RONDELI FOUNDATION
GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

რუსული დესტრუქციული კიბეროპერაციებისაგან თავდაცვის ძირითადი სტრატეგიული მიმართულებები

ანდრია გოცირიძე

123

ექსპერტის აზრი

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

ექსპერტის აზრი

ანდრია გოცირიძე

რუსული დესტრუქციული კიბეროპერაციებისაგან თავდაცვის ძირითადი სტრატეგიული მიმართულებები

123

2019

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 978-9941-8-1239-2

ფაქტორები, რომელთა გათვალისწინებითაც უნდა მოხდეს ეროვნული კიბერუსაფრთხოების ახალი სტრატეგიის შემუშავება. 21-ე საუკუნის მეორე ათწლეულის მიწურულს კიბერუსაფრთხოება, როგორც სახელმწიფო უსაფრთხოების შემადგენელი, სულ უფრო მეტ დატვირთვას იძენს. პოლიტიკური, სამხედრო, სოციალური თუ კრიმინალური პროცესები დიდწილად კიბერსივრცეშია გადანაცვლებული. კიბერდომეინი, დაპირისპირების მეხუთე სივრცე, გამუდმებით გამოიყენება პოლიტიკური, ეკონომიკური თუ სამხედრო მიზნების მისაღწევად. განვითარებული კიბერშეტევითი პოტენციალი საშუალებას აძლევს ბევრ სახელმწიფოს, უპირველეს ყოვლისა კი რუსეთს, გეოპოლიტიკური უპირატესობის მოსაპოვებლად წარმატებით გამოიყენოს კიბერსივრცე ომის/კონფლიქტის მიმდინარეობისას თუ მშვიდობიან დროს.

სახელმწიფოთაშორის ურთიერთობებსა თუ კონფლიქტებში კიბერელემენტის გამოყენებამ მოკლე პერიოდში მნიშვნელოვანი ცვლილება განიცადა. თუკი საუკუნის პირველ ათწლეულში სახელმწიფოთა მხრიდან მხარდაჭერილი კიბერშეტევები ძირითადად ტექნიკური ეფექტის მისაღწევად გამოიყენებოდა, მეორე ათწლეულის შუა პერიოდიდან თვალშისაცემია საინფორმაციო-ფსიქოლოგიური ზემოქმედების მიზნით განხორციელებული კიბეროპერაციების მზარდი რიცხვი. საქართველოსთვის ძირითად საფრთხედ ისევ რჩება რუსეთის აგრესიული კიბეროპერაციები, რომლებიც როგორც ტექნიკურ, ისე ფსიქოლოგიურ ეფექტზეა გათვლილი და მეტად სახიფათოა საქართველოსათვის. უნდა აღინიშნოს, რომ ბოლო წლებში რუსეთის დესტრუქციული კიბერაქტივობები პოსტსაბჭოთა ქვეყნების არეალს გასცდა და ევროპისა თუ აშშ-ის საარჩევნო პროცესები მრავალჯერ გახდა რუსეთის სამთავრობო სტრუქტურებთან დაკავშირებული ჰაკერების სამიზნე. კიბერსივრცე რუსული პროპაგანდისტული კონტენტის და, ზოგადად, რუსული საინფორმაციო კონფრონტაციის მოქმედების მნიშვნელოვან ასპარეზად იქცა, რაც კიდევ ერთხელ მოწმობს საინფორმაციო-ფსიქოლოგიურ შედეგზე ორიენტირებული კიბეროპერაციებისაგან მომდინარე საფრთხეზე.

რუსული კიბერსაფრთხეები: ძირითადი მიმართულებები და მიზნები

არსებული მდგომარეობით, საქართველოსთვის რუსეთის ფედერაციიდან მომდინარე კიბერსაფრთხე რეალურია და მისი დონე, 2008 წელთან შედარებით, გაზრდილია. კრემლმა არათუ შეცვალა საკუთარი აგრესიული კიბერპოლიტიკა, არამედ მნიშვ-

ნელოვნად აამაღლა სახელმწიფოს კიბერშეტევითი პოტენციალი და გააფართოვა კიბეროპერაციების გამოყენების არეალი. ტექნიკურ ეფექტზე ორიენტირებულ შეტევებს კიბერსივრცეში მიმდინარე ფსიქოლოგიური გავლენის ოპერაციებიც დაერთო. ამგვარმა ოპერაციებმა შესაძლოა გამოიწვიოს საინფორმაციო-ფსიქოლოგიური ეფექტი: კრემლის სასარგებლოდ ცნობიერების შეცვლა, პროდასავლური განწყობების შემცირება და პრორუსული ელიტის ფორმირება-გაძლიერება, რაც კონვენციური მოქმედებების წინაპირობას წარმოადგენს. საფრთხეების ზრდის ერთ-ერთი ფაქტორი ის გარემოებაცაა, რომ 2008 წელთან შედარებით მნიშვნელოვნად არის გაზრდილი საქართველოს დამოკიდებულება ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე, რაც პოტენციური კიბერთავდასხმების შემთხვევაში, ზრდის მოსალოდნელი ზიანის მასშტაბებს.

დემოკრატიულ სახელმწიფოში კრიტიკული ინფრასტრუქტურის დიდი ნაწილი კერძო სექტორშია თავმოყრილი. ბიზნესის განვითარება ეკონომიკის ზრდის და, ზოგადად, ეკონომიკური უსაფრთხოების ერთ-ერთი ძირითადი ფაქტორია. სწორედ ამიტომ ხდება ხშირად სახელმწიფოთაშორისი ურთიერთობების მსხვერპლი ბიზნესსექტორის კიბერსივრცეც, რაც, თავის მხრივ, სახელმწიფოზე ახდენს შესამჩნევ გავლენას. კიბერსივრცის მზარდი გამოყენების პროპორციულად იზრდება რისკები. სამწუხაროდ, კიბერსაფრთხეებზე იმუნიტეტი არ არსებობს.

21-ე საუკუნის დასაწყისიდან სხვადასხვა ინტენსივობისა და სირთულის რუსული კიბეროპერაციების სამიზნედ ათეულობით ქვეყანაში იქცა სახელმწიფო სტრუქტურები, მედია და კომუნიკაციის სფერო, ინდუსტრია, ენერგეტიკა, პოლიტიკური ორგანიზაციები და სხვა.

უკანასკნელი ორი ათწლეულის მანძილზე კიბერსივრცეში მიმდინარე მოვლენებისა და კონფლიქტებში კიბერელემენტის გამოყენების ანალიზი ცხადყოფს, რომ რუსეთის მიერ წარმოებული კიბეროპერაციების ნეგატიური ეფექტი მრავალგვარია და შეიძლება სხვადასხვა მიზანს ემსახურებოდეს:

- **ინდუსტრიის კონტროლის სისტემების მწყობრიდან გამოყვანა.** აშშ-ის დაზვერვის მონაცემებით[1], რუსეთი მინიმუმ 2015 წლიდან ფლობს შესაძლებლობას, ჰქონდეს დისტანციური წვდომა მოწინააღმდეგის კრიტიკული ინფორმაციული სისტემის მაკონტროლებელ პროგრამულ უზრუნველყოფაზე[2]. ამავე მონაცემებით, რუსეთთან აფილირებულმა კიბერაქტორებმა წარმატებით

შეძლეს რამდენიმე ვენდორის პროდუქტის ლოჯისტიკური ჯაჭვის კომპრომეტაცია იმგვარად, რომ ლეგალური განახლებების ჩამოწერის შედეგად, მომხმარებლის სისტემაში აღმოჩნდა რუსული მალვეარი[3]. მართალია, საქართველოში ICS-ის გამოყენება არცთუ ხშირია, თუმცა ინდუსტრიის მსხვილი წარმომადგენლების წარმოების ციკლი ავტომატიზებულია.

- **კიბერშპიონაჟი** – საქართველოს შესაბამისმა სამსახურებმა გამოავლინეს მასშტაბური კიბერსადაზვერვო ოპერაცია GEORBOT. ამერიკული კიბერუსაფრთხოების ორგანიზაციის Fire Eye-ს ანგარიშში არსებული მონაცემების მიხედვით, წლების მანძილზე არსებობდა არასანქცირებული წვდომა სამთავრობო და ძალოვან სტრუქტურათა რესურსებზე, სამხედრო ატაშეების ოფისებზე, ნატო-საქართველოს ურთიერთობასთან დაკავშირებულ დოკუმენტაციასა და სხვა სენსიტიურ მასალებზე. დისტანციურად ინსტალირებული მალვეარის მეშვეობით მუდმივად მიმდინარეობდა სხვადასხვა კატეგორიის ინფორმაციის გადინება[4]. ოპერაციას ახორციელებდა რუსული სპეცსამსახურების მიერ მართული ჰაკერული დაჯგუფება APT28, იგივე Fancy Bear, რომელიც შემდგომ არაერთხელ გახდა მსოფლიო საზოგადოების შეშფოთების საგანი. ორგანიზაციის მიზანს ჯაშუშური პროგრამების მეშვეობით თავდაცვასა და გეოპოლიტიკურ საკითხებზე ინფორმაციის შეგროვება წარმოადგენს, რაც მხოლოდ სახელმწიფოსათვის შეიძლება იყოს საინტერესო. APT28, რომელიც, სულ მცირე, 2007 წლიდან არსებობს, მოცემულ შემთხვევაში შეტევებს ახორციელებდა რუსეთის საერთაშორისო ინტერესების შესაბამისი სადაზვერვო ინფორმაციის მოსაპოვებლად, ძირითადად სამი მიმართულებით: კავკასიის რეგიონის, კერძოდ, საქართველოს; აღმოსავლეთ ევროპის რეგიონის, კერძოდ, უნგრეთისა და პოლონეთის; ევროპული და ევროატლანტიკური უსაფრთხოების ორგანიზაციების – NATO და ეუთო – მიმართულებით.
- **კიბერშეტევები მაღალტექნოლოგიური მალვეარის გამოყენებით.** უკრაინის კონფლიქტში რუსეთმა გამოიყენა კინეტიკური ეფექტის მქონე რთული ვირუსების (BlackEnergy და Ouroboros) ზემოქმედება კრიტიკულ ინფრასტრუქტურაზე. ამ ტიპის მალვეარები „თითქმის ათი წელი მზადდებოდა და უაღრესად რთულია, რომ კერძო პირის ან არასახელმწიფო აქტორის მიერ იყოს მომზადებული“.[5] ამგვარმა ქმედებებმა გააჩინა ვარაუდი,

რომ სამომავლოდ, კონფლიქტისას, რუსეთი დაბალტექნოლოგიური შეტევებით და კრიტიკული ინფრასტრუქტურის დროებითი შეფერხებით არ შემოიფარგლება.

- **კრიტიკული ინფრასტრუქტურის ფუნქციონირების სხვადასხვა ხარისხის მოშლა ან შეფერხება Ddos ან Defacement**[6]-ის ტიპის შეტევების შედეგად. ცნობილია, რომ სუსტად დაცული ინფრასტრუქტურის პირობებში დაბალტექნოლოგიური DDoS და Defacement შეტევაც კი შესაძლოა არაპროპორციულად მაღალი ზარალის მიზეზი გახდეს.
- **შეღწევა მიწოდების ჯაჭვის კომპრომეტაციის**[7] **გზით** – გულისხმობს ინფილტრაციას პროდუქტის მომწოდებლის ან წარმოების და ლოჯისტიკის ხარვეზის საშუალებით. ბოლო პერიოდში მეტად გახშირდა ამ ტიპის შეღწევის გამოყენება სახელმწიფოთა, განსაკუთრებით კი რუსეთის, მხრიდან.
- **ინსაიდერული საფრთხეები:** სისტემაში შეღწევის ერთ-ერთი უმარტივესი გზა ინსაიდერის მეშვეობით განხორციელებული ინფილტრაციაა. ინსაიდერად მოიაზრება ყოფილი ან მოქმედი თანამშრომელი, კონტრაქტორი და ყველა ის სუბიექტი, ვისაც შესაძლოა ლეგალური წვდომა ჰქონდეს საინფორმაციო სისტემებთან. ამ არხს ხშირად იყენებენ რუსული სპეცსამსახურები. უკანასკნელ პერიოდში რუსეთთან დაკავშირებული აშშ-ის გახმაურებული კიბერსკანდალები სწორედ ინსაიდერული საფრთხეებით იყო განპირობებული. გარდა მოტივირებული ინსაიდერული საფრთხისა, ყურადსაღებია მომხმარებლის ცნობიერების დაბალი დონით გამოწვეული ინსაიდერული კიბერინციდენტები. მალვეარის ინსტალაციისათვის რუსული კიბერაქტორები ხშირად იყენებენ ისეთ გავრცელებულ მეთოდს, როგორიცაა ფიშინგი[8], საქართველოში კი ფიშინგის მსხვერპლთა საერთო პროცენტი 40-50% მერყეობს, რაც მეტად სარისკო მაჩვენებელია. სწორედ ფიშინგის მეთოდით შეძლეს რუსეთის სპეცსამსახურებთან დაკავშირებულმა კიბერაქტორებმა ამერიკის დემოკრატიული პარტიის, გერმანიის ბუნდესთაგისა და სხვა სახელმწიფო დაწესებულებების თუ ბიზნესის წამომადგენლების ქსელების კომპრომეტაცია.
- **კიბეროპერაციები საინფორმაციო ფსიქოლოგიური ეფექტით.** კიბერარხებით გავრცელებულმა პროპაგანდისტულმა კონტენტმა შესაძლოა გამოიწვიოს საინფორმაციო-ფსიქოლოგიური ეფექტი: კრემლის სასარგებლოდ ცნობიერების შეცვლა, პრო-

დასავლური განწყობების შემცირება და პრორუსული ელიტის ფორმირება-გაძლიერება, რაც შეიძლება გახდეს კონვენციური მოქმედებების წინაპირობა.

როგორც ომისა თუ კონფლიქტის მიმდინარეობისას, ისე მშვიდობიან დროს რუსეთის მიერ განხორციელებული კიბეროპერაციები შესაძლოა სხვადასხვა სტრატეგიული თუ ტაქტიკური ამოცანის შესრულებას უკავშირდებოდეს. ამგვარი ამოცანების არასრული ჩამონათვალია, მაგალითად:

- სადამსჯელო ღონისძიება რუსეთის ინტერესებთან შეუთავსებელი ქმედების გამო ან ზეწოლის ბერკეტი პოლიტიკური ამოცანის შესასრულებლად;
- სამხედრო ამოცანის შესრულების გასაადვილებლად კონვენციურ ქმედებებთან ინტეგრირებული, მათი წინმსწრები ან თანმხლები ქმედება;
- კრიტიკული ინფრასტრუქტურის ხანგრძლივად მოშლა კინეტიკური შედეგების მქონე კიბეროპერაციის მეშვეობით, ეკონომიკური კოლაფსის, ფინანსური ზარალის, მასობრივი არეულობის გამოწვევის მიზნით;
- სახელმწიფო ინსტიტუტების გამართული ფუნქციონირების შეფერხება კრიტიკულ სერვისებთან წვდომის შეზღუდვით;
- პროდასავლური განწყობების შემცირება და ცნობიერების შეცვლა კრემლის სასარგებლოდ საინფორმაციო-ფსიქოლოგიური ზემოქმედებით;
- არჩევნების შედეგებით მანიპულაცია, არასასურველი კანდიდატის დისკრედიტაციის, დემოკრატიული წყობის შესუსტების, სახელმწიფო ინსტიტუტების ნდობის შერყევის მიზნით;
- სადაზვერვო ინფორმაციის მოპოვება კიბერშპიონაჟის აქტებით, სხვა სადაზვერვო მოქმედებები ეთნიკური, რელიგიური, პოლიტიკური ნიშნით ანტაგონისტური ჯგუფების ჩამოყალიბების, სამეზობლო, სახელმწიფოთაშორისი ურთიერთობების ძირგამომთხრელი საქმიანობა;
- პოლიტიკური ფიგურების, სამხედრო პირების, სოციალური ჯგუფების ან გადაწყვეტილების მიმღები წრეების დისკრედიტაციის, დაშინების და შანტაჟისათვის ქსელში არსებული ინფორმაციის მოპოვება ან ფაბრიკაცია.

საქართველოსთვის, მისი ჩრდილოელი მეზობლის დესტრუქციული და უკიდურესად აგრესიული ხასიათის გამო, ყველა ეს ტენდენცია მეტ-ნაკლებად იქნება საფრთხის შემცველი. არსებული ვითარება როგორც სამთავრობო სტრუქტურების, ისე კრიტიკული ინფრასტრუქტურის წარმომადგენლების მხრიდან მაღალ ცნობიერებას და კონკრეტულ ნაბიჯებს მოითხოვს, როგორც სტრატეგიულ, ისე ტაქტიკურ თუ საოპერაციო დონეებზე.

კიბერსივრცეში არსებული საფრთხეების ზრდის ტემპებისა და გავრცელების არეალიდან გამომდინარე, მნიშვნელოვანია გავაანალიზოთ, რას უპირისპირებს საქართველო არსებულ ტენდენციებს. უკანასკნელ ათწლეულში სახელმწიფო კიბერაქტორების მიერ კიბერუსაფრთხოების მიმართულებით გადადგმულმა ნაბიჯებმა განაპირობა ის რეალობა, რომ გაერთიანებული ერების საერთაშორისო სატელეკომუნიკაციო ორგანიზაციის კიბერუსაფრთხოების ინდექსში საქართველო მსოფლიო მასშტაბით პირველ ათეულში იკავებს ადგილს. აღნიშნული ინდექსის მისაღებად კვლევა მიმდინარეობს კიბერუსაფრთხოების 5 ძირითადი მიმართულებით: საკანონმდებლო ბაზა, ტექნიკური აღჭურვილობა, ორგანიზაციული სტრუქტურა, შესაძლებლობების განვითარება და თანამშრომლობა. ცხადია, ასეთ ავტორიტეტულ რეიტინგში დაწინაურება ეროვნული კიბერუსაფრთხოების სისტემის აღიარებაა. უნდა აღინიშნოს, რომ საქართველო დსთ-ის სივრცეში ლიდერ სახელმწიფოდ იქნა მიჩნეული[9]. მიუხედავად ამ წარმატებისა, კიბერუსაფრთხოების სტრატეგიული და კონცეპტუალური დოკუმენტაცია, ისევე, როგორც საკანონმდებლო ბაზა, საფუძვლიან განახლებას საჭიროებს, რადგან ეფექტური კიბერთავდაცვის გარეშე ქვეყანა ჩრდილოატლანტიკური ალიანსისათვის ვერ გახდება საიმედო პარტნიორი.

ზემოთქმულიდან გამომდინარე, საჭიროა განსაკუთრებული ყურადღება დაეთმოს რუსეთის, როგორც დესტრუქციული კიბერაქტორის განზრახვების, შესაძლებლობებისა თუ ღონისძიებების ასახვას კიბერუსაფრთხოების სტრატეგიულ დოკუმენტებში. ახალმა ეროვნულმა სტრატეგიამ და მასზე დაყრდნობით შემუშავებულმა ნორმატიულმა ბაზამ უნდა უზრუნველყოს კიბერუსაფრთხოების სრული ინტეგრაცია ფართო უსაფრთხოებასა და სახელმწიფო ცხოვრების ყველა სფეროში.

არსებული სტრატეგიის პრობლემები და ახალი კონცეპტუალური ბაზის ძირითადი მიმართულებები

მუდმივად ცვალებადი კიბერსივრცის პირობებში, სასიცოცხლოდ აუცილებელია ნათლად გამოიკვეთოს ის პრობლემატიკა, რომელიც თან ახლავს საქართველოს კიბერგანზომილების განვითარებას. განვიხილოთ რამდენიმე მათგანი:

უსაფრთხოებისა და კრიზისების მართვის საბჭოს გაუქმების შემდეგ, თითქმის წელიწადია **საქართველოს კიბერუსაფრთხოების არქიტექტურაში აღარ არსებობს მაკოორდინირებელი ორგანო,** რომელიც უზრუნველყოფდა სახელმწიფო კიბერაქტორების ურთიერთშეთანხმებულ მუშაობას, კერძო აქტორებთან თანამშრომლობას და სტრატეგიულ დოკუმენტაციაზე ერთობლივ მუშაობას. აღნიშნული, სავარაუდოდ, ერთ-ერთი მიზეზია იმისა, **რომ 2019 წელს საქართველო, სამწუხაროდ, კიბერუსაფრთხოების ეროვნული სტრატეგიის გარეშე შეხვდა:** წინა სტრატეგია 2018 წლის ჩათვლით მოქმედებდა, ახლის შექმნაზე მუშაობა 2019 წელს კი დაიწყო, მაგრამ ჯერ კიდევ საწყის ეტაპზეა და, სავარაუდოდ, რამდენიმე თვეს გასტანს. სხვათა შორის, ის, რომ საქართველო უკვე მესამე თაობის სტრატეგიაზე მუშაობს, მეტად პოზიტიურად აღიქმება საერთაშორისო საზოგადოებისა და კიბერექსპერტების მიერ, რაც განაპირობებს კიდეც საერთაშორისო რეიტინგებში მოწინავე პოზიციებს.

- **საფუძვლიანადაა გადასახედი კრიტიკული ინფრასტრუქტურის განსაზღვრის პარადიგმა.** დემოკრატიულ სახელმწიფოში კრიტიკული სერვისების უმეტესობა ბიზნესშია კონცენტრირებული, შესაბამისად, საუკეთესო პრაქტიკის მიხედვით, კრიტიკულ ინფრასტრუქტურას დიდწილად კერძო სექტორი წარმოადგენს.[10] ასეთი დარგებია ენერგეტიკისა და წყალმომარაგების სფერო, საბანკო და საფინანსო სექტორი, კვების, ქიმიური და სამხედრო მრეწველობა, სამედიცინო სეგმენტი და სხვა. საქართველოს კანონმდებლობით, კრიტიკული ინფორმაციული სისტემების სუბიექტთა ნუსხა მხოლოდ სამთავრობო ქსელების ერთ ნაწილს მოიცავს და არ ვრცელდება ბიზნესის საკუთრებაში არსებულ, სახელმწიფოსათვის კრიტიკულად მნიშვნელოვან დარგებზე.
- თავდაცვის სფეროს კრიტიკულ ინფრასტრუქტურად დღევანდელი კანონმდებლობა თავად თავდაცვის სამინისტროს სისტემას მიიჩნევს, მაგრამ არ ითვალისწინებს კერძო სექტორის იმ ობიექტებს, რომელთა გამართული ფუნქციონირება სასიცოცხ-

ლოდ აუცილებელია თავდაცვის სფეროსათვის (მაგ., მომსახურე კვების კომპანია, სამხედრო მრეწველობა, ლოჯისტიკური ჯაჭვის შემადგენელი კერძო აქტორები). საუკეთესო პრაქტიკა ითვალისწინებს ქვეყნის თავდაცვისუნარიანობისათვის შექმნილ საფრთხეზე მსჯელობას კრიტიკული ინფრასტრუქტურის ობიექტებზე თავდასხმის მასშტაბებიდან გამომდინარე. გადასახედია თავად **არსებული კრიტიკული ინფრასტრუქტურის დაყოფა თავდაცვის სფეროდ და დანარჩენ საჯარო სექტორად. სახელმწიფოში უნდა მოქმედებდეს ერთიანი ნუსხა კრიტიკული ინფრასტრუქტურისა, რომლის დაცვაც, აგრესიის წყაროსა და შეტევის მასშტაბებიდან გამომდინარე, სხვადასხვა სახელმწიფო აქტორის, მათ შორის, ზოგიერთ შემთხვევაში, თავდაცვის უწყების კომპეტენცია იქნება.**

- ქსელის დაცვის მეტ-ნაკლებად განვითარებული მექანიზმების მიუხედავად, არსებობს მტრულად განწყობილი სახელმწიფოს მხრიდან ინდუსტრიის კონტროლის სისტემებში დისტანციური ჰაკერული შეღწევის, supply chain-ის ოპერაციების მეშვეობით კომპრომეტირებული ტექნიკური მოწყობილობებისა და პროგრამული უზრუნველყოფის ჩანერგვის საფრთხე, რაც, არსებული კანონმდებლობის პირობებში, რისკის წინაშე აყენებს სახელმწიფოში არსებულ თითქმის ყველა ინფორმაციულ და საკომუნიკაციო ქსელსა თუ სისტემას. მარტივად რომ ვთქვათ, დღევანდელი შესყიდვების კანონმდებლობა არ ითვალისწინებს კიბერსაფრთხეებს და შესაძლებელს ხდის, რომ კრიტიკული ინფრასტრუქტურისა თუ სახელმწიფო დაწესებულებების კომპიუტერული ტექნიკა[11], მომსახურება, პროგრამული უზრუნველყოფა შეისყიდონ საკუთრივ რუსული ორგანიზაციებისაგან ან თუნდაც სხვა ქვეყნის კომპანიების რუსეთის ოფისისაგან. სამწუხაროდ, ასეთი შემთხვევები ახლო წარსულშიც იყო, როდესაც ოპტიკურ-ბოჭკოვანი მაგისტრალის შესყიდვა რუსული კომპანიის მიერ ხორციელდებოდა, ხოლო სამთავრობო დაწესებულებების გარკვეულ ნაწილს მობილურ საკომუნიკაციო მომსახურებას, სხვა კომპანიებთან ერთად, ამჟამად რუსული კომპანიაც უწევს. იგივე კანონმდებლობა საშუალებას იძლევა ინტერნეტიზაცია და საინფორმაციო ტექნოლოგიებთან დაკავშირებული სხვა მსხვილი პროექტები, ასევე სამთავრობო სტრუქტურების მობილური საკომუნიკაციო მომსახურება განახორციელონ ოკუპანტი ქვეყნის ბიზნესორგანიზაციებმა[12]. ცხადია, ამ მიზეზების გამო, სამთავრობო სტრუქტურების სა-

კომუნიკაციო მომსახურება ოკუპანტი სახელმწიფოს კომპანიის მხრიდან, რომელიც მრავალგანზომილებიანი ჰიბრიდული ომის პირობებში წარმატებით იყენებს კიბერსივრცეს, ყოვლად წარმოუდგენელია. კონცეპტუალურ დონეზე უნდა მოხდეს supply chain-ის რისკების მენეჯმენტის ინტეგრირება შესყიდვების პროცესსა თუ რისკების მართვის სისტემაში, რათა უზრუნველყოფილ იქნეს სახელმწიფო სექტორის მიერ გამოყენებული ტექნიკისა და ტექნოლოგიების უსაფრთხოება და სანდოობა. აუცილებელია მოხდეს კიბერტექნოლოგიების, როგორც სპეციფიკური საქონლისა და მომსახურების შესყიდვის განსაკუთრებული წესის შემუშავება, სადაც პროდუქტის სანდოობა და უსაფრთხოება ერთ-ერთი განმსაზღვრელი ფაქტორი იქნება. შეზღუდვა უნდა დაწესდეს რუსული წარმოების ან რუსეთის გავლით საინფორმაციო-ტექნოლოგიური სისტემების, ტექნოლოგიების ან მომსახურების შესყიდვაზე.[13]

- არსებული კონცეპტუალური და ნორმატიული ბაზა ვერ შეესაბამება ინსაიდერული საფრთხეების მზარდ მნიშვნელობას. საბაზრო ეკონომიკის პირობებში კრიტიკული სერვისების პროვაიდერი კერძო სექტორია. შესაბამისად, სახელმწიფო ორგანიზაციების ინფორმაციული მასივები ხშირად კონტრაქტორის ხელში ხვდება, რაც მნიშვნელოვნად ზრდის ინსაიდერული საფრთხეების მასშტაბს. საქართველოს რეალობაში, სახელმწიფო ორგანიზაციასთან ბიზნესურთიერთობის ფარგლებში, კონტრაქტორისათვის გადაცემული სენსიტიური ინფორმაციის დაცვა მხოლოდ ბიზნესორგანიზაციის კეთილ ნებაზეა დამოკიდებული. ბიზნესი კი მინიმალური დანახარჯით მაქსიმალური მოგების მიღებაზეა ორიენტირებული, ამიტომ უსაფრთხოებისათვის ზედმეტ დანახარჯებს ერიდება. საკითხი საჭიროებს სასწრაფო დარეგულირებას, რადგან არავინ იცის, რა რაოდენობის და რა სახის არასაიდუმლო, მაგრამ სენსიტიური ინფორმაციაა ამჟამად დაუცველი, რომელიც დაგროვილია კერძო ქსელებში. მაგალითისათვის სადაზღვევო კომპანიებისათვის ან მომსახურე სამედიცინო დაწესებულებებისათვის გადაცემული საჯარო მოხელეთა და სამხედრო მოსამსახურეთა პერსონალური თუ ჯანმრთელობის შესახებ ინფორმაციიის უზარმაზარი მასივებიც კმარა. ამ ტიპის ინფორმაცია განსაკუთრებით ძვირად ფასობს დარკნეტში, რაც შესაბამის სისტემებს მიმზიდველ სამიზნედ აქცევს როგორც ფინანსურად მოტივირებული კიბერკრიმინალის, ისე მტრულად განწყობილი

სახელმწიფოს კიბერაქტორებისათვის. აუცილებელია მკვეთრად იყოს განსაზღვრული მონაცემთა დაცვის ის სტანდარტი, რომლის შესრულებაც სახელმწიფო შესყიდვის განხორციელებისას სავალდებულო იქნება კონტრაქტორისთვის. მეორე მხრივ, სახელმწიფო უნდა დაეხმაროს კერძო კომპანიებს, კონტრაქტორებს, სახელმწიფოსათვის მნიშვნელოვანი ინფორმაციის კიბერუსაფრთხოების გარკვეული სტანდარტის პირობებში დამუშავების უზრუნველყოფაში.

- სასიცოცხლოდ მნიშვნელოვანია კიბერუსაფრთხოება არსებით პრობლემად აღიქვას სახელმწიფომ და ბიზნესსექტორის ტოპ-მენეჯმენტმა. სამწუხარო რეალობად რჩება ცნობიერების დაბალი დონე, რომელიც უშვებს, რომ სახელმწიფო უწყებებში ჯერ კიდევ ნებადართულია რუსული ანტივირუსული უზრუნველყოფისა თუ ელექტრონული ფოსტის გამოყენება. ასეთი შემთხვევები არცთუ იშვიათია. შედარებისათვის, სწორედ კიბერრისკების ზრდის მოტივით (მონაცემთა შეგროვება, ტრეკინგი) მისცა რეკომენდაცია ლიეტუვას შესაბამისმა სამთავრობო უწყებამ სახელმწიფო მოხელეებს, არ ესარგებლათ იანდექსტაქსის მომსახურებით. აუცილებელია, კიბერუსაფრთხოების ცნობიერების ასამაღლებელი ღონისძიებათა კომპლექსის შემუშავება და დანერგვა სახელმწიფო მმართველობის ყველა დონეზე.
- თუკი არსებული სტრატეგია და ნორმატიული ბაზა ნაწილობრივ მაინც არეგულირებს დესტრუქციული კიბეროპერაციების ტექნიკურ ეფექტს, კიბერარხებით გავრცელებული პროპაგანდისა და დეზინფორმაციის მავნე ზემოქმედება კონცეპტუალურ დოკუმენტაციაში განხილული არ არის. აუცილებელია კიბერუსაფრთხოების არქიტექტურაში რუსული კიბეროპერაციების საინფორმაციო-ფსიქოლოგიური ეფექტის პრევენციაზე პასუხისმგებელი უწყებებისა და მათი როლების განსაზღვრა. საფრთხეთა იდენტიფიცირების, საფრთხის წყაროების კვლევის, მოსალოდნელი საფრთხისა და დესტრუქციული აქტორების შესახებ მიზნობრივი ჯგუფების ინფორმირების ღონისძიებათა ორგანიზება.
- კიბერთავდასხმის შედეგები, აღმოჩენილი მალვეარის ტიპები და საფრთხის შემცველი აქტივობები რეპუტაციული რიკების გამო დახურულ ინფორმაციას წარმოადგენს, არადა ინფორმაციის სათანადო გაზიარების შემთხვევაში, რისკების მართვა გა-

ცილებით მარტივი და ეფექტურია. სტრატეგიულ დონეზე უნდა გადაწყდეს კიბერშეტევების შედეგებთან დაკავშირებით დროული გასაჯაროებისა და გამჭვირვალობის პოლიტიკის შემუშავება, საფრთხეებსა და რისკებზე ინფორმაციის გაცვლის უწყებათაშორისი და საჯარო-კერძო პლატფორმების შემუშავება.

ამრიგად, ახალი ეროვნული სტრატეგიის პირობებში აუცილებელია კიბერუსაფრთხოების მდგომარეობის უფრო მაღალ დონეზე გადასვლა და კიბერუსაფრთხოების მოთხოვნების ინტეგრირება სახელმწიფოს ცხოვრების სხვადასხვა სფეროში.

შენიშვნები

1. Hearing: World Wide Cyber Threats (Open).Testimony of The Honorable James Clapper, Director of National Intelligence. September 10, 2015. ხელმისაწვდომია: www.docs.house.gov/meetings/IG/IG00/20150910/103797/HHRG-114-IG00-Wstate-ClapperJ-20150910.PDF

2. **ICS (Industrial control system)** – კოლექტიური ტერმინი, რომელიც გამოიყენება კონტროლის სისტემებისა და მათთან დაკავშირებული ინსტრუმენტების აღსაწერად და აერთიანებს ინდუსტრიული პროცესების ავტომატიზაციისა და ოპერირებისათვის გამოყენებულ მოწყობილობებს, სისტემებს, ქსელებს და კონტროლის მექანიზმებს. დღეისათვის ფართოდ გამოიყენება კრიტიკული ინფრასტრუქტურის თითქმის ყველა მიმართულებაზე, როგორიცაა ინდუსტრია, ტრანსპორტი, ენერგეტიკა, ჰიდრომეურნეობა და სხვა, რის გამოც წარმოადგენს დესტრუქციული კიბეროპერაციების სამიზნეს. ICS-ის გავრცელებულ სახეობას წარმოადგენს ე.წ. **SCADA (Supervisory Control and Data Acquisition) და DCS (Distributed Control Systems) სისტემები.**

3. **მავნე პროგრამული უზრუნველყოფა –** Malware, malicious software – მალვეარი; კომპიუტერული პროგრამა, რომელიც გამოიყენება ინფორმაციულ სისტემებში არასანქცირებული შეღწევის, სენსიტიური ინფორმაციის შეგროვების, მოპარვის, განადგურების, შეცვლის, კრიპტაციის ან კომპიუტერზე უკანონო წვდომისათვის.

4. Fireeye special report, 2014. APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. ხელმისაწვდომია: www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

5. Sam Jones, "Cyber Snake Plagues Ukraine Networks," Financial Times, 7 March 2014. ხელმისაწვდომია: www.ft.com/content/615c29ba-a614-11e3-8a2a-00144feab7de. www.ft.com/content/615c29ba-a614-11e3-8a2a-00144feab7de

6. დაბალტექნოლოგიური კიბერშეტევის ფორმა, რომელიც არასანქცირებულად ცვლის საიტის (ვებგვერდის) გარეგნულ იერსახეს, ხშირად – პირველ გვერდს. ძირითადად, გამოიყენებენ ჰაქტივისტები ან კიბერტერორისტები საპროტესტო მესიჯის, პროპაგანდისტული მასალის ან სხვა კონტენტის გასავრცელებლად. ამ ტიპის თავდასხმა 2008 წლის ივლისში რუსეთთან აფილირებულმა ჰაკერებმა განახორციელეს საქართველოს პრეზიდენტის ვებგვერდზე და იქ განათავსეს ფაშისტური სიმბოლიკა.

7. ე.წ. **Supply chain-ის საფრთხეები** – პროდუქტის (კომპიუტერული ტექნიკა, პროგრამული უზრუნველყოფა და სხვა) მიწოდების პროცესში წარმოქმნილი საფრთხეები, რომლებიც გულისხმობს მომწოდებლის ხარვეზთან დაკავშირებული ინციდენტის ალბათობას, როდესაც მიმწოდებელი მხარე ვერ/არ აკმაყოფილებს უსაფრთხოების მოთხოვნებს ან საფრთხეს უქმნის მიმღების უსაფრთხოებას, სიცოცხლეს და ჯანმრთელობას.

8. **ფიშინგი (Phishing)** – კიბერკრიმინალის გავრცელებული ფორმა, რომლის მიზანია მსხვერპლის მოტყუების გზით მოახდინოს კომპიუტერის კომპრომეტაცია, მალვეარის ინსტალაცია და მოიპოვოს წვდომა სენსიტიურ ინფორმაციაზე. ფიშინგის განსაკუთრებულ ფორმას წარმოადგენს ე.წ. **Spear-Phishing**, რომელიც განკუთვნილია მომხმარებლის ვიწრო და სპეციფიკური წრისათვის (მმართველობა, გარკვეული ცოდნის, ინფორმაციის მატარებელი ჯგუფი). საჭიროებს კარგად მომზადებულ კონტექსტს ნდობის მოსაპოვებლად. გარდა ფინანსურად მოტივირებული კიბერკრიმინალისა, ფიშინგის სხვადასხვა ფორმა აქტიურად გამოიყენება სახელმწიფოთაშორის დესტრუქციულ კიბეროპერაციებში მოწინააღმდეგის ქსელის კომპრომეტაციისათვის.

9. The Global Cybersecurity Index (GCI) 2018. International Telecommunication Union (ITU). ხელმისაწვდომია: www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf?fbclid=IwAR1--Sw9bTs0N0qFHBbGcGTckqeyNryG1eBGHNP9k5Ar1oNZqFyS0yFOIXA

10. PRESIDENTIAL POLICY DIRECTIVE/PPD-21:SUBJECT: Critical Infrastructure Security and Resilience. February 12, 2013 ხელმისაწვდომია: www.obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil და www.dhs.gov/cisa/critical-infrastructure-sectors

11. გარდა იმისა, რომ არსებობს სენსიტიური მომსახურების ან პროდუქციის რუსული კომპანიებისაგან შესყიდვის მრავალი პრეცედენტი, ახლო წარსულში თავდაცვის უწყების მხრიდან, სხვა პროდუქციასთან ერთად, ადგილი ჰქონდა კომპიუტერული ტექნიკის შესყიდვას კომპანიისაგან, რომლის ხელმძღვანელი რუსეთის სასარგებლოდ ჯაშუშობისათვის ნასამართლევი პირია. უწყებამ მსგავსი ინციდენტი სათანადო კანონმდებლობის არარსებობით ახსნა. ცხადია, საკანონმდებლო ვაკუუმი მართლაც არის ერთ-ერთი ძირითადი, მაგრამ არა ერთადერთი პრობლემა მსგავსი ინციდენტების პრევენციისათვის, რადგან ე.წ. supply chain-ის საფრთხის სათანადოდ აღქმის შემთხვევაში, არასანდო აქტორის დისკვალიფიკაცია სახელმწიფო შესყიდვის პროცესიდან სავსებით შესაძლებელია უსაფრთხოების ინტერესებიდან გამომდინარე. იხ.: საქართველოს თავდაცვის სამინისტროს განცხადება, 2 ივლისი, 2018 წ. ხელმისაწვდომია: www.mod.gov.ge/ge/news/read/6668/saqartvelos-tavdacvis-saministros-gancxadeba

12. ტექნიკური თვალსაზრისით ეჭვს არ იწვევს, რომ მობილურ ოპერატორს აქვს ყოველგვარი საშუალება, გააკონტროლოს მომხმარებლის ზარები, მიმოწერა, უთვალთვალოს მის გადაადგილებას, დააფიქსიროს ლოკაცია და თუ საჭირო გახდა, თავად მობილური მოწყობილობა (ტელეფონი, ტაბლეტი და სხვა) ან მასში არსებული ინფორმაცია გამოიყენოს სადაზვერვო ან ძირგამომთხრელი საქმიანობისათვის. მობილური ინტერნეტის გამოყენების შემთხვევაში კი, ოპერატორის სურვილის შესაბამისად, ნებისმიერი აბონენტის პირადი თუ საჯარო ცხოვრება შეღწევადი ხდება. სწორედ *მობილური ოპერატორის შესაძლებლობები და ამ არხით მიღებული მეტამონაცემები გამოიყენა* რუსეთმა უკრაინის კონფლიქტში სხვადასხვა სირთულის სამხედრო თუ პოლიტიკური ამოცანის გადასაჭრელად, შანტაჟის, დაშინებისა თუ საარტილერიო დარტყმების კოორდინატების განსასაზღვრად.

13. მსგავსი პრეცედენტი აშშ-ის სპეცსამსახურებმა შექმნეს, სადაც ცნობილი *კასპერსკის სკანდალის* შემდგომ სახელმწიფო უწყებებს 90 დღე მიეცათ აღნიშნული პროგრამული უზრუნველყოფის დეინსტალაციისათვის. ხელმისაწვდომია: www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4