საქართველოს კიბერუსაფრთხოების პოლიტიკა, გამოწვევები და შესაძლებლობები

GCSD

საქართველოს კიბერუსაფრთხოების პოლიტიკა, გამოწვევები და შესაძლებლობები

ავტორი: ირაკლი ჭლარკავა

თბილისი, 2021

ავტორის შესახებ:

ირაკლი ჯღარკავა - საერთაშორისო ურთიერთობებისა და უსაფრთხოების სპეციალისტი. მიღებული აქვს მაგისტრატურის სამი ხარისხი შემდეგი სპეციალობებით: დესტაბილიზაციისა და ძალადობის მართვა (დანიელ მორგანის სახელობის ეროვნული უსაფრთხოების სკოლა, ქ. ვაშინგტონი, აშშ), სადაც იკვლევდა რუსეთის სტრატეგიას ნატოსა და საქართველოს მიმართ; ევროპის საჯარო მმართველობა და პოლიტიკა (ევროპის კოლეჯი), საკვლევი თემით - ევროკავშირის „ტრანსფორმაციის ძალის“ გავლენა საქართველოს ევროპეიზაციის გზაზე (Association Agreement, DCFTA); ნაციონალიზმი და ეთნიკურობის კვლევები (თბილისის სახელმწიფო უნივერსიტეტი), სადაც იკვლევდა 2015 წლის „ევროპის საიმიგრაციო კრიზისის“ გავლენას ევროპაში ულტრანაციონალიზმის წარმოშობაზე. ასევე, მიღებული აქვს თბილისის სახელმწიფო უნივერსიტეტის საერთაშორისო ურთიერთობების ბაკალავრის ხარისხი. მისი კვლევითი ინტერესის საგნებს წარმოადგენს: ეროვნული უსაფრთხოება, კიბერუსაფრთხოება, საინფორმაციო ომი, საქართველო-ევროკავშირის ურთიერთობები.

დაფინანსებულია საქართველოში აშშ-ის საელჩოს ალუმნი საგრანტო პროგრამის ფარგლებში. კვლევაზე პასუხისმგებელია მისი ავტორი და შინაარსი არ შეიძლება აღქმული იყოს როგორც აშშ-ის საელჩოს ან საქართველოს სტრატეგიის და განვითარების ცენტრის პოზიცია და მოსაზრება.

Funded through the Alumni Grants Program, U.S. Embassy in Georgia. The content of this document is the sole responsibility of the author and can under no circumstances be regarded as reflecting the position of the U.S. Embassy in Georgia or Georgian Center for Strategy and Development.

ტერმინთა განმარტება

კიბერსივრცე - სივრცე, რომელიც წარმოადგენს ერთმანეთთან ინტერნეტის საშუალებით დაკავშირებულ ციფრულ ტექნოლოგიებს.[I]

კიბერშეტევა - ქმედება, რომელიც იყენებს ელექტრონულ მოწყობილობას ან/და დაკავშირებულ ქსელს ან სისტემას კრიტიკული ინფრასტრუქტურის სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის/შეფერხების, განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით.[II]

კრიტიკული ინფრასტრუქტურა - სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური და საზოგადოებრივი უსაფრთხოებისთვის.[III]

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 ტერმინი ფართოდ გამოიყენება კრიტიკული ინფრასტრუქტურის თითქმის ყველა მიმართულებაზე, როგორიცაა: ინდუსტრია, ტრანსპორტი, ენერგეტიკა, ჰიდრომეურნეობა და სხვა, რის გამოც წარმოადგენს დესტრუქციული კიბეროპერაციების სამიზნეს. ICS-ს გავრცელებულ სახეობას წარმოადგენს ე.წ. SCADA (Supervisory Control and Data Acquisition) და DCS (Distributed Control Systems) სისტემები.[IV]

მალვეარი (Malware, malicious software) - მავნე კომპიუტერული პროგრამა (სხვადასხვა სახის ვირუსული პროგრამების საერთო სახელი), რომელიც ინფორმაციულ სისტემებზე არასანქცირებული შეღწევის, სენსიტიური ინფორმაციის შეგროვების, მოპარვის, განადგურების, შეცვლის, ან კომპიუტერზე უკანონო წვდომის მოსაპოვებლად გამოიყენება.[V]

ფიშინგი (Phishing) - კიბერკრიმინალის გავრცელებული ფორმა, რომლის მიზანია მსხვერპლის მოტყუების გზით მოახდინოს კომპიუტერზე წვდომა. ფიშინგი იგზავნება ელ. ფოსტის საშუალებით,კომპიუტერის დაინფიცირება კი მოცემულ ბმულზე ღილაკის დაჭერით ხდება ან თანდართული ფაილის ჩამოტვირთვით. ფიშინგის განსაკუთრებულ ფორმას წარმოადგენს ე.წ. Spear-Phishing, რომელიც განკუთვნილია მომხმარებლის ვიწრო და სპეციფიური წრისათვის (გარკვეული ცოდნის, ინფორამციის მატარებელი ინდივიდი ან ჯგუფი). ე.წ. Spear-Phishing-ი საჭიროებს კარგად მომზადებულ კონტექსტს ნდობის მოსაპოვებლად. ფიშინგ-შეტყობინების/ელ.ფოსტის დაგზავნა ხდება ერთობლივად ბევრ მისამართზე, ხოლო ე.წ. Spear-Phishing-ის გაგზავნა მიზანმიმართულად, ცალკეული ინდივიდების ელ. მისამართებზე.[VI]

ტერმინთა განმარტება

მიწოდების ჯაჭვის (Supply chain) საფრთხეები - პროდუქტის (კომპიუტერული ტექნიკა, პროგრამული უზრუნველყოფა და სხვა) მიწოდების პროცესში წარმოქმნილი საფრთხეები, რომლებიც გულისხმობენ მიმწოდებლის ხარვეზთან დაკავშირებული ინციდენტის ალბათობას, როდესაც მომწოდებელი მხარე ვერ/არ უზრუნველყოფს უსაფრთხოების მოთხოვნების დაკმაყოფილებას.[VII]

ვებგვერდის სერვისის უარყოფა (Denial-of-service/DoS attack) - კიბერთავდასხმის ერთ-ერთი სახე, სადაც თავდამსხმელი ცდილობს გახადოს ინტერნეტრესურსი ხელმიუწვდომელი. [VIII]

Defacement - დაბალტექნოლოგიური კიბერშეტევის ფორმა, რომელიც არასანქცირებულად ცვლის ვებ გვერდის გარეგნულ იერსახეს, ხშირად პირველ გვერდს. ძირითადად, გამოიყენება აქტივისტების ან კიბერტერორისტების მიერ საპროტესტო მესიჯის, პროპაგანდისტული მასალის ან სხვა კონტენტის გასავრცელებლად. [IX]

Distributed Denial-of-Service (DDoS) attack - არის მასშტაბური DoS შეტევა, სადაც თავდამსხმელი იყენებს ერთ ან მეტ, ხშირ შემთხვევაში, ათასობით IP მისამართს. ამ ტიპის შეტევები ძირითადად ხდება ვებ გვერდებზე. [X]

დარქნეტი/Darknet - ინტერნეტ-ქსელი შეზღუდული წვდომით, რომელიც უმთავრესად არალეგალური მიზნებისთვის გამოიყენება, მათ შორის უკანონო საქონლისა და მომსახურების გაცვლისთვის - ე.წ. შავი ბაზრობა. [XI]

აბსტრაქტი

აღნიშნული კვლევა მიზნად ისახავს საქართველოს ზოგადი კიბერუსაფრთხოების პოლიტიკის შეფასებას, და საქართველოს წინაშე არსებული კიბერგამოწვევებისა და შესაძლებლობების გამოვლენას. ნაშრომის საკვლევი კითხვებია: ***რატომ წარმოადგენს კიბერთავდასხმა საფრთხეს და როგორ შეიძლება საქართველომ მართოს კიბერსივრციდან მომავალი საფრთხეები?*** კვლევის მეთოდოლოგიურ ნაწილში გამოყენებული იქნა, როგორც დარგის ექსპერტების მოსაზრებები, ისე კიბერუსაფრთხოების მიმართულებით არსებული ოფიციალური დოკუმენტების ანალიზი. ნაშრომი დაყოფილია სამ ნაწილად: პირველ ნაწილში განხილულია საქართველოს კიბერუსაფრთხოების პოლიტიკა და მიმოხილულია მის წინაშე მდგარი გამოწვევები, მეორე ნაწილში, საუბარია საფრთხეების შესახებ და გაანალიზებულია კიბერთავდასხმები საქართველოს ეროვნულ უსაფრთხოებაზე გავლენის ჭრილში, ბოლო ნაწილში ყურადღება გამახვილებულია იმაზე, თუ როგორ უნდა ებრძოლოს ქვეყანამ კიბერსივცრიდან მომავალ საფრთხეებს, შეამციროს და მართოს იგი. კვლევის შედეგად, საქართველოს კიბერსაფრთხოების უმთავრეს გამოწვევებად გამოვლინდა შემდეგი: კიბერუსაფრთხოების პროაქტიული სახელმწიფო პოლიტიკის არარსებობა, ძლიერი აღმასრულებელი უწყების პრობლემა, სახელმწიფო უწყებებში კიბერცნობიერების დაბალი დონე, კადრების პრობლემა და კიბერუსაფრთხოების არაპრიორიტეტულობა.

შინაარსი

შესავალი

საქართველოს კრიტიკული ინფრასტრუქტურის წინააღმდეგ ბოლო დროს გახშირებული კიბერთავდასხმები საგანგაშოა ქვეყნის ეროვნული უსაფრთხოების ზოგადი სურათისთვის, კერძოდ იგი ასუსტებს თავდაცვისუნარიანობას, აჩენს რა საზოგადობაში დაუცველობის შეგრძნებას. შინაგან საქმეთა სამინისტროს სტატისტიკაზე დაყრდნობით, მატულობს კიბერდანაშაულის რიცხვი[1]. აღსანიშნავია, რომ რაც უფრო იზრდება ინტერნეტთან ხელმისაწვდომობა საზოგადოებაში, ქვეყნის მასშტაბით, მით უფრო იზრდება რისკი კიბერკრიმინალების წინაშე მათი მოწყვლადობის მხრივ. ეს მოსაზრება, საზოგადოებაში და საჯარო სფეროში დასაქმებულ პირებში (მათ შორის ეროვნული უსაფრთხოებისთვის საპასუხისმგებლო ფუნქციების მქონე პირებში) ე.წ. კიბერგანათლებისა და ცნობიერების ნაკლებობით შეიძლება აიხსნას. გარდა ამისა, ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ქვეყნის ეროვნული უსაფრთხოებისთვის უმთავრეს გამოწვევას, კიბერშპიონაჟი და მასთან დაკავშირებული საფრთხეების წინააღმდეგ ბრძოლა წარმოადგენს. ამასთანავე, კიბერკრიმინალების ერთ-ერთი მთავარი სამიზნეა საფინანსო და საბანკო სექტორი, რომლის დაუცველობა საქართველოს მოქალაქებს ფინანსურად დააზარალებს.

საქართველოს წინააღმდეგ კიბერთავდასხმის ისტორია ჯერ კიდევ 2008 წლის ივლისიდან იწყება, როცა რუსეთის მიერ განხორციელებულმა კიბერთავდასხმებმა, რომელთა სამიზნესაც სამთავრობო უწყებები, მედია საშუალებები და საბანკო სექტორი წარმოადგენდა, საგრძნობლად დააზიანა ქვეყნის კრიტიკული ინფრასტრუქტურა. ამას მოჰყვა 2008 წლის აგვისტოს ომი საქართველოს წინააღმდეგ. ეს იყო პირველი შემთხვევა, როდესაც კიბერთავდასხმა შეიარაღებულ კონფლიქტთან ერთად განხორციელდა. მას შემდეგ, მეზობელი რუსეთიდან საქართველო არაერთგზის გახდა კიბერთავდასხმების ობიექტი (2019 წლის ოქტომბრის ფართომასშტაბიანი თავდასხმა,[2] 2020 წლის სექტემბერში რიჩარდ ლუგარის სახელობის საზოგადოებრივი ჯანდაცვის კვლევითი ცენტრის მონაცემთა ბაზებზე კიბერთავდასხმა[3]).

---

1 მარი მალვენიშვილი, ნინი ბალარჯიშვილი, "კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები," ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI), თბილისი, აგვისტო, 2020.

2 "საქართველოს საგარეო საქმეთა სამინისტროს განცხადება 2019 წლის 28 ოქტომბერს საქართველოს წინააღმდეგ განხორციელებული ფართომასშტაბიანი კიბერშეტევის შესახებ," ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.10.2020).

3 "საქართველოს შინაგან საქმეთა სამინისტროს განცხადება 2020 წლის 1 სექტემბერს განხორციელებული კიბერშეტევის შესახებ," ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.10.2020).

რუსეთისთვის კიბერთავდასხმები წარმოადგენს ფსიქოლოგიური მანიპულაციისა და საინფორმაციო ომის ერთიან ინსტრუმენტს, რომლის მიზანია მოწინააღმდეგის ფსიქოლოგიური დასუსტება,[4] უნდობლობის გაჩენა საზოგადოებაში ხელისუფლების მიმართ და ზოგადად, სამიზნე ქვეყნის ეროვნული უსაფრთხოებისთვის ზიანის მიყენება (კიბერშპიონაჟის, საინფორმაციო ომის გამოყენებით, კრიტიკული ინფრასტრუტურაზე თავდასხმით). ამავე დროს, თუ გავითვალისწინებთ საქართველოს მისწრაფებებს ევრო-ატლანტიკურ სტრუქტურებში ინტეგრაციის მიმართულებით, კრიტიკულად მნიშვნელოანია ეფექტიანი კიბერუსაფრთხოების სისტემის არსებობა, რადგან მუდმივი კიბერთავდასხმების რისკი დასავლელ პარტნიორებში საქართველოს მიმართ უნდობლობას გააჩენს, რამაც შესაძლოა შეაფერხოს ქვეყნის დასავლურ სტრუქტურებთან ინტერგაცია. ამგვარად, ქვეყნის სტაბილური განვითარებისთვის კიბერსივრცეში არსებული სისუსტეები, ნათლად აჩვენებს ამ მიმართულებით პროაქტიული რეფორმების გატარების აუცილებლობას.

მეთოდოლოგია

აღნიშნული ნაშრომი ეყრდნობა კვლევის თვისებრივი მეთოდების შედეგად მიღებულ ინფორმაციას. კერძოდ, ოფიციალური დოკუმენტების ანალიზი და სიღრმისეული ინტერვიუ კიბერუსაფრთხოების დარგის ექსპერტებთან (პირველადი წყარო). ნაშრომში, აგრეთვე მოცემულია ჩვენი კვლევისთვის საინტერესო კიბერუსაფრთხოების შესახებ არსებული ლიტერატურისა და საერთაშორისო კვლევითი პუბლიკაციების ანალიზი (მეორადი წყარო).

4 Sarah P. White, "Understdaning Cyberwarfare, Lessons from the Russia-Georgia War," Modern War Institute, March 20, 2018, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.10.2020).

საქართველოს კიბერუსაფრთხოების პოლიტიკა და გამოწვევები

2008 წლის რუსეთ-საქართველოს ომის დროს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ, სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, მიზანმიმართული და მასობრივი კიბერთავდასხმები განახორციელა.[5] ამ კიბერთავდასხმებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა[6] და კიბერუსაფრთხოების მიმართულებით სახელმწიფო პოლიტიკის შემუშავების აუცილებლობა. კანონი ინფორმაციული უსაფრთხოების შესახებ, რომელიც 2012 წელს შევიდა ძალაში,[7] შეიძლება ამ მხრივ წინგადადგმულ ნაბიჯად მივიჩნიოთ. ეს კანონი დღემდე არეგულირებს სახელმწიფოს კიბერუსაფრთხოების პოლიტიკას. 2013-2015[8] და 2017-2018[9] წლებში, ასევე შემუშავდა საქართველოს კიბერუსაფრთხოების სტრატეგია და სამოქმედო გეგმა. საქართველოს კიბერგარემოს უსაფრთხოების უზრუნველსაყოფად შეიქმნა კიბერუსაფრთხოების სტრუქტურები თავდაცვის სამინისტროში (კიბერუსაფრთხოების ბიურო),[10] შინაგან საქმეთა სამინისტროსა და (კიბერდანაშაულის ბიურო),[11] იუსტიციის სამინისტროში (ციფრული მმართველობის სააგენტო). ამ სტრუქტურებმა ქვეყნის კიბერუსაფრთხოების პოლიტიკის სისტემური უზრუნველყოფა კიდევ უფრო განამტკიცეს. ინფორმაციული უსაფრთხოების შესახებ კანონის შესაბამისად, დადგინდა ინფორმაციული უსაფრთხოების მინიმალური სტანდარტი, შემოვიდა „კრიტიკული ინფორმაციული სისტემის სუბიექტის“ ცნება![12]

5 ანდრია გოცირიძე, ვლადიმერ სვანაძე, “კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები,” სსიპ კიბერუსაფრთხოების ბიურო, საქართველოს თავდაცვის სამინისტრო, 2015, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.10.2020).

6 *იქვე.*

7 საქართველოს კანონი “ინფორმაციული უსაფრთხოების შესახებ,” 2012 წლის 1 ივლისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

8 საქართველოს პრეზიდენტის ბრძანებულება №321, “საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013–2015 წწ. სამოქმედო გეგმის დამტკიცების შესახებ,” 2013 წლის 17 მაისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 25.10.2020).

9 საქართველოს მთავრობის დადგენილება №159, “საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ, “2017 წლის 13 იანვარი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 25.10.2020).

10 კიბერუსაფრთხოების ბიურო, საქართველოს თავდაცვის სამინისტრო, ხელმისაწვდომია **ბმულზე** (მოძიებულია:10.10.2020).

11 კიბერდანაშაულის ბიურო, საქართველოს შინაგან საქმეთა სამინისტრო, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.10.2020).

12 საქართველოს კანონი “ინფორმაციული უსაფრთხოების შესახებ,” 2012 წლის 1 ივლისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

„კრიტიკული ინფორმაციული სისტემის სუბიექტი" განიმარტა, როგორც ორგანიზაცია, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური და საზოგადოებრივი უსაფრთხოებისთვის. აღსანიშნავია, რომ კანონის თანახმად, ინფორმაციული უსაფრთხოების პოლიტიკის შესრულების პასუხისმგებლობა ვრცელდება მხოლოდ იმ იურიდიულ პირებსა და სახელმწიფო ორგანოებზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტებს წარმოადგენენ. მოქმედი კანონმდებლობით, ასეთი სულ 39 სუბიექტია.

ინფორმაციული უსაფრთხოების მართვის სტრუქტურა

არსებული კანონმდებლობით, ინფორმაციული უსაფრთხოების წესების შესრულების უზრუნველყოფა და მისი კოორდინაცია **ციფრული მმართველობის სააგენტოს** (მანამდე, მონაცემთა გაცვლის სააგენტო) კომპეტენციას წარმოადგენს. თავად სააგენტო კი, იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირია. ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს, რომელსაც სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO)[14] და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA)[15] მიერ დადგენილი სტანდარტებისა და მოთხოვნების შესაბამისად, ციფრული მმართველობის სააგენტო განსაზღვრავს. სააგენტოს დაქვემდებარებაშია აგრეთვე **კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი**, რომელიც საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვასა და კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრაზეა პასუხისმგებელი.[16]

რაც შეეხება თავდაცვის სტრუქტურებში ინფორმაციული უსაფრთხოების მინიმალური სტანდარტის დანერგვასა და დაცვას, მასზე პასუხისმგებელი **თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროა.** 2014 წლიდან, თავდაცვის სფეროს კრიტიკული ინფორმაციული სისტემის სუბიექტების უსაფრთხოებასა და კიბერთავდასხმის ან/და კომპიუტერული უსაფრთხოების ინციდენტების განეიტრალებაზე პასუხისმგებელია

13 საქართველოს მთავრობის დადგენილება №312, "კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ," 2014 წლის 29 აპრილი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

14 Intnational Organization for Standardization (ISO), ხელმისაწვდომია **ბმულზე** (მოძიებულია: 20.10.2020).

15 Information Systems Audit and Control Association (ISACA), ხელმისაწვდომია **ბმულზე** (მოძიებულია: 20.10.2020).

16 მარი მალვენიშვილი, ნინი ბალარჯიშვილი, "კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები," ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI), თბილისი, აგვისტო, 2020.

ბიუროს დაქვემდებარებაში მყოფი **კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი**.[17] აღსანიშნავია, რომ კიბერუსაფრთხოების ბიუროს მოქმედების სფერო არ ვრცელდება ციფრული მმართველობის სააგენტოზე.

2012 წლიდან საქართველოს **შინაგან საქმეთა სამინისტროს** ცენტრალური კრიმინალური პოლიციის დეპარტამენტის დაქვემდებარებაში ფუნქციონირებს **კიბერდანაშაულთან ბრძოლის სამმართველო**, რომელიც პასუხისმგებელია კიბერსივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენაზე, აღკვეთასა და პრევენციაზე, მთელი ქვეყნის მასშტაბით. სამმართველო ასევე წარმოადგენს საერთაშორისო საკონტაქტო პუნქტს, რომელიც ასრულებს საერთაშორისო საპოლიციო თანამშრომლობასთან დაკავშირებულ ფუნქციებს „კიბერდანაშაულის შესახებ" ევროპის საბჭოს კონვენციის შესაბამისად.

სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო - 2013 წლის კონსტიტუციური რეფორმის შემდგომ, ეროვნულ უსაფრთხოებასთან დაკავშირებულმა საკითხებმა, კიბერუსაფრთხოების ჩათვლით, საქართველოს მთავრობის პირდაპირ დაქვემდებარებაში გადაინაცვლა. კერძოდ, კიბერუსაფრთხოების პოლიტიკის ძირითად მაკოორდინირებელ უწყებად განისაზღვრა 2014 წელს ჩამოყალიბებული სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო. თუმცა, **„ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ"** საქართველოს კანონში შეტანილი ცვლილებების საფუძველზე, 2018 წლის 1-ლი იანვრიდან **სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო** გაუქმდა და მის ნაცვლად, პრემიერ-მინისტრის დაქვემდებარებაში, ჩამოყალიბდა **საგანგებო სიტუაციების მართვის სამსახური.** 2019 წელს გატარებული საკანონმდებლო ცვლილებების საფუძველზე კი, ეროვნული უსაფრთხოების საბჭო შეიქმნა, რომლის უმთავრეს მიზანს ეროვნული უსაფრთხოებისა და სახელმწიფო ინტერესებისთვის საფრთხის შემცველ საკითხებზე პოლიტიკური გადაწყვეტილებების მომზადება, სტრატეგიულ დონეზე ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის მიზნით, რეკომენდაციების შემუშავება და პრემიერ-მინისტრის ინფორმირება წარმოადგენს.[18]

ამგვარად, ბოლო წლებში სახელმწიფოს მიერ გადადგმული ნაბიჯები, კიბერუსაფრთხოების პოლიტიკის სტრუქტურული უზრუნველყოფის მიმართულებებით, ცალსახად დადებითი მოვლენაა. დარგის ექსპერტების მოსაზრებით, საკონანმდებლო ბაზის და ძირითადი სტრუქტურების შექმნამ განაპირობა ის, რომ გაერთიანებული ერების საერთაშორისო სატელეკომუნიკაციო ორგანიზაციის კიბერუსაფრთხოების ინდექსში[19]

[17] *იქვე.*

[18] *იქვე.*

[19] "Georgia ranks 9th in Europe for cyber security," Agenda.ge, April 2, 2019, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 28.10.2020).

საქართველო, მსოფლიო მასშტაბით, პირველ ათეულშია.[20] აღნიშნული ინდექსის მისაღებად კვლევა კიბერუსაფრთხოების 5 ძირითადი მიმართულებით მიმდინარეობს: საკანონმდებლო ბაზა, ტექნიკური აღჭურვილობა, ორგანიზაციული სტრუქტურა, შესაძლებლობების განვითარება და თანამშრომლობა.

თუმცა, კიბერუსაფრთხოების საბაზისო კანონმდელობის, პოლიტიკის სტრუქტურის ჩამოყალიბებისა და კიბერუსაფრთხოების სტრატეგიის ორჯერ შემუშავების მიუხედავად, კვალავაც პრობლემურია მისი აღსრულების საკითხი. დარგის ექსპერტები ხაზგასმით აღნიშნავენ ინფორმაციული უსაფრთხოების წესებისა და სტანდარტების დანერგვის პრობლემაზე, რადგან მიუხედავად კანონში "ინფორმაციული უსაფრთხოების შესახებ" გაწერილი ვალდებულებებისა, კრიტიკული ინფორმაციული სისტემის სუბიექტების უმეტესობაში მისი აღსრულება ჯერაც პრობლემურ საკითხად რჩება. ეს განპირობებულია იმ ფაქტით, რომ სახელისუფლებო დონეზე კიბერსივრციდან მომავალი საფრთხეები სერიოზულად არ აღიქმება, რაც კიბერცნობიერების დაბალი დონით აიხსნება. გარდა ამისა, კიდევ ერთ პრობლემას აღსრულების საკითხში, წარმოადგენს ის გარემოება, რომ ხელისუფლების ცვლილებისას, წინა ადმინისტრაციის დროს დაწყებული რეფორმები ჩერდება ან ქრება დღის წესრიგიდან და ახალი ადმინისტრაცია თავიდან იწყებს მასზე მუშაობას. ეს კი, გარდა დროისა და რესურსის დაკარგვისა, პოლიტიკური სისტემის არაჯანსაღ დამოკიდებულებაზე მიანიშნებს, ქვეყნის ეროვნული უსაფრთხოებისთვის კრიტიკულად მნიშვნელოვანი საკითხების მიმართ.

აღსანიშნავია, რომ IDFI-ის მიერ გამოთხოვილ დოკუმენტში, სახელმწიფო აუდიტის სამსახურის 2013-2020 წლებში „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონის აღსრულებასთან დაკავშირებით, კრიტიკული ინფორმაციული სისტემების სუბიექტების შემოწმების აქტებიდან და სამსახურის მიერ გაცემული რეკომენდაციების დასკვნიდან ნათლად იკვეთება, რომ კიბერუსაფრთხოების პოლიტიკის დაცვა და კანონის მოთხოვნების შესრულება კრიტიკული ინფორმაციის სუბიექტებად განსაზღვრულ 39 სამთავრობო დაწესებულებაში პრიორიტეტს არ წარმოადგენს. სამსახურების უმრავლესობის მხრიდან, ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები, აგრეთვე, ინფორმაციული უსაფრთხოების პოლიტიკა არ იყო დამტკიცებული, ხოლო ინფორმაციული უსაფრთხოების მენეჯერი (ასეთის არსებობის შემთხვევაში) წარმოადგენდა ფორმალურ თანამდებობას და ვერ პასუხობდა კანონით გათვალისწინებულ მოთხოვნებს.[21]

---

20 "Global Cybersecurity Index (GCI) 2018," International Telecomincation Union (ITU), ხელმისაწვდომია **ბმულზე** (მოძიებულია: 28.10.2020).

21 მარი მალვენიშვილი, ნინი ბალარჯიშვილი, "კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები," ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI), თბილისი, აგვისტო, 2020.

უკანასკნელ პერიოდში, კიბერუსაფრთხოების პოლიტიკის მიმართულებით სტაგნაცია ერთ-ერთი ექსპერტის აზრით, უკავშირდება უსაფრთხოებისა და კრიზისების მართვის საბჭოს გაუქმებას. რის შემდეგაც,

,,საქართველოს კიბერუსაფრთხოების არქიტექტურაში აღარ არსებობს ქმედითი მაკოორდინირებელი ორგანო, რომელიც უზრუნველყოფდა სახელმწიფო კიბერაქტორების ურთიერთშეთანხმებულ მუშაობას, კერძო აქტორებთან თანამშრომლობას და სტრატეგიულ დოკუმენტაციაზე ერთობლივ მუშაობას. აღნიშნული, სავარაუდოდ, ერთ-ერთი მიზეზია იმისა, რომ 2020 წელსაც საქართველო სამწუხაროდ, კიბერუსაფრთხოების ეროვნული სტრატეგიის გარეშე შეხვდა''.

კიბერთავდასხმების გავლენა საქართველოს ეროვნულ უსაფრთხოებაზე

კიბერსივრცეში საქართველოს მოწყვლადობის მაღალი ხარისხი საფრთხეს წარმოადგენს ეროვნული უსაფრთხოებისა და ქვეყნის შემდგომი სტაბილური განვითარებისთვის. საქართველოს გეოპოლიტიკური მდებარეობისა და არჩეული პროდასავლური კურსის გამო, ქვეყანა, ჩრდილოელი მეზობლის მხრიდან კიბერთავდასხმების განსაკუთრებულ სამიზნეს წარმოადგენს. კიბერუსაფრთხოების დარგის სპეციალისტების მოსაზრებით, საქართველოს კიბერსივრცისთვის ყველაზე რეალური საფრთხის შემცველი სწორედ რუსეთის კიბერაქტივობებია, თავისი საინფორმაციო-ტექნიკური და საინფორმაციო-ფსიქოლოგიური ეფექტით. საგულისხმოა, რომ კიბერსაფრთხეების მასშტაბი მზარდია, როგორც სირთულის, ისე მრავალფეროვნების თვალსაზრისით. რუსეთის მიერ განხორციელებულმა ან მხარდაჭერილმა, საინფორმაციო-ტექნიკურ შედეგზე ორიენტირებულმა, კიბერშეტევამ საქართველოში შესაძლოა გამოიწვიოს მნიშვნელოვანი ზარალი და მსხვერპლიც კი.სხვადასხვა კიბერარხებით გავრცელებულმა პროპაგანდისტულმა კონტენტმა კი, შესაძლოა საინფორმაციო-ფსიქოლოგიური ეფექტი იქონიოს: კრემლის სასარგებლოდ ცნობიერების შეცვლა, პროდასავლური განწყობების შემცირება და პრორუსული ელიტის ფორმირება-გაძლიერება. აქვე მნიშვნელოვანია, აღინიშნოს ბოლო წლებში საქართველოს პოლიტიკურ ასპარეზზე გამოჩენილი ღიად პრორუსული ძალები (რუსეთის გავლენის აგენტები),[22] რომელთა გააქტიურება სწორედ რუსეთის საუკეთესო ინტერესებს ემსახურება.

კიბერსივრციდან საფრთხეები შესაძლოა მომდინარეობდეს ისეთი აქტორებისაგან, როგორებიცაა:

- მაღალგანვითარებული კიბერშეტევითი პოტენციალის მქონე ქვეყნები (რუსეთი, ჩინეთი, ირანი, ჩრდ. კორეა და სხვა);
- ტერორისტული ორგანიზაციების კიბერდანაყოფები და იდეოლოგიურად მოტივირებული ან ექსტრემისტულად განწყობილი ჰაკერები;
- არასახელმწიფო აქტორები: ფინანსურად მოტივირებული კიბერდამნაშავეები.[23]

[22] ირაკლი ჯღარკავა, "საქართველო რუსეთის გავლენის აგენტების სამიზნედ კიბერეპოქაში" 2019, საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.11.2020).

[23] James R. Clapper, "Worldwide Cyber Threats," September 10, 2015, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 12.11.2020).

ექსპერტების თვალსაზრისით, ირანისა და ჩინეთის მხრიდან მომდინარე კიბერსაფრთხეები, საქართველოსთან მეგობრული ურთიერთობის გამო, მინიმალურია. თუმცა, ჩინეთის მხრიდან, უპირველეს ყოვლისა, არ უნდა გამოგვრჩეს არასახელმწიფო აქტორების მიერ განხორციელებული კიბერშპიონაჟის ალბათობა. რაც შეეხება ირანის ექსტრემისტულად განწყობილ ჰაკერებს, მათ ინტერესს შესაძლოა წარმოადგენდეს საქართველოში განთავსებული იმ სახელმწიფოების ინფრასტრუქტურა და მონაცემთა ბაზები, რომელთაც ისინი საკუთარ იდეოლოგიურ მოწინააღმდეგედ განიხილავენ (აშშ, ნატოს და ევროკავშირის წევრი ქვეყნები). ტერორისტული ორგანიზაციების მხრიდან დიდია ალბათობა ისეთი კიბერშეტევის განხორციელებისა, რომელიც გამოიწვევს ელექტრონული სერვისების და ვებ-გვერდების დროებით, ლოკალურ დაზიანებას. მასობრივი ზიანის ან მსხვერპლის გამომწვევი კიბერშეტევის ორგანიზება და განხორციელება, ამ ეტაპზე, ნაკლებად სავარაუდოა. რაც შეეხება ფინანსურად მოტივირებულ კიბერკრიმინალებს, მათი სამიზნე შესაძლოა საქართველოში საფინანსო და საბანკო სექტორი გახდეს.

დარგის ექსპერტების თვალსაზრისით, საქართველოს ეროვნული უსაფრთხოებისთვის საგულისხმოა კიბერსივრციდან მომდინარე შემდეგი საფრთხეების გათვალისწინება:

რუსეთიდან მომდინარე კიბერსაფრთხე - დღეს არსებული მდგომარეობით, საქართველოსთვის რუსეთის ფედერაციიდან მომდინარე კიბერსაფრთხე რეალურია და ბოლო წლებში მისი დონე გაზრდილია. კრემლმა არათუ შეცვალა საკუთარი აგრესიული კიბერპოლიტიკა, არამედ მნიშვნელოვნად აამაღლა სახელმწიფოს კიბერშეტევითი პოტენციალი და გააფართოვა კიბეროპერაციების გამოყენების არეალი. ტექნიკურ ეფექტზე ორიენტირებული შეტევებს, კიბერსივრცეში მიმდინარე ფსიქოლოგიური გავლენის ოპერაციებიც დაერთო. საფრთხეების ზრდის ერთ-ერთი ფაქტორი ის გარემოებაცაა, რომ 2008 წელთან შედარებით, მნიშვნელოვნად არის გაზრდილი საქართველოს დამოკიდებულება ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე, რაც პოტენციური კიბერთავდასხმების შემთხვევაში, თავის მხრივ, ზრდის მოსალოდნელი ზიანის მასშტაბებს. ექსპერტები, აგრეთვე მიუთითებენ, რუსეთის მიერ **ინდუსტრიის კონტროლის სისტემების (ICS)** მწყობრიდან გამოყვანის მექანიზმების ფლობაზე. აშშ-ის დაზვერვის მონაცემებით[24], რუსეთი, სულ ცოტა 2015 წლიდან ფლობს შესაძლებლობას განახორციელოს დისტანციური წვდომა მოწინააღმდეგის კრიტიკული ინფორმაციული სისტემის მაკონტროლებელ პროგრამულ უზრუნველყოფაზე. ამავე მონაცემებით, რუსეთთან აფილირებულმა კიბერაქტორებმა წარმატებით განახორციელეს რამდენიმე მწარმოებლის/გამყიდველის პროდუქტის მიწოდების ჯაჭვის (supply chain) კომპრომეტაცია, იმგვარად, რომ ლეგალური განახლებების ჩამოწერის შედეგად, მომხმარებლის სისტემაში რუსული მალვეარი/ვირუსი აღმოჩნდა. აღსანიშნავია, რომ

[24] *იქვე.*

კიბერთავდასხმების 60%-ზე მეტი შემთხვევები გამოვლინდა სწორედ მიწოდების ჯაჭვის ქსელში არსებული უსაფრთხოების სისუსტეების შედეგად.[25]

კიბერშპიონაჟი - განსაკუთრებით საგულისხმოა კიბერშპიონაჟის წინააღმდეგ ეფექტური ბრძოლა. კიბერშპიონაჟის შედეგად, კიბერკრიმინალებს შესაძლოა სახელმწიფოს ისეთი საიდუმლოებების შესახებ ჩაუვარდეთ ინფორმაცია ხელთ, რამაც ქვეყნის ეროვნული უსაფრთხოება დიდად დააზარალოს. კიპერშპიონაჟი შეიძლება განხორციელდეს ისეთი მეთოდებით, როგორიცაა ე.წ. ფიშინგი ანსაჯარო უწყებების სისტემის დავირუსება. ამ მხრივ, დარგის ექსპერტები მიიჩნევენ, რომ სახელმწიფო უწყებებში დასაქმებული ადამიანების კიბერცნობიერების დონე, რომლებიც შესაძლოა გახდნენ კიბერშპიონაჟისთვის ხელისშემწყობი ფაქტორები, საგანგაშოა. 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. 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 თავდაცვისა და გეოპოლიტიკურ საკითხებზე ინფორმაციის შეგროვება წარმოადგენს, რაც მხოლოდ სახელმწიფოსათვის შეიძლება იყოს საინტერესო.[26]

კრიტიკული ინფრასტრუქტურის ფუნქციონირების სხვადასხვა ხარისხის მოშლა ან შეფერხება DDoS ან Defacement ტიპის შეტევების შედეგად. ცნობილია, რომ სუსტად დაცული ინფრასტრუქტურის პირობებში, დაბალტექნოლოგიური DDoS და Defacement შეტევაც კი, შესაძლოა არაპროპორციულად მაღალი ზარალის მიზეზი გახდეს.

შეღწევა მიწოდების ჯაჭვის (supply chain) საფრთხეების გზით - გულისხმობს ინფილტრაციას პროდუქტის მომწოდებლის ან წარმოების და ლოჯისტიკის ხარვეზის საშუალებით. როგორც ექსპერტები აღნიშნავენ, უკანასკნელ პერიოდში, მეტად გახშირდა ამ ტიპის შეღწევის გამოყენება სახელმწიფოთა, განსაკუთრებით კი რუსეთის მხრიდან.

შიდა/ინსაიდერული საფრთხეები: სისტემაში შეღწევის ერთ-ერთი უმარტივესი გზა ინსაიდერის მეშვეობით განხორციელებული ინფილტრაციაა. ინსაიდერად მოიაზრება ყოფილი ან მოქმედი თანამშრომელი, კონტრაქტორი და ყველა ის სუბიექტი, ვისაც

25 Jake Frankenfield, "Supply Chain Attack," July 10, 2020, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

26 "APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?" Fireeye special report, 2014, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

შესაძლოა ლეგალური წვდომა ჰქონდეს საინფორმაციო სისტემებთან. ამ არხს ხშირად იყენებენ რუსული სპეცსამსახურები. მათ განსაკუთრებით აინტერესებთ ის პირები, ვინც ქვეყნის კრიტიკული ინფრასტრუქტურის უსაფრთხოებისთვის საპასუხისმგებლო პოზიციებზე მუშაობენ. აღსანიშნავია, რომ უკანასკნელ პერიოდში, აშშ-ის გახმაურებული, რუსეთთან დაკავშირებული, 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. საქართველოში ფიშინგის მსხვერპლთა საერთო პროცენტი კი 40-50%-მდე მერყეობს, რაც მეტად სარისკო მაჩვენებელია.[27] სწორედ ფიშინგის მეთოდით მოხდა ამერიკის დემოკრატიული პარტიის,[28] გერმანიის ბუნდესტაგისა და სხვა სახელმწიფო დაწესებულებების თუ ბიზნესის წამომადგენლების ქსელების კომპრომეტაცია რუსეთის სპეცსამსახურებთან დაკავშირებული კიბერაქტორების მიერ.[28]

კიბეროპერაციები საინფორმაციო ფსიქოლოგიური ეფექტით/საინფორმაციო ომი. კიბერარხებით გავრცელებულმა პროპაგანდისტულმა კონტენტმა (ე.წ. ყალბი ნიუსების გავრცელება), შესაძლოა გამოიწვიოს საინფორმაციო-ფსიქოლოგიური ეფექტი: კრემლის სასარგებლოდ ცნობიერების შეცვლა, პროდასავლური განწყობების შემცირება და პრორუსული ელიტის ფორმირება-გაძლიერება (რუსეთის გავლენის აგენტები).

ამგვარად, რაც უფრო განვითარდება საინფორმაციო და საკომუნიკაციო ტექნოლოგიები და გაზიარდება მათზე ჩვენი დამოკიდებულება, საფრთხეებიც მოიმატებს. ქვეყნის კრიტიკულ ინფრასტრუქტურაზე კარგად შესრულებული კიბერთავდასხმა გამოიწვევს შიშს, სამოქალაქო პანიკასა და მასობრივ არეულობებს. ასევე, პარალიზებული იქნება სახელმწიფო სტრუქტურები ყველა დონეზე და სახელმწიფო ინსტიტუტების მიმიმართ ნდობის საკითხი კითხვის ნიშნის ქვეშ დადგება. 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. ამავე დროს, მეტად მნიშვნელოვანია საზოგადოებრივი ცნობიერების ამაღლება, მუდმივი კონტაქტი კერძო სექტორში განთავსებულ კრიტიკულ ინფრასტრუქტურასთან, ადგილობრივი კანონმდებლობის საერთაშორისოსთან ჰარმონიზაცია და კიბერკრიმინალთან ბრძოლის სართაშორისო თანამშრომლობის მექანიზმების აქტიური გამოყენება.

---

[27] ანდრია გოცირიძე, კიბერუსაფრთხოების კონსულტანტი, ინტერვიუ, 2012 წლის 10 ნოემბერი, თბილისი.

[28] Raphael Satter, Jeff Donn, Chad Day, "Inside story: How Russians hacked the Democrats's emails," November 4, 2017, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 20.11.2020).

[29] BBC, "Russia 'was behind German parliament hack,'" May 13, 2016, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

როგორ შეიძლება მართოს საქართველომ კიბერსივრციდან მომავალი საფრთხეები

ცხადია, კიბერსივცრიდან მომავალი საფრთხეების სრული მართვა შეუძლებელია, რადგან კიბერუსაფრთხოების პოლიტიკის განვითარებასთან ერთად, კიბერკრიმინალებიც ხვეწენ თავდასხმის ახალ წესებს. თუმცა, კიბერუსაფრთხოების პროაქტიული პოლიტიკის არსებობის შემთხვევაში, შესაძლებელია სავარაუდო ზიანის შემცირება, პრევენცია და შესაბამისად, კიბერსივრცის მართვა.დარგის სპეციალისტების თვალსაზრისით, საქართველომ ქმედითი ნაბიჯები უნდა გადადგას, იმისათვის, რომ მოხდეს კიბერუსაფრთხოების ეროვნული სტრატეგიის შემუშავება, სადაც კიბერსივრიციდან მომავალი რისკები და საფრთხეები სწორად შეფასდება, გაანალიზდება და დეტალურად იქნება გაწერილი მათ წინააღმდეგ ბრძოლის მექანიზმები. აგრეთვე:

- უნდა შეიქმნას ძლიერი აღმასრულებელი ორგანო, რომელიც სახელმწფოს მიერ მიღებულ პოლიტიკას კოორდინაციასა და კონტროლს გაუწევს, როგორც სახელმწიფო უწყებებში, ისე კერძო სექტორში;
- სასიცოცხლოდ მნიშვნელოვანია სახელმწიფო ბიუჯეტში პრიორიტეტული გახდეს კიბერუსაფრთხოებასთან დაკავშირებული ხარჯები;
- სახელმწიფომ მეტად უნდა იზრუნოს ადამიანური კაპიტალის განვითარებაზე;
- მნიშვნელოვანია, როგორც ადგილობრივ დონეზე, სახელმწიფო უწყებებს შორის, ინფორმაციის გაცვლის მიზნით, ეფექტური თანამშრომლობა, ისე საერთაშორისო მიმართულებით ურთიერთობის გაძლიერება.

ამასთანავე, ექსპერტების თვალსაზრისით, საქართველოში კიბერუსაფრთხოების გაუმჯობესებისა და კიბერსივრციდან მომდინარე საფრთხეების უკეთ მართვის მიზნით, მნიშვნელოვანია სახელმწიფომ გაითვალისწინოს შემდეგი:

კრიტიკული ინფრასტრუქტურის განსაზღვრის დახვეწა და მისი საუკეთესო საერთაშორისო პრაქტიკასთან მიახლოება. დემოკრატიულ სახელმწიფოში კრიტიკული სერვისების უმეტესობა ბიზნესშია კონცენტრირებული, შესაბამისად, საუკეთესო საერთაშორისო პრაქტიკის მიხედვით, კრიტიკულ ინფრასტრუქტურას დიდწილად კერძო სექტორი წარმოადგენს.[30] ასეთი დარგებია ენერგეტიკისა და წყალმომარაგების სფერო, საბანკო და საფინანსო სექტორი, კვების, ქიმიური და სამხედრო მრეწველობა, სამედიცინო სეგმენტი და სხვა. საქართველოს

30 Critical Infrastructure Sectors, Cybersecurity & Infrastructure Security Agency, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

კანონმდებლობით, კრიტიკული ინფორმაციული სისტემების სუბიექტთა ნუსხა[31] მხოლოდ სამთავრობო ქსელების ერთ ნაწილს მოიცავს და იგი არ ვრცელდება ბიზნესის საკუთრებაში არსებულ სახელმწიფოსათვის კრიტიკულად მნიშვნელოვან დარგებზე.

თავდაცვის სფეროს კრიტიკული ინფრასტრუქტურის დახვეწა. დღეს მოქმედი კანონმდებლობა, თავდაცვის სფეროს კრიტიკულ ინფრასტრუქტურად თავად თავდაცვის სამინისტროს სისტემას მიიჩნევს, მაგრამ არ ითვალისწინებს კერძო სექტორის იმ ობიექტებს, რომელთა გამართული ფუნქციონირება სასიცოცხლოდ აუცილებელია თავდაცვის სფეროსათვის (მაგ., მომსახურე კვების კომპანია, სამხედრო მრეწველობა, ლოჯისტიკური ჯაჭვის შემადგენელი კერძო აქტორები).

შესყიდვების კანონმდებლობის ეროვნული უსაფრთხოების საკითხებთან ინტეგრირება. დღევანდელი შესყიდვების კანონმდებლობა[32] არ ითვალისწინებს კიბერსაფრთხეებს. ის შესაძლებელს ხდის კრიტიკული ინფრასტრუქტურისა თუ სახელმწიფო დაწესებულებებისთვის კომპიუტერული ტექნიკა, მომსახურებადა პროგრამული უზრუნველყოფა შესყიდულ იქნას საკუთრივ რუსული ორგანიზაციებისაგან ან თუნდაც სხვა ქვეყნის კომპანიების რუსეთის ოფისებისგან. იგივე კანონმდებლობა საშუალებას იძლევა ინტერნეტიზაციის და საინფორმაციო ტექნოლოგიებთან დაკავშირებული სხვა მსხვილი პროექტები, ასევე სამთავრობო სტრუქტურების მობილური საკომუნიკაციო მომსახურება, ოკუპანტი ქვეყნის ბიზნეს-ორგანიზაციებმა განახორციელონ. ეს კი სერიოზული რისკის ქვეშ აყენებს სახელმწიფოში არსებულ თითქმის ყველა ინფორმაციულ და საკომუნიკაციო ქსელსა თუ სისტემას. აქედან გამომდინარე, დარგის ექსპერტები საგანგაშოს უწოდებენ სამთავრობო სტრუქტურების საკომუნიკაციო მომსახურების გაწევის პრაქტიკას ოკუპანტი სახელმწიფოს კომპანიის/ების მხრიდან. რუსეთი მრავალგანზომილებიანი ჰიბრიდული ომის პირობებში წარმატებით იყენებს კიბერსივრცეს, ამიტომ კანონმდებლობაში არსებული მსგავსი ხარვეზები, რომლებიც ქვეყნის ეროვნულ უსაფრთხოებას პირდაპირი რისკის ქვეშ აყენებს, ყოვლად დაუშვებელია. ამგვარად, ექსპერტები მიიჩნევენ, რომ კონცეპტუალურ დონეზე უნდა მოხდეს მიწოდების ჯაჭვის (supply chain) რისკების მენეჯმენტის ინტეგრირება შესყიდვების პროცესსა თუ რისკების მართვის სისტემაში, რათა უზრუნველყოფილ იქნას სახელმწიფო სექტორის მიერ გამოყენებული ტექნიკისა და ტექნოლოგიების უსაფრთხოება და სანდოობა. ამავე დროს, აუცილებელია მოხდეს კიბერტექნოლოგიების, როგორც სპეციფიური საქონლისა და მომსახურების შესყიდვის განსაკუთრებული წესის შემუშავება, სადაც პროდუქტის სანდოობა და უსაფრთხოება ერთ-ერთი განმსაზღვრელი ფაქტორი იქნება. შეზღუდვა უნდა დაწესდეს რუსული

[31] საქართველოს მთავრობის დადგენილება №312, "კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ," 2014 წლის 29 აპრილი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

[32] საქართველოს კანონი "სახელმწიფო შესყიდვების შესახებ," 2005 წლის 18 მაისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 12.11.2020).

წარმოების ან რუსეთის გავლით საინფორმაციო-ტექნოლოგიური სისტემების, ტექნოლოგიების ან მომსახურების შესყიდვაზე.[33]

პოტენციური საფრთხეების შემცირება პრიტიკული სერვისების მომწოდებელი კერძო სექტორის მხრიდან / მონაცემთა დაცვის სტანდარტის უზრუნველყოფა. ექსპერტები აგრეთვე მიიჩნევენ, რომ ქვეყანაში, დღეს არსებული კონცეპტუალური და ნორმატიული ბაზა ვერ პასუხობს შიდა/ინსაიდერული საფრთხეების მზარდ მნიშვნელობას. მაშინ, როდესაც საბაზრო ეკონომიკის პირობებში, კრიტიკული სერვისების პროვაიდერი კერძო სექტორია, სახელმწიფო ორგანიზაციების ინფორმაციული მასივები ხშირად კონტრაქტორის ხელში ხვდება, რაც მნიშვნელოვნად ზრდის შიდა საფრთხეების მასშტაბს. საგულისხმოა, რომ საქართველოს რეალობაში, სახელმწიფო ორგანიზაციასთან ბიზნეს-ურთიერთობის ფარგლებში, კონტრაქტორისათვის გადაცემული სენსიტიური ინფორმაციის დაცვა, მხოლოდ ბიზნეს-ორგანიზაციის კეთილ ნებაზეა დამოკიდებული. ბიზნესი კი, მინიმალური დანახარჯით მაქსიმალური მოგების მიღებაზეა ორიენტირებული, ამიტომ უსაფრთხოებისათვის ზედმეტ გასავალს ერიდება. ეს საკითხი, შესაბამისი სახელმწიფო სტრუქტურების მხრიდან, სასწრაფო დარეგულირებას საჭიროებს, რადგან არავინ იცის რა რაოდენობის და რა სახის არასაიდუმლო, მაგრამ სენსიტიური ინფორმაციაა ამჟამად კერძო ქსელებში დაუცველად დაგროვილი. 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, ასევე მტრულად განწყობილი სახელმწიფოს კიბერაქტორებისათვის. ექსპერტების აზრით, განისაზღვროს მონაცემთა დაცვის ის სტანდარტი, რომლის შესრულებაც კონტრაქტორის მიერ სავალდებულო იქნება სახელმწიფო შესყიდვის განხორციელებისას. მეორე მხრივ, სახელმწიფო უნდა დაეხმაროს კერძო კომპანიებს, კონტრაქტორებს, სახელმწიფოსათვის მნიშვნელოვანი ინფორმაციის კიბერუსაფრთხოების გარკვეული სტანდარტის პირობებში დამუშავების უზრუნველყოფაში.

ზოგადი კიბერცნობიერების დონის ამაღლება. სასიცოცხლოდ მნიშვნელოვანია კიბერუსაფრთხოების, როგორც არსებითი პრობლემის აღქმა, სახელმწიფოსა თუ ბიზნეს სექტორის მაღალი რგოლის მენეჯმენტის მხრიდან. ექსპერტები სამწუხაროს უწოდებენ ცნობიერების იმ დონეს, რომელიც უშვებს რუსული ანტივირუსული უზრუნველყოფისა თუ ელექტრონული ფოსტის გამოყენებას სახელმწიფო უწყებების მხრიდან. შედარებისათვის, სწორედ კიბერრისკების ზრდის მოტივით (მონაცემთა შეგროვება, ტრეკინგი), ლიეტუვას

[33] *მსგავსი პრეცენდენტი აშშ-ის სპეცსამსახურებმა შექმნეს, სადაც, ცნობილი კასპერსკის სკანდალის შემდგომ, სახელმწიფო უწყებებს 90 დღე მიეცათ აღნიშნული პროგრამული უზრუნველყოფის დეინსტალაციისათვის.*

შესაბამისმა სამთავრობო უწყებამ რეკომენდაცია მისცა სახელმწიფო მოხელეებს, არ ესარგებლათ იანდექს-ტაქსის მომსახურებით.[34] იმ პირობებში როდესაც, რუსეთში სახელმწიფო და არასახელმწიფო აქტორებს შორის ზღვარი წაშლილია, დიდი რისკის შემცველია ქართული სახელმწიფო დაწესებულებებისთვის საკომუნიკაციო მომსახურების მიღება ოკუპანტი ქვეყნის კომპანიის მხრიდან, რომელიც მრავალგანზომილებიან ჰიბრიდულ ომს აწარმოებს საქართველოს წინააღმდეგ, მათ შორის წარმატებით იყენებს კიბერსივრცეს ამ პროცესში. უნდა აღინიშნოს, რომ მომსახურე კომპანიას შეუძლია ნებისმიერ ინტერესის ობიექტზე მიიღოს ინფორმაცია თუ სად რეკავს, რა პერიოდულობით, რომელ ვებ გვერდებს იყენებს, რა თემატიკით ინტერესდება, რას აგზავნის სამსახურებრივი ელ. ფოსტით, მოკლეტექსტური შეტყობინებით და სხვა. საჭიროების შემთხვევაში, ტექნიკურად შესაძლებელია კონტენტის გაშიფვრა, მომხმარებლის გადაადგილების მარშრუტის დადგენა და მობილური ხელსაწყოს ვირუსით ინფიცირება, ისე, რომ მოპოვებულ იქნას პირადი ცხოვრების ამსახველი თუ სამსახურებრივი კადრები. ამას გარდა, პროვაიდერის ხელში გადადის მონაცემთა ბაზების დიდი მასივი, რომლის სწორი ანალიზითაც, დაინტერესების შემთხვევაში, მნიშვნელოვანი სადაზვერვო ინფორმაციის მოპოვებაა შე საძლებელი. ამვარად, სახელმწიფო მმართველობის ყველა დონეზე, აუცილებელია, კიბერუსაფრთხოების ცნობიერების ასამაღლებელ ღონისძიებათა კომპლექსის შემუშავება და დანერგვა.

მიუხედავად იმისა, რომ სამხედრო პოტენციალის თვალსაზრისით განსხვავება ჩვენსა და მოწინააღმდეგეს შორის დიდია, ექსპერტები მიიჩნევენ, რომ კიბერსივრცე ის არეალია, სადაც პატარა ქვეყანას რეალურად შეუძლია წინააღმდეგობა გაუწიოს რიცხოვნობით დიდად აღმატებულ აგრესორს. იგი შესაძლოა გახდეს მის ქმედებებზე ასიმეტრიული პასუხის ერთ-ერთი წარმატებული ელემენტი ან წინააღმდეგობის მოქმედი ფრონტი. გარდა ამისა, დასანერგია მიდგომა, რომ კიბერუსაფრთხოება საერთო პასუხისმგებლობაა და რომ ინფორმაციის გაცვლის, ეფექტური საერთაშორისო თუ უწყებათაშორისი თანამშრომლობის გარეშე, ქვეყანა ვერ შეძლებს სრულყოფილად შეასრულოს სანდო პარტნიორის ფუნქცია კიბერსივრცეში.

34 "Lithuania Warns Yandex Taxi App Could Be Snooping on Users," Bloomberg, 2018 წლის 31 ივლისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

დასკვნა

2008 წლის შემდეგ, როდესაც საქართველო პირველად გახდა ფართომასშტაბიანი კიბერთავდასხმების ობიექტი, ქვეყანამ კიბერუსაფრთხოების პოლიტიკის მიმართულებით არაერთი ნაბიჯი გადადგა. მიიღო კანონი ინფორმაციული უსაფრთხოების შესახებ, ჩამოაყალიბა კიბერუსაფრთხოების მართვის სისტემა და ორჯერ შეიმუშავა კიბერუსაფრთხოების სტრატეგია. მიმდინარეობს მუშაობა მესამე სტრატეგიაზეც. ეს ნაბიჯები ცალსახად დადებითი მოვლენებია. თუმცა, მიუხედავად მიღებული კანონისა და კიბერუსაფრთხოების სტრატეგიებისა, უმთავრეს გამოწვევას სწორედ, რომ მათი ცხოვრებაში გატარება წარმოადგენს, როგორც სახელმწიფო სტრუქტურების ისე კერძო სექტორის მხრიდან, რაც ქვეყნის კრიტიკულ ინფრასტრუქტურას და შესაბამისად, ეროვნულ უსაფრთხოებას დიდი რისკის ქვეშ აყენებს.

ამრიგად, გახშირებული კიბერშეტევების ფონზე, რის ნათელ მაგალითადაც შეგვიძლია მოვიყვანოთ 2019 წლის ოქტომბერში განხორციელებული თავდასხმა, რომლის შედეგადაც გაითიშა საქართველოს პრეზიდენტის, სასამართლოების, საკრებულოებისა და მედიასაშუალებების ვებგვერდები, აგრეთვე, 2020 წლის სექტემბერში ლუგარის ლაბორატორიაზე განხორციელებული კიბერშეტევა, ნათელია, რომ კიბერუსაფრთხოებაზე ზრუნვა სახელმწიფოს ერთ-ერთი მთავარი პრიორიტეტი უნდა გახდეს. კიბერუსაფრთხოების მიმართულებით ქმედითი ნაბიჯების გადადგმა (მაღალტექნოლოგიური შეტევების თავიდან არიდება და საფრთხეების შემცირება) პირდაპირ დაკავშირებულია სოლიდურ ფინანსურ რესურსებთან, თუმცა, ვინაიდან ქვეყნის ეროვნული უსაფრთხოება დიდ არის ამ სფეროს განვითარებაზე დამოკიდებული, ქვეყნის ბიუჯეტში კიბერუსაფრთხოება უნდა გახდეს პრიორიტეტული. შესაბამისად, აუცილებელია, საქართველომ მეტი რესურსი დახარჯოს კიბერთავდაცვაზე, ეფექტიანი თავდაცვითი კიბერუსაფრთხოების პოლიტიკის შემუშავების მიმართულებით, რომელსაც ექნება უფრო პროაქტიული - გრძელვადიან პერსპექტივებზე გათვლილი მიზნები.

ბიბლიოგრაფია

პირველადი წყაროები:

- საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ," 2012 წლის 1 ივლისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

- საქართველოს კანონი "პერსონალურ მონაცემთა დაცვის შესახებ," 2012 წლის 16 იანვარი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.10.2020).

- საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონში ცვლილების შეტანის თაობაზე," 2020 წლის 26 ივნისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.11.2020).

- საქართველოს მთავრობის დადგენილება №312, "კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ," 2014 წლის 29 აპრილი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

- საქართველოს კანონი "ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ," 2015 წლის 23 მარტი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.10.2020).

- საქართველოს კანონი "სახელმწიფო შესყიდვების შესახებ," 2005 წლის 18 მაისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 12.11.2020).

- საქართველოს პრეზიდენტის ბრძანებულება №321, "საქართველოს კიბერუსაფრთხოების სტრატეგიისა და საქართველოს კიბერუსაფრთხოების სტრატეგიის განხორციელების 2013–2015 წწ. სამოქმედო გეგმის დამტკიცების შესახებ," 2013 წლის 17 მაისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 25.10.2020).

- საქართველოს მთავრობის დადგენილება №159, "საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ, "2017 წლის 13 იანვარი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 25.10.2020).

- საქართველოს მთავრობის დადგენილება №562 "საგანგებო სიტუაციების მართვის სამსახურის დებულების დამტკიცების შესახებ," 2017 წლის 25 დეკემბერი, ხელმისაწვდომია **ბმულზე** (მოძეიებულია: 20.10.2020).

- საქართველოს მთავრობის დადგენილება №337 "ეროვნული უსაფრთხოების საბჭოს აპარატის დებულების დამტკიცების თაობაზე," 2019 წლის 17 ივლისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 20.10.2020).

ინტერვიუ:

- **ანდრია გოცირიძე,** კიბერუსაფრთხოების კონსლუტანტი, კიბერუსაფრთხოების ბიუროს დირექტორი 2014-2017 წლებში, 2012 წლის 10 ნოემბერი, თბილისი.

- **მარი მალვენიშვილი,** კიბერუსაფრთხოების საგანმანათლებლო-კვლევითი ცენტრის (CYSEC) აღმასრულებელი დირექტორი, 2020 წლის 12 ნოემბერი, თბილისი.

- **მაქსიმ იავიჩი,** სამეცნიერო კიბერ უსაფრთხოების ასოციაციის პრეზიდენტი, კავკასიის უნივერსიტეტის პროფესორი, კიბერუსაფრთხოების მიმართულების ხელმძღვანელი, 2020 წლის 30 ოქტომბერი, თბილისი.

- **მიხეილ ბასილაია,** თანადამფუძნებელი, კიბერჰაუზი (Cyberhouse), 2020 წლის 6 ნოემბერი, თბილისი.

- **მიხეილ კაპანაძე,** ინფორმაციული სისტემების არქიტექტორი, 2020 წლის 6 ნოემბერი, თბილისი.

მეორადი წყაროები:

- გოცირიძე, ანდრია, სვანაძე, ვლადიმერ, "კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები," სსიპ კიბერუსაფრთხოების ბიურო, საქართველოს თავდაცვის სამინისტრო, 2015, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.10.2020).

- მალვენიშვილი, მარი, ბალარჯიშვილი, ნინი, "კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები," ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI), თბილისი, აგვისტო, 2020.

- ჯღარკავა, ირაკლი, "საქართველო რუსეთის გავლენის აგენტების სამიზნედ კიბერეპოქაში" 2019, საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.11.2020).

- BBC, "Russia 'was behind German parliament hack,'" May 13, 2016, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

Clapper R. James, "Worldwide Cyber Threats," September 10, 2015, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 12.11.2020).

Frankenfield, Jake, "Supply Chain Attack," July 10, 2020, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

Satter, Raphael, Donn, Jeff, Day, Chad, "Inside story: How Russians hacked the Democrats's emails," November 4, 2017, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 20.11.2020).

White P. Sarah, "Understdaning Cyberwarfare, Lessons from the Russia-Georgia War," Modern War Institute, March 20, 2018, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.10.2020).

"APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?" Fireeye special report, 2014, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

Critical Infrastructure Sectors, Cybersecurity & Infrastructure Security Agency, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

"Convention on Cybercrime," Council of Europe, 2001, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 20.10.2020).

"Lithuania Warns Yandex Taxi App Could Be Snooping on Users," Bloomberg, 2018 წლის 31 ივლისი, ხელმისაწვდომია **ბმულზე.**

[I] საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ," 2012 წლის 1 ივლისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

[II] საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ," 2012 წლის 1 ივლისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

[III] საქართველოს კანონი "ინფორმაციული უსაფრთხოების შესახებ," 2012 წლის 1 ივლისი, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 27.10.2020).

[IV] Inustrial Control System, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.11.2020).

[V] Fruhlinger, J., "Malware explained: How to prevent, detect and recover from it," May 17, 2019, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.11.2020).

[VI] Phishing vs Spear Phishing, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 12.11.2020).

[VII] Frankenfield, Jake, "Supply Chain Attack," July 10, 2020, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 15.11.2020).

[VIII] Denial-of-service (DoS) attack, ხელმისწავდომია **ბმულზე** (მოძიებულია: 10.11.2020).

[IX] Website Defacement, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 12.11.2020).

[X] Distributed Denial-of-Service (DDoS) attack, ხელმისწავდომია **ბმულზე** (მოძიებულია: 10.11.2020).

[XI] Reiff, Nathan, "What Is the Dark Net?" January 11, 2020, ხელმისაწვდომია **ბმულზე** (მოძიებულია: 10.11.2020).