RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

სამხედრო კიბეროპერაციები, როგორც რუსეთის იარაღი ევროპის ქვეყნებში პოლიტიკური დღის წესრიგის შესაცვლელად

მამუკა კირკიტაძე

149

ექსპერტის აზრი

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

ექსპერტის აზრი

მამუკა კირკიტაძე

სამხედრო კიბეროპერაციები, როგორც რუსეთის იარაღი ევროპის ქვეყნებში პოლიტიკური დღის წესრიგის შესაცვლელად

149

2020

პუბლიკაცია დაიბეჭდა ამერიკის შეერთებული შტატების საელჩოს ფინანსური მხარდაჭერით. გამოცემაში გამოთქმული მოსაზრებები ეკუთვნის ავტორებს და შეიძლება არ ასახავდეს საელჩოს თვალსაზრისს.

ტექნიკური რედაქტორი: არტემ მელიქ-ნუბაროვი

ISSN 1512-4835
ISBN 978-9941-8-2772-3

შესავალი

ბოლო წლებში კიბეროპერაციები რუსეთისთვის პოლიტიკური, ეკონომიკური და სამხედრო მიზნების მისაღწევ ეფექტურ საშუალებად ჩამოყალიბდა. პუტინის რეჟიმისათვის ეს არის იარაღი, რომელიც ქვეყნის შიგნით ოპოზიციური ლიდერების ჩასახშობად, ხოლო საერთაშორისო არენაზე უცხო ქვეყნებზე ზემოქმედებისათვის გამოიყენება.

მოსკოვი კიბერთავდასხმებსა და შპიონაჟს ომის ნაწილად მოიაზრებს, რაც ნათლად აისახა გენერალური შტაბის უფროსის, ვალერი გერასიმოვის 2013 წელს გაკეთებულ მოხსენებაში[1], სადაც იგი პოლიტიკური და სტრატეგიული მიზნების მისაღწევად არასამხედრო ჰიბრიდული მეთოდების მნიშვნელობაზე საუბრობს.

შეიძლება ითქვას, რომ კიბერშპიონაჟი რუსეთისთვის არახალი დისციპლინაა. საბჭოთა კავშირის დროს სსრკ-ის სახელმწიფო უშიშროების კომიტეტი (Комите́т госуда́рственной безопа́сности СССР), ცნობილი, როგორც „კაგებე“, დასავლეთის წინააღმდეგ მიმართული სადაზვერვო საქმიანობისთვის აქტიურად იყენებდა მაღალი დონის ტექნიკურ საშუალებებს, მათ შორის, რადიოელექტრონულ დაზვერვას (SIGINT). საბჭოთა კავშირის დაშლის შემდეგ კაგებეს ელექტრონული დაზვერვის ფუნქციები რუსეთის სადაზვერვო სამსახურებში გადანაწილდა და თანამედროვე საინფორმაციო ტექნოლოგიებთან ადაპტირდა.

დღეისათვის კრემლის სადაზვერვო სამსახურებში მრავალი კიბერდანაყოფია, რომლებიც სხვადასხვა მიზანს ემსახურება. ამ მხრივ განსაკუთრებით აქტიურია შეიარაღებული ძალების გენერალური შტაბის მთავარი სამმართველო (Гла́вное управле́ние Генера́льного шта́ба Вооружённых Сил Росси́йской Федера́ции), იგივე „გრუ“, რომელიც სამხედრო-სადაზვერვო საქმიანობასა და სამხედრო სპეცდანიშნულების რაზმების ოპერირებაზეა პასუხისმგებელი. სამმართველოს მთავარი მიზანია რუსეთის მთავრობის მაღალჩინოსნებისთვის, კერძოდ, თავდაცვის მინისტრისა და გენერალური შტაბის უფროსისთვის, სამხედრო ხასიათის დაზვერვის მიწოდება, ასევე, რუსეთის სამხედრო, ეკონომიკური და ტექნოლოგიური უსაფრთხოების უზრუნველყოფა. „გრუ“ ასევე კინეტიკური და ციფრული საშუალებების გამოყენებით ახორციელებს ფარული ჯაშუშობის, საინფორმაციო და დივერსიულ ოპერაციებს. მისი ქოლგის ქვეშ მოქმედი ჰაკერული დაჯგუფებები Sofacy/Fancy Bear[2] და Sandworm[3] არაერთხელ გახდნენ საერთაშორისო თანამეგობრობის კრიტიკის საგანი.

ქვემოთ განხილულია შემთხვევები, რომელთა მაგალითზეც კარგად ჩანს, თუ როგორ იყენებს რუსეთი სადაზვერვო სამსახურ „გრუსთან“ აფილირებულ ჰაკერულ დაჯგუფებებს ევროპის ქვეყნებში სასურველი პოლიტიკის გასატარებლად.

ჩეხეთი

ჩეხეთისა და რუსეთის დიპლომატიური ურთიერთობები არაერთხელ ყოფილა დაბალ ნიშნულზე, თუმცა ბოლო წლების განმავლობაში ორ ქვეყანას შორის ურთიერთობა საგრძნობლად დაიძაბა.

წელს პრაღაში, რუსეთის საელჩოს წინ მოედანს სახელი გადაერქვა და მოკლული რუსი ოპოზიციონერის – ბორის ნემცოვის სახელი ეწოდა. საელჩოს ახლოს გაიხსნა ასევე კრემლის კიდევ ერთი კრიტიკოსის, რუსი ჟურნალისტ ანა პოლიტკოვსკაიას სახელობის ხეივანი.

ჩეხეთის დედაქალაქში განხორციელებული ეს „პროვოკაციული ქმედებები“ კრემლის უკმაყოფილების მიზეზი გახდა, თუმცა მოსკოვის აღშფოთება საბჭოთა სამხედრო მარშლის – ივან კონევის ძეგლის დემონტაჟმა გამოიწვია და ამ ორ ქვეყანას შორის დაძაბულობა ცივი ომის დასრულების შემდეგ ყველაზე მაღალ წერტილამდე მივიდა. რუსეთის თავდაცვის მინისტრ სერგეი შოიგუს წარუმატებელ მცდელობას, სამშობლოში დაებრუნებინა საბჭოთა მარშლის ძეგლი, კრემლის მხრიდან საპასუხო ნაბიჯები მოჰყვა.

ძეგლის დემონტაჟიდან რამდენიმე დღეში ჩეხეთის საავადმყოფოებსა და აეროპორტზე ფართომასშტაბიანი კიბერთავდასხმა განხორციელდა, რომლის უკან, სლოვაკეთის ინტერნეტუსაფრთხოების კომპანიის (ESET) თქმით,[4] რუსეთის კვალი გამოიკვეთა.

აღსანიშნავია, რომ ასეთი კიბერშეტევები წარსულშიც არაერთხელ მომხდარა. ჩეხეთის უსაფრთხოების საინფორმაციო სამსახურის (BIS) 2017 წლის ანგარიშის მიხედვით, კრემლთან დაკავშირებული ორი კიბერჯაშუშური დაჯგუფება თურლა და APT28 2016-2017 წლებში საგარეო საქმეთა და თავდაცვის სამინისტროს, ასევე, ჩეხეთის არმიის ვებგვერდებზე კიბერშპიონაჟის კამპანიას ეწეოდა.[5]

ჩეხეთში განხორციელებული კიბერაგრესია ერთგვარი დეჟავუა. 2007 წელს ესტონეთში სწორედ საბჭოთა ძეგლის აღებას მოჰყვა რუსეთისაგან ფართომასშტაბიანი, კოორდინირებული

კიბერთავდასხმების კამპანია, რომელიც 3 კვირას გაგრძელდა და ქვეყანას სერიოზული ეკონომიკური ზიანი მოუტანა.

მოსკოვისთვის საბჭოთა კავშირი და მასთან დაკავშირებული ყველა დეტალი ისტორიულ სიდიადესთან ასოცირდება, ამიტომ გასაკვირი არაა, რომ „სამხედრო დიდების სიმბოლოების“ „შეურაცხყოფას“ სადამსჯელო ქმედებებით პასუხობს.

მონტენეგრო

რუსეთმა მონტენეგროს შიდა საქმეებში აქტიურად ჩარევა მას შემდეგ დაიწყო, რაც ქვეყანამ ჩრდილოატლანტიკურ ალიანსში გაწევრიანების მზადყოფნა გამოთქვა.[6] კრემლისთვის პოდგორიცა ყოველთვის წარმოადგენდა ინტერესის სფეროს, ნატოსთვის კი თავის რიგებში მონტენეგროს დამატება სტრატეგიული მნიშვნელობის სვლად შეიძლება მივიჩნიოთ. ცხადია, ქვეყანა, რომლის ჯარიც, სულ რაღაც, 2000 კაცისგან შედგება,[7] ნატოსთვის, სამხედრო თვალსაზრისით, მინიმალურ დანამატს წარმოადგენს, თუმცა სტრატეგიულად ბალკანეთის ამ პატარა ქვეყნის თავის რიგებში მიღება ჩრდილოატლანტიკურ ალიანსს სრულ კონტროლს ანიჭებს ადრიატიკის ზღვაზე მაშინ, როცა ადრიატიკის ზღვის დანარჩენი ქვეყნები, ალბანეთი, ხორვატია და იტალია, უკვე არიან ნატოს წევრები.

კრემლისთვის „გრუს“ მართული ოპერაციები გადამწყვეტ როლს ასრულებდა მონტენეგროში პრორუსული მთავრობის მოსასვლელად და ქვეყნის ჩრდილოატლანტიკური გეზის შესაცვლელად.

საპარლამენტო არჩევნებამდე სამი დღით ადრე „გრუს“ ოპერატორებმა მონტენეგროს მედიასაიტებზე, უმსხვილეს ტელეკომზე, არჩევნებზე მომუშავე არასამთავრობო ორგანიზაციებსა და სამთავრობო საიტებზე დაბალტექნოლოგიური, მაგრამ ეფექტური კიბერშეტევა განახორციელეს, რომელიც არჩევნების ხელშეშლას და ქვეყნის ჩრდილოატლანტიკური ალიანსისკენ მიმავალი გზიდან გადახვევას ემსახურებოდა.[8]

მონტენეგროს პოლიტიკური და სოციალური გარემოს კიბერსაშუალებებით მანიპულირების გარდა, კრემლი დაფინანსების გზით ოპოზიციის, პოლიტიკური ჯგუფების, სასულიერო პირების გადაბირებას და არჩევნების დისკრედიტაციას ცდილობდა.[9] საქმეში ასევე ჩაერთნენ „გრუს“ ოპერატორები, რომლებიც, სავარაუდოდ, პარლამენტზე თავდასხმას, პრემიერ-მინისტრის მოკვლას და

სამოქალაქო არეულობის მოწყობას გეგმავდნენ, მაგრამ მონტენეგროს სამართალდამცავებმა მათი აყვანა ოპერატიულად შეძლეს.[10] 2019 წელს მონტენეგროს სასამართლომ, სახელმწიფო გადატრიალების ბრალდებით, 20-მდე ადამიანს პატიმრობა შეუფარდა, მათ შორის, რუსეთის ორ მოქალაქეს – ედუარდ შიშმაკოვსა და ვლადიმირ პოპოვს დაუსწრებლად მიესაჯათ 15 წლამდე თავისუფლების აღკვეთა. გამოძიებამ დაადგინა, რომ შიშმაკოვი და პოპოვი „გრუს“ დაზვერვის ოფიცრები იყვნენ, რომლებმაც ვერშემდგარი სახელმწიფო გადატრიალების შემდეგ მონტენეგროს ტერიტორია სერბი მაღალჩინოსნების დახმარებით დატოვეს.[11]

დანია

თუ დანიის თავდაცვის სადაზვერვო სამსახურის (DDIS) ბოლო 10 წლის რისკების შეფასების ანგარიშებს გადავხედავთ, დავინახავთ, რომ კოპენჰაგენისთვის რუსეთიდან მომდინარე საფრთხეების გვერდით მოწინავე ადგილს იკავებს კიბერთავდასხმები და საინფორმაციო ოპერაციები, რომლებმაც შეიძლება ქვეყნის ეროვნულ უსაფრთხოებაზე იქონიოს სერიოზული გავლენა. დანია, როგორც ჩრდილოატლანტიკური ალიანსის ერთ-ერთი დამფუძნებელი ქვეყანა, რუსეთისთვის ყოველთვის წარმოადგენდა ინტერესის სფეროს.

კოპენჰაგენი კრემლის სადაზვერვო სამსახურის რადარზე აქტიურად 2014 წელს მოექცა, მაშინ, როდესაც დანიამ მზადყოფნა გამოთქვა ნატოს სარაკეტო თავდაცვის სისტემას შეერთებოდა.[12] ამ გადაწყვეტილებამ, რა თქმა უნდა, რუსეთის აღშფოთება გამოიწვია. მიხეილ ვანინმა, რუსეთის იმდროინდელმა ელჩმა, ნაცადი ხერხით – მუქარით სცადა დანიელების იძულება გადაწყვეტილებისთვის გადაეხედათ და აღნიშნა, რომ თუ კოპენჰაგენი ნატოს სარაკეტო თავდაცვის სისტემას შეუერთდებოდა, მაშინ ბალტიის ზღვაში დისლოცირებული დანიური ხომალდები რუსული ბირთვული რაკეტების სამიზნე გახდებოდა.[13]

მიუხედავად რუსეთის მუქარისა, დანია ნატოს სარაკეტო თავდაცვის სისტემის შემადგენლობაში შევიდა, თუმცა მუქარიდან რამდენიმე კვირის შემდეგ კრემლმა კიბერარხებით ზემოქმედება სცადა. ორი წლის განმავლობაში „გრუს“ სადაზვერვო კიბერდანაყოფს, კერძოდ, APT28-ს, დანიის საგარეო საქმეთა და თავდაცვის სამინისტროს თანამშრომლების ელექტრონულ მისამართებზე

ჰქონდა უკანონო წვდომა, რომლის მიზანიც ჩრდილოატლანტიკურ ალიანსთან დაკავშირებული დოკუმენტების ხელყოფა, სამინისტროს თანამშრომლების შანტაჟი და გადაბირება იყო.[14]

პოლონეთი

2014 წლის ზაფხულში პოლონეთში ნატოს ბაზების გაფართოების შესახებ მსჯელობა „გრუსთვის“ საკმარისი მიზეზი გახდა, რომ პოლონეთის მთავრობისა და თავდაცვის სექტორის უკანონო მონიტორინგი დაეწყო.

ნატოს უელსის სამიტზე მიღებული გადაწყვეტილებით, რუსეთიდან მომდინარე აგრესიის შესაკავებლად, პოლონეთში გაიზარდა ნატოს საპასუხო ძალების (NRF) დანაყოფები, რომლის ფარგლებშიც ასევე შეიქმნა ძალიან მაღალი მზაობის ერთობლივი სამუშაო ჯგუფი (Very High Readiness Joint Task Force), რომელსაც კონვენციური ომის პირობებში, გადაწყვეტილების მიღებიდან რამდენიმე დღეში მობილიზება და გადაადგილება შეუძლია.[15] ამის საპირწონედ, რუსულ სადაზვერვო სამსახურთან აფილირებულმა ჰაკერებმა, ინფორმაციის მოპოვების მიზნით, პოლონეთის მთავრობის ათამდე საიტზე უკანონო წვდომა მოიპოვეს. რუსეთის მთავარ მიზანს აღმოსავლეთ ევროპაში განთავსებული ნატოს ჯარებიდან მომდინარე საფრთხეების მონიტორინგი და შეფასება წარმოადგენდა, რაც მეტწილად კიბეროპერაციებით განახორციელა.[16]

კრემლის ანალოგიური რეაქცია მოჰყვა პოლონეთის განცხადებას, რომ მზად იყო, რუსეთის აგრესიის შესაკავებლად ქვეყანაში განეთავსებინა ამერიკული ბაზა გაზრდილი კონტიგენტით.[17] ოფიციალური ვარშავის ამ მოულოდნელმა განცხადებამ რუსული სადაზვერვო სამსახურების საპასუხო ქმედება გამოიწვია – პოლონეთის სამთავრობო საიტების, მათ შორის, საგარეო საქმეთა და ფინანსთა სამინისტროს ვებგვერდების მავნე პროგრამით (Malware) დაინფიცირება და ქსელებზე უკანონო წვდომა. პოლონეთის უსაფრთხოების სამსახურების განცხადებით, კრემლთან აფილირებულმა ჰაკერებმა უკანონოდ შეაღწიეს პოლონეთის ელიტური სამხედრო აკადემიის ვებგვერდზე, სადაც აშშ-ის მადისკრიმინირებელი წერილი განათავსეს.[18] ყალბი წერილი აქტიურად გაშუქდა რუსულ სახელმწიფო საინფორმაციო მედიაში. ეს მავნე კამპანია მიზნად ისახავდა ევროპის მთავარ სტრატეგიულ პარტნიორ აშშ-სა და პოლონეთს შორის ურთიერთობის დაძაბვას.

უკრაინა

როგორც სხვა პოსტსაბჭოთა ქვეყნებს, რუსეთი უკრაინას ყოველთვის თავის გავლენის სფეროდ მოიაზრებდა და დღემდე აქტიურად ცდილობს მის საშინაო და საგარეო პოლიტიკაზე გავლენის მოხდენას.

2014 წელს უკრაინაში დაწყებული საპროტესტო აქციები საბოლოოდ კრემლის მიმართ ლოიალურად განწყობილი პრეზიდენტის – ვიქტორ იანუკოვიჩის ქვეყნიდან გაქცევით და საპრეზიდენტო არჩევნების ნაადრევად დანიშვნით დასრულდა, რაც რუსეთისთვის ერთმნიშვნელოვანი მარცხის მომასწავებელი იყო.

მაიდანზე, სადაც ჯერ კიდევ „ღირსების რევოლუციის" ბედი წყდებოდა, უკრაინის შემადგენლობაში შემავალი ყირიმის ნახევარკუნძული სამხედრო აგრესიის საფრთხის წინაშე აღმოჩნდა. რუსეთის 35-ათასიანმა არმიამ, რომელშიც, სხვებთან ერთად, სადაზვერვო სამსახურის – „გრუს" ელიტური სპეცდანიშნულების დანაყოფებიც შედიოდნენ, რამდენიმე დღეში შტურმით აიღეს ყირიმის რეგიონული პარლამენტი და შენობაზე რუსეთის დროშა აღმართეს. უკრაინის ნახევარკუნძულის სამხედრო ძალით მიტაცება 16 მარტს არალეგიტიმური რეფერენდუმის ჩატარებით და ყირიმის რუსეთის ტერიტორიად გამოცხადებით დასრულდა.

კრემლის მიერ ყირიმის ანექსია 25 მაისს გამართულ არჩევნებზე კიბერთავდასხმით დაგვირგვინდა. „გრუსთან" აფილირებულმა ჰაკერულმა დაჯგუფებამ (CyberBerkut) ხმის მიცემამდე ოთხი დღით ადრე უკრაინის საარჩევნო სისტემის ინფრასტრუქტურას შეუტია და საკვანძო ფაილების წაშლა დაიწყო.[19] საარჩევნო ადმინისტრაციამ ხმის მიცემის პროცედურის დაწყებამდე დროულად შეძლო მიყენებული ზიანის აღმოფხვრა, თუმცა სადაზვერვო სამსახურების კიბერდანაყოფებმა არჩევნების დღეს კვლავ შეძლეს საარჩევნო ვებგვერდზე უნებართვო შეღწევა.[20] მოქალაქეებს საიტზე შესვლისას ულტრამემარჯვენე კანდიდატ დიმიტრი იაროშის სურათი დახვდათ, რომელიც იუწყებოდა, რომ საპრეზიდენტო არჩევნებში სწორედ მან გაიმარჯვა. ეს სათავისოდ გამოიყენა რუსულმა სახელმწიფო მედიამ და აქტიურად დაიწყო მცდარი ინფორმაციის საზოგადოებისთვის მიწოდება.

მიუხედავად იმისა, რომ 2014 წლის ინციდენტმა ვერ შეძლო არჩევნების შედეგზე გავლენის მოხდენა, რუსეთმა თავის მიზანს ნაწილობრივ მაინც მიაღწია. ნატოს კიბერცენტრის ელჩის, კენეტ

გირსის თქმით, კრემლის მიერ განხორციელებული ოპერაციების მიზანი საარჩევნო პროცესის ჩაშლა და დისკრედიტაცია იყო.[21]

რუსეთის მიერ ყირიმის ანექსია და არჩევნებზე საინფორმაციო თავდასხმების მეშვეობით ზეგავლენის მოხდენა უკრაინისთვის მხოლოდ დასაწყისი აღმოჩნდა. კრემლმა აქტიურად დაიწყო უკრაინის კიბერლაბორატორიად გამოყენება, რომლის ფარგლებშიც რამდენჯერმე წარმატებით სცადა კიევის კრიტიკული ინფრასტრუქტურის ხელყოფა.[22]

პოსტსაბჭოთა ქვეყნების საცდელ ვირთხებად გამოყენება კრემლისთვის ახალი არ არის, დაუსჯელობის სინდრომი რუსეთს საშუალებას აძლევს მეზობელ ქვეყნებზე აქტიურად გამოსცადოს როგორც კინეტიკური, ისე ახალი კიბერშესაძლებლობები, რომელიც გრძელვადიან პერიოდში დასავლეთის დისკრედიტაციისკენ არის მიმართული.

საქართველო

2019 წლის 22 ოქტომბერს ამერიკის შეერთებული შტატების წარმომადგენელთა პალატამ საქართველოს მხარდამჭერი ორპარტიული აქტი დაამტკიცა, რომლის მიზანს საქართველოს დამოუკიდებლობის, სუვერენიტეტისა და ტერიტორიული მთლიანობის მხარდაჭერა წარმოადგენს.[23] საქართველოს მხარდაჭერის აქტი აშშ-ის პრეზიდენტს ავალდებულებს სანქციები დაუწესოს ყველას, ვინც რუსეთის ფედერაციის მიერ ოკუპირებულ აფხაზეთსა და ცხინვალის რეგიონში ადამიანის უფლებების დარღვევასა და საქართველოს მოქალაქეების სიცოცხლის ხელყოფაში იღებს მონაწილეობას. დოკუმენტში ასევე ლაპარაკია საქართველოს დახმარებაზე კიბერუსაფრთხოების სფეროში.[24]

მხარდაჭერის აქტის მიღებიდან 6 დღეში, 2019 წლის 28 ოქტომბერს, საქართველოში განხორციელდა ფართომასშტაბიანი კიბერშეტევა პრეზიდენტის ადმინისტრაციის, სასამართლო სისტემის, სხვადასხვა მუნიციპალიტეტის საკრებულოების, არასამთავრობო და მედია ორგანიზაციების ვებგვერდებზე, სერვერებსა და სხვა მართვით სისტემებზე. კიბერშეტევის შედეგად რამდენიმე ტელევიზიამ შეწყვიტა მაუწყებლობა.[25]

საერთაშორისო პარტნიორების დახმარებით წარმოებული ერთობლივი გამოძიებით დადგინდა, რომ კიბერთავდასხმის უკან რუსეთის ფედერაციის შეიარაღებული ძალების გენერალური შტაბის მთავარი სამმართველოს ელიტური კიბერდაჯგუფება „Sandworm"

იდგა, რომელიც არაერთი დესტრუქციული კიბეროპერაციის ავტორია.[26] თავდასხმას საერთაშორისო თანამეგობრობის უპრეცენდენტო გამოხმაურება მოჰყვა.[27]

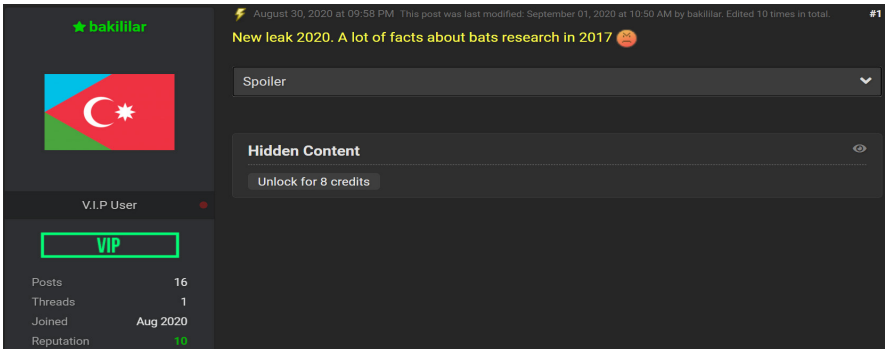
ოქტომბრის კიბერაგრესიიდან თითქმის ერთი წლის შემდეგ, 2020 წლის 1 სექტემბერს, კიბერთავდასხმა მოხდა ჯანდაცვის სამინისტროს კომპიუტერულ სისტემაზე. საქართველოს შინაგან საქმეთა სამინისტროს განცხადებით,[28] კიბერშეტევა მიზნად ისახავდა სამინისტროს ცენტრალურ აპარატსა და მის სტრუქტურულ ერთეულებში, მათ შორის, დაავადებათა კონტროლისა და რიჩარდ ლუგარის სახელობის საზოგადოებრივი ჯანდაცვის კვლევითი ცენტრის მონაცემთა ბაზებში დაცული სამედიცინო ხასიათის დოკუმენტაციისა და პანდემიის მართვასთან დაკავშირებული მნიშვნელოვანი ინფორმაციის მართლსაწინააღმდეგო დაუფლებასა და გამოყენებას. შსს-ის თქმით, კიბერშეტევის უკან ერთ-ერთი უცხო ქვეყნის სპეციალური სამსახური იდგა.

აღსანიშნავია, რომ საქართველოში ამერიკელი სენატორის, რიჩარდ ლუგარის სახელობის კვლევითი ცენტრი გახსნისთანავე გახდა კრემლის კრიტიკისა და მიზანმიმართული დეზინფორმაციის საგანი. რუსეთის ხელისუფლებასთან დაკავშირებული პირები დღემდე ღიად აკრიტიკებენ ლაბორატორიის მუშაობას და აშშ-სა და საქართველოს ხან ბიოლოგიური იარაღის დამზადებაში, ხან კიდევ საშიში ვირუსების გავრცელებაში ადანაშაულებენ. სექტემბერში განხორციელებულ კიბერთავდასხმას „უცნაურად" დაემთხვა დუმის დეპუტატ იური შვიტკინის კომენტარი, რომელიც რუსი ოპოზიციონერის, ალექსეი ნავალნის მოწამვლასთან დაკავშირებით გააკეთა. დეპუტატის თქმით, თითქოს „ნოვიჩოკის" ჯგუფის ნერვულ აგენტს რუსეთი არ აწარმოებს და მსგავსი ჯგუფის მომწამვლელი ნივთიერებები ამერიკასა და საქართველოში, კერძოდ, ლუგარის ლაბორატორიაში იქმნება.[29]

კიბერშეტევის შედეგად უკანონოდ მოპოვებული 14 GB-მდე მოცულობის დოკუმენტები უცხოურ ვებგვერდზე განთავსდა და დღემდე ხელმისაწვდომია ინტერნეტმომხმარებლებისთვის. შსს-ის თქმით, აღნიშნულ ფაილებთან ერთად ატვირთულია ფალსიფიცირებული დოკუმენტები, რომლებიც განზრახ არის გაყალბებული.

ყურადსაღებია ის ფაქტი, რომ საიტზე განთავსებული უკანონოდ მოპოვებული მასალის ავტორი მკვეთრად გამოხატულ ეროვნულ ნიშნებსა და სიმბოლოებს ატარებს. კერძოდ, მომხმარებელს პროფილის სურათად გამოყენებული აქვს ბაქოში მოქმედი სამხრეთ აზერბაიჯანის ეროვნული გამოღვიძების მოძრაობის

(SANAM) დროშა, ხოლო შერჩეული სახელით – Bakililar (ბაქოელი) თავის წარმომავლობას მკვეთრად უსვამს ხაზს. ამგავრი ქმედება, შეიძლება ე.წ False Flag ოპერაციის ნაწილი იყოს, რაც კვალის დაფარვის მიზნით და მხარის ასაქცევად ხშირად გამოიყენება. ასევე არ არის გამორიცხული ამ სვლით საქართველოს მიმართ მტრულად განწყობილი სახელმწიფო რეგიონში ჩვენს ერთ-ერთ სტრატეგიულ პარტნიორ ქვეყანასთან – აზერბაიჯანთან ურთიერთობის დაძაბვას ისახავდეს მიზნად.



ფაქტების გათვალისწინებით, შეგვიძლია ვივარაუდოთ, რომ სექტემბრის კიბერთავდასხმა რუსეთის სპეცსამსახურებთან დაკავშირებულმა ელიტურმა კიბერდაჯგუფებამ განახორციელა და მიმართული იყო კრემლის მიერ შეთხზული ლუგარის მითის გამყარების, საზოგადოების დაშინების, დაბნეულიბისა და უნდობლობის გამოწვევისკენ.

მცირე დროში საქართველოზე განხორციელებული ორი ფართომასშტაბიანი კიბერშეტევა შეიძლება სხვა ფაქტორებითაც იყოს განპირობებული.

რისი მიღწევა სცადა რუსეთმა?

ჩრდილოელი მეზობლის მიერ მართული დესტრუქციული კიბერშეტევები საქართველოს ეროვნული უსაფრთხოების ხელყოფას, სხვადასხვა სამთავრობო თუ არასამთავრობო ორგანიზაციის ფუნქციონირების შეფერხებით საზოგადოებაში მღელვარების გამოწვევას და, რაც მთავარია, წინასაარჩევნოდ ნიადაგის მოსინჯვას ისახავდა მიზნად.

რუსეთისთვის სხვა ქვეყნების შიდა პოლიტიკაში ჩარევა და ზეგავლენის მოხდენა ბოლო წლებში ჩვეულებრივ მოვლენად იქცა.

კრემლის სახელზე უკვე რამდენიმე ქვეყნის არჩევნებში ჩარევის ფაქტია გამოვლენილი, მათ შორისაა: ბრიტანეთი,[30] საფრანგეთი,[31] გერმანია,[32] ჰოლანდია,[33] ავსტრია,[34] ბელარუსია,[35] ბულგარეთი,[36] ნორვეგია[37] და აშშ[38].

ევროპარლამენტარ ვიოლა ფონ კრამონის თქმით, სასწაული იქნება, რუსეთმა ოქტომბერში დაგეგმილ არჩევნებში ჩარევა რომ არ სცადოს, რადგან ეს მათი ჩვეულებრივი ქცევაა.[39] საქართველოში გასამართ არჩევნებზე ასევე არაერთი კომენტარი გააკეთა საქართველოში ამერიკის ახლადდანიშნულმა ელჩმა კელი დეგნანმა, რომლის თქმითაც, სავარაუდოდ, რუსეთი საქართველოს არჩევნებში ჩარევას შეეცდება.[40] რუსეთის არჩევნებში ჩარევის ალბათობას კიდევ უფრო ზრდის ის ფაქტი, რომ საქართველო პროპორციული საარჩევნო სისტემისკენ მიიწევს.

საქართველოში გასამართ არჩევნებზე გამახვილდა ყურადღება ესტონეთის სადაზვერვო სამსახურის 2020 წლის ანგარიშშიც, სადაც ნათქვამია, რომ რუსეთის ინტერესის საგანი გახდება აშშ-ის საპრეზიდენტო და საქართველოს საპარლამენტო არჩევნები. ანგარიშის მიხედვით, ოფიციალური მოსკოვისთვის მნიშვნელოვანია არჩევნებში სასურველი შედეგი მიიღოს, საამისოდ კი შეეცდება მხარი დაუჭიროს ისეთ კანდიდატს, რომელიც დასავლურ პოლიტიკას რადიკალურად ემიჯნება.[41]

რას უნდა ველოდოთ ოქტომბერში?

სავარაუდოდ, ოქტომბერში კრემლი მაქსიმალურად ეცდება სხვადასხვა არხით გავლენა მოახდინოს არჩევნებზე, იქნება ეს კიბერაგრესია საქართველოს ცენტრალური საარჩევნო კომისიის ვებგვერდზე, უკვე ნაცადი ხერხით მედიაარხების მაუწყებლობის შეფერხება და საზოგადოების ინფორმაციულ ვაკუუმში მოქცევა თუ სოციალური მედიის დახმარებით კრემლისადმი ლოიალურად განწყობილი კანდიდატების პროპაგანდისტული მეთოდებით მხარდაჭერა.

აქტიურად უნდა ველოდოთ კრემლის მიერ მართულ ინტერნეტკვლევების სააგენტოს (Агентство интернет-исследований), იგივე რუსული ტროლების ფაბრიკის, ქართულ ინტერნეტსივრცეში გააქტიურებას, რომლის ძირითად მიზანს სოციალურ ქსელებში ყალბი, პროპაგანდისტული, კრემლის ნარატივს მორგებული ინფორმაციის გავრცელება წარმოადგენს. აღნიშნულ ორგანიზაციას ამოფარებული პირები თავს ესხმიან მათთვის არასასურველ პოლიტიკოსებს,

პარტიებს და სამოქალაქო საზოგადოების წარმომადგენლებს, სოციალური ქსელების მეშვეობით ახერხებენ საზოგადოებრივი აზრის სათავისოდ ტრანსფორმაციას, კრემლისთვის სასურველი მესიჯების შეფარულად თუ ცხადად მოქალაქეებში გავრცელებას.

წინასაარჩევნოდ გაზრდილი კიბერაქტივობების პარალელურად, სავარაუდოდ, გახშირდება საოკუპაციო ზოლიდან საქართველოს მოქალაქეების გატაცების და უკანონო ბორდერიზაციის ფაქტები. ასევე, ოკუპირებული აფხაზეთისა და სამაჩაბლოს ტერიტორიაზე მოსალოდნელია რუსული ჯარის გაძლიერებული სამხედრო წვრთნების ჩატარება, რითაც კრემლი ეცდება ქართველ მოსახლეობაში გააჩინოს შიშისა და დაუცველობის განცდა.

საყურადღებოა ის გარემოებაც, რომ საქართველოში გასამართი საპარლამენტო არჩევნების პარალელურად, ჩვენი მთავარი სტრატეგიული პარტნიორი – ამერიკის შეერთებული შტატები ახალი პრეზიდენტის არჩევას შეეცდება. ცხადია, ამერიკა თავის შიდა საქმეებზე მეტად კონცენტრირდება და ჩვენი ევროპელი პარტნიორების ყურადღებაც სწორედ ტრამპი-ბაიდენის დუელისკენ უფრო იქნება მიპყრობილი, ვიდრე საქართველოსკენ. ამ მოცემულობიდან გამომდინარე, რუსეთს, რა თქმა უნდა, ექნება დაუსჯელობის განცდა და ეცდება ძირგამომთხრელი ციფრული აგრესიით თუ სხვა საშუალებებით მაქსიმალურად დააზიანოს საქართველო, მავნე ქმედებებით გახლიჩოს საზოგადოება და ექსკლუზიური კონტროლი დაიბრუნოს ჩვენი ქვეყნის საშინაო და საგარეო პოლიტიკაზე.

დასკვნა

„ცივის ომის“ დასრულებისა და საბჭოთა კავშირის დაშლის შემდეგ კრემლი აქტიურად ცდილობს საერთაშორისო არენაზე წამყვანი პოზიციის დაბრუნებას, რასაც მეტწილად სადაზვერვო სამსახურების გამოყენებით ახორციელებს. დღესდღეობით, რუსეთის ფედერაცია იმ მცირე ქვეყნების ნაწილს მიეკუთვნება, რომლებმაც წარმატებით შეძლეს სამხედრო კომპონენტისთვის კიბერელემენტების მორგება. ამის ნათელი მაგალითია სადაზვერვო სამსახურებში ელიტური კიბერდივიზიების ჩამოყალიბება, რომლებიც მნიშვნელოვან როლს ასრულებენ რუსეთის საგარეო და საშინაო პოლიტიკის ფორმირებაში.

განურჩევლად გეოპოლიტიკური მდგომარეობისა თუ სტატუსისა, რუსეთი საინფორმაციო ოპერაციების დახმარებით აქტიურად ეწევა მისთვის არასასურველი ქვეყნებისა თუ პიროვნებების

დისკრედიტაციის კამპანიას. ფაქტია, კრემლისთვის პოსტსაბჭოთა ქვეყნების უმეტესობა ერთგვარ საცდელ პოლიგონს წარმოადგენს, სადაც წარმატებით სცდის როგორც სამხედრო, ისე საინფორმაციო, პროპაგანდისტულ ტაქტიკას, რაც გრძელვადიან პერსპექტივაში დასავლეთის დემოკრატიული წყობის ჩამოშლისკენაა მიმართული.

არსებული მდგომარეობიდან გამომდინარე, აუცილებელია საქართველოს მთავრობამ ადეკვატურად შეაფასოს რუსეთიდან მომდინარე საფრთხეები, მჭიდროდ ითანამშრომლოს სტრატეგიულ პარტნიორებთან და მაქსიმალურად გამოიყენოს ყველა შესაძლებლობა, რომ ნაკლები საფრთხე შეექმნას ჩვენი ქვეყნის დემოკრატიულ განვითარებას და ევროატლანტიკურ სტრუქტურებში გაწევრიანების გზას, რაც ერთადერთი სწორი ალტერნატივაა დემოკრატიული და უსაფრთხო ქვეყნის მშენებლობისთვის.

გამოყენებული ლიტერატურა

1. Герасимов Валерий, Ценность науки в предвидении, February 26, 2013. Еженедельник ВПК.www.vpk-news.ru/articles/14632
2. CrowdStrike, February 12, 2019. Who is FANCY BEAR (APT 28)? www.crowdstrike.com/blog/who-is-fancy-bear
3. Vanity Fear, October 29, 2019. INSIDE THE DISCOVERY OF SANDWORM, THE WORLD'S MOST DANGEROUS HACKERS. www.vanityfair.com/news/2019/10/the-discovery-of-sandworm-the-worlds-most-dangerous-hackers
4. Russian hackers may be behind cyber attacks on Czech hospitals, says ESET, April 22, 2020. https://news.expats.cz/weekly-czech-news/russian-hackers-may-be-behind-cyber-attacks-on-czech-hospitals-says-eset/
5. ZDNet, Czech Republic blames Russia for multiple government network hacks, December 3, 2018. www.zdnet.com/article/czech-republic-blames-russia-for-multiple-government-network-hacks/
6. European Westernt Balkans, December 28, 2016. Path to NATO: The Case of Montenegro. https://europeanwesternbalkans.com/2016/12/28/path-to-nato-the-case-of-montenegro
7. The GlobalFirepower. Montenegro Military Strength 2020. www.globalfirepower.com/country-military-strength-detail.asp?country_id=montenegro
8. Georgi Gotev, Euractiv, October 17, 2016. Montenegro hit by cyber-attacks on election day. www.euractiv.com/section/global-europe/news/montenegro-hit-by-cyber-attacks-on-election-day/
9. Heather A. Conly, May 14, 2019. Russian Malign Influence in Montenegro: The Weaponization and Exploitation of History, Religion, and Economics. Center for Strategic and International Studies. www.csis.org/analysis/russian-malign-influence-montenegro
10. Andrew E. Kramer and Joseph Orovic, May 9, 2019. Two Suspected Russian Agents Among 14 Convicted in Montenegro Coup Plot. New York Times. www.nytimes.com/2019/05/09/world/europe/montenegro-coup-plot-gru.html
11. AP News, May 9, 2019, 2 Russian spies sentenced in Montenegro in coup attempt https://apnews.com/9782460f2ca943cca88b628405033c2c
12. The Local, August 22, 2014, Denmark will join Nato's missile defense system. www.thelocal.dk/20140822/denmark-will-join-natos-missile-defense-system
13. Teis Jense, March 22, 2015, Russia threatens to aim nuclear missiles at Denmark ships if it joins NATO shield. www.reuters.com/article/us-denmark-russia/russia-threatens-to-aim-nuclear-missiles-at-denmark-ships-if-it-joins-nato-shield-idUSKBN0MI0ML20150322
14. Neil MacFarquhar, April 24, 2017. Denmark Says 'Key Elements' of Russian Government Hacked Defense Ministry. www.nytimes.com/2017/04/24/world/europe/russia-denmark-hacking-cyberattack-defense-ministry.html

15. Government of Poland, Poland in NATO - more than 20 years. www.gov.pl/web/national-defence/poland-in-nato-20-years

16. A Trend Micro Research Paper, 2016, Operation Pawn Storm Using Decoys to Evade Detection. www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf

17. Harriet Alexander, 2018. Poland asks Donald Trump to establish permanent US military base to counter Russian aggression. www.telegraph.co.uk/news/2018/05/30/poland-asks-donald-trump-establish-permanent-us-military-base/

18. Sean Lyngaas, 2020, Cyberscoop, Poland implicates Russia in cyberattack, info op aimed at undercutting U.S. relations. www.cyberscoop.com/poland-cyberattack-russia-us-military/

19. Mark Clayton, 2014, Ukraine election narrowly avoided 'wanton destruction' from hackers www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

20. Gabe Joselow, 2016, Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past. www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246

21. იქვე.

22. Andy Greenberg, 2017, Wired ,How an Entire Nation Became Russia's Test Lab for Cyberwar www.wired.com/story/russian-hackers-attack-ukraine/

23. U.S. Congress, 2020, H.R.598 - Georgia Support Act. www.congress.gov/bill/116th-congress/house-bill/598/text?q=%7B%22search%22%3A%5B%22H.R.598+Georgia+Support+act%22%5D%7D&r=1&s=2#HE7A4D682814743F9BFC51B27090FBBA2

24. იქვე.

25. BBC, 2019, Georgia hit by massive cyber-attack. www.bbc.com/news/technology-50207192

26. Interpressnews, 2020, Foreign Ministry: On 28 October, a large scale cyber-attack was carried out by Main Division of the General Staff of the Armed Forces of Russia. www.interpressnews.ge/en/article/105913-foreign-ministry-on-28-october-a-large-scale-cyber-attack-was-carried-out-by-main-division-of-the-general-staff-of-the-armed-forces-of-russia

27. Civil.ge, 2020, At UN Security Council, Estonia, UK, U.S. Condemn Russian Cyberattack on Georgia, https://civil.ge/archives/341090

28. Ministry of Internal Affairs of Georgia, Statement Of The Ministry Of Internal Affairs Of Georgia, September 03, 2020. https://police.ge/en/saqartvelos-shinagan-saqmeta-saministros-gantskhadeba/13926

29. РИА Новости, Депутат напомнил о лабораториях по изготовлению «Новичка» в Грузии и США, October 02, 2020. www.ria.ru/20200902/novichok-1576642485.html

30. Kate Holton, Guy Faulconbridge, 2017, Reuters, UK investigates Brexit campaign funding amid speculation of Russian meddling. www.reuters.com/article/us-britain-eu-investigation/uk-investigates-brexit-campaign-funding-amid-speculation-of-russian-meddling-idUSKBN1D157I

31. Ken Gude, 2017, Center for American Progress, Russia's 5th Column, www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-colum/

32. Financial Times, Nationalist AfD make historic breakthrough in German elections, www.ft.com/content/d18213e0-a105-11e7-b797-b61809486fe2

33. Andrew Higgins, 2017, New York Times, Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote. www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html?mcubz=1

34. DW, 'Putin's friends' in Austria's right-wing FPÖ achieve strong election result, www.dw.com/en/putins-friends-in-austrias-right-wing-fp%C3%B6-achieve-strong-election-result/a-40960928

35. Andrei Makhovsky, 2020, Reuters, Belarus accuses Russia of election meddling, seeks talks with Putin www.reuters.com/article/us-belarus-election-meddling/belarus-accuses-russia-of-election-meddling-seeks-talks-with-putin-idUSKBN23W1J0

36. RFE/RL, 2016, Bulgaria Faces Uncertainty After Election Of Pro-Russia President www.rferl.org/a/bulgaria-president-radev-pro-russia/28114949.html

37. NTB/The Local, 2017, Norway's Labour Party was hacked by Russia: report www.thelocal.no/20170203/norways-labour-party-was-hacked-by-russia-report

38. ABIGAIL ABRAMS, 2019, Time, What We Know So Far About Russia's 2016 Meddling https://time.com/5565991/russia-influence-2016-election/

39. On.ge, 2020, saswauli iqneba, ruseTma am arCevnebSi Careva rom ar scados, es maTi Cveulebrivi qcevaa — evroparlamentari

40. On.ge, 2020 ar maqvs konkretuli mtkicebulebebi, Tumca ruseTi albaT Seecdeba saqarTvelos arCevnebSi Carevas — degnani

41. International Security and Estonia 2020, www.valisluureamet.ee/pdf/raport-2020-en.pdf