www.rusi.org

თემატური ანგარიში

კიბერდანაშაულის გამოცდილება საქართველოში

ინფორმირებულობა, ვიქტიმიზაცია და მიმართთვიანობა

ჯოზეფ იარნეცკი, ნათია სესკურია და თათია ჩიხლაძე

თემატური ანგარიში

თავდაცვისა და უსაფრთხოების თემების ირგვლივ გავლენებისგან თავისუფალი მსჯელობის 192 წელი

გაერთიანებული სამეფოს თავდაცვისა და უსაფრთხოების კვლევების გაერთიანებული სამსახურების სამეფო ინსტიტუტი (RUSI) მსოფლიოს უძველესი და დიდი ბრიტანეთის წამყვანი კვლევითი ინსტიტუტია თავდაცვისა და უსაფრთხოების საკითხებში. მისი მისიაა ინფორმირება, გავლენის მოხდება და საჯარო დისკუსიების წახალისება უფრო უსაფრთხო და სტაბილური მსოფლიოს თაობაზე. RUSI-ს საქმიანობის ძირითადი მიმართულება კვლევა და მიგნებებზე დაფუძნებული, ობიექტური და ინოვაციური ანალიზის შეთავაზებაა დღევანდელობის კომპლექსურ გამოწვევებთან გამკლავების მიზნით.

ორგანიზაცია 1831 წელს დაარსდა და ამ დროიდან მოყოლებული, მისი საქმიანობის ძირითადი დასაყრდენი მისივე წევრებია. სწორედ მათი მხარდაჭერითა და ასევე, კვლევის, საგამომცემლო საქმიანობისა და კონფერენციების ორგანიზებიდან მიღებული შემოსავლის მეშვეობით ორგანიზაცია დაარსებიდან 192 წლის შემდეგაც ინარჩუნებს პოლიტიკურ დამოუკიდებლობას.

გამოქვეყნებულია 2023 წელს თავდაცვისა და უსაფრთხოების კვლევების სამსახურების სამეფო ინსტიტუტის მიერ.

RUSI: თემატური ანგარიში, 2023 წლის ივნისი. ISSN 2397-0286 (ელექტრონული გამოცემა).

ტექსტი ინგლისურიდან ქართულად თარგმნა ნათია ნადირაძემ, მარტი 2024.

British Embassy Tbilisi

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
რეგისტრაციის ნომერი: No. 210639

სარჩევი

სამადლობელი

წინამდებარე კვლევა განხორციელდა „დიდი ბრიტანეთი-საქართველოს კიბერთანამშრომლობის პროგრამის ფარგლებში, საქართველოში დიდი ბრიტანეთის საელჩოს მხარდაჭერითა და კონფლიქტის, სტაბილურობისა და უსაფრთხოების ფონდის ფინანსური უზრუნველყოფით. პროგრამა მიზნად ისახავს საქართველოს კიბერუსაფრთხოების ეკოსისტემის გაძლიერებას. პროგრამას საერთაშორისო და ადგილობრივი პარტნიორების კონსორციუმი ახორციელებს, რომელიც მჭიდროდ თანამშრომლობს რიგ სამთავრობო უწყებებთან საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიის განხორციელების ხელშეწყობის მიზნით შემდეგი სამი მიმართულებით:

- საქართველოს ეროვნული უსაფრთხოების საბჭოს ინფორმაციისა და კიბერუსაფრთხოების საკითხთა დეპარტამენტის მხარდაჭერა სტრატეგიის განხორციელების პროცესის კოორდინაციაში;
- ინფორმაციის მართვის ჩარჩოს შემუშავება უწყებათაშორისი კომუნიკაციის ხელშეწყობისთვის კიბერინციდენტებზე სწრაფი და ეფექტიანი რეაგირების უზრუნველსაყოფად;
- კიბერსაფრთხეების შესახებ საზოგადოებრივი ცნობიერების ამაღლება და მოქალაქეებისთვის შესაბამისი ცოდნისა და ინსტრუმენტების გადაცემა კიბერთავდასხმების ყველაზე გავრცელებული ფორმებისგან თავის დაცვის მიზნით.

სწორედ მესამე მიმართულებას უკავშირდება წინამდებარე ანგარიშის ძირითადი საკითხები: საქართველოში კიბერდანაშაულის შესახებ ინფორმირებულობა, ვიქტიმიზაცია და დანაშაულის მიმართვიანობა ტენდენციები.

ავტორები განსაკუთრებულ მადლობას უხდიან ნანა ტაბაღუას და *პოლიტიკისა და მართვის საკონსულტაციო ჯგუფის* სხვა თანამშრომლებს კვლევის პროცესში გაწეული დახმარებისთვის. განსაკუთრებით აღსანიშნავია სნეჰა დაუდას წვლილი პროექტის განხორციელებაში.

ასევე, გვსურს მადლიერებით მოვიხსენიოთ საქართველოს შინაგან საქმეთა სამინისტრო, განსაკუთრებით საინფორმაციო-ანალიტიკური დეპარტამენტის დანაშაულის ანალიზის განყოფილება, რომელმაც მოგვაწოდა 2020-2021 წლებში აღრიცხული კიბერდანაშაულის სტატისტიკა.

რეზიუმე

წინამდებარე დოკუმენტში მოცემული ინფორმაცია აყალიბებს დამოუკიდებელ მტკიცებულებათა ერთგვარ ბაზას, რომელიც საქართველოში კიბერდანაშაულისა და ონლაინ ქმედებებით გამოწვეული ზიანის გამოცდილებასა და აღქმას ეხება. განსაკუთრებული ყურადღება ეთმობა იმ ფაქტორებსა და მიზეზებს, რომლებიც განაპირობებს ამგვარი დანაშაულებისა და საფრთხეების მიმართ კონკრეტული ჯგუფების მოწყვლადობის ხარისხს. მისი მიზანია ხელი შეუწყოს მომავალში შესაბამისი პოლიტიკის განვითარებას და საზოგადოებაში კიბერდანაშაულების აღქმის შესწავლას, განსაკუთრებით კი იმ ასპექტებს, რომლებიც ინფორმირებულობას, ვიქტიმიზაციასა და მიმართვიანობის ტენდენციებს ეხება. ანალიზის საფუძველზე შეიძლება ითქვას, რომ ქართველების მოსაზრება იმასთან დაკავშირებით, თუ რა იგულისხმება კიბერდანაშაულში განსხვავდება საქართველოს სისხლის სამართლის კოდექსის განმარტებისგან. ამ დაკვირვებასა და სხვა მიგნებებზე დაყრდნობით, დოკუმენტში მოყვანილია შესაბამისი რეკომენდაციები, რომლებიც ემსახურება ცნობიერების ამაღლებას, უსაფრთხოებისა და ნდობის განმტკიცებასა და კიბერდანაშაულთან ეფექტიან ბრძოლას.

დოკუმენტში განხილული მიგნებები გამომდინარეობს თვისებრივი კვლევის შედეგად შეგროვებული მონაცემებიდან, უფრო კონკრეტულად კი, ეფუძნება ექსპერტებთან, კერძო და სამოქალაქო სექტორების წარმომადგენლებთან ჩაღრმავებული ინტერვიუების, ყველაზე დაუცველი ჯგუფების წარმომადგენლებთან ფოკუსჯგუფისა და საკონსულტაციო ვორკშოპის შედეგებს. ასევე, საქართველოს შინაგან საქმეთა სამინისტროს მიერ მოწოდებულ რაოდენობრივ მონაცემებს. აღსანიშნავია, რომ დოკუმენტში განხილული მტკიცებულებები არ არის საკმარისი იმისთვის, რომ მათ საფუძველზე შემუშავდეს კონკრეტული შესწორებების პაკეტი სისხლის სამართლის კოდექსისთვის და შესაბამისად, ეს საკითხი არ არის დოკუმენტში განხილული.

დოკუმენტში მიმოხილულია საქართველოს მოქალაქეების ონლაინ უსაფრთხოებისა და დაცულობის აღქმა და მათი ინფორმირებულობა იმასთან დაკავშირებით, თუ რას გულისხმობს კიბერსივრცეში უკანონო საქმიანობა. ირკვევა, რომ კიბერდანაშაულის ზოგადი გაგება ხშირად აერთიანებს კლასიკურ კიბერდანაშულსა და კიბერ მეთოდით ჩადენილ დანაშაულებსა და ზიანის შემცველ ინტერნეტაქტივობებს. აღსანიშნავია, რომ საზოგადოებამ უმეტესად არ იცის, კონკრეტულად რა სახის საქმიანობას განსაზღვრავს კიბერდანაშაულად საქართველოს სისხლის სამართლის კოდექსი. აქვე, ისიც უნდა ითქვას, რომ სისხლის სამართლის კოდექსის მიხედვით კიბერდანაშაულად ითვლება მხოლოდ კლასიკური კიბერდანაშაული, ანუ დანაშაული, რომელიც ჩადენილია კომპიუტერის ან სხვა მოწყობილობის საშუალებით, მისი გამოყენებით ან მის წინააღმდეგ.

კოდექსის არც ერთი მუხლი არ ეხება კიბერ მეთოდით ჩადენილ დანაშაულს ან ონლაინ ზიანს. შესაბამისად, გამომძიებლებსა და კიბერდანაშაულის მსხვერპლებს უწევთ სხვა სამართლებრივი ნორმების მოშველიება და მათი ინტერპრეტაცია, რათა დაადასტურონ, რომ დანაშაული ნამდვილად მოხდა.

კვლევის შედეგების მიხედვით შეიძლება ითქვას, რომ კიბერდანაშაულების საფრთხის შესახებ ცნობიერების დონე დაბალია და შესაბამისად, ასევე დაბალია პიროვნული რისკებისა და მათი შემცირების შესახებ ცოდნა. საქართველო არ არის ერთადერთი ქვეყანა რომელიც დგას ამგვარი პრობლემების წინაშე, თუმცა, ამ გარემოებამ არ უნდა შეაფერხოს საქართველოს მთავრობა, გამოიჩინოს მეტი ამბიციურობა მათ გადასაჭრელად.

ბოლო დროს მნიშვნელოვანი ნაბიჯები გადაიდგა საქართველოში კიბერდანაშაულის პრევენციისა და მათზე რეაგირების მიმართულებით. მათ შორის აღსანიშნავია საქართველოს სისხლის სამართლის კოდექსში შეტანილი ცვლილებები და ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველოსთვის მნიშვნელოვანი რესურსების გამოყოფა . თუმცა, ჯერ კიდევ ბევრი რამ არის გასაკეთებელი, განსაკუთრებით კი კიბერ მეთოდით ჩადენილი დანაშაულის მიმართულებით.

კვლევის შედეგები მიუთითებს, რომ მოქალაქეები ნაკლებად ენდობიან მთავრობას, როდესაც საქმე კიბერინციდენტების მიმართვიანობას ეხება. თუმცა, ამავდროულად, მთავრობა სანდო აქტორად მიიჩნევა კიბერდანაშაულთან დაკავშირებული საფრთხეებისა და კიბერჰიგიენის შესახებ ინფორმაციის გავრცელების კუთხით. საქართველოს მთავრობამ ეს აღქმები ეფექტიანად უნდა გამოიყენოს იმ ღონისძიებების შემუშავებისას, რომლებიც ზოგადი კიბერცნობიერების ამაღლებას და კიბერსაფრთხეებთან გამკლაებას ემსახურება.

კიბერდანაშაულების შესახებ ცნობიერების ამაღლების, მათგან თავის დაცვისა და შესაბამისი უწყებების მიმართ ნდობის ამაღლების მიზნით რეკომენდებულია „ერთიანი საზოგადოებრივი“ მიდგომის დანერგვა. ცნობიერების დონის ამაღლების მიზნით, საჭიროა საინფორმაციო კამპანიის ორგანიზება მთელი ქვეყნის მასშტაბით, როლის ფარგლებშიც განსაკუთრებით მოწყვლადი და მაღალი რისკის ქვეშ მყოფი ჯგუფებისთვის სპეციალური ინიციატივების განხორციელება მოხდება. მთავრობის მიმართ ნდობის განსხვავებული მაჩვენებლების გათვალისწინებითა და ფართომასშტაბიანი ეფექტის მისაღწევად, კამპანიის ფარგლებში, შესაძლებლობისამებრ, აუცილებელია სამოქალაქო საზოგადოებასთან თანამშრომლობა. მთავრობა ასევე უნდა შეეცადოს, თანხვედრაში მოიყვანოს კიბერდანაშაულის სამართლებრივი და საზოგადოებრივი განმარტება. ამ ინიციატივებთან ერთად საჭიროა იმგვარი ზომების მიღება, რომლებიც წაახალისებს მიმართვიანობას და გააძლიერებს საქართველოს კიბერუსაფრთხოების ეკოსისტემას.

შესავალი

საქართველოს კიბერუსაფრთხოების 2021-2024 წლების ეროვნული სტრატეგიის მიხედვით, კიბერდანაშაული სახელმწიფოს მიერ მართულ მტრულ კიბერშეტევებთან ერთად ყველაზე მთავარ კიბერსაფრთხეს წარმოადგენს.[1] ინტერნეტით დაფარვის არეალის გაზრდასთან ერთად, ასევე გაიზარდა კიბერდანაშაულის არეალი და გაფართოვდა კიბერ დამნაშავეების შესაძლებლობები.[2] ეს ცვლილებები აისახება კიბერდანაშაულის მსხვერპლების მიერ მიღებულ ზარალზეც, რომელიც 2020-2021 წლებში 125%-ით გაიზარდა, ანუ, 4 მილიონი ლარიდან (1.3 მილიონი ფუნტი სტერლინგი) დაახლოებით 8.9 მილიონამდე (2.9 მილიონი ფუნტი სტერლინგი). თუ გავითვალისწინებთ კიბერდანაშაულების გამოვლენისა და მათი ზეგავლენის შეფასებასთან დაკავშირებულ სიძნელეებს, რეალური მონაცემები, დიდი ალბათობით, ბევრად მაღალია.[3] გარდა ფინანსური ზარალისა, კიბერდანაშაულის მსხვერპლები განიცდიან მძიმე ემოციურ და ფსიქოლოგიურ სტრესს, ექმნებათ პრობლემები ციფრული სერვისების გამოყენებასთან დაკავშირებით და რაც ასევე მნიშვნელოვანია, ხდებიან საჯარო შერცხვენის ობიექტები.

კიბერდანაშაულებთან გამკლავების მიზნით, საქართველოს ხელისუფლებამ ახლახან დაამტკიცა საკანონმდებლო და ორგანიზაციული ცვლილებები. მათ შორისაა ცენტრალური კრიმინალური პოლიციის დეპარტამენტის მიერ კიბერდანაშაულთა მიკვლევისა და მონიტორინგის გაუმჯობესებისკენ მიმართული ღონისძიებები და 2021 წელს სისხლის სამართლის კოდექსში შესული ცვლილებები, რის შედეგადაც გაიზარდა კიბერდანაშაულის შესახებ მუხლების რაოდენობა. ამ და სხვა მცდელობების შედეგად, ოფიციალური სტატისტიკის მიხედვით, შეტყობინებული კიბერდანაშაულთა მაჩვენებელი 2020-დან 2021 წლამდე 48%-ით შემცირდა, ხოლო გახსნილ საქმეთა რიცხვი 6%-ით გაიზარდა.[4] მთავრობის მიერ გატარებულ ზომებს, სავარაუდოდ, მოჰყვა თავისი შედეგები, თუმცა, კვლევის ფარგლებში შეგროვებული მონაცემები ეჭვქვეშ აყენებს მათი პოზიტიური ზეგავლენის მასშტაბს. RUSI-სა და უსაფრთხოების კვლევების რეგიონული

1. საქართველოს მთავრობა, *საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია,* 2021, გვ.11-13
2. Sneha Dawda, Joseph Jarnecki and Natia Seskuria, 'RUSI Literature Review: Georgia's Cyber Threat and Policy Landscape', [ლიტერატურის მიმოხილვა: საქართველოს კიბერსაფრთხეები და პოლიტიკური ლანდშაფტი], RUSI and Regional Institute of Security Studies, April 2022, pp. 26–32 (დოკუმენტი არ არის საჯაროდ ხელმისაწვდომი)
3. ამ საკითხის ირგვლივ კვლევების შესახებ გაეცანით Ross Anderson et al., 'Measuring the Cost of Cybercrime' [კიბერდანაშაულების საფასურის შეფასება], in Rainer Böhme (ed.), *The Economics of Information Security and Privacy [ინფორმაციული უსაფრთხოებისა და პრივატულობის ეკონომიკა]* (Berlin: Springer Berlin Heidelberg, 2013), pp. 265–300; Ross Anderson et al., 'Measuring the Changing Cost of Cybercrime' [კიბერდანაშაულის ცვალებადი საფასურის შეფასება], 18th Workshop on the Economics of information Security, Boston, MA, June 2019.
4. საქართველოს შინაგან საქმეთა სამინისტრო, *2020-2021 წლებში აღრიცხული კიბერდანაშაულთა მიმოხილვა,* საინფორმაციო-ანალიტიკური დეპარტამენტი, 1 სექტემბერი, 2022 (ინფორმაცია არ არის საჯაროდ ხელმისაწვდომი), გვ. 3

ინსტიტუტის მიერ ჩატარებული პირველადი კვლევის მონაწილეები მიუთითებდნენ იმ მზარდ საფრთხეებზე, რომლებიც კიბერდანაშაულიდან მომდინარეობს და საუბრობდნენ იმ ფაქტორებზე, რომლებიც აფერხებს ამგვარი დანაშაულების მიმართვიანობას. ამ ფაქტორებიდან განსაკუთრებით აღინიშნა მთავრობის არასათანადო ძალისხმევა ცნობიერების ამაღლების, ნდობის განმტკიცებისა და სათემო დონეზე მუშაობის, ასევე, ადგილობრივი სამართალდამცავი სტრუქტურების მხარდაჭერის მიმართულებით. ეს დინამიკა კიდევ უფრო მკაფიოდ გამოიკვეთა წინამდებარე კვლევის სამიზნე ჯგუფებთან მუშაობისას, რომლებიც, დიდი ალბათობით, შეიძლება ჩაითვალოს კიბერდანაშაულისა და კიბერსაფრთხეების მიმართ ყველაზე მოწყვლად ჯგუფებად.[5]

წინამდებარე დოკუმენტი საქართველოში კიბერდანაშაულთან დაკავშირებულ ვითარებას სწორედ ამ მოწყვლადი ჯგუფების პერსპექტივიდან აფასებს. იმისთვის, რომ პასუხი გაეცეს მთავარ კითხვას - როგორია საქართველოში კიბერდანაშაულების გამოცდილება და რა ფაქტორები განაპირობებს მოსახლეობის დაუცველობას ამ მიმართულებით, დოკუმენტი თავდაპირველად მოკლედ მიმოიხილავს ქვეყანაში კიბერდანაშაულთან დაკავშირებულ სიტუაციას, განმარტავს ძირითად და ხშირად გამოყენებულ ტერმინებს და კვლევის მეთოდოლოგიას. პირველ თავში შეფასებულია მოსახლეობაში დაცულობის აღქმის დონე და მათი თავდაჯერებულობის ხარისხი, როდესაც საქმე კიბერდანაშაულის პრევენციას ეხება. იგივე თავი მიმოიხილავს საზოგადოების ინფორმირებულობის დონესა და ინფორმაციის გაზიარების გამოწვევებს.

მეორე თავში მკითხველი გაეცნობა კიბერდანაშაულის მხრივ არსებულ სიტუაციას და ასევე, განხილული იქნება არეები, სადაც კანონმდებლობა სათანადოდ არ ითვალისწინებს კიბერ მეთოდით ჩადენილი დანაშაულებისა და ონლაინ ზიანის საკითხებს. გარდა ამისა, მეორე თავში მოცემულია როგორც ინდივიდებზე, ასევე ორგანიზაციებზე კიბერდანაშაულთა ზეგავლენის ანალიზი. მესამე თავი აღწერს კიბერდანაშაულთა შეტყობინების სისტემას ინდივიდების, ორგანიზაციებისა და ასევე მთავრობის უწყებებში. ამავე თავში საუბარია იმაზეც, თუ როგორ აფერხებს შეტყობინებას ნდობის ნაკლებობა და სხვა ფაქტორები. დოკუმენტის დასკვნით ნაწილში მოცემულია რეკომენდაციები საქართველოს მთავრობისა და სხვა აქტორებისათვის იმ ზომებსა და ნაბიჯებთან დაკავშირებით, რომლებიც საჭიროა კიბერდანაშაულთან გამკლავებისთვის.

5. კვლევის სამიზნე ჯგუფებს წარმოადგენდა: ქალები, ეთნიკური უმცირესობები, ბავშვები, ხანდაზმულები, სოფლად მცხოვრები მოსახლეობა, ჟურნალისტები და მცირე და საშუალო საწარმოები. თითოეული ჯგუფი, როგორც აღმოჩნდა, განსაკუთრებით მოწყვლადია კიბერდანაშაულთა მიმართ.

განსაზღვრებები და ტერმინოლოგია

კიბერჰიგიენა

კიბერჰიგიენაში იგულისხმება კიბერუსაფრთხოების დაცვის საუკეთესო პრაქტიკა, ნაბიჯები და ზომები, რომლებიც ზრდის მომხმარებლის დაცულობას და მედეგობას კიბერსაფრთხეების მიმართ. კიბერჰიგიენას შეიძლება იცავდნენ როგორც ცალკეული ინდივიდები, ასევე ჯგუფები და ორგანიზაციებიც, თუმცა განსხვავდება კიბერჰიგიენის დაცვის ხარისხიც. მაგალითად, ორგანიზაციის შემთხვევაში კიბერჰიგიენის დაცვა გულისხმობს არსებული მონაცემების სარეზერვო ასლების რეგულარულ დამზადებას და შენახვას ინფორმაციის არავირტუალურ მატარებელზე. ასევე, მულტიფაქტორული იდენტიფიკაციის მეთოდების, რთული პაროლების გამოყენებასა და სისტემის რეგულარულ განახლებას.

კიბერდანაშაული და ონლაინ ზიანი

ცხრილში მოცემულია საქართველოს სისხლის სამართლის კოდექსის მე-9 თავის, 35-ე მუხლის (კიბერდანაშაული) მუხლები

ცხრილი 1: საქართველოს სისხლის სამართლის კოდექსის მუხლები, რომლებიც ეხება კიბერდანაშაულს

მუხლი	სახელწოდება
284	კომპიუტერულ სისტემაში უნებართვოდ შეღწევა
285	კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება
286	კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა
286[1]	კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით
286[2]	ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნა

წყარო: საქართველოს სისხლის სამართლის კოდექსი, დოკუმენტი 2287, 22 ივლისი 1999 (2023 წლის 9 თებერვლის რედაქცია), <https://matsne.gov.ge/ka/document/view/16426?publication=254/>, ნანახია: 18 მაისი 2023.

ყველა ზემოთ ჩამოთვლილი წარმოადგენს კლასიკურ კიბერდანაშულს, ანუ, სხვა სიტყვებით რომ ვთქვათ, დანაშაულებრივ ქმედებებს, რომლებიც ჩადენილია კომპიუტერების ან სხვა მოწყობილობების საშუალებით ან მათ წინააღმდეგ. საქართველოს სისხლის სამართლის კოდექსი არ ითვალისწინებს მუხლებს, რომლებიც შეეხება კიბერ მეთოდით ჩადენილ დანაშაულს, როცა კიბერმეთოდების გამოყენება ხდება იმ დანაშაულებრივი ქმედებების განსახორციელებლად, რომლებიც არ წარმოადგენს კლასიკურ კიბერდანაშაულს ან ონლაინ ზიანს, არამედ მოიცავს ქმედებების ფართო სპექტრს, ჩადენილს ონლაინ ან ინტერნეტის

გამოყენებით, რომლებსაც უარყოფითი გავლენა აქვთ, მაგალითად კიბერბულინგი.[6] მე-2 ცხრილში მოცემულია სისხლის სამართლის კოდექსის მუხლები, რომლებიც ყველაზე ხშირად გამოიყენება კიბერ მეთოდით ჩადენილი ან ონლაინ ზიანის შემცველ იმ საქმიანობებთან მიმართებაში, რომლებიც დანაშაულად კვალიფიცირდება.

ცხრილი 2: საქართველოს სისხლის სამართლის კოდექსის მუხლები, რომელთაც ხშირად მიემართებათ კიბერ მეთოდით ჩადენილი დანაშაული

მუხლი	სახელწოდება
151[1]	ადევნება
157	პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების ხელყოფა
157[1]	პირადი ცხოვრების საიდუმლოს ხელყოფა
158	კერძო კომუნიკაციის საიდუმლოების დარღვევა
159	პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა
189	საავტორო, მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა
210	ყალბი საკრედიტო ან საანგარიშსწორებო ბარათის დამზადება,გასაღება ან გამოყენება
255	პორნოგრაფიული ნაწარმოების ან სხვა საგნის უკანონოდ დამზადება ან გასაღება
314	ჯაშუშობა

წყარო: საქართველოს სისხლის სამართლის კოდექსი, დოკუმენტი 2287, 22 ივლისი 1999 (2023 წლის 9 თებერვლის რედაქცია)

წარმოდგენილი სია არასრულია და მხოლოდ იმ მუხლებს შეიცავს, რომლებიც ყველაზე მეტად ესადაგება კვლევის მონაწილეების მიერ აღწერილ კიბერდანაშაულის გამოცდილებას და აღქმებს. მაგალითად, თანხმობის გარეშე პირადი ინფორმაციის გაზიარება სოციალური მედიის მეშვეობით ყველაზე ახლოს 255-ე მუხლთან დგას. ეს გარემოება ასევე ცხადყოფს, რომ სისხლის სამართლის კოდექსი ითვალისწინებს იმ კიბერმეთოდით ჩადენილი დანაშაულისა და ონლაინ ზიანის მიმყენებელი ქმედებების დასჯასაც, რომლებიც მკაფიოდ უკავშირდება არსებულ მუხლებს და რომ ქართული საზოგადოების წარმოდგენით, კიბერდანაშაული შეიძლება გასცდეს ქვეყნის სისხლის სამართლის კოდექსის მე-9 თავის, 35-ე მუხლით განსაზღვრულ ქმედებებს.

მონაცემთა შეგროვების ეტაპზე, მკვლევრებს რესპონდენტებისთვის არ გაუზიარებიათ კიბერდანაშაულის კონკრეტული დეფინიცია, რათა უკეთ გაეგოთ კიბერდანაშაულის მიმართ მათი ინტუიციური ცოდნის ხარისხი. ამრიგად, მკვლევრებმა უარი თქვეს მონაწილეებისთვის კიბერდანაშაულის მზა განმარტების

6. ვირტუალურ ზიანთან დაკავშირებით იხილეთ: Ioannis Agrafiotis et al., 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate' [ვირტუალური ზიანის ტაქსონომია: კიბერთავდასხმების ზეგავლენა და მათი გავრცელება], *Journal of Cybersecurity* (ტომი. 4, No. 1, 2018), გვ. 1–15.

მიწოდებაზე და ამის ნაცვლად, საშუალება მისცეს რესპონდენტებს, გამოეთქვათ საკუთარი მოსაზრება კიბერდანაშაულის განმარტებასთან დაკავშირებით. შესაბამისად, ანგარიში კიბერდანაშაულის იმ განმარტებას ითვალისწინებს, რომლებიც საზოგადოების აღქმას შეესაბამება და რომელიც აერთიანებს როგორც კლასიკურ, ისე კიბერ მეთოდით ჩადენილ დანაშაულსა და ონლაინ ზიანს. ეს მიდგომა, თავის მხრივ ნიშნავს იმას, რომ წინამდებარე ანგარიშის წაკითხვისთვის, მნიშვნელოვანია შემდეგი მიგნებების გათვალისწინება:

1. საზოგადოებაში არსებული ვირტუალური დაუცველობის შეგრძნების გამომწვევი მიზეზები ყოველთვის არ არის გათვალისწინებული სისხლის სამართლის კოდექსის იმ მუხლებში, რომლებიც კიბერდანაშაულს ეხება;
2. მოქალაქეებმა მეტწილად არ იციან, თუ რას წარმოადგენს ვირტუალურ სივრცეში უკანონო აქტივობები და არ აქვთ ინფორმაცია, თუ რა ინსტრუმენტებია მათთვის ხელმისაწვდომი ან რა პროცედურები უნდა გაიარონ, დახმარების მისაღებად;
3. მოქალაქეები ძნელად ასხვავებენ კლასიკურ კიბერდანაშაულსა და კიბერ მეთოდით ჩადენილ დანაშაულსა და ონლაინ ზიანის შემცველ ქმედებებს.

ქვემოთ მოცემულ ცხრილში ნაჩვენებია განსხვავებები კიბერდანაშაულის მიმართ მოქალაქეთა აღქმებსა და სისხლის სამართლის კოდექსის ფორმულირებას შორის:

ცხრილი 3: კიბერდანაშაულის აღქმები და არსებული ნორმები

ქმედება	საზოგადოება აღიქვამს კიბერდანაშაულად	მიჩნეულია კიბერდანაშაულად სსკ-ს მიხედვით
კიბერბულინგი	X	
კიბერადევნება	X	
პირადი სურათების გაზიარება თანხმობის გარეშე	X	
კიბერთავდასხმა გამოსასყიდის გამოძალვის მიზნით (ე.წ. ransomware attacks)	X	X
კიბერთავდასხმა ციფრული სერვისების პარალიზების მიზნით (DDoS)	X	X
კიბერთავდასხმები კრიტიკული ინფრასტრუქტურის განადგურებისა და ქაოსის გამოწვევის მიზნით (ე.წ. wiperware attacks)	X	X
იდენტობის ქურდობა და გამოძალვა	X	

წყარო: ცხრილი შედგენილია ანგარიშის ავტორების მიერ

მეთოდოლოგია

კვლევა, რომლის შედეგებიც წინამდებარე დოკუმენტშია წარმოდგენილი 2022 წლის ივნისიდან 2023 წლის იანვრამდე პერიოდში ჩატარდა „გაერთიანებული სამეფო - საქართველოს კიბერთანამშრომლობის პროგრამის“ ფარგლებში, რომელიც, თავის მხრივ, - დიდი ბრიტანეთის საგარეო საქმეთა, თანამეგობრობისა და განვითარების სამინისტროს ფინანსური ხელშეწყობით ხორციელდება. კვლევის ფარგლებში გამოყენებულ იქნა პირველადი და მეორეული თვისებრივი მეთოდების კომბინაცია, რომელთა შესახებაც დეტალური ინფორმაცია ქვემოთ არის მოცემული.

ნახევრადსტრუქტურირებული ინტერვიუები

კვლევის ფარგლებში მკვლევრებმა ჩაატარეს 11 ნახევრადსტრუქტურირებული ინტერვიუ საქართველოს მთავრობის ყოფილ და მოქმედ წევრებთან, კიბერუსაფრთხოებისა და კიბერდანაშაულის ექსპერტებთან, სამოქალაქო საზოგადოების წარმომადგენლებთან, ჟურნალისტებსა და კერძო სექტორის ორგანიზაციების მმართველი წრეების წარმომადგნლებთან. მონაწილეები შეირჩნენ მიზნობრივი შერჩევის სტრატეგიის საფუძველზე შესაბამისი პროფესიული ჯგუფებიდან და კიბერდანაშაულთან დაკავშირებული პირადი გამოცდილების მიხედვით. შერჩევის აღნიშნული მეთოდი შეეხო როგორ სამთავრობო სტრუქტურების, ისე სამოქალაქო საზოგადოების წარმომადგენლებს. რესპონდენტთა უმეტესობა მანამდე არსებული ინსტიტუციური ურთიერთობების საფუძველზე შეირჩა, ხოლო ნაწილი - ლიტერატურის მიმოხილვაზე მუშაობის დროს. ასევე გამოყენებული იქნა ე.წ. „თოვლის გუნდას“ (snowballing) შერჩევის სტრატეგია. ინტერვიუები, ძირითადად, თბილისში, რესპონდენტებთან პირისპირ ჩატარდა ინგლისურ ენაზე (ერთი შემთხვევის გარდა, როდესაც ინტერვიუს დროს ქართული ენა იქნა გამოყენებული). სადაც პირისპირ შეხვედრა ვერ მოხერხდა, მკვლევრები სხვადასხვა ციფრულ პლატფორმას იყენებდნენ. ნახევრადსტრუქტურირებული ინტერვიუს ფორმატმა საშუალება მისცა მკვლევრებს შეენარჩუნებინათ გამოკითხვის თანმიმდევრული ხაზი და ამავე დროს, დაეტოვებინათ საკმარისი სივრცე რესპონდენტთან სპონტანური, მაგრამ სიღრმისეული მსჯელობისთვის. ინტერვიუები 2022 წლის სექტემბრიდან 2023 წლის იანვრამდე მიმდინარეობდა.

ფოკუსჯგუფები

კვლევის ფარგლებში ორგანიზებულ ოთხ ფოკუსჯგუფში სულ 41-მა პირმა მიიღო მონაწილეობა, რომლებიც წინასწარ განსაზღვრული მახასიათებლებით შეირჩნენ. მახასიათებლების განსაზღვრისას, თავის მხრივ, მკვლევრებმა გაითვალისწინეს,

თუ რამდენად უწყობდა ხელს კონკრეტული მახასიათებელი სამიზნე ჯგუფების კიბერდანაშაულისადმი მოწყვლადობას. შესაბამისად, გამოიყო შემდეგი ოთხი მოწყვლადი ჯგუფი (თითოეულს ცალკე ფოკუსჯგუფი დაეთმო): ჟურნალისტები, მშობლები/ მეურვეები[7] და მასწავლებლები, ეთნიკური უმცირესობები და ქალები. სხვა ჯგუფები, როგორიცაა ბავშვები, ასევე განიხილებოდნენ რესპონდენტებად, მაგრამ პრაქტიკული მოსაზრებების გამო, გადაწყდა, რომ ფოკუსჯგუფების რაოდენობა შეზღუდულიყო. ფოკუსჯგუფების მსვლელობა ჩაიწერა აუდიო ფორმატში, ხოლო ჩანაწერების საფუძველზე მომზადდა ტრანსკრიპტი. მონაწილეების პასუხების დასაფიქსირებლად მკვლევრებმა გამოიყენეს სპეციალური ფორმები. მონაწილეების შერჩევისას განსაკუთრებული ყურადღება მიექცა ქალების აქტიური მონაწილეობის პრინციპებსა და გეოგრაფიულ წარმომადგენლობას. შესაბამისად, 41 მონაწილედან 28 ქალი იყო, ხოლო 21 - არ ცხოვრობდა ურბანული ტიპის დასახლებაში. ფოკუსჯგუფები თბილისში გაიმართა ქართულ ენაზე, 3-დან 7 ოქტომბრამდე.

საკონსულტაციო/მონაცემების ვალიდაციის სამუშაო შეხვედრა

ინტერვიუებისა და ფოკუსჯგუფებში განხილვების შედეგების შესამოწმებლად, მკვლევართა ჯგუფმა ორგანიზება გაუწია კიბერუსაფრთხოების საკითხებში სამოქალაქო ჩართულობის ღონისძიებას, რომელიც 2022 წლის 22 დეკემბერს თბილისში გაიმართა ქართულ ენაზე და რომელშიც 49 პირი მონაწილეობდა, მათ შორის ჟურნალისტები, სამოქალაქო ორგანიზაციების წარმომადგენლები, მშობლები და ასევე მცირე და საშუალო ბიზნესის მფლობელები და წარმომადგენლები. შეხვედრის განმავლობაში მონაწილეები მცირე ჯგუფებად დაიყვნენ ზემოთ ჩამოთვლილი კატეგორიების მიხედვით. შედეგების ანალიზის მიზნით, ორგანიზატორებმა ჩაიწერეს სამუშაო შეხვედრა, ხოლო ჩანაწერის საფუძველზე მოამზადეს ტრანსკრიპტი.

ლიტერატურის მიმოხილვა

მკვლევრების ჯგუფი ასევე გაეცნო არსებულ ლიტერატურას, რომელიც მოპოვებულ იქნა ღია წყაროებიდან, ასევე, საქართველოში კიბერდანაშაულის შესახებ ჩატარებული კვლევების ანგარიშებს. ამ პროცესში მნიშვნელოვანი როლი შეასრულა პროექტში ჩართული მკვლევრების მიერ ლიტერატურის წინარე

7. პროექტის განხორციელების პროცესში კანონიერ წარმომადგენლებსა და მზრუნველებში იგულისხმებიან უფროსი ასაკის პირები, რომლებიც არ არიან ბავშვის მშობლები, მაგრამ აკისრიათ ბავშვზე რეგულარული ზრუნვის პასუხისმგებლობა. კანონიერი წარმომადგენელი შეიძლება იყოს მშვილებელი, მინდობით აღმზრდელი, ბებია და პაპა, ან სხვა ნათესავი ან სხვა პირი, რომელსაც ამგვარი პასუხისმგებლობა აკისრია.

მოკვლევამ საქართველოს კიბერუსაფრთხოების ეკოსისტემის შესახებ კვლევისას. გარდა ამისა, მკვლევრების ჯგუფმა გამოიყენა საქართველოს შინაგან საქმეთა სამინისტროს საინფორმაციო-ანალიტიკური დეპარტამენტის მიერ მიწოდებული დეტალური და სეგრეგირებული სტატისტიკური მონაცემები 2020-2021 წლებში აღრიცხული კიბერდანაშაულების შესახებ.

პირველადი მონაცემების შეგროვების პროცესში დაცული იყო მონაწილე პირთა ანონიმურობა.

შეზღუდვები

კვლევასთან დაკავშირებული ერთ-ერთი შეზღუდვა ისაა, რომ შეგროვებული მონაცემები ასრულებს გარკვეული ინდიკატორების როლს, თუმცა არ არის სრულად წარმომადგენლობითი. მიუხედავად იმისა, რომ მონაწილეთა რაოდენობა სრულიად საკმარისია იდეების ვალიდაციისა და მიგნებების ფორმულირებისთვის, ის არ იძლევა საქართველოს მთელს მოსახლეობაზე განზოგადების საშუალებას. ამ შეზღუდვის საპირწონედ, მკვლევრებმა უზრუნველყვეს რომ, ფოკუსჯგუფებში მონაწილეობა მიეღოთ რაც შეიძლება მრავალფეროვანი გამოცდილების მქონე მონაწილეებს, ხოლო რესპონდენტებად შეარჩიეს მაღალი კვალიფიკაციის მქონე ექსპერტები. კიდევ ერთი შეზღუდვა ის არის, რომ კვლევის ვიწრო ფოკუსიდან გამომდინარე, მთავარი ყურადღება დაეთმო კიბერდანაშაულთან დაკავშირებულ აღქმებსა და გამოცდილებას, ხოლო კვლევის მიღმა დარჩა ის კონკრეტული საკანონმდებლო და მარეგულირებელი ცვლილებები, რომლებიც მიზნად ისახავს არსებული აღქმების შეცვლას. ამის მიუხედავად, ხსენებული ცვლილებები უმნიშვნელოვანესია საქართველოში კიბერუსაფრთხოების გაუმჯობესებისთვის და შესაბამისად, ამ საკითხებს ცალკე კვლევა უნდა დაეთმოს.

I. დაცულობა და ნდობა

კიბერდანაშაული შედარებით ახალი საფრთხეა, რომელიც, ძალიან დინამიურად ვითარდება. იგი ხშირად ხდება შფოთვისა და წუხილის საგანი. როგორც ფოკუსჯგუფის მონაწილეებმა განაცხადეს, ისინი შიშობენ, რომ „შეიძლება კიბერდანაშაულის მსხვერპლები გახდნენ“. თუმცა, კიბერდანაშაულის მასშტაბის, ზეგავლენისა და მასთან გამკლავების შესახებ ცნობიერება საკმაოდ დაბალია. ეს გლობალური პრობლემაა, თუმცა იგი განსაკუთრებით მწვავედ იგრძნობა ისეთ ქვეყნებში, რომლებშიც სწრაფი ტემპებით მიმდინარეობს გაციფრულების პროცესი შესაბამისი ფართომასშტაბიანი საინფორმაციო კამპანიის გარეშე. საქართველოც სწორედ ამგვარ ქვეყნებს შორისაა.[8] ამ თავში შეფასებულია საქართველოში კიბერდანაშაულის შესახებ ცნობიერების და ინფორმირებულობის ხარისხი და შემუშავებულია რეკომენდაციები ამ მიმართულებით არსებული ხარვეზების აღმოფხვრასთან დაკავშირებით. რადგანაც ამ ნაწილში აქცენტი კეთდება, ძირითადად, მონაწილეების იმ გამოცდილებაზე, რომელიც დაცულობასა და ნდობას უკავშირდება, კიბერდანაშაული გამოიყენება მისი ფართო გაგებით, ანუ ტერმინში იგულისხმება როგორც კლასიკური კიბერდანაშაული, ისე კიბერმეთოდით ჩადენილი დანაშაული და ონლაინ ზიანი.

ინფორმირებულობა კიბერდანაშაულის შესახებ

პრიორიტეტული სფეროები

ცნობიერება კიბერდანაშაულის შესახებ განისაზღვრება იმით, თუ რამდენად ერკვევა საზოგადოება კიბერსაშუალებებიდან მომდინარე ან მათთან დაკავშირებულ დანაშაულებრივ საფრთხეებში. იგი გავლენას ახდენს დაცულობის შეგრძნებაზე და განაპირობებს აქტორების მოტივაციას, გაანეიტრალონ კიბერუსაფრთხებასთან დაკავშირებული რისკები. ცნობიერება და მისი ამაღლების ზომები საქართველოს ეროვნული კიბერუსაფრთხოების სტრატეგიის ერთ-ერთი პრიორიტეტული მიმართულებაა.[9] ყველა დაინტერესებულ მხარეს, მათ შორის კერძო კომპანიებს, ინდივიდებს, სამოქალაქო საზოგადოების ორგანიზაციებს, ცნობიერების გარკვეული დონე აქვთ.

8. არსებობს ინფორმაცია, რომ საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის ფარგლებში ჩატარდა „ცნობიერების ამაღლების ფართომასშტაბიანი კამპანია“, თუმცა, მთავრობის ერთი წარმომადგენლის გარდა, კვლევის ვერც ერთმა მონაწილემ ვერ გაიხსენა მსგავსის შესახებ.
9. საქართველოს მთავრობა, ‘საქართველოს ეროვნული კიბერუსაფრთხოების სტრატეგია’, გვ. 8–9.

კვლევის შედეგები მიუთითებს, რომ საქართველოში კიბერდანაშაულებისა და კიბერუსაფრთხოების შესახებ ცნობიერების დონე დაბალია, თუმცა, გასული წლების განმავლობაში სისხლის სამართლის კოდექსში შეტანილი ცვლილებებისა და ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველოს მანდატის გაფართოების შედეგად გაუმჯობესებაც შეინიშნება.[10] უფრო მეტიც, კიბერდანაშაულებსა და საფრთხეებს განსაკუთრებული აქტუალობა შესძინა ინტერნეტკავშირგაბმულობის გაუმჯობესებამ და საჯარო სერვისებისა და ინდივიდების პირადი მონაცემების წინააღმდეგ განხორციელებული თავდასხმების გახმაურებულმა ფაქტებმა.[11]

თუმცა, ცნობიერების საერთო დონე კვლავ გამოწვევად რჩება. კვლევის მიზნებისთვის პირველადი მონაცემების შეგროვების პროცესში გამოიკვეთა, რომ ცნობიერების განსაკუთრებით დაბალი დონე შეინიშნება სოფლად მცხოვრებ მოსახლეობაში, ბავშვებში, ხანდაზმულ მოქალაქეებსა და ეთნიკურ უმცირესობებში, რომლებიც სათანადოდ ვერ ფლობენ ქართულს.[12]

- **სოფლად მცხოვრები მოსახლეობა**. ცნობიერების დაბალი დონე, განსაკუთრებით სოფლად და რთული რელიეფის მქონე ადგილებში, გამოწვეულია ინტერნეტკავშირის შედარებით ცუდი ხარისხით, სახელმწიფო სერვისებზე შეზღუდული ხელმისაწვდომობით და სიღარიბის საშუალოზე მაღალი დონით.[13] ფოკუსჯგუფის ერთ-ერთმა მონაწილემ, რომელიც ერთ-ერთი სოფლის სკოლაში IT ადმინისტრატორია, განაცხადა, რომ სოფლის მცხოვრებლების უმეტესობა დასახმარებლად მიმართავს ხოლმე ისეთ ინტერნეტაქტივოვებთან დაკავშირებით, როგორიცაა, მაგალითად, პაროლის შეყვანა ან გამოცვლა და ასევე, ინტერნეტბანკთან დაკავშირებითაც. მიუხედავად იმისა, რომ ის ცდილობს ასწავლოს, „მათ არ სურთ განავითარონ ეს უნარები, რადგან ვერ ხვდებიან, თუ რაოდენ სარისკოა პირადი ინფორმაციის სხვისთვის გადაცემა“.
- **ბავშვები**. მშობლების, მასწავლებლების, მეურვეებისა და ექსპერტების მიერ მოწოდებული ინფორმაციის მიხედვით, ბავშვებს არ აქვთ კიბერდანაშაულის

10. საქართველოს მთავრობა, საქართველოს სისხლის სამართლის კოდექსი, დოკუმენტი 2287, 22 ივლისი 1999 (2023 წლის 9 თებერვლის რედაქცია), თავი 9, მუხლი 35, „კიბერდანაშაული“
11. საქართველოს მთავრობა, საქართველოს სისხლის სამართლის კოდექსი, დოკუმენტი 2287, 22 ივლისი 1999 (2023 წლის 9 თებერვლის რედაქცია), თავი 9, მუხლი 35, „კიბერდანაშაული“ საქართველოს მთავრობა, „საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია“, გვ. 12–13; ირაკლი ჯღარკავა, „საქართველოს კიბერუსაფრთხოების პოლიტიკა, გამოწვევები და შესაძლებლობები“, საქართველოს სტრატეგიისა და განვითარების ცენტრი, 2021.
12. ინტერვიუები მთავრობის ყოფილ მაღალჩინოსან მოხელესა და სსო-ს ხელმძღვანელთან. პირველი ინტერვიუ ჩაწერილია თბილისში, ხოლო მეორე - ციფრული პლატფორმის მეშვეობით, 3-18 ოქტომბერი 2023.
13. საქართველოს სტატისტიკის ეროვნული სამსახური, „საინფორმაციო და საკომუნიკაციო ტექნოლოგიების გამოყენება შინამეურნეობებში“, <https://www.geostat.ge/ka/modules/categories/106/sainformatsio-da-sakomunikatsio-teknologiebis-gamoqeneba-shinameurneobebshi>, ბოლოს ნანახია 2022 წლის 20 აპრილს; ინტერვიუ ცენტრალური მთავრობის მოქმედ საჯარო მოხელესთან, თბილისი, 4 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან მოხელესთან ციფრული პლატფორმის გამოყენებით, 18 ოქტომბერი 2022.

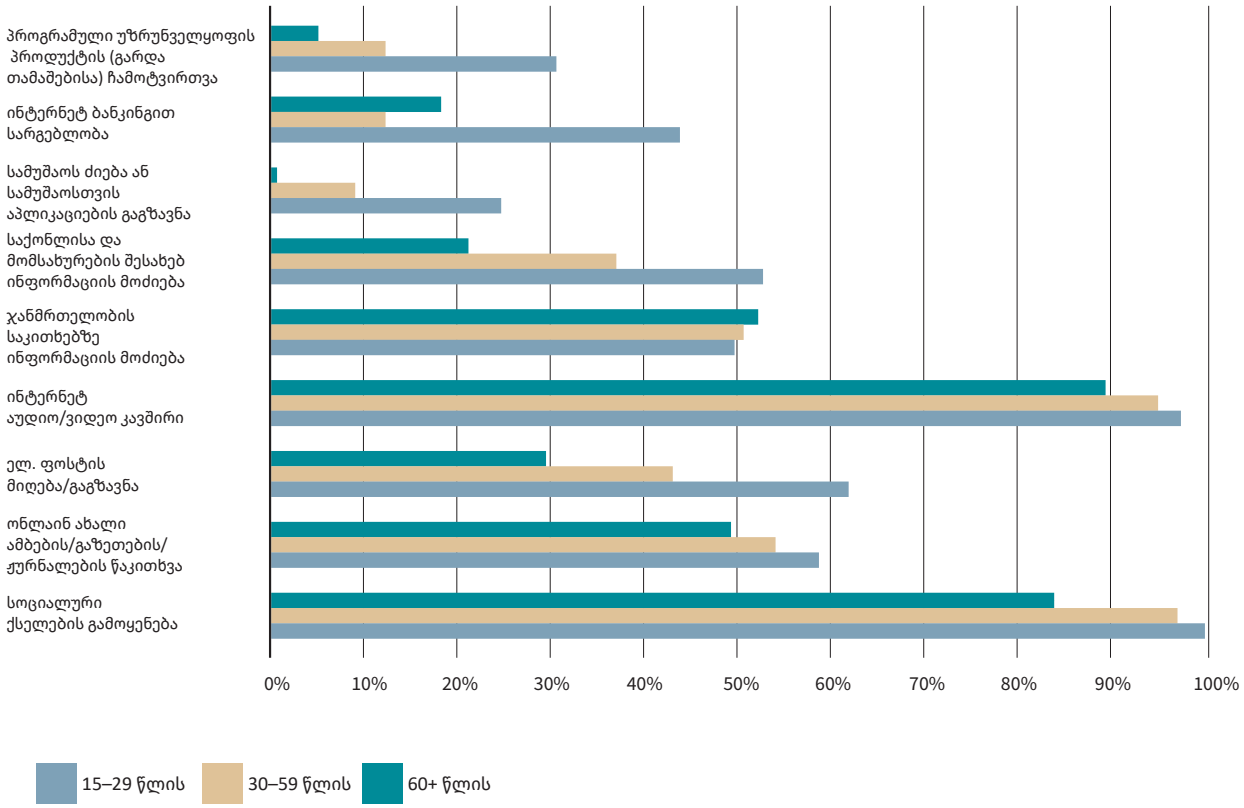
შესახებ ცნობიერების საბაზისო დონეც კი. თუმცა, ბავშვები ინტერესს იჩენენ და გარკვეული ცოდნაც აქვთ ისეთი „საინტერესო და სახალისო“ საკითხის შესახებ, როგორიცაა, მაგალითად, „ჰაკერობა“.[14] ბავშვებში ცნობიერების დაბალი დონე, ძირითადად, გამოწვეულია რისკების გაუცნობიერებლობით: ისინი ფიქრობენ, რომ ყველაფრის ნდობა შეიძლება, როცა საქმე ინტერნეტს ეხება და პირადი მონაცემების დაცვის მნიშვნელობის შესახებ ბევრი არაფერი იციან. გარდა ამისა, ბავშვები არ იღებენ შესაბამის დახმარებას სკოლებისა და მშობლებისგან.[15]

- **ხანდაზმულები**. საქართველოს სტატისტიკის ეროვნული სამსახურის მონაცემების მიხედვით, ხანდაზმული მოსახლეობა (60 წელი და ზევით), საშუალოზე დაბალი სიხშირით იყენებს ინტერნეტს და ძირითადად ერთგვაროვანი მიზნებისთვის (იხ. სურათი 1). ამ მოსაზრებას ამყარებს ფოკუსჯგუფებში განხილვებისა და ინტერვიუების შედეგად შეგროვებული მონაცემებიც. ამ მონაცემებზე დაყრდნობით, შეიძლება ითქვას, რომ ხანდაზმულებთან დაკავშირებული დინამიკა განპირობებულია ტექნოლოგიების შეზღუდული გამოყენებით, ინტერნეტში განთავსებული ინფორმაციისადმი ნდობის მაღალი ხარისხით, ციფრულის წიგნიერების დეფიციტითა და მთავრობის, ასევე სამოქალაქო სექტორის მხრიდან დაბალი მხარდაჭერით.[16] ერთ-ერთმა რესპონდენტმა - ყოფილმა საჯარო მოხელემ, განაცხადა, რომ ხანდაზმულები არ იყენებენ ინტერნეტს (ან იყენებენ, მაგრამ არა სტატისტიკურად მნიშვნელოვანი სიხშირით) და შესაბამისად, დაცულნი არიან კიბერდანაშაულისგან.[17] ეს სახიფათო და მცდარი დაშვებაა, რომლის მიხედვითაც ინტერნეტის ხშირი მოხმარება ზრდის მომხმარებლის ვიქტიმიზაციის ალბათობას. სწორედ ამ მცდარი დაშვების გამო, ხანდაზმულებზე ნაკლებად ვრცელდება ციფრული სერვისები და მხარდაჭერა, რომელიც შეამცირებდა კიბერდანაშაულის რისკებს ამ ასაკობრივი ჯგუფის წინააღმდეგ.
- **ეთნიკური უმცირესობები, რომლებიც სათანადოდ ვერ ფლობენ ქართულ ენას.** ამ ჯგუფში კიბერდანაშაულის შესახებ ცნობიერების დაბალი დონე გამოწვეულია იმ რესურსებზე და ინფორმაციაზე შეზღუდული ხელმისაწვდომობით, რომლებიც ქართულ ენაზე მოიპოვება.[18] შესაბამისად, ამ ჯგუფს უწევს მათ მშობლიურ ენაზე არსებულ წყაროებზე დაყრდნობა ან, რაც უფრო ხშირად ხდება, რუსულენოვანი წყაროების გამოყენება. საქართველოში მცხოვრები სხვადასხვა ეთნიკური ჯგუფისთვის რუსული

14. ინტერვიუ სსო-ს მაღალი რანგის წარმომადგენელთან, თბილისი, 6 ოქტომბერი 2022.
15. ფოკუსჯგუფში განხილვები, თბილისი, 3-7 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან მოხელესთან ციფრული პლატფორმის გამოყენებით, 7 ოქტომბერი 2022.
16. ფოკუსჯგუფში განხილვები, თბილისი, 3-7 ოქტომბერი 2022; ინტერვიუები სსო-სა და პროფესიული ასოციაციების მაღალი რანგის წარმომადგენლებთან, თბილისი, 3–6 ოქტომბერი 2022.
17. ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან მოხელესთან, თბილისი, 5 ოქტომბერი 2022.
18. ფოკუსჯგუფებში განხილვები, თბილისი, 3-7 ოქტომბერი 2022; ინტერვიუები ჟურნალისტებთან, თბილისი, 3 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან მოხელესთან ციფრული პლატფორმის გამოყენებით, 7 ოქტომბერი 2022.

საერთო მეორე ენის ფუნქციას ინარჩუნებს.[19] ერთ-ერთმა ყოფილმა საჯარო მოხელემ ხაზი გაუსვა, რომ რუსულ ენაზე ხელმისაწვდომი წყაროები, დიდი ალბათობით, ხშირად გამოიყენება დეზინფორმაციის ინსტრუმენტად და შესაბამისად, ამ რესურსების ხშირად გამოყენებამ შესაძლოა, გაზარდოს ეროვნული უსაფრთხოების რისკები.[20] მტკიცებულებების ნაკლებობის გამო, მნიშვნელოვანია, რომ ეს საკითხი სიღრმისეულად იქნეს შესწავლილი.

სურათი 1: ინტერნეტის გამოყენების მიზნობრიობა ასაკობრივ ჭრილში, ივლისი 2021



წყარო: საქართველოს სტატისტიკის ეროვნული სამსახური, „საინფორმაციო და საკომუნიკაციო ტექნოლოგიების გამოყენება შინამეურნეობებში“, < https://www.geostat.ge/ka/modules/categories/106/sainformatsio-da-sakomunikatsio-teknologiebis-gamoqeneba-shinameurneobebshi >, ბოლოს ნანახია: 20 აპრილი 2022.

ადამიანები მოწყვლად ჯგუფებში არ ფლობენ მხოლოდ ერთ მაიდენტიფიცირებელ ნიშანს. არამედ, შესაძლოა მათ მოწყვლადობის რამდენიმე მახასიათებელი

19. Rusudan Amirejibi and Kakha Gabunia, ‘Georgia’s Minorities: Breaking Down Barriers to Integration’ [საქართველოს უმცირესობები: ინტეგრაციის ბარიერების გადალახვა], Carnegie Europe, 9 June 2021; Tamar Maisuradze, ‘Russian Language in Georgia: Not Number One’ [რუსული ენა საქართველოში უკვე აღარ არის პირველი ენა], *JAM News*, 21 December 2016, <https://jam-news.net/russian-language-in-georgia-not-number-one/>, ბოლოს ნანახია: 7 თებერვალი 2023.
20. ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან მოხელესთან ციფრული პლატფორმის გამოყენებით, 7 ოქტომბერი 2022.

ერთად ჰქონდეთ გამოკვეთილი. პირველადი მონაცემების შეგროვების პროცესმა დაადასტურა, რომ მოწყვლადობის რამდენიმე მახასიათებლის ერთდროული არსებობა ზრდის არასათანადო კიბერცნობიერების ალბათობას. ამგვარად, ხანშიშესულ პირს, რომელიც ამავე დროს სოფლად ცხოვრობს და ქართული კარგად არ იცის, დიდი ალბათობით, კიბერცნობიერების დაბალი დონე აქვს.

პირველადი მონაცემების ანალიზმა ასევე გამოავლინა, რომ, მართალია, დაბალი კიბერცნობიერება იშვიათად გხვდება საჯარო მოხელეებში, ჟურნალისტებში, პოლიციის თანამშრომლებსა და მცირე და საშუალო ბიზნესის მფლობელებსა და მენეჯერებში, ამგვარ შემთხვევებს, არსებობის შემთხვევაში, მაღალი საზოგადოებრივი ზეგავლენა აქვთ.

- **მაღალი რანგის საჯარო მოხელეები**. მიუხედავად იმისა, რომ კვლევის მონაწილეებს მკვეთრად კრიტიკული დამოკიდებულება არ გამოუხატავთ მთავრობის წევრებისა და მაღალი რანგის მოხელეების დაბალი კიბერცნობიერების გამო, ისინი მაინც ფიქრობენ, რომ მთავრობის მიერ მიღებულ გადაწყვეტილებში მაღალი პრიორიტეტი არ მიენიჭა კიბერდანაშაულს.[21] ერთ-ერთი მონაწილე, რომელსაც ქონდა მაღალჩინოსნებთან ურთიერთობის გამოცდილება, ამტკიცებდა, რომ ეს განაპირობა ცნობიერების დაბალმა დონემ იმ კიბერდანაშაულებთან დაკავშირებით, რომელიც საფრთხეს უქადის სამთავრობო უწყებებს. ამავე რესპონდენტის აზრით, საჭიროა სამინისტროების დონეზე კიბერსავარჯიშოს ჩატარება ამ საკითხების ირგვლივ ცნობიერებისა და ცოდნის გაუმჯობესების მიზნით.[22]
- **ჟურნალისტები.** კვლევაში მონაწილე ჟურნალისტების აზრით, მათი კიბერცნობიერების დონე სასურველზე დაბალია, ხოლო მედია არასათანადოდ აშუქებს კიბერდანაშაულს. [23] ფოკუსჯგუფებში განხილვის მონაწილე ერთ-ერთმა ჟურნალისტმა ხაზი გაუსვა იმ ფაქტს, რომ მედია ორგანიზაციები არ უზრუნველყოფენ ტრენინგებს კიბერჰიგიენისა და კიბერსაფრთხეების საკითხების ირგვლივ, რაც, მისი მტკიცებით, შედეგად იწვევს კიბერდანაშაულის ანალიზისა და ამ საკითხებისადმი ყურადღების ნაკლებობას. როგორც ექსპერტი, ასევე არაექსპერტი რესპონდენტები (ფოკუსჯგუფის და ინტერვიუების) და ვალიდაციის სამუშაო შეხვედრის მონაწილეები იზიარებდნენ მოსაზრებას იმის თაობაზე, რომ მედიის მიერ კიბერდანაშაულის შემთხვევების გაშუქებას აკლია სიღრმე და დეტალები.[24]

21. ფოკუსჯგუფში განხილვები, თბილისი, 3-7 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან მოხელესთან ციფრული პლატფორმის გამოყენებით. 7 ოქტომბერი 2022.
22. ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან მოხელესთან ციფრული პლატფორმის გამოყენებით. 7 ოქტომბერი 2022.
23. ფოკუსჯგუფში განხილვები, თბილისი, 3-she media7 ოქტომბერი 2022; ინტერვიუ ჟურნალისტთან, თბილისი, 3 ოქტომბერი 2022.
24. იქვე.; ინტერვიუები სსო-ების წარმომადგენელთან ციფრული პლატფორმის გამოყენებით, 20 ოქტომბერი 2022.

- **პოლიცია.** კიბერდანაშაულის შეტყობინებისთვის ადამიანები პირდაპირ პოლიციას მიმართავენ. რესპონდენტმა, რომელიც ერთ-ერთ სამთავრობო უწყებაში მუშაობს, ხაზი გაუსვა იმ ფაქტს, რომ პოლიციის თანამშრომლებს ჩაუტარდათ ინტენსიური ტრენინგები ცნობიერების ამაღლებისა და დაზარალებულებისთვის მიმართვიანობის შემდეგ ეფექტიანი მხარდაჭერის უზრუნველყოფის მიზნით.[25] თუმცა, არც ყოფილ სამთავრობო მოხელეებს და არც ფოკუსჯგუფების მონაწილეებს არ აღუნიშნავთ, რომ პოლიციას ახლა აქვს იმის შესაძლებლობა, რომ ხელი შეუწყოს მიმართვიანობის მაჩვენებლის ზრდას, რაც, სამოქალაქო სექტორის წარმომადგენლების აზრით ერთ-ერთი ის საკითხია, რომელიც განსაკუთრებულ ყურადღებას საჭიროებს.[26] ცხადია, მრავალმა რესპონდენტმა ისაუბრა იმ გამოწვევებისა და წუხილების შესახებ, რომელიც პოლიციისთვის მიმართვიანობის საკითხს უკავშირდება (იხ. „მიმართვიანობის პროცედურები“).
- **მცირე და საშუალო ბიზნესის მფლობელები და მენეჯერები**. გლობალურად, კლასიკურ კიბერ დანაშაულებრივ ქმედებას, როგორც წესი, ფინანსური მოტივი უდევს საფუძვლად. მიუხედავად იმისა, რომ არსებული მონაცემების სიმწირე არ იძლევა საქართველოში ამ სურათის დადასტურების საშუალებას, შეტყობინებული კიბერდანაშაულების სტატისტიკა, ნამდვილად ადასტურებს ამ ტენდენციის არსებობას (იხ. თავი II). კიბერდანაშაულის ძირითადი სამიზნე ბიზნეს სექტორია. რისკი განსაკუთრებით იზრდება იმ მცირე და საშუალო ბიზნესებისთვის, რომელთა მფლობელები და მენეჯერებიც კიბერცნობიერების მაღალი დონით არ გამოირჩევიან.[27] ეს გარემოება საფრთხეს უქმნის არა მხოლოდ მათ შემოსავალს, არამედ, თუ თავდასხმებმა სისტემატური ხასიათი მიიღო, ეროვნულ ეკონომიკურ უსაფრთხოებასაც.

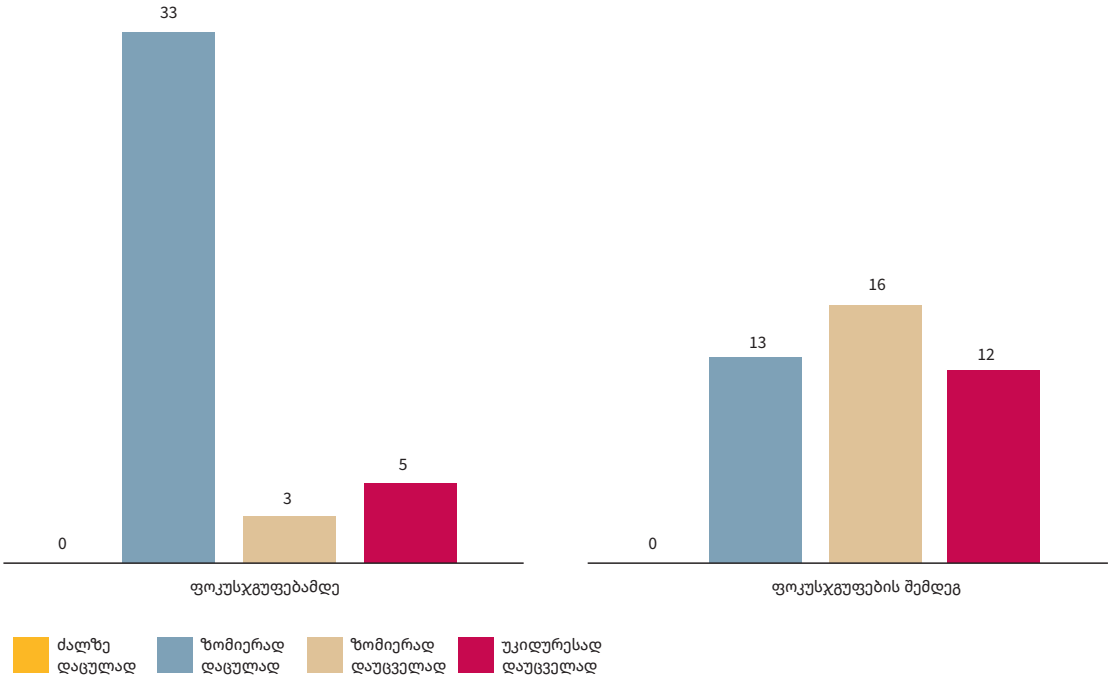
ზემოხსენებულ ჯგუფებში ცნობიერების ნაკლებობა უარყოფით გავლენას ახდენს იმაზე, თუ რამდენად კარგად ესმის საზოგადოებას კიბერდანაშაულის რისკები. გარდა ამისა, დაბალი კიბერცნობიერება აქვეითებს საფრთხეებთან გამკლავების მზადყოფნის უნარს ეროვნულ დონეზე, რადგან დაბალი ცნობიერების გამო როგორც ინდივიდები, ასევე ორგანიზაციები ვერ ახერხებენ კიბერსაფრთხეების წინააღმდეგ ქმედითი ზომების მიღებას. შესაბამისად, ზემოთ აღწერილ გავლენიან ჯგუფებს უნდა მიენიჭოთ მაღალი პრიორიტეტი კიბერცნობიერების გაუმჯობესებისკენ მიმართული კამპანიის დაგეგმვისა და განხორციელების პროცესში.

25. ინტერვიუ მთავრობის მაღალჩინოსან მოხელესთან, თბილისი, 4 ოქტომბერი 2022.
26. ინტერვიუები სსო-ების წარმომადგენლებთან, თბილისი, 3-4 ოქტომბერი 2022.
27. ინტერვიუ საქართველოს მთავრობის მაღალჩინოსან მოხელესთან, თბილისი, 4 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან წევრთან ციფრული პლატფორმის გამოყენებით, 18 ოქტომბერი 2022.

დაცულობის შეგრძნება და ნდობა

ფოკუსჯგუფების მონაწილეებს სთხოვეს შეეფასებინათ, რამდენად დაცულად გრძნობენ თავს ინტერნეტ და ციფრული სერვისებით სარგებლობისას. ფოკუსჯგუფის დაწყებისას 41-დან 33-მა მონაწილემ დაცულობის შეგრძნება შეაფასა, როგორც „ზომიერი“, ხოლო რვა მონაწილემ განაცხადა, რომ თავს „ზომიერად“ ან „ძალზე“ დაუცველად გრძნობდნენ. ფოკუსჯგუფის დასრულების შემდეგ განწყობები შეიცვალა და 28 მათგანმა მიუთითა, რომ თავს ზომიერად ან ძალზე დაუცველად გრძნობდნენ (იხ. სურათი 2).

სურათი 2: დაცულობის შეგრძნება, მონაცემები ფოკუსჯგუფებიდან



წყარო: დიაგრამა შედგენილია ფოკუსჯგუფებში განხილვების შედეგების მიხედვით.

ფოკუსჯგუფების მონაწილეებმა იმსჯელეს იმის შესახებ, თუ რა ტიპის ქმედებებს აღიქვამენ კიბერდანაშაულად. მათ ასევე მოიყვანეს მაგალითები რეალური გამოცდილებიდან. როგორც ზემოთ ითქვა, მკვლევრებს არ განუმარტავთ მონაწილეებისთვის, თუ რას გულისხმობს კიბერდანაშაული. ამის ნაცვლად, ისინი მსუბუქი ხელმძღვანელობით წარუძღვნენ განხილვებს, რათა მონაწილეებს არ გადაეხვიათ ძირითადი თემიდან. ამგვარად, მონაწილეებს შესაძლებლობა მიეცათ დამოუკიდებლად გაემახვილებინათ ყურადღება როგორც კლასიკურ, ისე კიბერ მეთოდით ჩადენილ კიბერდანაშაულსა და ვირტუალურ საფრთხეებზე. 20-მა მონაწილემ მიუთითა, რომ მათ ნაკლებად დაცულად იგრძნეს თავი ფოკუსჯგუფის დასრულების შემდეგ (იხ. სურათი 2), რაც კიბერცნობიერების

დაბალ დონეზე მიუთითებს. ეს მოსაზრება კიდევ უფრო გამყარდა მონაწილეების კომენტარებით. მაგალითად, ერთ-ერთმა მონაწილემ, პროფესიით ჟურნალისტმა, შენიშნა, რომ ფოკუსჯგუფში მონაწილეობის შემდეგ კიდევ უფრო გაუმძაფრდა დაუცველობის განცდა, რადგან მანამდე სრულიად ნათლად არ ჰქონდა წარმოდგენილი, თუ რა ზიანის მოტანა შეეძლოთ კიბერდამნაშავეებს.[28]

უფრო მეტიც, ყველა გამოკითხული ექსპერტის აზრით, ქართველები ჯეროვნად ვერ აფასებენ კიბერდანაშაულის საფრთხეებს.

დაცულობის შეგრძნება არაერთგვაროვანია. ფოკუსჯგუფში განხილვის დაწყებამდე, ქალები კაცებზე მეტად დაცულად გრძნობდნენ თავს: 25-მა ქალმა მიუთითა, რომ ისინი ზომიერად ან ძალზე დაცულად გრძნობდნენ თავს. შედარებისთვის, ამ მოსაზრებას მხოლოდ რვა მამაკაცი იზიარებდა.[29] თუმცა, ფოკუსჯგუფებში განხილვების დასრულების შემდეგ დაცულობის მაჩვენებელი ორივე ჯგუფში დაქვეითდა: 17-მა ქალმა და სამმა კაცმა მიუთითა, რომ მათი დაცულობის აღქმა ზომიერად ან მნიშვნელოვნად გაუარესდა. ქალების ფოკუსჯგუფის 12-დან 9 მონაწილემ აღნიშნა, რომ მათი აზრით, ვიქტიმიზაციის საფრთხე მათ უფრო ემუქრებათ, ვიდრე კაცებს.[30] ეს მონაცემები, შესაძლოა, მიუთითებდეს, რომ საქართველოში ქალები უფრო გრძნობენ კიბერსდანაშაულის საფრთხეს. მონაცემების მიხედვით, ასევე, შეიძლება ვივარაუდოთ, რომ მომეტებული საფრთხის შეგრძნება შეიძლება განპირობებული იყოს კიბერცნობიერების დაბალი დონით. თუმცა, ამ ვარაუდის გასამყარებლად დამატებითი კვლევებია საჭირო.

ცოდნა კიბერდანაშაულის შესახებ

კიბერჰიგიენა

როგორც ზემოთ ითქვა, კიბერჰიგიენაში იგულისხმება იმ გამოცდილი და ეფექტიანი ქმედებების ერთობლიობა, რომელიც ამცირებს კიბერსაფრთხეების რისკს. მაგალითად, ითვლება, რომ ორგანიზაცია იცავს კიბერჰიგიენას, თუ იგი მუდმივად ქმნის და ინახავს მონაცემების სარეზერვო ასლებს, იყენებს მულტიფაქტორული ავტორიზაციის სისტემას და რთულ პაროლებს, ასევე რეგულარულად აახლებს სისტემებს. კიბერჰიგიენის გაუმჯობესება მნიშვნელოვანი ნაბიჯია ეროვნული კიბერეკოსისტემის გაძლიერებისკენ. ტრადიციული არგუმენტის მიხედვით, რაც მეტი ინდივიდი და ორგანიზაცია დაიცავს

28. ჟურნალისტების ფოკუსჯგუფი, თბილისი, 6 ოქტომბერი 2022.
29. ფოკუსჯგუფების მონაწილეთა სრული რაოდენობა 41-ს შეადგენდა, მათგან 28 ქალი და 13 კაცი. სულ ჩატარდა 4 ფოკუსჯგუფი შემდეგი კონკრეტული ჯგუფებისთვის: ეთნიკური უმცირესობების წარმომადგენლები (9); ქალები (12); ჟურნალისტები (10); და მშობლები, კანონიერი წარმომადგენლები და მასწავლებლები (10).
30. ქალების ფოკუსჯგუფი, თბილისი, 4 ოქტომბერი 2022.

ყოველდღიურ პრაქტიკაში კიბერჰიგიენას, მით უფრო შემცირდება მათი ვიქტიმიზაციის რისკი კიბერკრიმინალების მიერ.

მიუხედავად იმისა, რომ კიბერჰიგიენა მნიშვნელოვანი მექანიზმია, რომელიც საერთო კიბერმედეგობის გაუმჯობესებას ემსახურება, მნიშვნელოვანია აღინიშნოს, რომ ეს მხოლოდ ერთ-ერთ ღონისძიებას წარმოადგენს ამ მიზნის მისაღწევად. საერთაშორისო დონეზე აპრობირებულ პრაქტიკად იქცა პროდუქტისა და სერვისის დაცვა დიზაინის ეტაპზევე, რაც გაანეიტრალებს კიბერუსაფრთხოების რისკს, ხოლო სერვისის ან პროდუქტის საბოლოო მომხმარებელს აღარ ექნება გადაწყვეტილების მიღების შესაძლებლობა, რაც თავის მხრივ, შეამცირებს ინდივიდუალურ არჩევანზე დამოკიდებულებას.[31] თუმცა, კიბერუსაფრთხოების გაუმჯობესება ეროვნული კიბერმედეგობის გაუმჯობესებისთვის ერთ-ერთ მნიშვნელოვან ნაბიჯად რჩება.

მიჩნეულია, რომ კიბერჰიგიენა და კიბერცნობიერება ერთმანეთთან პირდაპირ კავშირშია. როგორც ასეთი, კიბერცნობიერების დაბალი დონე არასათანადო კიბერჰიგიენას ნიშნავს. კვლევის ფარგლებში გამოკითხული ექსპერტების უმეტესობა ამტკიცებს, რომ კიბერჰიგიენის დაცვა გადამწყვეტი ფაქტორია, როდესაც საქმე კიბერდანაშაულებრივი ქმედებების წარმატებასა და მარცხს ეხება. ერთ-ერთმა რესპონდენტმა დასძინა, რომ „კიბერჰიგიენა საზოგადოების ძირითადი პრობლემაა, რომელიც პირდაპირ კავშირშია კიბერდანაშაულთან“.[32] მსგავსად ექსპერტებისა, ფოკუსჯგუფის მონაწილეებიც ხშირად ამბობდნენ, რომ „არ იციან, თუ როგორ უნდა მოიქცნენ“ მათ წინააღმდეგ განხორციელებული კიბერდანაშაულის შემთხვევისას, მათ შორის, არ იციან, მაგალითად, თუ როგორ უნდა შეინახონ კიბერმტკიცებულება. კვლევის შედეგებზე დაყრდნობით შეიძლება ითქვას, რომ კიბერჰიგიენა ქართველებისთვის სამ ძირითად საკითხს უკავშირდება. ესენია: ქცევები, ინსტრუმენტები და სანდო წყაროები.

ქცევები

კიბერჰიგიენა განაპირობებს იმას, თუ როგორ ემზადებიან ადამიანები კიბერსაფრთხეებთან გასამკლავებლად და როგორ რეაგირებენ მათზე. გონივრული ქცევა გულისხმობს სკეპტიკურ დამოკიდებულებას არასანდო

31. იხილეთ, მაგალითისთვის, დიდი ბრიტანეთის ეროვნული კიბერუსაფრთხოების ცენტრის (NCSC) აქტიური კიბერთავდაცვის პროგრამა, „2022 წლის მიმოხილვა“, 1 ნოემბერი 2022, გვ. 17, <https://www.ncsc.gov.uk/collection/annual- review-2022/resilience/active-cyber-defence>, ბოლოს ნანახია: 5 მაისი 2023. იხილეთ, ასევე, ახლახან გამოქვეყნებული აშშ-ს ეროვნული კიბერუსაფრთხოების სტრატეგია, რომელშიც საუბარია ეროვნული კიბერუსაფრთხოების რისკების მართვისადმი ინოვაციური მიდგომის შესახებ, თეთრი სახლი, „ეროვნული კიბერუსაფრთხოების სტრატეგია“, მარტი 2023, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>, ბოლოს ნანახია: 5 მაისი 2023.

32. ინტერვიუ სსო-ს ხელმძღვანელთან, თბილისი, 3 ოქტომბერი 2022; ინტერვიუ სსო-ს წარმომადგენლებთან, თბილისი, 3 ოქტომბერი 2022; ინტერვიუ ქალთა ორგანიზაციის წევრებთან ციფრული პლატფორმის გამოყენებით, 20 ოქტომბერი 2022; ინტერვიუ with senior government official, თბილისი, 4 ოქტომბერი 2022.

ბმულების მიმართ და კონფიდენციალური მონაცემების გაუზიარებლობას. კვლევის შედეგები მიუთითებს, რომ არაგონივრული ქცევა, განსაკუთრებით კი პირადი ინფორმაციის - მაგალითად, პაროლების გაზიარება, უსაფრთხოების ზომების მიუღებლობა პროაქტიულად (როგორიცაა, მაგალითად, მულტიფაქტორული ავტორიზაცია) და ინტერნეტში განთავსებული ინფორმაციის უპირობოდ ნდობა, საკმაოდ გავრცელებულია საქართველოში. ინტერვიუს დროს მონაწილე ექსპერტებმა არადამაკმაყოფილებლად შეაფასეს ქვეყანაში არსებული კულტურული დამოკიდებულება კიბერუსაფრთხოების ზომების პროაქტიულად მიღების მიმართ. მათი თქმით, ადამიანები „მხოლოდ მას შემდეგ იწყებენ უსაფრთხოებაზე ზრუნვას, როდესაც... [მათ] ანგარიშებს „ტეხენ“.[33] ვალიდაციის სამუშაო შეხვედრისას, მცირე და საშუალო მეწარმეებმა, რომლებსაც არ უზრუნიათ საკუთარი კომანიების კიბერუსაფრთხოებაზე, განაცხადეს, რომ მათ წინააღმდეგ არასდროს განხორციელებულა კიბერთავდასხმა და შესაბამისად, არ მიაჩნდათ, რომ ხარჯი ღირდა ამ ძალისხმევად.

არაექსპერტი მონაწილეები ამბობდნენ, რომ ადამიანები საკმარისად არ ითვალისწინებენ კონფიდენციალურობის ფაქტორებს და მაგალითებად მოჰყავდათ პაროლების გაზიარების შემთხვევები, მათ შორის საკუთარ გამოცდილებაზე დაყრდნობითაც. ფოკუსჯგუფის ერთ-ერთმა მონაწილემ გაიხსენა სოფლად მცხოვრები ქალების ამბავი, რომლებსაც მათი პარტნიორები აიძულებენ პაროლის გაზიარებას მათი „ინტერნეტაქტივობების გაკონტროლების მიზნით.“[34] კიბერცნობიერების კამპანიის დაგეგმვისა და განხორციელების პროცესში სათანადო ყურადღება უნდა დაეთმოს კიბერჰიგიენის მნიშვნელობას. ამასთან, მნიშვნელოვანია, რომ ადამიანებმა არ იგრძნონ თავი შერცხვენილად, თუ ისინი არასათანადო ზომებს იღებენ კიბერსფრთხეების წინააღმდეგ.

ინსტრუმენტები

ინფორმაცია კიბერჰიგიენის ხელმისაწვდომი ინსტრუმენტებისა და მათი გამოყენების შესახებ საზოგადოებისთვის ნაკლებადაა ხელმისაწვდომი. ფოკუსჯგუფებში განხილვებისას, როდესაც მონაწილეებს წარუდგინეს კიბერჰიგიენის ღონისძიებების ნუსხა და სთხოვეს დაეხარისხებინათ ისინი ქმედუნარიანობის მიხედვით, ყველა მონაწილეს დასჭირდა სულ მცირე ერთი ღონისძიების განმარტება. უფრო ხშირად კი, მკვლევრებს უწევდათ სათითაოდ განემარტათ ყველა ღონისძიება მონაწილეთათვის.[35] ასევე აღსანიშნავია, რომ

33. ინტერვიუ ჟურნალისტთან, თბილისი, 3 ოქტომბერი 2022.
34. ქალების ფოკუსჯგუფი, თბილისი, 4 ოქტომბერი 2022.
35. ჩამოთვლილი კიბერჰიგიენის ზომები: სხვადასხვა პაროლი სხვადასხვა ანგარიშისთვის, მულტიფაქტორული ავტორიზაცია, გამომგზავნის ელექტრონული ფოსტის მისამართის შემოწმება, პაროლების ან პიროვნების მაიდენტიფიცირებელი ინფორმაციის გაუმჟღავნებლობა ვირტუალურ სივრცეში, კოდირებული კომუნიკაციის საშუალებების გამოყენება, ანტივირუსული პროგრამის გამოყენება, მოწყობილობის/პროგრამების ავტომატური განახლება, როუტერის სახელისა და კოდური სიტყვის გამოცვლა.

მონაწილეებმა, ერთი და იგივე ღონისძიებები მიიჩნიეს მეტ-ნაკლებად ეფექტიანად, რაც იმაზე მიუთითებს, რომ საზოგადოებაში სუსტია კონსენსუსი ძლიერ ან სუსტ უსაფრთხოების ზომებთან დაკავშირებით.[36] მონაწილეებს არც ერთი ზომა არ მიუჩნევიათ იმთავითვე უსარგებლოდ, რაც ვერ გამოდგება საზოგადოებაში კიბერცნობიერების დაბალი დონის მყარ ინდიკატორად, თუმცა, ამ შედეგით შეიძლება ვივარაუდოთ, რომ მონაწილეებს არ ჰქონდათ ინფორმაცია და ცოდნა კიბერუსაფრთხოების ძირითადი კონცეფციის შესახებ, რომელსაც შედარებისთვის გამოიყენებდნენ. ამ მიგნებას ამყარებს ფოკუსჯგუფების მონაწილეების კომენტარი, რომლის მიხედვითაც მათ იშვიათად უხდებოდათ კომუნიკაცია კიბერჰიგიენის საუკეთესო პრაქტიკების შესახებ. ასევე, ექსპერტებმაც აღნიშნეს, რომ მოსახლეობაში დაბალია კიბერცნობიერება და ადამიანები არ ენდობიან კიბერუსაფრთხოების ისეთ საბაზისო ინსტრუმენტებსაც კი, როგორიც არის, მაგალითად პაროლების მართვისთვის შექმნილი პროგრამები და აპლიკაციები. [37]

კერძო სექტორის წარმომადგენლების მსგავსად, ორგანიზაციებსაც უჭირთ ჯეროვნად შეაფასონ კიბერუსაფრთხოების ზომების მნიშვნელობა. მაგალითად, ფოკუსჯგუფის მონაწილე ერთ-ერთმა ჟურნალისტმა აღნიშნა, რომ მისი დამსაქმებელი – ერთ-ერთი მედიაკომპანია, თანამშრომლებისთვის არ უზრუნველყოფს კიბერუსაფრთხოების ინსტრუმენტებს და არც კიბერჰიგიენის გაუმჯობესებისკენ მიმართულ ტრენინგებს ან ცნობიერების ამაღლების კამპანიებს ატარებს მიუხედავად იმისა, რომ ჟურნალისტებს აქვთ კიბერდანაშაულების გამოცდილება (იხ. „კიბერდანაშაულით გამოწვეული გავრცელებული საფრთხეები“). ფოკუსჯგუფის სხვა მონაწილემაც დაადასტურა, რომ მსგავსი გამოცდილება მასაც ჰქონდა. მისი თქმით, მათი ორგანიზაციები სათანადო ძალისხმევას არ სწევენ კიბერუსაფრთხოების გაუმჯობესებისთვის. ამ ტენდენციაზე ისაუბრეს ექსპერტებმაც, რომელთა აზრითაც, ეს პრობლემა ენდემურია და რომ ორგანიზაციებს აკისრიათ პასუხისმგებლობა, უფრო გააქტიურდნენ ამ მიმართულებით.

ამ მოსაზრებებისგან განსხვავებით, ვალიდაციის სამუშაო შეხვედრისას, მცირე და საშუალო ბიზნესის წარმომადგენლებმა განაცხადეს, რომ ბოლო ხანებში მათი კომპანიების კიბერუსაფრთხოების უზრუნველყოფასთან დაკავშირებული ხარჯები 5-10%-ით გაიზარდა (მთლიან შემოსავალთან მიმართებაში). მათი თქმით, ეს თანხა ხმარდება ისეთი ტექნიკური ღონისძიებების გატარებას, როგორიცაა, მაგალითად, ტრენინგი ან IT-ის გამართულ მუშაობაზე პასუხისმგებელი პერსონალის სადღეღამისო მომსახურება, აღნიშნული ხარჯები ასევე ხმარდება

36. ზომები სტანდარტულად განაწილებული არ ყოფილა რესპონდენტებს შორის – ზომები, რომლებიც საშუალოზე მეტი მონაწილის მიერ იყო მიჩნეული განსაკუთრებით ეფექტიანად ან არაეფექტიანად, იყო „განსხვავებული პაროლი სხვადასხვა ანგარიშისთვის“ და „მულტიფაქტორული ავტორიზაცია“, რომლებსაც მონაწილეები ეფექტიანად მიიჩნევდნენ და „მოწყობილობების/პროგრამების ავტომატური განახლება“, რომლებიც რესპონდენტების მიერ არაეფექტიან ზომებად იქნა მიჩნეული.
37. ინტერვიუები სსო-ების მაღალი რანგის წარმომადგენელთან, თბილისი, 6 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან წევრთან ციფრული პლატფორმის მეშვეობით, 18 ოქტომბერი 2022.

არატექნიკურ ღონისძიებებსაც, მაგალითად, საფრთხეების მყისიერი მიმართვიანობის მექანიზმებს და ინფორმაციის გაუთქმელობის შეთანხმებებს. ცხადია, ამგვარი პროგრესი დამაიმედებელია, თუმცა, საწყისი მონაცემების ანალიზი მიუთითებს, რომ ეს პრაქტიკა უფრო გამონაკლისია, ვიდრე - წესი.

სანდო წყაროები

პასუხად შეკითხვაზე „ყველაზე მეტად რომელ წყაროს ენდობით, როდესაც საქმე კიბერჰიგიენის შესახებ ინფორმაციას ეხება?“ ფოკუსჯგუფის მონაწილეებმა ყველაზე სანდო წყაროებად სამთავრობო საინფორმაციო კამპანიები (49%), სამართალდამცავი სამსახურების ვებგვერდები (41%) და ახალი ამბების/მედია ორგანიზაციები (41%) დაასახელეს.[38] მიუხედავად იმისა, რომ როდესაც საქმე კიბერდანაშაულის მიმართვიანობას ეხება, მთავრობა მაღალი ნდობით არ სარგებლობს (იხ. ქვემოთ „კიბერდანაშაულის მიმართვიანობა მოქალაქეების მიერ“), გაცილებით მაღალია მისი, როგორც კიბერჰიგიენის შესახებ ინფორმაციის წყაროს სანდოობა ფოკუსჯგუფის მონაწილეებში, რაც, მათივე თქმით, ინტერესების თანხვედრით აიხსნება. მონაწილეების უმეტესობა იზიარებს მოსაზრებას იმის შესახებ, რომ მთავრობას არ აქვს სურვილი გაიზარდოს ვიქტიმიზაციის მაჩვენებელი, რაც მაღალ ხარჯებსა და უსაფრთხოების მომეტებულ რისკებთან იქნებოდა დაკავშირებული. შესაბამისად, მთავრობა ცდილობს რაც შეიძლება სანდო ინფორმაცია მიაწოდოს საზოგადოებას. ეს განწყობა სამართალდამცავი უწყებების ვებგვერდებზეც ვრცელდება. რაც შეეხება მედიასაშუალებებს, მონაწილეების არჩევანი განპირობებული იყო იმ ფაქტით, რომ მედია ორგანიზაციები, ზოგადად, ინფორმაციის გავრცელების ეფექტიანი წყაროა, თუმცა, ფოკუსჯგუფის რამდენიმე მონაწილემ უკმაყოფილება გამოთქვა იმასთან დაკავშირებით, რომ მედია ნაკლებად აშუქებს კიბერდანაშაულის პრობლემებს.

სურათი 3: კიბერჰიგიენის შესახებ ინფორმაციის წყაროები

მთავრობის მიერ ორგანიზებული საინფორმაციო კამპანიები	**49%**	0%
სამართალდამცავი უწყებების ვებგვერდები	41%	2%
ახალი ამბების სააგენტოები/მედიაორგანიზაციები	41%	20%
სოციალური მედია	37%	49%
სამთავრობო ვებგვერდები	37%	0%
მეგობრები ამ ოჯახის წევრები	24%	**54%**
არასამთავრობო ორგანიზაციები	22%	27%

წყარო: შედგენილია ავტორების მიერ ფოკუსჯგუფებში განხილვების მიხედვით

ინფორმაციის სანდო წყაროების შესახებ კითხვაზე პასუხებისგან განსხვავებით, აღმოჩნდა, რომ მონაწილეები კიბერჰიგიენის შესახებ ინფორმაციას ყველაზე ხშირად მეგობრებისა და ოჯახის წევრებისგან (54%) და სოციალური მედიიდან

38. პროცენტული მაჩვენებლები შეესაბამება შემდეგ რაოდენობრივ მაჩვენებლებს: 49%=20; 41%=17.

(49%) იღებენ (კითხვა: საიდან იღებთ ინფორმაციას კიბერჰიგიენის შესახებ?“).[39] მიუხედავად იმისა, რომ ეს შედეგები, თავისთავად, დიდ პრობლემას არ წარმოადგენს, საფიქრებელია, რომ კიბერცნობიერების დაბალი დონე კვლევის მონაწილეებს შორის, სავარაუდოდ, მათ პირად კონტაქტებს შორისაც კიბერჰიგიენის დაბალ დონეზე მიუთითებს. უფრო მეტიც, ექსპერტებმა რამდენჯერმე გაუსვეს ხაზი იმ საფრთხეებს, რომლებიც უკავშირდება სოციალურ მედიას, როგორც დეზინფორმაციის გავრცელების ინსტრუმენტს.[40] ცხადია, ეს იმას არ ნიშნავს, რომ სოციალური მედიის ყველა ასპექტი ნეგატიურ ჭრილში უნდა იქნეს განხილული. მაგალითად, ფოკუსჯგუფის ერთ-ერთმა მონაწილემ ახსენა ფეისბუქჯგუფი ქალებისთვის, რომლის წევრებიც ერთმანეთს მხარდაჭერას უწევენ და ამხნევებენ, სამართალდამცველებს შეატყობინონ მათი ყოფილი პარტნიორების მიერ გამოწვეული ონლაინ ზიანის შესახებ.[41]

მიუხედავად იმისა, რომ ეს ვარიანტი არ ყოფილა მითითებული, ფოკუსჯგუფების 11-მა მონაწილემ კიბერჰიგიენის შესახებ ინფორმაციის მიღების სანდო წყაროდ არასამთავრობო ორგანიზაციები დაასახელა. მათ შორის არიან ეთნიკური უმცირესობების ფოკუსჯგუფის ცხრა მონაწილიდან ექვსი, ასევე, ოთხი ჟურნალისტი (10-დან) და ერთი ქალი (ქალების ფოკუსჯგუფის 12 მონაწილიდან). არასამთავრობო ორგანიზაცია, როგორც ინფორმაციის სანდო წყარო, არც ერთხელ არ დასახელებულა მშობლების, მეურვეებისა და მასწავლებლების ფოკუსჯგუფის მონაწილეების მიერ.[42] შემდგომი მსჯელობისას, აღნიშნული მონაწილეებმა ორი ფაქტორით ახსნეს. პირველი, ეს არის მიწოდების მხარე, რაც იმას გულისხმობს, რომ ეთნიკური უმცირესობების წარმომადგენლებს ხელი მიუწვდებათ კიბერჰიგიენის შესახებ ვრცელ ინფორმაციაზე სწორედ არასამთავრობო ორგანიზაციების მეშვეობით. ერთ-ერთმა რესპონდენტმა მკვლევრებს აუხსნა, რომ არასამთავრობო ორგანიზაციების ყურადღების ცენტრში ხშირად ექცევიან ეროვნული უმცირესობები და ჟურნალისტები, როგორც მაღალი რისკის ჯგუფები. მეორე ფაქტორი მოთხოვნას უკავშირდება: ჟურნალისტებისა და ეთნიკური უმცირესობების წარმომადგენლების განცხადებით, ისინი მეტად ენდობიან არასამთავრობო ორგანიზაციებს, ვიდრე – მთავრობის მხარდაჭერას (იხ. „კიბერდანაშაულის მიმართვიანობა მოქალაქეების მიერ“).

39. პროცენტული მაჩვენებლები შეესაბამება შემდეგ რაოდენობრივ მაჩვენებლებს: 54%=22; 49%=20. ზოგიერთმა მონაწილემ შესაძლოა აირჩია როგორც „მეგობრები და ოჯახის წევრები“, ასევე „სოციალური მედია“.
40. ინტერვიუ ჟურნალისტებთან, თბილისი, 3 ოქტომბერი 2022; ინტერვიუ სსო-ს ხელმძღვანელთან, 3 ოქტომბერი 2022; ინტერვიუ სსო-ს წარმომადგენელთან, თბილისი, 3 ოქტომბერი 2022
41. ქალების ფოკუსჯგუფი, თბილისი, 4 ოქტომბერი 2022.
42. ინტერვიუ ჟურნალისტთან, თბილისი, 3 ოქტომბერი 2022.

პროფესიული და განათლების ეკოსისტემა

კვლევის შედეგების მიხედვით პროფესიული და განათლების ეკოსისტემა, რომელიც ფოკუსირებულია კიბერდანაშაულსა და კიბერუსაფრთხოებაზე საქართველოში, შესაძლებლობების დეფიციტს განიცდის. შედეგად, ქვეყანაში იგრძნობა პროფესიულ დონეზე განვითარებული კიბერცნობიერების მქონე კვალიფიციური ექსპერტების ნაკლებობა. თუმცა, ეს სიტუაცია სწრაფად იცვლება, განსაკუთრებით რუსეთის უკრაინაში შეჭრის შემდეგ, რის შედეგადაც, რუსი ეროვნების მრავალი კიბერპროფესიონალი საქართველოში ჩამოვიდა. თუმცა, ჯერ კიდევ დასადგენია რა გზას ირჩევენ რუსი ემიგრანტები – ქართულ კომპანიებში მუშაობას თუ რუსული სახელმწიფო კიბერუსაფრთხოების მხარდაჭერას.[43]

მიუხედავად იმისა, რომ ქვეყნების უმეტესობა მსგავსი გამოწვევების წინაშე დგას, როდესაც საქმე კიბერპროფესიონალებსა და კიბერგანათლების განვითარებას ეხება, არსებობს რამდენიმე ძირითადი მიმართულება, რომელთა განვითარებაც საქართველოს სწრაფი ტემპებით შეუძლია.

განათლება

კვლევის ფარგლებში გამოკითხულმა არაერთმა ექსპერტმა გამოთქვა უკმაყოფილება საქართველოში უმაღლესი განათლების საფეხურზე კიბერუსაფრთხოების პროგრამების ნაკლებობასთან დაკავშირებით.[44] მაგალითად, ორმა რესპონდენტმა აღნიშნა, ქვეყანაში ერთადერთი საბაკალავრო პროგრამა არსებობს კიბერუსაფრთხოების დარგში, რომელსაც კავკასიის უნივერსიტეტი ახორციელებს ნიუ ჯერსის უნივერსიტეტთან ერთად.[45] თუმცა, კიდევ ერთი რესპონდენტის განცხადებით, კიდევ უფრო მწვავედ დგას ქვეყანაში სამაგისტრო პროგრამების სიმწირე. მისი მტკიცებით, თითზე ჩამოსათვლელი სამაგისტრო დონის კურსები მაღალკვალიფიციური კადრისთვის ჩიხურ სიტუაციას ქმნის.[46] იმავე რესპონდენტის თქმით, სიტუაციიდან გამოსავალია ამ პროგრამების რაოდენობის ზრდა და მსგავსი კურსების შემოღება ეროვნული თავდაცვის აკადემიაში, რაც სამთავრობო სტრუქტურების შიგნით შექმნიდა კიბერუსაფრთხოების შესაძლებლობების განვითარების ბაზას. [47]

43. *The Bell*, 'Russia's IT Exodus and the Kremlin's Futile Efforts to Reverse It'[რუსეთის IT გამოსვლა და კრემლის ფუჭი ძალისხმევა მის შესაჩერებლად], 24 იანვარი 2023, <https:// en.thebell.io/russia-s-it-exodus-and-the-kremlin-s-futile-efforts-to-reverse-it/>, ბოლოს ნანახია: 25 აპრილი 2023.
44. ინტერვიუ სსო-ს მაღალი რანგის წარმომადგენელთან, თბილისი, 6 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მრჩეველთან, თბილისი, 4 ოქტომბერი 2022; ინტერვიუ სსო-ს მაღალი რანგის წარმომადგენელთან, თბილისი, 4 ოქტომბერი 2022.
45. ინტერვიუ მთავრობის ყოფილ მრჩეველთან, თბილისი, 4 ოქტომბერი 2022; ინტერვიუ სსო-ს მაღალი რანგის წარმომადგენელთან, თბილისი, 6 ოქტომბერი 2022.
46. ინტერვიუ მთავრობის ყოფილ მრჩეველთან, თბილისი, 4 ოქტომბერი 2022.
47. იქვე.

მონაცემების შეგროვების პროცესში, როგორც ინდივიდუალურმა რესპონდენტებმა, ასევე ფოკუსჯგუფების მონაწილეებმა საგანგებოდ აღნიშნეს განათლების სისტემის, როგორც კიბერდაცულობისა და ნდობის განმამტკიცებელი მექანიზმის მნიშვნელობა. ამავე დროს, არაერთმა მონაწილემ ხაზი გაუსვა იმ ფაქტს, რომ ამჟამად ამ ინსტრუმენტის გამოყენება სათანადოდ არ ხდება. გარდა ამისა, მონაწილეებმა დაასახელეს ის ზომები, რომლებიც შესაძლებელს გახდის განათლების სისტემის ეფექტიანად გამოყენებას, და ასევე იმსჯელეს ამ ზომების გატარების ზეგავლენის შესახებ:

- სტუდენტებში კიბერცნობიერებისა და კიბერუსაფრთხოების უნარების გაუმჯობესება,[48] რაც ასევე გულისხმობს შესაბამისი საკითხების ინტეგრირებას სასწავლო პროგრამებში ან სპეციალური სასწავლო სესიების ორგანიზებას სტუდენტებისთვის, რაც, თავის მხრივ, გაზრდის ამ მაღალი რისკჯგუფის დაცულობის ხარისხს კიბერდანაშაულისა და ონლაინ საფრთხეებისგან (იხ. „კიბერდანაშაულის მიერ წარმოქმნილი საერთო საფრთხეები“). გარდა ამისა, ამგვარი მიდგომის დანერგვის შედეგად, ბავშვები და ახალგაზრდები გაეცნობიან კიბერდანაშაულების სამართალდამცავი ორგანოებისთვის მიმართვიანობის პროცედურებს (იხ. თავი III).
- ნდობაზე დაფუძნებული ურთიერთობის ჩამოყალიბება მშობლებს/მეურვეებსა და ბავშვებს შორის კიბერუსაფრთხოების საკითხების ირგვლივ.[49] სკოლებს შეუძლიათ ორგანიზება გაუწიონ ან უმასპინძლონ სასწავლო სესიებს, რათა როგორც მშობლებმა/კანონიერმა წარმომადგენლებმა, ისე ბავშვებმა ერთობლივად გაიუმჯობესონ ცოდნა კიბერდანაშაულის საფრთხეებისა და მათი განეიტრალების/შერბილების გზების შესახებ, რაც, თავის მხრივ, ხელს შეუწყობს საზოგადოებაში ცნობიერების დონის ამაღლებას და ასევე გააქარწყლებს მშობლების/მეურვეების შიშს იმასთან დაკავშირებით, რომ ბავშვები, მათი მხრიდან კიბერუსაფრთხოებაზე ზრუნვას უნდობლობის გამოვლინებად ჩათვლიან.[50]
- ცნობიერების ამაღლების მულტიპლიკაციის ეფექტი.[51] სკოლები ხშირად ასრულებს სათემო ჰაბების ფუნქციას, განსაკუთრებით სასოფლო დასახლებებისთვის.[52] ცნობიერების ამაღლებისკენ მიმართული აქტივობების მასპინძლობა მათ მიერ, დიდი ალბათობით, მიიზიდავს თემის სხვა წევრებსაც და შედეგად, გაზრდის ინტერვენციის ზეგავლენის არეალს. უფრო მეტიც, როგორც რამდენიმე რესპონდენტმა მიუთითა, სკოლები დაკავშირებულია

48. იქვე.; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან წევრთან ციფრული პლატფორმის მეშვეობით, 7 ოქტომბერი 2022, ინტერვიუ მთავრობის ყოფილ მრჩეველთან, თბილისი, 4 ოქტომბერი 2022..
49. ინტერვიუ სსო-ს მაღალი რანგის წარმომადგენელთან, თბილისი, 3 ოქტომბერი 2022; ინტერვიუ სსო-ს ხელმძღვანელთან, თბილისი, 6 ოქტომბერი 2022.
50. ვალიდაციის სამუშაო შეხვედრა, თბილისი, 22 დეკემბერი 2022.
51. იქვე.; ინტერვიუ მთავრობის მაღალჩინოსან მოხელესთან, თბილისი, 4 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან წევრთან ციფრული პლატფორმის მეშვეობით, 7 ოქტომბერი 2022.
52. ინტერვიუ მთავრობის მაღალჩინოსან მოხელესთან, თბილისი, 4 ოქტომბერი 2022.

რამდენიმე სოციალურ ქსელთან და შესაბამისად, ძალისხმევის მრავალჯერადი ეფექტიც უფრო საგრძნობი იქნება.

კვალიფიკაციის ამაღლება და სერტიფიცირება

რესპონდენტებმა, განსაკუთრებით ტექნიკური განათლებით ან კერძო სექტორში მუშაობის გამოცდილებით, ხაზი გაუსვეს იმ ბარიერებს, რომელთა გადალახვაც უწევთ კიბერუსაფრთხოების სპეციალისტებს კვალიფიკაციის ამაღლებისა და სერტიფიცირებისთვის.[53] ეს ნაწილობრივ კერძო სექტორში ინვესტიციების პრობლემას უკავშირდება, თუმცა, შესაძლოა, ასევე იყოს გამოწვეული პარტნიორი ქვეყნების მიერ კიბერუსაფრთხოების სფეროში კიბერშესაძლებლობების განვითარების დაბალრისკიანი ინვესტიციებით. ერთ-ერთმა მონაწილემ აღნიშნა, რომ, როდესაც საქმე კვალიფიკაციის/სერტიფიცირების საკითხს ეხება, კიბერუსაფრთხოების განვითარებისკენ მიმართული ინვესტიციები თავს არიდებს რისკებს, ხოლო ინიციატორები ნაკლებად უჭერენ მხარს ისეთ სქემებს, რომელთა წარუმატებლობის ალბათობის საშუალო მაჩვენებელი მაღალია ან ისეთ სენსიტიურ თემებს ეხება, როგორიცაა მაგალითად ქსელებში შეღწევადობის ტესტირება, რაც შედეგად მიწოდების მნიშვნელოვან დეფიციტს იწვევს და ეროვნული კიბერთავდაცვის შესაძლებლობებს ზღუდავს.[54] კვალიფიკაციის ამაღლებისა და სერტიფიცირების სქემები შეიძლებოდა ასევე ყოფილიყო გამოყენებული საჯარო სექტორში თანამშრომელთა შენარჩუნებისთვის. საჯარო სექტორში მუშაობის გამოცდილების მქონე არაერთი რესპონდენტის აზრით, მთავრობა შეძლებს ტექნიკური პერსონალის დიდხანს შენარჩუნებას, თუ მათ უკეთესი ხარისხის ტექნიკური გადამზადების შესაძლებლობებს შესთავაზებს.[55] ეს მიმართულება პირდაპირ კავშირშია საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიის 3.2 ამოცანასთან, რომელიც წამყვან სამთავრობო უწყებებში ეროვნული კიბერშესაძლებლობების განვითარებას ეხება.[56]

საქართველო არ არის ერთადერთი ქვეყანა, სადაც ეროვნულ დონეზე კიბერშესაძლებლობებისა და ცნობიერების გაუმჯობესება დამატებით ძალისხმევას საჭიროებს. ყველა თუ არა, ქვეყნების უმეტესობას უჭირს ამ პრობლემასთან გამკლავება. მაგალითად, საქართველო ჩამორჩება გლობალურ ლიდერებს - აშშ-სა და ჩინეთს. თუმცა, როგორც ერთ-ერთმა გამოკითხულმა

53. ინტერვიუ სსო-ს ხელმძღვანელთან, თბილისი, 6 ოქტომბერი 2022; ინტერვიუ მთავრობის ყოფილ მრჩეველთან, თბილისი, 4 ოქტომბერი 2022.
54. ინტერვიუ სსო-ს ხელმძღვანელთან, თბილისი, 6 ოქტომბერი 2022.
55. იქვე.; ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან წევრთან ციფრული პლატფორმის მეშვეობით, 18 ოქტომბერი 2022.
56. საქართველოს მთავრობა, „საქართველოს ეროვნული კიბერუსაფრთხოების სტრატეგია“, გვ. 20.

ექსპერტმა განაცხადა, საქართველო მოწინავე პოზიციას იკავებს რეგიონში. ეს საკითხი შემდგომ კვლევას საჭიროებს.[57]

გზამკვლევი კიბერცნობიერების ამაღლების კამპანიისთვის

პირველადი მონაცემების შეგროვების ეტაპზე, მონაწილეების უმეტესობამ ხაზი გაუსვა კიბერდანაშაულის შესახებ ცნობიერების ამაღლების მიზნით ღონისძიებების გატარების საჭიროებას. ქვემოთ მოცემული რეკომენდაციები, რომლებიც მონაწილეებს ეკუთვნის, ეხება ამ ღონისძიებების სტრუქტურას. რეკომენდაციები ასევე გათვალისწინებულია მე-4 თავში, რომელიც კონკრეტულად რეკომენდაციებს ეძღვნება.

- **მარტივად გასაგები შინაარსი.** მონაწილეები მუდმივად აღნიშნავდნენ, რომ საჭიროა, შინაარსი იყოს გასაგები, ხოლო კამპანიის გზავნილები მკაფიო, მოკლე და დასამახსოვრებელი და უნდა ეხებოდეს ისეთ კონკრეტულ საკითხებს, როგორიცაა, საფრთხის ბუნება, პაროლების ჰიგიენა ან პირადი ინფორმაციის დაცვის უფლება. კამპანია ასევე უნდა შეიცავდეს პრაქტიკულ მაგალითებს და ნამდვილ ამბებს, რომლებიც განსაკუთრებული ზეგავლენით გამოირჩევა. როგორც ერთ-ერთმა რესპონდენტმა - აკადემიური სფეროს წარმომადგენელმა განაცხადა, „კომუნიკაციის მიზნებისთვის, ცოდნასთან ერთად გადამწყვეტი მნიშვნელობა ენიჭება ნამდვილ ამბებსაც“. კამპანია აგებული უნდა იყოს ინტუიციურ კომუნიკაციაზე და მნიშვნელოვანია ვიზუალური ინსტრუმენტების, მათ შორის, ვიდეომასალის გამოყენებაც ინფორმაციის გამარტივებისთვის. აუცილებელია, რომ კამპანია წარიმართოს რამდენიმე ენაზე, რაც უზრუნველყოფს ეთნიკური უმცირესობების ჩართულობას.
- **აუდიტორიაზე მორგებული კომუნიკაციის ინსტრუმენტები.** კამპანია მორგებული უნდა იყოს აუდიტორიაზე. ზოგადი ხასიათის გზავნილებთან ერთად, აუცილებელია კონკრეტულ ჯგუფებზე მორგებული ინფორმაციის გავრცელებაც. მაგალითად, ერთ-ერთმა მონაწილემ ვალიდაციის სამუშაო შეხვედრაზე აღნიშნა, რომ ლიცენზირებულ პროგრამებზე საუბარი უშედეგოა იმ ჯგუფთან, რომელიც სიღარიბის ზღვარზე ცხოვრობს, ხოლო მეორე რესპონდენტმა - ექსპერტმა, რომელიც ქალთა ჯგუფთან მუშაობს, ასევე დაბეჯითებით გაუსვა ხაზი ქალებისა და გოგონებისთვის პირადი ინფორმაციის დაცვის მნიშვნელობის შესახებ ცნობიერების ამაღლებას, რადგან ეს ჯგუფი ყველაზე მეტად დგას ისეთი საფრთხეების წინაშე, როგორიცაა, მაგალითად, პირადი ინფორმაციის უნებართვო გავრცელება.

57. ინტერვიუ მთავრობის მაღალჩინოსან მოხელესთან, თბილისი, 5ოქტომბერი 2022.

- **ფოკუსირება მაღალი მოწყვლადობისა და ზეგავლენის ჯგუფებზე.** ზოგი ჯგუფი უფრო მოწყვლადია კიბერდანაშაულების მიმართ. ასევე, არიან ჯგუფებიც, რომლებიც გადამწყვეტ როლს ასრულებენ დანაშაულების პრევენციის ან მათი შედეგების შერბილებაში (იხილეთ ზემოთ თავი პრიორიტეტული მიმართულებების შესახებ). ცნობიერების ამაღლებისკენ მიმართული ინტერვენციები დამატებით ზომებს უნდა ითვალისწინებდეს სწორედ ამგვარი ჯგუფებისთვის. მაგალითად, დამატებითი ძალისხმევაა საჭირო სოფლად მცხოვრები მოსახლეობისთვის, რომლებიც ცუდად ფლობენ ქართულ ენას. სამიზნე ჯგუფების შერჩევა უნდა ითვალისწინებდეს კიბერდანაშაულის შესახებ ცნობიერების საშუალო დონესა და პრიორიტეტს ანიჭებდეს გზავნილებს, რომლებიც გააუმჯობესებს ადამიანების ცხოვრების ხარისხს. ამგვარი გზავნილების მაგალითია მოწოდება მცირე და საშუალო ბიზნესის უსაფრთხო გაციფრულებისკენ.
- **უწყებათაშორისი კოორდინაცია.** კიბერუსაფრთხოების ეროვნული სტრატეგიის თანახმად, ციფრული მმართველობის სააგენტო წამყვანი უწყებაა, რომელიც პასუხისმგებელია ცნობიერების ამაღლებაზე, ხოლო შინაგან საქმეთა სამინისტრო - კიბერდანაშაულის საკითხებზე. შესაბამისად, ორივე უწყება თანაბრად უნდა იყოს ჩართული კიბერდანაშაულის საფრთხეებისა და კიბერჰიგიენის მნიშვნელობის შესახებ გზავნილების შედგენასა და გავრცელებაში. რესპონდენტების აზრით, კიბერცნობიერების კამპანიის წარმატებისთვის აუცილებელია ორივე უწყებას შორის მჭიდრო თანამშრომლობა და მათი კოორდინირებული მოქმედება სხვა სამთავრობო უწყებებთან. საჯარო სექტორის სხვა აქტორებში, რომელთა ჩართულობაც კვლევის მონაწილეებმა მნიშვნელოვნად მიიჩნიეს წარმატებული კამპანიისთვის, მოიაზრება საქართველოს ეროვნული ბანკი და განათლების, მეცნიერების, კულტურისა და სპორტის სამინისტრო.
- **სხვადასხვა პლატფორმების გამოყენება.** ფოკუსჯგუფების თითქმის ყველა მონაწილემ და ინდივიდუალური ინტერვიუების რესპონდენტებმა, რომლებმაც აზრი გამოთქვეს კიბერდანაშაულის შესახებ ცნობიერების ამაღლების კამპანიის შესახებ, ხაზი გაუსვეს სხვადასხვა პლატფორმის გამოყენების მნიშვნელობას. მათი აზრით, აუცილებელია, რომ კამპანია არ იყოს შეზღუდული მხოლოდ სოციალური მედიით. მიუხედავად იმისა, რომ ონლაინ პლატფორმები კომუნიკაციის მნიშვნელოვანი ინსტრუმენტია, ტრადიციული მედია ჯერ ისევ ფართოდ გამოიყენება, განსაკუთრებით ისეთი დაუცველი ჯგუფების მიერ, როგორიცაა ხანდაზმულები. მრავალფეროვანი პლატფორმების გამოყენების გარეშე, მაღალია იმის რისკი, რომ კამპანია ხმას ვერ მიაწვდენს ძირითად სამიზნე ჯგუფებს.

- **„ერთიანი საზოგადოებრივი/whole-of-society“ მიდგომის გამოყენება დაგეგმვისა და განხორციელების პროცესში.** ცნობიერების ამაღლების კამპანიაში ჩართულები უნდა იყვნენ სხვადასხვა დაინტერესებული მხარეები და აქტორები როგორც საჯარო, ასევე კერძო და სამოქალაქო სექტორიდან, მათ შორის, არასამთავრობო ორგანიზაციები, სამოქალაქო საზოგადოების ორგანიზაციები, მედია და საერთაშორისო პარტნიორები. ძალზე მნიშვნელოვანია, მაგალითად, კერძო სათამაშო ბიზნესკომპანიების ჩართულობა იმ ფონზე, როდესაც ხშირია არალეგალური ონლაინ საბანკო გადარიცხვები გატეხილი ონლაინ აზარტული თამაშების ანგარიშების მეშვეობით (იხ. „კიბერდანაშაულების მიერ წარმოქმნილი გავრცელებული საფრთხეები“). კომერციულ ბანკებსაც ეძლევათ უნიკალური შესაძლებლობა, წვლილი შეიტანონ ცნობიერების ამაღლებაში. ერთ-ერთმა რესპონდენტმა - მთავრობის ყოფილმა წარმომადგენელმა მაგალითად მოიყვანა ონლაინ ბანკის ერთ-ერთ პორტალზე გამოქვეყნებული გზამკვლევი სახელწოდებით „რა არის „ფიშინგი“? კიდევ ერთმა რესპონდენტმა საჯარო სექტორში მუშაობის გამოცდილებით ხაზი გაუსვა „ფიშინგის“ გავრცელებულ შემთხვევებს 2021 წელს და აღნიშნა, რომ აუცილებელია პროფესიული ასოციაციების მათსავე სფეროში ცნობიერების გაზრდის მცდელობების მხარდაჭერა.

II. ვიქტიმიზაცია: საფრთხეები და ზიანი

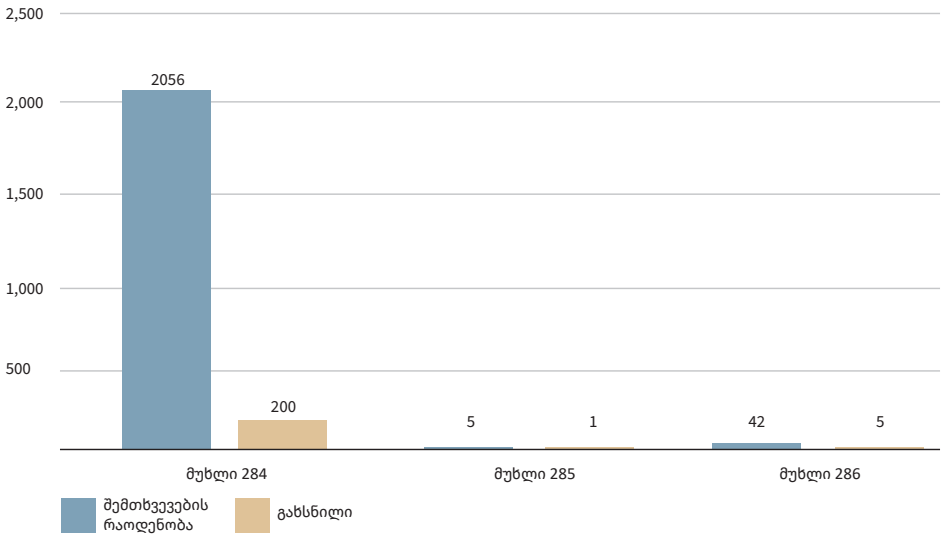
წინამდებარე თავში გაანალიზებულია საქართველოში კიბერდანაშაულების შედეგად ვიქტიმიზაციის მდგომარეობა ნახევრადსტრუქტურირებულ ინტერვიუებზე, ფოკუსჯგუფების განხილვებზე და ვალიდაციის სამუშაო შეხვედრის შედეგად შეგროვებული ინფორმაციაზე და საქართველოს შინაგან საქმეთა სამინისტროს მიერ მოწოდებული სტატისტიკურ მონაცემებზე დაყრდნობით. ამავე თავში განხილულია ის ინსტრუმენტები და ტაქტიკა, რომლებსაც კიბერდამნაშავეები იყენებენ მსხვერპლების წინააღმდეგ. პირველი ნაწილი ეხება შინაგან საქმეთა სამინისტროს ანგარიშს კიბერდანაშაულთან დაკავშირებით და ამ მონაცემების შედარებას კვლევის ფარგლებში მოპოვებულ პირველად მონაცემებთან. მეორე და მესამე ნაწილები მიმოიხილავს ყველაზე მეტად მოწყვლადი ჯგუფების დაუცველობის ფაქტორებს. განსაკუთრებული ყურადღება ეთმობა ქალებს, ბავშვებს, ჟურნალისტებს, ეთნიკური უმცირესობების წარმომადგენლებსა და მცირე და საშუალო ბიზნესს.

ვითარება კიბერდანაშაულის კუთხით

შინაგან საქმეთა სამინისტროს მიერ მოწოდებული ინფორმაციის თანახმად, საქართველოში, 2020-2021 წლებში კიბერდანაშაულის 3.257 შემთხვევა დაფიქსირდა. აქედან, 2.143 შემთხვევა 2020 წელს მოხდა, ხოლო 1.114 – 2021-ში. ამ მონაცემების მიხედვით ირკვევა, რომ 2020-დან 2021-მდე პერიოდში შეტყობინებული კიბერდანაშაულების მაჩვენებელი თითქმის განახევრდა. ამის პარალელურად, თითქმის გაორმაგდა გახსნილი დანაშაულების მაჩვენებელი, რაც 2020 წელს 9.6%-ს შეადგენდა, ხოლო 2021 წელს - 19.7%-ს. თუმცა, რიცხობრივად გახსნილი შემთხვევების მაჩვენებელი მხოლოდ 13-ით გაიზარდა: 206-დან 209-მდე.[58]

58. შინაგან საქმეთა სამინისტრო, „2020-2021 წლებში აღრიცხული კიბერდანაშაულთა მიმოხილვა“, გვ. 3.

სურათი 4: შინაგან საქმეთა სამინისტროს მიერ აღრიცხული კიბერდანაშაულთა სტატისტიკა მუხლების მიხედვით, 2020

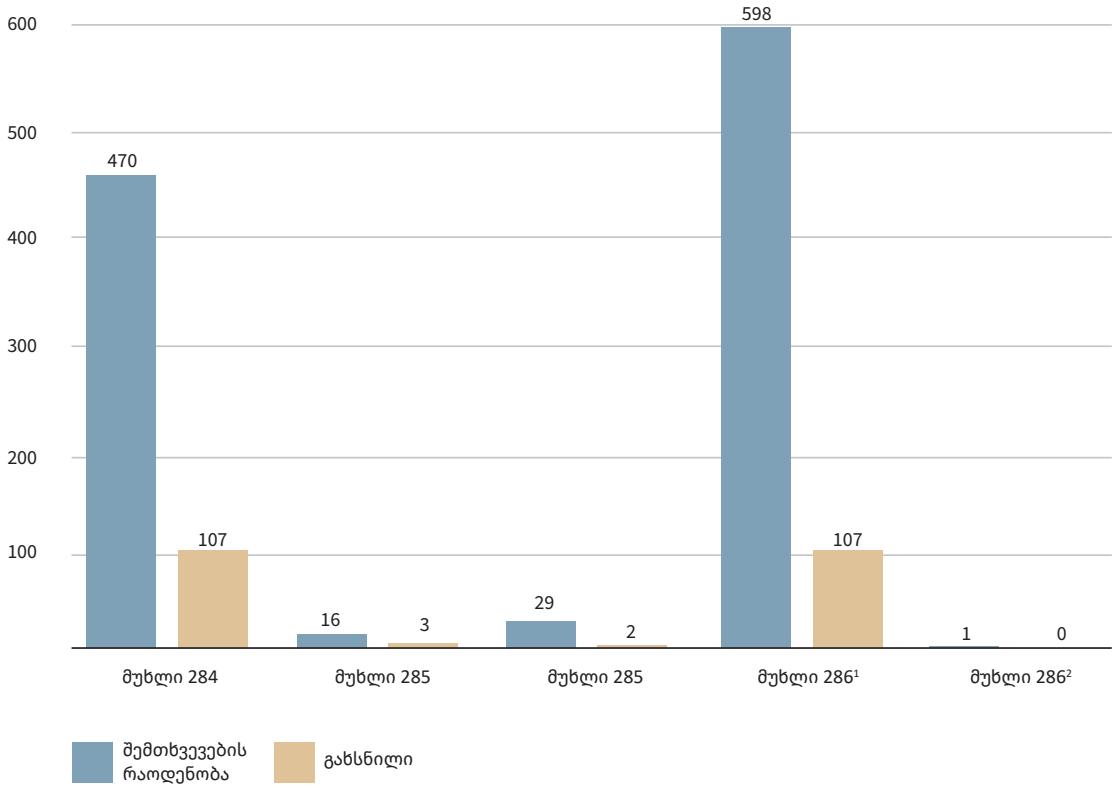


წყარო: შინაგან საქმეთა სამინისტრო, „2020-2021 წლებში აღრიცხული კიბერდანაშაულთა მიმოხილვა“. საინფორმაციო-ანალიტიკური დეპარტამენტი, 1 სექტემბერი 2022 (ინფორმაცია არ არის საჯაროდ ხელმისაწვდომი), გვ. 3.

2020 წლის მონაცემები შეიცავს 284-ე მუხლით გათვალისწინებულ დანაშაულებს (კომპიუტერულ სისტემაში უნებართვოდ შეღწევა), რომელიც შინაგან საქმეთა სამინისტროს მიერ დაფიქსირებული ყველაზე გავრცელებული დანაშაულია (98%). რაც შეეხება 285-ე და 286-ე მუხლებით გათვალისწინებულ დანაშაულებს (კომპიუტერული მონაცემების ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება; კომპიუტერული მონაცემების ან/და კომპიუტერული სისტემის ხელყოფა), ისინი მხოლოდ დაფიქსირებული შემთხვევების 0.2% და 1.9%-ს შეადგენს.[59]

59. იქვე., გვ. 3–4

სურათი 5: შინაგან საქმეთა სამინისტროს მიერ აღრიცხული კიბერდანაშაულთა სტატისტიკა მუხლების მიხედვით, 2021



წყარო: შინაგან საქმეთა სამინისტრო, „2020-2021 წლებში აღრიცხული კიბერდანაშაულთა მიმოხილვა“.

2021 წლამდე ფინანსურად მოტივირებული დანაშაულები, რომლებიც გულისხმობდა კომპიუტერული მონაცემების ან სისტემების ბოროტად გამოყენებას, სისხლის სამართლის კოდექსის 284-ე და 177-ე მუხლებით (ქურდობა) რეგულირდებოდა. 2021 წელს განხორციელებული რეფორმების შედეგად, კოდექსში გაჩნდა ახალი - 286[1] მუხლი, „კომპიუტერული მონაცემების ან/და კომპიუტერული სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით“, რომელზეც ამჟამად მოდის კიბერდანაშაულთა უდიდესი წილი (54%). ამ დამატების შედეგად, კიბერდანაშაულთა საერთო სტატისტიკაში 96%-დან 42%-მდე შემცირდა 284-ე მუხლით გათვალისწინებული დანაშაულთა მაჩვენებელი.[60] მონაცემების შედეგად ირკვევა, რომ საქართველოში ფინანსური სარგებელი კიბერდამნაშავეთა მთავარი მოტივაციაა.

შინაგან საქმეთა სამინისტროს მიერ მოწოდებული ინფორმაცია სეგრეგირებულია მსხვერპლთა ასაკის, სქესის, განათლების დონის, დასაქმების სტატუსის და რეგიონების მიხედვით. მონაცემები მიუთითებს, რომ კიბერდანაშაულთა უდიდესი ნაწილი თბილისში ხდება (55.8% - 2020, 46% - 2021). ეს გარემოება მიუთითებს, რომ კიბერდანაშაულის შესახებ ცნობიერების დონე როგორც მსხვერპლებში, ისე პოლიციის თანამშრომლებში დედაქალაქში შედარებით მაღალია (იხ. „ინფორმირებულობა კიბერდანაშაულის შესახებ“). ეთნიკური უმცირესობებით კომპაქტურად დასახლებული რეგიონები - ქვემო ქართლი და სამცხე-ჯავახეთი, სადაც, ეთნიკური უმცირესობების ფოკუსჯგუფის მონაწილეების აზრით, მოსახლეობა მეტად მოწყვლადია კიბერდანაშაულების მიმართ (იხ. ქვემოთ), შინაგან საქმეთა სამინისტროს მონაცემებში ვიქტიმიზაციის მაღალი მაჩვენებლით არ გამოირჩევიან. 2020 წელს ქვემო ქართლის რეგიონზე მსხვერპლების მხოლოდ 4.5% მოდიოდა, ხოლო სამცხე-ჯავახეთში - 1.9%. 2021 წელს კიბერდანაშაულთა განაწილება რეგიონულ ჭრილში მნიშვნელოვნად არ განსხვავდებოდა 2020 წლის სურათისგან: კიბერდანაშაულთა 1.214 მსხვერპლიდან მხოლოდ 3.2% აღირიცხა ქვემო ქართლში, ხოლო სამცხე-ჯავახეთში - 2.1%.[61]

შინაგან საქმეთა სამინისტროს მონაცემების მიხედვით, როგორც 2020, ასევე 2021 წელს კიბერდანაშაულის შესახებ შეტყობინებას უფრო მეტი კაცი აკეთებდა, ვიდრე - ქალი. რაც შეეხება მსხვერპლების ასაკობრივ განაწილებას, 25-35 წლამდე ასაკობრივ კატეგორიაში შემავალი ადამიანები ყველაზე ხშირად ხდებოდნენ კიბერდანაშაულის სამიზნეები. მსხვერპლთა მეორე ყველაზე დიდი ჯგუფი 35-45 წლამდე ასაკობრივ კატეგორიას მიეკუთვნება. სამართალდამცავებმა ყველაზე ნაკლები მიმართვიანობა 0-14 და 14-17 წლამდე ასაკის პირებისგან მიიღეს.[62] შსს-ს მონაცემების მიხედვით, ქალები და ბავშვები ნაკლებად ხდებიან კიბერდამნაშავეების სამიზნეები. ამის ძირითადი მიზეზი შეიძლება იყოს ის ფაქტი, რომ შინაგან საქმეთა სამინისტროს მიერ მოწოდებული ინფორმაცია მხოლოდ იმ ქმედებებს ეხება, რომლებიც კიბერდანაშაულად კვალიფიცირდება

60. იქვე
61. იქვე, გვ. 3–7.
62. იქვე, გვ. 6, 9.

სისხლის სამართლის კოდექსით. როგორც ზემოთ აღინიშნა, საქართველოს სისხლის სამართლის კოდექსის მიხედვით, „კიბერდანაშაულის“ კატეგორიაში შემავალი ყველა დანაშაულებრივი ქმედება კლასიკური კიბერდანაშაულია, ხოლო კიბერ მეთოდით ჩადენილი დანაშაულები და დამაზიანებელი ონლაინ აქტივობები, რომელთა სამიზნეც ყველაზე ხშირად ბავშვები და ქალები ხდებიან, კიბერდანაშაულის განსაზღვრების მიღმა რჩება. შესაბამისად, ის ქმედებები, რომლებსაც კვლევის მონაწილეები ინტუიციურად უკავშირებენ კიბერდანაშაულს, როგორიცაა, მაგალითად, კიბერშევიწროება, კიბერადევნება, კიბერთაღლითობა და პირადი ინფორმაციის გაჟონვა, არ აისახება ოფიციალურ სტატისტიკაში.

შინაგან საქმეთა სამინისტროს მონაცემებისა და კვლევის დროს შეგროვებული პირველადი მონაცემების შედარებითი ანალიზი უჩვენებს, რომ ფართო საზოგადოებაში მიღებული კიბერდანაშაულის განსაზღვრება განსხვავდება იმისგან, თუ როგორ განმარტავს მოქმედი საკანონმდებლო ჩარჩო კიბერდანაშაულებს. როგორც ფოკუსჯგუფში განხილვებისას, ასევე ინტერვიუების რესპონდენტებმა, კიბერდანაშაულების შესახებ მსჯელობისას აღნიშნეს, რომ კიბერ მეთოდით ჩადენილი დანაშაულები და ზიანის შემცველი ონლაინ ქმედებები კიბერდანაშაულებში ერთიანდება. ბავშვებისა და მათი მშობლების წინაშე მდგომი კიბერრისკების შესახებ მსჯელობისას, ერთ-ერთმა მშობელმა, რომელიც ვალიდაციის სამუშაო შეხვედრაში მონაწილეობდა, ასე განმარტა კიბერსაფრთხე: „საშიში ურთიერთობები, კიბერბულინგი, ფინანსური მაქინაციები და დეზინფორმაცია“.[63] ეს პასუხი აერთიანებს როგორც კლასიკურ კიბერდანაშაულს, ასევე კიბერ მეთოდით ჩადენილ დანაშაულებს და დამაზიანებელ ონლაინ აქტივობებს, განსაკუთრებით, კი კიბერბულინგს. მსგავს დამოკიდებულებას იზიარებდნენ კვლევაში მონაწილე სხვა მშობლებიც.

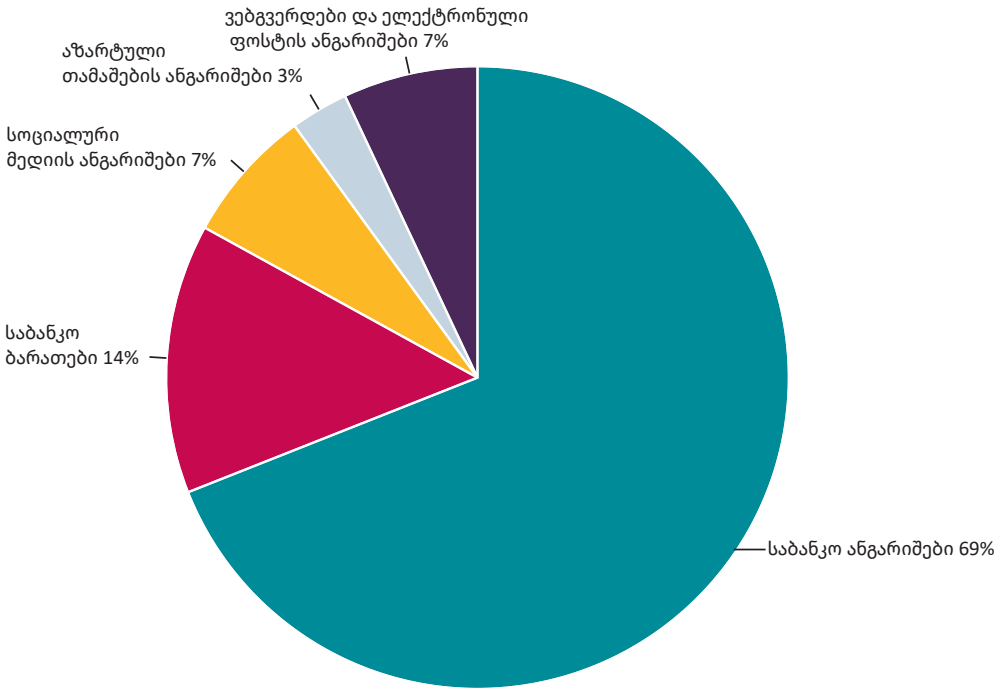
ასევე, პასუხად კითხვაზე „რა გაწუხებთ ყველაზე მეტად, როდესაც საქმე კიბერდანაშაულს ეხება?“, ვალიდაციის სამუშაო შეხვედრის მონაწილე მასწავლებლებმა, ბავშვების წინაშე მდგარ კიბერრისკებზე საუბრისას, კიბერადევნებასა და კიბერბულინგთან ერთად, დაასახელეს კლასიკურ კიბერდანაშაულში შემავალი ფინანსური თაღლითობაც.[64] მონაწილეებმა, რომლებიც სამოქალაქო სექტორსა და ჟურნალისტების ჯგუფს წარმოადგენდნენ, ასევე ერთი ქოლგის ქვეშ მოაქციეს დამაზიანებელი ონალაინ აქტივობები, კლასიკური კიბერდანაშაული და კიბერ მეთოდით ჩადენილი დანაშაულები და გააერთიანეს საფრთხედ, რომელიც განსაკუთრებით ქალებსა და ბავშვებს ემუქრება. ქალების ფოკუსჯგუფის მონაწილეებმა ხაზი გაუსვეს ონლაინბულინგს, პირადი ინფორმაციის გაჟონვასა და შანტაჟს ყოფილი პარტნიორების მხრიდან, როგორც ყველაზე დიდ საფრთხეებს, როდესაც საქმე კიბერდანაშაულებს ეხება.

63. ვალიდაციის სამუშაო შეხვედრა, თბილისი, 22 დეკემბერი 2022.
64. იქვე.

კიბერდანაშაულისგან მომდინარე ძირითადი საფრთხეები

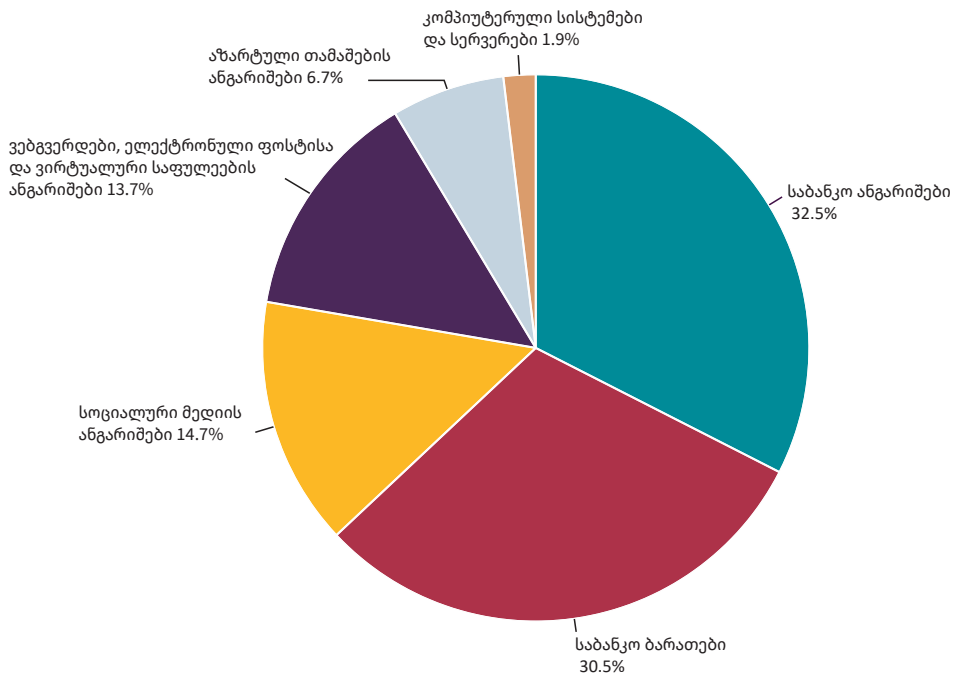
2020-2021 წლებში, შინაგან საქმეთა სამინისტრომ საბანკო ანგარიშები და ბარათები, სოციალური მედია და აზარტული თამაშების ანგარიშები კიბერდანაშაულის ძირითად სამიზნეებად მიიჩნია (იხ. სურათები 6 და 7).

სურათი 6: კიბერდანაშაულის სამიზნეები, 2020



წყარო: შინაგან საქმეთა სამინისტრო, „2020-2021 წლებში აღრიცხული კიბერდანაშაულთა მიმოხილვა“. გვ. 4.

სურათი 7: კიბერდანაშაულების სამიზნეები, 2021



წყარო: შინაგან საქმეთა სამინისტრო, „2020-2021 წლებში აღრიცხული კიბერდანაშაულთა მიმოხილვა“. გვ. 4.

2020 წელს, საბანკო ანგარიშებში უნებართვო შეღწევამ, ძირითადად, აზარტული თამაშების მიზნით, კიბერდანაშაულთა სტატისტიკაში ყველაზე დიდი წილი დაიკავა (76%).[65] ამ შემთხვევებში, მსხვერპლებს საბანკო ბარათები აზარტული თამაშების ვებგვერდებთან ჰქონდათ მიბმული. კიბერკრიმინალებმა გატეხეს მათი ანგარიშები მსხვერპლების პირადი ინფორმაციის მოპარვისა და უნებართვო ტრანზაქციების განხორციელების მიზნით. ასევე ხშირი იყო ე.წ. „ფიშინგის“ შემთხვევები, რაც, ძირითადად გულისხმობს ბმულების გაზიარებას სოციალურ ქსელებში (Facebook, Instagram) და მოპარული/ნაპოვნი საბანკო ბარათების მაღაზიებში შესყიდვების განსახორციელებლად გამოყენების ფაქტები. უფრო მეტიც, გაიზარდა უკონტაქტო ბანკომატებიდან თანხების უნებართვო მოხსნის შემთხვევების სტატისტიკაც. სოციალურ ქსელებს რაც შეეხება, ჩვეულებრივ პრაქტიკად იქცა მომხმარებლების პირადი ანგარიშების გატეხა და შემდგომ ამ ანგარიშების გამოყენება მსხვერპლის პირადი ინფორმაციის მოპოვებისა და მსხვერპლების მეგობრებისა და ოჯახის წევრებისგან თაღლითური გზებით საბანკო მონაცემების მიღების მიზნით.

2021 წელს მნიშვნელოვნად შემცირდა აზარტული თამაშების მიზნით საბანკო ანგარიშების უკანონოდ გამოყენების შემთხვევები. შინაგან საქმეთა სამინისტროს მიერ მოწოდებული ინფორმაციით, სტატისტიკის გაუმჯობესება გამოიწვია სამინისტროსა და კერძო სექტორს შორის თანამშრომლობამ, რომელმაც, თავის

65. შინაგან საქმეთა სამინისტრო, ‘2020-2021 წლებში აღრიცხული კიბერდანაშაულთა მიმოხილვა“, გვ. 4.

მხრივ, ხელი შეუწყო ბანკებისა და აზარტული თამაშების ანგარიშების დაცვის გაუმჯობესებული მექანიზმების ამოქმედებას. 2021 წელს გავრცელებულ კიბერდანაშაულებში აღირიცხა Facebook-ის ანგარიშების თაღლითური გამოყენების შემთხვევები, რომლებიც გულისხმობს დამნაშავეების მიერ მსხვერპლის მეგობრებისგან საბანკო ინფორმაციის ან ფინანსური დახმარების მიღებას, „ფიშინგს“ - არარსებული სესხების შეთავაზება ან მაღაზიების ყალბი ვებგვერდების გამოყენება მსხვერპლებისგან საბანკო ინფორმაციის მიღების მიზნით, ასევე საბანკო ბარათების უკანონო გამოყენებას. მიუხედავად 2021 წელს დაფიქსირებული კლებისა, მსხვერპლებისთვის მიყენებული ზარალი მნიშვნელოვნად გაიზარდა 2020 წელს დაფიქსირებული 3.9 მილიონი ლარიდან 8.9 მილიონ ლარამდე.[66]

კიბერდანაშაულის გავრცელებული ზემოხსენებული საფრთხეების გარდა, პირველადი მონაცემების შეგროვების პროცესში გამოიკვეთა კიდევ ერთი ზოგადი გამოწვევა: საზოგადოებაში კიბერდანაშაულის მიმართ დაბალი ინტერესი, რაც გამოწვეულია პოტენციური კიბერსაფრთხეების შესახებ ცნობიერების დაბალი დონით. ამ საკითხს განსაკუთრებულად გაუსვა ხაზი ერთ-ერთმა რესპონდენტმა, რომელმაც კიბერცნობიერების დონე, მეტადრე უსაფრთხოების ისეთი საბაზისო კომპონენტი, როგორიცაა პაროლების მართვა, დაახასიათა, როგორც „ძალზე, ძალზე დაბალი“.[67] ეს პრობლემა კარგად აღწერა ქალების ფოკუსჯგუფის ერთ-ერთმა მონაწილემ, რომელმაც განაცხადა, რომ რადგანაც სოფელში მას იცნობენ როგორც IT უნარების მქონეს, მეზობლები ხშირად სთხოვენ დახმარებას სოციალური ქსელის ანგარიშის ან სულაც ონლაინ ბანკის პაროლის შესაცვლელად.

ფოკუსჯგუფებისა და ვალიდაციის სამუშაო შეხვედრის მონაწილეებს შორის კიბერცნობერებისა და კიბერჰიგიენის დაბალ დონეზე მიუთითებს მათ მიერ ხშირად გამოხატული ისეთი სენტიმენტები, როგორიცაა „ეს მე არ მეხება“ ან „ეს მე არ მემუქრება“. მშობლების, მეურვეებისა და მასწავლებლების ფოკუსჯგუფის ერთ-ერთმა მონაწილემ განაცხადა, რომ ნაკლებად სავარაუდოა, კიბერკრიმინალებმა მიზანში ამოიღონ, ვინაიდან მისი ფინანსური მდგომარეობა მაინცდამაინც სახარბიელო არ არის. მსგავსი მოსაზრება გამოთქვა კიდევ ერთმა მონაწილემ მცირე და საშუალო მეწარმეების ჯგუფიდან. მისი აზრით, ადგილობრივი საშუალო ზომის კომპანიები ნაკლებად იქცევენ კიბერკრიმინალების ყურადღებას, რომლებიც მაღალშემოსავლიან მსხვერპლებს უფრო ირჩევენ. კვლევის ფარგლებში გამოკითხულმა ექსპერტმა განაცხადა, რომ ადამიანები ხშირად მას შემდეგ იწყებენ კიბერუსაფრთხოებაზე ზრუნვას, რაც კიბერდანაშაულის მსხვერპლები ხდებიან.[68]

66. იქვე, გვ. 5.
67. ინტერვიუ სსო-ს მაღალი რანგის წარმომადგენელთან, თბილისი, 6 ოქტომბერი 2022.
68. ინტერვიუ მთავრობის ყოფილ მაღალჩინოსან მოხელესთან ციფრული პლატფორმის მეშვეობით, 18 ოქტომბერი 2022.

კიბერმოწყვლადობის ხარისხი სხვადასხვა ჯგუფში

პირველადი მონაცემების ანალიზის მიხედვით ირკვევა, რომ კიბერდანაშაულების მიმართვიანობის სტატისტიკაში, როგორც ზემოთ ითქვა, არ ხვდება კიბერ მეთოდით ჩადენილი დანაშაულები ან ზიანის შემცველი ონლაინ აქტივობების მრავალფეროვანი სპექტრი. ეს თვალსაჩინო ხდება კონკრეტული ჯგუფების - განსაკუთრებით, ქალების, ბავშვებისა და ჟურნალისტების გამოცდილებაზე დაკვირვებისას. მონაწილეებთან განხილვისას კიბერ მეთოდით ჩადენილი დანაშაულების ხსენების სიხშირე ნათლად მიუთითებს იმ განსხვავებაზე, რომელიც არსებობს ფართო საზოგადოების მიერ კიბერდანაშაულის აღქმასა და კიბერდანაშაულის ოფიციალურ გაგებას შორის.

ქალები

ქალების ფოკუსჯგუფის 12 მონაწილიდან ცხრამ განაცხადა, რომ ქალებს უფრო ემუქრებათ კიბერდანაშაული - მისი ფართო გაგებით, რომელიც კლასიკურ კიბერდანაშაულთან ერთად მოიცავს კიბერ მეთოდით ჩადენილი დანაშაულისა და საფრთხის შემცველი ონლაინ აქტივობების რისკებს. გარდა ამისა, ქალები განსაკუთრებით მოწყვლადები არიან კონკრეტული კიბერ მეთოდით ჩადენილი დანაშაულებისა და საფრთხის შემცველი ისეთი ონლაინ ქმედებების მიმართ, როგორიცაა, მაგალითად, პერსონალური მონაცემების უნებართვოდ გავრცელება, კიბერშევიწროვება მოქმედი ან ყოფილი პარტნიორების მხრიდან და კიბერბულინგი.[69] ვალიდაციის სამუშაო შეხვედრაში მონაწილე სამოქალაქო საზოგადოების წარმომადგენლები და ჟურნალისტები ამტკიცებდნენ, რომ ზემოხსენებული ჯგუფების განსაკუთრებული მოწყვლადობა განპირობებულია სოციალური და კულტურული ფაქტორებით: ქართული საზოგადოება ჯერ კიდევ კონსერვატიულია და ქალები ხშირად ხდებიან საჯარო შერცხვენის საგანი, მაგალითად, პირადი მონაცემების უკანონო გავრცელების შედეგად.[70] აქედან გამომდინარე, დამნაშავეები ამ ტაქტიკას ქალების წინააღმდეგ ხშირად იყენებენ. ვალიდაციის სამუშაო შეხვედრის ერთ-ერთმა მონაწილემ ამ მოსაზრების დასადასტურებლად განაცხადა, რომ პირადი ინფორმაციის გავრცელებას მამაკაცების წინააღმდეგ ნაკლებად მიმართავენ, რადგან მაშინაც კი, თუ ამგვარი

69. ქალების ფოკუსჯგუფი, თბილისი, 4 ოქტომბერი 2022.
70. თუმცა, მნიშვნელოვანია აღინიშნოს, რომ საქართველო, ამ მხრივ, არ არის ერთადერთი გამონაკლისი. ლიტერატურა ნათლად მიუთითებს ამ ტენდენციის არსებობის შესახებ სხვა ქვეყნებშიც. იხილეთ, მაგალითისთვის, Tim Owen, Wayne Noble and Faye Christabel Speed, *New Perspectives on Cybercrime* [ახალი პერსპექტივები კიბერდანაშაულის შესახებ] (London: Palgrave Macmillan, 2017), გვ. 141–58; Nicola Henry and Anastasia Powell, 'Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence' [ჩანერგილი ზიანი: გენდერი, სირცხვილი და სექსუალური ძალადობა ტექნოლოგიების მეშვეობით], ძალადობა ქალების წინააღმდეგ (ტომი. 21, #. 6, 2015), გვ. 758–79.

ფაქტი მოხდა, კაცების წინააღმდეგ ნაკლებად გორდება შერცხვენის კამპანია პირადი ინფორმაციის გამჟღავნების შედეგად.[71]

ქალები ასევე ხშირად ხდებიან კიბერბულინგის სამიზნეები. ერთ-ერთმა ინტერვიუერმა აღნიშნა, რომ კიბერბულინგს განსაკუთრებით ხშირად ქალი პოლიტიკოსების წინააღმდეგ მიმართავენ.[72] როგორც მმართველი, ასევე ოპოზიციური პარტიების წარმომადგენელი ქალები ხშირად ხდებიან კიბერბულინგის სამიზნეები. თუმცა, თავდასხმები უფრო ხშირად ოპოზიციის ლიდერი ქალებისკენაა მიმართული. ქალების ფოკუსჯგუფის ერთ-ერთმა მონაწილემ განაცხადა, რომ კიბერბულინგთან დაკავშირებული ყველაზე შემაშფოთებელი ფაქტორი ისაა, რომ მისი აზრით, მსხვერპლების 99%-ს ქალები ან ბავშვები შეადგენენ.

ვალიდაციის მონაწილე სამოქალაქო საზოგადოების წარმომადგენლებმა და ჟურნალისტებმა რამდენიმე კონკრეტული გამოწვევა დაასახელეს, რომლებთან გამკლავებაც კიბერდანაშაულის და დამაზიანებელი ონლაინ აქტივობების მსხვერპლებს უწევთ:

- ცნობიერების დაბალი დონე საკუთარი უფლებების შესახებ. მსხვერპლები ხშირად ადანაშაულებენ საკუთარ თავს და არ იციან, რომ დანაშაულის შედეგად მათი უფლებები ილახება და რომ მათ შეუძლიათ სამართალდამცავ ორგანოებს შეატყობინონ მომხდარის შესახებ.
- ინფორმაციის ნაკლებობა იმის შესახებ, თუ ვის შეიძლება მიმართონ დახმარებისთვის. უმეტეს შემთხვევებში, ქალებმა არ იციან, რომ არსებობს სპეციალური საგამოძიებო სამსახური, დამოუკიდებელი საგამოძიებო ორგანო, რომელსაც შეუძლიათ მიმართონ თუ მათი პირადი ინფორმაცია უკანონოდ გავრცელდა.
- ცოდნის ნაკლებობა კიბერძალადობის მტკიცებულებების შენახვის შესახებ. მსხვერპლებმა ხშირად არ იციან, თუ როგორ მოეპყრონ პირადი მონაცემების გაჟონვის მტკიცებულებებს. თუ დამნაშავეები წაშლიან მასალას, რომელიც უკანონოდ გაავრცელეს, დანაშაულის გამოძიება მნიშვნელოვნად რთულდება.[73]

ბავშვები

მშობლების, მეურვეებისა და მასწავლებლების ფოკუსჯგუფის 10-დან შვიდმა მონაწილემ განაცხადა, რომ ბავშვები უკიდურესად დაუცველები არიან ონლაინ სივრცეში, ხოლო დანარჩენმა სამმა მონაწილემ დაუცველობის ხარისხი შეაფასა, როგორც საშუალო. ინტერვიუების მონაწილეებმაც გაიზიარეს ეს მოსაზრება. ერთმა რესპონდენტმა აღნიშნა, რომ ბავშვები ერთ-ერთი ყველაზე დაუცველი ჯგუფია, რადგან ისინი ინტერნეტში „საკმაოდ აქტიურები არიან, ხოლო მათი

71. ვალიდაციის სამუშაო შეხვედრა, თბილისი, 22 დეკემბერი 2022.
72. ინტერვიუ ჟურნალისტთან, თბილისი, 3 ოქტომბერი 2022.
73. ვალიდაციის სამუშაო შეხვედრა, თბილისი, 22 დეკემბერი 2022.

ცნობიერების დონე დაბალია“.[74] სხვა რესპონდენტების თქმით, ბავშვებს ხშირად ჰგონიათ, რომ ინტერნეტში რასაც ხედავენ, ყველაფერი სარწმუნოა.[75]

თუმცა, ასევე გამოიკვეთა განსხვავებული მოსაზრებებიც. კვლევის ზოგიერთმა მონაწილემ განაცხადა, რომ ბავშვებში კიბერცნობიერება მშობლებთან ან მასწავლებლებთან შედარებით მაღალია. ერთ-ერთი რესპონდენტი ასევე ამტკიცებდა, რომ გავრცელებული წარმოდგენისგან განსხვავებით, ბავშვები უკეთ ერკვევიან კიბერსაფრთხეებში, რადგან ისინი „ციფრული ეპოქის შვილები“ არიან.[76] ვალიდაციის სამუშაო შეხვედრის მონაწილე რამდენიმე მასწავლებლის თქმით, ისინი, კოლეგებთან ერთად, ხშირად ეკითხებიან რჩევას მოსწავლეებს კიბერუსაფრთხოების საკითხებთან დაკავშირებით. თუმცა, ამ მოსაზრებას მოწინააღმდეგეებიც გამოუჩნდნენ, რომლებიც ამტკიცებდნენ, რომ მათ, ვინც მოსწავლეებს რჩევისთვის მიმართავს, კიბერცნობიერების დაბალი დონე აქვთ და ეს არ უკავშირდება ბავშვების განსაკუთრებულ ცოდნას ამ სფეროში.[77] ვალიდაციის სამუშაო შეხვედრის მონაწილეები, რომლებიც სამოქალაქო საზოგადოებისა და მედია ორგანიზაციებში მუშაობენ, ასევე ფიქრობენ, რომ მართალია, ბავშვებმა იციან, თუ როგორ უნდა მოძებნონ და გამოიყენონ მობილური აპლიკაციები, მაგრამ ეს არ ნიშნავს, რომ ისინი ასევე კარგად ერკვევიან კიბერუსაფრთხოებასა და კიბერჰიგიენაში.[78]

მშობლებმა და მეურვეებმა, რომლებიც პირველადი მონაცემების შეგროვების ეტაპზე მონაწილეობდნენ კვლევაში, ორ ძირითად კატეგორიად დაჰყვეს ბავშვების წინააღმდეგ კიბერძალადობის შემთხვევები: არასრულწლოვანების მიერ ჩადენილი კიბერბულინგი და ზრდასრულების მიერ ჩადენილი ქმედებები, როგორიცაა, ადევნება და პირადი ინფორმაციის გამოძალვა და შანტაჟი. ვალიდაციის სამუშაო შეხვედრის ერთ-ერთმა მონაწილემ გაიხსენა შემთხვევა, როდესაც მამაკაცი მესიჯებს უგზავნიდა 12 წლის გოგონას და შეხვედრას სთხოვდა. გოგონას მშობლების სწრაფი რეაგირების შედეგად, სამართალდამცავებმა შეძლეს დამნაშავის დაკავება.[79] ამ და მსგავსი საკითხების ირგვლივ დისკუსიებისას გამოიკვეთა, რომ ონლაინ საფრთხეების შესახებ სახელმწიფოს მიერ ორგანიზებული საინფორმაციო კამპანიის არარსებობის ფონზე, მშობლების უნარი, დაიცვან საკუთარი შვილები ამგვარი საფრთხეებისგან ორ ფაქტორზეა დამოკიდებული: კიბერსაფრთხეების შესახებ მშობლების ცნობიერების დონე და საკუთარ შვილებთან სიახლოვის ხარისხი, რომელიც გავლენას ახდენს კიბერსაფრთხეებისა და რისკების შესახებ კომუნიკაციის ეფექტიანობაზე შვილსა და მშობელს შორის. მშობლები თანხმდებიან, რომ უმეტეს შემთხვევებში, ეს ორი ფაქტორი ერთად არ არის ხოლმე წარმოდგენილი.

74. ინტერვიუ მთავრობის ოფიციალურ პირთან, თბილისი, 4 ოქტომბერი 2022.
75. ინტერვიუ სსო-ს ხელმძღვანელსა და მაღალი რანგის წარმომადგენელთან, თბილისი, 3 ოქტომბერი 2022.
76. ინტერვიუ სსო-ს მაღალი რანგის წარმომადგენელთან, თბილისი, 6 ოქტომბერი 2022.
77. ვალიდაციის სამუშაო შეხვედრა, თბილისი, 22 დეკემბერი 2022.
78. იქვე.
79. იქვე.

ჟურნალისტები

ჟურნალისტების ფოკუსჯგუფის შედეგებით ირკვევა, რომ ყველა მონაწილე საკუთარ პროფესიას რისკფაქტორად მიიჩნევს, როდესაც საქმე კიბერდანაშაულებს ეხება. ათიდან შვიდმა მონაწილემ განაცხადა, რომ ისინი უკვე გახდნენ კიბერდანაშაულის მსხვერპლები. პასუხად კითხვაზე „დარწმუნებულები ხართ თუ არა, რომ შეგიძლიათ დაიცვათ ინფორმაცია, როდესაც იყენებთ ინტერნეტსა და სოციალურ მედიას?, ჟურნალისტების ფოკუსჯგუფის ყველა მონაწილემ განაცხადა, რომ ისინი ან საშუალოდ დარწმუნებულები არიან ან - საერთოდ არა.[80]

ჟურნალისტებს, ზოგადად, აწუხებთ „უკანონო და ფარული მიყურადება უსაფრთხოების სამსახურების მიერ“. მათი აზრით, კიბერდანაშაულის უმთავრესი საფრთხე სწორედ მათი პირადი ინფორმაციის შესაძლო გაჟონვიდან მომდინარეობს. [81] ჟურნალისტების ფოკუსჯგუფის ერთ-ერთი მონაწილის თქმით, ის და მისი კოლეგები ამ რისკს იმდენად სერიოზულად აღიქვამენ, რომ სისტემატურად იღებენ ზომებს მის გასანეიტრალებლად. ასევე უნდა აღინიშნოს, რომ კვლევის რამდენიმე მონაწილემ - ინტერვიუებისა და ფოკუსჯგუფების რესპონდენტებმა, გამოთქვეს შეშფოთება იმასთან დაკავშირებით, რომ ინფორმაციული უსაფრთხოების შესახებ კანონის საფუძველზე[82] უსაფრთხოების სამსახურებს, შესაძლოა, უფრო ფართო უფლებამოსილება მინიჭებოდათ მიყურადებასა და თვალთვალთან დაკავშირებით, რაც კიდევ უფრო სერიოზული რისკის ქვეშ დააყენებდა ჟურნალისტებს (იხილეთ „ნდობა“). თუმცა, ასევე უნდა აღინიშნოს, რომ უსაფრთხოების სამსახურებს ამ კანონის მიღებამდეც გააჩნდათ ტექნიკური თვალთვალის უფლებამოსილება. მაგალითად, ელექტრონული კომუნიკაციების შესახებ კანონში 2013-2014 წლებში შესული ცვლილებების შედეგად, უსაფრთხოების სამსახურებს მიენიჭათ „ფარული საგამოძიებო საქმიანობის“ განხორციელების უფლება.[83]

ეთნიკური უმცირესობები

ეთნიკური უმცირესობების ფოკუსჯგუფის შედეგების მიხედვით, როდესაც საქმე კიბერრესურსებზე წვდომას ეხება, ეთნიკურად სომეხი და აზერბაიჯანელი მოქალაქეების წინაშე მდგარი უმთავრესი გამოწვევა ენობრივი ბარიერია. ქართული ენის არასათანადოდ ფლობა სერიოზულ დაბრკოლებას წარმოადგენს ნებისმიერი ტიპის ინფორმაციის - მათ შორის, კიბერჰიგიენის შესახებ ინფორმაციის

80. ჟურნალისტების ფოკუსჯგუფი, თბილისი, 6 ოქტომბერი 2022.
81. იქვე.; ინტერვიუ ჟურნალისტთან, თბილისი, 3 ოქტომბერი 2022.
82. საქართველოს მთავრობა, საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, 6391-Iს, < https://matsne.gov.ge/ka/document/view/1679424?publication=7>, ბოლოს ნანახია: 30 მაისი 2023.
83. საქართველოს მთავრობა, საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ, 1514, მუხლი 8, < https://matsne.gov.ge/ka/document/view/29620?publication=46>, ბოლოს ნანახია: 30 მაისი 2023.

მიღებისას. ეთნიკური უმცირესობების ფოკუსჯგუფის 11 მონაწილიდან ცხრამ განაცხადა, რომ მათი ეთნიკური წარმომავლობა ხელს უშლით მიიღონ ინფორმაცია და გამოიყენონ ინსტრუმენტები, რომლებიც უზრუნველყოფდა მათ ონლაინ დაცვას.

კვლევის სხვა მონაწილეების თქმით, როდესაც საქმე კიბერცნობიერებას ეხება, მნიშვნელოვანი განსხვავებები არსებობს ქალაქებსა და სოფლებს შორის (იხ. „პრიორიტეტული სფეროები“). შესაბამისად, სამცხე-ჯავახეთისა და ქვემო ქართლის რეგიონებში მცხოვრები ეთნიკური უმცირესობები ორმაგად მოწყვლადები არიან კიბერსაფრთხეების წინაშე.

მცირე და საშუალო ბიზნესი

მცირე და საშუალო ბიზნესის წარმომადგენლებმა გაიხსენეს მრავალი შემთხვევა, როდესაც მათი კომპანიები კიბერკრიმინალების მსხვერპლები გახდნენ. მათი თქმით, ბიზნესკომპანიების წინააღმდეგ ჩადენილი კიბერდანაშაულის ყველაზე გავრცელებული სახეა კიბერდამნაშავეების მიერ მათი კუთვნილი ინფორმაციის მითვისება და გამოსასყიდის მოთხოვნა. ვალიდაციის სამუშაო შეხვედრის მონაწილეებმა კერძო სექტორიდან აღნიშნეს, რომ ხსენებულ შემთხვევებში დამნაშავეები კომპანიის პაროლებს ტეხდნენ, ხშირად არასათანადო კიბერჰიგიენის შედეგად. ერთ-ერთმა მონაწილემ ახსენა შემთხვევა, როდესაც კომპანიის ყოფილმა თანამშრომელმა შეძლო კოლეგის მარტივი პაროლის გამოცნობა და მისი მეშვეობით კლიენტების და ფასების შესახებ ინფორმაციის მიღება. ამის შემდეგ, ყოფილმა თანამშრომელმა მითვისებული ინფორმაცია სხვა კომპანიების სასარგებლოდ გამოიყენა და ყოფილ სამსახურს კლიენტები წაართვა.[84]

რესპონდენტების აზრით, კიბერდანაშაულის პრევენციული ზომები „მეტისმეტად ძვირია“, განსაკუთრებით მცირე კომპანიებისთვის. ვალიდაციის სამუშაო შეხვედრის ერთ-ერთი მონაწილის თქმით, სერიოზული კიბერინციდენტის შემდეგაც კი, მცირე და საშუალო კომპანიები ამჯობინებენ ხარჯი გაწიონ შედარებით იაფფასიანი მონაცემთა ასლების შემნახველი პროგრამების შეძენისთვის, რომლებიც, ძირითადად, დაშვებული შეცდომის შედეგების გამოსწორებას ემსახურება, ვიდრე იმ ინსტრუმენტების დანერგვისთვის, რომლებიც, პირველ ყოვლისა, სწორედ კიბერდანაშაულის რისკებს პრევენციულად შეამცირებდა და კიბერდამნაშავეებს განზრახვის შესრულებაში ხელს შეუშლიდა. აღსანიშნავია, რომ, ზოგადად, მცირე და საშუალო ბიზნესის წარმომადგენლებს შორის კიბერრისკების აღქმის დონე საკმაოდ დაბალია. ერთ-ერთმა რესპონდენტმა, რომელიც მცირე კომპანიას წარმოადგენდა ვალიდაციის სამუშაო შეხვედრაზე, განაცხადა, რომ მის სამსახურს არ გადაუხდია უფრო მეტი თანხა კიბერუსაფრთხოების ღონისძიებებში, რადგან ამ დრომდე არ დამდგარან

84. ვალიდაციის სამუშაო შეხვედრა, თბილისი, 22 დეკემბერი 2022.

კიბერშეტევის სერიოზული საფრთხის წინაშე.[85] მცირე და საშუალო ბიზნესის ამგვარი დამოკიდებულება მხოლოდ საქართველოში არ შეინიშნება, თუმცა ეს არ ნიშნავს, რომ მთავრობამ არ უნდა გადადგას ქმედითი ნაბიჯები ამ პრობლემის გადასაჭრელად.

85. იქვე.

III. მიმართვიანობა

პირველადი მონაცემების შეგროვების ეტაპზევე მიმართვიანობა საქართველოში კიბერდანაშაულის შესახებ არსებული გამოცდილების ყველაზე მნიშვნელოვან საკითხად გამოიკვეთა. ერთ-ერთი მაღალი რანგის საჯარო მოხელის თქმით, ქვეყანაში 2019 წლიდან შეინიშნება მოქალაქეთა მიერ კიბერდანაშაულის ფაქტების მიმართვიანობის მზარდი ტენდენცია.[86] თუმცა, კვლევის შედეგები ეჭვქვეშ აყენებს ამ მოსაზრებას და მიუთითებს, რომ ჯერ კიდევ მყარია დანაშაულის შეუტყობინებლობის ტენდენცია განსაკუთრებით კონკრეტულ ჯგუფებში. მიმართვიანობის დაბალი მაჩვენებლები გამოწვეულია არსებული მექანიზმების შესახებ ცნობიერების დაბალი დონითა და ასევე, მთავრობისა და სამართალდამცავი ორგანოების მიერ დანაშაულის ეფექტიანად გამოძიების შესაძლებლობის მიმართ ნდობის ნაკლებობით. მნიშვნელოვანია აღინიშნოს, რომ უნდობლობა მთავრობის მიმართ, როდესაც საქმე კიბერდანაშაულის მიმართვიანობასთან მიდის, ეწინააღმდეგება იმ პოზიტიურ განწყობას, რომელსაც მოქალაქეები მთავრობის, როგორც კიბერჰიგიენის შესახებ ცნობიერების ამაღლების კამპანიის წარმმართველის მიმართ ამჟღავნებდნენ (იხ. თავი I). წინამდებარე თავი მიმოიხილავს საქართველოში მოქმედ მიმართვიანობის მექანიზმებსა და მათ გამოყენებასთან დაკავშირებულ პროცესებს, ასევე, პოლიციის შესაძლებლობებისა და მათი საქმიანობის მიმართ მოსახლეობის ნდობას.

მექანიზმები

მიმართვიანობის პროცესი

2012 წლიდან, მას შემდეგ, რაც შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში კიბერდანაშაულთა ბრძოლის სამმართველო შეიქმნა, სამინისტროს შესაძლებლობები კიბერდანაშაულთან ბრძოლის მიმართულებით მნიშვნელოვნად გაძლიერდა. დანაშაულის ანალიზის სამმართველო აანალიზებს კიბერდანაშაულის იმ შემთხვევებს, რომლებიც შინაგან საქმეთა სამინისტროს ელექტრონულ საგამოძიებო პროგრამაში აღირიცხება პოლიციის ცენტრალური და რეგიონული დეპარტამენტების მიერ. აქ იგულისხმება სისხლის სამართლის კოდექსის 35-ე თავით (კიბერდანაშაულები) გათვალისწინებული ის დანაშაულებიც, რომლებიც პირველ ცხრილშია მოცემული.

შინაგან საქმეთა სამინისტრო აღრიცხავს როგორც კლასიკურ კიბერდანაშაულს, ასევე კიბერმეთოდებით ჩადენილ დანაშაულსაც, თუმცა ეს უკანასკნელი არ განიხილება როგორც კიბერდანაშაული. ისეთი მუხლები, როგორიცაა 151[1]

86. ინტერვიუ საჯარო მოხელესთან, თბილისი, 4 ოქტომბერი 2022.

(„ადევნება“) ასევე ითვალისწინებს კიბერფაქტორებს ინფორმაციის მოძიებისა და სამართლებრივი დევნის პროცესში. შინაგან საქმეთა სამინისტროს მიხედვით, ინფორმაციის მთავარი წყარო საგამოძიებო ელექტრონული პროგრამაა, რომელიც გამოიყენება კიბერდანაშაულის შესახებ სისხლის სამართლის საქმეებისთვის მასალების მოძიებისა და მონაცემების აღრიცხვის მიზნით.

ამჟამად, კიბერდანაშაულის მიმართვიანობის შეტყობინების შემდეგი მექანიზმების გამოყენება შეუძლიათ:

1. პოლიციის განყოფილებაში წერილობითი განცხადებით მიმართვა
2. გადაუდებელი დახმარების ნომერზე (112) დარეკვა
3. კიბერდანაშაულის შესახებ ელექტრონული შეტყობინების გაგზავნა ცენტრალური კრიმინალური პოლიციის განყოფილების შესაბამის ელექტრონულ მისამართზე
4. ცენტრალური კრიმინალური პოლიციის ცხელ ხაზზე დარეკვა.

ერთ-ერთი რესპონდენტის თქმით, რომელიც ამჟამად სამთავრობო უწყებაში მუშაობს, ცენტრალური კრიმინალური პოლიციის ცხელი ხაზი დიდად ეფექტიანი მექანიზმი არ არის, რადგან ბევრმა არ იცის მისი არსებობის შესახებ. მოქალაქეების უმეტესობა, ამავე რესპონდენტის თქმით, ამჯობინებს გადაუდებელი დახმარების ცხელ ხაზზე - 112-ზე დარეკვას.[87] მიმართვიანობის არსებული მექანიზმების შესახებ ცოდნის დეფიციტი გაურკვევლობას იწვევს იმ მოქალაქეებს შორისაც კი, რომლებიც უარზე არ არიან შესაბამის უწყებებს კიბერდანაშაულის შესახებ შეატყობინონ. გაურკვევლობის კიდევ ერთი შედეგია ის, რომ მოქალაქეები კიბერდანაშაულის შეტყობინების მიზნით ალტერნატიულ, არაოფიციალურ არხებს, მაგალითად, სოციალურ მედიას იყენებენ. წარსულში ყოფილა შემთხვევები, როდესაც დაზარალებულები დახმარებას მონაცემთა გაცვლის სააგენტოს (ამჟამინდელი ციფრული მმართველობის სააგენტოს წინამორბედი) ოფიციალურ Facebook-ის გვერდზე ითხოვდნენ. ცენტრალური კრიმინალური პოლიციის განყოფილებისკენ გადამისამართების მცდელობას მნიშვნელოვანი პოზიტიური ცვლილებები არ მოჰყოლია.[88]

როდესაც საქმე კერძო სექტორს ეხება, პოლიტიკის დონეზე ბანკების ზედამხედველობა საქართველოს ეროვნული ბანკის პასუხისმგებლობაა, თუმცა, მის მანდატში გათვალისწინებული არ არის ტექნიკური მხარდაჭერის შეთავაზება. მხოლოდ კროტიკული ინფრასტრუქტურის სტატუსის მქონე ბანკებს ევალებათ კიბერდანაშაულის მიმართვიანობა საქართველოს ეროვნული ბანკისთვის. რაც შეეხება კერძო სექტორს, ციფრული მმართველობის სააგენტო ვალდებულია დაეხმაროს კერძო სექტორის სუბიექტებს კიბერსაფრთხეებთან გამკლავებაში. ეს პასუხისმგებლობა ვრცელდება მესამე კატეგორიის კრიტიკული ინფრასტრუქტურის ობიექტებზე, კერძოდ, ბანკებზე, სადაზღვევო კომპანიებზე,

87. იქვე.
88. ინტერვიუ მთავრობის ყოფილ მაღალი რანგის წარმომადგენელთან, თბილისი, 5 ოქტომბერი 2022.

ენერგოკომპანიებზე, საზღვაო პორტებსა და ტერმინალებზე, საქართველოს ავიახაზებსა და გადამზიდ კომპანიებზე. მიუხედავად მიმართვიანობის რამდენიმე მექანიზმისა, თითქმის ყველა რესპონდენტი აღინიშნავს, რომ მსხვერპლები ამ მექანიზმებს იშვიათად იყენებენ, რაც აფერხებს კიბერდანაშაულზე ეფექტიან რეაგირებას. ყოფილმა საჯარო მოხელემ ეს გარემოება მიმართვიანობის მექანიზმების შესახებ ცნობიერების დაბალი დონით და მასთან დაკავშირებული გაურკვევლობით ახსნა.[89] ინტერვიუების შედეგად გამოიკვეთა, რომ ექსპერტების მოსაზრებებიც კი არაერთგვაროვანია, როდესაც საკითხი მიმართვიანობის პროცედურებს, უფრო კონკრეტულად კი, შესაბამისი უწყებების პასუხისმგებლობას ეხება. ერთ-ერთი ექსპერტის მოსაზრებით, ბიზნეს სექტორისა და სამოქალაქო საზოგადოების ორგანიზაციები, რომლებსაც მიმართვიანობის ოფიციალური ვალდებულება არ აკისრიათ, როგორც წესი, არ მიმართავენ პასუხისმგებელ უწყებებს რადგან არ იციან თუ როგორ მუშაობის მიმართვიანობის მექანიზმი და რომელი უწყებას უნდა მიმართონ ამ შემთხვევაში.[90] ინტერვიუების არაერთი რესპონდენტი, ასევე ფოკუსჯგუფებისა და ვალიდაციის სამუშაო შეხვედრის მონაწილე აცხადებს, რომ კიბერდანაშაულის შეუტყობინებლობა უკავშირდება მსხვერპლების დაბალ მოლოდინებს: მათ ნაკლებად სჯერათ, რომ ინციდენტი გამოძიებული იქნება მწირი ადამიანური რესურსებისა და შეზღუდული ტექნიკური შესაძლებლობების გამო.

მიმართვიანობის ოფიციალური მექანიზმების გამოყენება კიდევ უფრო პრობლემურია სოფლად. ქალაქებს გარეთ, ადგილზე მოქმედ პოლიციის განყოფილებებს არ აქვთ საკმარისი შესაძლებლობა და ცოდნა, რაც შესაძლებელს გახდიდა კიბერინციდენტებზე ეფექტიან რეაგირებას. ეს ფაქტორი კიდევ უფრო აფერხებს სასოფლო დასახლებებში კიბერდანაშაულების შეტყობინებას. ფოკუსჯგუფების მონაწილეებმა, რომლებიც სოფლად ცხოვრობენ, ასევე აღნიშნეს, რომ, ხშირად, მათ ურჩევნიათ საკუთარი ოჯახის წევრს ან სანაცნობო წრის წარმომადგენელს დაეკითხონ რჩევა, ვიდრე პოლიციის ადგილობრივ განყოფილებაში განაცხადონ კიბერდანაშაულის შესახებ.

მიმართვიანობა მოქალაქეების მიერ

როდესაც საქმე მოქალაქეთა მიერ კიბერდანაშაულების მიმართვიანობას ეხება, ცნობიერებისა და ნდობის დაბალი დონე, კრიტიკულად მნიშვნელოვანი საკითხებია. ფოკუსჯგუფების რამდენიმე მონაწილემ აღნიშნა, რომ ისინი წარსულში გამხდარან „ფიშინგის“ მსხვერპლები, რის თაობაზეც პოლიციაშიც განაცხადეს. თუმცა, გამოძიება წარმატებით არ დასრულებულა. ამასთან, აღსანიშნავია, რომ მიმართვიანობის სავალდებულო პროცედურა არც თუ ისე

89. ინტერვიუ მთავრობის ყოფილ მაღალი რანგის წარმომადგენელთან ციფრული პლატფორმის მეშვეობით, 7 ოქტომბერი 2022.
90. ინტერვიუ მთავრობის ყოფილ მაღალი რანგის წარმომადგენელთან ციფრული პლატფორმის მეშვეობით, 18 ოქტომბერი 2022

ცოტა დროსა და სერიოზულ ძალისხმევას მოითხოვს. ფოკუსჯგუფის კიდევ ერთმა მონაწილემ, რომელსაც იურიდიული განათლება აქვს, გაიხსენა, რომ კიბერდანაშაულის მიმართვიანობისას მას პოლიციელები აგდებულად მოექცნენ. თუმცა, იგი ბოლომდე მიჰყვა საქმეს და სასამართლოში საკუთარი კანონიერი ინტერესები თავად დაიცვა, თუმცა, ამ შემთხვევაში მას ზურგს უმაგრებდა საკუთარი პროფესიული გამოცდილება და შესაბამისი პროცედურების ცოდნა.[91]

მონაწილეების თქმით, უმეტეს შემთხვევაში, მიმართვიანობის პროცედურების დაცვა დროის ფუჭად კარგვა იქნებოდა. ამის ნაცვლად, მათ ამჯობინეს მიემართათ კერძო სექტორის იმ სუბიექტებისთვის, სადაც კიბერდანაშული მოხდა - უმეტესად კომერციულ ბანკებს და მიეღოთ თავდაცვის საჭირო ზომები.[92] ეს სიტუაცია მხოლოდ საქართველოსთვის არ არის დამახასიათებელი. ბანკებისთვის დასახმარებლად მიმართვა, მაგალითად, კიბერთაღლითობის ან კიბერ მეთოდებით ჩადენილი დანაშაულის შემთხვევებისას, მსოფლიოში გავრცელებული პრაქტიკაა. თუმცა, საქართველოში ამ მხრივ პრობლემას ქმნის ის ფაქტი, რომ ამ ბანკებისთვის დასახმარებლად მიმართვა არა ნებაყოფლობითი, არამედ იძულებითი არჩევანია, რაც განპირობებულია მსხვერპლის ან დაზარალებულის გადაწყვეტილებით, არ მიმართოს სამართალდამცავ უწყებებს და ამის ნაცვლად დასახმარებლად ბანკს ან სხვა ბიზნესკომპანიებს მიმართოს. კვლევის ფარგლებში გამოკითხულმა ერთ-ერთმა ექსპერტმა, რამდენადმე განსხვავებული მოსაზრება გამოთქვა და ხაზი გაუსვა, რომ ბოლო წლებში ბანკებმა მნიშვნელოვნად გაზარდეს ძალისხმევა ცნობიერების ასამაღლებლად, რაც მიზნად ისახავს კლიენტების დაცვას კიბერდანაშაულებისგან. თუმცა, ასევე აღინიშნა, რომ მოქალაქეები, ძირითადად, მაინც მას შემდეგ მიმართავენ თავდაცვით ზომებს, რაც კიბერდამნაშავეების ქმედებების მსხვერპლები ხდებიან, შესაბამისად, ეს ზომები ნაკლებადაა პრევენციული და უფრო რეაგირების ხასიათს ატარებს.[93] ამის მაგალითად, ფოკუსჯგუფების რამდენიმე მონაწილემ გაიხსენა საკუთარი გამოცდილება, კერძოდ, მათ მხოლოდ მას შემდეგ დაიწყეს ბანკების მიერ შეთავაზებული დაზღვევის სერვისებით სარგებლობა, რაც მათ წინააღმდეგ კიბერშეტევა განხორციელდა.

ბავშვები და ახალგაზრდები

მონაცემთა შეკრების ეტაპიდანვე განისაზღვრა, რომ ბავშვები ერთ-ერთ ყველაზე მოწყვლადი ჯგუფია, განსაკუთრებით, როცა საქმე ეხება კიბერ მეთოდებით ჩადენილ დანაშაულსა და ზიანის შემცველ ონლაინ ქმედებებს, მაგალითად, კიბერბულინგს. მშობლების, კანონიერი წარმომადგენლებისა და მასწავლებლების ფოკუსჯგუფის მონაწილეების უმრავლესობა ფიქრობს, რომ ბავშვები უკიდურესად დაუცველები არიან ინტერნეტსივრცეში, ხოლო ინტერვიუს რესპონდენტებისა

91. ეთნიკური უმცირესობების ფოკუსჯგუფი, თბილისი, 5 ოქტომბერი 2022.
92. იქვე.
93. ინტერვიუ მთავრობის ყოფილ მაღალი თანამდებობის პირთან, თბილისი, 5 ოქტომბერი 2022.

და ვალიდაციის სამუშაო შეხვედრის მონაწილეების აზრით, კიბერბულინგი ერთ-ერთი ყველაზე ფართოდ გავრცელებული პრობლემაა ბავშვებისა და ახალგაზრდებისთვის (იხ. „კიბერმოწყვლადობის ხარისხი სხვადასხვა ჯგუფში“).[94] ცნობიერების დონე მიმართვიანობის არსებული მექანიზმების შესახებ უკიდურესად დაბალია ბავშვების წინააღმდეგ ჩადენილი კიბერდანაშაულის შემთხვევაში. ბევრი მშობელი ცდილობს საკუთარი ძალებით გაუმკლავდეს ამგვარ შემთხვევებს და არ მიმართოს სამართალდამცავ ორგანოებს.[95] ბავშვების წინააღმდეგ ჩადენილ კიბერდანაშაულებზე საქმის წარმოებისთვის შინაგან საქმეთა სამინისტრო განსხვავებულ პროცედურებს მიმართავს ქვეყნის არასრულწლოვანთა მართლმსაჯულების კოდექსის თანახმად, რომელიც ხაზს უსვამს მშობლების, კანონიერი წარმომადგენლებისა და მასწავლებლების სამართლებრივ პროცესებში ჩართულობის მნიშვნელობას. შესაბამისად, გამომძიებლები, რომლებიც ამგვარ საქმეებში არიან ჩართულები, ვალდებულები არიან, სპეციალური მომზადება გაიარონ.[96]

ქალები

კვლევისას ასევე გამოვლინდა, რომ კიბერბულინგი ერთ-ერთ ყველაზე სერიოზულ პრობლემას წარმოადგენს ქალების, ახალგაზრდა ქალებისა და გოგონებისთვის. ქალებს ხშირად ემუქრებიან და აშანტაჟებენ პირადი ინფორმაციის გავრცელებით.[97] კვლევაში მონაწილე რამდენიმე ექსპერტმა გაიხსენა ახლახან მომხდარი შემთხვევა, როდესაც ცნობილი ჟურნალისტებისა და პოლიტიკოსების წინააღმდეგ სწორედ ეს მუქარა გამოიყენეს.[98] ამგვარი შემთხვევების წარუმატებელი გამოძიება კიდევ უფრო აღრმავებს უნდობლობას სამართალდამცავი ორგანოების მიმართ, რაც, თავის მხრივ, აისახება ქალების მიერ ამ დანაშაულების მიმართვიანობის დინამიკაზე.

კიდევ ერთ მწვავე პრობლემას ხსენებული კანონდარღვევების შესახებ არასათანადო ცოდნა წარმოადგენს. ბევრმა ქალმა არ იცის, რომ კიბერშესაძლებელი შანტაჟი და მუქარა პირადი ან სენსიტიური ინფორმაციის გამჟღავნების თაობაზე სისხლის სამართლის დანაშაულად კვალიფიცირდება. ხშირად ეს პრობლემა კომპლექსური და ღრმად გამჯდარი კულტურული ფაქტორებით აიხსნება. მათ შორისაა სირცხვილის გრძნობა და სტიგმა სექსუალური ელემენტის შემცველ დანაშაულებთან დაკავშირებით. ამგვარი შემთხვევებისას მიმართვიანობის მაჩვენებელი უკიდურესად დაბალია, რადგან ქალები, რომლებიც შიშობენ, რომ

94. მშობლების, კანონიერი წარმომადგენლებისა და მასწავლებლების ფოკუსჯგუფი, თბილისი, 7 ოქტომბერი 2022.
95. იქვე
96. ინტერვიუ სამთავრობო უწყების მოქმედ თანამშრომელთან, თბილისი, 4 ოქტომბერი 2022.
97. ქალების ფოკუსჯგუფი, თბილისი, 4 ოქტომბერი 2022.
98. ინტერვიუ ქალების საკითხებზე მომუშავე სსო-ს წევრთან ციფრული პლატფორმის მეშვეობით, 20 ოქტომბერი 2022; ინტერვიუ სსო-ს ხელმძღვანელსა და მაღალი რანგის წევრთან, თბილისი, 3 ოქტომბერი 2022.

მათი პირადი ინფორმაცია არ იქნება სათანადოდ დაცული, თავს არიდებენ სამართალდამცავ უწყებებთან კონტაქტს. ერთ-ერთი რესპონდენტის, ექსპერტის მოსაზრებით, შინაგან საქმეთა სამინისტროს სჭირდება სენსიტიურ საკითხებთან მიმართებაში კარგად მომზადებული გამომძიებლები, რომლებიც იმუშავებენ ქალების წინაშე მდგარ კიბერსაფრთხეებზე. [99]

მსხვერპლი ქალები ხშირად მიმართავენ ქალების საკითხებზე მომუშავე სამოქალაქო საზოგადოების ორგანიზაციებს რჩევისთვის, მათ შორის იმის დასადგენად, კვალიფიცირდება თუ არა მათ წინააღმდეგ განხორციელებული ქმედება სისხლის სამართლის დანაშაულად. ერთ-ერთი ექსპერტის მოსაზრებით, ქალები ყველაზე მეტად განიცდიან კიბერდანაშაულის ვიწრო განსაზღვრების უარყოფითი ზეგავლენას.[100] უმეტესობა შემთხვევებში, ქალები ხდებიან კიბერ მეთოდებით ჩადენილი დანაშაულის ან ზიანის შემცველი ონლაინ ქმედებების მსხვერპლები, როცა მათ მდგომარეობას კიდევ უფრო ამძიმებს ტრადიციული გენდერული როლები და კონსერვატიული შეხედულებები სექსუალურ თავისუფლებაზე. ამ დანაშაულებს არ ეხება ინდივიდუალური მუხლები სისხლის სამართლის კოდექსში. ამის ნაცვლად, ისინი გათვალისწინებულია სხვადასხვა მუხლში. მაგალითად, ადევნებას ეხება მუხლი 151[1]. ამგვარი შემთხვევები იშვიათობას არ წარმოადგენს, თუმცა, როგორც ერთ-ერთმა ექსპერტმა მკვლევრებთან საუბარში განაცხადა, ის ფაქტი, რომ მუხლში ნახსენები არ არის სიტყვა „კიბერ“, მნიშვნელოვნად ართულებს სამართლიანობის აღდგენას როგორც მსხვერპლის, ასევე სამართალდამცავი ორგანოებისთვის.[101] როგორც ასეთი, ზიანის შემცველი ონლაინ აქტივობების, კიბერ მეთოდებით ჩადენილი დანაშაულის ან არსებულ მუხლებში კიბერელემენტების არასათანადოდ გათვალისწინება, ბარიერებს უქმნის ქალმებს სამართლის პოვნის პროცესში და ზღუდავს შინაგან საქმეთა სამინისტროს შესაძლებლობებს, გაუწიოს სამართლის მაძიებელ ქალებს სათანადო დახმარება.

ინფორმაციის გაზიარების ეფექტიანი სისტემების ნაკლებობა

კვლევის ფარგლებში გამოკითხული სამთავრობო უწყებების როგორც ყოფილი, ასევე მოქმედი წარმომადგენლები თანმხდებიან, რომ გამოწვევაა ინფორმაციის უწყებათაშორისი გაზიარების მექანიზმების ნაკლებობა. მიუხედავად იმისა, რომ საქართველოს ეროვნული კიბერუსაფრთხოების სტრატეგიის სამოქმედო გეგმა ითვალისწინებს კონკრეტულ აქტივობებს ინფორმაციის გაზიარების პლატფორმის შექმნასთან დაკავშირებით, ამჟამად ამგვარი პლატფორმა ჯერ კიდევ არ არსებობს.

99. ინტერვიუ ქალების საკითხებზე მომუშავე სსო-ს წევრთან ციფრული პლატფორმის მეშვეობით, 20 ოქტომბერი 2022.
100. იქვე.
101. იქვე.

[102] სამთავრობო უწყების ერთ-ერთი ყოფილი თანამშრომელი ფიქრობს, რომ შესაძლებელია ორი სხვადასხვა სისტემის შექმნა კრიტიკული და არაკრიტიკული ინფრასტრუქტურის სუბიექტებისთვის.[103] კიდევ ერთმა რესპონდენტმა, რომელიც წარსულში სამთავრობო უწყებაში მუშაობდა, განაცხადა, რომ მისი აზრით, ინფორმაციის გაზიარების პროცესი შეიძლება განისაზღვროს სექტორული მიმართულებებით და დაიწყოს, მაგალითად, ენერგეტიკული ან ფინანსური სექტორებით.[104]

უმეტეს შემთხვევებში, სააგენტოებს შორის ინფორმაციის გაზიარება არაფორმალური მეთოდებით ხორციელდება და პირადი კომუნიკაციის ფორმა აქვს. ზოგადად, სააგენტოები ნაკლებად ავლენენ ენთუზიაზმს, როდესაც საქმე ინფორმაციის გაზიარებას ეხება. რამდენიმე რესპონდენტმა ეჭვქვეშ დააყენა შინაგან საქმეთა სამინისტროსა და კიბერუსაფრთხოების ბიუროს შორის ინფორმაციის მიმოცვლის ეფექტიანობა.[105] შესაბამისად, სახეზეა ინფორმაციის გაზიარების მექანიზმების სარგებლიანობის აღიარების საჭიროება სხვადასხვა დაინტერესებული მხარის მიერ. აღსანიშნავია, რომ როგორც ყოფილი, ასევე მოქმედი ოფიციალური პირები აღიარებენ, რომ ამ მხრივ ჯერ-ჯერობით არ გადადგმულა რაიმე ნაბიჯი ეფექტიანი სისტემის შესაქმნელად, რაც უდავოდ საჭიროა.

რაც შეეხება კერძო სექტორს, ციფრული მმართველობის სააგენტოსთან მოქმედებს სპეციალური პლატფორმა, რომლის გამოყენებაც ინციდენტების შესახებ ინფორმაციის გასაცვლელად შეუძლიათ როგორც კერძო სუბიექტებს, ასევე ინდივიდებსაც. სააგენტო აპირებს გააუმჯობესოს პლატფორმის მიერ სტატისტიკური მონაცემების მართვის მექანიზმი.[106]

სამთავრობო უწყებებს შორის ინფორმაციის გაზიარებასთან დაკავშირებულ ცვლილებებს ეხება დიდი ბრიტანეთსა და საქართველოს შორის კიბერპარტნიორობის პროგრამის ერთ-ერთი მიმართულება, რომელიც ითვალისწინებს ინფორმაციის მიმოცვლის ეფექტიანი ჩარჩოს განვითარებას. ინფორმაციის გაცვლა ასევე წარმოადგენს კიბერუსაფრთხოების ეროვნული სტრატეგიის ერთ-ერთ მნიშვნელოვან აქტივობას.

ნდობა

ფოკუსჯგუფების მონაწილეებისა და ინტერვიუების რესპონდენტების უმეტესობამ სამართალდამცავი უწყებების მიმართ ნდობის ნაკლებობა კიბერდანაშაულის

102. საქართველოს მთავრობა, „საქართველოს ეროვნული კიბერუსაფრთხოების სტრატეგია“, გვ. 3 და გვ. 20.
103. ინტერვიუ მთავრობის ყოფილ მაღალი თანამდებობის პირთან, თბილისი, 4 ოქტომბერი 2022.
104. ინტერვიუ მთავრობის ყოფილ მაღალი თანამდებობის პირთან ციფრული პლატფორმის მეშვეობით, 18 ოქტომბერი 2022.
105. ინტერვიუ მთავრობის ყოფილ მაღალი თანამდებობის პირთან, თბილისი, 5 ოქტომბერი 2022; იქვე.
106. ინტერვიუ მთავრობის ყოფილ მაღალი თანამდებობის პირთან, თბილისი, 4 ოქტომბერი 2022.

მიმართვიანობის ერთ-ერთ ყველაზე სერიოზულ სირთულედ დაასახელა. გარდა ამისა, კვლევის ფარგლებში გამოიკვეთა ორი მნიშვნელოვანი ფაქტორი: უნდობლობა სამართალდამცავი ორგანოების შესაძლებლობების მიმართ და მათი ზოგადი სანდოობა.

ნდობის ნაკლებობა სამართალდამცავი უწყებების შესაძლებლობების მიმართ

ფოკუსჯგუფების მონაწილეების უმეტესობა ფიქრობს, რომ პოლიციას არ შეუძლია მოახდინოს ეფექტიანი რეაგირება კიბერინციდენტებზე, უმთავრესად, გამოძიებისთვის საჭირო რესურსებისა და შესაძლებლობების ნაკლებობის გამო. გარდა ამისა, პრობლემურად მიიჩნევა მიმართვიანობის პროცესის ხანგრძლივობა, რაც ბარიერს ქმნის მოქალაქეებისთვის, განსაკუთრებით, იმის გათვალისწინებითაც, რომ მათ არ სჯერათ მცდელობის წარმატებით დასრულებისა.

მიუხედავად შინაგან საქმეთა სამინისტროს შესაძლებლობების ეტაპობრივი გაუმჯობესებისა, კვლევაში მონაწილე რამდენიმე ექსპერტმა განაცხადა, რომ ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველოს წინაშე კვლავ რჩება ისეთი გამოწვევები, როგორიცაა ადამიანური და ტექნიკური რესურსების დეფიციტი. კვლევის არაექსპერტული გამოცდილების მქონე რესპონდენტები ვარაუდობენ, რომ კიბერდანაშაულების გამოძიება სირთულეებთან არის დაკავშირებული, რადგან მათი კომპლექსურობა აღემატება მთავრობის შესაძლებლობებს. ამ პრობლემის სიმწვავე კიდევ უფრო იგრძნობა სასოფლო დასახლებებში, სადაც, პოლიცია ჯერ კიდევ მოუმზადებელია ისეთ საკითხებში, რომლებიც ეხება კიბერდანაშაულის მსხვერპლთან მოპყრობას და მასთან მუშაობას. ამის დასტურად, ფოკუსჯგუფების რამდენიმე მონაწილემ დაიჩივლა პოლიციის არაკომპეტენტურობის შესახებ მცირე სასოფლო და საქალაქო დასახლებებში. ეს პრობლემა, თავის მხრივ, ხშირად ხდება შეუტყობინებლობის მიზეზი, რადგანაც მსხვერპლებს ურჩევნიათ საკუთარი ძალებით გაუმკლავდნენ მომხდარს. მაგალითად, მსუბუქი თაღლითობის შემთხვევაში, მრავალი მონაწილის თქმით, ისინი ამჯობინებენ მთლიანად მიენდონ ბანკებს ან თავი არ შეიწუხონ მიმართვიანობით და შესაბამისად შეეგუონ ფინანსურ დანაკარგს.

ჟურნალისტების ფოკუსჯგუფის მონაწილეების უმეტესობამ, რომლებსაც ჰქონდათ კიბერდანაშაულის მსხვერპლობის გამოცდილება, განაცხადა, რომ ამჯობინეს დახმარებისთვის არაფორმალური ქსელისთვის მიემართათ, ვიდრე მომხდარის შესახებ სამართალდამცავებისთვის მიემართათ.[107] მაგალითად, ერთ-ერთი რეგიონული მედიაორგანიზაციის ხელმძღვანელმა გაიხსენა, როგორ მიმართეს სამართალდამცავებს მათი ოფიციალური YouTube არხის წინააღმდეგ

107. ჟურნალისტების ფოკუსჯგუფი, თბილისი, 6 ოქტომბერი 2022.

განხორციელებული კიბერ შეტევის შემთხვევის საკითხზე.[108] პასუხად, პოლიციამ განაცხადა, რომ ინციდენტის გამოძიება მათ შესაძლებლობებს აღემატებოდა და კომპანიას თვითონ უნდა ეზრუნა ონლაინ ანგარიშების დაცულობის გაუმჯობესებაზე. ეს შემთხვევა ასევე მიუთითებს, რომ ზოგადად, სამართალდამცავ უწყებებს არ აქვთ საკმარისი კავშირები მსხვილ ტექკომპანიებთან, რაც მათ დაეხმარებოდა ამგვარი პრობლემების გადაჭრაში. პოლიციის პასუხის შემდეგ, დაზარალებულმა მედიაორგანიზაციამ პირადი კონტაქტები გამოიყენა და არაფორმალურად შეეცადა დახმარების მიღებას.

სამართალდამცავი უწყებები და ნდობის ხარისხი

უნდობლობა სამართალდამცავი უწყებების მიმართ განსაკუთრებით თვალშისაცემად ჟურნალისტების ფოკუსჯგუფის მონაწილეებში იგრძნობოდა. რამდენიმე მონაწილემ აღნიშნა, რომ ისინი ცნობიერების ამაღლების მიზნით სახელმწიფო არხებით გავრცელებულ რესურსებსაც კი არ ენდობოდნენ. ჟურნალისტების განსაკუთრებულ შეშფოთებას იწვევდა მტკიცე რწმენა იმასთან დაკავშირებით, რომ სამართალდამცავ უწყებებსა და სახელმწიფო უსაფრთხოების სამსახურს შეუძლიათ მათი კონფიდენციალურობის დარღვევა და პირადი მონაცემების ბოროტად გამოყენება.

კონფიდენციალურობის საკითხი მწვავე პრობლემაა სასოფლო დასახლებებში. კვლევის მონაწილე ერთ-ერთი ექსპერტის აზრით, სასოფლო თემებში კონფიდენციალურობის შენარჩუნება თითქმის შეუძლებელია, რაც ხელს უშლის მოქალაქეების მიერ დანაშაულის მიმართვიანობისას. კონფიდენციალურობის დაცვის შესახებ ეჭვებს განსაკუთრებით ქალები გამოხატავენ, რადგან ისინი უფრო ხშირად ხდებიან პირადი ინფორმაციის უკანონო გავრცელების მსხვერპლები და შესაბამისად, მეტად ფრთხილობენ ამ საკითხთან დაკავშირებით, განსაკუთრებით, იმ პირობებში, როდესაც სასოფლო დასახლებებში მომსახურე პოლიციის თანამშრომლები არ გამოირჩევიან მონაცემთა დაცვისა და მასთან დაკავშირებული ჰიგიენის გონივრული დაცვით. ერთ-ერთი რესპონდენტის, მთავრობის ყოფილი მოხელის აზრით, მსხვერპლები უფრთხიან რეპუტაციულ ზარალს, რაც შეიძლება პოლიციის მიერ მათი პერსონალური ინფორმაციის გაუფრთხილებელმა მოპყრობამ გამოიწვიოს.[109] ქალების ფოკუსჯგუფის რამდენიმე მონაწილემ აღნიშნა, რომ ისინი, როგორც წესი, დახმარებისთვის სხვა ქალებს მიმართავენ ისეთ სივრცეებში, როგორიცაა მაგალითად, Facebook-ის ჯგუფი, თუმცა, დახმარება ხშირად იმაში გამოიხატება, რომ ქალები ერთმანეთს ამხნევებენ და ძალას მატებენ პოლიციამდე მისასვლელად.

108. იქვე.
109. ინტერვიუ მთავრობის ყოფილ მაღალი თანამდებობის წევრთან, 5 ოქტომბერი 2022.

კვლევის ფარგლებში გამოკითხულმა რამდენიმე ექსპერტმა შეშფოთება გამოთქვა სახელმწიფო უსაფრთხოების სამსახურის ოპერატიულ-ტექნიკური სააგენტოს გაზრდილ უფლებამოსილებასთან დაკავშირებით, რაც უწყებას ინფორმაციული უსაფრთხოების შესახებ კანონით მიენიჭა.[110] ზოგადად, ოპერატიულ-ტექნიკური სააგენტოს შესაძლებლობების მიმართ ნდობა საკმაოდ მაღალია, თუმცა, იგივე არ ვრცელდება სააგენტოს საქმიანობის მოტივის მიმართ, რაც განპირობებულია საზოგადოებაში გავრცელებულ მოსაზრებასთან იმასთან დაკავშირებით, რომ უწყება ბოროტად სარგებლობს მოქალაქეთა პერსონალური მონაცემებით. შესაბამისად, ერთ-ერთი რესპონდენტის აზრით, სააგენტომ მნიშვნელოვანი რესურსები უნდა მიმართოს კომუნიკაციის გაუმჯობესებისკენ, რათა საზოგადოებაში მის მიმართ ნდობა გაიზარდოს. თუმცა, საზოგადოებაში არსებული განწყობების გათვალისწინებით, ეს იოლი ამოცანა არ იქნება.

როდესაც საქმე მიმართვიანობას ეხება, ნდობა კერძო სექტორის მიმართ შედარებით მაღალია. მრავალმა მონაწილემ აღნიშნა, რომ ისინი ენდობიან ბანკებს და იმ შემთხვევაში, თუ ისინი ფინანსურად მოტივირებული კიბერდანაშაულის მსხვერპლები გახდებიან, ურჩევნიათ ამის შესახებ პოლიციას კი არა, ბანკს შეატყობინონ. მრავალი მონაწილე უარყოფითად აფასებს მთავრობის აქტივობებს და აღნიშნავს, რომ სახელმწიფო უწყებებმა უფრო პროაქტიულად უნდა მიიღონ ცნობიერების ამაღლებისკენ მიმართული ზომები და დაეხმარონ მოსახლეობას, გაიუმჯობესონ ცოდნა კიბერჰიგიენის შესახებ.

110. ინტერვიუები, 2022 წლის ოქტომბრიდან 2023 წლის იანვრამდე 2023.

IV. მიგნებები და რეკომენდაციები

წინამდებარე თავში წარმოდგენილია კვლევის მიგნებები, რომლებიც ანგარიშის წინა თავებში მოცემულ ანალიზს ეყრდნობა. ამავე თავში შეტანილია რეკომენდაციები, რომლებიც მიგნებებზე დაყრდნობით სხვადასხვა დაინტერესებული მხარისთვის შემუშავდა, რომელთა შორის არიან საქართველოს საჯარო, კერძო და სამოქალაქო სექტორების წარმომადგენლები და საერთაშორისო აქტორები.

მიგნება 1: საბანკო ანგარიშებზე უნებართვო წვდომა, საკრედიტო და სადებეტო ბარათებთან დაკავშირებული თაღლითობა, სოციალური მედიისა და აზარტული თამაშების ანგარიშების გატეხვა ის უმთავრესი კლასიკური კიბერ დანაშაულებია, რომლებიც საფრთხეს უქმნის ქვეყნის მოსახლეობას.

რეკომენდაცია: შინაგან საქმეთა სამინისტრომ უნდა გააგრძელოს მუშაობა კერძო სექტორის ძირითად პარტნიორებთან ყველაზე გავრცელებულ კიბერდანაშაულებთან საბრძოლველად. სამინისტრომ ასევე უნდა გააანალიზოს მიმდინარე თანამშრომლობა კერძო სექტორის წარმომადგენელ პარტნიორებთან, განსაკუთრებით კი, აზარტული თამაშების კომპანიებთან, რათა შეიმუშაოს მულტიაქტორული მოდელი ყველაზე გავრცელებულ კიბერდანაშაულებთან გამკლავების მიზნით. მოდელმა უნდა განსაზღვროს კერძო კომპანიების შერჩევის, მათთან კომუნიკაციისა და ინტერაქციის მექანიზმი და ჩამოაყალიბოს ჩარჩო ერთობლივი საქმიანობის ეფექტიანობის შესაფასებლად. ეს რეკომენდაცია შეესაბამება ეროვნული კიბერუსაფრთხოების სტრატეგიის მე-2 მიზნის 2.2 ამოცანას, რაც გულისხმობს საჯარო-კერძო თანამშრომლობის მხარდაჭერასა და კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანი სისტემის განვითარებას.[111]

მიგნება 2: პრობლემურია ინფორმაციის გაზიარების პლატფორმების ფუნქციონირება, როგორც სამთავრობო უწყებებს, ასევე კერძო და სამოქალაქო სექტორის აქტორებს შორის. განსაკუთრებულად მწვავედ დგას შემდეგი საკითხები:

- ა) კვლევაში მონაწილე ექსპერტებში შეინიშნება ზოგადი გაურკვევლობა იმასთან დაკავშირებით, არსებობს თუ არა ინფორმაციის გაზიარების პლატფორმა
- ბ) ინფორმაციის მიმოცვლისა და გაზიარების პროცესის ინსტიტუციონალიზაციისა და სისტემიზაციის ნაკლებობა, რაც აიძულებს შესაბამის უწყებებს დაეყრდნონ პირად კონტაქტებსა და ინფორმაციის გაზიარების არაფორმალურ მექანიზმებს.

რეკომენდაცია: კიბერდანაშაულთან და კიბერ საფრთხეებთან დაკავშირებული ინფორმაციის გაცვლის სისტემის შემდგომი განვითარება. უნდა შემუშავდეს

111. საქართველოს მთავრობა, „საქართველოს ეროვნული კიბერუსაფრთხოების სტრატეგია“, გვ. 17–18.

ან გაუმჯობესდეს კიბერდანაშაულსა და კიბერსაფრთხეებთან დაკავშირებული ინფორმაციის უწყებათაშორისი მიმოცვლის პრაქტიკები, დიდი ბრიტანეთ - საქართველოს კიბერპარტნიორობის ჩარჩოში მითითებული რეკომენდაციების შესაბამისად, რაც, თავის მხრივ, თანხვედრაშია საქართველოს ეროვნულ კიბერუსაფრთხოების სტრატეგიასა და ქვეყნის ამბიციასთან, შემოიღოს საერთაშორისოდ აპრობირებული საუკეთესო პრაქტიკები.[112] ინფორმაციის გაცვლის პრაქტიკის დანერგვა აუცილებელია მთავრობის მასშტაბით, შესაბამისად, კიბერუსაფრთხოებაზე პასუხისმგებელი სააგენტოების საქმიანობის კოორდინაცია უსაფრთხოების ეროვნული საბჭოს მანდატში უნდა შევიდეს.

მიგნება 3: დაბალია საზოგადოების ცნობიერების დონე კიბერდანაშაულების საფრთხეებთან დაკავშირებით. უფრო კონკრეტულად:

- ზოგ მოწყვლად ჯგუფში შეინიშნება ცნობიერების საშუალოზე დაბალი დონე. ამ ჯგუფებს შორისაა ბავშვები, ხანდაზმული მოქალაქეები, სოფლად მცხოვრებლები და ეთნიკური უმცირესობები, განსაკუთრებით ისინი, რომლებსაც უჭირთ ქართულ ენაზე მეტყველება.
- კიბერცნობიერების დაბალ დონეს ისეთ გავლენიან ჯგუფებში, როგორიცაა, მაგალითად, ჟურნალისტები, პოლიციის თანამშრომლები და მასწავლებლები, მულტიპლიკატორი ეფექტი აქვს, რაც უარყოფით გავლენას ახდენს უფრო ფართო საზოგადოებაზე.
- სათანადოდ არ ხდება განათლების სისტემის გამოყენება კიბერცნობიერების ასამაღლებლად. კვლევის შედეგები მიუთითებს, რომ შესაძლებელია ამ მხრივ სკოლების, როგორც სათემო ცენტრების გამოყენება ადგილობრივ დონეზე ცნობიერების ამაღლებისთვის. ასევე, რეკომენდებულია დაწყებით და საშუალო განათლების პროგრამებში კიბერუსაფრთხოების საკითხების შეტანა.
- კიბერდანაშაულის შესახებ ცნობიერების დაბალი დონე განაპირობებს კიბერჰიგიენის ირგვლივ ცოდნის დეფიციტს და შესაბამისი პრაქტიკის სიმწირეს მოსახლეობაში.
- მთავრობის მიერ განხორციელებული საინფორმაციო კამპანიები და სამართალდამცავი უწყებები კიბერჰიგიენის შესახებ ინფორმაციის ყველაზე სანდო წყაროდ მიიჩნევა, თუმცა მოქალაქეები მაინც ყველაზე ხშირად მეგობრებსა და ოჯახის წევრებს ეყრდნობიან კიბერჰიგიენის შესახებ ინფორმაციის მისაღებად.
- მცირე და საშუალო ბიზნესების ნაწილი კიბერსაფრთხეებს სერიოზულად არ მიიჩნევს დაბალი შემოსავლებისა და კომპანიების ზომის გამო.
- გარკვეული ჯგუფების ცნობიერება გავლენას ახდენს მთლიანად საზოგადოების ცნობიერებასა და ინფორმირებულობაზე.
- კიბერდანაშაულის შესახებ ცნობიერების ამაღლებისკენ მიმართული აქტივობები არათანმიმდევრული და დეცენტრალიზებულია. საჯარო სექტორსა და სამოქალაქო საზოგადოებაში მწირია ინფორმაცია ამ აქტივობების შესახებ.

112. იქვე, გვ. 10.

რეკომენდაცია: მთავრობამ უნდა წამოიწყოს კიბერდანაშაულის შესახებ ცნობიერების ამაღლების ფართომასშტაბიანი კამპანია კიბერუსაფრთხოების ეროვნული სტრატეგიის პირველი მიზნით გათვალისწინებული ვალდებულების თანახმად. ეროვნულ დონეზე კამპანიის კოორდინაცია უნდა ითავოს ციფრული მმართველობის სააგენტომ შინაგან საქმეთა სამინისტროსთან მჭიდრო კოორდინაციით.[113] ამ ორ უწყებას შორის თანამშრომლობა მეტად მნიშვნელოვანია, რადგანაც ერთი მათგანი – ციფრული მმართველობის სააგენტო, პასუხისმგებელია ცნობიერების ამაღლებასა და სტრატეგიული კომუნიკაციის მნიშვნელოვანი ზომების გატარებაზე საქართველოს ეროვნული კიბერუსაფრთხოების სტრატეგიის მიხედვით, ხოლო შინაგან საქმეთა სამინისტრო წარმოადგენს წამყვან უწყებას კიბერდანაშაულთან რეაგირებისა და მისი აღმოფხვრის კუთხით და შესაბამისად, ყველაზე უკეთ შეუძლია განსაზღვროს ის საკითხები და მიმართულებები, რომელთან დაკავშირებითაც ცნობიერების ამაღლების ღონისძიებებს ყველაზე მეტი გავლენა ექნება. კამპანია, თავისი არსით, უნდა ეფუძნებოდეს მრავალი აქტორის ჩართულობას და იყენებდეს სხვადასხვა სამთავრობო უწყებაში, განყოფილებასა და დეპარტამენტებში, ასევე კერძო სექტორსა და სამოქალაქო საზოგადოების ორგანიზაციაში მიმდინარე და სამომავლოდ დაგეგმილ ღონისძიებებს და ამით აღიარებდეს, რომ კიბერუსაფრთხოება „ყველას პასუხისმგებლობაა“.[114] კამპანიაში გათვალისწინებული უნდა იყოს პირველ თავში აღწერილი წარმატებული საინფორმაციო კამპანიის პრინციპები. ქვემოთ მოცემულია უშუალოდ კამპანიასთან დაკავშირებული კონკრეტული რეკომენდაციები.

რეკომენდაცია: პრიორიტეტი მიენიჭოს სამთავრობო უწყებებისა და სამართალდამცავი ორგანოების ჩართულობას კიბერუსაფრთხოების ცნობიერების ამაღლების კამპანიაში. მთავრობის მიერ ორგანიზებული საინფორმაციო კამპანიები, ასევე სამართალდამცავი უწყებები, კიბერჰიგიენის შესახებ რესურსების ყველაზე სანდო წყაროდ მიიჩნევიან. ციფრული მმართველობის სააგენტოს, შინაგან საქმეთა სამინისტროს და შესაძლოა, ცენტრალური კრიმინალური პოლიციის დეპარტამენტის ჩართულობა საგანგებოდ უნდა იყოს აღნიშნული კამპანიასთან დაკავშირებულ საინფორმაციო და საკომუნიკაციო მასალებში. ჩართულობა შესაძლებელია გამოხატული იყოს ხსენებული უწყებების წარმომადგენლების მედიასთან ურთიერთობით, მათი ლოგოების განთავსებით კამპანიის ფარგლებში მომზადებულ პუბლიკაციებზე და ასევე, უწყებების ოფიციალური სოციალური მედიის გვერდების გამოყენებით კამპანიის ძირითადი გზავნილების გასავრცელებლად. ზემოთ ჩამოთვლილი ჩართულობის მხოლოდ რამდენიმე მაგალითია და ცხადია, შესაძლებელია სხვა ფორმების და მექანიზმების გამოყენებაც.

113. იქვე, გვ. 16.
114. იქვე, გვ. 14.

რეკომენდაცია: გზავნილები უნდა კონცენტრირდეს შემდეგ სამ ძირითად მიმართულებაზე: კიბერდანაშაულის ბუნება, კიბერჰიგიენა და მიმართვიანობა.

1. **კიბერდანაშაულის ბუნება:** კიბერდანაშაულის აღქმა საზოგადოებაში არ ემთხვევა სისხლის სამართლის კოდექსში მოცემულ განმარტებას. ერთი მხრივ, ეს შეუსაბამობა შესაძლებელია მიუთითებს იმაზე, რომ გადასახედია არსებული იურიდიული დებულებები. თუმცა, მეორე მხრივ, საჭიროა ცნობიერების ამაღლება იმის თაობაზე, თუ რომელი კიბერ აქტივობები კვალიფიცირდება დანაშაულად, იქნება ეს კლასიკური კიბერდანაშული თუ კიბერ მეთოდით ჩადენილი დანაშაული. ცნობიერების ამაღლების კამპანია, რომელსაც ციფრული მმართველობის სააგენტო და შინაგან საქმეთა სამინისტრო უნდა წარუძღვნენ, ერთ-ერთ მიზნად უნდა ისახავდეს კიბერდანაშაულის ნიშნებისა და ბუნების შესახებ საზოგადოების განათლებას. ამისთვის, კი, აქცენტი უნდა გაკეთდეს ქალებისა და ახალგაზრდების გამოცდილებაზე, განსაკუთრებით კი ისეთ პრობლემებზე, რომლებიც ეხება პირადი და პერსონალური ინფორმაციის ბოროტად გამოყენებას.
2. **კიბერჰიგიენა.** ერთ-ერთ მთავარ პრობლემას წარმოადგენს ის, რომ ადამიანებმა ან არ იციან, რომ საჭიროა კიბერჰიგიენის გაუმჯობესება ან არ იციან, რა არის ამისთვის საჭირო. ნაწილობრივ, ეს პრობლემა გამოწვეულია კიბერდანაშაულიდან მომდინარე რისკების, ინდივიდუალური და ორგანიზაციული მოწყვლადობისა და ვიქტიმიზაციის პოტენციური ზეგავლენის შესახებ დაბალი ცნობიერებით, რაც ხელს უშლის ცნობიერების დონის ამაღლებაზე ზრუნვას. სწორი მოტივაციის პირობებში, ადამიანები იწყებენ კიბერჰიგიენის ზომების გატარებას, რომლებსაც, განურჩევლად იმისა, ინდივიდუალურ თუ ორგანიზაციულ დონეზეა მიღებული, გადამწყვეტი მნიშვნელობა ენიჭება ეროვნული კიბერუსაფრთხოების მედეგობის გაუმჯობესებისთვის. გარდა ამისა, კიბერჰიგიენა აუცილებელია კიბერუსაფრთხოების მიმართ „მთლიანად საზოგადოების“ მიდგომის დამკვიდრებაში.
3. **მიმართვიანობა.** მიმართვიანობის დაბალი მაჩვენებლის მიზეზი ცნობიერების ნაკლებობა ან მიმართვიანობის არსებული მექანიზმების ირგვლივ დაბნეულობაა. შესაბამისად, კამპანიის დაგეგმვისა და განხორციელების პროცესში განსაკუთრებული ყურადღება უნდა დაეთმოს მოსახლეობისთვის ინფორმაციის მიწოდებას მიმართვიანობის სხვადასხვა საშუალების შესახებ (იხ. „მიმართვიანობის მექანიზმები“). ამ საკითხთან დაკავშირებულ მთავარ გზავნილებში ხაზი უნდა გაესვას, რომ მიმართვიანობის არ არის რთული ან გაჭიანურებული პროცესი, ხოლო ძირითადი აქცენტი სოფლად მცხოვრებ მოსახლეობაზე უნდა გაკეთდეს. როგორც კამპანიის სხვა მიმართულებების შემთხვევაში, კომუნიკაცია მიმართვიანობის შესახებ უნდა განხორციელდეს სხვადასხვა ფორმატისა და ენის გამოყენებით. კიდევ ერთი მნიშვნელოვანი საკითხი, რომელიც უნდა აისახოს გზავნილებში შეტყობინების შესახებ, ეხება

უნდობლობას, რომელსაც ქალები იჩენენ სამართალდამცავი ორგანოების მიმართ.

რეკომენდაცია: სკოლებისა და მასწავლებლების რესურსის უკეთ გამოყენება კიბერდანაშაულის შესახებ საზოგადოების ცნობიერების დონის ასამაღებლად. ცნობიერების ამაღლების ეროვნული კამპანია უნდა ფოკუსირდეს სკოლებზე, რომლებიც აერთიანებს მოწყვლად (ბავშვები) და გავლენის მქონე (მასწავლებლები) ჯგუფებს და სათემო ცენტრების ფუნქციას ასრულებს. კამპანიის ფარგლებში აუცილებელია მუშაობა განათლების, მეცნიერების, კულტურისა და სპორტის სამინისტროსთან კამპანიის ფარგლებში სკოლების გამოყენების მიზნით. სკოლებს შეუძლიათ, მაგალითად, კიბერცნობიერებისა და კიბერჰიგიენის შესახებ ინფორმაციის გავრცელება, ასევე, სათემო ღონისძიებების მასპინძლობა.

რეკომენდაცია: საინფორმაციო კამპანია, წარმატებებისა და გამოწვევების შესწავლის მიზნით, მიმდინარეობის პროცესშივე უნდა დაეყრდნოს მონიტორინგს, კვლევას და შეფასებას. მონიტორინგის, კვლევის, შეფასებისა და შეფასების ეფექტიანი სისტემის ჩამოყალიბება კამპანიის საწყისი ეტაპიდან დასრულებამდე, ასევე, მისი განხორციელების შემდგომი ანალიზი, გადამწყვეტი იქნება ეფექტიანობის დადგენისა და ხარვეზების აღმოჩენის მიზნით. ამ სისტემის მეშვეობით ხელისუფლებას შეეძლება დაადგინოს, თუ რამდენად ღირებული იყო კამპანიის ფარგლებში განხორციელებული აქტივობები, რაც საფუძველს ჩაუყრის საუკეთესო პრაქტიკების შემუშავებას. აღსანიშნავია, რომ საქართველოს შეეძლება გამოვლენილი საუკეთესო პრაქტიკების გაზიარება რეგიონულ დონეზე. მონიტორინგის, კვლევისა და შეფასების ჩარჩოს განვითარება უნდა მოხდეს ციფრული მმართველობის სააგენტოს, როგორც კამპანიის წარმმართველი უწყებისა და შინაგან საქმეთა სამინისტროს ერთობლივი ძალისხმევითა და კოორდინაციით, რადგან შინაგან საქმეთა სამინისტრო ყველაზე მეტადაა დაინტერესებული კიბერმოწყვლადობის დონის შემცირებაში კამპანიის მეშვეობით.

რეკომენდაცია: საჭიროა ტრენინგების ციკლის უზრუნველყოფა კიბერჰიგიენის საკითხებში გავლენიანი ჯგუფებისთვის. მთავრობამ, სამოქალაქო საზოგადოების ორგანიზაციებმა და საერთაშორისო დონორებმა მხარი უნდა დაუჭიროს ტრენინგებს კიბერჰიგიენის საფუძვლებში (ქცევები, ინსტრუმენტები, საინფორმაციო რესურსები) ჯგუფებისთვის, რომლებიც მულტიპლიკატორის ეფექტს ფლობენ სხვადასხვა პროფესიულ ქსელებში, მათ შორის, მასწავლებლებში, ჟურნალისტებსა და ადგილობრივ სამართალდამცავ უწყებებში. ტრენინგების მიზანი უნდა იყოს მონაწილეებისთვის მარტივი და პრაქტიკული გამოსავლების შეთავაზება და მათთვის საკვანძო რესურსების, მაგალითად, სახელმძღვანელო ბუკლეტების მიწოდება, სადაც, დეტალურად იქნება გაწერილი საუკეთესო პრაქტიკები. სატრენინგო კურსების დაგეგმვისა და განხორციელებისას გამოყენებული უნდა იქნეს პროფესიული ქსელებისა და კავშირების (მაგალითად,

საქართველოს ჟურნალისტური ეთიკის ქარტიის[115]) რესურსები პოტენციური მონაწილეების მობილიზებისთვის.

რეკომენდაცია: მთავრობის მიერ აქტივობების ფართო სპექტრის დაგეგმვა და მათ შორის სინერგიის უზრუნველყოფა. კამპანია, მიუხედავად მისი მნიშვნელობისა, ვერ იქნება ყველა პრობლემის გამოსავალი. რასაკვირველია, კიბერდანაშაულის შესახებ ცნობიერების გაუმჯობესება და კიბერჰიგიენის გაჯანსაღება განამტკიცებს სახელმწიფოს მედეგობას, თუმცა, ეს არ გამორიცხავს სხვა ღონისძიებებს, მაგალითად, ნაცვლად კეთილ ნებაზე დაყრდნობისა, რეკომენდებულია მიმწოდებლებისთვის კიბერუსაფრთხოების ზომების გატარების ვალდებულების შემოღება, რათა რისკები შემცირდეს საბოლოო მომხმარებლისთვის.

ამგვარად, კიბერუსაფრთხოების ეროვნული სტრატეგიის მიზნების შესაბამისად, კიბერცნობიერების ამაღლების ეროვნული კამპანია კიბერუსაფრთხოების გაუმჯობესების ამბიციური ღონისძიებების მხოლოდ ერთ-ერთ კომპონენტს წარმოადგენს.

რეკომენდაცია: ცნობიერების ამაღლების მიმდინარე და განხორციელებული აქტივობების დოკუმენტირება. მთავრობამ უნდა ითავოს ცნობიერების ამაღლებისკენ მიმართული საქმიანობის სისტემატიზაცია და უზრუნველყოს გამჭვირვალე კომუნიკაცია აქტივობების შესახებ. ციფრული მმართველობის სააგენტო და შინაგან საქმეთა სამინისტრო მუდმივად უნდა აახლებდნენ აქტივობების ჩამონათვალს და ეს ინფორმაცია, ცნობიერების ამაღლების წარსულში განხორციელებულ აქტივობებთან ერთად, საჯაროდ უნდა იყოს ხელმისაწვდომი. იდეალურ შემთხვევაში, სია უნდა მომზადდეს და განახლდეს სამოქალაქო საზოგადოების აქტორებთან თანამშრომლობით. არასამთავრობო ორგანიზაციებს უნდა შეეძლოთ საკუთარი აქტივობების ნებაყოფლობით აღნუსხვა ამავე სიაში.

მიგნება 4: საზოგადოებაში კიბერდანაშაულის ინტუიციური აღქმა უფრო ფართოა, ვიდრე საქართველოს სისხლის სამართლის კოდექსით გათვალისწინებული განსაზღვრება. კოდექსის მუხლები, რომლებიც კიბერდანაშაულს უკავშირდება, მხოლოდ კლასიკურ კიბერდანაშაულს ეხება მაშინ, როცა საზოგადოების წარმოდგენაში კიბერდანაშაული ასევე გულისხმობს კიბერ მეთოდებით ჩადენილ დანაშაულებრივ და დამაზიანებელ ონლაინ ქმედებებს. ამგვარი განსხვავება იწვევს გაუგებრობას და აცდენას მოლოდინებს შორის. მაგალითად, ქალები ხშირად აღნიშნავენ, რომ ისინი უფრო ხშირად ხდებიან ისეთი კიბერ მეთოდებით ჩადენილი დანაშაულის მსხვერპლები, როგორიცაა პირადი მონაცემების უნებართვო გავრცელება ან გავრცელების მუქარა, თუმცა მთავრობა ამგვარ ქმედებას კიბერდანაშაულად არ მიიჩნევს. ამგვარად, კიბერდანაშაულის მასშტაბის

115. იხილეთ „საქართველოს ჟურნალისტური ეთიკის ქარტიის ქცევის კოდექსი“, 1 ივნისი 2019, < https://www.qartia.ge/ka/dokumentebi/article/36725-saqarthvelos-zhurnalisturi-ethikis-qartiis-qcevis-kodeqsi>, ბოლოს ნანახია: 30 მაისი 2023.

აღქმა მთავრობისა და მოსახლეობის მიერ მნიშვნელოვნად განსხვავდება ერთმანეთისგან.

რეკომენდაცია: პარლამენტის იურიდიულ საკითხთა კომიტეტმა და შინაგან საქმეთა სამინისტროს იმ უწყებებმა, რომლებიც პოლიტიკის დაგეგმვისა და შემუშავების პროცესს წარმართავენ, უნდა შეისწავლონ სისხლის სამართლის კოდექსში ცვლილებების შეტანის საკითხი, რათა შესაბამის მუხლებში ჯეროვნად იქნეს გათვალისწინებული და ასახული კიბერ მეთოდებით ჩადენილი დანაშაულის ასპექტები. პარლამენტის იურიდიულ საკითხთა კომიტეტმა და შინაგან საქმეთა სამინისტროს შესაბამისმა უწყებებმა უნდა განახორციელონ ინიციატივები, რომელთა ფარგლებშიც გათვალისწინებული უნდა იყოს სისხლის სამართლის კოდექსის ზოგიერთი მუხლის ცვლილება, რათა კოდექსში ნახსენები იყოს კიბერ, ციფრული ან ონლაინ მეთოდები. ამგვარი ინიციატივები უნდა ემსახურებოდეს იმის დადგენას, თუ რამდენად არის შესაძლებელი ან სასურველი კიბერ მეთოდებით ჩადენილი დანაშაულის ასპექტების უკეთ გამოვლენა და აღიარება. ამგვარი ცვლილება თანხვედრაში იქნება საქართველოს კიბერუსაფრთხოების ეროვნულ სტრატეგიასთან, რომლის მიხედვითაც „კიბერ“ ელემენტი ... ხელს უწყობს სხვადასხვა დანაშაულებრივი ქმედების ჩადენას ... და წარმოადგენს დანაშაულის ჩადენის დამხმარე საშუალებას“, რაც სცილდება კიბერდანაშაულის „ვიწრო, კლასიკურ გაგებას“.[116]

მიგნება 5: უმაღლესი განათლების დონეზე არასაკმარისია კიბერუსაფრთხოების განათლების მიღებისა და მომზადების შესაძლებლობები

რეკომენდაცია: გაფართოვდეს კიბერუსაფრთხოებისა და კიბერდანაშაულის საკითხებში უმაღლესი განათლების შესაძლებლობები. მთავრობამ დახმარება უნდა გაუწიოს უნივერსიტეტებს, დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემიასა და სხვა სასწავლო დაწესებულებებს, რათა მათ შეძლონ შესაბამისი პროგრამებისა და აკადემიური თუ სამეცნიერო ხარისხების შეთავაზება კიბერუსაფრთხოებისა და კიბერდანაშაულის სფეროებში. ამ მიზნით მთავრობას შეუძლია, მაგალითად, სპონსორობა გაუწიოს ახლადშემუშავებულ კიბერუსაფრთხოების პროგრამას. ამგვარი მიდგომა საშუალებას მისცემს მთავრობას, რეაგირება მოახდინოს კიბერუსაფრთხოებისა და ზოგადად, კომპიუტერული ტექნოლოგიების მიმართულებით დასაქმების გენდერულ დისბალანსზე, მაგალითად, ქალებისთვის დამატებითი სასტიპენდიო სქემების შეთავაზების მეშვეობით. ამ მხრივ, საწყის ეტაპზე ყურადღება უნდა მიექცეს სამაგისტრო დონის განათლების შესაძლებლობებს, როგორც ეს ნათქვამია საქართველოს კიბერუსაფრთხოების ეროვნულ სტრატეგიაში. უფრო კონკრეტულად კი, სტრატეგიაში ნათქვამია, რომ „საბაკალავრო და სამაგისტრო კურსები უნდა დამკვიდრდეს საქართველოში აკრედიტებულ სასწავლებლებში.“ [117]

116. საქართველოს მთავრობა, „საქართველოს ეროვნული კიბერუსაფრთხოების სტრატეგია“, გვ. 13
117. იქვე, გვ. 16.

მიგნება 6: მოქალაქეების მიერ კიდებერდანაშაულის, იქნება ეს დაზარალებულის აღქმით კლასიკური თუ კიბერ მეთოდებით ჩადენილი დანაშაული, მიმართვიანობის სტატისტიკა საკმაოდ დაბალია, რაც განპირობებულია შემდეგი მიზეზებით:

- ინფორმაციის ნაკლებობა იმასთან დაკავშირებით, თუ რას გულისხმობს კიბერდანაშული და რა ქმედებებს ენიჭება კიბერდანაშაულის კვალიფიკაცია;
- ინფორმაციის ნაკლებობა მიმართვიანობის ოფიციალური მექანიზმების შესახებ: სად და როგორ ხდება მიმართვიანობა, როგორ უნდა შეინარჩუნონ/შეინახონ მტკიცებულებები და რა სახის დახმარება არის ხელმისაწვდომი. ეს პრობლემა განსაკუთრებით მწვავეა მშობლებისთვის, რომლებსაც უჭირთ გარკვევა, თუ ვის და როგორ უნდა მიმართონ, როდესაც მათი შვილები კიბერდანაშაულის მსხვერპლები ხდებიან
- დაბალი ნდობა პოლიციის შესაძლებლობების მიმართ, განსაკუთრებით, სოფლად მცხოვრებ მოსახლეობაში, როდესაც საქმე მიმართვიანობის ფაქტებზე რეაგირებას ეხება;
- პოლიციის მიერ მიწოდებული ინფორმაციის პასუხისმგებლობით მოპყრობისა და კონფიდენციალურობის დაცვის მიმართ ეჭვი, რაც განსაკუთრებით მძაფრდება, როდესაც საქმე ეხება კიბერდამნაშავეების მიერ სენსიტიური ან პირადი მონაცემების, მაგალითად, ფოტოსურათების მოპარვისა და ბოროტად გამოყენების ფაქტებს. ქალი-მსხვერპლების შემთხვევაში მიმართვიანობის ალბათობა კიდევ უფრო მცირდება კულტურული და სოციალური სტიგმის გამო.
- როდესაც საქმე მიმართვიანობას ეხება, მოქალაქეები უფრო მეტად ბანკებს ენდობიან, ვიდრე სამართალდამცავ უწყებებს.

რეკომენდაცია: ადგილობრივი პოლიციის თანამშრომლებისთვის კურსების ჩატარება კლასიკური და კიბერ მეთოდებით ჩადენილი დანაშაულის, ასევე, ზიანის შემცველი ონლაინ აქტივობის მსხვერპლებისთვის სათანადო დახმარების აღმოჩენის შესახებ. მიუხედავად იმისა, რომ გარკვეული ნაბიჯები გადაიდგა კიბერდანაშაულთან გამკლავების მიმართულებით, მსხვერპლზე ორიენტირებული ღონისძიებები ჯერ კიდევ არაპრიორიტეტულად რჩება. ადგილობრივი სამართალდამცავი უწყებებისთვის სასარგებლო იქნებოდა ტრენინგი სენსიტიური და კონფიდენციალური მონაცემების შეგროვებისა და კიბერდანაშაულისა და ზიანის მომტანი ონლაინ აქტივობების (ანუ, კიბერდანაშაულის მისი ფართო გაგებით) მსხვერპლების მოპყრობის შესახებ. ტრენინგის ფარგლებში განსაკუთრებული ყურადღება უნდა მიექცეს კიბერ მეთოდებით ჩადენილ დანაშაულებსა და ზიანის მომტან ონლაინ აქტივობებთან დაკავშირებულ სენსიტიურობასა და იმ ფაქტს, რომ ამგვარი დანაშაულის სამიზნეები ყველაზე მეტად ქალები და ბავშვები ხდებიან. ტრენინგები მიზნად უნდა ისახავდნენ ადგილობრივი პოლიციის თანამშრომლების შესაძლებლობებს, რაც, თავის მხრივ, ხელს შეუწყობს მიმართვიანობის მაჩვენებლის გაზრდასა და დანაშაულების შესახებ მონაცემების შეგროვებას. ამ აქტივობების განხორციელების

პროცესში განსაკუთრებული ყურადღება უნდა დაეთმოს პოლიციის მიერ შესაბამისი პროცედურების ზედმიწევნით დაცვას ან მათ გაუმჯობესებას იმგვარად, რაც გაამართლებს ქალების მოლოდინებს მათი პირადი ინფორმაციის და კონკრეტული საქმის მასალების კონფიდენციალურობის დაცვასთან დაკავშირებით, ხოლო იმ შემთხვევაში, თუ ეს ასე არ ხდება, მათ უნდა იცოდნენ, რომ მოქმედებს ანგარიშვალდებულების ეფექტიანი სისტემა, რაც უზრუნველყოფს მსხვერპლებთან დაკავშირებული მონაცემების დაცულობას.

მიგნება 7: კიბერუსაფრთხოების ეკოსისტემაში სერტიფიცირებული/კვალიფიციური პერსონალის ნაკლებობა, რომლებიც მუშაობენ განსაკუთრებულად სენსიტიურ საკითხებზე.

რეკომენდაცია: საერთაშორისო დონორმა ორგანიზაციებმა, რომლებიც აფინანსებენ კიბერუსაფრთხოების კვალიფიკაციის მინიჭებისა და სერტიფიკაციის აქტივობებს, მეტი რისკი უნდა გაწიონ. კიბერშესაძლებლობების განვითარების კუთხით მომუშავე საერთაშორისო დონორებმა მხარი უნდა დაუჭირონ კვალიფიკაციასა და სერტიფიკაციაზე წვდომას, რაც, მოცემულ პირობებში, დეფიციტურია საქართველოს ეკოსისტემისთვის. ამჟამად, დონორები მეტად ფრთხილობენ რისკებთან დაკავშირებით და მხარს, ძირითადად, ისეთ სქემებს უჭერენ, რომლებიც წარუმატებლობის დაბალი ალბათობით გამოირჩევიან, ხოლო სენსიტიურ თემებს თავს არიდებენ. დაფინანსების მოცულობის ზრდას მაღალი რისკის შემცველ კვალიფიკაციის/სერტიფიკაციის პროგრამებისთვის თან უნდა ახლდეს მონიტორინგის, შეფასებისა და სწავლის ღონისძიებები. გარდა ამისა, საჭიროა დაფინანსებულ კურსებთან დაკავშირებით რისკების ჰოლისტური შეფასების განხორციელება, მათ შორის, ისეთ საკითხებთან დაკავშირებით, როგორიცაა ეთიკური და იურიდიული ფაქტორების გათვალისწინების ხარისხი. კურსების თემატიკის განსაზღვრა უნდა დაეფუძნოს კიბერუსაფრთხოების ეროვნული სტრატეგიის მე-3.1 ამოცანას, ხოლო დამატებითი თემების გამოვლენისთვის გამოყენებული უნდა იქნეს მონაწილეობითი და საჭიროებებზე დაფუძნებული მიდგომა.[118]

მიგნება 8: საქართველოში კიბერდანაშაულის შესახებ მონაცემები მწირია

რეკომენდაცია: შინაგან საქმეთა სამინისტრომ უნდა ჩაატაროს კიბერდანაშაულების ცდომილების ყოველწლიური ანალიზი იმ მახასიათებლების მიხედვით, რომლებიც აძლიერებს მოწყვლადობის რისკს და შედეგები საჯაროდ გამოაქვეყნოს. სამინისტროს საინფორმაციო-ანალიტიკური დეპარტამენტის ანალიტიკური განყოფილების დანაშაულის ანალიზის სამმართველო ყოველწლიურად უნდა გაანალიზოს დანაშაულის სტატისტიკა რეგიონის, სქესის, დასაქმების სტატუსისა და ასაკის მიხედვით. ამ ფუნქციის მხარდასაჭერად, მნიშვნელოვანია დანაშაულის ანალიზის სამმართველოსთვის შესაბამისი რესურსების გამოყოფა. ამ ღონისძიების

118. იგივე, გვ. 20

სასურველი შედეგი გულისხმობს საზოგადოების ცნობიერების ამაღლებას კიბერდანაშაულის კონკრეტული საფრთხეების შესახებ. ასევე, ბიზნესკომპანიებსა და ორგანიზაციებს შეეძლებათ უკეთ მოემზადონ კიბერსაფრთხეებთან გასამკლავებლად, ხოლო სამოქალაქო საზოგადოების ორგანიზაციებს უკეთ შეეძლებათ განსაზღვრონ, თუ ვის და რა სახის დახმარება ესაჭიროება. ეს რეკომენდაცია თანხვედრაშია საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგიის 2.2 ამოცანასთან, რომელიც გულისხმობს კიბერდანაშაულთან წინააღმდეგ ბრძოლის ეფექტიანი სისტემის განვითარებას, რადგან რეკომენდაციით გათვალისწინებული მონაცემების ანალიზი ხელს უწყობს კიბერდანაშაულის წინააღმდეგ გასატარებელი ღონისძიებების უკეთ ორგანიზებას.[119]

მიგნება 9: მშობლებს უჭირთ შვილების დაცვა სხვადასხვა სახის კიბერდანაშაულისა და კიბერზიანისგან, როდესაც საქმე ინტერნეტის სახლში მოხმარებას ეხება.

რეკომენდაცია: ინტერნეტის მიმწოდებლებმა მომხმარებლებს უნდა შესთავაზონ მშობლებისთვის უსაფრთხოების კონტროლი, როგორც სტანდარტული პაკეტის ნაწილი. მთავრობამ ან საქართველოს კომუნიკაციის ეროვნულმა კომისიამ უნდა გაითვალისწინოს ინტერნეტის მიმწოდებლებისთვის ბავშვების კონტროლის საოჯახო ფართოზოლოვან პაკეტში სავალდებულო მოთხოვნად შემოღების საკითხი დამატებითი საფასურის გარეშე.

119. იგივე. გვ. 18.

დასკვნა

ანგარიშში წარმოდგენილი ანალიზი გვიჩვენებს, რომ ბოლო წლებში საქართველოს მთავრობამ გარკვეულ, თუმცა, მცირე წარმატებას მიაღწია კიბერდანაშაულთან გამკლავების მიმართულებით. კოორდინირებული ძალისხმევის შედეგად ცვლილებები შევიდა საქართველოს სისხლის სამართლის კოდექსში, გაიზარდა პოლიციის შესაძლებლობები და დამყარდა თანამშრომლობითი ურთიერთობები კერძო სექტორთან კიბერდანაშაულის ყველაზე გავრცელებული ფორმების პრევენციისა და მათზე რეაგირების მიზნით. ხსენებული ძალისხმევის წარმატების დასტურად მთავრობის წარმომადგენლებს მოჰყავთ შეტყობინებული კიბერდანაშაულის კლების ტენდენცია, თუმცა, ეს ცვლილებები არ ასახავს სრულ სურათს. საქართველოს სისხლის სამართლის კოდექსით გათვალისწინებული კიბერდანაშაულის მაჩვენებლის კლება უკავშირდება მხოლოდ კლასიკურ კიბერ დანაშაულს და მთლიანად დამოკიდებულია მსხვერპლის არჩევანზე, განაცხადონ მომხდარი დანაშაულის შესახებ. კვლევის ფარგლებში ჩატარებული ფოკუსჯგუფების შედეგების ანალიზი მოწმობს, რომ ხშირია კიბერ მეთოდებით ჩადენილი დანაშაულები და ზიანის შემცველი ონლაინ აქტივობები, რომლებიც, განსაკუთრებით, მოწყვლად ჯგუფებს ემუქრება. ასევე, შეინიშნება მკვეთრად გამოხატული განსხვავება მიმართვიანობის პრაქტიკებში.

კიბერდანაშაულის მიმართ საქართველოს მედეგობასა და მთავრობის მიერ პრობლემის მასშტაბის გასიგრძეგანების უნარს რამდენიმე ფაქტორი ასუსტებს, მათ შორის: ცნობიერების დაბალი დონე, კიბერდანაშაულის განსაზღვრებასა და აღქმას შორის არსებული შეუსაბამობები და მიმართვიანობის წახალისების მექანიზმების არარსებობა.

კიბერდანაშაულის საფრთხეების შესახებ ცნობიერების დაბალი დონე საერთო პრობლემაა და განსაკუთრებით მოწყვლად ჯგუფებში შეინიშნება, მათ შორის, ბავშვებში, ხანდაზმულ და სოფლად მცხოვრებ მოსახლეობასა და ეთნიკური უმცირესობების ჯგუფებში, რომლებიც სათანადოდ ვერ ფლობენ ქართულს. შედეგად, არათანაბრად არის განაწილებული კიბერდანაშაულის რისკების მართვის ცოდნა და კიბერჰიგიენის ხარისხი, რაც, ზოგადად, დაბალია. მიუხედავად იმისა, რომ საქართველო, ამ მხრივ, გამონაკლისი არ არის, არსებული სიტუაცია კიდევ უფრო ამძიმებს ეროვნულ დონეზე არსებულ რისკებს, რომლებიც კიდევ უფრო გაიზრდება სხვადასხვა საფრთხის - იქნება ის ინდივიდუალურ თუ ორგანიზაციულ დონეზე, აღმოცენების გზადაგზა. შესაბამისად, კიბერდანაშაულის გამოცდილება ხშირად უკავშირდება მოქალაქეების მიერ მათ წინაშე მდგარი რისკების ან საფრთხეების ამოცნობის უუნარობას და შედეგად, მისით გამოწვეულ გაურკვევლობას ან გაუგებრობას.

კიბერდანაშაულის ინტუიციური გაგება საზოგადოებაში - იგულისხმება, როგორც კიბერ მეთოდებით ჩადენილი დანაშაულები, ასევე, ზიანის შემცველი ონლაინ

აქტივობები, მაგალითად, კიბერბულინგი და ონლაინ თაღლითობა, არ შეესაბამება იმ განსაზღვრებებს, რომლებითაც ხელმძღვანელობს სისხლის სამართლის კოდექსი და რომლის მიხედვითაც კიბერდანაშაული შემოიფარგლება მხოლოდ კლასიკური კიბერდანაშაულის სამართალდარღვევებით და არ შეიცავს მკაფიო დებულებებს სხვა კიბერ მეთოდებით ჩადენილი დანაშაულების ასპექტებისთვის. ეს განსხვავება ნათლად ასახავს იმ შეუსაბამობას კიბერდანაშაულის მიმართ, რომელიც მთავრობის ხედვასა და საზოგადოებრივ წარმოდგენაში არსებობს. ამგვარი შეუსაბამობა, როგორც ასეთი, თავისთავად პრობლემას არ წარმოადგენს, იგი ზეგავლენას ახდენს იმაზე, თუ როგორ აღიქვამს მოსახლეობა მთავრობის მცდელობას და მიუთითებს იმ სფეროებსა და საკითხებზე, რომლებიც საზოგადოების თვალში ყველაზე მეტად მოწყვლადია და შესაბამისად, ყველაზე მეტ ყურადღებას საჭიროებს.

მიმართვიანობის დაბალი მაჩვენებელი ხელს უშლის მთავრობას, უფრო ნათელი წარმოდგენა შეექმნას პრობლემის მასშტაბის შესახებ. მიმართვიანობის ხელშემშლელ ფაქტორებს შორისაა, უპირველეს ყოვლისა, ცნობიერების დაბალი დონე: ადამიანები ხშირად ვერ ხვდებიან, რომ კიბერდანაშაულის მსხვერპლები გახდნენ; მათ არ იციან, როგორ უნდა განაცხადონ მომხდარის შესახებ და როგორ დაიცვან მტკიცებულებები. ეს გაურკვევლობა, ნაწილობრივ, მიმართვიანობის მაჩვენებელზეც ახდენს გავლენას. სხვა მნიშვნელოვან ფაქტორებს შორისა უნდობლობაც, რომელსაც, თავის მხრივ, ორი ასპექტი აქვს: ადამიანებს სჯერათ, რომ მთავრობას, ამ კონკრეტულ შემთხვევაში, სამართალდამცავი უწყებებს, არ აქვთ საკმარისი უნარი, აწარმოონ კიბერდანაშაულის გამოძიება. ისინი წუხან, რომ ისინი, ვისაც აბარია მათი საქმეების გამოძიება, არ დაიცავენ კონფიდენციალურობას ან გაამჟღავნებენ პირად მონაცემებს. ეს განცდა განსაკუთრებით მძაფრად იგრძნობა სოფლად მცხოვრებ ჯგუფებში. შესაბამისად, კიბერდანაშაული ხშირად აღიქმება როგორც პირადი ტვირთი, რომლის შესამსუბუქებლადაც ადამიანებს ხელი არ მიუწვდებათ სამართალდამცავ ორგანოების მხარდაჭერაზე.

ხსენებული პრობლემების მოგვარება მთავრობისგან მოითხოვს ძლების გაერთიანებას, დეპარტამენტებში არსებული რესურსების გამოყენებას, ასევე კერძო სექტორისა და სამოქალაქო საზოგადოების წარმომადგენლებთან თანამშრომლობას. პირველ რიგში, სახელმწიფომ უნდა დაგეგმოს და განახორციელოს ცნობიერების ამაღლების ამბიციური კამპანია ეროვნულ დონეზე ცნობიერების ამაღლებისა და საზოგადოების მედეგობის გაძლიერების მიზნით. კამპანია ასევე უნდა ემსახურებოდეს ნდობის განმტკიცებას, რათა სამართალდამცავმა ორგანოებმა შეძლონ მოსახლეობისათვის მსხვერპლებზე და მათ საჭიროებაზე ორიენტირებული დახმარების გაწევა. გარდა ეროვნულ დონეზე განსახორციელებელი კამპანიისა, საჭიროა სხვა საქმიანობის განხორციელებაც, მაგალითად, უმაღლესი განათლების შესაძლებლობების შექმნა კიბერუსაფრთხოების მიმართულებით, პოლიციის დეპარტამენტებისთვის მიზნობრივი ტრენინგის ჩატარება და ინტერნეტ სერვისის მიმწოდებლების

დავალდებულება მშობლების მიერ ბავშვების უსაფრთხოების მექანიზმების ინტეგრირებისთვის, როგორც მინიმალურად აუცილებელი სტანდარტი. ეს ზომები ხანგრძლივი ვადის განმავლობაში განამტკიცებს საერთო მედეგობას კიბერდანაშაულების მიმართ.

კვლევის ფარგლებში ყურადღება არ გამახვილებულა რამდენიმე ისეთ საკითხზე, რომლებიც აუცილებლად უნდა გაითვალისწინოს ხელისუფლებამ, მაგალითად, მწარმოებლებისა და მიმწოდებლებისთვის კიბერუსაფრთხოების მოთხოვნების დავალდებულება, რათა მოხდეს კიბერუსაფრთხოების რისკის აცილება მომხმარებლებისთვის, მრავალმხრივი თანამშრომლობის განვითარება საერთაშორისო კიბერდანაშაულზე რეაგირებისთვის და აქცენტი საწარმოებზე. ბოლო საკითხი განსაკუთრებულად მნიშვნელოვანია კიბერუსაფრთხოების უზრუნველყოფისთვის საქართველოს ეკონომიკის მზარდი დიგიტალიზაციის ფონზე.

კიბერსაფრთხეების და კიბერდანაშაულების მზარდი დინამიკის ფონზე, როდესაც ამგვარი დანაშაულების მასშტაბი და ზეგავლენის არეალი ფართოვდება, ხოლო რეგიონული უსაფრთხოების კონტექსტი კვლავ დაძაბულია, საქართველომ უნდა გამოიყენოს შესაძლებლობა და განავითაროს საკუთარი შესაძლებლობები სამომავლო მზაობისთვის. ამისთვის სახელმწიფომ უნდა დანერგოს "ერთიანი საზოგადოებრივი" მიდგომა და აღიაროს, რომ კიბერუსაფრთხოების შესაძლებლობები და ცოდნა კერძო სექტორშია კონცენტრირებული. ამ ზომების გატარება გააძლიერებს საქართველოს, როგორც კიბერუსაფრთხო ქვეყნის მედეგობას და გააძლიერებს მის თავდაცვის უნარიანობას კიბერსაფრთხეების წინაშე, ასევე დაუმკვიდრებს მას კიბერუსაფრთხოების სფეროში რეგიონული ლიდერის რეპუტაციას.

ავტორების შესახებ

ჯოზეფ იარნეცკი RUSI-ის კიბერსაკითხებზე მომუშავე გუნდის მკვლევარია. მისი გამოცდილება მოიცავს ისეთ საკითხებს, როგორიცაა, კიბერშესაძლებლობების განვითარება, კიბერდანაშაულით გამოწვეული ზიანი, ახალი ტექნოლოგიების გამოწვეული შესაძლო საფრთხეები და შესაძლებლობები, კიბერთავდასხმა გამოსასყიდის გამოძალვის მიზნით ("ransomware") და კიბერსტრატეგიებისადმი მულტიაქტორული მიდგომები. ამჟამად, მისი ძირითადი საკვლევი თემა ეხება კიბერდანაშაულის გამოცდილებას, ტექკომპანიების როლს კიბერთავდაცვის ეროვნულ სისტემებში, ახალ ტექნოლოგიებთან დაკავშირებულ შესაძლებლობებს და რისკებს. მისი განსაკუთრებული ინტერესის სფეროა პასუხისმგებლობა და მისი როლი კიბერუსაფრთხოების მიმართ "ერთიანი საზოგადოებრივი" მიდგომის დანერგვაში.

ნათია სესკურია უსაფრთხოების კვლევების რეგიონული ინსტიტუტის დამფუძნებელი და აღმასრულებელი დირექტორია. ინსტიტუტი, რომელიც თბილისში ახორციელებს საქმიანობას, RUSI-ს ოფიციალური პარტნიორია. ნათია, ასევე RUSI-ს ასოცირებული მკვლევარია. ნათია ასევე არის Chatham House-ში მრჩეველი და რუსეთის პოლიტიკის ლექტორი. ნათიას ფართო გამოცდილება აქვს პოლიტიკის და სტრატეგიული დაგეგმვის მიმართულებით, ასევე თავდაცვისა და უსაფრთხოების საკითხების ანალიზში. წარსულში იგი მუშაობდა საქართველოს ეროვნული უსაფრთხოების საბჭოსა და თავდაცვის სამინისტროში. მისი საკვლევი ინტერესები მოიცავს ისეთ საკითხებს, როგორიცაა რუსეთის შიდა და საგარეო პოლიტიკა, განსაკუთრებით, რუსეთის ფედერაციის ურთიერთობა მეზობელ ქვეყნებთან და მისი სტრატეგიული მიდგომა ოკუპირებული რეგიონებისა და დასავლეთის ქვეყნების მიმართ. ნათიას ხშირად იწვევენ კომენტარისთვის წამყვანი მედიასაშუალებები, მათ შორის BBC, France 24 და CNN.

თათია ჩიხლაძე უსაფრთხოების კვლევების რეგიონული ინსტიტუტის მკვლევარი და საქართველოში ბრიტანული უნივერსიტეტის ასოცირებული პროფესორია. მის კვლევითი ინტერესები მოიცავს ისეთ საკითხებს, როგორიცაა შავი ზღვის რეგიონული უსაფრთხოება, ჰიბრიდული ომი და პოსტსაბჭოთა ავტორიტარული რეჟიმების მედეგობა. თათიას ანალიტიკური საქმიანობის მდიდარი გამოცდილება აქვს, მათ შორის საქართველოს საჯარო უწყებებშიც, მაგალითად, ეროვნული უსაფრთხოების საბჭოში, შერიგებისა და სამოქალაქო თანასწორობის საკითხებში საქართველოს სახელმწიფო მინისტრის აპარატსა და შინაგან საქმეთა სამინისტროში. თათიამ დოქტორის ხარისხი გერმანიაში, ბრემენის უნივერსიტეტში დაიცვა. გარდა ამისა, მოპოვებული აქვს სოციალური მეცნიერებების მაგისტრის აკადემიური ხარისხი ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტისგან, ხოლო რუსეთისა და აღმოსავლეთ ევროპულ საკითხებში - ოქსფორდის უნივერსიტეტისგან.