Killnet Gloats About DDoS Attacks Downing Starlink", White House, p. 1, 2022. https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov*

შეერთებული შტატების გადაწყვეტილება, გაეგზავნათ საბრძოლო ტანკები უკრაინაში.

ილონ მასკი

Killnet-მა განაცხადა, რომ მათ შეძლეს განეხორციელებინათ სიმბოლური ***DDoS*** შეტევები, რომლებიც მიზნად ისახავდა რუსეთის მხარდაჭერას და უკრაინის მხარდამჭერების დასჯას. მაგალითად, ერთ-ერთი *„სამიზნე იყო **ილონ მასკის (Elon Musk)** ფართოზოლიანი სატელიტური ქსელი **Starlink-ი,** რომელზეც განახორციელეს კიბერთავდასხმები, რის შედეგადაც 18 ნოემბერს ბევრი მომხმარებელი ჩიოდა, რომ ისინი რამდენიმე საათის განმავლობაში ვერ ახერხებდნენ თავიანთ ანგარიშებზე შესვლას. აღნიშნული კიბერშეტევების განხორციელებაში სხვადასხვა დაჯგუფებებიც იყვნენ ჩართულები - მაგალითად, ჰაკერული დაჯგუფება **Radis, Halva, Anonymous Russian** და სხვა“.*[147] ***Killnet-მა*** 17 ნოემბერს *„კიბერთავდასხმები განახორციელა თეთრი სახლის ვებ-გვერდზე, რომელსაც დაარქვა „სატესტო შეტევის 30 წუთი“. ამ შეტევების თაობაზე დაჯგუფებამ გამოაქვეყნა განცხადება, სადაც ვკითხულობთ, რომ მათ სურდათ უფრო დიდი დროის განმავლობაში განეხორციელებინათ თავდასხმები“.*[148] თეთრი სახლი ***DDoS*** შეყევებისგან თავდასაცავად იყენებს სამხედრო დონის დაცვას - ***Automattic-ს.*** ამის შემდეგ, 22 ნოემბერს მათ განახორციელეს *„კიბერშეტევები უელსის პრინცის ვებ-გვერდზე და გამოაქვეყნეს განცხადება, სადაც ნათქვამი იყო, რომ შემდეგი იქნებოდა დიდი ბრიტანეთის ჯანდაცვის სისტემა, ლონდონის საფონდო ბირჟა, ბრიტანეთის არმია და ასე შემდეგ“.*[149]

ჰაქტივისტური დაჯგუფების მიზნები და ამოცანები ზედმეტად რთულ საგანს წარმოადგენს, კიბერთავდასხმების დიდი ნაწილი შეადგენს ***DDoS*** შეტევებს. უნდა დავაკვირდეთ მათ ქმედებებს, ვინაიდან რუსეთ-უკრაინის ომი აქტიურ ფაზაშია,

[147] *Bracken B., "Killnet Gloats About DDoS Attacks Downing Starlink", White House, p. 1, 2022. https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov*
[148] *Bracken B., "Killnet Gloats About DDoS Attacks Downing Starlink", White House, p. 1, 2022. https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov*
[149] *Bracken B., "Killnet Gloats About DDoS Attacks Downing Starlink", White House, p. 1, 2022. https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov*

Killnet-ის სამიზნეების სია შეიძლება გაფართოვდეს და კიბერთავდასხმებმაც მიიღოს უფრო მძაფრი, უფრო დამაზიანებელი ფორმა

საყურადღებოა ის ფაქტიც, რომ ***„ტელეგრამზე“*** → ***Killnet_reserve-ის*** *გამომწერების რაოდენობამ მოიმატა ბოლო პერიოდში 34 ათასიდან მიმდევრების დონემ 85 ათასს გადააჭარბა“.*[150] თუ ამას შევადარებთ ***უკრაინის IT არმიას***, მათ ჰყავთ 200 ათასზე ზე მეტი გამომწერი. აქვე აღსანიშნავია, რომ ***Killnet-ს „ანონიმური სუდანის“*** გარდა ასევე ჰყავს შვილობილი დაჯგუფებები - ***Passion Group, NoName*** და სხვა. ისინი თავიანთი ბოტნეტებით ეხმარებიან ***Killnet-ს DDoS*** შეტევების წარმოებისთვის. როგორც ცნობილია ბოლო პერიოდში *„აღნიშნულმა ჰაქტივისტურმა დაჯგუფებამ* ***Dark Web Marketplace-ისგან*** *მიიღო ფინანსური დახმარება 44 000 აშშ დოლარი“.*[151]

რობ ჯოისი

ამერიკის შეერთებული შტატების ეროვნული კიბერუსაფრთხოების სააგენტოს დირექტორი ***რობ ჯოისი (Rob Joyce)*** ამბობს, რომ რუსეთის ფედერაცია და მის მიერ დაქირავებული ჰაკერები ახორციელებენ თავდასხმებს უკრაინის საინფორმაციო ტექნოლოგიების სისტემებზე. კერძოდ, ერთ-ერთ *„მათ სამიზნეს წარმოადგენს დახურული წრიული სატელევიზიო კამერები, რომლებსაც ადგილობრივი ხელისუფლება და კერძო ბიზნესი იყენებს გარემოს მონიტორინგისთვის“.*[152] რუსი ჰაკერები ცდილობენ, კატეხონ სხვადასხვა მაღაზიებისა და დაწესებულებების უსაფრთხოების კამერები, რათა ინფორმაცია მოიპოვონ დახმარების კოლონების გადაადგილების შესახებ. ***ჯოისი*** ამბობს, რომ ისინი ასევე *„აკვირდებიან რუსი ჰაკერების შესვლას საჯარო ვებკამერებში, რაც ყველასთვის ხელმისაწვდომია, თუმცა*

[150] *Vijayan J. "Inside Killnet: Pro-Russia Hacktivist Group's Support and Influence Grows", Dark Reading, p. 1. 2023. https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows*
[151] *Vijayan J. "Inside Killnet: Pro-Russia Hacktivist Group's Support and Influence Grows", Dark Reading, p. 1. 2023. https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows*
[152] *the Guardian, "Russian hackers 'target security cameras inside Ukraine coffee shops", p. 1, 2023. https://www.theguardian.com/world/2023/apr/11/russian-hackers-target-security-cameras-inside-ukraine-coffee-shops?fbclid=IwAR3JWtpSmI9UvvADsMqx5aVTbM8SjpsvCIUYPX389Ff_HxSarZV_ctLoMIQ*

რუსი ჰაკერები ასევე ამას იყენებენ და უყურებენ დახმარების მიმწოდებელ კოლონებსა და მატარებლებს".[153] ***რობ ჯოისის*** თქმით, *„მათ იციან, რომ რუსები ასევე აკვირდებიან ლოჯისტიკურ სატრანსპორტო კომპანიებს, რათა მეტი გაიგონ უკრაინაში იარაღის მიწოდების შესახებ".*[154]

პეტრე დიდი

ბოლო დროს რუსეთიდან ჰაკერული საქმიანობის შესახებ ინფორმაციამ დიდი რაოდენობით გამოჟონა, ეს იმ ფონზე, როდესაც უკრაინაში ომი მიმდინარეობს და რუსეთის ბევრი მოქალაქეც არ უჭერს მხარს თავის ქვეყანას ამ ომში. რაც შეეხება გამოჟონილ ინფორმაციას, ცნობილი გახდა, რომ მოსკოვის ჩრდილო-აღმოსავლეთ გარეუბანში წლების განმავლობაში არსებობს თითქოს შეუმჩნეველი ოფისი, სადაც აბრაზე გამოტანილია - *„ბიზნესცენტრი".* ამ ოფისის მახლობლად თანამედროვე კორპუსებია აშენებული, მეორე მხარეს ძველი სასაფლაოა, სადაც ომის მემორიალებია წარმოდგენილი. აღნიშნული ტერიტორია ის ადგილია, სადაც ***პეტრე დიდი (Peter the Great)*** ოდესღაც წვრთნიდა თავის არმიას. ცნობილი გახდა, რომ აღნიშნულ ოფისში ჰაკერულ საქმიანობაში გარკვეული პირები ეხმარებიან რუსეთს სამხედრო ოპერაციებში. გავრცელებული ინფორმაციის თანახმად, ისინი ***NTC Vulkan-ის*** თანამშრომლები არიან - პროგრამული უზრუნველყოფის ინჟინერები. ერთი შეხედვით, შეიძლება მათი საქმიანობა კიბერუსაფრთხოების კონსულტაციას მივამსგავსოთ, მაგრამ აღნიშნული კომპანიისგან ინფომრაციისა და ფაილების გაჟონვამ ფარდა ახადა ყველაფერს. ათასობით დოკუმენტი გვაჩვენებს, თუ როგორ მუშაობენ ისინი რუსეთის სამხედრო და სადაზვერვო მიმართულებით ჰაკერული

[153] *the Guardian, "Russian hackers 'target security cameras inside Ukraine coffee shops", p. 1, 2023. https://www.theguardian.com/world/2023/apr/11/russian-hackers-target-security-cameras-inside-ukraine-coffee-shops?fbclid=IwAR3JWtpSml9UvvADsMqx5aVTbM8SjpsvCIUYPX389Ff_HxSarZV_ctLoMIQ*

[154] *the Guardian, "Russian hackers 'target security cameras inside Ukraine coffee shops", p. 1, 2023. https://www.theguardian.com/world/2023/apr/11/russian-hackers-target-security-cameras-inside-ukraine-coffee-shops?fbclid=IwAR3JWtpSml9UvvADsMqx5aVTbM8SjpsvCIUYPX389Ff_HxSarZV_ctLoMIQ*

ოპერაციების მხარდასაჭერად, როგორ ამზადებენ თავდასხმებს კრიტიკულ ინფრასტრუქტურაზე, ავრცელებენ დეზინფორმაციას და ცდილობენ ინტერნეტსივრცეში სიტუაციების კონტროლს. ასევე, ცნობილია, რომ *„მათი საქმიანობა დაკავშირებულია რუსეთის სახელწიფო სამსახურებთან, როგორებიც არის:* ***FSB, GOU, GRU, SVR*** *და სხვა“.*[155] აღნიშნული კომპანიიდან გაჟონილ დოკუმენებში ვხვდებით ისეთ საკითხებს, რომელიც *„**Vulkan-ს** პირდაპირ აკავშირებს სახელგანთქმულ ჰაკერულ დაჯგუფება **Sandworm-თან,** რომელმაც უკრაინაში ორჯერ გამოიწვია ნახევარ მილიონზე მეტი ადამიანის უშუქოდ და გათბობის გარეშე დატოვება, კიბერთავდასხმებით ჩაშალა ოლიმპიადა სამხრეთ კორეაში და შექმნა მსოფლიოში ყველაზე დესტრუქციული მავნე პროგრამა **NotPetya“.***[156] ამ ინფორმაციის გავრცელება ერთ-ერთი კომპანიის თანამშრომელმა შეძლო, რომელმაც უკმაყოფილება გამოხატა რუსეთის შეჭრის გამო უკრაინაში. წყარომ აღნიშნული დოკუმენტები გერმანულ გამომცემლობებს გადასცა, ხოლო ინფორმაციის გავრცელების შემდეგ სხვადასხვა ცნობილმა გამომცემლობებმა, როგორებიც არის: ***The Guardian, The Washington Post*** და სხვა, დაიწყეს ჟურნალისტური გამოძიება, ხუთმა დასავლურმა სადაზვერვო სააგენტომ დაადასტურა, რომ აღნიშნული ფაილები და დოკუმენტები ავთენტური იყო. ფაილები შეიცავს ელექტრონულ წერილებს, პროექტების გეგმებს, კონტრაქტებს, შიდა საინფორმაციო დოკუმენტაციებს, ბიუჯეტებს და სხვა. ამ ფაილებით ირკვევა, რომ რუსი ჰაკერები არაერთხელ უმიზნებდნენ უკრაინულ კომპიუტერულ სისტემებს, ზოგიერთი მათგანი ცნობილი ისედაც იყო, ზოგიერთი არა. ასევე, შესაძლო თავდასხმები, რაც ჯერ არ განხორციელებულა. ამ ინფორმაციაზე დაყრნობით, რუსეთი როგორც რეალურ სივრცეში, ასევე ციფრულ სამყაროშიც მუდმივ კონფლიქტშია დასავლეთთან - ამერიკის შეერთებულ შტატებთან, დიდ ბრიტანეთთან, ნატოსთან, ევროკავშირთან, ავსტრალიასთან, ზელანდიასთან, კანადასთან და ასე შემდეგ. ასევე დოკუმენტებში წარმოდგენილია პოტენციური სამიზნეები და საილუსტრაციო მასალები, რუკა,

[155] *Harding L., Simeonova S., Ganguly M.,Dan Sabbagh D.,"'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics", The Guardian, p. 1, 2023. https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics*

[156] *Harding L., Simeonova S., Ganguly M.,Dan Sabbagh D.,"'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics", The Guardian, p. 1, 2023. https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics*

რომელზეც განთავსებულია შესაძლო კიბერთავდასხმისთვის ნაჩვენები ობიექტები ამერიკის შეერთებულ შტატებში, შვეიცარიაში ატომური ელექტროსადგურის შესახებ მნიშვნელოვანი დეტალები, რაც შემდგომი კიბერთავდასხმებისთვის იქნება საჭირო.

ამით იმის თქმა გვინდა, რომ უკრაინის სასიკეთოდ ამ ბოლო პერიოდის განმავლობაში კიბერსივრცეში ბევრი მოვლენა ვითარდება, თუმცა არც ომის დაწყების პირველი დღეებიდან იყო მთლად კატასტროფულად საქმე, თუ გავითვალისწინებთ და გავიხსენებთ იმ პროცესებს, როგორც განვითარდა 2022 წლის 24 თებერვლის შემდეგ. ექსპერტების ანალიზით, როგორც რეალურ სივრცეში, ასევე ვირტუალურ სივრცეში მნიშვნელოვანი ზარალი განიცადა რუსეთმაც. უკრაინაში რუსეთის მიერ წამოწყებულმა ომმა 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. ***„ანონიმუსმა“,*** რომელიც თავისუფალი, არაცენტრალიზებული ჰაკერული ორგანიზაციაა და აერთიანებს ე.წ. *ჰაკტივისტებს,* გამოაქვეყნა განცხადება, თითქოს მათ შეაღწიეს რუსეთის უსაფრთხოების სისტემებში და გამოიტანეს რუსეთის აგენტების სიები, რასაც ეტაპობრივად გამოაქვეყნებდნენ სახელმწიფოების მიხედვით. თუ ***„ანონიმუსის“*** ჰაკერებმა მართლაც შეაღწიეს რუსეთის უსაფრთხოების სისტემებში, იქიდან რაიმე ღირებული გამოიტანეს, ეს მართლად მნიშვნელოვანი იქნება, რომ გამოქვეყნდეს.

ომის დაწყების შემდეგ *“კიევში დაფუძნებულმა კიბერუსაფრთხოების კომპანია* ***Unit Technologies-მა*** *დაიწყო ჰაკერების დაჯილდოება, თუ ისინი წაშლიდნენ და*

დააზიანებდნენ რუსულ ვებ-გვერდებს. კომპანიამ ამ საქმისთვის 100 000 აშშ დოლარი გამოყო".[157]

"უკრაინამ ხელშეკრულება გააფორმა ***სამხრეთ-აღმოსავლეთ აზიის ქვეყნების ასოციაციასთან (Association of Southeast Asian Nations),*** *რის მიხედვითაც, ავსტრალია და სამხრეთ კორეა აძლიერებენ სამხედრო დახმარებას. ამ პროცესების ფონზე სამხრეთ კორეა და იაპონია შეუერთდნენ ნატოს კოოპერატიულ კიბერთავდაცვით ცენტრს (CCDCOE), რაც რუსეთისთვის აღიქმება, როგორც ნატოს გაფართოება აზია-წყნარ ოკეანეში და ახლო აღმოსავლეთში".*[158] აქედან გამომდინარე, ლოგიკური იქნება, აზია-წყნარი ოკეანის ქვეყნები მოემზადონ მასშტაბური დეზინფორმაციისთვის, დაზვერვისთვის და კიბერთავდასხმებისთვის.

ტომ ტუგენდატი

დიდი ბრიტანეთის უშიშროების მინისტრი ***ტომ ტუგენდატი (Tom Tugendhat)*** საუბრობს რუსეთის მხრიდან მოსალოდნელ კიბერსაფრთხეებზე. მისი თქმით, უკრაინაზე შეტევები რუსეთის მხრიდან მხოლოდ წლის განმავლობაში სამჯერ გაიზარდა და ხორციელდება სარაკეტო თავდასხმების პარალელურად

[157] *Janofsky A., "This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites", The Record by Recorded Future, p. 1, 2022. https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/*

[158] *Rahman A.b.F.M., "The Next Cyber Phase of the Russia-Ukraine War Will Echo in Asia", The Diplomat, p. 1. 2023. https://thediplomat.com/2023/02/the-next-cyber-phase-of-the-russia-ukraine-war-will-echo-in-asia/*

"რუსული ბარბაროსობა სცილდება ბრძოლის ველს და მიზანმართულად ხორციელდება ასევე მშვიდობიანი მოსახლეობის წინააღმდეგ, ჩვენ ვიცით, რომ არსებობს მუდმივი საფრთხე უკრაინის კრიტიკული ინფრასტრუქტურის კუთხით".[159]

ომის დაწყების პირველ პერიოდში უკრაინას ჰქონდა გარკვეული წარმატება მოგერიების თვალსაზრისით, *"რაშიც დიდი წვლილი მიუძღვის დიდ ბრიტანეთს, რადგან მათ შეიმუშავეს დახმარების პაკეტი 6,35 მილიონი ფუნტის სახით."*[160] ეს უკრაინას ეხმარება ინციდენტების აღმოფხვრასა და კოორდინირებულ რეაგირებაზე, ინფორმაციის სწრაფად გაზიარებაზე, დამატებითი აპარატურის შეძენისთვის, ფუნქციონირებასა და პროგრამულ უზრუნველყოფაზე. ცნობილია, რომ ევროპის მასშტაბით რუსეთის მხრიდან კიბერთავდასხმები არ გაზრდილა. თუმცა პოლონეთი აცხადებს, რომ მთავრობის ადმინისტრაციულ სისტემებსა და ვებ-გვერდებზე კიბერთავდასხმებმა ომის დაწყების შემდეგ მოიმატა. მაგალითად, 2022 წლის ოქტომბრის ბოლოს, პოლონეთის სენატის სხდომის შემდეგ განხორციელდა სამთავრობო სისტემებზე კიბერშეტევა. პოლონეთმა პრორუსული ჰაკერული ჯგუფი ***NoName057***[161] დაადანაშაულა. იყო ასევე მეორე ჰაკერული ჯგუფი ***Ghostwriter,***[162] რომელიც კიბერთავდასხმებს ახორციელებს ბელორუსიიდან და აქვს კავშირები კრემლის სამხედრო დაზვერვასთან. ამის შემდეგ პოლონეთის პარლამენტის ზედა პალატამ ერთხმად მიიღო რეცოლუცია, სადაც რუსეთის მთავრობას ტერორისტული რეჟიმი უწოდეს. ასევე უნდა აღინიშნოს, უკრაინამ და აშშ-მა ბოლო პერიოდში დახურეს ცხრა ვებ-გვერდის სერვერები, რომლებიც კიბერკრიმინალებს სთავაზობდნენ კრიპტოვალუტის გადაცვლის სერვისებს. ასეთი ვებ-გვერდები იყო: *„101crypta.com, trust-exchange.org, 24xbtc.com* და სხვა. აღნიშნული კრიპტოვალუტის ბირჟები გარეკლამებული იყო კრიმინალურ ფორუმებზე".[163]

---

[159] *National Cyber Security Centre, "Ukraine cyber defenders in UK for high-level talks", NCSC, p. 1, 2022. https://www.ncsc.gov.uk/news/ukraine-cyber-defenders-in-uk-for-high-level-talks*

[160] *Griffiths C., "The Latest 2023 Cyber Crime Statistics (updated February 2023)" AAG, p. 1, 2022. https://aag-it.com/the-latest-cyber-crime-statistics/*

[161] *Lyngaas S., "Microsoft blames Russian military-linked hackers for ransomware attacks in Poland and Ukraine", cnn politics, p. 1, 2022. https://edition.cnn.com/2022/11/10/politics/microsoft-russian-linked-hackers-poland-ukraine/index.html*

[162] *Toulas B., "Poland warns of attacks by Russia-linked Ghostwriter hacking group", BleepingComputer, p. 1, 2022. https://www.bleepingcomputer.com/news/security/poland-warns-of-attacks-by-russia-linked-ghostwriter-hacking-group/*

[163] *Kovacs E., "US, Ukraine Shut Down Cryptocurrency Exchanges Used by Cybercriminals", Security Week, p. 1, 2023. https://www.securityweek.com/us-ukraine-shut-down-cryptocurrency-exchanges-used-by-cybercriminals/?fbclid=IwAR0xr7MGMHg_RJ2PPh5DRrMlYCJvuoY_34j4CJzKe3A4v8v4tEnNzTuqAyA*

როგორც ვხედავთ, რუსეთ-უკრაინის კონვენციური ომის პარალელურად ციფრული მიმართულებითაც აქტიურ რეჟიმშია და ზარალის დათვლა ამ დრომდე ზუსტად შეუძლებელია. თუმცა, იმ ყოველდღიურ ინფორმაციაზე დაყრდნობით შეგვიძლია დავასკვნათ, რომ ვირტუალურ სივრცეშიც დიდ ზარალს უნდა ველოდოთ. იმის მიუხედავად, რომ უკრაინას ეხმარებან ამერიკის შეერთებული შტატები, ნატო, ევროკავშირი, დიდი ბრიტანეთი, საქართველო და სხვა ქვეყნები, მაინც ვერ ხერხდება თუნდაც ვირტუალურ სივრცეში ბოლომდე უსაფრთხოების უზრუნველყოფა.

სხვადასხვა აქტორები, რომლებიც გამოირჩევიან ჰაკერული თაღლითური და ინფრასტრუქტურის დამაზიანებელი თავდასხმებით, ცდილობენ, სარგებელი ნახონ - რუსეთ-უკრაინის კონფლიქტი გამოიყენონ ერთგვარ ინსტრუმენტად. მაგალითად, ახალი ამბების, დეზინფორმაციის გავრცელება, შემოწირულობების მოთხოვნა მავნე ბმულებით, დახმარების ფონდების სახელებით და ყალბი ვებ-მისამართებით ან ლტოლვილთა მხარდაჭერის ყალბი ვებ-გვერდებით და სხვა. კიბერსაფრთხეების ანალიტიკოსებმა შეადგინეს კიბერჯგუფების ცხრილი, რომლებიც რუსეთ-უკრაინის კონფლიქტში არიან ჩართულები, ანალიზის გაკეთების საშუალებას გვაძლევს კიბერსაფრთხეების ლანდშაფტის შესაფასებლად. რუსეთის მხრიდან დაფინანსებულმა ***მოწინავე საფრთხის ჯგუფებმა (APT)*** გამოავლინეს უნარი, შეინარჩუნონ მუდმივი, ამოუცნობი, გრძელვადიანი წვდომა და უნებართვო წვდომა ქსელებში, ლეგიტიმური სერთიფიკატების გამოყენებით. რა თქმა უნდა, როგორც უკვე განვიხილეთ რუსეთის დაქირავებული და მართული ჰაქტივისტური ჯგუფები, როგორებიც არიან ***Killnet-ი*** და ***„ანონიმური სუდანი“*** წარმოადგენენ დიდ საფრთხეს უკრაინისთვის და ქვეყნებისთვის, რომლებიც მხარს უჭერენ მას, თუმცა ამის გარდა კიდევ ბევრი მართული მოწინავე საფრთხის ჯგუფები არიან ჩართულები აღნიშნულ პროცესში. ისინი წარმოადგენენ კიბერშეტევების ყველაზე მაღალ რისკს, როგორებიც არიან რუსეთის ***APT*** ჯგუფები: *„**APT28, Turla, Gamaredon, Energetic Bear, APT29, Sandworm** და სხვა“.*[164]

მოგეხსენებათ, ევროკავშირი, ამერიკის შეერთებული შტატები და ნატო ყოველდღიურად მუშაობენ რუსეთისთვის სანქციების დაწესებაზე. აშშ-ის პრეზიდენტის ადმინისტრაციამ უამრავ შეზღუდვასთან ერთად *„განსაზღვრა რუსეთის*

[164] *Curatedintel, "Curated Intelligence Stands With Ukraine", p. 1, 2022. https://www.curatedintel.org/2022/02/curated-intelligence-stands-with-ukraine.html*

ფედერაციის მოწყვეტა გლობალური ინტერნეტსივრციდან",[165] რაც ნამდვილად შემაშფოთებელ საფუძველს იძლევა კიბერკრიმინალებისთვის, რომლებიც რუსეთის მხარეს მოქმედებენ. რუსეთის ფედერაცია ცდილობს, პარალელურად გააკონტროლოს ინფორმაციის ნაკადი, რაც ცენზურის საზღვრების დაწესებას გულისხმობს ციფრულ ეპოქაში. რუსეთი ცდილობს, დაბლოკოს, დააჯარიმოს და ცენზურა დაუწესოს ყველა დასავლური სოციალური მედიის პლატფორმას. *,,რუსეთის მთავრობამ გამოსცა ბრძანება, რომ სახელმწიფო ვებ-გვერდები დაუკავშირდნენ სახელმწიფოს კონტროლირებად დომეინის სისტემის სერვერებს, რათა სრულად მოხდეს გადართვა რუსული ჰოსტინგების პროვაიდერებზე".*[166]

დიმიტრი ალპეროვიჩი

კიბერანალიტიკური ცენტრის ***Silverado Policy Accelerator*** დირექტორი ***დიმიტრი ალპეროვიჩი (Dmitri Alperovitch)*** განმარტავს:

„რუსეთის ფედერაციამ საერთო ჯამში ვერ მიაღწია კიბერტაქტიკურ წარმატებას. იყო შიში, რომ სხვა ქვეყნებზეც გავრცელდებოდა ისეთი მნიშვნელოვანი კიბერთავდასხმები რუსეთის ფედერაციის მხრიდან, როგორიც უკრაინაზე, თუმცა ეს არ მომხდარა".[167]

არსებობს პროგნოზი, რომ რუსეთის მხრიდან კიბერშეტევები უფრო გაძლიერდება. როცა საქმე რუსეთს ეხება, ყველაფრის პროგნოზირება რთულია, მაგრამ სპეციალისტების მიერ გაკეთებული არაერთი ანალიზი ამაზე მეტყველებს.

[165] *Franck T., "Biden vows wider sanctions on Russia in effort to cut Moscow off from the global economy", cnbc, p. 1, 2022. https://www.cnbc.com/2022/02/24/biden-vows-wider-sanctions-on-russia-in-effort-to-cut-moscow-off-from-the-global-economy.html*

[166] *Flashpoint Team, "Understanding Russia's "Sovereign Internet": What Happens If Russia Isolates Itself from the Global Internet?", p. 1, 2022. https://flashpoint.io/blog/russian-runet-sovereign-internet/*

[167] *Maigre M., "NATO's Role in Global Cyber Security", p. 1, 2022. https://www.gmfus.org/news/natos-role-global-cyber-security*

თავდასხმები გაძლიერდება მხოლოდ უკრაინის მიმართულებით თუ სხვა ქვეყნებსაც მოიცავს, ამ ეტაპზე არავინ იცის. ფაქტი ფაქტად რჩება, გადის დრო და რუსეთი ცდილობს, ომი იყოს ხანგრძლივი და დამღლელი, მათ შორის კიბერსივრცეშიც. 2023 წელს გამოქვეყნდა ***უკრაინის კიბერუსაფრთხოების სააგენტოს ანგარიში,*** სადაც ვკითხულობთ:

„კიბერთვდასხმები მთლიანად შეესაბამება რუსეთის ფედერაციის ზოგად სამხედრო თავდასხმით სტრატეგიას".[168]

მიკე ეოიანგი

მიკე ეოიანგი (Mieke Eoyang), რომელიც პენტაგონში თავდაცვის მდივნის თანაშემწის მოადგილე გახლავთ კიბერპოლიტიკის საკითხებში, აცხადებს:

„რუსეთის კიბერშესაძლებლობების გათვალისწინებით, მათ მოლოდინის საწინააღმდეგოდ იმოქმედეს, რაც შთაბეჭდილებას ქმნის, რომ რუსეთი არ იყო მზად ასეთი ხანგრძლივი და მძლავრი კიბერომისთვის".[169]

ამ ეტაპზე რუსეთის ფედერაცია იყენებს ინფორმაციული ოპერაციების სრულ სპექტრს, ღიად მხარდაჭერილი და ფარული პლატფორმებით თუ ანგარიშებით დამთავრებული - ამახინჯებს ფაქტებს, მოვლენებს, ხალხს აწვდის გამოგონილ ვერსიებს და ცდილობს, ასე გავიდეს ფონს. ექსპერტები აღნიშნული ქმედების სამ მიზანს გამოყოფენ: პირველი - ეს არის უკრაინის ხელისუფლებისთვის ძირის გამოთხრა, მეორე - უკრაინისთვის საერთაშორისო მხარდაჭერის შეჩერება, მესამე - რუსეთის შიგნით მოსახლეობის მხარდაჭერს შენარჩუნება.

---

[168] *Kovacs E. "A Year of Conflict: Cybersecurity Industry Assesses Impact of Russia-Ukraine War", p. 1, 2023. https://www.securityweek.com/one-year-of-russia-ukraine-war-cybersecurity-industry-sums-up-impact/*

[169] *Kagubare I., "Russia's cyber forces 'underperformed expectations' in Ukraine: senior US official", The Hill, p. 1, 2022. https://thehill.com/policy/cybersecurity/3738506-russias-cyber-forces-underperformed-expectations-in-ukraine-senior-us-official/*

ჩვენ არ ვიცით, ომი კიდევ რამდენ ხანს გაგრძელდება. მართალია, უკრაინას ინტენსიურად ეხმარებიან მოწინავე ქვეყნები, მაგრამ ანალიტიკოსების მტკიცებით, ეს საკმარისი არ არის. რაც ხდება რეალური ომის პირობებში, თითქმის იგივე ხდება ვირტუალური ომის პირობებში, ანუ ინტერნეტსივრცეში. ამ ორი მოვლენის განხილვა განყენებულად შეუძლებელია. უკრაინას სჭირდება უახლესი ტექნოლოგიებით აღჭურვილი თავდაცვითი სისტემები არა მხოლოდ იარაღის სახით, არამედ კიბერუსაფრთხოების თვალსაზრისით. თუ ვინმე ამ საკითხს ზერელედ უყურებს, ის ცდება, კიბერსივრცის დაპყრობას შეუძლია, მწყობრიდან გამოიყვანოს მნიშვნელოვანი ინფრასტრუქტურა და საომარი ბაზებიც კი. საჭიროა დიდი ყურადღება, აღჭურვა, დაკვირვება, შესწავლა და მოქმედება.

დღეს რუსეთის ხელისუფლება ხშირად ახსენებს ბირთვულ იარაღს. ყველამ ვიცით, რომ ეს იქნება სრული კატასტროფა კაცობრიობისთვის. არ არის გამორიცხული, ამ შემთხვევაშიც მხოლოდ შეშინების მიზნით წამოწყებულ პროპაგანდასთან გვქონდეს საქმე, მაგრამ ვიცით რა, რუსეთის ხასიათი და ბუნება, ვერ ვენდობით, კრემლი ნამდვილად არის ამაზე წამსვლელი. ამიტომ მთელი მსოფლიო ვალდებულია, წინ აღუდგეს რუსულ აგრესიას - ნატომ, ევროკავშირმა, ამერიკის შეერთებულმა შტატებმა უნდა შეიმუშაონ ეფექტური პროგრამები, სადაც დეტალურად იქნება გაწერილი უკრაინის დახმარება. ფაქტობრივად, ყველა წამყვანმა ქვეყანამ თავისი გადამწყვეტი სიტყვა უნდა თქვას და ეს საქმითაც გამოხატოს.

კიბერსარგებელი, ხარჯები და ზარალი

უკვე აღვნიშნეთ, რომ მსოფლიო მასშტაბით იხარჯება ძალიან დიდი თანხები, როგორც ქვეყნების, ასევე საერთაშორისო ორგანიზაციების მხრიდან. მსოფლიოში წამყვანი სამეცნიერო-საკონსულტაციო კომპანია ***„Gartner“-ის*** მონაცემების მიხედვით კიბერუსაფრთხოების ხარჯებთან დაკავშირებით, მაგალითად, 2019 წელს

დანახარჯი შეადგენდა 124,116 მილიარდ დოლარს,[170] ხოლო 2022 წელს 133.7 მილიარდ დოლარს მიაღწია.[171]

ასევე ***„Gartner"-ის*** ვარაუდით, მომხმარებელთა დანახარჯები ინფორმაციული უსაფრთხოებისა და რისკების მართვის ბაზრისთვის 2022-2026 წლებში გაიზრდება 267,3 მილიარდი დოლარით, რაც, რა თქმა უნდა, ძალან დიდი ფინანსური რესურსია.[172]

თუმცა საყურადღებოა, მსოფლიოსთვის მიყენებული ზარალი ბევრად აღემატება უსაფრთხოების სფეროში დახარჯულ თანხებს, ***„Cybersecurity Ventures"-ის*** ანგარიშში ნავარაუდებია, რომ ეს არის 6 ტრილიონი აშშ დოლარი. არსებობს მოლოდინი, გლობალური კიბერდანაშაულის ხარჯები ყოველწლიურად გაიზრდება და 2025 წლისთვის მიაღწევს **10,5 ტრილიონ** აშშ დოლარს[173] ეს კი მიანიშნებს იმაზე, რომ კიბერომებისა და კიბერშეტევების ტენდენცია მასშტაბურ სახეს იძენს.

"Astute Analytica"-მ 2022 წელს გამოაქვეყნა კვლევა, რომელშიც ნათქვამია, რომ კიბერუსაფრთხოების გლობალურმა ბაზარმა 2021 წლისთვის 162,9 მილიარდს მიაღწია. კიბერუსაფრთხოების ბაზრის 41.6 პროცენტს წარმოადგენენ ისეთი

[170] *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, Consulting Agency Gartner, 2018, p 1. https://www.gartner.com*
[171] *Sobers R. 110 Must-Know Cybersecurity Statistics for 2020, Software Company Varonis, 2020, p 1. https://www.varonis.com*
[172] *Gartner, "Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 2Q22 Update", United Kingdom, p. 1, 2022. https://www.gartner.com/en/documents/4016190*
[173] *Morgan S. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", 2022. p. 1, https://cybersecurityventures.com/*

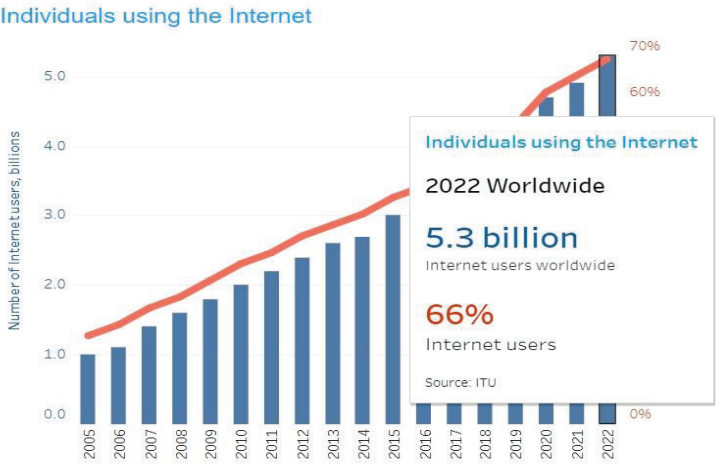
ტექნოლოგიური კომპანიები, როგორებიც არიან: Trend Micro, Cisco, Palo Alto, IBM და სხვა.[174]

კვლევითი კომპანია ***„Accenture"-ის*** ვარაუდით, კიბერუსაფრთხოების სექტორში მომსახურების გლობალური ბაზარი 2022-2025 წლებში გაიზრდება წელიწადში 13 პროცენტით და 2025 წლისათვის 94 მილიარდი დოლარი იქნება. კიბერუსაფრთხოების სექტორში მომსახურების გლობალურ ბაზარში შედგის აპლიკაციები, ოპერაციების ავტომატიზაცია, კრიტიკული ინფრასტრუქტურა და სხვა.[175]

კიბერუსაფრთხოება 21-ე საუკუნეში არის უმთავრესი პრიორიტეტი როგორც სახელმწიფოებისთვის, საერთაშორისო-კერძო ორგანიზაციებისთვის და მომხმარებლებისათვის, განსაკუთრებით კოვიდ 19 -ის შემდეგ, რამაც შეცვალა ცხოვრებისა და მუშაობის ფორმები, გამოიწვია ციფრულ ინფრასტრუქტურაზე უფრო დიდი დამოკიდებულება. პანდემია, შეიძლება ვთქვათ, დასრულდა, მაგრამ მიდგომები და მუშაობის სტილი მაინც შენარჩუნდა. საერთაშორისო წამყვანი ანალიტიკური კომპანია ***„GlobalData"-ს*** ვარაუდით, *"კიბერუსაფრთხოების გლობალური შემოსავალი 2021 წლიდან, რომელიც იყო 220 მილიარდი დოლარი, 2026 წლისთვის 334 მილიარდ დოლარამდე გაიზრდება".*[176]

[174] *IT (global market), "Information Security (Global Market)", Tadviser Goverment. Business. IT, p. 1, 2022. https://tadviser.com/index.php/Article:Information_Security_(Global_Market)#.2A_The_global_IB_services_market_will_reach_.2494_billion_by_2025*
[175] *IT (global market), "Information Security (Global Market)", Tadviser Goverment. Business. IT, p. 1, 2022. https://tadviser.com/index.php/Article:Information_Security_(Global_Market)#.2A_The_global_IB_services_market_will_reach_.2494_billion_by_2025*
[176] *Frank E. "Global Cyber Security Revenue to Reach $334 Billion in 2026: GlobalData", Security Review Magazine, p. 1, 2022. https://securityreviewmag.com/?p=24826*

საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU) *კვლევაზე დაყრდნობით, "2022 წლისთვის მსოფლიო მოსახლეობის 66 პროცენტი იყენებს ინტერნეტს, ეს არის დაახლოებით 5,3 მილიარდი ადამიანი. 2019 წელთან შედარებით მონაცემები 24 პროცენტით არის გაზრდილი. აქედან გამომდინარე, დაახლოებით 2,7 მილიარდი ადამიანი ჯერ კიდევ არ მოიხმარს ინტერნეტს".*[177]



ცხრილი 5: ინდივიდები, რომლებიც იყენებენ ინტერნეტს. *წყარო: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx*

კიბერსაფრთხეები და თავდაცვითი მექანიზმები

უკვე არაერთხელ აღვნიშნეთ, რომ თანამედროვე ტექნოლოგიებმა ყველა სფერო მოიცვა და თითქმის ნებისმიერი ადამიანის ცხოვრებაში შეაღწია. აქედან

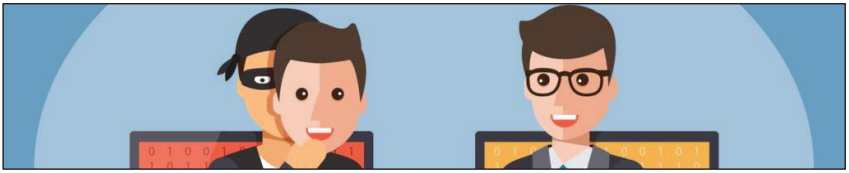
[177] *Committed to connecting the world, "Statistics", p. 1, 2022. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx*

გამომდინარე, მნიშვნელოვანია როგორც ინდივიდუალურ, ასევე ორგანიზაციულ თუ სახელმწიფო დონეზე ვიცოდეთ, როგორ ავიცილოთ კიბერსაფრთხეები, როგორ დავაღწიოთ თავი, რა არის გამოსავალი, როდესაც ვხდებით კიბერშეტევის სამიზნეები, როგორ შეიძლება, მინიმუმამდე დავწიოთ კიბერრისკები. ჩვენ უპირველესად უნდა გავიგოთ, რა პროგრამებს იყენებენ ჰაკერები და რა მეთოდებით მოქმედებენ, რათა მიაღწიონ სასურველ მავნე მიზანს. ისინი იყენებენ დამაზიანებელ პროგრამებს, თაღლითურ კიბერთავდასხმებს, ვირუსებს და ასე შემდეგ. ამას მოსდევს ზარალი როგორც ინდივიდუალურ, ასევე სახელმწიფო დონეზე არა მხოლოდ ფინანსურად, ინფრასტრუქტურული და ფსიქოლოგიური თვალსაზრისითაც.

კიბერიარაღი ბოროტი ჰაკერების ხელში

კიბერშეტევებისთვის თავდამსხმელებს უამრავი პროგრამა, მეთოდი და საშუალება გააჩნიათ - ეს არის თითქმის დაუსრულებელი ჩამონათვალი. თუმცა ჩვენ გამოვყოფთ რამდენიმე მათგანს, აქტუალურ პროგრამას და ვირუსს, რომელსაც ყოველდღიურ რეჟიმში იყენებენ შავქუდიანი თუ აგრესორი სახელმწიფოების მიერ დაქირავებული ჰაკერები, რომლებიც ცდილობენ, დააზიანონ სხვა ქვეყნების კრიტიკული ინფრასტრუქტურა.

აქ უნდა განვიცილოთ და ავსხნათ, თუ რას წარმოადგენს კომპიუტერული ვირუსი. კომპიუტერული ვირუსი არის მავნე პროგრამა, რომელიც ჩვეულებრივი, ,,ცხოვრებისეული'' ვირუსებივით ინფიცირდება და მრავლდება, საერთო ჯამში კი აინფიცირებს პროგრამებსა და ფაილებს. ხშირად ვირუსი მაშინ აღწევს სისტემაში, როდესაც ის დაუცველია. მაგალითად, თუ არ გვიყენია კომპიუტერულ მოწყობილობაზე ანტივირუსი ან არ ვიცავთ კომპიუტერს, არ მოვიხმართ იმ ინდივიდუალური სტანდარტების დაცვით, რამაც შეიძლება მინიმუმამდე შეამციროს რისკები.



ახლა კი შევეხოთ ისეთ კიბერშეტევას, კიბერფსიქოლოგიურ თავდასხმას, როგორიცაა ***სოციალურ ინჟინერია.***[178] აღნიშნული ტერმინი სპეციალურ ლიტერატურაში ხშირად კი გვხვდება, მაგრამ ბევრმა არ იცის, ზუსტად რა იგულისხმება და რას ნიშნავს. იგი კიბერუსაფრთხოების სფეროში წარმოადგენს ერთგვარ ფსიქოლოგიურ მანიპულაციას, როდესაც თავდამსხმელი კიბერსივრცის საშუალებით ონლაინ რეჟიმში ადამიანზე ახდენს ზემოქმედებას და აკეთებინებს მისთვის სასურველ საქმეს. ეს შეიძლება გამოიყენებოდეს კონფიდენციალური ინფორმაციის გამოძალვისთვის, რაც ერთგვარ ნდობაზეა დამოკიდებული და გულისხმობს ინფორმაციის მოპოვებას თაღლითობისათვის ან არალიცენზირებული წვდომისთვის სისტემებზე. სოციალურ ინჟინერიას აქტიურად იყენებენ ტერორისტები.

ფსიქოლოგიურ კიბერშეტევას წარმოადგენს ასევე ***ფიშინგი (Phishing),***[179] რომელიც უფრო ფინანსურ სარგებელზეა გათვლილი და აქტიურად გამოიყენება მსოფლიო მასშტაბით, იგი უფრო ადამიანების ემოციებზე თავდასხმას გულისხმობს, ვიდრე ინფრასტრუქტურაზე. თავდამსხმელი ცდილობს, მოტყუებით, თაღლითური სქემებით, ყალბი ვებ-გვერდებით და კონტენტის შექმნით მოიპოვოს მსხვერპლის პირადი მონაცემები, ბარათების მონაცემები, მანიპულაცია მოახდინოს ადამიანის ემოციებზე, შეიყვანოს შეცდომაში და გამოსძალოს ფინანსები.

[178] *Rosencrance L. Madelyn Bacon M., "social engineering", p. 1, 2021. https://www.techtarget.com/searchsecurity/definition/social-engineering*

[179] *Lord N., "What is a Phishing Attack? Defining and Identifying Different Types of Phishing Attacks", Datainsider, p. 1, 2022. https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks*

ასევე, ფინანსურ სარგებელზე ორიენტირებული კიბერშეტევაა ***გამოსასყიდი (Ransomware) მალვარე***[180] [181] ტიპის თავდასხმა. ამ პროგრამას შეუძლია თქვენი ფაილების, დოკუმენტებისა და ზოგადად ინფორმაციის დაშიფრვა, ანუ გამოუსადეგარ ფაილებად გადაქცევა. რა თქმა უნდა, ამ შემთხვევაში თავდამსხმელს აქვს მისი გამოსწორების შესაძლებლობაც. როდესაც ასეთი კიბერშეტევა ხდება, თავდამსხმელი ცდილობს ფულის გამოძალვას, თუ ფულს გადავუხდით, ის გვპირდება, რომ ფაილების დეშიფრაციის ე.წ. გასაღებს მოგვცემს. თუმცა ეს ყველა ვარიანტში მის კეთილ ნებაზეა დამოკიდებული. თუ თავდამსხმელი პროფესიონალია და კარგად მალავს თავის თავს, რთულია რაიმე ბერკეტის ხელში ჩაგდება. მსგავსი ხასიათის კიბერშეტევები საფრთხეს უქმნის სხვადასხვა კრიტიკული სფეროების ფუნქციონირებას ქვეყნებში - მედიცინა, ეკოლოგია, ეკონომიკა და ა.შ. რაც დიდ ზარალთან არის დაკავშირებული. გამოსასყიდი კიბერშეტევის თავდაცვითი მექანიზმების გასაძლიერებლად არაერთი საერთაშორისო ორგანიზაცია მუშაობს, თუმცა ამ სფეროში ჯერ-ჯერობით რაიმე მნიშვნელოვანი გარღვევა არ მომხდარა.

ბოროტი ჰაკერების ხელში მნიშვნელოვან კიბერიარაღს წარმოადგენს ***DDoS*** შეტევები, რაც იწვევს ტრაფიკის გაზრდას იმ დონეზე, რომ ვებ-გვერდი, სისტემა ან კომპიუტერი ითიშება, გამოჰყავს მწყობრიდან და გამოუსადეგარი ხდება. აღნიშნული თავდასხმის მაგალითები მსოფლიო მასშტაბით ბევრია, მათ შორის საქართველოზეც განხორციელდა 2008 წელს რუსეთ-საქართველოს ომის დროს და 2019 წელს, როდესაც რუსეთის ფედერაციამ საქართველოს სამთავრობო ვებ-გვერდებსა და ტელეკომპანიებზე განახორციელა მასირებული კიბერშეტევები, რამაც მწყობრიდან გამოიყვანა სისტემები და ვებ-გვერდები.

---

[180] *მალვარე (malware) მავნე პროგრამა, რომელსაც კიბერკრიმინალები ქმნიან მონაცემების მოპარვის, კომპიუტერების და მისი სისტემების დაზიანების ან/და განადგურების მიზნით.*

[181] *Fruhlinger J., "Ransomware explained: How it works and how to remove it", p. 1, 2020. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html*

DDoS[182] შეტევების დროს ხშირად იყენებენ ***Botnets,***[183] აღნიშნული ტერმინი წარმოადგენს ორი სიტყვის შემოკლებულ ერთობლივ ვარიანტს - ***robot-ისა (რობოტი)*** და ***Internet-ის (ინტერნეტი).*** იგი არის ინტერნეტთან დაკავშირებული მოწყობილობები, რომლებსაც აქვთ ერთი მოწყობილობიდან მართვის შესაძლებლობა. ასევე, ჰაკერები ***Botnets*** იყენებენ სპამების[184] გასაგზავნად, იგი საშუალებას იძლევა, ჰაკერმა შეაღწიოს ნებისმიერ მოწყობილობაში და მოიპაროს ინფორმაცია. აღსანიშნავია, რომ ხშირ შემთხვევაში ჰაკერები ისე აინფიცირებენ სხვადასხვა კომპიუტერულ მოწყობილობებს და იყენებენ თავდასხმებისთვის, ეს მფლობელმა არც იცის.

აქ უნდა გამოვყოთ ხშირად გამოყენებადი პროგრამა - აპლიკაცია, რომელშიც ჩაშენებულია მავნე კოდი. ეს გახლავთ ტროიანი ***(Trojan),***[185] მას ***„ტროას ცხენებსაც"*** უწოდებენ. იგი ძალიან მარტივად შეიძლება აღმოჩნდეს ჩვენს კომპიუტერულ მოწყობილობებში - გადმოიწერთ რაიმე პროგრამას და იქ აღმოჩნდება ჩაშენებული კოდი, ან ელფოსტი|თ მოგივათ რაიმე ბმული, თუ შეხვალთ, კომპიუტერი ავტომატურად გადმოიწერს პროგრამას. ტროიანი ხშირ შემთხვევაში გამოიყენება იმ მიზნით, რომ თავდამსხმელმა მოიპოვოს წვდომა მომხმარებლის პირად ინფორმაციაზე (პაროლები, საბანკო ინფორმაცია, პირადი მონაცემები და ა.შ.) ან დააზიანოს, წაშალოს ფაილები, დააინფიციროს კომპიუტერი და ქსელთან დაკავშირებული სხვა მოწყობილობებიც. თავდამსხმელს ტროას აპლიკაცია უნებართვო მიყურადების, ანუ მოსმენის საშუალებასაც აძლევს.

---

[182] *Imperva, "Distributed Denial of Service (DDoS)", p. 1, 2022. https://www.imperva.com/learn/ddos/denial-of-service/*

[183] *Crowdstrike, "What is it a Botnet?", p. 1, 2022. https://www.crowdstrike.com/cybersecurity-101/botnets/*

[184] *სპამი არის ელექტრონული წერილი, რომელიც იგზავნება მიმღების დაუკითხავად. აღნიშნული შეტყობინებები უმეტესწილად სარეკლამო ხასიათისაა. სპამებს ხშირად აგზავნიან ბოროტი ჰაკერები.*

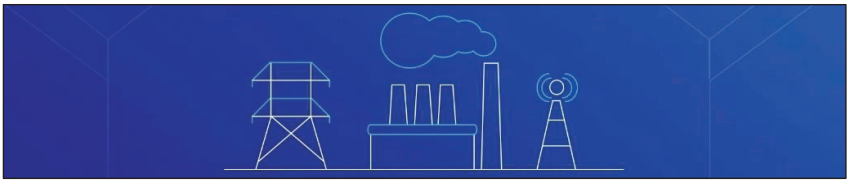
[185] *Johansen G. A., "What is a Trojan? Is it a virus or is it malware?", p. 1. 2020. https://us.norton.com/blog/malware/what-is-a-trojan#*

აღნიშნული ვირუსებისგან, მავნე პროგრამებისგან და კიბერშეტევებისგან თავდასაცავად რუტინული შრომაა საჭირო. ყველა საერთაშორისო თუ ადგილობრივი ორგანიზაცია, წამყვანი თუ განვითარებადი ქვეყნები აღნიშნავენ, რომ აუცილებელია კიბერსტანდარტების დაცვა, კომპიუტერული ტექნოლოგიების სწორად გამოყენება, რათა მოხდეს ზარალის მინიმუმამდე შემცირება. ვინაიდან დასაწყისში ყურადღება ვირუსებზე გავამახვილეთ, ახლა უნდა განვმარტოთ, თუ როგორ შეიძლება თავიდან ავიცილოთ კომპიუტერული მოწყობილობის დაინფიცირება. მაგალითად, აპრობირებულ და აქტუალურ საკითხს წარმოადგენს ***USB-ის*** ე.წ. „ფლეშკის“ გამოყენება, რაც ხშირ შემთხვევებში რისკს წარმოადგენს. ძალიან მარტივად ხდება ***USB-ის*** დაინფიცირება და იგი შემდეგ ხდება სხვა კომპიუტერული მოწყობილობების დაინფიცირების წყაროც. აუცილებლად საჭიროა ყოველ ჯერზე მისი გადამოწმება და გასუფთავება, ანუ „დაფორმატება“. უსაფრთხოების მიზნით ასევე მნიშვნელოვანია, როდესაც კომპიუტერი, მობილური მოწყობილობა გვთხოვს სისტემის განახლებას. არ უნდა გადავდოთ, განვაახლოთ, ანუ „დავააპდეითოთ“. მოძველებული სისტემა ყოველთვის ზრდის დაუცველობის რისკს.

მნიშვნელოვანია, რომ გვქონდეს გააქტიურებული ***აღდგენის*** ანუ ***„ბექაფის“ (Backup)*** ფუნქცია, მისი განახლება უნდა მოხდეს პერიოდულად. ხშირ შემთხვევაში ერთ-ერთ ყველაზე დიდ საფრთხეს სუსტი პაროლები წარმოადგენს, რთული პაროლების დაყენება და მათი უსაფრთხოთ შენახვა რუტინული მოქმედებაა უსაფრთხოების კუთხით. სჯობს, ყველა მნიშვნელოვანი ფაილი დავიცვათ პაროლებით, რათა კიბერშეტევის შემთხვევაში მათზე ხელმისაწვდომობის პროცენტი მინიმუმამდე შემცირდეს. ***მეხსიერების „ღრუბლები“ (cloud),*** რომელიც ***Google Drive-ის*** სახელით არის ცნობილი, ხშირად უსაფრთხო სივრცე ჰგონიათ, თქვენი ელექტრონული

ფოსტის გატეხვის შემთხვევაში მეხსიერების ღრუბელზე წვდომა თავდამსხმელს მარტივად ექნება. შესაბამისად, მნიშვნელოვანი ინფორმაციის შენახვა აღნიშნულ სივრცეში წარმოადგენს ერთგვარ რისკს.

კრიტიკული ინფრასტრუქტურის უსაფრთხოების პრობლემა, თანამედროვე კიბერსაფრთხეების პირობებში



სახელმწიფოები ცდილობენ, განავითარონ თავიანთი პოტენციალი, სხვადასხვა დარგები და სფეროები - ეკონომიკა, მედიცინა, განათლება, კულტურა, სოფლის მეურნეობა და სხვა. ეს სასიცოცხლოდ მნიშვნელოვანია ნებისმიერი სახელმწიფოსთვის. ბუნებრივია, როდესაც ყველა სფერო გამართულად მუშაობს, ეკონომიკური მდგომარეობაც უმჯობესდება. 21-ე საუკუნეში აღნიშნულ და სხვა სფეროებშიც დიდი წილი უკავია ციფრულ მიმართულებას, ანუ ინტერნეტსივრცეს, კომპიუტერულ ინდუსტრიას. როგორც უკვე არაერთხელ აღვნიშნეთ, ახალმა ტექნოლოგიებმა როგორც დადებითი გავლენა იქონია, ასევე წარმოშვა ბევრი საფრთხე, ბევრი არასასურველი მდგომარეობა, პრობლემა, გაურკვევლობა და ფინანსური ზარალი. აღნიშნული პროცესი დღესაც მიმდინარეობს, ანუ ზარალი დღითი დღე იზრდება და ამის გამკლავებას სხვადასხვა კერძო თუ საერთაშორისო ორგანიზაციები ბოლომდე ვერ ახერხებენ.

ჩვენ უკვე აღვნიშნეთ ზევით, რომ სახელმწიფოებისთვის ერთ-ერთ ყველაზე რისკის შემცველი მოვლენა კრიტიკულ ინფრასტრუქტურაზე კიბერთავდასხმებია, რაც ხშირ შემთხვევაში ქვეყნის პარალიზებას იწვევს. ჩვენ უკვე განმარტებული გვაქვს თუ რა არის კიბერშეტევა, კიბერომი და სხვა, ამიტომ რადგან ასეთ სპეციფიკურ თემას ვეხებით, მნიშვნელოვანია ასევე ავხსნათ, თუ რა არის კრიტიკული ინფრასტრუქტურა. და მაინც რა მოიაზრება კრიტიკულ ინფრასტრუქტურაში?

მაგალითად, ამერიკის შეერთებულ შტატებში ***შიდა უსაფრთხოების დეპარტამენტი (DHS)*** გამოყოფს კრიტიკული ინფრასტრუქტურის 16 სექტორს:

1. ***"ქიმიური სექტორი:*** *ძირითადი ქიმიკატები, სპეციალიზებული ქიმიკატები, სასოფლო-სამეურნეო ქიმიკატები, ფარმაცევტული საშუალებები, სამომხმარებლო პროდუქტები;*
2. ***კომერციული ობიექტების სექტორი:*** *გასართობი და შეღიასაშუალებები, თამაში, განთავსება (განლაგება), გარე ღონისძიებები, სახალხო კრება, უძრავი ქონება, საცალო პროდუქცია, სპორტული ლიგები;*
3. ***კომუნიკაციების სექტორი:*** *ენერგეტიკული სექტორი, რომელიც დაკავშირებულია ელექტროსაკომუნიკაციო ტექნოლოგიებთან, საინფორმაციო ტექნოლოგიების სექტორის კონტროლის სისტემები და სერვისები, ფინანსური მომსახურების სექტორის კომუნიკაციები, გადაუდებელი დახმარების სექტორის კომუნიკაციები;*
4. ***კრიტიკული წარმოების სექტორი:*** *პირველადი ლითონის წარმოება, რკინისა და ფოლადის ქარხნები, ფეროშენადნობების წარმოება, ალუმინის წარმოება და დამუშავება, ფერადი ლითონის წარმოება და დამუშავება, მანქანა-დანადგარების წარმოება, ძრავების, ტურბინებისა და ელექტროგადამცემი მოწყობილობების წარმოება, ელექტრომოწყობილობის, ტექნიკისა და კომპონენტების წარმოება, სატრანსპორტო აღჭურვილობის წარმოება, ავტომობილების წარმოება, საავიაციო, კოსმოსური პროდუქტებისა და ნაწილების წარმოება, რკინიგზის მოძრავი შემადგენლობის წარმოება;*
5. ***კაშხლების სექტორი:*** *ენერგია, საკვები და სოფლის მეურნეობა, სატრანსპორტო სისტემები, ძირითადი გზები (შეიძლება გადიოდეს კაშხლებზე), წყალი;*
6. ***თავდაცვის სამრეწველო ბაზის სექტორი:*** *სამხედრო ბაზები;*
7. ***გადაუდებელი დახმარების სექტორი:*** *სამართალდამცავები, სახანძრო და სასწრაფო დახმარება, გადაუდებელი დახმარების მენეჯმენტი, სასწრაფო სამედიცინო მომსახურება, სსიპ სამსახური, სახიფათო მასალები, ტაქტიკური გუნდები (მაგ., SWAT), საავიაციო დანაყოფები (ანუ პოლიცია და მეღვაკის ვერტმფრენები),*

საზოგადოებრივი უსაფრთხოების საპასუხო პუნქტები (მაგალითად, 911-ის სატელეფონო ცენტრები);

8. ***ენერგეტიკის სექტორი:*** *ელექტროობა,* ***ბუნებრივი აირი*** *და სხვა;*
9. ***ფინანსური მომსახურების სექტორი:*** *სადეპოზიტო დაწესებულებები, საინვესტიციო პროდუქტების მომწოდებლები,* ***სასადაზღვევო*** *კომპანიები,* ***საკრედიტო*** *ორგანიზაციები და სხვა.*
10. ***სურსათისა და სოფლის მეურნეობის სექტორი:*** *ფერმები,* ***რესტორნები,*** *საკვების წარმოების, გადამუშავებისა და შენახვის ობიექტები;*
11. ***სამთავრობო ობიექტების სექტორი:*** *განათლება, ეროვნული ძეგლები;*
12. ***ჯანდაცვისა და საზოგადოებრივი ჯანდაცვის სექტორი;***
13. ***საინფორმაციო ტექნოლოგიების სექტორი;***
14. ***ბირთვული რეაქტორების, მასალებისა და ნარჩენების სექტორი:*** *ატომური ელექტროსადგურები, არაენერგეტიკული ბირთვული რეაქტორები, ბირთვული საწვავის ციკლის ობიექტები, გაუქმებული ბირთვული ენერგიის რეაქტორები, ბირთვული და რადიოაქტიური ნარჩენების ტრანსპორტირება, შენახვა და განკარგვა;*
15. ***სატრანსპორტო სისტემების სექტორი:*** *ავიაცია, საგზაო ინფრასტრუქტურა და საავტომობილო გადაზიდვა, საზღვაო ტრანსპორტის სისტემა,* ***მასობრივი ტრანზიტი*** *და სამგზავრო რკინიგზა,* ***მილსადენის*** *სისტემები, სარკინიგზო ტვირთები, ფოსტა და მიწოდება;*
16. ***წყლის სისტემების სექტორი.”***[186]

დაგვეთანხმებით, რომ კრიტიკული ინფრასტრუქტურის სექტორები ძალიან მრავალფეროვანია, მაგრამ ასევე მათზე კიბერთავდასხმებიც მრავალფეროვანი. ჰაკერები ყოველდღიურად ცდილობენ ახალი მეთოდების შემუშავებას, თუ როგორ დააზიანონ და შეიჭრან უნებართვოდ კრიტიკული ინფრასტრუქტურის სისტემებში.

როგორც ცნობილია, სავარაუდოდ, რუსმა ჰაკერებმა *„2015 წლის დეკემბერში კიბერთავდასხმები განახორციელეს* ***Prykarpattyaoblenergo Control Center -ზე (PCC),*** *რამაც 230 000 ადამიანი 6 საათის განმავლობაში ელექტროენერგიის გარეშე დატოვა“.*[187] **ფაქტი**

[186] *TechTarget Contributor, "critical infrastructure", p. 1. 2020. https://www.techtarget.com/whatis/definition/critical-infrastructure*
[187] *Wagner D., "The Growing Threat of Cyber-Attacks on Critical Infrastructure", p. 1. 2016. https://www.irmi.com/articles/expert-commentary/cyber-attack-critical-infrastructure*

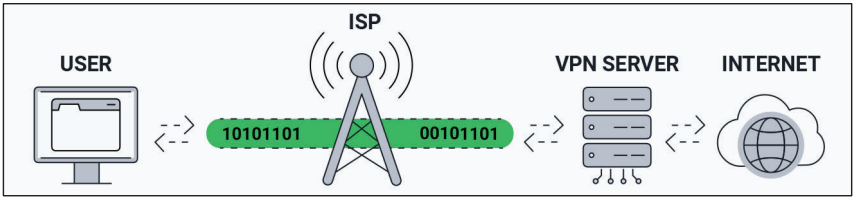
მნიშვნელოვანია იმითაც, რომ ეს იყო პირველი შემთხვევა, როდესაც კიბერშეტევა წარმატებით იქნა გამოყენებული ელექტროქსელების წინააღმდეგ.

რაც შეეხება უშუალოდ კიბერშეტევას, აღმოჩნდა, რომ აღნიშნული *„კიბერშეტევა იყო საზედამხედველო კონტროლისა და მონაცემთა შეგროვების* ***(SCADA)*** *კიბერთავდასხმა“.*[188] ასევე იყო ფიშინგის შეტევა ელექტრონული ფოსტის გამოყენებით. ასეთი კიბერშეტევის დასაწყებად სტანდარტულ საკითხს წარმოადგენს, რა ტენდენციაც დღეს გრძელდება - ფიშინგი ამჟამადაც აქტუალურია და კვლავ გამოიყენება კრიტიკული ინფრასტრუქტურის წინააღმდეგ.

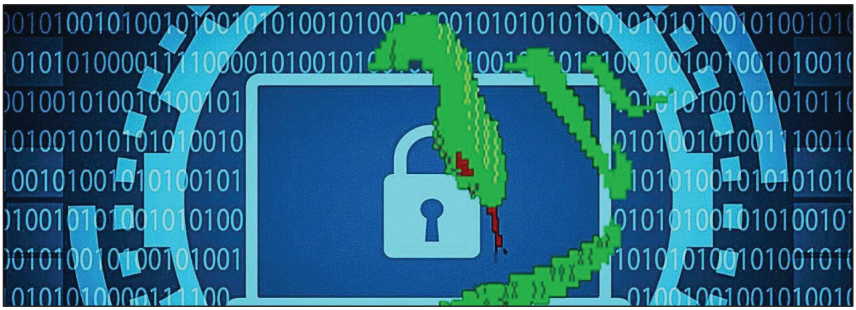
ПРИКАРПАТТЯ ОБЛЕНЕРГО

ამ თავდასხმიდან ერთი წლის შემდეგ, *„ისევ განხორციელდა კიბერშეტევა* ***PrykarpattyaOblenergo-ზე,*** *რამაც უკრაინაში ივანო-ფრანკოვსკის რეგიონის მოსახლეობის ნახევარი, დაახლოებით 700 000 ადამიანი, დეკემბრის შუა რიცხვებში ელექტროენერგიის გარეშე დატოვა“.*[189] აქაც ექვები ისევ და ისევ რუსეთის ფედერაციაზეა, *„სავარაუდოდ, რუსი ჰაკერების ჯგუფმა* ***(Sandworm-მა)*** *გამოიყენა დამაზიანებელი მავნე პროგრამა* ***„BackEnergy 3”.*** *ასევე გამოიყენეს* ***“KillDisk”,*** *ანუ მყარი დისკის მკვლელი პროგრამა,* ***“Spear Phishing”, VPN, DDoS სატელეფონო შეტევები*** *და ა.შ.“*[190]

[188] *Ball T., "Top 5 critical infrastructure cyber attacks", p. 1. 2022. https://techmonitor.ai/technology/cybersecurity/top-5-infrastructure-hacks*
[189] *Industrial Control Systems Security, p.1. 2016. https://www.sans.org/industrial-control-systems-security/*
[190] *Industrial Control Systems Security, p.1. 2016. https://www.sans.org/industrial-control-systems-security/*



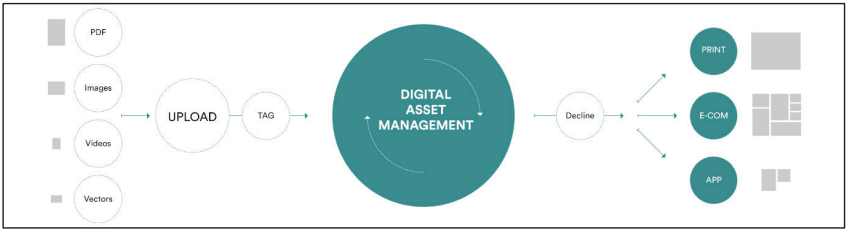
მაგალითები გვიჩვენებს, რომ კიბერთავდასხმები კრიტიკულ ინფრასტრუქტრუაზე უკვე სტანდარტულ საკითხს წარმოადგენს. აღსანიშნავია, რომ კრიტიკულ ინფრასტრუქტრუაზე თავდასხმა შეფასებულია, როგორც კიბერომი, თუმცა მაგალითები, რაც ჩვენ მოგვყავს, არ არის კიბერომის სტატუსით ცნობილი და აღიარებული იმიტომ, რომ თავდამსხმელები იყენებენ ***VPN-ს*** და ასევე სხვადასხვა დამცავ საშუალებებს. ეს ართულებს მათი მდებარეობის დადგენას და იმასაც, რომელი ქვეყნის ხელისუფლება დგას ამა თუ იმ კიბერშეტევის უკან და აქვს თუ არა საერთოდ პოლიტიკური მიზანი.



მაგალითად, 2016 წელს სანფრანცისკოს სარკინიგზო სისტემაზე განხორციელდა კიბერშეტევა. ამ დროს *„ჰაკერებმა გამოიყენეს გამოსასყიდი პროგრამები სახელად **Mamba,** რამაც თავდამსხმელებს საშუალება მისცა არაავტორიზებული წვდომისა და 2000-ზე მეტი სისტემის დაშიფვრისა“.*[191] ***Mamba*** სახელწოდება მომდინარეობს გველის ნაირსახეობიდან. ამავე წელს ირანის ისლამური რესპუბლიკის მიერ კიბერშეტევა განხორციელდა ნიუ-იორკის კაშხალზე - *„ირანის ისლამური სახელმწიფოს დაფინანსებული ჰაკერები **(ITSeC Tram** და **Mersad Company)** შეიჭრნენ ნიუ-*

[191] *Swati Khandelwal S., "San Francisco Metro System Hacked with Ransomware; Resulting in Free Rides", p. 1. 2016. https://thehackernews.com/2016/11/transit-system-hacked.html*

*იორკის **Bowman Dam-ის** ზედამხედველობის კონტროლისა და მონაცემთა შეგროვების სისტემებში **(SCADA)“.**[192]*



ჰაკერებმა ისარგებლეს დაუცველი მოდემის კავშირით და უსაფრთხოების კონტროლის არარსებობით ***Dam-ის*** სისტემებისთვის. თავდასხმამ არც ისე დიდი ზარალი გამოიწვია, მაგრამ შთაბეჭდილება დატოვა, რომ ისინი უბრალოდ სისტემებს ცდიდნენ, რამდენად მარტივად მოახერხებდნენ შეღწევას.

ჰაკერები 2017 წელს შეიჭრნენ და კონტროლი აიღეს ამერიკის შეერთებული შტატების წყლის ორგანოს ფიჭურ ქსელზე. აღსანიშნავია, რომ მათი მიზნები სხვებისგან განსხვავებული იყო, *„წყლის გათიშვის ან მოწამვლის ნაცვლად გამოიყენეს ფიჭური მარშრუტიზატორები გადასახადების 15 000 პროცენტით გაზრდის მიზნით, თვეში 300 დოლარიდან 50 000 დოლარამდე, ორი თვის განმავლობაში. შეღწევა მარტივად განხორციელდა იმის ხარჯზე, რომ ფუნქციონირებდა მოძველებული **firmware** და ქარხნულად დაინსტალირებული პაროლი ობიექტის **Sixnet BT** მარშრუტიზატორებისათვის“.*[193]

დამზიანებელი კიბერშეტევა მოხდა 2020 წელს ტაივანის სახელმწიფო ენერგეტიკულ კომპანია ***CPC Corp - ზე,*** რომელიც პასუხისმგებელია ნავთობის მიწოდებასა და

[192] *FBI, "Iranian DDoS Attacks", p. 1. 2016. https://www.fbi.gov/wanted/cyber/iranian-ddos-attacks*
[193] *Walton B., "Water Utility Cyberattack Rings Up Hefty Data Charges", p. 1. 2017. https://www.circleofblue.org/2017/water-management/water-utility-cyberattack-rings-hefty-data-charges/*

თხევადი ბუნებრივი აირის იმპორტზე. *"ჰაკერებმა გამოიყენეს გამოსასყიდი პროგრამა. მიუხედავად იმისა, რომ წარმოება დაუზიანებელი დარჩა, ჰაკერებმა კომპანიის გადახდის სისტემაში ქაოსი შეიტანეს, რაც გულისხმობს იმას, რომ მომხმარებლები ვეღარ იყენებდნენ VIP ბარათებს ანგარიშსწორებისათვის, არ მუშაობდა გადახდის აპლიკაციები. ამ საქმეში ეჭვმიტანილია ჰაკერების ჯგუფი სახელწოდებით* ***Winnti***". [194]

2020 წელს მასირებული კიბერშეტევების სამიზნე გახდა ისრაელის წყლის სისტემები. *"კიბერთავდასხმები ხორციელდებოდა ისრალის სატუმბი სადგურების, კანალიზაციის, ჩამდინარე წლების ქარხნებისა, სასოფლო-სამეურნეო ტუმბოების მართვისა და კონტროლის სისტემებზე. საერთო ჯამში კიბერშეტევებმა ვერავითარი ზიანი ვერ მიაყენა, მაგრამ თავდასხმები მიზნად ისახავდა წყალში ქლორისა და სხვა ქიმიკატების მომწამლავ დონემდე მიყვანას, ასევე წყლის მიწოდების შეფერხებას სიცხისა და პანდემიის დროს. ჰაკერთა ჯგუფმა მიაკვლია სისტემების სუსტ წერტილს, ეს გახლდათ ძველი პაროლები, რაც სისტემაში შესაღწევად გამოიყენეს".*[195]

DARKSIDE HACKER GROUP

ბოლო წლებში ერთ-ერთი ყველაზე დამანგრეველი კიბერშეტევა 2021 წელს კოლონიურ ნავთობის მილსადენზე განხორციელდა, რომელიც უმსხვილესი მილსადენია ამერიკის შეერთებულ შტატებში და ამარაგებს აღმოსავლეთ სანაპიროს გაზით, დიზელისა და ავია საწვავის 45 პროცენტზე მეტს. კიბერშეტევის შედეგად იძულებულნი გახდნენ, მთლიანად შეეწყვითად მომარაგება, დაეკეტათ ქსელები და შეეჩერებინათ ოპერაციები. მიუხედავად იმისა, რომ მათ კიბერთავდაცვითი ტექნოლოგიების საშუალებით მოახერხეს სისტემების ფუნქციონირების დაბრუნება, *"18 მაისის მონაცემებით 11 000-მდე ბენზინგასამართი სადგური გაზის გარეშე იყო დარჩენილი. ჰაკერთა ჯგუფმა* ***„DarkSide"-მა*** *ასევე კომპანიის სერვერებიდან 100 გიგაბაიტზე მეტი მონაცემი მოიპოვა, მას შემდეგ რაც კომპანიამ 5 მილიონი დოლარი გადაიხადა კრიპტოვალუტით, ჰაკერთა დაჯგუფებამ კონტროლის მექანიზმები დაბრუნა. აღსანიშნავია, რომ ამ კიბერთავდასხმის შემდეგ ამერიკის შეერთებულ შტატებში გაზის*

[194] *National Cybersecurity Centre NCSC Federal Intelligence Service FIS, "Information Assurance", Reporting and Analysis Centre for Information Assurance MELANI, p. 18, 2020. https://www.newsd.admin.ch/newsd/message/attachments/63536.pdf*

[195] *Paganini P., "Piping botnet: Researchers warns of possible cyberattacks against urban water services", p. 1. 2020. https://securityaffairs.co/wordpress/75389/hacking/piping-botnet-water-services.html*

საშუალო ღირებულებამ ერთ გალონზე ისტორიულ მაქსიმუმს მიაღწია, რაც 6 წელზე მეტ ხანს გაგრძელდა".[196]

მაგალითები გვიჩვენებს, რომ ხშირად კრიტიკულ ინფრასტრუქტურაზე თავდასხმა იწვევს ისეთ ზიანს, რომლის გამოსწორებასაც წლები სჭირდება. რაც უფრო სუსტია სახელმწიფო, მით მეტი დროა საჭირო პრობლემის გამოსასწორებლად. ამიტომაც, ყველა სახელმწიფო დიდ მნიშვნელობას ანიჭებს კრიტიკული ინფრასტრუქტურის დაცვას.

უნდა გავიაზროთ, რომ ბუნებრივი კატაკლიზმები ერთადერთი საფრთხე აღარ არის ინფრასტრუქტურისათვის. იქიდან გამომდინარე, რომ ტექნოლოგიები სწრაფად ვითარდება და ყველა სფეროს მოიცავს, სხვადასხვა სექტორის, მათ შორის კრიტიკული სექტორის წარმომადგენლები დღითი-დღე აქტიურად ცდილობენ ახალი ტექნოლოგიების ინტეგრირებას. მათ წინაშე არსებული გამოწვევები და საფრთხეები შესაბამისად ვითარდება და იზრდება. ქსელების უსაფრთხოება მნიშვნელოვან საკითხს წარმოადგენს, რათა კავშირი დარჩეს უწვეტი, მუდმივი კონტროლი და შემოწმება საჭიროა, ეს ინფრასტრუქტურის დაცვასა და რისკების შემცირებას ხელს უწყობს, თუმცა ყოველთვის არ არის საკმარისი. კრიტიკული ინფრასტრუქტურის სამართავ მოწყობილობებს არ უნდა ჰქონდეს კავშირი ინტერნეტთან. იმ შემთხვევაში, თუ აუცილებელია ინტერნეტთან წვდომა, ეს უნდა განხორციელდეს უსაფრთხოების სათანადო კონტროლით.

კიბერსისტემების თავდაცვითი სტანდარტები

ყველა სახელმწიფო თუ საერთაშორისო ორგანიზაცია ცდილობს კიბერტექნოლოგიური მოწყობილობებისა და პერსონალური მონაცემების დაცვას. უპირველესად მნიშვნელოვანია, ავხსნათ, რა ტექნოლოგიებთან გვაქვს საქმე. ამ შემთხვევაში არ ვგულისხმობთ კინეტიკურ მოწყობილობებს, რომელზე მუშაობაც

[196] *Support the Guardian Available for everyone, funded by readers, "How the Colonial Pipeline hack is part of a growing ransomware trend in the US", p. 1. 2021. https://www.theguardian.com/technology/2021/may/13/colonial-pipeline-ransomware-attack-cyber-crime*

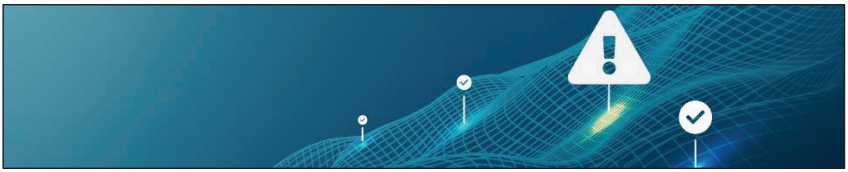
მსოფლიო მასშტაბით აქტიურად მიმდინარეობს და იხარჯება კოლოსალური თანხები. მნიშვნელოვანია, წარმოვაჩინოთ ის პრობლემები, რა ზიანიც გვადგება თითოეულ ჩვენთაგანს ტექნოლოგიების არასტანდარტულად, არაეთიკურად მოხმარების შემთხვევაში. წარმოიდგინეთ, ბოროტმა ჰაკერმა თქვენს კომპიუტერულ მოწყობილობაში შემოაღწია, მას ექნება თქვენ პირად მონაცემებზე წვდომა, ასევე შეეძლება თქვენი მოსმენა, ვიდეოკამერის საშუალებით კადრების გადაღება, რაც თქვენს კომპიუტერულ მოწყობილობაშია ჩაშენებული, მიკროფონის გამოყენებით თქვენი ხმის ჩაწერა. აღნიშნული ფარულად და უკანონოდ მოპოვებული ინფორმაცია, რა თქმა უნდა, თქვენს წინააღმდეგ იქნება გამოყენებული, ამ შემთხვევაში თქვენ გახდებით შანტაჟის მსხვერპლი. ახლა წარმოვიდგინოთ თქვენი სამუშაო სივრცე, სამსახური, ამ შემთხვევაში რისკის ქვეშ დგებით არა მარტო თქვენ, არამედ მთელი კომპანია, ორგანიზაცია ან სახელმწიფო - გააჩნია, რომელ სფეროში მოღვაწეობთ. თუ თქვენი კომპიუტერი მიერთებულია ქსელს, ჰაკერს უფრო მარტივად ექნება შესაძლებლობა, დააინფიციროს და უნებართვო წვდომა მოიპოვოს სხვა თანამშრომლების კომპიუტერებზეც, რაც საერთო ჯამში დიდ ზარალს გამოიწვევს.

რა ტექნოლოგიებთან და სისტემებთან გვაქვს ყოველდრიურად? პირველი გახლავთ პერსონალური კომპიუტერი. იგი შედგება სისტემური ბლოკის ***(Case),*** მონიტორის, კლავიატურისა და ე.წ. ,,მაუსისაგან''. პერსონალურ კომპიუტერში მოვიაზრებთ ლეპტობსაც. კომპიუტერები და ლეპტობები მუშაობს სხვადასხვა ოპერაციულ სისტემებზე, როგორებიცაა: ***Linux, Windows, MacOS*** და სხვა. აქედან ყველაზე პოპულარულ და გავრცელებულ სისტემას ***Windows-ი*** წარმოაგდენს. მიუხედავად იმისა, რომ ბოლო ***Windows-ის*** ვერსია საკმაოდ დაცულია და ტექნოლოგიებზე მომუშავე კომპანიები ცდილობენ, ახალ კიბერსტანდარტებს მოარგონ თავიანთი პროგრამები, ვიმეორებთ - თუ არ დავიცავთ სტანდარტებსა და რეკომენდაციებს, მაინც აღმოვჩნდებით საფრთხის წინაშე.

მნიშვნელოვანია, პერსონალურ კომპიუტერზე ან ლეპტოპზე გვეყენოს ლიცენზირებული სისტემა, არ აქვს მნიშვნელობა, რომელი იქნება. არავითარ

შემთხვევაში არ უნდა დავაყენოთ უფასო, ანუ გატეხილი ვერსია, რომელსაც ბევრი ხარვეზი, შეცდომა, ე.წ. „ბაგი“ აქვს. მუშაობის დროს ჩვენ ვიყენებთ ბევრ აპლიკაციასა და პროგრამას, ამისთვის საჭიროა აღნიშნული აპლიკაციები ან პროგრამები გადმოვტვირთოთ სანდო ვებ-გვერდებიდნ. უკვე აღვნიშნეთ, ხშირად ისეთი ვებ-გვერდები, რომლებიც სანდოდ მიგვაჩნია, იქიდან გადმოტვირთულ ფაილს შეიძლება გამოჰყვეს ვირუსი და თქვენი კომპიუტერი მარტივად დააინფიციროს. როდესაც კიბერუსაფრთხოებასა და თავდაცვით მექანიზმებზე ვსაუბრობთ, აუცილებელია, აღვნიშნოთ, რომ კიბერსფეროში არსებობს ასეთი ტერმინი - ***კიბერჰიგიენა.***[197] [198] იგი არის ის ზოგადი წესები და რუტინული მოქმედებები, რაც ყოველთვის უნდა დაიცვან ადამიანებმა. ***კიბერჰიგიენა*** ნიშნავს ,,პრაქტიკების'' ერთობლიობის დაცვას. თუ ჩვენ პროგრამებსა და აპლიკაციებს არ ვანახლებთ და ისინი მოძველებულია, ეს პირდაპირპროპორციულად აისახება ჩვენს უსაფრთხოებაზე, იზრდება დაუცველობის რისკი.

კიბერჰიგიენის უგულებელყოფა - რისკები



რა რისკებს შეიცავს კიბერჰიგიენის უგულებელყოფა? აღნიშნული საკითხი ფართო სპექტრს მოიცავს, მაგალითად: მონაცემთა დაკარგა ***(Loss of Data),***[199] უსაფრთხოების დარღვევა ***(Security Breach),***[200] ვადაგასული პროგრამული უზრუნველყოფა ***(Out of Date Software),***[201] ძველი უსაფრთხოების პროგრამული

[197] *კბერჰიგიენის დეფინიცია - კიბერჰიგიენა არის მითითება იმ ნაბიჯებზე, როშლებსაც კომპიუტერებისა და სხვა მოწყობილობების მომხმარებლები იყენებენ სისტემების უსაფრთხოდ შესანარჩუნებლად, ასევე ონლაინ უსაფრთხოების გასაუმჯობესებლად. აღნიშნული პრაქტიკა ხშირად რუტინის ნაწილია.*

[198] *Brook Ch., "What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More", p. 1, 2022. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more*

[199] *შყარი დისკები და კიბერშეხსიერების ღრუბლები (cloud), როშელსაც არ გააჩნია სარეზერვო შეხსიერება, წარმოადგენს კიბერთავდასხმის მაღალ რისკს, რამეც შეიძლება გამოიწვიოს თქვენი მნიშვნელოვანი ინფორმაციის დაკარგვა.*

[200] *უსაფრთხოების დარღვევა და უნებართვო წვდომა ჩვენს პირად კომპიუტერულ მოწყობილობებზე ხდება, მავნე პროგრამების, ვირუსების, თაღლითური ფსიქოლოგიური მანიპულაციების, ფიშინგ თავდასხმების შეშვეობით.*

[201] *პროგრამებისა და აპლიკაციების მოძველებული ვერსიები ქმნის დაუცველობის რისკებს.*

უზრუნველყოფა ***(Older Security Software),***[202] არასწორად განთავსებული მონაცემები ***(Misplaced Data).***[203]

კიბერჰიგიენის დაცვა - გზამკვლევი

რა თქმა უნდა, ტექნოლოგიური სისტემების დაცვა რთულ საკითხს წარმოადგენს და ფართო სპექტრს მოიცავს, მაგრამ ექსპერტების მტკიცებით, კიბერჰიგიენის სტანდარტების დაცვამ შეიძლება სურათი საგრძნობლად გააუმჯობესოს. როდესაც ვსაუბრობთ აპლიკაციების ან პროგრამების განახლებაზე, რთული პაროლების შემუშავებასა და ფაილების, მნიშვნელოვანი ინფორმაციის უსაფრთხოდ შენახვაზე, საკითხი უფრო დეტალურ განხილვას საჭიროებს. ჩვენ შევეცდებით, თითოეული მათგანი სიღრმისეულად განვიხილოთ, რაც ხელს შეუწყობს თქვენი კიბერუსაფრთხოების გარემოს მაღალ დონეზე აყვანას და რისკების შემცირებას.

გამოვყოფთ ხუთ ძირითად პუნქტს. საკითხი, შეიძლება ითქვას, არ არის ჩარჩოში მოქცეული:

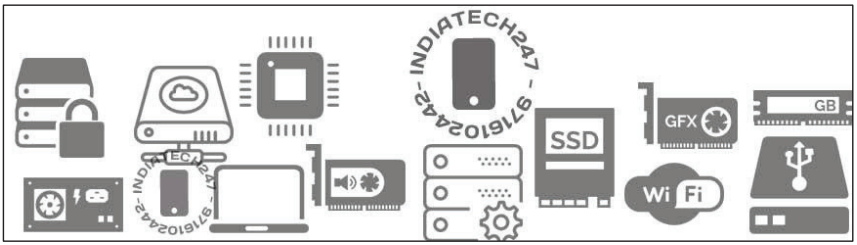
- ***აპარატურის განახლება (Hardware Updates);***
- ***პაროლების ცვლილება (Password Changes);***
- ***მონაცემთა სარეზერვო ასლის შექმნა (Back Up Data);***
- ***პროგრამული უზრუნველყოფის და ოპერატიული სისტემების განახლება (Software Updates);***

[202] *ანტივირუსები და უსაფრთხოების სხვა პროგრამები უნდა განახლდეს დროულად.*
[203] *ფაილები და ინფორმაციები, რომლებიც თქვენთვის მნიშვნელოვანია, შეიძლება არც დაზიანებული იყოს და არც წაშლილი, მაგრამ არადაგეგმარებულად ბევრი მონაცემების შენახვამ და ფაილების ქაოტურად განლაგებამ შეიძლება გამოიწვიოს კიბესაფრთხეების რისკები.*

- ***მყარი დისკის დაშიფრვა (BitLocker Encryption).***

განვიხილოთ თითოეული მათგანი დეტალურად:

აპარატურის განახლება



აუცილებელია, დროის გასვლასთან ერთად, მოხდეს აპარატურის ჩანაცვლება, განახლება ახალი ტექნიკით, რაც თავისი შესაძლებლობებითა და მონაცემებით იქნება სრულ თანხვედრაში სხვადასხვა განახლებულ აპლიკაციებთან თუ პროგრამებთან.

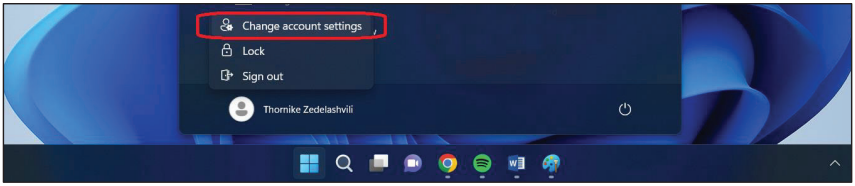
პაროლების ცვლილება

აუცილებელია პაროლების ხშირი ცვლა. კიბერუსაფრთხოების ექსპერტები სხვადასხვა პერიოდსა და ინტერვალს განსაზღვრავენ პაროლების უსაფრთხოებისთვის. საერთო ჯამში დაახლოებითი პერიოდი 1 თვიდან 3 თვემდეა. აქვე აღსანიშნავია, რომ სოციალური ქსელები და ელექტრონული ფოსტები ავტომატურად რეკომენდაციას გვაძლევენ პაროლის შეცვლის თაობაზე. ასევე რეკომენდებულია, ვებ-გვერდებზე, ელექტრონულ ფოსტებზე, სოციალურ ქსელებსა თუ უშუალოდ კომპიუტერულ ტექნიკაზე გქონდეთ სხვადასხვა პაროლები დაყენებული. მარტივად წარმოვიდგინოთ - ჩვენ მოვიხმართ რომელიმე ვებ-გვერდს ან აპლიკაციას, რომელიც თავდასხმის სამიზნე გახდა, ამ შემთხვევაში ჰაკერს თქვენს პაროლზე წვდომა აქვს, მას მარტივად ეძლევა საშუალება თქვენს ინფორმაციაზე წვდომისა. თუ ყველგან გვიყენია ერთი და იგივე პაროლი, რაც ხშირი შემთხვეაა,

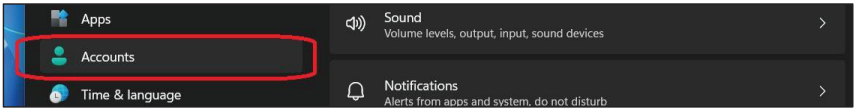
თავდამსხმელს საქმე უადვილდება. რაც შეეხება პაროლის სირთულესა და სიმარტივეს, უკვე იმდენად დახვეწეს სხვადასხვა ორგანიზაციებმა, რომლებიც საზოგადოებას ემსახურებიან აპლიკაციებითა და ვებ-გვერდებით (სადაც აუცილებელია რეგისტრაციის გავლა), რომ თვითონ აქვთ მოთხოვნა, პაროლი შედგებოდეს როგორც დიდი და პატარა ასოებისგან, ასევე იეროგლიფებისა და ციფრებისგან, მოთხოვნა მოქმედებს ერთობლიობის რაოდენობასთან დაკავშირებითაც. შესაბამისად, ეს ჩვენთვის გამარტივებულ საკითხს წარმოადგენს, მაგრამ მაინც გასათვალისწინებელია. თუმცა უნდა ვიცოდეთ, ეს არ გახლავთ საბოლოო გამოსავალი, ხშირად რთული კომბინაციის პაროლიც კი ბოროტი ჰაკერებისთვის მარტივად გასაშიფრი ხდება. ამიტომ უნდა გავითვალისწინოთ რამდენიმე რჩევა: მაგალითად, თუ გვაქვს მოთხოვნა, რომ პაროლი უნდა იყოს მინიმუმ 6 სიმბოლოსგან შემდგარი, უმჯობესია დავაყენოთ 12 სიმბოლოიანი, ან უფრო მეტი სიმბოლოსგან შემდგარი. თუ გვაქვს მოთხოვნა, რომ აუცილებლად უნდა იყოს ერთი ასო დიდი, უმჯობესია, ორი ან სამი დიდი ასო გამოვიყენოთ, ციფრებისა და იეროგლიფების შემთხვევაშიც ასეთი სტრატეგია სჯობს, რაც თავდამსხმელს ფაქტობრივად არ მისცემს სისტემაში წვდომის საშუალებას.

აღნიშნული საკითხი გავიაროთ დეტალურად: გავხსნათ საწყისი ***(Start menu)*** მენიუ, შევიდეთ შეცვალეთ ანგარიშის პარამეტრებში ***(Change account Settings),*** გადავიდეთ ანგარიშში ***(Accounts),*** შემდეგ შევიდეთ ოფციებში ***(Sing-in Options),*** საიდანაც გავხსნით პაროლების ფანჯარას ***(Password),*** ჩავწერთ ჩვენს მიერ სასურველ პაროლს, პირველ რიგში ზედა ფანჯარაში ძველ პაროლს, შემდეგ ქვედა ორ ფანჯარაში ჩვენთვის ახალ სასურველ პაროლს და დავაჭერთ ***(Click)*** შეცვლას ***(Change).*** ეს არის კომპიუტერზე პაროლის შეცვლის მარტივი ხერხი, რომელიც პერიოდულად უნდა განვახორციელოთ, რათა ვიყოთ უფრო უსაფრთხოდ. ასეთი სისტემა ყველა ვებ-გვერდსა და აპლიკაციას გააჩნია, ჩვენ მსგავსი პროცედურა ყველა მათგანზე უნდა შევსარულოთ.

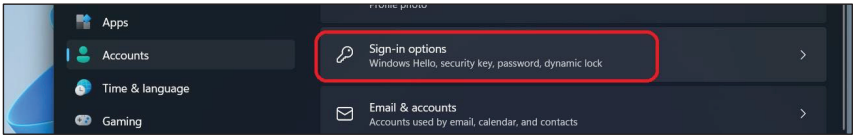
სურათი 5: სტარტ მენიუს გახსნა.



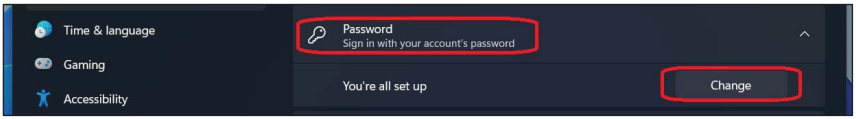
სურათი 6: შესაცვლელი ანგარიშის პარამენტრებში შესვლა.



სურათი 7: ანგარიშებში შესვლა.



სურათი 8: ოფციებში შესვლა.

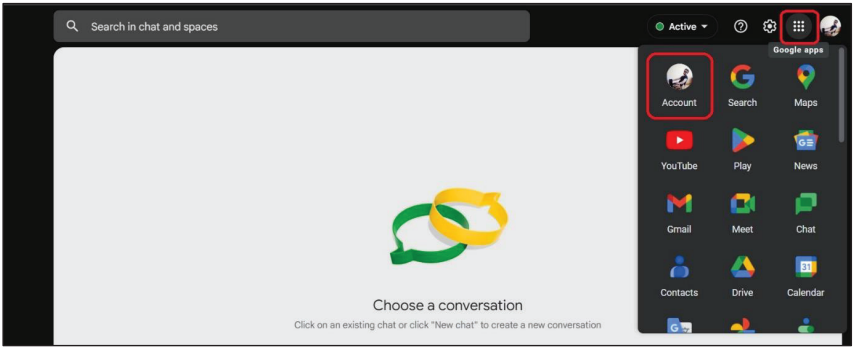


სურათი 9: ფანჯრის გახსნა, საიდანაც შესაძლებელია პაროლების ცვლილება.

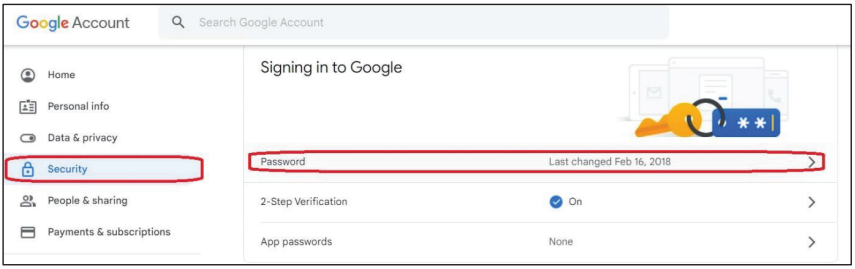
მაგალითად: პაროლის ცვლილება ელექტრონულ ფოსტა ***“ჯიმეილსა” (Gmail.com)*** და ***“ფეისბუქზე” (Facebook.com),*** ესენი წარმოადგენენ პოპულარულ და ყველაზე ხშირად მოხმარებად ვებ-გვერდებს. განვიხილოთ, თუ როგორ ხდება პაროლების შეცვლა.

შევდივართ ჩვენს ელექტრონულ ფოსტაზე, მარჯვენა ზედა კუთხეში ვხსნით ***„გუგლი აპლიკაციების“ (Google Apps)*** ფანჯარას, გადავდივართ ანგარიშში ***(Account),*** სადაც ვებ-გვერდი გაგვიხსნის ჩვენს ანგარიშს, მარცხენა მხარეს მენიუს ბარში ავირჩევთ ***უსაფრთხოების*** ღილაკს ***(Security),*** შემდეგ გაიხსნება ***“გუგლში შესვლა“ (Signing in to Google),*** დავაჭერთ ***პაროლს (Password),*** აღნიშნული მოქმედებების შემდეგ ***„გუგლი“*** მოგვთხოვს ძველი პაროლის შეყვანას, შემდეგ კი მოგვცემს

საშუალებას, ახალი პაროლით ჩავანაცვლოთ ძველი. დავაჭერთ ღილაკ ***დამახსოვრებას (Save)*** და პაროლი შეიცვლება.

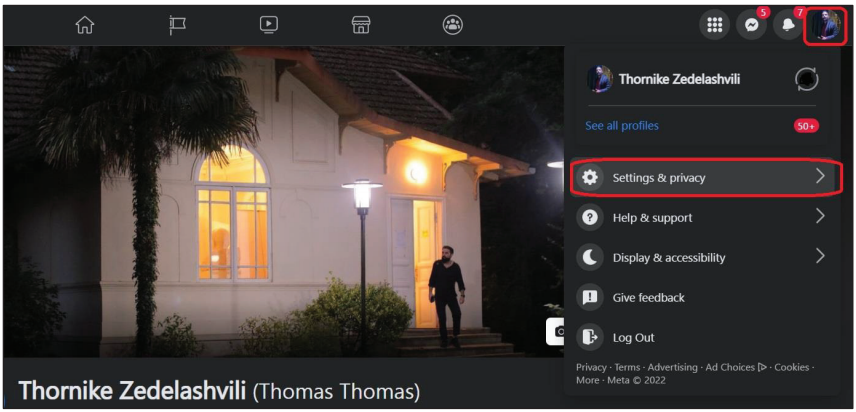


სურათი 10: „გუგლი აპლიკაციების“ ფანჯრის გახსნა და ჩვენს ანგარიშში გადასვლა.

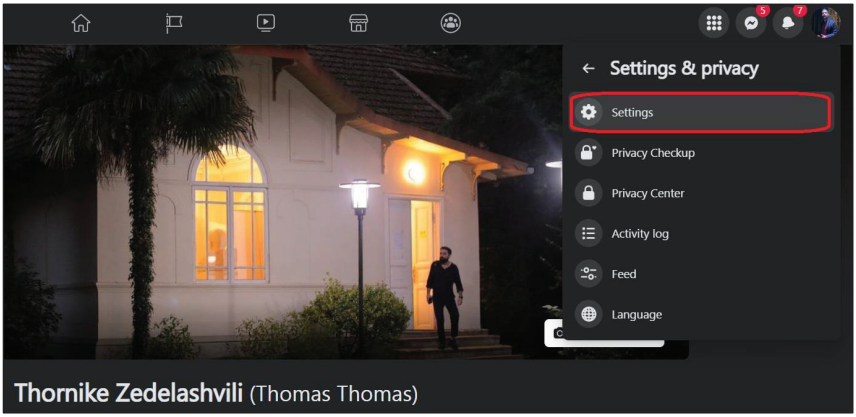


სურათი 11: უსაფრთხოების ღილაკის არჩევა და პაროლის შეცვლა.

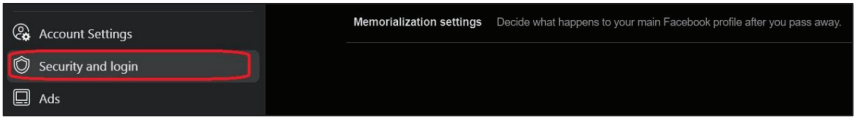
ფეისბუქის შემთხვევაში პაროლის ცვლილება ხდება შემდეგნაირად: შევდივართ ჩვენს პროფილზე, ზედა მარჯვენა კუთხეში ვხსნით ჩვენს ანგარიშს ***(Account),*** გახსნილ ფანჯარაში ავირჩევთ - ***პარამეტრები და კონფიდენციალურობა (Settings & Privacy),*** შემდეგ ***პარამეტრები (Settings),*** აქედან გადავალთ პარამეტრების ბლოკში, სადაც მრცხენა მხარეს გამოტანილ მენიუში ავირჩევთ ***უსაფრთხოებასა და შესვლას (Security & login),*** სადაც გაიხსნება გვერდი, შესვლის ***(Login)*** ქვემენიუში ავირჩევთ ***პაროლის შეცვლას (Change password),*** საიდანაც უკვე სტანდარტული ფორმით შევცვლით პაროლს.



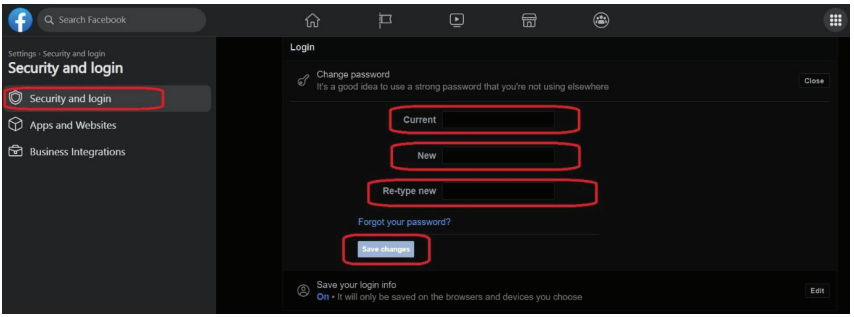
სურათი 12: ანგარიშის გახსნა და „პარამეტრები & კომფიდენციალურობა“-ში გადასვლა.



სურათი 13: პარამეტრებში შესვლა.



სურათი 14: მენიუში „უსაფრთხოება და შესვლა“-ში გადასვლა.



სურათი 15: ქვემენიუში ღილაკი პაროლის შეცვლის არჩევა, პაროლის ცვლილება და დამახსოვრება.

გაითვალისწინეთ, არსებობს ორბიჯიანი და სამბიჯიანი პაროლების დაყენების საშუალებაც, რაც უფრო მეტად დაცულს ხდის თქვენს პირად კიბერსივრცეს. ეს კი გულისხმობს, როგორც პაროლის შეყვანის შემდეგ მობილურ ტელეფონზე კოდის მოსვლას და ასევე შტრიხკოდს. ეს ასევე რეკომენებულია ჩვენს მიერ.

მონაცემთა სარეზერვო ასლის შექმნა

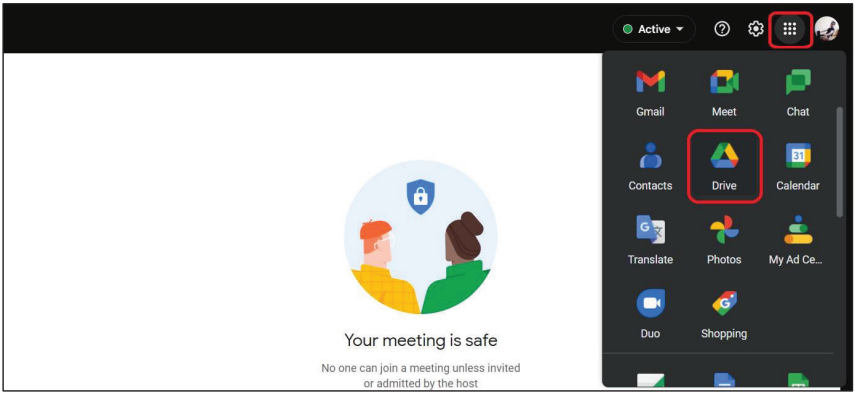
იგი აუცილებელია იმ შემთხვევაში, თუ ჩვენ გავხდებით თავდასხმის მსხვერპლი და შეგვეზღუდება საკუთარ ფაილებზე, სურათებზე, დოკუმენტებსა და სხვა დანარჩენზე წვდომა. მონაცემთა სარეზერვო ასლები ***(Backup)*** წარმოადგენს ერთგვარ რეზერვს, შენახულ მეხსიერებას. ეს ნიშნავს იმას, რომ ჩვენი ფაილების დაკარგვის, დაზიანების თუ წაშლის შემთხვევაში მარტივად შევძლებთ პირვანდელი სახის დაბრუნებას და აღდგენას. ეს საკითხი არ არის მხოლოდ ჰაკერული თავდასხმებისგან წარმოშობილი პრობლემა - არსებობს შემთხვევები, როდესაც შეიძლება უნებლიედ წავშალოთ ესა თუ ის დოკუმენტი, ფაილი, სურათი და სხვა. მონაცემთა სარეზერვო

ასლი მნიშვნელოვანი ფუნქციაა, რათა მარტივად მოხდეს აღდგენა და პრობლემის გადაჭრა.

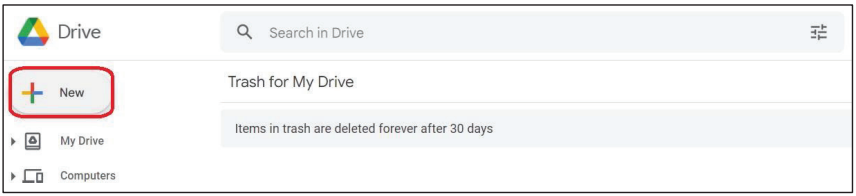
ჩვენ არ ვსაუბრობთ სისტემურ მონაცემთა სარეზერვო ასლების შექმნაზე. ეს სხვა საკითხს წარმოადგენს - კომპიუტერული სისტემების, პროგრამების თუ სხვა სახის უზრუნველყოფის აღდგენა მარტივი საქმე არ გახლავთ, იგი მოითხოვს დიდ მეხსიერებას და ფინანსებს, ეს უფრო მეგა კომპანიების საქმესა და ინტერესის სფეროს წარმოადგენს, თუმცა ხშირად ისინიც სრულად ვერ ახდენენ სისტემური სარეზერვო ასლების შექმნას.

აღნიშნული საკითხი განვიხილოთ უფრო დეტალურად: კიბერუსაფრთხოების ექსპერტები მონაცემთა სარეზერვო ასლების შექმნის უამრავ მეთოდს, ვებ-გვერდსა და პროგრამას გვთავაზობენ. ყველაზე მნიშვნელოვანი, რაც უნდა გავითვალისწინოთ, არის ის, რომ ჩვენი კომპიუტერული მოწყობილობის მეხსიერება არ გამოვიყენოთ მონაცემთა სარეზერვო ასლის შესაქმნელად, რადგან თუ გავხდით კიბერთავდასხმის მსხვერპლი, სარეზერვო ასლებიც რისკის ქვეშ დადგება. რომელი მეთოდი შეიძლება გამოვიყენოთ? სამწუხაროდ, ყველა კიბერრეზერვის სივრცეს გააჩნია ლიმიტი, რაც შეიძლება არასაკმარისი აღმოჩნდეს. სხვადასხვა კომპანიები გარკვეული ფინანსების სანაცვლოდ გვთავაზობენ ლიმიტის გაზრდას. საერთო ჯამში ეს საკითხი ხარჯებთან კი არის დაკავშირებული, მაგრამ უსაფრთხოების თვალსაზრისით სჯობს, ფინანსები გავიღოთ, ვიდრე მეტად ვიზარალოთ. ამ შემთხვევაში ჩვენ რეკომენდაციას ვუწევთ „გუგლი დრაივს“ ***(Google Drive),*** რომელიც დიდი პოპულარობით სარგებლობს საზოგადოებაში. როგორ შეიძლება შევქმნას სარეზერვო ასლები „გუგლი დრაივზე“? ეს არ წარმოადგენს დიდ სირთულეს, ამისთვის გვჭირდება, რეგისტრაცია „გუგლიზე“, უნდა გვქონდეს ანგარიში (პროფილი), შემდეგ შეგვიძლია შევიდეთ ვებ-გვერდ ***„http://drive.google.com“ -ზე*** ან ***„http://gmail.com“ -ზე,*** ანუ ***„გუგლი მეილზე“.*** ამ შემთხვევაში განვიხილოთ ელექტრონული ფოსტიდან გადასვლის მაგალითი - ფოსტაზე შესვლის შემდეგ, ზედა მარჯვენა კუთხეში ვხსნით ფანჯარას - ***„გუგლის აპლიკაციები“ (Google Apps),*** შემდეგ ვაჭერთ ***„გუგლი დრაივს“ (Drive)*** და გადავდივართ ***„გუგლი დრაივის“*** სივრცეში, სადაც მარცხენა კუთხეში უნდა დავაჭიროთ ღილაკს - ***„ახალი“ (New),*** შემდეგ გვაქვს რამდენიმე ვარიანტი, მაგალითად, ***ახალი ფოლდერის შექმნა (New Folder), ფაილის ატვირთვა (File upload)*** და ***ფოლდერის ატვირთვა (Folder upload),*** ახალი ფოლდერის

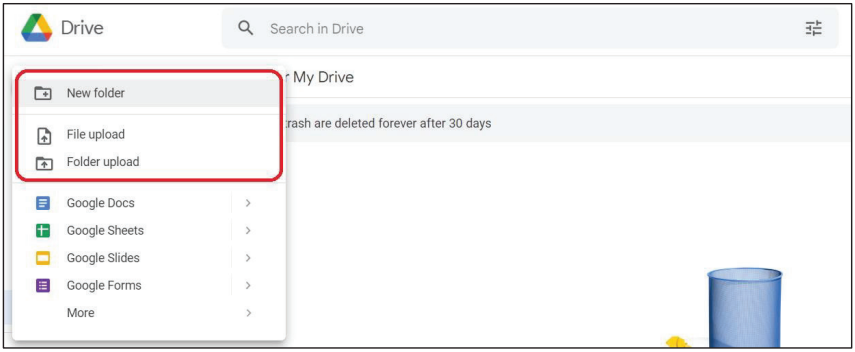
შექმნის შემთხვევაში გაგვიხსნის ახალ ფოლდერს, მოგვთხოვს სახელის დარქმევას, შემდეგ შეგვეძლება აღნიშნულ ფოლდერში ახალი ფაილის დამატება. თუ ავირჩევთ თავიდანვე ფაილის ატვირთვას, გაგვიხსნის ფანჯარას, სადაც მოვძებნით კომპიუტერში ჩვენთვის სასურველ ფაილებს ,,დარეზერვებისთვის''. მოვნიშნავთ და დავაჭერთ ღილაკს - ***გახსნა (Open),*** ამ შემთხვევაში აღნიშნული სიტყვა ითარგმნება, როგორც ***ატვირთვა.***



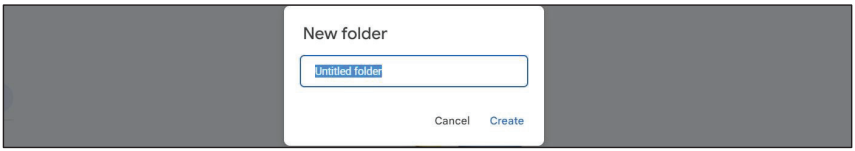
სურათი 16: „გუგლის აპლიკაციების“ ფანჯრის გახსნა და „გუგლი დრაივის“ არჩევა.



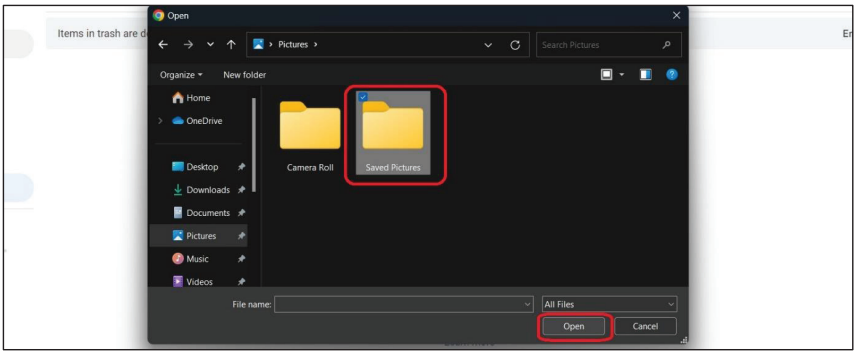
სურათი 17: ღილაკი „ხალის“ არჩევა.



სურათი 18: ახალი ფოლდერი შექმნა, ფაილის ატვირთვა, ფოლდერის ატვირთვა.



სურათი 19: ახალი ფოლდერის გაკეთება.



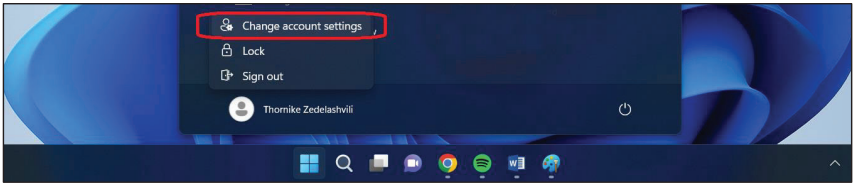
სურათი 20: ფაილის ან ფოლდერის ატვრთვა.

პროგრამული უზრუნველყოფის და ოპერატიული სისტემების განახლება

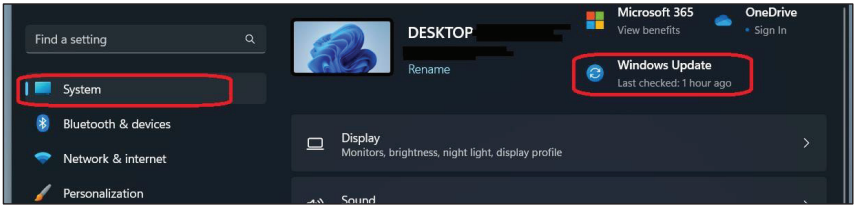
კომპიუტერულ სისტემებს გააჩნია ავტომატურად განახლების საშუალება, მაგრამ ხშირ შემთხვევაში ჩვენი ნებართვის გარეშე ეს საკითხი ვერ გადაწყდება. სისტემები განახლების წინ გვისვამენ შეკითხვას: განახლდეს თუ არა ჩვენი სისტემა, პროგრამა, აპლიკაცია? კვლევებით დასტურდება, რომ უმეტესად ადამიანებს ეზარებათ დროული და მუსმივი განახლებები, რაც შემდეგ იწვევს კიბერუსაფრთხოების რისკების გაზრდას. არაერთხელ ვთქვით და გავიმეორებთ: მოძველებული სისტემა დაუცველობის რისკს ყოველთვის ზრდის.

ამ შემთხვევაში დეტალურად განვიხილოთ ორი წამყვანი კომპიუტერული სისტემა. ***Windows-ი*** და ***MacOS-ი. Windows-ის*** ოპერადიული სისტემების განახლება დიდ სირთულეს არ წარმოადგენს - როგორც აღვნიშნეთ, იგი ავტომატურ რეჟიმში გვეკითხება ნებართვას განახლების შესახებ და გვაწვდის სრულყოფილ ინფორმაციას. აღსანიშნავია, რომ ***Windows-ის*** სისტემას აქვს ბევრი ***ხარვეზი (Bug),*** მაგრამ კომპანია ***Microsoft-ი,*** რომელიც აღნიშნულ ოპერატიულ სისტემას ქმნის, ზუსტად ამ განახლებებით ცდილობს, გამოასწოროს სხვადასხვა ხარვეზები. როგორ განვაახლოთ ან გავიგოთ ჩვენი ოპერატიული სისტემა განახლებულია თუ არა? ამისთვის საჭიროა, შევიდეთ ***საწყის მენიუში (Start menu),*** შემდეგ გადავიდეთ ***შეცვალეთ ანგარიშის პარამეტრებში (Change account Settings),*** ავირჩიოთ ღილაკი ***სისტემა (System)*** და მარცხენა მხარეს ფანჯარაში გამოტანილ მენიუში მოვძებნოთ და დავაჭიროთ ღილაკს - ***ვინდოუსის განახლება (Windows Update).*** აქ ჩვენ შეგვიძლია ვნახოთ, როგორც განახლების ისტორია, ასევე შევამოწმოთ განახლებულია თუ არა ჩვენი სისტემა.

სურათი 21: საწყისი მენიუს გახსნა.



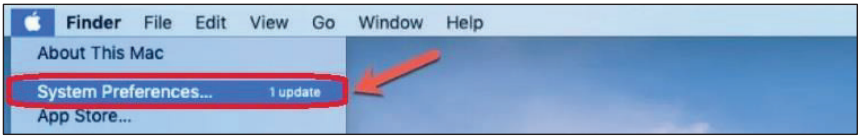
სურათი 22: შეცვალე ანგარიშის პარამეტრებში გადასვლა.



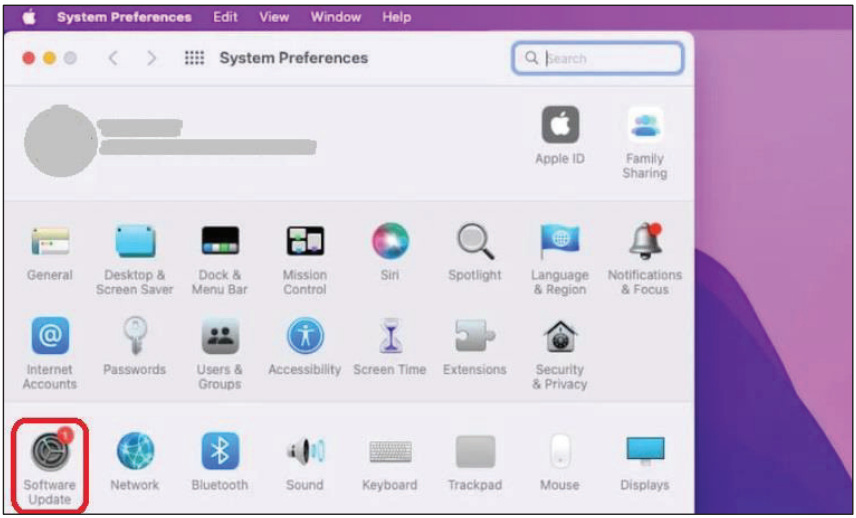
სურათი 23: ღილაკი „სისტემის“ არჩევა და Windows-ის განახლება.

macOS

რაც შეეხება ***Apple-ის*** პროდუქციას, აქ ყველაფერი ცოტა სხვაგვარადაა - ***Mac-ის*** სისტემის განახლება და შემოწმება შეგვიძლია შემდეგი მოქმედებით: ეკრანის ზედა მარცხენა კუთხეში დავაჭერთ ***„ეფლის ლოგოს“ (Apple icon),*** შემდეგ ავირჩევთ ღილაკს - ***სისტემის პარამეტრები (System preferences),*** გადავალთ ***პროგრამული უზრუნველყოფის განახლებაში (Software Update)*** და დავაჭერთ ღილაკს - ***განაახლე ახლავე (Update now),*** რის შედეგადაც ჩვენი ოპერატიული სისტემა განახლდება, ან შეამოწმებს, განახლებულია თუ არა.



სურათი 24: „ეფლის ლოგოს“ მოძებნა და სისტემის პარამეტრებში შესვლა.



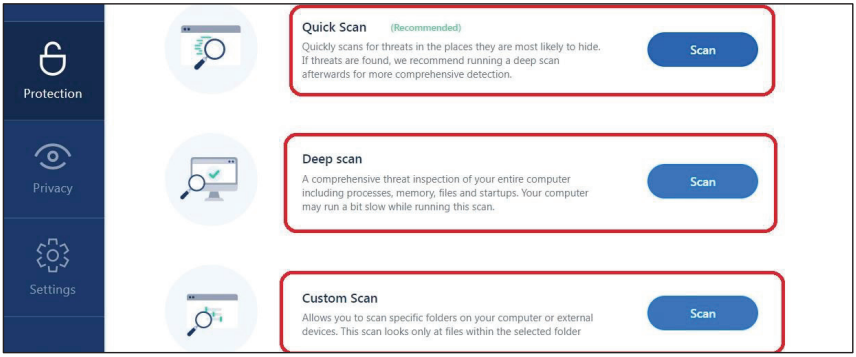
სურათი 25: პროგრამული უზრუნველყოფის განახლებაში გადასვლა.

სურათი 26: დაჭერა ღილაკზე „განაახლე ახლავე“.

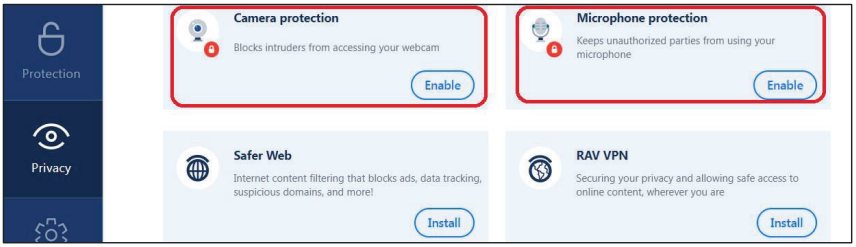
პროგრამული უზრუნველყოფისა და სისტემების ერთ-ერთ მნიშვნელოვან თავდაცვით მექანიზმს წარმოადგენს ანტივირუსი. იგი არის ის მნიშვნელოვანი ინსტრუმენტი ჩვენს ხელში, რომელსაც შეუძლია მავნე კოდის, ფაილების, პროგრამების აღმოჩენა და წაშლა. ანტივირუსის მიმართულებით მრავალფეროვნება გვაქვს და შეგვიძლია, ბევრი ფასიანი თუ უფასო პროგრამა დავაყენოთ. შეგვიძლია, თითოეული მათგანის აღწერას გავეცნოთ და იმის მიხედვით გადავწყვიტოთ, რომელი უფრო სასურველია ჩვენთვის. რა თქმა უნდა, ყველა მათგანს ვერ განვიხილავთ. შესაბამისად, გამოვყოფთ იმ ანტივირუსებს, რომელიც ***Windows 11 - ის***

ვერსიას ოფიციალურად მოჰყვება. პირველი, ეს არის ***RAV Antivirus*** და მეორე - ***McAfee Security Center.***

RaV Antivirus-ი გვთავაზობს ***სწრაფ სკანირებას (Quick scan),*** იმ მიზნით, რომ სწრაფად აღმოაჩენს სხვადასხვა კომპიუტერულ განყოფილებაში ვირუსს ან მავნე პროგრამას, რასაც წაშლის. ასევე, შეგვიძლია ავირჩიოთ კომპიუტერის ***ღრმა სკანირება (Deep scan),*** რომლის შემთხვევაშიც ანტივირუსი მთლიანად დაასკანერებს კომპიუტერულ სისტემას. მესამე ვარიანტი - მოვნიშნოთ ინდივიდუალურად ის სივრცეები, რომელთა გადამოწმებაც გვინდა ***(Custom Scan). RaV Antivirus-ით*** შეგვიძლია ჩვენი კომპიუტერის, კამერისა და მიკროფონის დაცვა, რათა არ მოხდეს უნებართვო შეღწევა და ჩვენი კამერისა თუ მიკროფონის გამოყენება თავდამსხმელის მხრიდან. ამ ყველაფრის განხორციელება მარტივად არის შესაძლებელი, რაც ჩვენს მიერ წარმოდგენილ სურათებზეა ნაჩვენები.



სურათი 27: სწრაფი, ღმა და ჩვენი შეხედულებისამებრ სკანირება.



სურათი 28: კომპიუტერის კამერისა და მიკროფონის სკანირება.

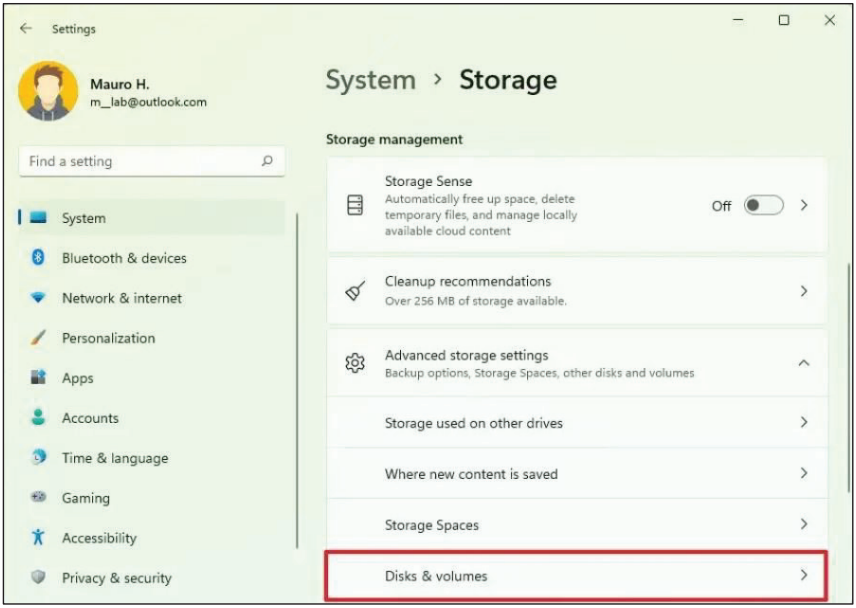
რაც შეეხება ***McAfee Security Center-ს,*** იგი ასევე წარმოადგენს ანტივირუსს, რომელიც ბევრ თავდაცვით ფუნქციას გვთავაზობს ***RaV Antivirus-ის*** მსგავსად. მათი ფუნქციები ერთმანეთისგან მნიშვნელოვნად არ განსხვავდება.

მყარი დისკის დაშიფრვაა

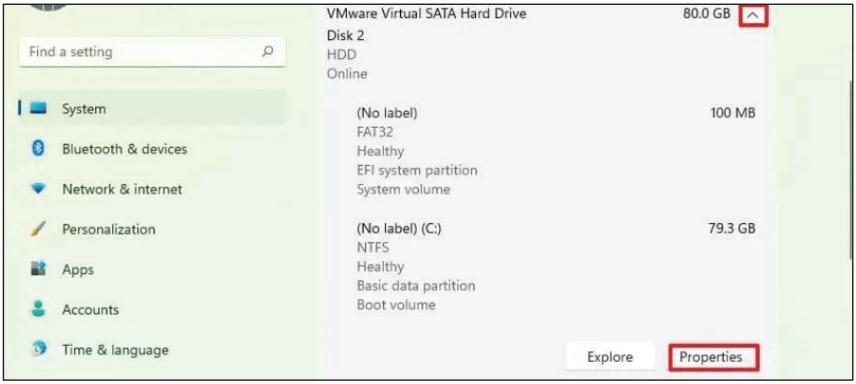
იქიდან გამომდინარე, რომ ხშირად რეალურ სივრცეშიც კი არ ვართ დაზღვეული უნებართვო წვდომისგან პირად კომპიუტერულ მოწყობილობაზე, აუცილებელია, ინდივიდუალური თავდაცვითი ხერხები გამოვიყენოთ. ერთ-ერთი ასეთია მყარი დისკის დაშიფრვა. Windows-ის უახლეს ვერსიებს აქვთ ფუნქცია ***„BitLocker",*** რომელიც გულისხმობს მყარი დისკის დაცვას პაროლით.

დეტალურად გავიაროთ, თუ როგორ ხდება ***Windows 11-ზე „BitLocker"-ის*** ჩართვა არამყარი და მყარი დისკების შემთხვევაში, ასევე ***USB*** ფლეშ დისკის შემთხვევაში:

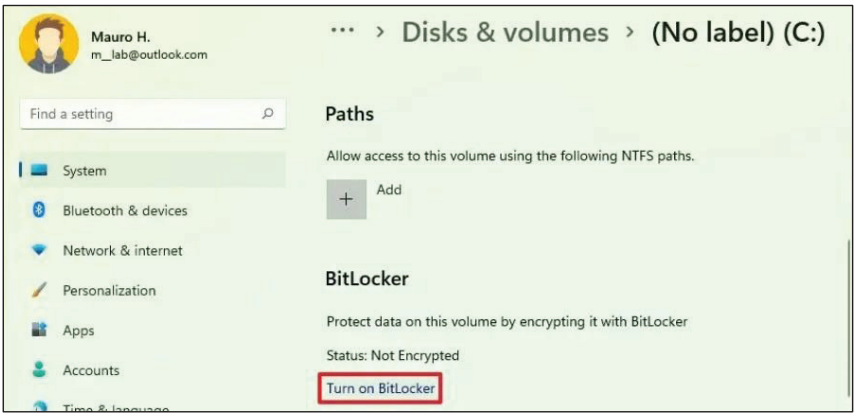
პარამეტრები (Settings) → სათავსო (Storage) → "მეხსიერების მენეჯმენტის" (Storage management) განყოფილება → მეხსიერების გაფართოებული პარამეტრები (Advanced storage settings) → დისკები და მოცულობა (Disks & volumes) → დისკი მოცულობით დაშიფრვისთვის (Disk volume) → მოცულობა (Volume) → BitLocker დაშიფრვა (encryption) → საკუთრება (Properties) → ჩართვა BitLocker (Turn on) → ოპერაციული სისტემის დისკის (Operating system drive) განყოფილება → BitLocker-ის ჩართვა (Trun on BitLocker) → აღდგენის გასაღების სარეზერვო ასლის ვარიანტი (the option to backup the recovery key) | შენახვა ჩვენს Microsoft ანგარიშში (Save to your Microsoft account) → შემდეგი (next) → მხოლოდ გამოყენებული დისკის სივრცის დაშიფრვა (Encrypt used disk space only) → შემდეგი (next) → ახალი დაშიფრვის რეჟიმი (New encryption mode) → შემდეგი (next) → BitLocker მუშაობის სისტემის შემოწმება (Run BitLocker system check) → ახლავე გადატვირთვა (Restart now).



სურათი 29: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (1). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*

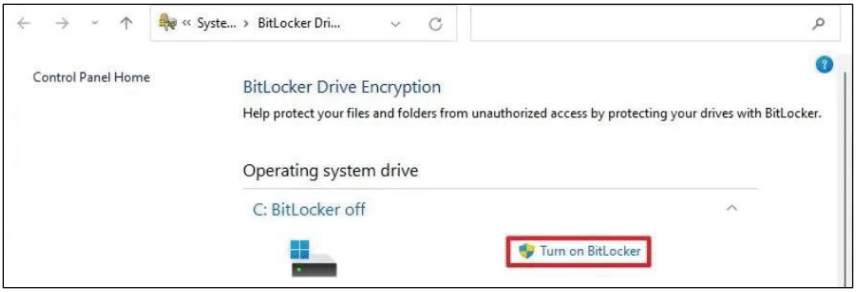


სურათი 30: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (2). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*



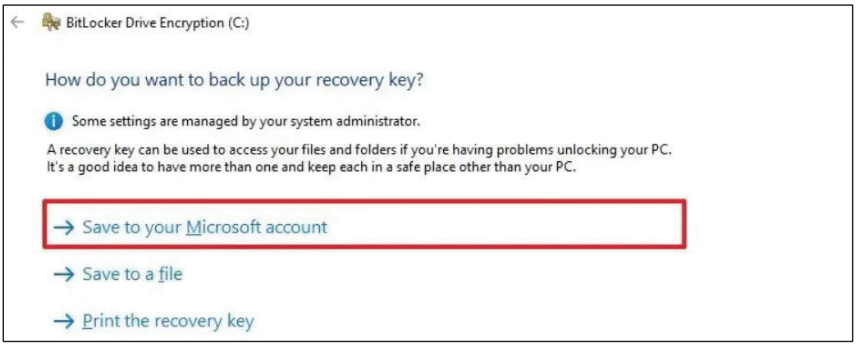
სურათი 31: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (3). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/



სურათი 32: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (4). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/

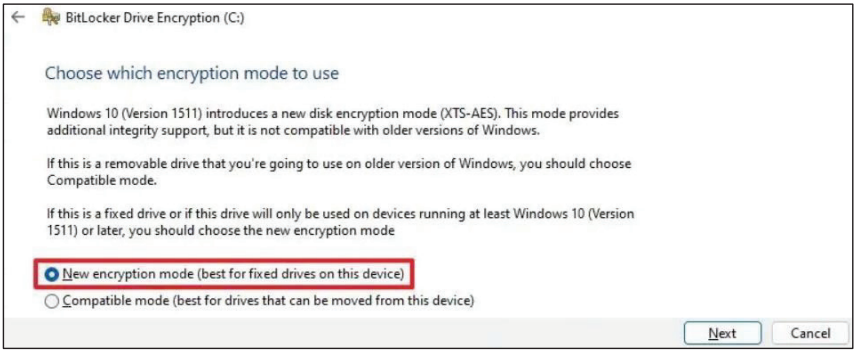


სურათი 33: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (5). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/

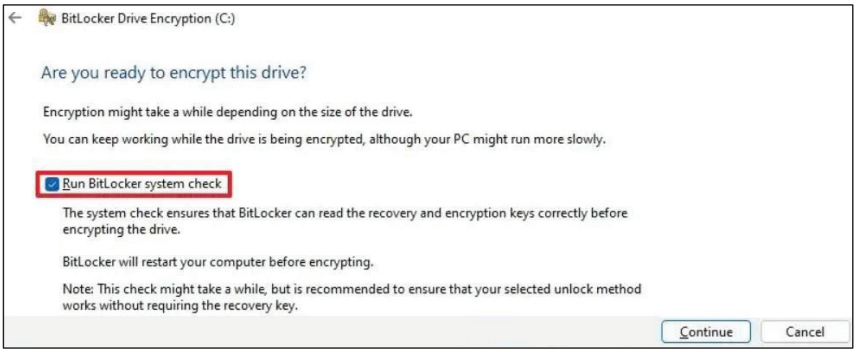
სურათი 34: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (6). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/



სურათი 35: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (7). *წყარო:*

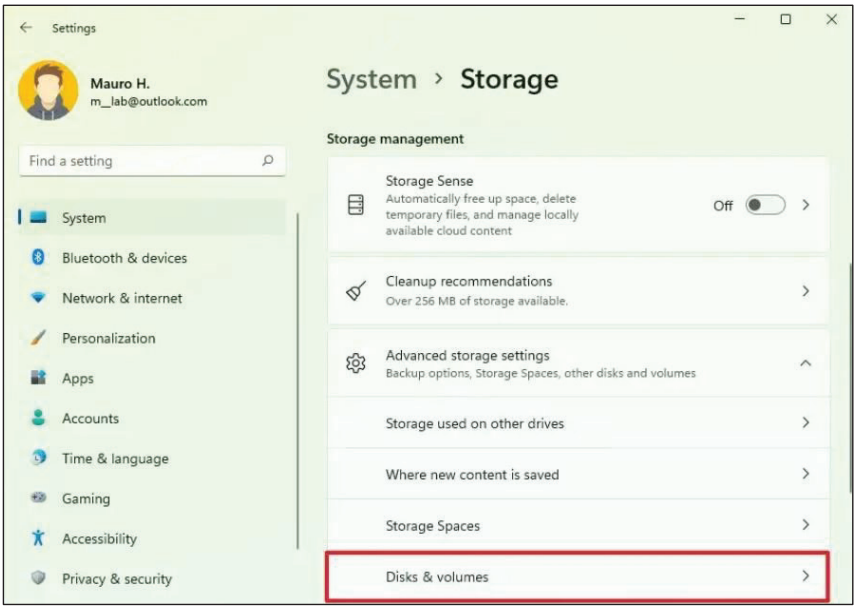
https://pureinfotech.com/enable-bitlocker-windows-11/



სურათი 36: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (8). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*

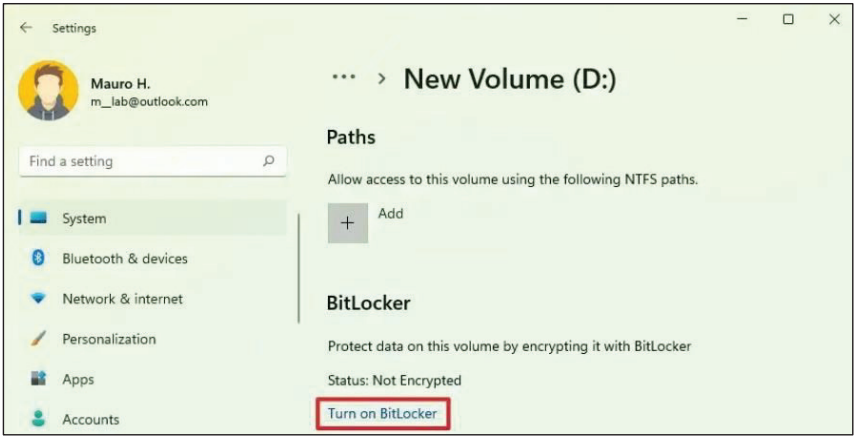
BitLocker-ის ჩართვა მყარ მონაცემთა დისკზე (ფიქსირებულ მონაცემთა დისკზე):

პარამეტრები (Settings) → სათავსო (Storage) → "მეხსიერების მენეჯმენტის" (Storage management) განყოფილება → მეხსიერების გაფართოებული პარამეტრები (Advanced storage settings) → დისკები და მოცულობა (Disks & volumes) → მყარი მონაცემთა დისკის დაშიფრვა (ფიქსირებულ მონაცემთა დისკი) → მოცულობა (Volume) → BitLocker დაშიფვრა (encryption) → საკუთრება (Properties) → BitLocker-ის ჩართვა (Trun on BitLocker) → „მყარ მონაცემთა დისკის“ განყოფილება (ფიქსირებული მონაცემთა დისკი) (Fixed data drives) → BitLocker-ის ჩართვა (Trun on BitLocker) → დისკის განბლოკვისთვის პაროლის გამოყენების შემოწმება (Use a password to unlock the drive) → პაროლის შექმნა და დადასტურება (BitLocker-ის განბლოკთვისთვის) → შემდეგი (next) → გასაღებით აღდგენის ვარიანტი | შენახვა ჩვენს Microsoft ანგარიშში (Save to your Microsoft account) / შენახვა USB ფლეშ დისკზე / ფაილში შენახვა / აღდგენის დაყენება → შემდეგი (next) → მხოლოდ გამოყენებული დისკის სივრცის დაშიფვრა (Encrypt used disk space only) → შემდეგი (next) → ახალი დაშიფრვის რეჟიმი (New encryption mode) → შემდეგი (next) → დაშიფრვის დაწყება (Start encrypting) → დახურვა (Close). *აღნიშნული ინსტრუქციის შესრულების შემდეგ, BitLocker-ი დაშიფრავს მთელ მოცულობას მყარ დისკზე.*

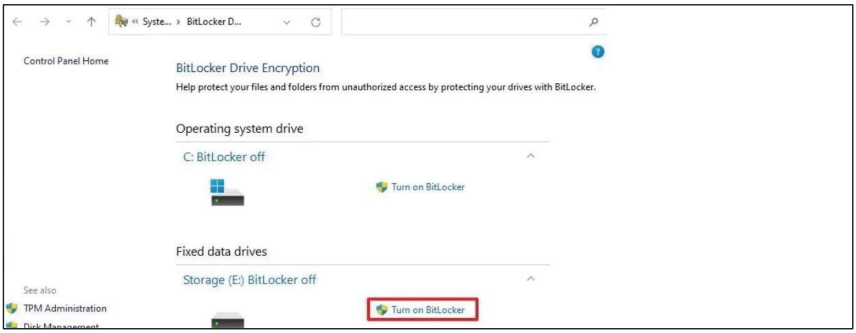


სურათი 37: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (1). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*

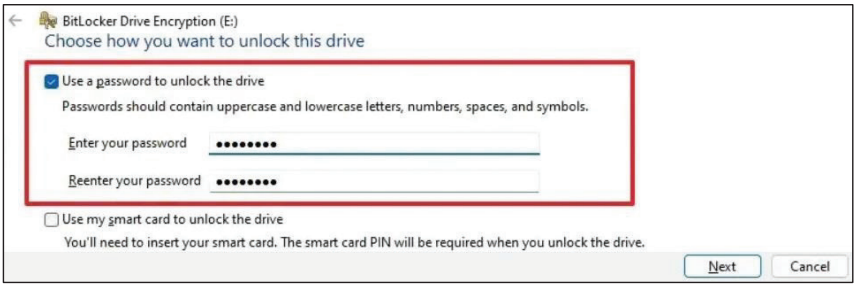
სურათი 38: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (2). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*



სურათი 39: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (3). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*



სურათი 40: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (4). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*

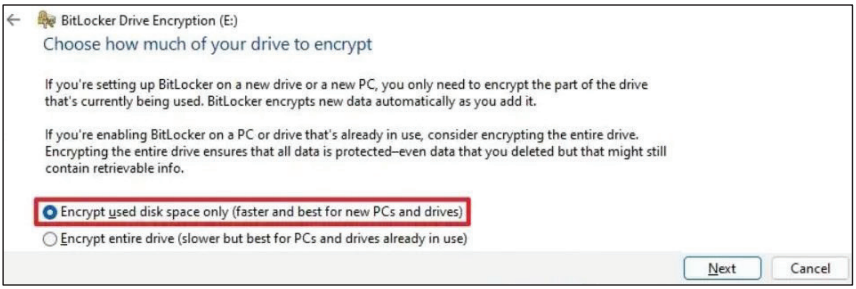


სურათი 41: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (5). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 42: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (6). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/

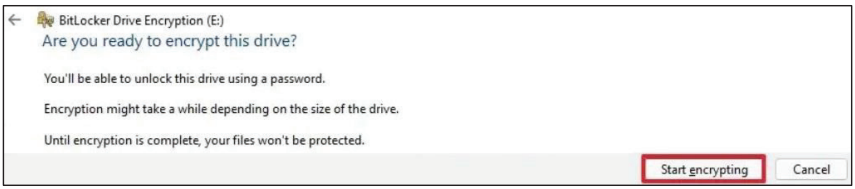


სურათი 43: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (7). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 44: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (8). *წყარო:*

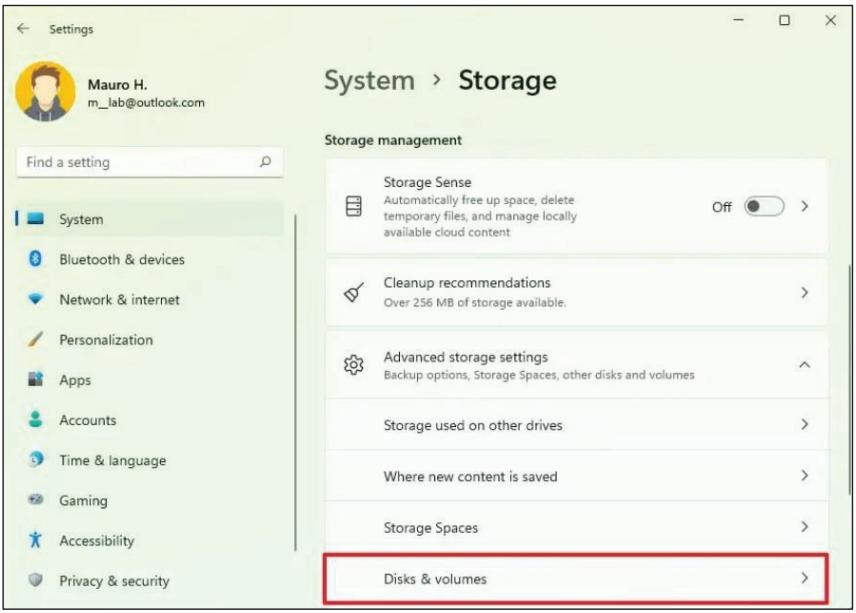
https://pureinfotech.com/enable-bitlocker-windows-11/



სურათი 45: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (9). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*

BitLocker-ის ჩართვა USB ფლეშ დისკზე:

პარამეტრები (Settings) → შენახვა (Save) → "მეხსიერების მენეჯმენტის" (Storage management) განყოფილება → მეხსიერების გაფართოებული პარამეტრები (Advanced storage settings) → დისკები და მოცულობა (Disks & volumes) → USB ფლეშ დისკის დაშიფრვა (encrypting) → მოცულობა (Volume) → BitLocker To Go დაშიფრვა (encryption) → საკუთრება (Properties) → ჩართვა BitLocker (Turn on) → "მოხსნად მონაცემთა დისკები BitLocker To Go" (Removable data drives BitLocker To Go) → ჩართვა BitLocker (Turn on) სათავსოსთვის (რეზერვისთვის) → დისკის განბლოკვისთვის პაროლის გამოყენების შემოწმება (Use a password to unlock the drive) → პაროლის შექმნა და დადასტურება (BitLocker-ის განბლოკვისთვის) → შემდეგი (next) → გასაღებით აღდგენის ვარიანტი | შენახვა ჩვენს Microsoft ანგარიშში (Save to your Microsoft account) / ფაილში შენახვა / აღდგენის დაყენება → შემდეგი (next) → მხოლოდ გამოყენებული დისკის სივრცის დაშიფვრა (Encrypt used disk space only) → შემდეგი (next) → თავსებადი რეჟიმი (the Compatible mode) → შემდეგი (next) → დაშიფრვის დაწყება (Start encrypting) → დახურვა (Close). *აღნიშნული მოქმედების დასრულების შემდეგ თქვენს USB ფლეშ დისკზე არსებული მონაცემები დაშიფრული იქნება BitLocker To Go-ით.*

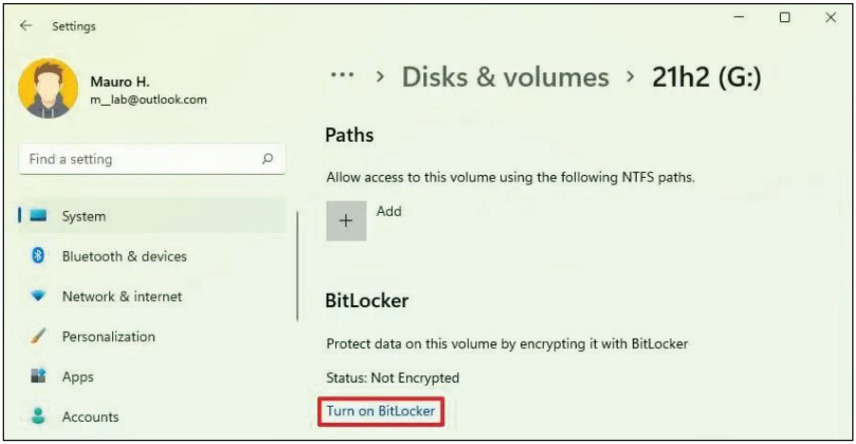


სურათი 46: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (1). *წყარო:*

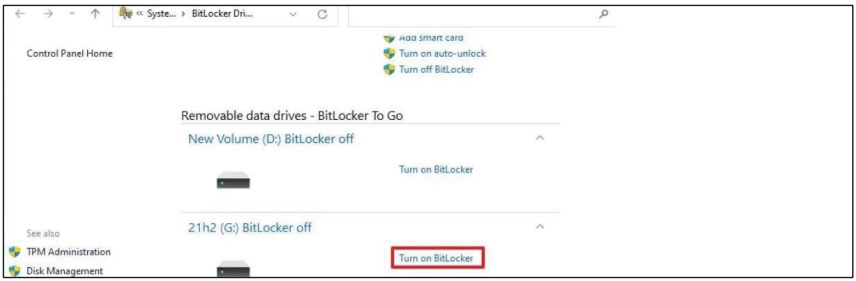
https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 47: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (2). *წყარო:*

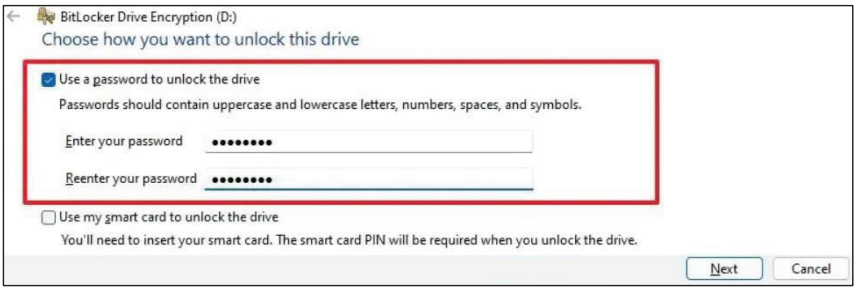
https://pureinfotech.com/enable-bitlocker-windows-11/



სურათი 48: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (3). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*



სურათი 49: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (4). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*



სურათი 50: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (5). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*

სურათი 51: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (6). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 52: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (7). *წყარო:*

https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 53: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (8). *წყარო:*

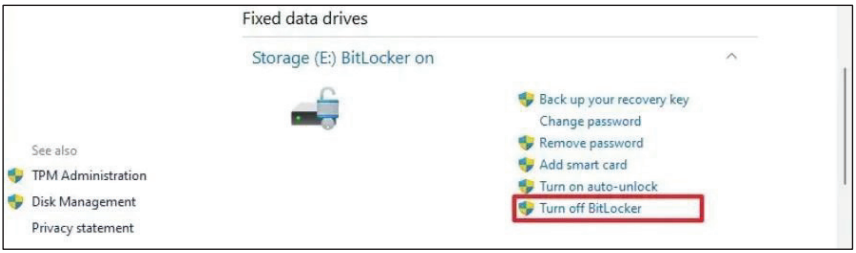
https://pureinfotech.com/enable-bitlocker-windows-11/

BitLocker-ის გამორთვა:

საწყისი მენიუ (Start menu) → კონტროლ პანელი (Control Panel) → სისტემა და უსაფრთხოება (System and Security) → BitLocker დისკის დაშიფრვა (Drive Encryption) →

BitLocker-ის დისკი → BitLocker-ის გამორთვის (Turn off) განყოფილება → BitLocker-ის გამორთვა (Turn off).[204] *გამორთვას შეიძლება გარკვეული დრო დასჭირდეს, გააჩნია, რა მოცულობაზეა საუბარი.*

სურათი 54: BitLocker-ის გამორთვა Windows 11-ზე (1). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*



სურათი 55: BitLocker-ის გამორთვა Windows 11-ზე (2). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*

[204] *Huc M., "How to enable BitLocker on Windows 11", pureinfotech, p. 1, 2022. https://pureinfotech.com/enable-bitlocker-windows-11/*

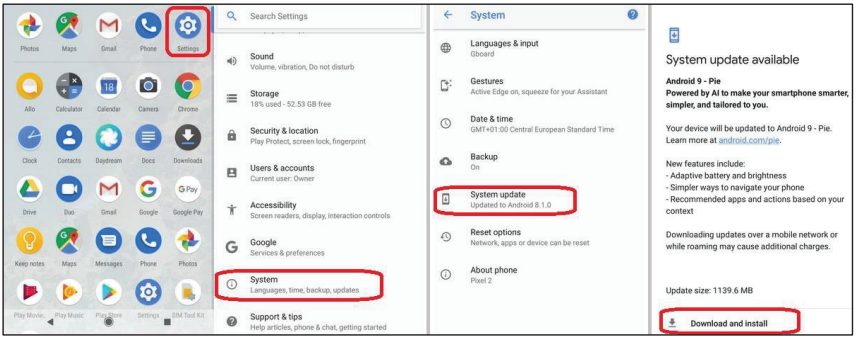
რა უნდა ვიცოდეთ სმარტფონების გამოყენების დროს - მობილური მოწყობილობების კიბერჰიგიენა

ხშირ შემთხვევაში მომხმარებელს ჰგონია, რომ პერსონალური კომპიუტერი არაფრით განსხვავდება მობილური ტელეფონისგან და მისი უსაფრთხოება ისევე უნდა დავიცვათ, როგორც კომპიუტერის. რა თქმა უნდა, მობილური ტელეფონის მონაცემები ბევრი რამით ჰგავს პერსონალური კომპიუტერის კიბერჰიგიენას, მაგრამ არის რიგი განსხვავებებიც. ვინაიდან მობილურ ხელსაწყოებზე მუშაობს Android-ი და IOS სისტემები, განსხვავებები უსაფრთხოების ნაწილში ბუნებრივია. ადამიანები მობილურ ხელსაწყოებს იყენებენ ინტენსიურად, ეს სფერო უკვე იმ დონეზე განვითარდა, ახალ ტექნოლოგიებზეა დაკავშირებული ყველანაირი აპლიკაცია, მათ შორის ელფოსტა, ინტერნეტ ბანკინგი, სოციალური ქსელები და ა.შ. ასევე მობილურ ტელეფონში გვაქვს პირადი ინფორმაცია, ფაილები, ფოტო და ვიდეო მასალა. ამიტომ მობილური ხელსაწყოების უსაფრთხოება მნიშვნელოვან საკითხს წარმოადგენს, რათა არ მოხდეს უნებართვო წვდომა, არ მოხდეს ინფორმაციის უკანონო მოპოვება, მოსმენა, ინტერნეტ ბანკინგზე წვდომა და ფინანსური ზარალი. ხშირ შემთხვევაში ადამიანებს სამსახურის ელფოსტაც მობილურზე აქვთ მიბმული. ეს კი უფრო მეტად გვავალდებულებს კიბერჰიგიენის დაცვას.

უკვე აღვნიშნეთ, დროთა განმავლობაში კომპიუტერული ტექნიკა ძველდება, ვითარდება ტექნოლოგიები და იქმნება ახალი სისტემები, პროგრამები, რაც საჭიროებს მაღალ მონაცემებს, ჩვენი ძველი მოწყობილობები ვეღარ აკმაყოფილებს. უპირველესად, უსაფრთხოება უნდა დავიწყოთ შესაბამისი კომპიუტერული ტექნიკისა და მოწყობილობების შეძენით. მნიშვნელოვანია, ჩვენი კომპიუტერული ტექნიკა და მობილური ხელსაწყო მონაცემებით აკმაყოფილებდეს კიბერუსაფრთხოების

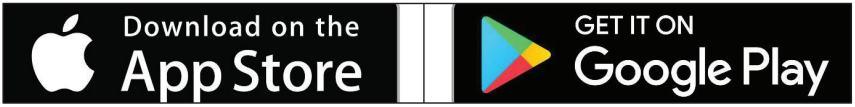
ნორმებს. აქ ერთ-ერთ მნიშვნელოვან საკითხს პროგრამული უზრუნველყოფა და სისტემების განახლება წარმოადგენს.

როგორც კომპიუტერზე, ასევე მობილურ მოწყობილობებზეც, ***Android-ი*** და ***iOS-ი,*** პერიოდულად გვთავაზობს სისტემის განახლებას, ამ დროს სისტემა გვეკითხება - განახლდეს თუ არა. შეგვიძლია, სისტემა გადავამოწმოთ და განვაახლოთ, როცა ამის სურვილი გვექნება, ეს არ წარმოადგენს სირთულეს. ***Android*** სისტემის გადასამოწმებლად ან განახლებისთვის უნდა შევიდეთ პარამეტრებში ***(Settings)*** გადავიდეთ სისტემებში ***(System)*** და დავაჭიროთ ღილაკს - სისტემის განახლება ***(System update),*** ხოლო ***IOS*** სისტემის განახლებისთვის უნდა შევიდეთ პარამეტრებში ***(Settings),*** შემდეგ გადავიდეთ მთავარში ***(General)*** და დავაჭიროთ ღილაკს - სისტემის განახლება ***(Software Update).*** ჩვენი სისტემა დაიწყებს განახლებას, თუ განახლებულია და აყენია ბოლო ვერსია, დაგვიწერს, რომ სისტემა არ საჭიროებს განახლებას.



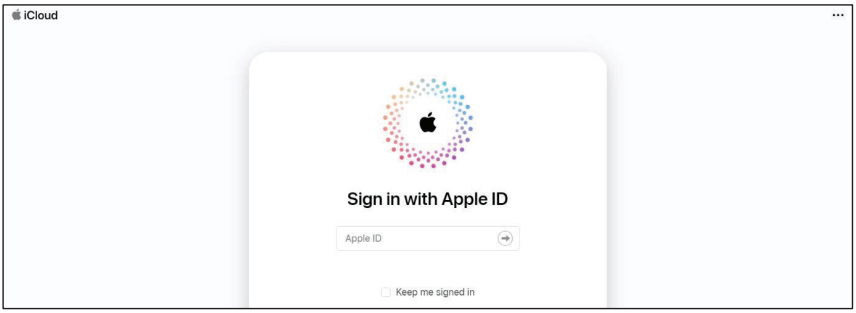
სურათი 56: Android სისტემის განახლება ან გადამოწმება.

სურათი 57: IOS სისტემის განახლება ან გადამოწმება.



რაც შეეხება პროგრამულ უზრუნველყოფას, კომპიუტერისგან განსხვავებით, სადაც ***Windows-ი*** აყენია, მობილურში გვაქვს განსხვავებული ფორმატი - ***Android*** სისტემაზე არის ასეთი აპლიკაცია - ***Google Play Story,*** საიდანაც საშუალება გვაქვს, ნებისმიერი საინტერესო და საჭირო აპლიკაცია გადმოვწეროთ. იმ შემთხვევაში, თუ ***Play Story-ზე*** აპლიკაცია, რომელიც ჩვენ გვჭირდება, არ იძებნება, შეგვიძლია, გადმოვწეროთ სხვადასხვა ვებ-გვერდებიდან ***apk*** დასაინსტალირებელი ვერსია. თუმცა გაითვალისწინეთ, ეს მეთოდი შეიცავს თქვენი მობილური მოწყობილობის დავირუსების რისკს და არ არის რეკომენდებული. ***iOS*** სისტემაზე ფუნქიონირებს ასეთი აპლიკაცია - ***App Store,*** რომელიც იგივე დანიშნულებას ასრულებს, რასაც ***Android-ი,*** თუმცა ***iOS*** სისტემაზე ***apk*** ვერსიების დაყენება შეუძლებელია, რაც ერთგვარად უსაფრთხოების ხარისხს ზრდის.

დღეს ბევრი კარგავს მობილურ ტელეფონს. აქედან გამომდინარე, უნდა ვიცოდეთ, რა ბერკეტი გაგვაჩნია, რა შეგვიძლია, მოვიმოქმედოთ მობილური მოწყობილობის მოსაძებნად. თუ ჩვენს მობილურზე აყენია Android სისტემა, შეგვიძლია, კომპიუტერით ან სხვა მოწყობილობით შევიდეთ საძიებო სისტემა Google-ზე, ჩავწეროთ ინგლისურად: ,,იპოვე ჩემი ტელეფონი'' ***(Find my Phone),*** სადაც მოგვთხოვს ავტორიზაციას Gmail-ის საშუალებით. გაითვალისწინეთ, იმ ელფოსტით გაიაროთ ავტორიზაცია, რომელიც მობილურ მოწყობილობაზე გიყენიათ. თუ ჩვენი ტელეფონი ჩართულია, გვიჩვენებს, სად არის ტერიტორიულად. ხშირად მოპარულ ტელეფონს თიშავენ, ამ შემთხვევაში ამ მოქმედების განხორციელება შედეგს არ გვაძლევს, მაგრამ თუ მობილური მოწყობილობა შემთხვევით დავკარგეთ, ან იმ პიროვნებამ, ვინც მობილური მოგვპარა, ეს ვერ გაითვალისწინა და ჩართული დატოვა, აუცილებლად ვიპოვით. ასევე, ეს გვაძლევს საშუალებას, მობილური დავბლოკოთ, წავშალოთ მონაცემები და გავააქტიუროთ ხმოვანი სიგნალი.

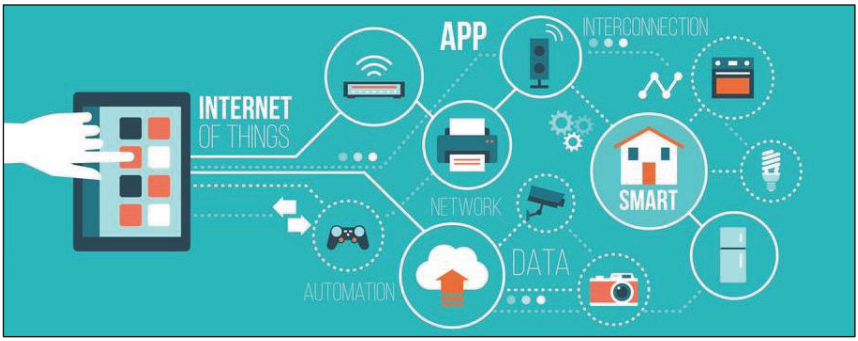


სისტემა ***iOS-ზე*** ასევე მარტივად შეგვიძლია ჩვენი მობილური მოწყობილობის მოძებნა, ამისთვის საჭიროა შევიდეთ ***iCloud.com-ზე,*** სადაც მოგვთხოვს, გავიაროთ ავტორიზაცია, შემდეგ გაგვიხსნის რუკას, სადაც დავინახავთ, სად არის ჩვენი ტელეფონი.

მობილური მოწყობილობის უსაფრთხოებისთვის უნდა გავითვალისწინოთ, რომ იმ შემთხვევაში, თუ არ ვიყენებთ ***Bluetooth-ს,*** უნდა გამოვრთოთ, რადგან შეიძლება

თავდამსხმელმა სწორედ ***Bloetooth-ის*** გამოყენებით შემოაღწიოს უნებართვოთ ჩვენს მობილურ მოწყობილობაში.

ინტერნეტიდან მომდინარე საფრთხეები, როგორ დავიცვათ თავი კიბერსივრცეში



მსოფლიო იმდენად შეეჩვია ტექნოლოგიურ მიღწევებს, ახალ, უფრო ეფექტურ ინტერნეტკავშირსა და მარტივ კომუნიკაციას, რომ საზოგადოება აღარ ფიქრობს, რა როგორ ხდება, თითქოს დეტალურად აღარავის აინტერესებს, როგორ ვამყარებთ მარტივად ინტერნეტის საშუალებით კავშირს, როგორ ვაგვარებთ უამრავ საქმეს და ასე შემდეგ.

ბოლოს და ბოლოს, რა არის ეს ინტერნეტი? მისი სრული დასახელებაა: ***"International Net",***[205] რაც ქართულად ნიშნავს საერთაშორისო ქსელს, მას ,,მსოფლიო ქსელსაც" უწოდებენ. ინტერნეტი არის გლობალური ქსელი, სადაც უამრავი კომპიუტერია დაკავშირებული ერთმანეთთან. იგი ეფუძნება IP პროტოკოლს და ქმნის გლობალურ საინფორმაციო სივრცეს.

მოდით, დეტალურად განვიხილოთ, როგორ ხდება ინტერნეტის მოხმარება, რა დაუცველი სივრცეები არსებობს და როგორ შეიძლება თავიდან ავირიდოთ

[205] *Terra J., "What is the Internet? Reviewing the Basics", Simplilearn, p. 1, 2022. https://www.simplilearn.com/what-is-internet-article*

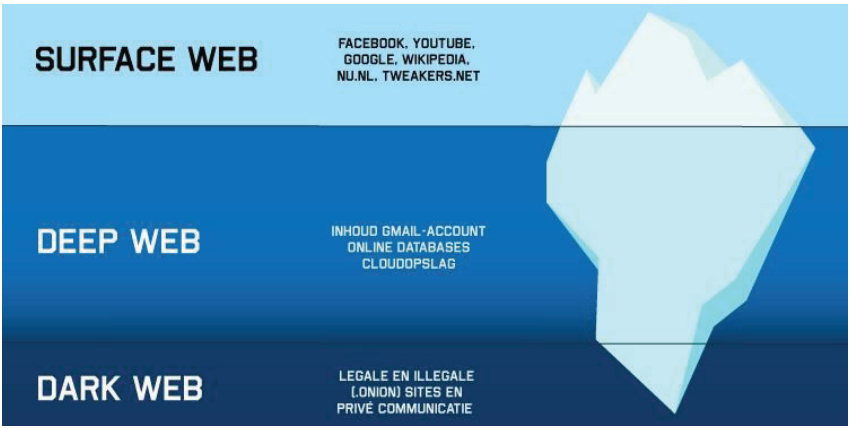
საფრთხეები. არსებობს სხვადასხვა ინტერნეტბრაუზერები - მაგალითად, ***Microsoft Edge, Chrome, Opera, Mozilla Firefox*** და სხვა, რომლებიც წარმოადგენენ ჩვეულებრივ პროგრამას, რომლის საშუალებითაც ჩვენ ვამყარებთ ინტერნეტთან კავშირს - ვსტუმრობთ სხვადასხვა ვებ-გვერდებს, სოციალურ ქსელებს, საძიებო სისტემებს, ვიყენებთ ელექტრონულ ფოსტას და ასე შემდეგ. ამ შემთხვევაში რისკები იზრდება - შესაძლებელია, როგორც ჩვენი ბრაუზერი იყოს დაუცველი და ამით ისარგებლონ ბოროტმა ჰაკერებმა, ასევე არსებობს უამრავი ვებ-გვერდი სადაც შეიძლება უნებურად რამე ვირუსი გადმოვწეროთ, ან რომელიმე ისეთ ვებ-გვერდს ვესტუმროთ, რომელიც დაუცველია.

ჩვენ ყურადღება უნდა მივაქციოთ მნიშვნელოვან საკითხს, რომ არსებობს პროტოკოლი ***http*** და ***https,*** რაც გულისხმობს კომუნიკაციას თქვენსა და სერვერს შორის. ***http-სა*** და ***https-ს*** შორის განსხვავება ის არის, რომ ***http*** ნიშნავს დაუცველობას, ანუ ჩვენი კავშირი თავდამსხმელისთვის არის ხელმისაწვდომი, შეუძლია მარტივად ჩარევა და ინფორმაციის გადაქაჩვა, ხოლო https არის პროტოკოლი, რომელიც გულისხმობს, რომ ჩვენი კავშირი დაცულია. ხშირ შემთხვევაში მომხმარებლები ამას ყურადღებას არ აქცევენ, მაგრამ ეს ძალიან მნიშვნელოვანი საკითხსია, რათა ავტორიზებული კომუნიკაცია იყოს ჩვენსა და სერვერს შორის. ეს გულისხმობს, რომ ჩვენს კომპიუტერულ მოწყობილობასა და სერვერს შორის მონაცემები დაცულია, თავდამსხმელი ვერ მოახდენს უკანონო ჩარევას და ინფორმაციის მოპოვებას. ამ შემთხვევაში რისკს წარმოადგენს ონლაინ შოპინგი, აუცილებლად უნდა დავაკვირდეთ, როგორ ვებ-გვერდზე ვახორციელებთ აღნიშნულს.

სწორედ იმიტომ, რომ ამ საკითხს ნაკლები ყურადღება ექცევა მომხმარებლებში და ზარალიც დიდ ნიშნულზეა, სხვადასხვა მეგაკომპანიები ქმნიან ინტერნეტ ბრუზერებს, მათ შეიმუშავეს ერთგვარი თავდაცვითი მექანიზმი, რომელიც მომხმარებლის გაფრთხილებას გულისხმობს, თუ რომელიმე ვებ-გვერდი არ აკმაყოფილებს დაცულ პროტოკოლს, ბრაუზერი გვაფრთხილებს, რომ აღნიშნული ვებ-გვერდი წარმოადგენს საფრთხეს ჩვენი კომპიუტერისთვის. რაც ყველაზე მნიშვნელოვანია, ჩვენ მაინც გვაქვს არჩევანის საშუალება, გაფრთხილების

მიუხედავად, ვესტუმროთ ამ ვებ-გვერდს თუ არა. ამიტომ, თქვენი უსაფრთხოება საერთო ჯამში ისევ თქვენივე ქმედებებზეა დამოკიდებული.

არსებობს ასეთი პოპულარული რეკლამის ფორმა - ***Popup baner-ი,*** რომელსაც უამრავი ვებ-გვერდი იყენებს. ეს წარმოადგენს უწყინარ რეკლამას, მაგრამ ხშირად ასეთი ბანერები შეიცავენ დავირუსებულ კონტენტს, რომელიც ჩვენი ბრაუზერის პროგრამასაც ავირუსებს. აქ კიდევ ერთხელ უნდა გავამახვილოთ ყურადღება ფიშინგ, ანუ თაღლითურ კიბერთავდასხმებზე, რასაც ჰაკერები ახორციელებენ ყალბი ვებ-გვერდების შექმნით - ისინი ორიგინალს ჰგავს და ამით პირადი ბანკის მონაცემების გამოძალვას ცდილობენ, რაც, ბუნებრივია საბოლოო ჯამში ფინანსური ზარალით მთავრდება.



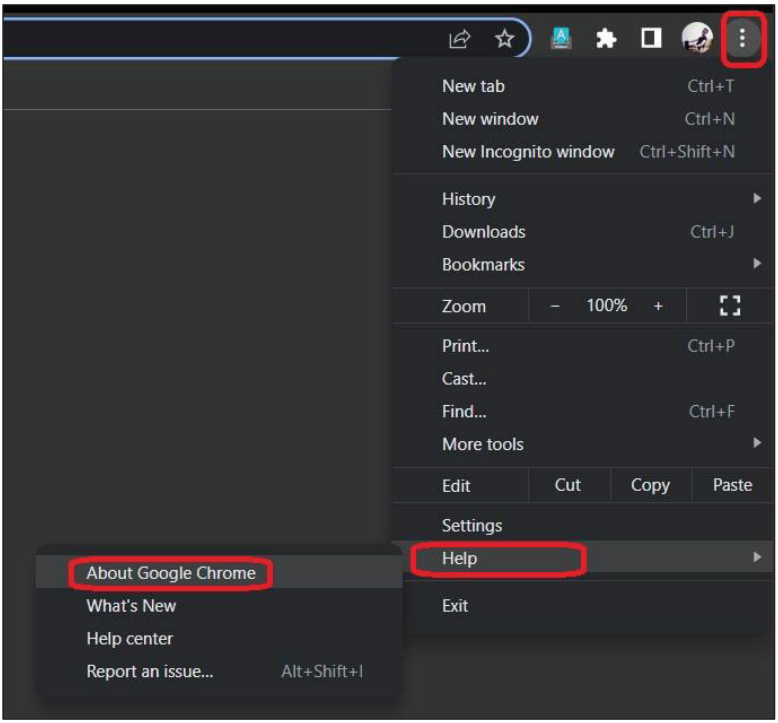
სურათი 58: ზედაპირული ქსელი (სუფთა ვები), ღრმა ქსელი, ბნელი ქსელი (დაფარული ქსელი).

წყარო: https://www.vpn.nl/faq/dark-web

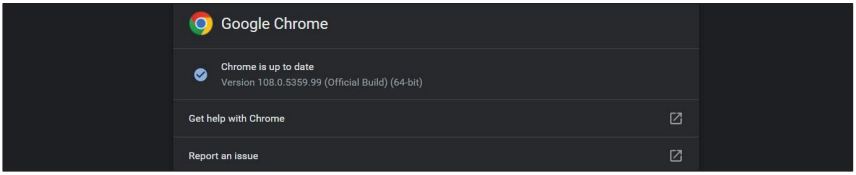
საერთოდ, ინტერნეტში არსებობს სამი სივრცე: ***Surface Web*** - ნიშნავს ზედაპირულ ქსელს, მოიხსენიებენ ***Clear Web-ის*** სახელითაც (სუფთა ვები), ***Deep Web*** - ღრმა ქსელი, მისი შინაარსი შეიძლება იქნას ნაპოვნი პირდაპირ ***URL-ს*** ან ***IP*** მისამართით, ***Darknet*** - ბნელი ქსელი, ცნობილია, როგორც დაფარული ქსელი". ,,დარკნეტში'' მოხვედრა მარტივი არ არის, არსებობს სხვადასხვა პროგრამული საშუალებები, რის

შედეგადაც ჩვეულებრივ რიგით ადამიანსაც შეუძლია ისარგებლოს. აქ მხოლოდ ***ბიტკოინით*** (ელექტრონული ვალუტა) ხდება გადახდა და შეგვიძლია, იოლად შევიძინოთ იარაღი, ნარკოტიკი, ქვეყნების მოქალაქეობა და სხვა.

როგორ დავიცვათ თავი აღნიშნული საფრთხეებისგან? ჩვენ უკვე ვისაუბრეთ კიბერჰიგიენაზე, ანტივირუსებზე, სისტემურ განახლებებსა და სხვადასხვა თავდაცვით მექანიზმებზე. ასევე მნიშვნელოვანია, ჩვენი ინტერნეტბრაუზერი იყოს გადამოწმებული და განახლებული, რეკომენდებულია, ახალი ვერსიის არსებობის შემთხვევაში ჩავანაცვლოთ ძველი ვერსია. თითქმის ყველა ინტერნეტბრაუზერის განახლება ხდება ერთი და იგივე ინსტრუქციით - მაგალითად, განვიხილოთ ბრაუზერი ***Chrome.*** მარჯვენა მხარეს უნდა ჩამოვშალოთ მენიუ, გადავიდეთ ***დახმარების ველში - (Help),*** შემდეგ ***„გუგლი-ჩრომის'' შესახებ (About Google Chrome),*** აქ გამოჩნდება, განახლებულია თუ არა ჩვენი ინტერნეტბრაუზერი.



სურათი 59: „გუგლი-ჩრომის“ განახლება.



სურათი 60: გადამოწმება, განახლებულია თუ არა ბროუზერი „გუგლი-ჩრომი“.

როგორ უნდა გამოვიყენოთ ელექტრონული ფოსტა უსაფრთხოდ - კიბერრისკები და თავდაცვითი ფუნქციები

ჩვენ უკვე ბევრ კონტექსტში ვახსენეთ ***ელექტრონული ფოსტა.*** კიბერსივრცის განვითარებასთან ერთად იხვეწება სისტემები და პროგრამები, ასევე იხვეწება ელექტრონული ფოსტის მოდელები, სოციალური ქსელები და ასე შემდეგ.

ელექტრონული ფოსტა შექმნის დღიდან აქტიურად გამოიყენება. მიუხედავად იმისა, რომ იხვეწება ტექნოლოგიები და იზრდება უსაფრთხოების ნორმები, მაინც არსებობს დაუცველი ხვრელები.

ელექტრონული ფოსტა (e-mail) შეიქმნა 1965 წელს. იდეა თავიდანვე იყო ინტერნეტქსელში წერილების მიღება და გაგზავნა. ამ ქსელში ხშირად მავნებლობენ, უნებართვოდ სარგებლობენ - ასეთ თარლითებს ,,სპამერებს'' უწოდებენ, ხოლო გამოგზავნილ კონტენქტს - სპამს. ცნობილმა კომპანიებმა, რომლებიც ***ელექტრონული ფოსტის*** მომსახურებას ეწევიან, შეიმუშავეს თავდაცვითი მექანიზმები - გამოგზავნილი ***სპამები*** იბლოკება ავტომატურად. შეიძლება მეილზე მოგვივიდეს სარეკლამო შეტყობინებები, ყალბი ფიშინგ ბმულები, ვირუსები და სხვა. აქ ჩნდება კითხვა: საიდან შეიძლება იცოდეს სპამის გამომგზავნმა ჩვენი ელფოსტის მისამართი? ეს მარტივია, გამომგზავნები მონაცემებს იღებენ სხვადასხვა საშუალებებით, მაგალითად, იმ ვებ-გვერდებიდან, სადაც ჩვენ ავტორიზაცია გვაქვს გავლილი - სოციალური ქსელები, ფორუმები და ა.შ. ისინი ინფორმაციას აგროვებენ,

შემდეგ კი ხშირად ელფოსტების სიას ყიდიან ***Darknet-ში*** (ამ ინტერნეტსივრცეზე ჩვენ უკვე ვისაუბრეთ).

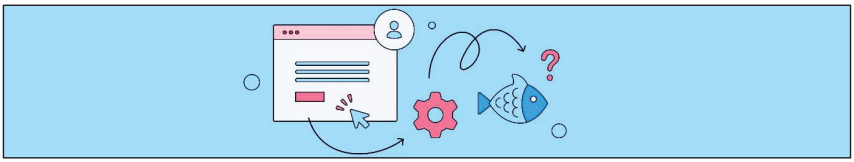
რეკომენდებული არ არის სპამების დატოვება თქვენს ელექტრონულ ფოსტაზე. პერიოდულად აუცილებელია ჩვენი ,,სპამველის'' გასუფთავება, რათა არ მოხდეს თქვენს მიერ შემთხვევით გახსნა ან გადაზიარება ვინმესთან. ამ შემთხვევაში რისკი მაღალია, რომ დავირუსდეს თქვენი კომპიუტერული თუ მობილური მოწყობილობა. ასევე შეიძლება დაზარალდეს ის, ვისაც შემთხვევით გაუგზავნით. აუცილებელია ვიცოდეთ, თუ ჩვენი ელექტრონული ფოსტა არის სამსახურის, არავითარ შემთხვევაში არ გამოვიყენოთ სოციალურ ქსელებში, ფორუმებსა და სხვა სახის ვებ-გვერდებზე რეგისტრაციისთვის.

ელექნტრონული ფოსტის დადებით მხარეებზე შეგვიძლია ბევრი ვისაუბროთ, იგი მნიშვნელოვან კომპონენტს წარმოადგენს ყველა მიმართულებით - ორგანიზაციებში, სახელმწიფო სტრუქტურებში და ა.შ.

ელფოსტა წარმოადგენს ქსელურ მომსახურებას, რომელსაც ყოველდღიურ რეჟიმში შეუძლია ინფორმაციის გაცვლა. ელფოსტის საშუალებით ოფიციალურ დონეზე ურთიერთობა ხდება სახელმწიფო სტრუქტურებსა თუ ქვეყნებსა და ორგანიზაციებს შორის. ამიტომაც, ამ მიმართულებით, როგორც უკვე აღვნიშნეთ, კიბერსაფრთხეების რისკი მაღალია - შესაძლებელია, ადვილად მოხდეს უნებართვო წვდომა, გაგზავნილი შეტყობინების შინაარსის შეცვლა და ასე შემდეგ.

21-ე საუკუნეში გვაქვს მრავალფეროვნება ელექტრონული ფოსტის მოდელების მიმართულებით - მაგალითად ***Yahoo mail-ი, Gmail-ი, Outlook mail-ი*** და სხვა. აღნიშნული მეგაკომპანიები უფასოდ გვთავაზობენ როგორც ვებ-გვერდებზე ფოსტის

შექმნას, ასევე მათ აპლიკაციებსაც, რომელსაც ვიყენებთ მობილურებსა და სხვა კომპიუტერულ მოწყობილობებზე. შესაბამისად, უმჯობესია, როგორც სხვა პროგრამები და აპლიკაციები, ფოსტის აპლიკაციაც გადმოვიწეროთ ლიცენზირებული ოფიციალური ვებ-გვერდიდან. ასე უფრო დაცული იქნება ჩვენი უსაფრთხოება.



მსოფლიო მასშტაბით პროცენტულად ყველაზე მეტად ხდება ფიშინგ თავდასხმები. როდესაც ელექტრონულ ფოსტაზე ვსაუბრობთ, აუცილებელია, კიდევ ერთხელ შევეხოთ ამ მოვლენას და უფრო დეტალურად გამოვყოთ მისი ტიპები. ფიშინგ შეტევის უამრავი მიმართულება არსებობს, ჩვენ მხოლოდ რამდენიმეს განვიხილავთ: ***Spear Phishing, Vishing, Email Phishing, Https Phishing, Pop-up Phishing, Clone Phishing, Smishing, Search Engine Phishing.***

"Spear Pishing-ი *ქართულად შეიძლება ითარგმნოს როგორც გამიზნული თაღლითობა ან მიზანში ამოღებული ინდივიდი, რომელზეც თავდამსხმელი წინასარ აგროვებს ინფორმაციას, რათა მოახდინოს აქცენტირებული თავდასხმა იმ პირადი ინფორმაციის გათვალისწინებით, რაც მან მსხვერპლის შესახებ მოიპოვა.*

Vishing *თავდასხმა ორი სიტყვის გაერთიანებას წარმოადგენს -* ***Voice Pishing,*** *რომელიც ხმოვან ფიშინგს გულისხმობს. ეს არის მობილურის საშუალებით მსხვერპლის შეცდომაში შეყვანა რომელიმე კომპანიის სახელით, თავდამსხმელის მხრიდან შეიძლება განხორციელდეს ზარი, მეტი სანდოობისთვის იყოს ხმოვანი საუბრის მცდელობა, ან ხმოვანი შეტყობინებები, რაც საბოლოო ჯამში პირადი მონაცემების მოპარვას ემსახურება.*

Email Pishing-ი *არის ელექტრონული ფოსტის თაღლითობა, როდესაც თავდამსხმელი იყენებს ელფოსტას. ამ შემთხვევაში თავდამსხმელი აგზავნის რაიმე ტექსტს, რომელიც გამიზნულია მსხვერპლის შეცდომაში შეყვანისთვის და პირადი მონაცემების მოპოვებისთვის.*

Https Phishing-ი *წარმოადგენს ყალბი ვებ-გვერდის ბმულის გაგზავნას, რომელიც ხშირად ელექტრონული ფოსტის საშუალებით იგზავნება, როდესაც თავდამსხმელი ორიგინალ ვებ-გვერდთან მიმსგავსებულ ბმულს აგზავნის, სადაც აუცილებელია ავტორიზაციის გავლა, მაგალითად, საბანკო რეკვიზიტები და სხვა.*

Pop-up Phishing-ი *არის გავრცელებული ფორმა, სხვადასხვა ვებ-გვერდებზე გვხვდება Pop-up ბანერი. ეს უფრო მეტად დამახასიათებელია სარეკლამო ბანერებისთვის, უმეტესად კი იგი წარმოადგენს ვირუსის გავრცელების წყაროს. როდესაც ჩვენ ვაწვებით აღნიშნულ ბანერს, ან გასათიშად, ან გვგონია, რომ რაიმე პროდუქციის რეკლამაა და გვინდა ვებ-გვერდზე გადასვლა, სრულად ნახვა, ზოგჯერ ჩვენს კომპიუტერულ მოწყობილობაში იწერება მავნე პროგრამა, ვირუსდება და შესაძლებელია, ბევრი მნიშვნელოვანი ფაილი თუ პროგრამა დაინფიცირდეს.*

Clone Phishing-ი *წარმოადგენს უკვე შექმნილი ორიგინალი შეტყობინების ასლს - თავდამსხმელი აკეთებს ასლს და მასში სვამს მავნე ბმულს.*

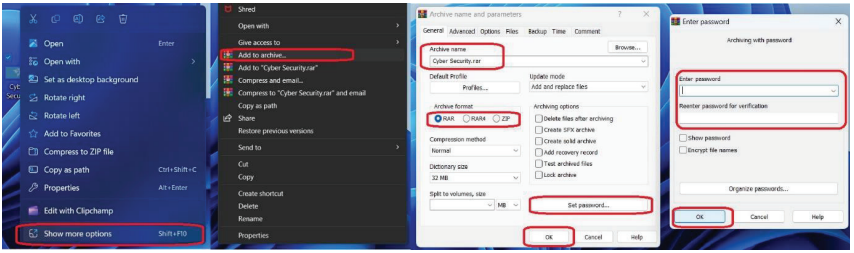
Smishing-ი *არის ორი სიტყვის ერთობლიობა -* ***Sms Pishing-ი,*** *რომელიც გულისხმობს შეტყობინების რაიმე ფორმით გამოგზავნას და ფიშინგ თავდასხმას.*

Search Engine Phishing-ი *ითარგმნება როგორც საძიებო სისტემის ფიშინგ შეტევა, თავდამსხმელი წინასწარ აკეთებს სხვადასხვა მიმზიდველი პროდუქციის ვებ-გვერდებს. როდესაც საძიებო სისტემაში ჩვენ ვეძებთ ჩვენთვის სასურველ პროდუქციას, შეიძლება უნებურად გავხდეთ თავდასხმის მსხვერპლი, გადავიდეთ საეჭვო ვებ-გვერდზე, მოგვთხოვოს ავტორიზაციის გავლა ან ონლაინ შესყიდვისთვის პირადი მონაცემები, საბანკო ანგარიშები, რომლის შევსების შემდეგ ინფორმაცია მიუვა თავდამსხმელს".*[206]

ფიშინგ თავდასხმების ტიპები, როგორც აღვნიშნეთ, ბევრია და არა მხოლოდ ფიშინგ თავდასხმების. ყველა მათგანს ვერ განვიხილავთ, მაგრამ აუცილებელია გავითვალისწინოთ ის მიდგომები რაც საჭიროა კიბერუსაფრთხოებისთვის. არავითარ შემთხვევაში არ უნდა გადავიდეთ საეჭვო და უცხო ბმულებზე. თუ საეჭვო ფაილს საეჭვო ავტორისგან მივიღებთ, არ უნდა გადმოვიწეროთ. ნუ გამოვრიცხავთ, რომ ნაცნობისგანაც მივიღოთ მიმაგრებული ფაილი. ამ შემთხვევაშიც საჭიროა დაკვირვება - ნუ გავხსნით სპამებს, ნუ შევიყვანთ პირად მონაცემებს. თუ არ მიაქცევთ

[206] *Fortinet, "19 Types of Phishing Attacks", p. 1. 2022. https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks*

ყურადღებას დეტალებს და გადაწყვეტთ პირადი დოკუმენტაციის გაგზავნას, ამ შემთხვევაში არსებობს თავის დაზღვევის რამდენიმე ვარიანტი - რეკომენდაციის სახით გირჩევთ, გაგზავნამდე ***დაარქივოთ (archive)*** გასაგზავნი ფაილი. დაარქივების დროს ჩვენ შეგვიძლია ნებისმიერ სასურველ ფაილს დავადოთ პაროლი, ეს არ წარმოადგენს სირთულეს - ფაილზე, რომელიც გვინდა, რომ დავაარქივოთ, უნდა მივიტანოთ კურსორი და დავაწვეთ მაუსის მარჯვენა ღილაკს, შემდეგ გაიხსნება ფანჯარა, სადაც დავაჭერთ - მეტი ვარიანტის ჩვენება (Show more options) → არქივში დამატება (Add to archive) → პაროლის დაყენება (Set password) → ok → არქივის ფორმატი (Archive format) | rar / rar4 / zip → ok.



სურათი 61: დაარქივება.

შემდეგ ***zip*** ან ***rar*** ფაილი შეგვიძლია ავტვირთოთ ელფოსტის გასაგზავნი შეტყობინების ველში და გადავაგზავნოთ. ასევე არსებობს ფოსტით კავშირის დროს პრივატულობის სხვადასხვა მეთოდი - ერთ-ერთ მათგანს წარმოადგენს ***Pretty Good Privacy,*** რომელიც საშუალებას გვაძლევს, ფაილები დავშიფროთ და ისე გავაგზავნოთ. ამისთვის დაგეხმარებათ პროგრამა ***Enigmail,*** რომელიც უფასოდ შეგიძლიათ გადმოიწეროთ, როგორც ***Windows-ის*** სისტემაზე, ასევე ყველა სისტემაზე, რომელზეც დაგჭირდებათ. თუმცა არსებობს სხვა მსგავსი პროგრამები და აპლიკაციებიც, რომლებიც იგივე ფუნქციას ასრულებენ.

რა საფრთხეები არსებობს სოციალურ ქსელში და როგორ დავიცვათ ჩვენი პირადი მონაცემები გასაჯაროებისგან?

ტექნოლოგიების გაუმჯობესებასთან ერთად შეიცვალა ადამიანების ურთიერთობები, 21-ე საუკუნეში გვაქვს საშუალება, ერთი კონტინენტიდან მეორე კონტინენტზე ონლაინ რეჟიმში დავამყაროთ კავშირი და გადავჭრათ უამრავი საკითხი, ამას ჩვენ ვახერხებთ ინტერნეტის საშუალებით, მაგრამ ამაში გვეხმარება ისეთი სოციალური ვებ-გვერდები და აპლიკაციები, როგორებიცაა „ფეისბუქი“, „ინსტაგრამი“, „ტვიტერი“ და სხვა.

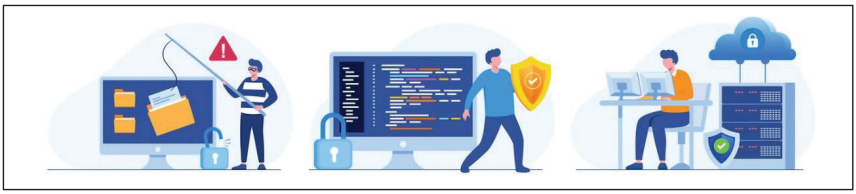
ქართულ სინამდვილეში ერთ-ერთ მოწინავე პოზიციას სოციალური ქსელი „ფესიბუქი“ იკავებს, სადაც შეგვიძლია პროფილის შექმნა, პირადი ინფორმაციის მითითება, სურათის ატვირთვა, მიმდინარე ინფორმაციის გაზიარება და ასე შემდეგ.

ამ შემთხვევაში რამდენად ვართ დაცულები? რა თქმა უნდა, დაცულები არ ვართ, თუ ჩვენ რამეს ვაკეთებთ სოციალურ ქსელში, ეს არის საჯარო. იმ შემთხვევაში, თუ ჩვენ არ გვაქვს დახურული პროფილი (პროფილის დახურვა ყველა სოციალურ ქსელში შეგვიძლია), ამცირებს რისკებს, მაგრამ სრულად არ ქმნის ჩვენს უსაფრთხო კიბერგარემოს.

სოციალურ ქსელებთან მიმართებაში აუცილებელია ისევე დავიცვათ კიბერჰიგიენა, როგორც ამას ელექტრონულ ფოსტასთან მიმართებაში ვაკეთებთ. სოციალურ ქსელებში ხშირად ვრცელდება ვირუსის შემცველი სხვადასხვა ბმულები,

შეიძლება პირადი შეტყობინების სახითაც მოგივიდეთ. არავითარ შემთხვევაში არ უნდა გახსნათ საეჭვო ბმულები. ამ შემთხვევაშიც საკვანძო საკითხს წარმოადგენს პაროლი. არ უნდა გვქონდეს სუსტი პაროლი, უმჯობესია, გამოვიყენოთ ორბიჯიანი ან სამბიჯიანი პაროლები, რაზეც უკვე ვისაუბრეთ ერთ-ერთ თავში - იხილეთ „კიბერჰიგიენის დაცვა - გზამკვლევი“.

რა არის ინფორმაციული უსაფრთხოება? - განმარტებები და სტანდარტები



როდესაც კიბერსივრცეზე ვსაუბრობთ, ასევე ვახსენებთ ინფორმაციულ უსაფრთხოებას, რაც განმარტებას საჭიროებს - ეს არ არის მხოლოდ კიბერუსაფრთხოების ერთ-ერთი განშტოება, იგი არსებობს არავირტუალური სახითაც.

ინფორმაციის უსაფრთხოების მართვის სისტემა (ISMS) ცალკე სფეროა და იქამდე განისაზღვრა, სანამ კომპიუტერი და ვირტუალური სამყარო გაჩნდებოდა. კონკრეტულად, რას ნიშნავს ინფორმაციული უსაფრთხოება? ეს არის ინფორმაციის დაცვის სტრატეგია, მექანიზმები, რომელიც ძალზე მრავალფეროვანია მსოფლიო მასშტაბით - არსებობს სხვადასხვა სტანდარტები და მიდგომები. ჩვენ ვერ გავიგებთ ინფორმაციული უსაფრთხოების არსს, თუ არ ავხსენით, რა არის ინფორმაცია. ეს გახლავთ მონაცემები, ბეჭდური თუ არაბეჭდური ვირტუალური სახით, სურათები, ვიდეო და აუდიო მასალები და სხვა. შესაბამისად, ამ მასალების დაცვა

მნიშვნელოვანი საკითხია, რათა არ დავზარალდეთ. ამ კუთხით შეიძლება ,,ბოროტმა'' ჰაკერებმა უამრავი მავნებლობა ჩაიდინონ, მათ შორის ჩვენი სახელით.

ინფორმაციულ უსაფრთხოებას ხშირად ექსპერტები შემოკლებით ***InfoSec-ით*** აღნიშნავენ. იგი შეიცავს ინსტრუმენტებსა და პროცესებს, რომლებსაც ორგანიზაციები იყენებენ ინფორმაციის დასაცავად. ასევე შეიცავს პოლიტიკის პარამეტრებს, რაც ხელს უშლის არაავტორიზებული ადამიანების წვდომას პირად ინფორმაციაზე, არ აქვს მნიშვნელობა, ეს იქნება ორგანიზაციის ინფორმაცია თუ პირადი მონაცემები. ამ შემთხვევაში უპირველესია ქსელისა და ინფრასტრუქტურის უსაფრთხოება, ტექსტირება და აუდიტი.

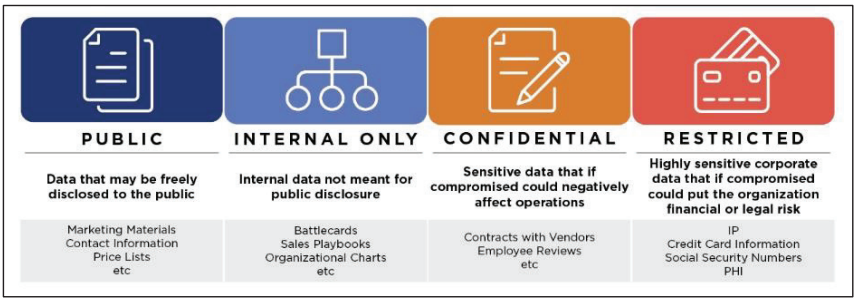
ინფორმაციული უსაფრთხოების მიზანია, სენსიტიური ინფორმაცია დაიცვას არაავტორიზებული წვდომისგან, გადაწერისგან, შეფერხებისა და განადგურებისგან. აუცილებელია, უზრუნველყოს ისეთი კრიტიკული მონაცემების უსაფრთხოება და კონფიდენციალურობა, როგორიცაა პიროვნების პირადი მონაცემები, ფინანსური, ანგარიშის დეტალები, ინტელექტუალური საკუთრება და სხვა.

თუ არ იქნება ინფორმაციული უსაფრთხოება დაცული, ამის საპასუხო შედეგი იქნება პირადი ინფორმაციის ქურდობა, მონაცემთა გაყალბება, წაშლა და სხვა. ასეთმა თავდასხმებმა შეიძლება შეაფერხოს სამუშაო პროცესი, ფინანსური ზიანი მიადგეს კომპანიას და შეელახოს რეპუტაცია.

ISO International Organization for Standardization

ინფორმაციული უსაფრთხოების სტანდარტებს, კლასიფიკაციასა და მიდგომებს განსაზღვრავს ***საერთაშორისო სტანდარტიზაციის ორგანიზაცია (ISO),*** რა თქმა უნდა, მსოფლიო მასშტაბით მხოლოდ ეს ორგანიზაცია არ არის ჰეგემონი ამ მიმართულებით, მაგრამ როგორც ევროკავშირი, ასევე ნატო და ის წამყვანი ქვეყნები, რომლებიც თავად ადგენენ თავიანთ ტერიტორიაზე ინფორმაციული უსაფრთხოების სტანდარტებს, თანამშრომლობენ საერთაშორისო სტანდარტიზაციის ორგანიზაციასთან. ეს ორგანიზაცია ინფორმაციული უსაფრთხოების სტანდარტს აღნიშნავს ***ISO 27001-ით.*** იგი ახდენს კლასიფიკაციას, რაც არის პროცესი, როდესაც ორგანიზაციები ფასდება, რა დონეზე აქვთ დაცული მონაცემები. აღნიშნული სისტემა შეიცავს კონფიდენციალურობის ოთხ დონეს:

- ***"კონფიდენციალური (Confidential)*** *- წვდომა აქვს მხოლოდ მაღალ ხელმძღვანელობას;*
- ***შეზღუდული (Restricted)*** *- თანამშრომლების უმეტესობას აქვს წვდომა;*
- ***შიდა (Internal)*** *- ყველა თანამშრომელს აქვს წვდომა;*
- ***საჯარო (Public)*** *- ყველას აქვს წვდომა".*[207]

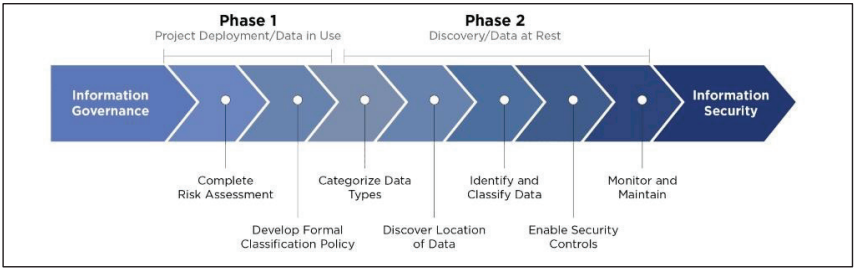


ფიგურა 4: კომფიდენციალურობის ოთხი დონე. *წყარო: https://edge.siriuscom.com/security/7-steps-to-effective-data-classification*

აღნიშნული კლასიფიკაციის მიხედვით, ორგანიზაციაში განაწილებული უნდა იყოს თანამშრომლებზე სხვადასხვაგვარი წვდომა. მაგალითისთვის ავიღოთ ორგანიზაცია, რომელიც ემსახურება საზოგადოებას სამედიცინო სფეროში. ამ შემთხვევაში ექიმს ხელი მიუწვდება პაციენტის პირად მონაცემებზე, მაგრამ ხელი არ უნდა მიუწვდეობდეს ფინანსურ ჩანაწერებზე ან სხვა სახის სენსიტიურ ინფორმაციაზე.

გამოყოფენ ასევე 7 ნაბიჯს მონაცემთა ეფექტური კლასიფიკაციისთვის, რომელიც ასევე ეფექტური ინფორმაციის დაცვას გულისხმობს:

[207] *Irwin L., "What is ISO 27001 Information Classification?", ITgovernance, 2022. https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001#:~:text=What%20is%20ISO%2027001%20Information%20Classification%3F&text=Information%20classification%20is%20a%20process,granted%20access%20to%20view%20it.*



ფიგურა 5: მონაცემთა ეფექტური კლასიფიკაციის 7 ნაბიჯი. *წყარო: https://edge.siriuscom.com/security/7-steps-to-effective-data-classification*

1. "სრული სენსიტიური მონაცემების რისკის შეფასება (Complete a risk assessment of sensitive data)

განსაზღვრეთ თქვენი მონაცემთა კლასიფიკაციის მიზნები გასაუბრებაზე დაყრდნობით, რომელიც მოიცავს ძირითად დაინტერესებულ მხარეებს, მათ შორის, იურიდიულ და ბიზნესერთეულების ლიდერების ჩათვლით.

2. ფორმალური კლასიფიკაციის პოლიტიკის შემუშავება (Develop a formalized classification policy)

*"აღნიშნული პოლიტიკა უნდა იყოს დაფუძნებული პრინციპებზე, ამ შეხვედრებში სხვადასხვა ექსპერტებისგან და ორგანიზაციებისგან, შეიძლება სხვადასხვა განსაზღვრებები შეგხვდეთ, მაგრამ საერთო ჯამში არსებობს სამი ძირითადი პრინციპი, რასაც ხშირად **CIA Triad-ს** უწოდებენ, ქართულად ჟღერს როგორც **„სი აი ეი ტრიადა":***

- ***კონფიდენციალურობა (Confidentiality)***

აღნიშნული ზომები საჭიროა მიიღოთ იმისთვის, რომ ინფორმაციის არაავტორიზებული წვდომა აირიდოთ თავიდან. ამ პრინციპის მიზანია პერსონალური ინფორმაციის კონფიდენციალურობის შენარჩუნება და იმის უზრუნველყოფა, რომ ის ხილული და ხელმისაწვდომი იყოს მხოლოდ იმ პირებისთვის, რომლებსაც სჭირდებათ ორგანიზაციული საქმიანობისთვის.

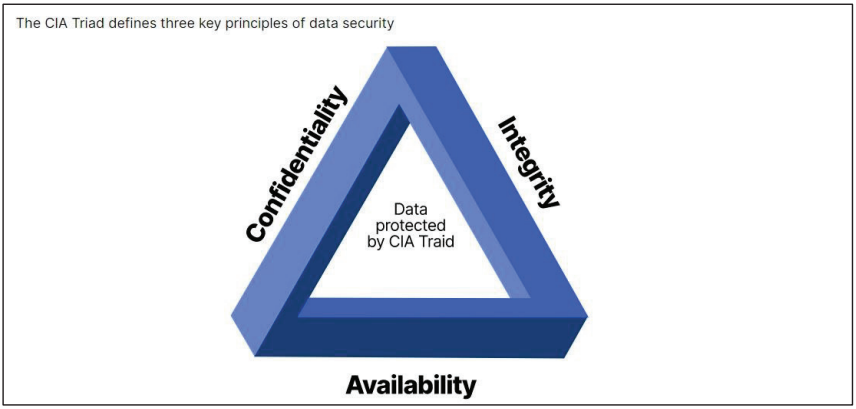
- ***მთლიანობა (Integrity)***

პრინციპი მოიცავს დაცვას მონაცემების არაავტორიზებული ცვლილებებისგან (დამატებები, წაშლა და სხვა.) მთლიანობის პრინციპი უზრუნველყოფს მონაცემების სიზუსტეს და სანდოობას.

- ***ხელმისაწვდომობა (Availability)***

პრინციპი გულისხმობს, გახადოს პროგრამული სისტემები და მონაცემები სრულად ხელმისაწვდომი, მომხმარებლების საჭიროების მიზნით. ხელმისაწვდომობის პრინციპის მიზანია ტექნოლოგიური

ინფრასტრუქტურის, აპლიკაციებისა და მონაცემების ხელმისაწვდომობა, როდესაც ისინი საჭიროა ორგანიზაციული პროცესისთვის ან ორგანიზაციის მომხმარებლებისთვის".[208]



ფიგურა 6: CIA Triad განსაზღვრავს მონაცემთა უსაფრთხოების სამ ძირითად პრინციპს. *წყარო: https://www.imperva.com/learn/data-security/information-security-infosec/*

3. "მონაცემთა ტიპების კატეგორიზაცია (Categorize the types of data)

ბევრი ორგანიზაციის მფლობელისთვის გამოწვევას წარმოადგენს თუ რა სახის სენსიტიური მონაცემები არსებობს მის ორგანიზაციაში, მაგრამ აუცილებლად უნდა გაწიოს ორგანიზაციამ აღნიშნული ძალისხმევა, რათა დადგინდეს, თუ რა სახის ინფორმაციასთან აქვს საქმე, რის შედეგადაც შეშუშავდება ინფორმაციული უსაფრთხოების სტრატეგია. ორგანიზაცია დეტალურად უნდა სცემდეს შემდეგ კითხვებზე პასუხს:

კლიენტებისა და პარტნიორების რა მონაცემებს აგროვებს თქვენი ორგანიზაცია?
რა მონაცემებს ქმნის მათ შესახებ?
რა საკუთრების მონაცემებს ქმნით?
რა ტრანზაქციის მონაცემებთან გაქვთ საქმე?
რა არის კონფიდენციალური და რა არა ყველა შეგროვებული, შექმნილი მონაცემიდან?

4. იპოვეთ (აღმოაჩინეთ) თქვენი მონაცემების მდებარეობა (Discover the location of your data)

*თქვენს ორგანიზაციაში მონაცემების ტიპების დადგენის შემდეგ, მნიშვნელოვანია ელექტრონული კატალოგის ყველა ადგილის აღმოჩენა, სადაც მონაცემები ინახება. მონაცემთა ნაკადი ორგანიზაციის შიგნით და გარეთ არის მთავარი. როგორ ინახავს და აზიარებს თქვენი ორგანიზაცია მონაცემებს შიგნით და გარეთ? იყენებთ ე.წ. შეხსიერების ონლაინ ღრუბლებს? (როგორიცაა **OneDrive, Dropbox** და სხვა).*

[208] *Imperva, "Information Security: The Ultimate Guide", 2022. https://www.imperva.com/learn/data-security/information-security-infosec/*

იყენებთ ორგანიზაციაში საქმიანობისთვის მობილურ მოწყობილობებს? აღნიშნული მიდგომა დაგეხმარებათ არასტრუქტურირებული მონაცემების ინვენტარის დაგეგმარებაში და იმის აღმოჩენაში, თუ სად ინახება თქვენი კომპანიის სრული მონაცემები. ამ მცდელობებში შეგიძლიათ გამოიყენოთ საკვანძო სიტყვები, მონაცემთა კონკრეტული ტიპები ან ფორმატები, მაგალითად: სამედიცინო ჩანაწერის ნომრები, სოციალური უსაფრთხოების ნომრები, საკრედიტო ბარათების ნომრები და სხვა.

5. მონაცემების იდენტიფიცირება და კლასიფიკაცია (Identify and classify data)

მას შემდეგ, რაც გაიგებთ, სად ინახება თქვენი მონაცემები, შეგიძლიათ ამის შემდეგ იდენტიფიცირება და კლასიფიცირება მოახდინოთ იმიტომ, რომ შემდეგ შესაძლებელი იყოს მათი დაცვა. თქვენ შეგიძლიათ, ორგანიზაციაში დანერგოთ ჯარიმების რეჟიმი, ანუ დაკარგულ ინფორმაციაზე შემოიღოთ ფინანსური გადასხადი.

6. კონტროლის ჩართვა (Enable controls)

აუცილებელია კონტროლის მექანიზმების ჩამოყალიბება, საბაზისო კიბერუსაფრთხოების ზომების მიღება და პოლიტიკის განსაზღვრა თითოეული მონაცემის კლასიფიკაციის მიხედვით. ეს გაგიადვილებთ, უზრუნველყოთ შესაბამისი გადაწყვეტილებები. მაღალი რისკის მქონე მონაცემები მოითხოვს დაცვის მაღალ დონეს, ხოლო ლოგიკურად დაბალი რისკის მქონე მონაცემებს ნაკლები დაცვა სჭირდება. თქვენ მონაცემების დონის მიხედვით შეგიძლიათ განახორციელოთ უსაფრთხოების შესაბამისი კონტროლი.

7. მონიტორინგი და შენარჩუნება (Monitor and maintain)

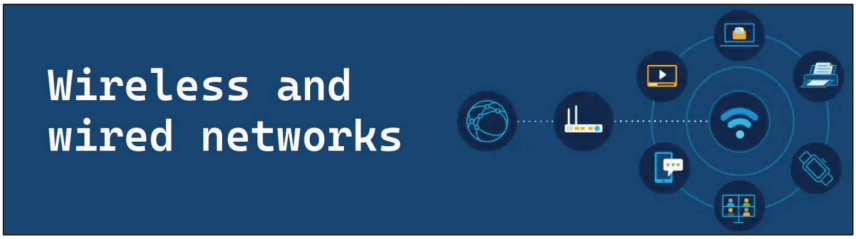
ყოველთვის მზად იყავით ორგანიზაციის მონაცემთა კლასიფიკაციის სისტემების მონიტორინგისთვის და მათ შესანარჩუნებლად. კლასიფიკაციის ჰოლიტიკა უნდა იყოს დინამიური. აღნიშნული უნდა იყოს ხშირად განხილვადი და განახლებადი, რომელიც ძირითადად მოიცავს, მომხმარებლებს, თუ თქვენი სისტემები იქნება დაცული და ხშირად განახლებადი, ნდობის ხარისხი მომხმარებლებში იქნება მაღალი".[209]

ხშირ შემთხვევაში ორგანიზაციები თავს არიდებენ სრული კლასიფიკაციის ჩამოყალიბებას და უსაფრთხოების ნორმების დაცვას, რადგან აღნიშნული საკითხი წარმოადგენს ძვირადღირებულს და არის შრომატევადი, რომელსაც სჭირდება კონტროლი და მზად ყოფნა. არადა, კარგი დაცვისა და ინფორმაციის შენახვის პოლიტიკა დაგეხმარებათ მონაცემთა ნაკრების შემცირებაში.

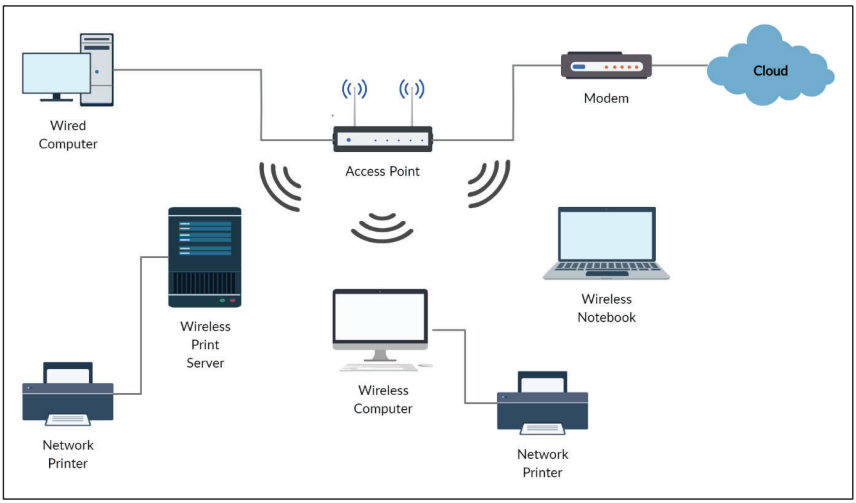
ჩვენ უკვე აღვნიშნეთ, რომ ინფორმაციული უსაფრთხოება არის ძალიან ფართო სფერო, რომელსაც ასევე ფართო რისკები ახასიათებს და ხშირ შემთხვევაში ეს უცოდინრობით არის გამოწვეული.

[209] *Eck T., "7 Steps to Effective Data Classification", Sirius Edge, 2019. https://edge.siriuscom.com/security/7-steps-to-effective-data-classification*

რა სახის ქსელები არსებობს მსოფლიო მასშტაბით და რას ნიშნავს უსადენო ქსელი?



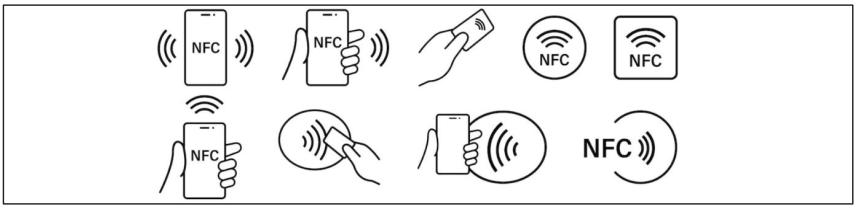
რა სახის ქსელები არსებობს მსოფლიო მასშტაბით? ასეთი კითხვა შეიძლება ყველა ჩვენთაგანს გაუჩნდეს - საინტერესოა, როგორია მათი მუშაობის პრინციპი? მსოფლიო მასშტაბით გვაქვს როგორც სადენიანი, ასევე უსადენო ქსელები ***(Wireless and wired networks)***, როდესაც სიხშირით ვაკავშირებთ მოწყობილობას ინტერნეტთან ან რამე ქსელთან. უსადენო ქსელებში შედის ყველასთვის ცნობილი ***ბლუთუზი (Bluetooth), ვაიფაი (Wifi), ენ ეფ სი (NFC), ინფრარედი (IR).*** ბლუთუზის გამოყენება ხშირად ხდება, როდესაც ერთ მოწყობილობას ვაკავშირებთ მეორესთან. მაგალითად, შეგვიძლია, სმარტფონი დავუკავშიროთ მანქანაში ჩამონტაჟებულ მოწყობილობას და მობილურიდან ვმართოთ მუსიკალური რეჟიმი, მანქანიდან ვუპასუხოთ ზარებს და დავრეკოთ.



სურათი 62: როგორ მუშაობს სადენიანი და უსადენო ქსელები. *წყარო:*

https://www.pinterest.com/pin/464011567858877829/

რაც შეეხება ვაიფაის, მასზე მოთხოვნილება ყოველდღიურად იზრდება - დაწესებულებები, რომლებიც ემსახურებიან საზოგადოებას, თითქმის ყველგან ხელმისაწვდომია უსადენო ინტერნეტთან წვდომა. გლობალური ინტერნეტიზაციის პირობებში ხელმისაწვდომია ქუჩაშიც კი. ვაიფაის ადაპტერის დაცვა უმეტესწილად ხდება პაროლის დადებით - მაგალითად, როდესაც რესტორანში მივდივართ, იქაც ვარკვევთ, რა პაროლი უდევთ ვაიფაის სიხშირეზე, რათა გვქონდეს ინტერნეტთან წვდომა. ეს ხდება იქიდან გამომდინარე, რომ ,,ბოროტმა ჰაკერებმა'' ვერ შეძლონ ვაიფაიზე მარტივად თავდასხმა და სიხშირის მავნებლური მიზნებისთვის გამოყენება. პაროლი ხშირად ვერ ახდენს ქსელის დაცვას. ასევე რისკს წარმოადგენს ისიც, რომ ,,ბოროტი ჰაკერები'' ხანდახან თვითონ ქმნიან ღია, უპაროლო ვაიფაის, სადაც შეიძლება ცდუნდეთ და უბრალოდ დააკავშიროთ თქვენი კომპიუტერული მოწყობილობა ან მობილური ტელეფონი, რის შემდეგაც თქვენ ხდებით მსხვერპლი, თქვენი მოწყობილობა და ინფორმაცია ამ შემთხვევაში იქნება დაუცველი ისე, რომ შეიძლება ვერაფერს მიხვდეთ.



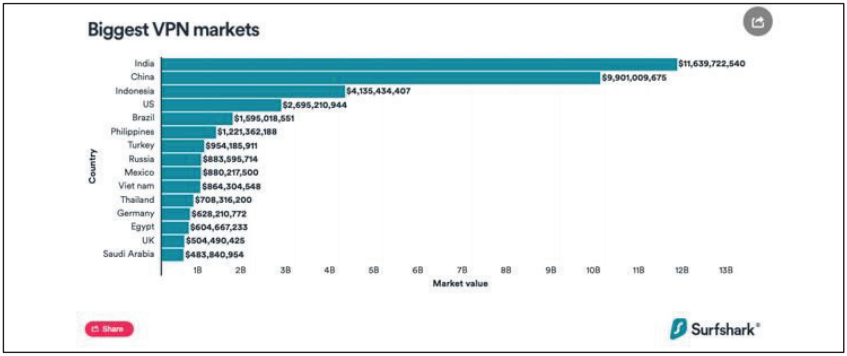
ჩვენ ასევე ვახსენეთ ***NFC*** და ***IR*** ტექნოლოგია, რომელიც ინტენსიურად გამოიყენება დღევანდელ რეალობაში. ***NFC*** ტექნოლოგია მეტწილად გამოიყენება ბარათებთან მიმართებაში, ხოლო ***IR*** არის ტექნოლოგია, რომელიც სატელეკომუნიკაციო მოწყობილობებშია ჩამონტაჟებული, რაც საშუალებას იძლევა, მობილურით ვმართოთ სხვადასხვა მოწყობილობები.

რაც შეეხება უსაფრთხოებას, ისინი არ არიან დაცული უნებართვო წვდომისაგან. უნდა შევეცადოთ, მაქსიმაურად მოვახდინოთ ჩვენი ტექნოლოგიური მოწყობილობების განახლება, არ გავცეთ პირადი ინფორმაცია, არც კი ვცადოთ არასანდო ქსელებთან დაკავშირება, დავაყენოთ რთული პაროლები.

რა არის VPN, რატომ შეიქმნა და რა ფუნქცია აკისრია მას?

VPN-ი წარმოადგენს აქტუალურ ქსელს, რომელსაც მსოფლიო მასშტაბით უბრალო ადამიანიდან დაწყებული, ,,ბოროტი ჰაკერით'' დამთავრებული, იყენებს. ***VPN-ი*** შექმნა ტექნოლოგიური მოწყობილობების მწარმოებელმა მეგა კომპანია ***Cisco-მ.*** დღეს ინტერნეტსივრცეში უამრავი სახის ***VPN*** პროგრამას შეხვდებით. რაც შეეხება ზოგადად ამ ქსელს, მისი უპირველესი მიზანი იყო დისტანციური კავშირი მომხდარიყო დახურულ ქსელში. მარტივად, რომ ვთქვათ, თანამშრომლები, რომლებიც არ მუშაობდნენ ოფისში, შეძლებოდათ თავიანთი სამსახურის ქსელთან დაკავშირება. დღეს ***VPN-ის*** ტექნოლოგიას სხვა უამრავი დანიშნულებითაც იყენებენ - მაგალითად, რუსეთში ***VPN-ის*** მომხმარებელთა რაოდენობამ მოიმატა მას შემდეგ, რაც კომპანია ***„მეტა“-მ*** შეზღუდა თავის აპლიკაციებზე და ვებ-გვერდებზე წვდომა. ***VPN-ის*** საშუალებით ხდება რეგიონის ცვლილება ციფრულ დონეზე, რის მეშვეობითაც რუსეთის მოქალაქეები მაინც სარგებლობენ აღნიშნული სოციალური ქსელებით. ეს ტექნოლოგია გვეხმარება უსაფრთხო კავშირში სხვა ქსელებთან - ჩვენ შეგვიძლია, ***VPN*** გამოვიყენოთ უსაფრთხო კავშირისთვის. აღსანიშნავია, რომ არის ქვეყნები, სადაც ***VPN-ის*** გამოყენება იზღუდება ან სრულად არის აკრძალული. *“დედამიწაზე დაახლოებით 8 მილიარდი ადამიანი ცხოვრობს, ხოლო 5 მილიარდზე მეტი მომხმარებელი იყენებს ინტერნეტს, აქედან 2022 წელისთვის* ***VPN-ს*** *დაახლოებით*

*1.2 მილიარდი ადამიანი იყენებს". **VPN-ის** მომხმარებელთა ყველაზე დიდი რაოდენობა ინდოეთიდან 45 პროცენტი, ხოლო ინფონეზიიდან 42 პროცენტია".*[210]



ცხრილი 6: ყველაზე დიდი VPN-ის მომხმარებელი ქვეყნები. *წყარო: https://www.websiterating.com/*

"2027 წლისთვის VPN-ის ბაზარი, სავარაუდოდ, 107,5 მილიარდ დოლარს მიაღწევს".[211]

[210] *Ahlgren M., "How Many People Use a VPN? (Usage Statistics for 2022)", Websiterating, p. 1, 2022. https://www.websiterating.com/*
[211] *Carter R., "The Ultimate List of VPN Statistics for 2023", Findstack, p. 1, 2021. https://findstack.com/resources/vpn-statistics/*

დასკვნა

ფაქტია, ინტერნეტსივრცის წარმოშობამ და შემდეგ კიბერსაფრთხეების გაჩენამ რადიკალურად შეცვალა კაცობრიობის ცნობიერება. მეტიც, მთელ რიგ საკითხებთან დაკავშირებით შეიცვალა როგორც მიდგომები და ფორმები, ასევე შინაარსი. ინტერნეტსისტემებზე აიგო უამრავი დარგი, ეკონომიკური მიმართულებები, სამხედრო ინდუსტრია და როგორც ზემოთ აღვნიშნეთ, დაიწყო განსხვავებული ომების ეპოქა - ირეალური ისე შეერწყა რეალურს, უკვე ჭირს განსხვავება და იმის გამორჩევა, რომელი უფრო დგას წინა პლანზე, რომლით იწყება და რომლით მთავრდება.

ნატო, ევროკავშირი, ამერიკის შეერთებული შტატები - გავლენიანი ქვეყნები და მნიშვნელოვანი ორგანიზაციები თავიანთ დღის წესრიგს უკვე იმაზე აგებენ, როგორ მოიგერიონ და დააბალანსონ საკუთარი თუ საერთაშორისო კიბერსივრცეები, როგორ გაუწიონ წინააღმდეგობა დაუმორჩილებელ სახელმწიფოებს, რომლებიც შემჩნეულნი არიან კიბერმეკობრეობასა და კიბერთავდასხმებში. სამწუხაროდ, რამდენიმე მრავალრიცხოვანმა ქვეყანამ მსგავსი ქმედებები ერთ-ერთ პრიორიტეტად გაიხადა და საკუთარი მიმართულებები სწორედ ინტერნეტსივრცის თავისებურ გადანაწილებაზე ააგო.

თავდაცვა და დამნაშავეების გამოვლენა, კიბერტერორიზმის გაუვნებელყოფა, განეიტრალება - დღეს ეს საკითხები იქცა მთავარ გამოწვევებად კაცობრიობისთვის. რომ არა ევროკავშირის, ამერიკის შეერთებული შტატებისა და ნატო-ს თავდადება, რუსეთი და მისი სატელიტი სახელმწიფოები მეტასტაზებივით მოედებოდნენ მთელ ინტერნეტსივრცეს და უპირობოდ მოინდომებდნენ მის გაკონტროლებას.

როდესაც ვსაუბრობთ კიბერსივრცეში წარმოშობილ პრობლემებსა და საფრთხეებზე, ისე ნუ გავიგებთ, თითქოს ამ სფეროს სასიკეთო არაფერი გააჩნია - პირიქით, ეს გახლავთ არნახული პროგრესი და რევოლუციური ნახტომი ტექნოლოგიური მიღწევების თვალსაზრისით. მსგავსი ტექნოლოგიური რევოლუცია, როგორიც მე-20 საუკუნის ბოლოს და 21-ე საუკუნის დასაწყისში მოხდა, ვფიქრობთ, მსოფლიო ისტორიას არ ახსოვს. რა თქმა უნდა, გავა წლები, საუკუნეები, იქნება უფრო მეტი მიღწევები, მაგრამ ფაქტია, ამ ეტაპზე საფუძველი ჩაეყარა რაღაც ისეთს, რაც უახლოეს ხანში აუცილებლად გამოიწვევს არნახულ სიკეთეს, არნახულ აფეთქებას

ტექნოლოგიურ სფეროში. ბუნებრივია, სადაც არის სიკეთე და წინსვლა, იქვე ჩნდება ბოროტება და პრობლემა. ის, რომ დღეს კიბერდანაშაული სტატისტიკური თვალსაზრისით მკვეთრად არის გაზრდილი, ეს განპირობებულია ჩვენი მოსახლეობის ცნობიერების დაბალი დონით. ვგულისხმობთ ცნობიერების დაბალ დონეს ამ სფეროში, თორემ საერთო ჯამში საქართველო ყოველთვის განათლებულ სახელმწიფოდ ითვლებოდა და ითვლება. სწორედ ჩვენი წიგნი დაგეხმარებათ იმ ელექტრონულ და მათ შორის რეალურ ლაბირინთებში გზამკვლევად, სადაც დღეს ცხოვრობს და მოღვაწეობს მთელი კაცობრიობა.

სადაც ბოროტებას ვახსენებთ, აუცილებლად იქვე უნდა ვახსენოთ რუსეთის ფედერაცია, დღეს მისი ხელისუფლება ხშირად ახსენებს ბირთვულ იარაღს. ყველამ ვიცით, რომ ეს იქნება სრული კატასტროფა კაცობრიობისთვის. არ არის გამორიცხული, ამ შემთხვევაშიც მხოლოდ შეშინების მიზნით წამოწყებულ პროპაგანდასთან გვქონდეს საქმე, მაგრამ ვიცით რა, რუსეთის ხასიათი და ბუნება, ვერ ვენდობით, კრემლი ნამდვილად არის ამაზე წამსვლელი. ამიტომ მთელი მსოფლიო ვალდებულია, წინ აღუდგეს რუსულ აგრესიას - ნატომ, ევროკავშირმა, ამერიკის შეერთებულმა შტატებმა უნდა შეიმუშაონ ეფექტური პროგრამები, სადაც დეტალურად იქნება გაწერილი უკრაინის დახმარება. ფაქტობრივად, ყველა წამყვანმა ქვეყანამ თავისი გადამწყვეტი სიტყვა უნდა თქვას და ეს საქმითაც გამოხატოს.

ჩვენ არ ვიცით, ომი კიდევ რამდენ ხანს გაგრძელდება. მართალია, უკრაინას ინტენსიურად ეხმარებიან მოწინავე ქვეყნები, მაგრამ ანალიტიკოსების მტკიცებით, ეს საკმარისი არ არის. რაც ხდება რეალური ომის პირობებში, თითქმის იგივე ხდება ვირტუალური ომის პირობებში, ანუ ინტერნეტსივრცეში, რაც აღნიშნულ წიგნში ფართოდ გავაანალიზეთ და განვიხილეთ. ამ ორი მოვლენის განხილვა განყენებულად შეუძლებელია. უკრაინას სჭირდება უახლესი ტექნოლოგიებით აღჭურვილი თავდაცვითი სიეტემები არა მხოლოდ იარაღის სახით, არამედ კიბერუსაფრთხოების თვალსაზრისით. თუ ვინმე ამ საკითხს ზერელედ უყურებს, ის ცდება, როგორც უკვე ზევით განვმარტეთ და ბევრი მაგალითებიც მოვიყვანეთ, კიბერსივრცის დაპყრობას შეუძლია, მწყობრიდან გამოიყვანოს მნიშვნელოვანი ინფრასტრუქტურა და საომარი ბაზებიც კი. საჭიროა დიდი ყურადღება, აღჭურვა, დაკვირვება, შესწავლა და მოქმედება.

როგორც ვთქვით, ზუსტად ვერავინ იტყვის, როდის დასრულდება რუსეთ-უკრაინის ომი, მაგრამ არსებობს რამდენიმე შესაძლო სცენარი, როგორი შედეგით შეიძლება დასრულდეს მოლაპარაკებები, რომელსაც ალტერნატივა არ გააჩნია. ყველაფერს, რომ თავი დავანებოთ, ეს არის საშუალება, რომელმაც უნდა შეაჩეროს საშინელება, რომელიც 21-ე საუკუნეში არა მარტო უკრაინას და მის ხალხს, არამედ მთლიანად მსოფლიოს დაატყდა თავს.

და მაინც, საზოგადოების გარკვეულ წრეებში აქტიურად დაობენ იმაზე, ვინ მოიგებს ომს? ამ კითხვაზე პასუხის გასაცემად, ილუზიებს, მკითხაობას და ჩვენ პირად სურვილებს არათუ დროებით, არამედ საერთოდ თავი უნდა დავანებოთ, და შევეცადოთ, ცოტა რეალურად შევხედოთ სიტუაციას. ვინ იქნება გამარჯვებული, ფაქტობრივად იგივეა, რომ ვთქვათ - ის, ვინც არ იქნება დამარცხებული. სწორედ აქ მივადექით საკითხს, რომ ერთია - ვინ რას ელოდებოდა ან ელის ამ ომიდან, მეორეა - ვინ რას მიიღებს საბოლოოდ. ამ ომში, შესაძლოა, თავიდან არ ჩანდა, მაგრამ უკვე ბევრი ზოგი პასიური და ზოგი აქტიური აქტორი გამოიკვეთა. მით, უფრო, ვხედავთ, რუსეთ-უკრაინის ომი, ნელ ნელა გადაიქცა დასავლეთისა და რუსეთის შეიარაღებულ დაპირისპირებად, რომლის საბრძოლო მოქმედებები უკრაინის ტერიტორიაზე მიმდინარეობს. შესაბამისად, ომის რაღაც ეტაპზე მინიმუმ შეჩერება (ან „გაყინულ კონფლიქტად“ გადაქცევა) და მაქსიმუმ დამთავრებაც, როგორც არაერთხელ ვთქვით, სწორედ ამ აქტორების პოლიტიკურ ნებაზეა მეტწილად დამოკიდებული. ოღონდ არ დაგვავიწყდეს, ამ პოლიტიკურ ნებას უმთავრესი რამ უნდა უძღვოდეს წინ: არც ერთ აქტორს არ უნდა, გამოჩნდეს დამარცხებული, მეტიც, პირველ რიგში თავის მოქალაქეებთან, ასევე საერთაშორისო საზოგადოებასთან უნდა თქვან, რომ მათ მიზანს მიაღწიეს. წინააღმდეგ შემთხვევაში, ამ ქვეყნების თუ ორგანიზაციების ლიდერებს პოლიტიკური კრახი გარანტირებული ექნებათ. ვნახოთ, სადამდე გაგრძელდება საბრძოლო მოქმედებები, ვის უმტყუნებს ნერვები პირველად, ან ვის გაეხსნება გონება და იტყვის, რომ უკვე გაჩერების დროა, ესეც სავარაუდოდ, მალე გამოჩნდება. მანამდე კი... ყოველდღიურად ხალხი იღუპება, აქტორების რაოდენობა იზრდება. იმედია, საღი პოლიტიკური ნებაც გამოჩნდება, მაგრამ ასეთ მდგომარეობაში კიდევ ერთ დიდ პრობლემასთან გვაქვს საქმე - ინფორმაციის ნაკლებობა, ევროატლანტიკური ღირებულებების არასაკმარისი პროპაგანდა მართლაც სამწუხაროდ არაორაზროვან და ფუჭ შეხედეულებებს ქმნის.

აქვე აღსანიშნავია, რომ ევროპაში მასობრივი განადგურების იარაღის სამი ტიპია განთავსებული: ბირთვული, ბიოლოგიური და ქიმიური. ნატომ შეძლო და ღიად კონფლიქტში არ ჩაერთო. მისი ალიანსის საზღვრები ხელშეუხებელია, რუსეთმა ეს იცის და წევრმა ქვეყნებმაც იციან, მათ აქვთ ძალიან სერიოზული თავდაცვითი და უსაფრთხოების ფარი: მის წინააღმდეგ გამოსაყენებელი ერთადერთი იარაღია ბირთვული იარაღი. როგორც ნატოს გენერალურმა მდივანმა იენს სტოლტენბერგმა განაცხადა: *,,ატომური იარაღის ნებისმიერი გამოყენება აბსოლუტურად მიუღებელია, ის მთლიანად შეცვლის კონფლიქტის ხასიათს და რუსეთმა უნდა იცოდეს, რომ ბირთვული ომი არ შეიძლება მოიგოს და არ უნდა იბრძოლოს".*[212]

ბირთვული საფრთხე ყოველთვის იარსებებს მანამ, სანამ რუსეთი არ მოხვდება მკაცრად კონტროლირებადი საერთაშორისო შეთანხმების ფარგლებში. ყურადღება უნდა მიექცეს იმ ფაქტს, რომ გარკვეულ ქვეყნებში ფსევდო-ლიბერალური და ფსევდოდემოკრატიული მოძრაობების მხარდაჭერა, ცალკეული სუბიექტების საშინაო საქმეებში არცთუ იშვიათად ჩარევა და ამავე დროს ეროვნულ ინტერესებზე, ტრადიციებზე, კულტურულ ღირებულებებზე ზეწოლა აძლიერებს რევანშისტურ ძალებს ამ ქვეყნებში და საბოლოოდ აყალიბებს ანტიდასავლურ განწყობებს მოსახლეობის დიდ ნაწილში, რითაც შეიძლება რუსეთმა ისარგებლოს და რომელიც მომავალში ევროატლანტიკური ინტეგრაციის სერიოზულ ხელისშემშლელ ფაქტორად მოგვევლინოს.. დასავლეთმა მეტი ყურადღება უნდა მიაქციოს ასპირანტ ქვეყნებს, რაც უფრო მალე გათავისუფლდება რუსეთზე დამოკიდებულებისგან, მით უფრო ადვილი იქნება მომავალში. მეტი ძალისხმევაა საჭირო უსაფრთხოებისა და თავდაცვის სისტემების გაძლიერებასა და დაფინანსებაზე.

[212] *Siebold S., Bart Meijer B., "NATO warns Russia of "severe consequences" in case of a nuclear strike", Reuters, p. 1, 2022, https://www.reuters.com/world/europe/nato-warns-russia-severe-consequences-case-nuclear-strike-2022-09-27/*

ცხრილების, დიაგრამების, ფიგურებისა და სურათების ნუსხა

სურათი 7: ანგარიშებში შესვლა.

სურათი 8: ოფციებში შესვლა.

სურათი 9: ფანჯრის გახსნა, საიდანაც შესაძლებელია პაროლების ცვლილება.

სურათი 10: „გუგლი აპლიკაციების“ ფანჯრის გახსნა და ჩვენს ანგარიშში გადასვლა.

სურათი 11: უსაფრთხოების ღილაკის არჩევა და პაროლის შეცვლა.

სურათი 12: ანგარიშის გახსნა და „პარამეტრები & კომფიდენციალურობა“-ში გადასვლა.

სურათი 13: პარამეტრებში შესვლა.

სურათი 14: მენიუში „უსაფრთხოება და შესვლა“-ში გადასვლა.

სურათი 15: ქვემენიუში ღილაკი „პაროლის შეცვლის“ არჩევა, პაროლის ცვლილება და დამახსოვრება.

სურათი 16: „გუგლის აპლიკაციების“ ფანჯრის გახსნა და „გუგლი დრაივის“ არჩევა.

სურათი 17: ღილაკი „ხალის“ არჩევა.

სურათი 18: ახალი ფოლდერი შექმნა, ფაილის ატვირთვა, ფოლდერის ატვირთვა.

სურათი 19: ახალი ფოლდერის გაკეთება.

სურათი 20: ფაილის ან ფოლდერის ატვრთვა.

სურათი 21: საწყისი მენიუს გახსნა.

სურათი 22: შეცვალე ანგარიშის პარამეტრებში გადასვლა.

სურათი 23: ღილაკი „სისტემის“ არჩევა და Windows-ის განახლება.

სურათი 24: „ეფლის ლოგოს“ მოძებნა და სისტემის პარამეტრებში შესვლა.

სურათი 25: პროგრამული უზრუნველყოფის განახლებაში გადასვლა.

სურათი 26: დაჭერა ღილაკზე „განაახლე ახლავე“.

სურათი 27: სწრაფი, ღმა და ჩვენი შეხედულებისამებრ სკანირება.

სურათი 28: კომპიუტერის კამერისა და მიკროფონის სკანირება.

სურათი 29: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (1).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 30: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (2).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 31: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (3).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 32: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (4). *წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/*

სურათი 33: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (5).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 34: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (6).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 35: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (7).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 36: BitLocker-ის დაშიფვრის ჩართვა Windows 11-ზე (8).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 37: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (1).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 38: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (2).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 39: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (3).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 40: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (4).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 41: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (5).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 42: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (6).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 43: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (7).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 44: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (8).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 45: BitLocker-ის ჩართვა Windows 11-ის ფიქსირებულ მონაცემთა დისკზე (9).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 46: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (1).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 47: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (2).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 48: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (3).

წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 49: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (4).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 50: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (5).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 51: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (6).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 52: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (7).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 53: BitLocker-ის ჩართვა To Go USB ფლეშ დრაივზე - Windows 11 (8).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 54: BitLocker-ის გამორთვა Windows 11-ზე (1).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 55: BitLocker-ის გამორთვა Windows 11-ზე (2).
წყარო: https://pureinfotech.com/enable-bitlocker-windows-11/

სურათი 56: Android სისტემის განახლება ან გადამოწმება.

სურათი 57: IOS სისტემის განახლება ან გადამოწმება.

სურათი 58: ზედაპირული ქსელი (სუფთა ვები), ღრმა ქსელი, ბნელი ქსელი (დაფარული ქსელი).

წყარო: https://www.vpn.nl/faq/dark-web

სურათი 59: „გუგლი-ჩრომის“ განახლება.

სურათი 60: გადამოწმება, განახლებულია თუ არა ბროუზერი „გუგლი-ჩრომი“.

სურათი 61: დაარქივება.

სურათი 62: როგორ მუშაობს სადენიანი და უსადენო ქსელები.
წყარო: https://www.pinterest.com/pin/464011567858877829/

გამოყენებული აბრევიატურა

ISO (International Standarts Organization)
საერთაშორისო სტანდარტების ორგანიზაცია

EN (European Standards)
ევროპის სტანდარტების ორგანიზაცია

NCSA (NATO Communication and Information Systems Services Agency)
ნატოს კომუნიკაციებისა და ინფორმაციის სისტემების მომსახურების სააგენტო

NITC (NATO Infosec Technical Centre)
ნატოს ინფორმაციის უსაფრთხოების ტექნიკური ცენტრი

NCIRC (NATO Computer Incident Response Capability)
ნატოს კომპიუტერული ინციდენტების რეაგირების ცენტრი

CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence)
ნატოს კოოპერატიული კიბერთავდაცვის ცენტრი

NCS (NATO Committee for Standardisation)
ეროვნული კიბერუსაფრთხოება

ICT (Information and communications technology)
საინფორმაციო და საკომუნიკაციო ტექნოლოგიები

DNS (The Domain Name System)
დომენების სახელების სისტემა

com, edu, gov (Company, education, government)
კომპანია, სწავლება, სამთავრობო

EDT (Emerging and Disruptive Technologies)
განვითარებადი და დამრღვევი (დამღუპველი) ტექნოლოგიები

NSO (NATO Standardization Office)
სტანდარტიზაციის ოფისი

DIANA (Defence Innovation Accelerator for the North Atlantic)
თავდაცვის ინოვაციის ამაჩქარებელი ჩრდილო ატლანტიკისთვის

NIS (Directive on security of network and information systems)
დირექტივა ქსელისა და საინფორმაციო სისტემების უსაფრთხოების შესახებ

ISACs (Information Sharing and Analysis Centers)
ინფორმაციის ანალიზისა და გაზიარების ცენტრები

CSIRT (Computer Security Incident Response Team)
კომპიუტერული უსაფრთხოების შემთხვევების რეაგირების ჯგუფი

SOC (Security Operations Centers)
უსაფრთხოების ოპერაციების ცენტრები

NCSI (National Cyber Security Index)
ეროვნული კიბერუსაფრთხოების ინდექსის

ENISA (The European Union Agency for Cybersecurity)
ევროკავშირის კიბერუსაფრთხოების სააგენტო

(EU4Digital Facility)
ევროკავშირის 4 ციფრული დაწესებულება (ობიექტი)

(EU4Digital Initiative)
ევროკავშირის 4 ციფრული ინიციატივა

(EU4Figital)
ევროკავშირის 4 ფიგურა

CENELEC (European Committee for Electrotechnical Standardization)
ელექტროტექნიკური სტანდარტიზაციის კომიტეტი

IEC (International Electrotechnical Commission)
საერთაშორისო ელექტროტექნიკური კომისია

ETSI (European Telecommunications Standards Institute)
ევროპის სატელეკომუნიკაციო სტანდარტების ინსტიტუტი

NSA (National Security Agency)
ეროვნული უსაფრთხოების სააგენტო

SIGINT (Signals Untelligence Systems)
სიგნალების ინტელექტუალური სისტემები

INFOSEC (Information Security)
ინფორმაციული უსაფრთხოება

CYBERCOM (Cyber Command)
კიბერსარდლობა

CISA (Cyber Infrastructure Security Agency)
კიბერუსაფრთხოებისა და ინფრასტრუქტურის სააგენტო

NIST (National Institute of Standards and Technology)
სტანდარტებისა და ტექნოლოგიების ეროვნული უნივერსიტეტი

ONCD (Office of the National Cyber Director)
ეროვნული კიბერდირექტორის ოფისი

FBI (Federal Bureau of Investigation)
გამოციების ფედერალური ბიურო

CIA (Central Intelligence Agency)
ცენტრალური სადაზვერვო სააგენტო

IT (Information technology)
ინფორმაციული ტექნოლოგიები

FTC (The Federal Trade Commission)
ფედერალური სავაჭრო კომისია

COPPA (Children's Online Privacy Protection Act)
ბავშვთა ონლაინ კონფიცენციალურობის აქტი

TSA (The Transportation Security Administration)
ტრანსპორტის უსაფრთხოების ადმინისტრაცია

CAP (Civil Air Patrol)
სამოქალაქო საჰაერო პატრული

OIG (Office of Inspector General)
გენერალური ინსპექტორის ოფისი

DHS (United States Department of Homeland Security)
შეერთებული შტატების შიდა უსაფრთხოების დეპარტამენტი

DOD (Department of Defense)
თავდაცვის დეპარტამენტი

OMB (Office of Management and Budget)
ამერიკის შეერთებული შტატების მართვისა და მენეჯმენტის ოფისი

KGB (Committee for State Security)
КГБ (Комитет государственной безопасности)
სახელმწიფო უსაფრთხოების კომიტეტი

GRU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation)
ГРУ (Главное разведывательное управление)
დაზვერვის მთავარი სამმართველო

ФАПСИ (Федеральное агентство правительственной связи и информации при Президенте Российской Федерации)
FAPSI (Federal Agency of Government Communications and Information)

რუსეთის ფედერაციის პრეზიდენტთან არსებული სამთავრობო კომუნიკაციებისა და ინფორმაციის ფედერალური სააგენტო

GURRSS (Communications Electronic Intelligence Chief Unit)
კომუნიკაციების ელექტრონული დაზვერვის მთავარი განყოფილება

FSB (Federal Security Service)
უსაფრთხოების ფედერალური სამსახური

UKIB (Computer and Information Security Service)
კომპიუტერული და ინფორმაციული უსაფრთხოების სამსახური

SVR RF (Foreign Intelligence Service of the Russian Federation)
СВР России (Служба внешней разведки Российской Федерации)
რუსეთის ფედერაციის საგარეო დაზვერვის სამსახური

FSO (Federal Protective Service)
ФСО (Федеральная служба охраны)
ფედერალური დაცვის სამსახური

TSIB (Center for Information Security)
ინფორმაციული უსაფრთხოების ცენტრი

TSNIIKHM (Central Scientific Research Institute of Chemistry and Mechanics)
ქიმიისა და მექანიკის ცენტრალური სამეცნიერო კვლევითი ინსტიტუტი

DDoS (Distributed denial-of-service attack)
განაწილებული ორყოფის შეტევა

ARSIB (Association of Chief Information Security Officers)
საინფორმციო უსაფრთხოების მთავარ ოფიცერთა ასოციაცია

CTF (Capture the Flag)
დაიჭირე დროშა (დროშის ხელში ჩაგდება)

MFA (Multi-Factor Authentication)
მრავალფაქტორიანი ავთენტიფიკაცია

NCCCI (National Computer Incident Coordination Centre)
რუსეთის კომპიუტერული ინციდენტების ეროვნულმა საკოორდინაციო ცენტრი

SATCOM (Communications Satellite)
კავშირგაბმულობის თანამგზავრი

APT (advanced persistent threat)
მოწინავე საფრთხის ჯგუფები

SCC (Supreme Cyberspace Council)
კიბერსივრცის უმაღლესი საბჭო

IRGC (Islamic Revolutionary Guard Corps)
ირანის ისლამური რესპუბლიკის რევოლუციური გვარდიის კორპუსი

the Basij (The Mobilization)
ბასიჯი (ქართულად ითარგმნება როგორც „მობილიზაცია“)

NPDO (National Passive Defense Organization)
ირანის ისლამური რესპუბლიკის პასიური თავდაცვის ორგანიზაცია

SNSC (The Supreme National Security Council)
ეროვნული უშიშროების უმაღლესი საბჭო

NCC (National Cyberspace Council)
კიბერსივრცის ეროვნული საბჭო

EWCDO (Electronic warfare and cyber defense organization)
ელექტრონული ომისა და კიბერ თავდაცვის ორგანიზაცია

AFGS (Armed Forces General Staff)
შეიარაღებული ძალების გენერალური შტაბი

MOIS (Ministry of Intelligence and Security)
დაზვერვისა და უსაფრთხოების სამინისტრო

aka FATA (Iran's cyber police)
ირანის კიბერპოლიცია

PLASSF (People's Liberation Army Strategic Support Force)
სტრატეგიული მხარდაჭერის ძალები

NSCS (National Security Council)
ინდოეთის ეროვნული უშიშროების საბჭოს სამდივნო

ITU (The International Telecommunication Union)
საერთაშორისო სატელეკომუნიკაციო კავშირი

PCC (Prykarpattyaoblenergo Control Center)
Prykarpattyaoblenergo კონტროლის ცენტრი

SCADA (supervisory control and data acquisition)
სამეთვალყურეო კონტროლი და მონაცემთა მოპოვება

DAM (Digital asset management)
ციფრული აქტივების მართვა

CPC Corp (Taiwan State Energy Company)
ტაივანის სახელმწიფო ენერგეტიკულ კომპანია

ISMS (Information Security Management System)
ინფორმაციის უსაფრთხოების მართვის სისტემა

NFC (Near-field communication)
ახლო ველზე კომუნიკაცია

IR (Information retrieval)
ინფორმაციის მოძიება

VPN (a virtual private network)
ვირტუალური დაფარული ქსელი

R&D (Research & Development lab)
კვლევებისა და განვითარების ლაბორატორია

IISS (International Institute for Strategic Studies)
სტრატეგიული კვლევების საერთაშორისო ინსტიტუტი

CIP (Critical Infrastructure Protection)
კრიტიკული ინფრასტრუქტურის დაცვა

INCD (Israel National Cyber Directorate)
ისრაელის ეროვნული კიბერდირექცია

JCPOA (the Joint Comprehensive Plan of Action)
ერთობლივი ყოვლისმომცველი სამოქმედო გეგმა

MOU (Memorandum of Understanding)
ურთიერთთანამშრომლობის მემორანდუმი

ბიბლიოგრაფია

Verhelst A., "A comparative analysis of Article 5 Washington Treaty (NATO) and Article 42(7) TEU (EU)", EPRS - European Parliamentary Research Service, p. 1, 2022. www.europarl.europa.eu/RegData/etudes/ATAG/2022/739250/EPRS_ATA(2022)739250_EN.pdf

Faulconbridge G., "Putin sees no threat from NATO expansion, warns against military build-up", Reuters, p. 1, 2022,

https://www.reuters.com/world/europe/russia-calls-finland-sweden-joining-nato-mistake-with-far-reaching-consequences-2022-05-16/

Nato, "Doorstep statement - by NATO Secretary General Jens Stoltenberg at the start of the 2023 NATO Summit in Vilnius", p. 1, 2023. https://www.nato.int/cps/en/natohq/opinions_217038.htm?selectedLocale=en

NATO, "Cyber defence", p. 1, 2022, https://www.nato.int

NATO, "NATO Secretary General addresses the Brussels Forum: "We need a bold strategy for our new security reality", p. 1. 2022. https://www.nato.int

Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 16. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 19. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 20. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 25. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 27. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 28. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Klimburg A., "National Cyber Security Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE Publication, Tallinn, Estonia, p. 34. 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Nato Cooperative Cyber Defence Centre of Excellence, "Research Report Military Movement: Risks from 5G Networks", Tallinn, p. 48. 2022. https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf

Ertan A., Kuprys L. C. A., Lillemets P., Nordli L. C. G., "Cyber Exercises: A Vision for NATO CyCon 2021 Workshop Summary Report", the NATO Cooperative Cyber Defence Centre of Excellence, p. 7, 2021. https://ccdcoe.org/uploads/2022/07/Cyber-Exercises-A-Vision-for-NATO-Summary-Doc-August-2021.pdf

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/

NATO, "Funding NATO", p. 1. 2022. https://www.nato.int

Maggie M., "NATO establishes program to coordinate rapid response to cyberattacks", Politico, p. 1. 2022. https://www.politico.com

Edwards S. S., Loomis W., Handler S., "Supersize cyber", Atlantic Cuncil, p. 1. 2022. https://www.atlanticcouncil.org

Digital Editor, World Economic Forum, "New European Union cybersecurity proposal takes aim at cybercrime", p. 1, 2022. https://www.weforum.org/agenda/2022/09/new-european-union-cybersecurity-proposal-takes-aim-at-cybercrimes/

European Parliament, "Cyber: How big is the threat?", 2019. P. 1. https://www.europarl.europa.eu

Europa Commission, "State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks", 2017. P. 1. https://ec.europa.eu

World Economic Forum, "Wild Wide Web - Consequences of Digital Fragmentation", 2020. P. 1. https://reports.weforum.org

Ministère de l'Europe et des Affaires étrangères, "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace", 2018. P. 1. https://www.diplomatie.gouv.fr

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

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

European Commission, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient", 2020. P. 1. https://ec.europa.eu

European Commission, "Jount Communication to the Eorupean Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade", 2020. P. 14. https://eur-lex.europa.eu

NIS Cooperation group, "EU coordinated risk assessment of the cybersecurity of 5G networks", 2019. PP. 4-12. report__eu_risk_assessment_E4583F51-F351-6B15-A1317185D4FB353A_62132.pdf

National Cyber Security Index, p.1, 2022. https://ncsi.ega.ee/ncsi-index/

Funded by the European Union, "The EU4Digital Initiative", p. 1, 2022. https://eufordigital.eu/discover-eu/the-eu4digital-initiative/

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.

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

Tyson M., "The US federal cybersecurity bureaucracy: A guide", CSO united states, may 16. p. 1, 2022. https://www.csoonline.com/

Bielby K., "OIG: DHS Has Improved Cybersecurity Collaboration With DOD But Gaps Remain", p. 1. 2021, https://www.hstoday.us/

Homland Security, "President Biden has made cybersecurity, a critical element of the Department of Homeland Security's (DHS) mission, a top priority for the Biden-Harris Administration at all levels of government", p. 1. 2022. https://www.dhs.gov/topics/cybersecurity

United States Air Force Auxiliary, "The CAP Guide to Effective Communication", 2021. https://www.gocivilairpatrol.com/media/cms/P_12_1_Oct_2021_E4A84FC1A6F2B.pdf

Bielby K., "OIG: DHS Has Improved Cybersecurity Collaboration With DOD But Gaps Remain", p. 1. 2021, https://www.hstoday.us/

Dress B., "White House moves to boost cybersecurity at federal agencies", p. 1, 2022. https://thehill.com/policy/cybersecurity/591497-white-house-moves-to-boost-cybersecurity-at-federal-agencies/

Caspit B., "Ahead of elections, Israel fears foreign cyber meddling", Al-monitor, p. 1, 2019,

https://www.al-monitor.com/originals/2019/02/israel-russia-iran-benjamin-netanyahu-cyber-attacks-election.html

Solomon S., "Energy minister says Israel foiled 'serious' attack on power station", The Times of Israel, p. 1, 2020, https://www.timesofisrael.com/energy-minister-says-israel-foiled-serious-attack-on-power-station/

Bigelow J., S., Montgomery J., "ITIL (Information Technology Infrastructure Library)", Techtarget, p. 1, https://www.techtarget.com/searchdatacenter/definition/ITIL

Solomon S., "Israel wins second-largest number of cybersecurity deals globally", p. 1, 2018, https://www.timesofisrael.com/israel-nabs-second-largest-number-of-cybersecurity-deals-globally/

Orbach M., Shulman S., "The 50 most promising Israeli startups - 2023", p. 1, 2023, https://www.calcalistech.com/ctechnews/article/hjtwkuqx2

Topwar, "British experts from IISS named 15 countries with maximum cyber capabilities", p. 1, 2021, https://en.topwar.ru/184530-britanskie-jeksperty-iz-iiss-nazvali-15-stran-s-maksimalnymi-kibervozmozhnostjami.html

Forcepoint, "What Is Critical Infrastructure Protection (CIP)?", p. 1, https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip

ნიკოლეიშვილი ლ., „რუსეთ-უკრაინის ომის დასრულების შესაძლო სცენარები", სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემია, გორი, 5-8 გვ. 2022.

Euronews, "Vladimir Putin recognises Ukrainian separatist regions, in escalation of tensions", p. 1, 2022. https://www.euronews.com/2022/02/21/putin-dangles-donbas-recognition-as-tensions-in-eastern-ukraine-continue-to-rise

Vishnu V. V., "Russia-Ukraine War: Anonymous Declares 'cyber War' Against Russia, Targets Govt Websites", Republic World, p. 1. 2022. https://www.republicworld.com/world-news/russia-ukraine-crisis/russia-ukraine-war-anonymous-declares-cyber-war-against-russia-targets-govt-websites-articleshow.html

Trinko M., "Anonymous Hacked Gazprom and Leaked 768,000 Emails from Company Employees", Gagadget, p. 1. 2022. https://gagadget.com/en/116384-anonymous-hacked-gazprom-and-leaked-768000-emails-from-company-employees/

Borogan I. Soldatov A. "The Dawn of a New Era: The Birth of the FSB," in The New Nobility: the restoration of Russia's security state and the enduring legacy of the KGB, New York, p. 13, 2011.

Borogran I. Soldatov A., "Putin's Overseas Offensive,", New York", PP. 225-227, 2017.

Graham L., "Lonely Ideas: Can Russia Compete?", MIT Press, p. 93, 2013.

Soldatov A. Borogan I., "How Putin Tried to Control the Internet", Vice, p. 1, 2015. https://www.vice.com/en/article/qvyzn4/how-putin-tried-to-control-the-internet

Russian Federation, "Information Security Doctrine of the Russian Federation September 2000", Ministry of Foreign Affairs, p. 1, 2000. https://info.publicintelligence.net/RU-InformationSecurity-2000.pdf

Российской Федерации, "Доктрина информационной безопасности Российской Федерации", 2000 г. N Пр-1895, https://base.garant.ru/182535/

Bennett G., "FPS & FAPSI – RIP," Conflict Studies Research Centre, Occasional Brief No 96, PP. 1-2, 2003, https://www.files.ethz.ch/isn/96240/03_Mar_2.pdf

Association of Heads of Information Security Services, "Projects of the CTF movement in Russia" p. 1, 2022. http://aciso.ru/aciso-projects/3861/

Infoforum, "National Forum on Information Security", p. 1, 2014. https://old.infoforum.ru/conference/conference/view/id/5

Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021. https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/

Janofsky A., "This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites", The Record by Recorded Future, p. 1, 2022. https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/

Интернет-портал: Безопасность пользователей в сети интернет,"НКЦКИ: рекомендации по защите информационных ресурсов от компьютерных атак", p. 1, 2022. https://safe-surf.ru/specialists/news/676114/

Cisco Annual Report, "Reimagining the future of connectivity", 2022. https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf

Curatedintel, "Curated Intelligence Stands With Ukraine", p. 1, 2022. https://www.curatedintel.org/2022/02/curated-intelligence-stands-with-ukraine.html

BBC, "Iran profile - timeline", p. 1, 2020. https://www.bbc.com/news/world-middle-east-14542438

independent, "Iran, Russia sign MoU for petroleum investment", p. 1, 2022. https://www.independent.co.ug/iran-russia-sign-mou-for-petroleum-investment/

Ajorlo H., "Understanding the threats and barriers to reviving the JCPOA", Aljazeera, p. 1, 2021. https://studies.aljazeera.net/en/analyses/understanding-threats-and-barriers-reviving-jcpoa

Gramer R., Amy Mackinnon A., "Iran and Russia Are Closer Than Ever Before", p. 1, 2022. https://foreignpolicy.com/2023/01/05/iran-russia-drones-ukraine-war-military-cooperation/

Connell M., "Deterring Iran's Use of Offensive Cyber: A Case Study", CNA, PP. 2-4, 2014. https://www.cna.org/archive/CNA_Files/pdf/dim-2014-u-008820-final.pdf

Zetter K., "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", Crown Publishers, an imprint of Random House LLC, p. 1, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Anderson C. Sadjadpour K., "Iran's Cyber Threat: Espionage, Sabotage, and Revenge", Carnegie Endowment for International Peace, PP. 15-17, 2018. https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

Denning D., "Following the developing Iranian cyber threat", The Conversation, p. 1, 2017. https://theconversation.com/following-the-developing-iranian-cyberthreat-85162

Nadimi F., "Iran's Passive Defense Organization: Another Target for Sanctions", p. 1, 2018. https://www.washingtoninstitute.org/policy-analysis/irans-passive-defense-organization-another-target-sanctions

Katzman K., "Iran: Internal Politics and U.S. Policy and Options," Congressional Research Service, PP. 4-7, 2018. https://sgp.fas.org/crs/mideast/RL32048.pdf

Small Media, "Iranian Internet Infrastructure and Policy Report," smallmedia.org.uk, PP. 3-5, 2014. https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb2014.pdf

U.S. Department of the Treasury, "Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators," Press Release, p. 1, 2018. https://home.treasury.gov/news/press-releases/sm0250

U.S. Navy, "Iranian Naval Forces: A Tale of Two Navies," Office of Naval Intelligence, PP. 13-15, 2017. https://www.oni.navy.mil/Portals/12/Intel%20agencies/iran/Iran%20022217SP.pdf

Library of Congress, "Iran's Ministry of Intelligence and Security: A Profile", Federal Research Division, PP. 2-4, 2012. https://irp.fas.org/world/iran/mois-loc.pdf

U.S. Department of the Treasury, "Treasury Announces Sanctions Against Iran", Press Release, p. 1, 2013. https://home.treasury.gov/news/press-releases

Cilluffo F., Fixler A., "Monograph - Evolving Menace Iran's Use of Cyber-Enabled Economic Warfare", FDD American Leadership, p. 1, 2018. https://www.fdd.org/analysis/2018/11/06/evolving-menace/

Schmitt M. N.,"Noteworthy Releases of International Cyber Law Position - Part II: Iran", p. 1, 2020. https://lieber.westpoint.edu/iran-international-cyber-law-positions/

China Aerospace Studies Institute, "PLA's Science of Military Strategy", 2013. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf

Farrell H., "The Chinese government fakes nearly 450 million social media comments a year. This is why", washingtonpost, p. 1, 2016.

https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/

Singh M. C., "China's Cyber Warfare Capabilities", Indian Defence Review, p. 1, 2020. http://www.indiandefencereview.com/news/chinas-cyber-warfare-capabilities/

Levine M. Date J., "22 Million Affected by OPM Hack, Officials Say", ABC News, p. 1, 2015. https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731

Kartha T., "The Rejig of India's National Security Architecture Has Been a Long Time Coming", The Wire, p. 1, 2018. https://thewire.in/security/ajit-doval-national-security-council-secretariat

Jinghua L., "What Are China's Cyber Capabilities and Intentions?", IPI Global Observatory, p. 1, 2019. https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/

ნიკოლეიშვილი ლ. "რეგიონალური აქტორის, რუსეთის კიდევ ერთი იარაღი/ინსტრუმენტი საქართველოს წინაღმდეგ", სსიპ დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემია, გორი, 4-11 გვ. 2021.

ლილუაშვილი გ. „საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში", გვ. 1-27. 2018. http://ssg.gov.ge

ლილუაშვილი გ. „რუსეთი საქართველოში ჰიბრიდული ომის ხუთი ძირითადი ინსტრუმენტით მოქმედებს" გვ. 1, 2019. http://parliament.ge

Latvian Public Broadcasting, „Latvia suspends Rossiya RTR channel", p. 1, 2016. https://eng.lsm.lv

Lithuanian National Radio and Television, „Lithuanian regulatory agency suspends RTR Planeta", p. 1, 2015. https://www.lrt.lt

Baltic News Network, „Lithuanian media regulator has decided to take off air for a three-month period Russian state-owned TV channel RTR Planeta.", p. 1, 2015. https://bnn-news.com

Russian Federation, "of the 2015 Russian National Security Strategy", Russia Matters, p. 1, 2015. https://www.russiamatters.org/node/21421

Smoleňová I. „The Pro-Russian Disinformation Campaing in The Czech Respublic and Slovakia", Prague Security Studies Institute, p. 1-18. 2015. http://www.pssi.cz

Information Agency „Stop Fake", „Disinformation and European erosion in Romania", p. 1, 2019. https://www.stopfake.org

Information Agency "MyTh Detector", „Geworld Spreads News by Russian Troll Factory on Legalization of Necrophilia and Bestiality in Europe", p. 1, 2018. https://www.mythdetector.ge

Kioski, „Yle Kioski Investigated: This is How Pro-Russia Trolls Manipulate Finns Online – Check the List of Forums Favored by Propagandists" p. 1. 2015. https://kioski.yle.fi

News and View for Ukraine "Euromaidanpress", „Ukraine remains top target of Russian disinformation", p. 1, 2019. http://euromaidanpress.com

Król A. „Russian Information Warfare in the Baltic States — Resources and Aims", p. 1, 2017. https://warsawinstitute.org

ბასილაია ე. „გერმანული მედია: რუსები 2008 წელს ბირთვული იარაღის გამოყენებას აჰირებდნენ", გვ. 1, 2017. http://resonancedaily.com

იაგორაშვილი ი. „რუსეთის 2 მითი ბალტიისპირეთის ქვეყნების შესახებ“, გვ. 1, 2019. http://www.mythdetector.ge

საქართველოს საზოგადოებრივი მაუწყებელი, „euvsdesinfo.eu აქვეყნებს სტატიას - საქართველოს 100-წლიანი ბრძოლა კრემლის დეზინფორმაციასთან“, გვ. 1, 2019. https://1tv.ge

საქართველოს მთავრობა, "საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგია", საქართველო, თბილისი, 2021. https://matsne.gov.ge/ka/document/view/5263611?publication=0

“National Cyber Security intex", "67. Georgia 51.95", 2022. pp. 1-2, https://ncsi.ega.ee/country/ge/?allData=1

CISA Central, "Cyber-Attack Against Ukrainian Critical Infrastructure", p. 1, 2021.

https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

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

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

Tom Burt - Corporate Vice President, Customer Security & Trust,"Russian cyberattacks pose greater risk to governments and other insights from our annual report", Microsoft, p. 1, 2021.

https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/

Cisco Annual Report, "Reimagining the future of connectivity", 2022. https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf

CyberScoop, "Ukraine warns of ‘massive cyberattacks’ coming from Russia on critical infrastructure sites", p. 1, 2022, https://cyberscoop.com/ukrainians-warn-of-massive-cyberattacks/

Sigal L., "What You Need to Know About the Anonymous Sudan Hacker Group", CYE Blog, 2023. p. 1. https://cyesec.com/blog/what-you-need-to-know-about-the-anonymous-sudan-hacker-group

Check Point Research Team, "The New Era of Hacktivism - State-Mobilized Hacktivism Proliferates to The West and Beyond", p. 1, 2022. https://research.checkpoint.com/2022/the-new-era-of-hacktivism/

Lyngaas S., "Pro-Russia hackers claim disruption of US Congress website", cnn politics, p. 1, 2022. https://edition.cnn.com/2022/07/08/politics/congress-website-disrupted/index.html

Vijayan J., "Pro-Islam 'Anonymous Sudan' Hacktivists Likely a Front for Russia's Killnet Operation", Dark Reading, 2023. p. 1, https://www.darkreading.com/attacks-breaches/pro-islam-anonymous-sudan-hacktivists-front-russia-killnet-operation?fbclid=IwAR3RMbRQqQbRcMxmv-iZNGRGsvGEyuMUOK5IRfACYLzZQBPbcPmH6yo5uDA

Bracken B., "Killnet Gloats About DDoS Attacks Downing Starlink", White House, p. 1, 2022. https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov

Vijayan J. "Inside Killnet: Pro-Russia Hacktivist Group's Support and Influence Grows", Dark Reading, p. 1. 2023. https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows

the Guardian, "Russian hackers 'target security cameras inside Ukraine coffee shops", p. 1, 2023. https://www.theguardian.com/world/2023/apr/11/russian-hackers-target-security-cameras-inside-ukraine-coffee-shops?fbclid=IwAR3JWtpSmI9UvvADsMqx5aVTbM8SjpsvCIUYPX389Ff_HxSarZV_ctLoMIQ

Harding L., Simeonova S., Ganguly M.,Dan Sabbagh D.,"'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics", The Guardian, p. 1, 2023. https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

Harding L., Simeonova S., Ganguly M.,Dan Sabbagh D.,"'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics", The Guardian, p. 1, 2023. https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

Janofsky A., "This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites", The Record by Recorded Future, p. 1, 2022.

https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/

Rahman A.b.F.M., "The Next Cyber Phase of the Russia-Ukraine War Will Echo in Asia", The Diplomat, p. 1. 2023. https://thediplomat.com/2023/02/the-next-cyber-phase-of-the-russia-ukraine-war-will-echo-in-asia/

National Cyber Security Centre, "Ukraine cyber defenders in UK for high-level talks", NCSC, p. 1, 2022. https://www.ncsc.gov.uk/news/ukraine-cyber-defenders-in-uk-for-high-level-talks

Griffiths C., "The Latest 2023 Cyber Crime Statistics (updated February 2023)" AAG, p. 1, 2022.

https://aag-it.com/the-latest-cyber-crime-statistics/

Lyngaas S., "Microsoft blames Russian military-linked hackers for ransomware attacks in Poland and Ukraine", cnn politics, p. 1, 2022.

https://edition.cnn.com/2022/11/10/politics/microsoft-russian-linked-hackers-poland-ukraine/index.html

Toulas B., "Poland warns of attacks by Russia-linked Ghostwriter hacking group", BleepingComputer, p. 1, 2022. https://www.bleepingcomputer.com/news/security/poland-warns-of-attacks-by-russia-linked-ghostwriter-hacking-group/

Kovacs E., "US, Ukraine Shut Down Cryptocurrency Exchanges Used by Cybercriminals", Security Week, p. 1, 2023. https://www.securityweek.com/us-ukraine-shut-down-cryptocurrency-exchanges-used-by-cybercriminals/?fbclid=IwAR0xr7MGMHq_RJ2PPh5DRrMlYCJvuoY_34j4CJzKe3A4v8v4tEnNzTuqAyA

Curatedintel, "Curated Intelligence Stands With Ukraine", p. 1, 2022. https://www.curatedintel.org/2022/02/curated-intelligence-stands-with-ukraine.html

Franck T., "Biden vows wider sanctions on Russia in effort to cut Moscow off from the global economy", cnbc, p. 1, 2022.

https://www.cnbc.com/2022/02/24/biden-vows-wider-sanctions-on-russia-in-effort-to-cut-moscow-off-from-the-global-economy.html

Flashpoint Team, "Understanding Russia's "Sovereign Internet": What Happens If Russia Isolates Itself from the Global Internet?", p. 1, 2022. https://flashpoint.io/blog/russian-runet-sovereign-internet/

Maigre M., "NATO's Role in Global Cyber Security", p. 1, 2022.

https://www.gmfus.org/news/natos-role-global-cyber-security

Kovacs E. "A Year of Conflict: Cybersecurity Industry Assesses Impact of Russia-Ukraine War", p. 1, 2023. https://www.securityweek.com/one-year-of-russia-ukraine-war-cybersecurity-industry-sums-up-impact/

Kagubare I., "Russia's cyber forces 'underperformed expectations' in Ukraine: senior US official", The Hill, p. 1, 2022.

https://thehill.com/policy/cybersecurity/3738506-russias-cyber-forces-underperformed-expectations-in-ukraine-senior-us-official/

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

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

Gartner, "Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 2Q22 Update", United Kingdom, p. 1, 2022. https://www.gartner.com/en/documents/4016190

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

IT (global market), "Information Security (Global Market)", Tadviser Goverment. Business. IT, p. 1, 2022. https://tadviser.com/index.php/Article:Information_Security_(Global_Market)#.2A_The_global_IB_services_market_will_reach_.2494_billion_by_2025

Frank E. "Global Cyber Security Revenue to Reach $334 Billion in 2026: GlobalData", Security Review Magazine, p. 1, 2022. https://securityreviewmag.com/?p=24826

Committed to connecting the world, "Statistics", p. 1, 2022. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Rosencrance L. Madelyn Bacon M., "social engineering", p. 1, 2021. https://www.techtarget.com/searchsecurity/definition/social-engineering

Lord N., "What is a Phishing Attack? Defining and Identifying Different Types of Phishing Attacks", Datainsider, p. 1, 2022. https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks

Fruhlinger J., "Ransomware explained: How it works and how to remove it", p. 1, 2020. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Imperva, "Distributed Denial of Service (DDoS)", p. 1, 2022.

https://www.imperva.com/learn/ddos/denial-of-service/

Crowdstrike, "What is it a Botnet?", p. 1, 2022. https://www.crowdstrike.com/cybersecurity-101/botnets/

Johansen G. A., "What is a Trojan? Is it a virus or is it malware?", p. 1. 2020. https://us.norton.com/blog/malware/what-is-a-trojan#

TechTarget Contributor, "critical infrastructure", p. 1. 2020. https://www.techtarget.com/whatis/definition/critical-infrastructure

Wagner D., "The Growing Threat of Cyber-Attacks on Critical Infrastructure", p. 1. 2016. https://www.irmi.com/articles/expert-commentary/cyber-attack-critical-infrastructure

Ball T., "Top 5 critical infrastructure cyber attacks", p. 1. 2022. https://techmonitor.ai/technology/cybersecurity/top-5-infrastructure-hacks

Industrial Control Systems Security, p.1. 2016. https://www.sans.org/industrial-control-systems-security/

Swati Khandelwal S., "San Francisco Metro System Hacked with Ransomware; Resulting in Free Rides", p. 1. 2016. https://thehackernews.com/2016/11/transit-system-hacked.html

FBI, "Iranian DDoS Attacks", p. 1. 2016. https://www.fbi.gov/wanted/cyber/iranian-ddos-attacks

Walton B., "Water Utility Cyberattack Rings Up Hefty Data Charges", p. 1. 2017. https://www.circleofblue.org/2017/water-management/water-utility-cyberattack-rings-hefty-data-charges/

National Cybersecurity Centre NCSC Federal Intelligence Service FIS, "Information Assurance", Reporting and Analysis Centre for Information Assurance MELANI, p. 18, 2020. https://www.newsd.admin.ch/newsd/message/attachments/63536.pdf

Paganini P., "Piping botnet: Researchers warns of possible cyberattacks against urban water services", p. 1. 2020. https://securityaffairs.co/wordpress/75389/hacking/piping-botnet-water-services.html

Support the Guardian Available for everyone, funded by readers, "How the Colonial Pipeline hack is part of a growing ransomware trend in the US", p. 1. 2021. https://www.theguardian.com/technology/2021/may/13/colonial-pipeline-ransomware-attack-cyber-crime

Brook Ch., "What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More", p. 1, 2022. https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

Huc M., "How to enable BitLocker on Windows 11", pureinfotech, p. 1, 2022. https://pureinfotech.com/enable-bitlocker-windows-11/

Terra J., "What is the Internet? Reviewing the Basics", Simplilearn, p. 1, 2022. https://www.simplilearn.com/what-is-internet-article

Fortinet, "19 Types of Phishing Attacks", p. 1. 2022. https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

Irwin L., "What is ISO 27001 Information Classification?", ITgovernance, 2022. https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001#:~:text=What%20is%20ISO%2027001%20Information%20Classification%3F&text=Information%20classification%20is%20a%20process,granted%20access%20to%20view%20it.

Imperva, "Information Security: The Ultimate Guide", 2022. https://www.imperva.com/learn/data-security/information-security-infosec/

Eck T., "7 Steps to Effective Data Classification", Sirius Edge, 2019. https://edge.siriuscom.com/security/7-steps-to-effective-data-classification

Ahlgren M., "How Many People Use a VPN? (Usage Statistics for 2022)", Websiterating, p. 1, 2022. https://www.websiterating.com/

Carter R., "The Ultimate List of VPN Statistics for 2023", Findstack, p. 1, 2021. https://findstack.com/resources/vpn-statistics/

Siebold S., Bart Meijer B., "NATO warns Russia of "severe consequences" in case of a nuclear strike", Reuters, p. 1, 2022, https://www.reuters.com/world/europe/nato-warns-russia-severe-consequences-case-nuclear-strike-2022-09-27/

ლევან ნიკოლეიშვილის ბიოგრაფია

პროფესორი, პოლიტიკის მეცნიერების დოქტორი, თადარიგის პოლკოვნიკი.

დავით აღმაშენებელის სახელობის ეროვნული თავდაცვის აკადემიის უსაფრთხოების კვლევების სამაგისტრო პროგრამის პროფესორი; ლექციებს კითხულობდა სხვადასხვა უმაღლეს სასწავლებლებში: საქართველოს ტექნიკურ უნივერსიტეტში, ილიას სახელმწიფო უნივერსიტეტში, წმინდა ანდრიას ქართულ უნივერსიტეტსა და კავკასიის საერთაშორისო უნივერსიტეტში.

1984–1992 წლებში სწავლობდა თბილისის ივანე ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტის ისტორიის ფაკულტეტზე. 1995 წელს შეიარღებაზე კონტროლისა და ვერიფიკაციის კურსი (გერმანია);1997 წელს - გაერთიანებული სამეფოს ენების თავდაცვის სკოლა (დიდი ბრიტანეთისა და ჩრდილოეთ ირლანდიის გაერთიანებული სამეფო); 2001 წელს - აშშ-ის არმიის სამეთაურო და გენერალური შტაბის კოლეჯი (აშშ);2003 წელს-ნატო–ს თავდაცვის კოლეჯი (იტალია).

1992-1997 წლებში -თავდაცვის სამინისტროს, საგარეო ურთიერთობათა სამმართველოს ინფორმაციის განყოფილების უფროსი, ვერიფიკაციის განყოფილების უფროსი; 1997-1998 წლებში - მრჩეველ-რეფერენტი (ეროვნული უშიშროების საბჭო); 1998-1999 წლებში - ვერიფიკაციის ცენტრის უფროსი (შეიარაღებული ძალების გენერალური შტაბი); 2001-2002 წლებში - მთავარი ოპერატიული სამმართველოს უფროსი (შეიარაღებული ძალები გენერალური შტაბი); 2003 წელს - თავდაცვის დეპარტამენტის უფროსი (ეროვნული უშიშროების საბჭო); 2004-წელს - სახელმწიფო უშიშროების მინისტრის მოადგილე; 2004-2005 წლებში - შეიარაღებული ძალების გენერალური შტაბის უფროსის მოადგილე; 2005 წლის თებერვლიდან 2006 წლის დეკემბრამდე -შეიარაღებული ძალების გენერალური შტაბის უფროსი; 2006 წლის დეკემბრიდან-2007 წლის ივლისამდე იყო თავდაცვის მინისტრის პირველი მოადგილე, საპარლამენტო მდივანი;

ომისა და სამხედრო ძალების ვეტერანი; დაჯილდოებულია მედლებით მხედრული მამაცობისათვის და გენერალი მაზნიაშვილი; საქართველოს პრეზიდენტის 2003 წლის 9 ოქტომბრის N 1299 განკარგულებით მიენიჭა სახელმწიფო მრჩეველის საკლასო ჩინი.

თორნიკე ზედელაშვილის ბიოგრაფია

2015 წელს დაამთავრა გორის სახელმწიფო უნივერსიტეტის სოციალურ მეცნიერებათა ბიზნესისა და სამართალმცოდნეობის 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. 2022 წლიდან არის უკრაინული საერთაშორისო რეფერირებადი ჟურნალის - policymaker-ის ბორდის წევრი, ასევე ფილოსობიისა და კოსმოლოგიის საერთაშორისო ორგანიზაციის წევრი. ამავე წლიდან არის ქიმიური, ბიოლოგიური, რადიოლოგიური და ბირთვული საფრთხეების სტრატეგიული კვლევების ინსტიტუტის მკვლევარი.

ლევან ნიკოლეიშვილი

პროფესორი, პოლიტიკის მეცნიერების დოქტორი, თადარიგის პოლკოვნიკი.

დავით აღმაშენებლის სახელობის ეროვნული თავდაცვის აკადემიის უსაფრთხოების კვლევების სამაგისტრო პროგრამის პროფესორი; ლექციებს კითხულობდა სხვადასხვა უმაღლეს სასწავლებლებში: საქართველოს ტექნიკურ უნივერსიტეტში, ილიას სახელმწიფო უნივერსიტეტში, წმინდა ანდრიას ქართულ უნივერსიტეტსა და გავკასიის საერთაშორისო უნივერსიტეტში.

1984–1992 წლებში სწავლობდა თბილისის ივანე ჯავახიშვილის სახელობის სახელმწიფო უნივერსიტეტის ისტორიის ფაკულტეტზე. 1995 წელს შეიარაღებაზე კონტროლისა და ვერიფიკაციის კურსი (გერმანია);1997 წელს - გაერთიანებული სამეფოს ენების თავდაცვის სკოლა (დიდი ბრიტანეთისა და ჩრდილოეთ ირლანდიის გაერთიანებული სამეფო); 2001 წელს - აშშ-ის არმიის სამეთაურო და გენერალური შტაბის კოლეჯი (აშშ);2003 წელს-ნატო-ს თავდაცვის კოლეჯი (იტალია).

1992-1997 წლებში -თავდაცვის სამინისტროს, საგარეო ურთიერთობათა სამმართველოს ინფორმაციის განკუთვილების უფროსი, ვერიფიკაციის განყოფილების უფროსი; 1997-1998 წლებში - მრჩეველ-რეფერენტი (ეროვნული უშიშროების საბჭო); 1998-1999 წლებში - ვერიფიკაციის ცენტრის უფროსი (შეიარაღებული ძალების გენერალური შტაბი); 2001-2002 წლებში - მთავარი ოპერატიული სამმართველოს უფროსი (შეიარაღებული ძალები გენერალური შტაბი); 2003 წელს - თავდაცვის დეპარტამენტის უფროსი (ეროვნული უშიშროების საბჭო); 2004-წელს - სახელმწიფო უშიშროების მინისტრის მოადგილე; 2004-2005 წლებში - შეიარაღებული ძალების გენერალური შტაბის უფროსის მოადგილე; 2005 წლის თებერვლიდან 2006 წლის დეკემბრამდე -შეიარაღებული ძალების გენერალური შტაბის უფროსი; 2006 წლის დეკემბრიდან-2007 წლის ივლისამდე იყო თავდაცვის მინისტრის პირველი მოადგილე, საპარლამენტო მდივანი;

ომისა და სამხედრო ძალების ვეტერანი; დაჯილდოებულია მედლებით მხედრული მამაცობისათვის და გენერალი მაზნიაშვილი; საქართველოს პრეზიდენტის 2003 წლის 9 ოქტომბრის N 1299 განკარგულებით მიენიჭა სახელმწიფო მრჩეველის საკლასო ჩინი.

თორნიკე ზედელაშვილი

2015 წელს დაამთავრა გორის სახელმწიფო უნივერსიტეტის სოციალურ მეცნიერებათა ბიზნესისა და სამართალმცოდნეობის 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. 2022 წლიდან არის უკრაინული საერთაშორისო რეფერირებადი ჟურნალის - policymaker-ის ბორდის წევრი. ასევე ფილოსობიისა და კოსმოლოგიის საერთაშორისო ორგანიზაციის წევრი. ამავე წლიდან არის ქიმიური, ბიოლოგიური, რადიოლოგიური და ბირთვული საფრთხეების სტრატეგიული კვლევების ინსტიტუტის მკვლევარი.