ნატა გოდერძიშვილი

რუსეთის კიბერსტრატეგიის განვითარება, ტაქტიკები და გლობალური კიბერუსაფრთხოების ინფრასტრუქტურაში ჩარევის შემთხვევები

რუსეთის კიბერსტრატეგიის განვითარება, ტაქტიკები და გლობალურ კიბერუსაფრთხოების ინფრასტრუქტურაში ჩარევის შემთხვევები

ავტორი: **ნატა გოდერძიშვილი**

თბილისი

2024

პუბლიკაციის შესახებ

წინამდებარე პუბლიკაცია შეიქმნა აშშ-ის სახელმწიფო დეპარტამენტის მხარდაჭერით. დოკუმენტში გამოთქმული შეხედულებები და მოსაზრებები ეკუთვნის ავტორს და არ ასახავს ან წარმოადგენს სტრატეგიისა და განვითარების ცენტრის (CSD) ან შეერთებული შტატების სახელმწიფო დეპარტამენტის შეხედულებებსა და მოსაზრებებს.

შინაარსი

შესავალი

მოცემული კვლევა ეხება რუსეთის კიბერსტრატეგიის, ტაქტიკისა და გლობალური კიბერუსაფრთხოების ეკოსისტემაში მისი ჩარევის განვითარებას ადრეული პერიოდიდან დღემდე. დოკუმენტში განხილულია ისტორიული კონტექსტი, ტაქტიკური მანევრები, მნიშვნელოვანი გავლენის მქონე კიბეროპერაციები და კიბერსივრცეში რუსეთის სამომავლო სტრატეგიული პერსპექტივები. კვლევის მიზანია ყოვლისმომცველი ანალიზი იმის შესახებ, თუ როგორ გახდა რუსეთი მნიშვნელოვანი მოთამაშე კიბერუსაფრთხოების გლობალურ არენაზე და რა გავლენას ახდენს მისი საქმიანობა საერთაშორისო უსაფრთხოებაზე.

ლიტერატურის მიმოხილვა

კვლევის მომზადებისას ძირითადი რესურსების ბაზას წარმოადგენს:

რუსეთის სტრატეგიული და კონცეპტუალური ჩარჩოდოკუმენტები, სამართლებრივი აქტები;

ანგარიშები და კვლევები;

კიბერშეტევების მაგალითები.

მეთოდოლოგია

რუსეთის კიბერუსაფრთხოების სტრატეგიული გარემოს შესაფასებლად ჩატარებული ეს კვლევა მრავალფეროვან მეთოდოლოგიურ მიდგომებს ეყრდნობა, რათა სრულად და სიღრმისეულად გაანალიზდეს ამ მიმართულებით არსებული მდგომარეობა, მნიშვნელოვანი გავლენის მქონე შედეგები და სამომავლო პერსპექტივები. კვლევის პროცესი მოიცავს დოკუმენტურ მიმოხილვას, მონაცემთა დამუშავებას, საერთაშორისო გამოცდილების შედარებით ანალიზს.

კვლევის საწყის ეტაპზე ჩატარდა საჯაროდ ხელმისაწვდომი მონაცემებისა და ღია წყაროების ანალიზი. მათ შორის შესწავლილი იქნა რუსეთის კიბერუსაფრთხოების და, ზოგადად, ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტები და კონცეფციები, რომლებიც გავლენას ახდენს შიდა და გარე კიბერუსაფრთხოების კონტექსტზე. ასევე შესწავლილ იქნა კიბერუსაფრთხოების სფეროში ჩატარებული კვლევები, რაოდენობრივი და ხარისხობრივი მონაცემები, რაც საფუძვლად დაედო ფაქტობრივი გარემოებების ანალიზს და კვლევის ფარგლებში ჩამოყალიბებულ ძირითად მიგნებებს.

მოცემული მეთოდოლოგიური მიდგომები უზრუნველყოფს კვლევის მრავალმხრივ ხასიათს, მის მტკიცებულებებზე დამყარებულ დასაბუთებას და მაღალპროფესიულ სანდოობას.

განხილვა

კიბერსივრცე, როგორც რუსეთის პოლიტიკური ინსტრუმენტი

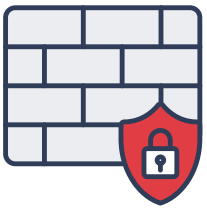
რუსეთის მხრიდან დასავლეთის სამხედრო და სამოქალაქო ინფრასტრუქტურაზე მიმართული კიბერშეტევები თანამედროვე ცხოვრების მუდმივ და საკმაოდ კომპლექსურ გამოწვევად იქცა მისი პოლიტიკური მოწინააღმდეგეებისთვის.

ტრადიციულად, რუსეთის მიერ განხორციელებული კიბეროპერაციები პოლიტიკური გავლენის მიღმა არ მწიფდება, არამედ პირიქით - ყველა შეტევას, როგორც წესი, ფართო სტრატეგიული და გეოპოლიტიკური სარჩული უდევს.

კიბერსივრცეში რუსეთის საქმიანობას მკაფიოდ ჩამოყალიბებული ეროვნული მოტივები და სახელმწიფოებრივი ზრახვები გააჩნია. რუსეთის საგარეო პოლიტიკური მიზანი კიბერსივრცეშიც გავლენის სფეროების გაფართოება, საერთაშორისო ასპარეზზე საკუთარი პოზიციების გამყარება და დასავლეთის ქვეყნებთან ასიმეტრიული ბრძოლით გეოპოლიტიკური მიზნების მიღწევაა, რაც, უპირველეს ყოფლისა, მოიცავს ნატოსა და ევროკავშირის, მათი მოკავშირე ქვეყნების წინააღმდეგ კიბეროპერაციების განხორციელებას, დასავლეთის სამხედრო და ეკონომიკური პოტენციალის დაქვეითების მცდელობებს (Vasara, 2020). ამრიგად, მოსკოვისთვის კიბერსივრცე წარმოადგენს სტრატეგიულ ინსტრუმენტს გეოპოლიტიკურ ბრძოლებში უპირატესობის მოსაპოვებლად და მოწინააღმდეგის დასასუსტებლად.

რუსეთის კიბეროპერაციებზე აგრეთვე გავლენას ახდენს მისი სამხედრო, სადაზვერვო და პოლიტიკური წრეების ინსტიტუციური კულტურა. რუსეთის კიბერშესაძლებლობები ინტეგრირებულია სამხედრო-სადაზვერვო ინსტიტუტებში, რაც ხელს უწყობს კიბერშეტევების ერთიანად კოორდინირებულად წარმართვას და მათ ეფექტიანობას. საბჭოთა პერიოდის უსაფრთხოებისა და სამხედრო დოქტრინაზე დაფუძნებული კიბერსტრატეგია აგრესიულ და რისკებზე დაფუძნებულ გამოხატულად შემტევით მიდგომებს გულისხმობს.

კიბერსტრატეგიის ტრანსფორმაცია – ისტორიული პერსპექტივა



რუსეთის კიბერსტრატეგიამ აღმოცენება პოსტსაბჭოთა პერიოდის ადრეული 1990-იანი წლებიდან დაიწყო, როდესაც კიბერსივრცეში რუსეთის პოლიტიკური ოპერაციები ჯერ კიდევ ad-hoc აქტივობებით და ნაკლები ინტენსივობით ხასიათდებოდა. რუსეთის სტრატეგიული მიდგომები, კიბერშესაძლებლობები და წარმოებული კიბერშეტევები მნიშვნელოვანად შეიცვალა 1990-იანი წლებიდან დღემდე (NATO StratCom, 2021).

90-იანების პერიოდში რუსეთი ჯერ კიდევ პირველ ნაბიჯებს დგამდა კიბეროპერაციების პოტენციალის გაცნობიერების მხრივ, 2000-იანი წლებიდან კი იგი კიბეროპერაციების წარმოებისას უფრო ორგანიზებულ და ცენტრალიზებულად კონტროლირებად მიდგომაზე გადავიდა.

ბოლო ორი ათწლეულის განმავლობაში რუსეთის სამხედრო დოქტრინამ და ომის კონცეფციამ ფუნდამენტური სახეცვლილება განიცადა, მათ შორის მნიშვნელოვნად განვითარდა კიბეროპერაციების როლი და მნიშვნელობა (CNA, 2017). თუკი, ტრადიციული გაგებით, რუსეთისთვის ომის წარმოება შეიარაღებულ კონფლიქტს მოიცავდა, განახლებული კონცეპტუალური მოდელით რუსეთისთვის ომი შეიარაღებული კონფლიქტისა და არასამხედრო ზომების ერთობლიობას წარმოადგენს (NATO CCDCOE, 2020).

რა თქმა უნდა, რუსეთის მიერ საომარი მოქმედებების წარმოებისას არასამხედრო ზომის გამოყენების შემთხვევები ისტორიაში არახალია, თუმცა კონცეპტუალური ფორმა ამ მიდგომას 2000-იანი წლებიდან, უფრო მეტად კი უკრაინაში მიმდინარე მოვლენებიდან მიეცა. რუსეთის სამხედრო ელიტაში ჩამოყალიბდა კონსენსუსი, რომ ომის არაძალადობრივი ზომები შეიძლება იმდენად ეფექტიანი იყოს, რომ ომის იარაღად მათი გამოყენება უმნიშვნელოვანეს უპირატესობას იძლეოდეს.

რუსეთის ომის განახლებული კონცეპტუალური მოდელი დასავლეთის მიერ სხვადასხვა ტერმინებით გამოიხატება, როგორებიცაა: “ჰიბრიდული ომი”, “საინფორმაციო ომი”, “ახალი თაობის ომი”, “გერასიმოვის დოქტრინა” და ა.შ. ყველა ზემოაღნიშნული ტერმინი კი მიუთითებს ომის წარმოების არასამხედრო ზომებზე გადასვლას (GFSIS, 2023).

რუსული კიბერსტრატეგიის გააზრებისთვის მნიშვნელოვანია მისი ოფიციალური შეხედულებების გაანალიზება ინფორმაციულ ომსა და კიბერუსაფრთხოებაზე, როგორც მის შემა-

დგენედ ნაწიდზე. რუსი სამხედრო ექსპერტები კიბერუსაფრთხოებას განიხიდავენ (ისევე, როგორც ეს ანაღიტიკურ დოკუმენტებშია განმარტებული) როგორც დასავლური ცნებას და ძირითადი ფოკუსი გადმოაქვთ ინფორმაციულ ომსა და ინფორმაციულ უსაფრთხოებაზე (NATO CCDCOE. 2020).

ბოღო ათწღეულებში საინფორმაციო ომის მნიშვნელობა სულ უფრო და უფრო იზრდება, რაც პირდაპირ ისახება რუსეთის ფედერაციის სტრატეგიებში და რადიკაღურად ცვღის ქვეყნის სამხედრო კონცეფციას. რუსეთის გაგებით, კიბერუსაფრთხოება ინფორმაციული უსაფრთხოების შემადგენელი ნაწიდია, ხოღო ორივე ერთად კი - საინფორმაციო ომის კომპონენტი (Darczewska, 2015). სახეცვღიდი დოქტრინის თანახმად, საინფორმაციო ომი კიბერ და ინფორმაციულ ოპერაციებს მოიცავს და თანამედროვე კონფღიქტის განუყოფელი შემადგენელი ნაწიდია. კიბერსივრცე რუსეთისთვის არის მხრავაღმხრივი ინსტრუმენტი (როგორც ტექნიკური, ასევე ფსიქოღოგიური მახასიათებღებით) სახეღმწიფოთაშორისი კონფღიქტების საწარმოებღად (Chatamhouse, 2023).

რუსეთის სამხედრო დოქტრინა საინფორმაციო ომის ორ ძირითად - ტექნიკურ და ფსიქოღოგიურ მხარეებს გამოყოფს. ტექნიკური განზომიღება მოიცავს იმას, რასაც ჩვენ კიბერუსაფრთხოებას ვუწოდებთ, ხოღო ფსიქოღოგიური ნაწიდი ორიენტირებულია მოსახღეობისა და გადაწყვეტიღების მიმღები პირების კოგნიტიურ ზეგავღენაზე, რასაც შედეგად უნდა მოჰყვეს მოწინააღმდეგის ნების შესუსტება და მათი გადაწყვეტიღების მიღების პროცესებისა და სტრუქტურების დაზიანება.

რუსეთის ფედერაციის შეიარაღებული ძაღების 2011 წღის კონცეფცია ინფორმაციულ სივრცეში აქტივობების შესახებ ინფორმაციულ ომს განსაზღვრავს როგორც კონფრონტაციას, რომეღიც მიზნად ისახავს ინფორმაციული სისტემების დაზიანებას, პოღიტიკური, ეკონომიკური და სოციაღური სისტემების შესუსტებას და მოსახღეობის ფსიქოღოგიურ მანიპულაციას (NSA, 2011).

გენერაღი გერასიმოვიც ხაზს უსვამს ინფორმაციული სფეროს მნიშვნელობას, რომეღიც კრიტიკულ ინფრასტრუქტურებსა და მოსახღეობაზე დისტანციურად და ფარულად გავღენის მოპოვების საშუაღებას იძღევა (CRS, 2020). უფრო მეტიც, იგი "სამხედრო და არასამხედრო ზომების კოორდინირებული გამოყენებისას" არასამხედრო ზომებს უპირატესობას ანიჭებს და აღნიშნავს, რომ სამხედრო ძაღის ექსპღუატაცია მხოღოდ მაშინ უნდა მოხდეს, როდესაც შეუძღებეღია "არასამხედრო მეთოდებით დასახული მიზნების მიღწევა" (NATO CCDCOE, 2020).

2014 წლის განახლებულმა სამხედრო დოქტრინამ გააძლიერა ეს კონცეფცია და უფრო კონკრეტულად განსაზღვრა თანამედროვე სამხედრო კონფლიქტების მახასიათებლები, კერძოდ: "*комплексное применение военной силы, политических, экономических, информационных и иных мер невоенного характера, реализуемых с широким использованием протестного потенциала населения и сил специальных операций*" (Russian Military Doctrine, 2014).

როგორც ვხედავთ, ინფორმაციული ზომების, ICT-ის ასახვა ომის წარმოების მახასიათებლებში და დოქტრინაღურ დოკუმენტებში ცაღსახად მიგვითითებს კონცეპტუაღურ ცვლილებებზე, რომელიც განვითარდა რუსეთის სახელმწიფოებრივ აღქმაში თანამედროვე ომის შესახებ.

რუსეთისთვის საინფორმაციო ომი, მათ შორის კიბეროპერაციები, თანამედროვე კონფლიქტის განუყოფელ ნაწილად განიხილება, ტრადიციული სამხედრო ძალის გამოყენების თუ მის გარეშე. როგორც წესი, რუსეთი საინფორმაციო ომის სტრატეგიას იყენებს ოფიციაღური საომარი მოქმედებების დაწყებამდე და მის პარაღელურად, რაც მოქნილ და ფარულ საშუაღებას წარმოადგენს გავლენის მოსაპოვებლად და სტრატეგიული მიზნების მისაღწევად (NATO StratCom, 2024).

საინფორმაციო სივრცის მნიშვნელობა რუსეთის ფედერაციის ეროვნული სტრატეგიის პრიორიტეტების განხორციელების უზრუნველსაყოფად განახლებულ დოკუმენტებში სულ უფრო აქტიურად განიხილება. 2016 წლის ინფორმაციული უსაფრთხოების განახლებული დოქტრინით (Russian Information Security Doctrine, 2016) გაძლიერდა წინამორბედი კონცეპტუაღური დოკუმენტების სულისკვეთება, რომლითაც ხელახლა ხაზგასმით აღინიშნა რუსეთისთვის საინფორმაციო სივრცეში ძირითადად უცხოელი აქტორებით წარმოქმნილი მზარდი საფრთხე და მათი გავლენა სოციაღურ ღირებულებებსა და ეროვნულ სტაბილურობაზე.

სტრატეგიული დოკუმენტები რუსეთს წარმოაჩენს როგორც თავდაცვითი კიბერშესაძლებლობების განმავითარებელ ქვეყანას. ოფიციაღურ სტრატეგიულ და კონცეპტუაღურ დოკუმენტებში რუსეთის ხედვა საინფორმაციო ომის შესახებ წარმოჩენილია როგორც "აგრესიული დასავლეთის" საფრთხის ქვეშ მყოფი თავდაცვითი ძალის გამოძახილი, თუმცა რუსი სამხედრო ექსპერტების, მკვლევარების, მეცნიერების ნარატივში ნათლად ჩანს ინტერესი კიბერიარაღის შექმნის მიმართ, მისი ეფექტიანობის, საომარ მოქმედებებთან შესაბამისობისა და ხელმისაწვდომობის გამო. შემტევითი კიბერისურსების ეს

ექსპერტულ-ანალიტიკური დოკუმენტები უფრო ზუსტად ასახავს რუსეთის კიბერ და ინფორმაციული ოპერაციების გამოყენების რეალურ პრაქტიკას, რომელსაც ის თანამედროვე საომარი მოქმედებების პარალელურად ახორციელებს (NATO CCDCOE, 2020).

გარდა შიდა ეროვნული სტრატეგიული ჩარჩოს ფორმირებისა, რუსეთი მრავალი წელია აქტიურად ცდილობს საერთაშორისო არენაზე კიბერპოლიტიკის ახალი დღის წესრიგის შექმნას. აღსანიშნავია რუსეთის უწყვეტი მცდელობები, რომ გაეროს ფორმატში შექმნას კიბერაქტივობების რეგულირების ახალი საერთაშორისო სამართლებრივი ჩარჩო. ამრიგად, ინფორმაციულ ომს სტრატეგიულად მნიშვნელოვანი ადგილი უჭირავს რუსეთის სამხედრო დოქტრინაში. რუსეთის მიდგომა საინფორმაციო ომის მიმართ მჭიდროდ არის დაკავშირებული მის ფართო სამხედრო და გეოპოლიტიკურ სტრატეგიებთან. კიბერსივრცის ტექნიკური და ფსიქოლოგიური ფაქტორების კომბინაციით, რუსეთი მიზნად ისახავს ინფორმაციული უპირატესობის მოპოვებას მოწინააღმდეგეზე. ამ სტრატეგიის ცოდნა აუცილებელია რუსეთის კიბეროპერაციების განხორციელების მოტივაციის გასაგებად და ეფექტიანი კონტრზომების მისაღებად.

კიბერუსაფრთხოების ინფრასტრუქტურაში ჩარევის ტაქტიკები

როგორც ვნახეთ, რუსეთის კიბერუსაფრთხოების დოქტრინა წარმატებით ინტეგრირებულია ქვეყნის პოლიტიკურ მისწრაფებებსა და სტრატეგიული გადაწყვეტილებების მიღების პროცესში. თუკი დასავლეთი, უახლოეს წარსულამდე, კიბერსაფრთხეებს უპირატესად ტექნიკური ზომებით პასუხობდა, რუსეთისთვის კიბერსივრცის გამოყენება გაცილებით ფართო მასშტაბის ზომათა ერთობლიობას ქმნის, როგორიცაა: ინფორმაციული მანიპულაციები, დივერსია, კინეტიკური და ელექტრონული ომის კომბინაცია, დაბალი ინტენსივობის სახელმწიფოთაშორისი ოპერაციები, რომელთა მიზანი შესაძლოა ისეთი შორსმიმავალი იყოს, როგორიცაა უცხო სახელმწიფოში პოლიტიკური რეჟიმის შეცვლა. ამრიგად, რუსეთი დღეს ფართოდ იყენებს შეტევით კიბერშესაძლებლობებს პოლიტიკური ოპონენტების დასასუსტებლად, როგორც ბევრად უფრო ფართო სტრატეგიის ნაწილს.

რუსეთის კიბეროპერაციებში ჩართული აქტორები და უწყებები სამხედრო სტრატეგიის შეცვლის კვალდაკვალ განვითარდნენ.

2010-იან წლებში რუსეთი იწყებს სამხედრო კიბერსტრუქტურების ფორმირებას. მთავარ როლს კვლავ ფსბ (ფედერალური უსაფრთხოების სამსახური) და გრუ (სამხედრო დაზვერვის მთავარი დირექტორატი) ასრულებენ. მიუხედავად იმისა, რომ საწყისი ეტაპიდანვე რუსეთმა კიბერშესაძლებლობები დააფუძნა და გააერთიანა თავის სამთავრობო, სამხედრო და დაზვერვის ინსტიტუტებში, ქვეყნის უსაფრთხოების სამსახურები კიბეროპერაციების საწარმოებლად დღემდე აქტიურად იყენებენ გარე რესურსს - ჰაკერულ კრიმინალურ ქსელებს, პატრიოტ ჰაკერებს, კიბერკრიმინალებს და ისეთ კერძო ორგანიზაციებს, როგორიცაა ინტერნეტკვლევის სააგენტო (IRA) (NATO StratCom, 2021). რუსეთის სამივე სადაზვერვო სააგენტოს (FSB, GRU და SVR) გააჩნია და იყენებს შემტევით კიბერშესაძლებლობებს, მიუხედავად ბრალდებების მრავალგზის უარყოფისა (CRS, 2022).

უსაფრთხოების ფედერალური სამსახურის (FSB) კიბერშეტევების (კიბერჯაშუშობა, გამოსასყიდი პროგრამა და ფიშინგი) სამიზნე სექტორებია: ენერგეტიკა, ავიაცია, თავდაცვა და კერძო ორგანიზაციები. საგარეო დაზვერვის სამსახური (SVR) ცნობილია მაღალი დონის ტექნიკური ექსპერტიზითა და კიბერშპიონაჟით სამთავრობო და კერძო სექტორის სისტემებზე (Cybersecurity and Infrastructure Security Agency [CISA], 2024). SVR-ს უკავშირდება SolarWinds-ის კიბერთავდასხმის შემთხვევა (RCDC, 2022).

სამხედრო დაზვერვის სამსახური (GRU), როგორც წესი, მონაწილეობს ისეთ მნიშვნელოვან კიბეროპერაციებში, როგორიცაა არჩევნებში ჩარევა და თავდასხმები კრიტიკულ ინფრასტრუქტურაზე. იგი იყენებს ისეთ დაჯგუფებებს, როგორიცაა: APT28 (Fancy Bear) და Sandworm. 2015 წელს ფრანგული ტელევიზიის წინააღმდეგ კიბერშეტევაში, ისევე როგორც 2016 წელს ეროვნულ დემოკრატიულ კომიტეტზე თავდასხმასა და 2017 წელს NotPetya ვირუსის გავრცელებაში, პასუხისმგებლობა სწორედ GRU-ზე მოდის.

რუსეთი კიბეროპერაციებს მრავალფეროვანი ტექნიკებისა და ტაქტიკის ერთობლიობით ახორციელებს. სტანდარტულად, ეს ოპერაციები მოიცავს შემდეგ საფეხურებს: დაზვერვა, შეღწევა, მონაცემთა შეგროვება, ანალიზი და საბოლოო ქმედება (IISS, 2021).

კრიტიკულ ერონულ ინფრასტრუქტურებზე განხორციელებული შეტევითი კიბეროპერაციები, რომელთაც დასავლეთი რუსეთის სახელმწიფოზე მიმართავს, საკმაოდ ვრცელი და კომპლექსურია. მაგალითად:

- **კრიტიკულ საკომუნიკაციო და ეროვნულ ინფრასტრუქტურაზე წვდომის მასშტაბური უარყოფა:** 2007 წლის ესტონეთის (NATO STRATCOM, 2007), 2008 წლის საქართველოს (GFSIS, 2019), 2015 წელს უკრაინის და 2016 წელს მონტენეგროს წინააღმდეგ კიბერთავდასხმები. 2008 წელს რუსეთ-საქართველოს ომის პარალელურად განხორციელებული DDoS შეტევები ისტორიულ წყაროებში პირველ კიბერ-ომად არის მოხსენიებული. ეს ფართომასშტაბიანი კიბერთავდასხმები რუსეთის ტრადიციულ სამხედრო-პოლიტიკურ სტრატეგიასთან კიბერშესაძლებლობების არაკონვენციური მექანიზმების კომბინირების პირველი მაგალითები იყო.

- რუსეთის მიერ აშშ-ისა და დასავლეთის ქვეყნების **საარჩევნო პროცესებში კიბერშესაძლებლობებითა და ინფორმაციული კამპანიებით ჩარევა** ასევე ტრადიციად იქცა. ყველაზე თვალსაჩინო ამ თვალსაზრისით 2016 წელს აშშ-ის საპრეზიდენტო არჩევნებზე გავლენის მოხდენის მცდელობას უკავშირდება, როდესაც გრუს ორკესტრირებული ოპერაციები საარჩევნო პროცესში საზოგადოებრივი აზრის შეცვლას და ნდობის შერყევას ისახავდა მიზნად. საპრეზიდენტო და საპარლამენტო არჩევნების ირგვლივ კიბეროპერაციები (მაგალითად, 2017 წლის საფრანგეთის საპრეზიდენტო არჩევნები) შემდგომშიც გაგრძელდა. დასავლეთის ქვეყნებში პოლიტიკური და საზოგადოებრივი განხეთქილების გაღრმავება, სხვადასხვა პოლარიზებული წრეების გაჩენა, ნიჰილიზმის გაღრმავება, ფსიქოლოგიური მანიპულირება - ყოველივე ეს წინასაარჩევნო პერიოდში კიბერსივრცეში რუსეთის მართული ძალებით ხორციელდებოდა.

- **საერთაშორისო გამოძიების ჩაშლის მცდელობები**, მაგალითად: სპორტში დოპინგის გამოყენების შესახებ, მალაიზიის ავიახაზების MH17 თვითმფრინავის ჩამოგდების და გაერთიანებულ სამეფოში ქიმიური იარაღის გამოყენების შემთხვევები.

- **დეზინფორმაციული კამპანიები, არალეგალურად მოპოვებული მონაცემების სახეცვლილი ფორმით გასაჯაროება.** ყალბი/დამახინჯებული ინფორმაციის გასაჯაროება სოციალურ ქსელებში ონლაინ Proxy ძალების საშუალებით, მაგალითად, ლუგარის ლაბორატორიისა და საქართველოს ჯანდაცვის სისტემის წინააღმდეგ განხორციელებული კიბერშეტევა, მოპოვებული მონაცემების ცვლილება და ბნელ ქსელზე (Dark Web-ზე) განთავსება. რუსეთი ასევე ცნობილია დეზინფორმაციის გავრცელებისას "ტროლებისა" და "ბოტების" აქტიური გამოყენებით.

კრიტიკულ ფიზიკურ-საინფორმაციო ინფრასტრუქტურაზე შეტევები. მაგალითად: ჩრდ. ამერიკისა და ევროპის დამაკავშირებელი ინტერნეტის გადამცემ წყალქვეშა კაბელებზე წვდომის მოპოვება. რუსეთის მხრიდან ინტერნეტტრაფიკის მიყურადება ნატოს მიერ რაელურ საფრთხედ იქნა შეფასებული (Birnbaum, 2017).

კიბეროპერაციები საომარი მოქმედებების კვალდაკვალ. 2014 წლის ყირიმის ანექსიისა და აღმოსავლეთ უკრაინაში საომარი მოქმედებების პარალელურად, ისევე, როგორც 2022 წლიდან მიმდინარე საომარ მოქმედებებში, რუსეთი ფართოდ იყენებს კიბეროპერაციებს, რომლებიც მიზნად ისახავს უკრაინის კრიტიკული ინფრასტრუქტურის, სამხედრო კომუნიკაციის, ენერგოსექტორის მწყობრიდან გამოყვანას და მედიასაშუალებების განადგურებას. ამ შემთხვევებშიც რუსეთის კიბერშესაძლებლობები სამხედრო მიზნებთან მჭიდროდაა ინტეგრირებული (ChatamHouse, 2023). მხოლოდ 2020 წელს უკრაინის უშიშროების სამსახურმა უკრაინის საჯარო უწყებების ვებსაიტებზე მიმართული 103 რუსული კიბერშეტევა გაანეიტრალა. უკრაინის კიბერთავდაცვის სახელმწიფო ცენტრის სტატისტიკური ანგარიშის მიხედვით, 2022 წელს ოფიციალურად გამოვლენილი და გამოძიებული იქნა რუსეთის ან მასთან დაკავშირებული აქტორების მიერ განხორციელებული 2194 კიბერშეტევა უკრაინის კრიტიკულ ინფრასტრუქტურაზე (SCPS, 2022). კიბერთავდასხმები მიზნად ისახავდა საინფორმაციო სისტემებში შეღწევას მონაცემებით მანიპულირებისთვის ან დეზინფორმაციის განხორციელებისთვის, რათა მომხდარიყო უკრაინის ხელისუფლებისდელეგიტიმაცია (RCDC, 2022).

რუსეთის კიბეროპერაციებს ახასიათებს ძლიერი აგრესია და დაუნდობლობა. ხშირია რუსეთის შეტევები სამოქალაქო ობიექტებზე, მოსახლეობაზე და კრიტიკულად მნიშვნელოვან არასამხედრო ინფრასტრუქტურაზე (Cyber Peace Institute, 2023). მაგალითისთვის საკმარისი იქნება NotPetya-ს წინააღმდეგ კიბერშეტევაც, რომელიც დღემდე ყველაზე დიდი ზიანის (10 მილიარდ დოლარზე მეტი) მომტანი აღმოჩნდა დასავლეთის არაერთი ქვეყნის საჯარო და კერძო სექტორისთვის.

დასკვნა

რუსეთის საინფორმაციო ომის კონცეფცია და კიბეროპერაციების განმახორციელებელი დანაყოფები, სავარაუდოდ, სამომავლოდაც მოახდენენ გავლენას ეროვნული უსაფრთხოების პოლიტიკასა და სტრატეგიაზე (IISS, 2021). რუსეთის საინფორმაციო ომის დოქტრინის კიბერთავდაცვითმა ხასიათმა და შეტევითი კიბერშესაძლებლობების ოფიციალურმა არაღიარების პოლიტიკამ (Interfax, 2017) შეიძლება კიდევ უფრო გააძლიეროს რუსეთის მხრიდან შეტევითი აგრესიული კიბეროპერაციები, თავდასხმითი კიბერშესაძლებლობების არქონის შესახებ ნარატივის პარალელურად.

რუსეთ-უკრაინის ომის დასრულების შედეგები, რა თქმა უნდა, მნიშვნელოვან გავლენას იქონიებს რუსეთის კიბერსტრატეგიის შემდგომ განვითარებაზე (NATO CCDCOE, 2023). რუსეთის სახელმწიფოს მიერ დაფინანსებული კიბერსაფრთხის აქტორები კვლავ გააგრძელებენ ოპერაციებს უკრაინაში რუსული არმიის სტრატეგიული და ტაქტიკური მიზნების მისაღწევად. მიუხედავად იმისა, რომ რუსული კიბერ აქტივობა ძირითადად უკრაინაში არსებულ სამიზნეებზეა ორიენტირებული, დასავლეთსა და, ზოგადად, უკრაინის მხარდამჭერ ქვეყნებში დიდია აღბათობა მსგავსი ხასიათის კიბეროპერაციების გავრცელების (RCDC, 2023).

მიუხედავად შეიარაღებული კონფლიქტის შედეგებისა და რუსეთის კიბერშესაძლებლობების თეორიული დასუსტების შესაძლებლობის, ზედმეტად ოპტიმისტური იქნება ვარაუდი, რომ რუსეთი შეამცირებს აგრესიულ პოლიტიკას დასავლეთის მიმართ, მათ შორის კიბერსივრცის გამოყენებით საკუთარი საგარეო პოლიტიკური კურსის გატარებას.

რუსეთის გამარჯვების ყველაზე ნეგატიური სცენარის შემთხვევაშიც კი აუცილებლად უნდა ვივარაუდოთ, რომ გახშირდება დესტაბილიზაციისკენ მიმართული ინციდენტები, საფრთხეები და შეტევები დასავლეთის კიბერინფრასტრუქტურაზე. გაიზრდება ფოკუსი კიბერშესაძლებლობების გამოყენებით სტრატეგიული მიზნების მიღწევაზე.

კონფლიქტის უშედეგოდ გაგრძელებისას ასევე სავარაუდოა რეგიონში მაღალი დაძაბულობის და არასტაბილური კიბერგარემოს შენარჩუნება, ხოლო წაგების შემთხვევაშიც კი არ არსებობს კიბერსივრცეში სიმშვიდის მიზეზი, ვინაიდან დამარცხებული რუსეთის სტრატეგია კვლავ მიმართული იქნება კიბეროპერაციებით წარმატების მოპოვების, რეპუტაციის აღდგენის და გლობალური ლიდერის როლის წარმოჩენისკენ. მით უმეტეს,თუკი

სანქციები და ომის დანაკარგები მნიშვნელოვნად შეამცირებს რუსეთის კონვენციურ სამხედრო რესურსებს, ის აუცილებლად შეეცდება ძალების აღდგენამდე კიბერსივრცე გამოიყენოს როგორც საომარი ველი.

ამრიგად, რუსეთის პოსტსაომარი მოქმედებების შესაძლებლობების სურათი დიდი ოპტიმიზმის საშუალებას არ გვიტოვებს. რუსეთი შეინარჩუნებს კიბერშესაძლებლობებს და აქტიურად გააგრძელებს შეიარაღებული თავდასხმის მსგავს/ტოლფას ან უფრო ნაკლები ინტენსივობის კიბერშეტევებს ნატოს, ევროკავშირის და მათი მოკავშირე ქვეყნების მიმართ პოლიტიკური სტაბილურობის დარღვევისა და კრიტიკული ინფრასტრუქტურების დაზიანების მიზნით.

რუსეთი თავისი მიზნების მიღწევის პროცესში შეეცდება მოძებნოს ახალი მოკავშირეები (მაგალითად ჩინეთი, რომელიც ცდილობს დაიმკვიდროს ადგილი ევროპის გეოპოლიტიკურ სივრცეში) და დაიხმაროს მათი კიბერ/სამხედრო შესაძლებლობები, რაც პოტენციურად მეტ ზიანს მოუტანს დასავლეთს (Ibid).

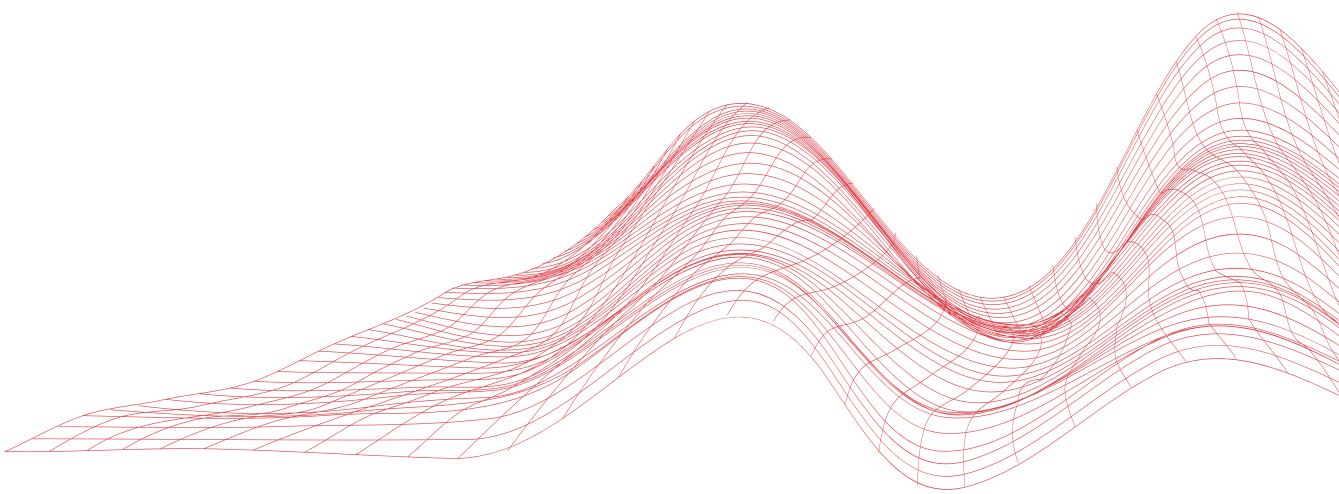
ამ შესაძლო სამომავლო სცენარების გათვალისწინებით და იმ მოცემულობის მიღებით, რომ რუსეთის კიბერაგრესია, უკრაინაში ომის შედეგების მიუხედავად, დღის წესრიგში დარჩება, აუცილებელია დასავლეთის ქვეყნების ერთობლივი ძალისხმევის გაძლიერება კიბერშესაძლებლობების ოპტიმიზაციის თვალსაზრისით (Center for European Policy Analysis, 2023). კერძოდ:

- მეტი და უფრო აქტიური თანამშრომლობა ნატოსა ევროკავშირის წევრი და პარტნიორი ქვეყნების მთავრობებს, კერძო სექტორს, აკადემიის წარმომადგენლებსა და საერთაშორისო ორგანიზაციებს შორის. ქვეყნებს შორის თანამშრომლობა და ინფორმაციის გაზიარება მკვეთრად აუმჯობესებს კოლექტიურ კიბერუსაფრთხოებას.

- მნიშვნელოვანია ფოკუსის გადატანა კიბერინციდენტებზე რეაგირებიდან პრევენციულ და პროაქტიულ ღონისძიებებზე და შესაბამისი აქტივობების მხარდამჭერ მოკლევადიან ტაქტიკებსა და გრძელვადიან სტრატეგიებზე. მნიშვნელოვანია რუსეთის კიბერსტრატეგიისა და ბოლოდროინდელი შეტევებიდან რუსეთის კიბერშესაძლებლობების, დაზვერვის, ტაქტიკისა და ინსტრუმენტების გაანალიზება, დასკვნების გამოტანა და აღნიშნულზე მორგებული თავდაცვითი, რეაგირებისა და პრევენციული კიბერსტრატეგიების ჩამოყალიბება.

- კრიტიკულად საჭიროა კიბერთავდაცვითი და კიბერშეტევითი შესაძლებლობების განვითარება, რეაგირების ეფექტიანი ღონისძიებების პარალელურად.

- და ბოლოს, აუცილებელია მიმდინარე კიბეროპერაციების მარეგულირებელ ჩარჩოში მოქცევა ნატოს უსაფრთხოების პოლიტიკის გათვალისწინებით.



ბიბლიოგრაფია

Vasara, A. (2019) Theory of Reflexive Control: Origins, Evolution, and Application in the Framework of Contemporary Russian Military Strategy. Finnish National Defence University
https://www.doria.fi/bitstream/handle/10024/176978/Vasara_FDS22_Theory%20of%20Reflexive%20Control%20%28web1%29-1.pdf?sequence=3&isAllowed=y

NATO Strategic Communication Center of Excellence (2021) Russia's Strategy in Cyberspace
https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf CAN (2016) Russia's Approach to Cyber Warfare
https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf

4. NATO CCDCOE (2020) The Past, Present and Future of Russia's Cyber Strategy and Forces
https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf

Georgian Foundation for Strategic and International Studies (2020) HYBRID WARFARE AND RUSSIA'S MODERN WARFARE
https://gfsis.org.ge/files/library/opinion-papers/201-expert-opinion-eng.pdf

NATO CCDCOE (2020) 12th International Conference on Cyber Conflict
https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf

Center for Eastern Studies (2019) The devil is in the details: Information warfare in the light of Russia's military doctrine.
https://www.files.ethz.ch/isn/191967/pw_50_ang_the-devil-is-in_net.pdf

Chatham House (2023) Russian Cyber and Information Warfare in Practise https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/summary

Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (2011)
https://nsarchive.gwu.edu/document/17098-russian-government-conceptual-views-regarding

Congressional Research Service (2016) Russian Armed Forces: Military Doctrine and Strategy
https://crsreports.congress.gov/product/pdf/IF/IF11625

Военная доктрина Российской Федерации (2014)
https://rg.ru/documents/2014/12/30/doktrina-dok.html

NATO Strategic Communication Center of Excellence (2021) Analysis of Russia's Information Campaign
https://stratcomcoe.org/publications
Доктрина информационной безопасности Российской Федерации (2014)
http://www.kremlin.ru/acts/bank/41460/page/1

NATO's Strategic Communications Center of Excellence (2020) Russia's Cyber Policy Efforts in the United Nations
https://ccdcoe.org/library/publications/russias-cyber-policy-efforts-in-the-united-nations/

NATO Strategic Communication Center of Excellence (2021) Russia's Strategy in Cyberspace
https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210

Congressional Research Service (2016) Russian Cyber Units.
https://crsreports.congress.gov/product/pdf/IF/IF11718

CISA SVR-Affiliated Activity. (2020)
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

RCDC (2020) Russian Use of Offensive Cyber Capabilities.
https://www.nksc.lt/doc/rkgc/Report_Russian_Use_of_Offensive_Cyber_Capabilities_in_UA.pdf

International Institute of Strategic Studies (2020) Russia – Cyber Capabilities and National Power
https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---russia.pdf

NATO STRATCOMCOE (2007) Cyber Attacks on Estonia
https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

GFSIS (2008) Cyber Dimension of the 2008 Russo-Georgian War
https://gfsis.org/en/the-cyber-dimension-of-the-2008-russia-georgia-war

Birnbaum, M. (2017) Russian Submarines Are Prowling Around Vital Undersea Cables, Washington Post.
https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html

Chatham House (2023) Russian Cyber and Information Warfare in Practice
https://www.chathamhouse.org/sites/default/files/2023-12/2023-12-14-russian-cyber-info-warfare-giles.pdf

Ukrainian State Cyber Defence Center (2020)
https://scpc.gov.ua/en

CyberPeace Institute (2020) Cyber Attacks in Times of Conflict
https://cyberconflicts.cyberpeaceinstitute.org

Kremlin Official Denial of Cyber Offensive Capabilities (2016)
https://www.interfax.ru/russia/545066

NATO CCDCOE (2021)Preparing for a Post-Armed Conflict Strategic Environment
https://ccdcoe.org/library/publications/preparing-for-a-post-armed-conflict-strategic-environment/

CEPA (2021) Time to Strike Back Against Russia's Shadow War
https://cepa.org/article/time-to-strike-back-against-russias-shadow-war/