RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

რუსეთის კიბერაქტივობები – მზარდი საფრთხე საქართველოსათვის

ანდრო გოცირიძე

95

ექსპერტის აზრი

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

ექსპერტის აზრი

ანდრო გოცირიძე

რუსეთის კიბერაქტივობები – მზარდი საფრთხე საქართველოსათვის

95

2018

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 978-9941-27-873-0

კიბერსივრცეში მიმდინარე ოპერაციები წარმოადგენს კომპიუტერული ქსელებისა და ელექტრონული სერვისების კონფიდენციალურობის, ერთიანობისა და ხელმისაწვდომობის დარღვევისა და ხელყოფის განზრახ მცდელობას. ასეთი ქმედება შესაძლოა მიზნად ისახავდეს როგორც სერვისის დაზიანებას ან შეფერხებას, ისე კომპიუტერული ქსელის გამოყენებას თავდასხმის მიზნით, ინფორმაციის მოპოვებას და მონაცემთა ბაზებზე არასანქცირებულ წვდომას. უკანასკნელ ათწლეულში კიბეროპერაციები, გარდა ტექნიკური ეფექტის მისაღწევი ქმედებებისა, გამოიყენება *ღია ან ფარული არხების მეშვეობით სამიზნე აქტორის აღქმის სასურველი მიმართულებით შესაცვლელად.*

კიბერდომეინი საჰაერო, სახმელეთო, საზღვაო და კოსმოსურის გვერდით დაპირისპირების მეხუთე სივრცედ დამკვიდრდა. კიბერელემენტების გამოყენება პოლიტიკური, ეკონომიკური თუ სამხედრო მიზნების მისაღწევად, გეოპოლიტიკური უპირატესობის მოსაპოვებლად, თანამედროვე მსოფლიოს რეალობაა. არსებული მონაცემებით, ორმოცამდე სახელმწიფოს უკვე აქვს კიბერშეტევითი პოტენციალი და წარმატებით ავითარებს მას. კიბერელემენტი დღეისათვის უკვე იქცა ყველა ომის, კონფლიქტისა თუ დაპირისპირების მნიშვნელოვან შემადგენელ ნაწილად.

საქართველოსთვის, როგორც რუსეთის დაინტერესების მუდმივი ობიექტისთვის, კიბერსივრცის დაცვა საკუთარი ეროვნული უსაფრთხოებისა და თავდაცვის წინააღმდეგ გამოყენებისაგან პრიორიტეტულ მიმართულებას წარმოადგენს. კრემლი საქართველოს თავისი გავლენის სფეროდ მოიაზრებს, რის გამოც ჩვენი ქვეყანა რუსეთის ჰიბრიდული ომის სამიზნეა. რუსეთის ჰიბრიდული აქტივობები მოიცავს დიპლომატიურ, ეკონომიკურ, სამხედრო, პოლიტიკურ, კულტურულ, სოციალურ თუ რელიგიურ საინფორმაციო არეალს და აერთიანებს როგორც ტექნიკურ, ასევე ფსიქოლოგიურ ეფექტზე ორიენტირებულ კიბეროპერაციებს.

ესტონეთის, საქართველოს, უკრაინის კონფლიქტებისას, განსაკუთრებით კი, ყირიმის ანექსიის დროს, კიბერელემენტის მზარდი ინტენსივობით გამოყენება რუსეთის ბოლოდროინდელი აქტივობებსა და ჰიბრიდული ომის ტაქტიკას ინფორმაციული ოპერაციების, პროვოკაციების, კიბერთავდასხმების სამხედრო ოპერა-

ციებთან სტრატეგიული ინტეგრაციის წარმატებულ მაგალითად წარმოაჩენს. რუსეთის მონაწილეობით მიმდინარე კონფლიქტების ანალიზი ცხადყოფს, რომ იგი კონფლიქტის ტერიტორიებს იყენებს კიბერშეტევითი პოტენციალის გამოსაცდელ ერთგვარ პოლიგონად.

თუკი 2007 წელს ესტონეთის წინააღმდეგ განხორციელებული კიბერთავდასხმა „ბრინჯაოს ჯარისკაცისთვის“ – სადამსჯელო ოპერაცია და ერთგვარი პოლიტიკური გზავნილი – სამოქალაქო მღელვარების, მასობრივი არეულობის გამოწვევას ისახავდა მიზნად და პოლიტიკურ პროცესებში კიბერელემენტის გამოყენების პირველი მცდელობა იყო, უკვე მომდევნო წელს რუსეთ-საქართველოს ომში კიბერელემენტის გამოყენება უშუალოდ კონვენციური მოქმედებების კარგად ორგანიზებულ თანამდევ პროცესს წარმოადგენდა და საინფორმაციო ვაკუუმის შექმნას, დეზინფორმაციის გავრცელებას და საქართველოსათვის საერთაშორისო მხარდაჭერის არხების გადაკეტვას ემსახურებოდა. უკრაინის კონფლიქტში რუსულმა კიბერშეტევებმა კიდევ უფრო მეტი განვითარება ჰპოვეს და გარდა ტრადიციული შედეგებისა, რუსეთმა შეძლო გამოეყენებინა მსხვილი მობილური ოპერატორების შესაძლებლობა აბონენტების ფარული მოსმენებისათვის, მათი ადგილმდებარეობის განსაზღვრისა თუ სხვა მონაცემთა მიღებისათვის, რაც გამოიყენეს როგორც ფსიქოლოგიური ზემოქმედებისა და ინფორმაციის მოხსნისთვის, ისე ადგილმდებარეობის განსაზღვრისათვის საარტილერიო დარტყმის კოორდინატების გადასაცემად. გარდა ამისა, უკრაინის კონფლიქტში რუსეთი პირველად დაესხა თავს და მწყობრიდან გამოიყვანა უკრაინული ენერგოსისტემის ნაწილი.[1]

უკანასკნელი ორი წლის მანძილზე რუსეთის დესტრუქციული კიბერაქტივობები გასცდა პოსტსაბჭოთა ქვეყნების არეალს და ევროპისა თუ აშშ-ის საარჩევნო პროცესები მრავალჯერ იქცა რუსეთის სამთავრობო სტრუქტურებთან დაკავშირებული ჰაკერების სამიზნედ.

რუსეთის თავდაცვის სამინისტროს კიბერდანაყოფები, რომლებიც პასუხისმგებელი არიან შემტევი კიბერღონისძიებების ჩატარებაზე, პროპაგანდაზე ორიენტირებულ ქმედებებსა და მოწინააღმდეგის მართვისა და კონტროლის სისტემებში მავნებელი პროგრამული უზრუნველყოფის ჩანერგვაზე, საქართველოსთვის

ყველაზე რეალურ და სერიოზულ საფრთხეს შეიცავენ. რუსეთის მაღალი რანგის სამხედროებზე დაყრდნობით, საინფორმაციო ოპერაციების ჯარებმა 2016 წლის სექტემბერში პირველად მიიღეს მონაწილეობა სამეთაურო-საშტაბო სწავლებაში – „Кавказ-2016“, რაც კიდევ ერთხელ ადასტურებს რუსეთის განზრახვას – სამხედრო გზით აკონტროლოს საინფორმაციო სივრცე.

არსებული ინფორმაციით, რუსეთი აქტიურად ავითარებს კრიტიკული ინფრასტრუქტურის ICS (**Industrial Control Systems**)-ზე დისტანციური წვდომის საშუალებებს. ექსპერტთა მონაცემებით, უცნობმა რუსმა აქტორებმა წარმატებით შეძლეს ICS-ის რამდენიმე მწარმოებლის პროგრამის დაზიანება, ლეგალური პროგრამული უზრუნველყოფის განახლებებში **მავნე პროგრამული კოდის** ჩანერგვა და ამ გზით მომხმარებლის სისტემასთან პირდაპირი წვდომის დამყარება.[2]

უკრაინის ენერგოსისტემაზე განხორციელებულმა კიბერშეტევებმა გააჩინა განცდა, რომ რუსეთი მომავალ კონფლიქტში არ შემოიფარგლება მხოლოდ DDoS და Defacement შეტევებით ან კიბერშპიონაჟის ოპერაციებით და არ არსებობს გარანტია, რომ იგი არ განახორციელებს კრიტიკული ინფრასტრუქტურის წინააღმდეგ მიმართულ აქციას, რასაც შესაძლოა ნგრევა და მსხვერპლიც კი მოჰყვეს. გასათვალისწინებელია, რომ სუსტად დაცული ინფრასტრუქტურის პირობებში ისეთი თავდასხმებიც კი, როგორიცაა DDoS და Defacement შეტევა, შესაძლოა არაპროპორციული ზარალის მიზეზი გახდეს.

როგორც დასაწყისში აღინიშნა, გარდა მწყობრიდან გამოყვანის ან გამოყენების მიზნით მოწინააღმდეგის ქსელზე წარმოებული თავდასხმებისა, რუსეთი კიბერსივრცეს იყენებს ფსიქოლოგიური ეფექტის მისაღწევად, რაც კრემლის სასარგებლოდ ადამიანების ქცევის ან ცნობიერების შეცვლის მცდელობებს გულისხმობს.

რუსეთის სამხედრო წრეებში დამკვიდრებული ცნების „ინფორმაციული კონფრონტაციის“ ძირითადი ეფექტი მიზნობრივი აუდიტორიის ცნობიერების ფორმირება და ქცევის მანიპულირებაა. რუსეთი საინფორმაციო სფეროს განიხილავს, როგორც ახალი ტიპის სამხედრო კონფლიქტის სტრატეგიულად გადამწყვეტ, კრიტიკულად მნიშვნელოვან დომეინს, რომელიც შესაძლოა გამოყენებულ

იქნეს, როგორც საკუთარ მოსახლეობაზე კონტროლის განსახორციელებლად, ისე მოწინააღმდეგე ქვეყნებზე გავლენის მოსაპოვებლად. ინფორმაციული ომი კრემლისთვის მსოფლიო არენაზე დომინირების მისაღწევი საკვანძო საშუალებაა. სამხედრო წრეები პრიორიტეტულად მიიჩნევენ ძალებისა და საშუალებების განვითარებას ომის, კრიზისისა თუ მშვიდობიან პერიოდში ინფორმაციული უპირატესობის მისაღწევად, რაც ინფორმაციულ კონტენტსა და ამ კონტენტის გავრცელების ტექნიკურ საშუალებებზე კონტროლს გულისხმობს. „ინფორმაციული კონფრონტაცია“ დასავლური საზოგადოების წინააღმდეგ ფსიქოლოგიური ომის საბჭოთა პერიოდის ტაქტიკას ემყარება და რუსეთის სტრატეგიის ერთ-ერთი ძირითადი ასპექტია. ზოგადად, ინფორმაციულ-ფსიქოლოგიური ზემოქმედება წარმოადგენს რუსეთის მიერ ინსპირირებული კონფლიქტების საწყის ფაზას, რომელიც მოიცავს არაკონვენციური ოპერაციების ჩატარებას საზოგადოებრივი აზრის მანიპულირების მიზნით ქვეყნის შიგნით, სამიზნე ქვეყანაში და საერთაშორისო მედიაში. ყირიმის ანექსიამ გვაჩვენა, რომ ინტენსიური, აქტიური ღონისძიებების ფონზე რუსული საბრძოლო დანაყოფები სამიზნე ტერიტორიაზე შეღწევას ადგილობრივი შეიარაღებული ფორმირებების საფარქვეშ იწყებენ. ამით სრულდება არაკონვენციური ოპერაციების ფაზა. თუ ოპერაცია წარმატებული აღმოჩნდა, იწყება ინტერვენციის ლეგიტიმაციისაკენ მიმართული ღონისძიებები „უმცირესობის უფლებათა დაცვის“ ლეგენდით. მეორე ფაზა უკვე კონვენციურ ქმედებებს გულისხმობს, თუმცა, მაგალითად, იმავე ყირიმის ანექსიის პირველი არაკონვენციური ფაზის წარმატებამ ძალზე გაამარტივა კონფლიქტის კონვენციური ფაზა რუსეთის სასარგებლოდ.

ინფორმაციული უპირტესობის მოსაპოვებლად ერთ-ერთ სერიოზულ ინსტრუმენტს რუსეთის არსენალში წარმოადგენს ინფორმაციული ომის სტრატეგიული და ტაქტიკური ამოცანების მხარდამჭერი ფსიქოლოგიური ოპერაციების კიბერუზრუნველყოფა. ამგვარი ოპერაციების კიბერელემენტი მოიცავს დაინტერესების ობიექტების ქსელების კომპრომეტაციას ისეთი ინფორმაციის მოპოვების მიზნით, რომელიც შესაძლოა გამოყენებულ იქნეს დაშინების, შანტაჟის, დისკრედიტაციის ან ფალსიფიკაციის მიზნით, ასევე, მასმედიის საშუალებებში კონტროლირებადი გავრცელებისთვის.

ინფორმაციული კონფრონტაციის პროცესში დომინირებისათვის რუსეთი მრავალფეროვან საშუალებებს იყენებს: გართულებული ატრიბუციის გამო რუსული სადაზვერვო სამსახურები აარსებენ კონსპირაციის მაღალი დონის მქონე **ჰაქტივისტურ** ჯგუფებს ან მოქმედებენ უკვე არსებულთა საფარქვეშ. ჰაქტივისტური კიბერშეტევები წარმოადგენდა ერთ-ერთ ელემენტს რუსეთის მთავრობის მიერ მხარდაჭერილ კიბერშეტევებში 2007 წელს ესტონეთის, 2008 წელს კი საქართველოს წინააღმდეგ, ასევე მუდმივად იყო ჩართული რუსეთ-უკრაინის კონფლიქტში მეიდანზე განვითარებული პროცესებისას თუ ყირიმის ანექსიისას.

უკანასკნელ პერიოდში ღია წყაროებსა თუ პარტნიორი სპეცსამსახურების მონაცემებში დომინირებს მოსაზრება, რომ სწორედ რუსეთი იდგა დაეშთან ასოცირებული „Cyber Chaliphate“-ის ჰაქტივიზმის საფარქვეშ[3] საფრანგეთის სატელევიზიო არხ TV5 Monde-ზე 2015 წლის აპრილში განხორციელებული თავდასხმის უკან. იგივე ჯგუფია პასუხისმგებელი ამერიკის ცენტრალური სარდლობის ტვიტერის ანგარიშის გატეხვაზე. შეტევა ფრანგულ მაუწყებელზე კარგად იყო ორგანიზებული და დაიწყო ჯერ კიდევ იანვრის თვეში არხის თანამშრომლებისათვის ფიშინგ-წერილების დაგზავნის კამპანიით, რამაც კიბერკრიმინალებს შესაძლებლობა მისცა 3 თვის შემდეგ მოეპოვებინათ კონტროლი ათამდე საინფორმაციო არხსა და მათ სოციალურ მედიაარხებზე, გაევრცელებინათ ჯიჰადისტური პროპაგანდა და გამოექვეყნებინათ სირიაში დისლოცირებული ფრანგი სამხედროების პირადი მონაცემები.

არსებობს არაერთი ტექნიკური დადასტურება, რომ კიბერტერორისტების ეს ყველაზე რეზონანსული თავდასხმა წარმოადგენდა რუსეთის სახელმწიფოს მიერ წარმოებულ/მხარდაჭერილ კიბერშეტევას – ე.წ. false flag ოპერაციას „Cyber Chaliphate“-ის საფარქვეშ. გართულებული ატრიბუციის მიუხედავად, ამ მოსაზრებას ამყარებს კიბერშეტევის ხელწერა და მავნე კოდებში კირილიცის ელემენტების შემცველობა, რომელიც კრემლის კონტროლქვეშ მოქმედ ჰაკერულ დაჯგუფება APT28-ის (რუსეთის სპეცსამსახურებთან აფილირებული ორგანიზაცია, რომელიც პასუხისმგებელია საქართველოს, უკრაინის, ევროკავშირის ქვეყნებსა თუ აშშ-ის კიბერსივრცეზე მრავალჯერადი კიბერშპიონაჟისა თუ სხვა კიბერ-

თავდასხმის ფაქტებზე) ხელწერის იდენტურია. დამატებით არგუმენტს წარმოადგენს ის გარემოებაც, რომ შეტევის დრო ემთხვევა ფრანგულ-რუსული ურთიერთობების გაუარესებას („მისტრალის“ საკითხი, საფრანგეთის იმჟამინდელი პრეზიდენტის უარი მოსკოვში 9 მაისის ღონისძიებებში მონაწილეობაზე და სხვა).

დღესდღეობით ტერორისტული ორგანიზაციების მხრიდან ისეთი კიბერშეტევის განხორციელების ალბათობა, რომელსაც მასობრივი ზიანის ან მსხვერპლის გამოწვევა შეუძლია, ძალზე დაბალია. მათი კიბერშესაძლებლობები მხოლოდ ელექტრონული სერვისების და ვებგვერდების დროებითი, ლოკალური დაზიანებისთვისაა საკმარისი, თუმცა გაცილებით სერიოზული იქნება საფრთხე, თუკი თავიანთი კიბერშესაძლებლობების არსებითად გასაუმჯობესებლად ტერორისტული ორგანიზაციები განვითარებული კიბერშესაძლებლობების მქონე რომელიმე სახელმწიფოსთან ითანამშრომლებენ. ყურადსაღებია, რომ რუსეთი ამგვარი თანამშრომლობის პირველ პრეცედენტს იძლევა, მიუხედავად იმისა, რომ ტერორისტულ ორგანიზაციასთან თანამშრომლობა სახელმწიფოთათვის პოლიტიკური რისკის შემცველია.

მოსკოვის მიერ მართული კიბერაქტივობების ფლაგმანი – დაჯგუფება კიბერბერკუტი – რუსული სამხედრო ოპერაციებისა და სტრატეგიული ამოცანების კიბერმხარდაჭერას ეწევა. დაჯგუფება აწარმოებს როგორც ტექნიკურ, ისე პროპაგანდისტულ შეტევებს. კიბერბერკუტი 2014 წლიდან არის აქტიურად ჩართული კიბერშპიონაჟსა თუ DDoS-ის შეტევებში როგორც ნატოს, უკრაინის წინააღმდეგ, ისე გერმანიის სამთავრობო საიტების წინააღმდეგ. ფოკუსირება ხდება ჰაკერული გზით მოპოვებული დოკუმენტაციის ონლაინგამოქვეყნებაზე, რაც ძირითადად ემსახურება მთავრობების დისკრედიტაციას, არჩევითი ორგანოებისადმი ნდობის შემცირებას, მოწინააღმდეგის დემორალიზებას, დაშინებას.

რუსეთი ინფორმაციის შეცვლისათვის ან მანიპულირებისათვის ფართოდ იყენებს ანაზღაურებად კომენტატორთა არმიას, ე.წ. „ტროლებს“. ანაზღაურებადი ტროლების უმსხვილესი დაჯგუფება – ინტერნეტის კვლევის სააგენტო (The Internet Research Agency (IRA), იგივე Trolls from Olgino) არის სახელმწიფოსგან დაფინანსებული ორგანიზაცია, რომელიც მოქმედებს კრემლის დავალებით

და ძირითადად აქვეყნებს პროსამთავრობო კონტენტს ან კრემლის სასარგებლოდ ერთვება ონლაინდისკუსიაში. ორგანიზაციის ამოცანაა „დასავლური გავლენის“ და რუსეთის მიმართ ნეგატიური მედიის წინააღმდეგ ბრძოლა. ამას გარდა, ზოგიერთი ტროლის ფუნქციას ცრუ კონტენტის გავრცელება წარმოადგენს.

რუსეთისათვის მანიპულაციის ერთ-ერთ საშუალებაა კრემლის მიერ კონტროლირებადი მრავალრიცხოვანი ინტერნეტბოტები, რომლებიც სოციალურ მედიაში კონტენტის ავტომატურად გამავრცელებელ აპლიკაციას წარმოადგენს. ბოტს შეუძლია ჩაძიროს არასასურველი ინფორმაცია, შეუძლებელი გახადოს რეალური კონტენტის ნახვა, გაავრცელოს სპეციფიკური მესიჯი ან შეასრულოს სხვა, განსხვავებული სირთულის თუ შინაარსის ამოცანა.

თავად კონტენტი, რომლის გავრცელებასაც ემსახურება ზემოაღნიშნული საშუალებები, წარმოადგენს *ცრუ და ნამდვილი ინფორმაციის ნაზავს, რომელიც მიმართულია სამიზნე აუდიტორიის დაბნევის, დემორალიზაციისა და მასზე გავლენის მოპოვებისკენ. სამიზნე აუდიტორიას წარმოადგენს საკუთარი მოსახლეობა, სხვა ქვეყნების მოსახლეობის გარკვეული ჯგუფები, ქვეყნის შიდა და სამიზნე ქვეყნების პოლიტიკური ელიტა. პროპაგანდის გავრცელების არხები მრავალფეროვანია და მოიცავს სატელევიზიო და რადიო არხებს, ბოტებს და ტროლებს სოციალურ მედიაში, ოპტიმიზებულ საძიებელ სისტემებს, მოსყიდულ ჟურნალისტებს საზღვარგარეთის მედიაში და სხვა.*

სასურველი ინფორმაციული კონტენტის გასავრცელებლად ზემოაღნიშნული საშუალებებისთვის ტექნიკური საშუალებების განვითარება ან არსებულის კონტროლი მინიმუმ სამი მიმართულებით ხდება:

- დაინტერესების ქვეყანაში მართვადი საკომუნიკაციო სივრცის, სამაუწყებლო არხების შექმნა და სოციალურ ქსელებში დომინირება პოლიტიკური თუ ეკონომიკური არასტაბილურობის განცდის დათესვის მიზნით;
- პრორუსული პოლიტიკური პარტიების თუ ჯგუფების საინფორმაციო მხარდაჭერის კიბერარხების შექმნა პრორუსული ელიტის ჩამოყალიბების მიზნით; განწყობის დანერგვა, რომ პრო-

რუსული ძალები შესაძლოა მოხვდნენ პარლამენტში ან მთავრობის ფორმირებაში მიიღონ მონაწილეობა;

- სოციალური ქსელებისა თუ კიბერსივრცის სხვა სეგმენტის გამოყენება ძირგამომთხრელი საქმიანობისთვის, განსაკუთრებით – მეზობლებთან ურთიერთობის კონტექსტში, რამაც შესაძლოა დააზიანოს სტრატეგიულ პარტნიორებთან ან მეზობელ სახელმწიფოებთან ურთიერთობა და აგრესიის შემთხვევაში გაართულოს პოლიტიკური თუ სხვა სახის მხარდაჭერის მიღება.

წამყვანი სადაზვერვო სამსახურების მონაცემებით, რუსული პროპაგანდა, ზემოაღნიშნული არხების გამოყენებით სასურველი კონტენტის გავრცელებით, ძირითადად რამდენიმე პოსტულატის დანერგავს ცდილობს:

- გაკოტრებული დასავლური ლიბერალური წესრიგი უნდა შეიცვალოს ევრაზიული ნეოკონსერვატორული პოსტლიბერალური მსოფლიო წესრიგით, რომელიც იცავს ტრადიციებს, კონსერვატიულ ღირებულებებს და ჭეშმარიტ თავისუფლებას;
- დასავლეთი ახდენს რუსეთის დემონიზებას; სინამდვილეში ეს უკანასკნელი მხოლოდ ცდილობს საკუთარი ინტერესებისა და სუვერენიტეტის დაცვას;
- აშშ ერევა სუვერენული სახელმწიფოების შიდა პოლიტიკაში და ცვლის ხელისუფლებებს მთელ მსოფლიოში.

ამრიგად, რუსეთიდან მომდინარე კიბერსაფრთხეების მასშტაბი მზარდია, როგორც სირთულის, ისე მრავალფეროვნების თვალსაზრისით. რუსეთის მიერ განხორციელებულმა ან მხარდაჭერილმა, ტექნიკურ შედეგზე ორიენტირებულმა კიბერშეტევამ საქართველოში შესაძლოა გამოიწვიოს მნიშვნელოვანი ზარალი და მსხვერპლიც კი, ხოლო კიბერარხებით გავრცელებულმა პროპაგანდისტულმა კონტენტმა – კრემლის სასარგებლოდ ცნობიერების შეცვლა, პროდასავლური განწყობების შემცირება და პრორუსული ელიტის ფორმირება-გაძლიერება, რაც შეიძლება გახდეს კონვენციური მოქმედებების წინაპირობა. შესაბამისად, **საჭიროა განსაკუთრებული ყურადღება დაეთმოს რუსეთის, როგორც დესტრუქციული კიბერაქტორის განზრახვების, შესაძლებლობებისა**

თუ ღონისძიებების შესახებ ინფორმაციის მოპოვებისა და ანალიზის მექანიზმის ჩამოყალიბებას და ამ მხრივ აქტიური მუშაობის წარმართვას.

სასიცოცხლოდ აუცილებელია ყურადღება დაეთმოს არა მარტო ქსელის დაცვის ოპერაციებს, არამედ **მოხდეს კიბერშესაძლებლობების ინტეგრირება სხვა სამხედრო ოპერაციებში.** კიბერელემენტს, როგორც ბოლო დროს განვითარებულმა მოვლენებმა ცხადყო, ჰიბრიდული ომის ტაქტიკაში ერთ-ერთი საკვანძო ადგილი უჭირავს და სულ უფრო მეტი ამოცანის გადასაჭრელად გამოიყენება. მნიშვნელოვანია ჩვენი ქვეყნის მასშტაბით სამხედრო წვრთნებში კიბერელემენტის მუდმივი ჩართვა და საერთაშორისო კიბერსავარჯიშოებში ქართული უწყებების, კერძო სექტორისა თუ აკადემიური წრეების მონაწილეობა. ძირითადი სამუშაო ამ მხრივ ჯერ კიდევ გასაწევია და თავად გამოწვევაც, საერთო შეფასებით, ინტელექტუალური უფროა, ვიდრე ტექნიკური.

დასანერგია მიდგომა, **რომ კიბერუსაფრთხოება საერთო პასუხისმგებლობაა და რომ ინფორმაციის გაცვლის, ეფექტური საერთაშორისო თუ უწყებათშორისი თანამშრომლობის გარეშე ქვეყანა ვერ შეძლებს სრულყოფილად შეასრულოს სანდო პარტნიორის როლი კიბერსივრცეში**. ამ კონტექსტში უმნიშვნელოვანეს როლი ეკისრება მომხმარებლის **ცნობიერების ამაღლებისკენ მიმართულ ღონისძიებებს.**

მიუხედავად იმისა, რომ სამხედრო პოტენციალის თვალსაზრისით განსხვავება ჩვენსა და მოწინააღმდეგეს შორის უზარმაზარია, კიბერსივრცე ის არეალია, სადაც პატარა ქვეყანას რეალურად შეუძლია წინააღმდეგობა გაუწიოს რიცხოვნობით დიდად აღმატებულ აგრესორს და იგი შესაძლოა გახდეს მის ქმედებებზე ასიმეტრიული პასუხის ერთ-ერთი წარმატებული ელემენტი ან წინააღმდეგობის მოქმედი ფრონტი.

შენიშვნები

1. უკრაინის კონფლიქტში კიბერელემენტის ფართოდ გამოყენება ვრცლად განხილულია NATO CCD COE-ის გამოცემულ კრებულში: Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015.

2. ეს ინფორმაცია ისევე, როგორც რუსეთის ფედერაციის თავდაცვის მინისტრის განცხადება კიბერსარდლობის შექმნის შესახებ, სერიოზულ საფრთხედ მიიჩნია აშშ-ის სადაზვერვო თანამეგობრობამ. მაგ., Statement for the Record. Hearing: Worldwide Cyber Threat. House Permanent Select Committee on Intelligence. James R. Clapper, Director of National Intelligence. "Computer security studies assert that Russian cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures. Unknown Russian actors successfully compromised the product supply chains of at least three ICS vendors so that customers downloaded malicious software ("malware") designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates, according to private sector cyber security experts." www.docs.house.gov/meetings/IG/IG00/20150910/103797/HHRG-114-IG00-Wstate-ClapperJ-20150910.PDF

3. დაეშის და მასთან ასოცირებული კიბერსტრუქტურების ტერორისტული ბუნება ეჭვს არ იწვევს, რუსეთმა კი ამ მოქმედებით ტერორისტებთან თანამშრომლობის პრეცედენტი შექმნა, რაც თავისთავად საფრთხის შემცველია თუნდაც ტერორისტული ორგანიზაციების კიბერშესაძლებლობების არსებითად გაუმჯობესების კუთხით. მიუხედავად იმისა, რომ ეს ქმედება იყო რუსეთის სპეცსამსახურების მხრიდან ტიპური false flag operation, ჰაქტივიზმის საფარქვეშ ჩატარებული ოპერაციის კვალიფიკაციას აძლევს შეტევას. იხ., მაგალითად, აშშ-ის Defence Intelligence Agency-ს რეპორტი RUSSIA MILITARY POWER - Building a Military to Support Great Power Aspirations "Under the guise of hacktivism, a group called "CyberCaliphate," seemingly ISIS associated, conducted a hack against French station TV5 Monde in January 2015. The CyberCaliphate group was later linked to Russian military hackers. The same group hijacked the Twitter feed of the U.S. Central Command". www.dia.mil/Military-Power-Publications