ხათუნა მშვიდობაძე

საქართველოს კიბერბარომეტრი

ანბარიში

თბილისი
2015

British Embassy Tbilisi

Foreign & Commonwealth Office

NCA National Crme Agency

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

საქართველოს კიბერბარომეტრი *ანგარიში*

ხათუნა მშვიდობაძე

მომზადებულია ბრიტანეთის საელჩოსათვის თბილისში და დანაშაულის წინააღმდეგ ბრძოლის ბრიტანეთის ეროვნული სააგენტოსთვის

რედაქტორები: **დევიდ სმითი, რუსუდან მარგიშვილი**

ტექნიკური რედაქტორი: **ნინო ყაველაშვილი**

ISBN 978-9941-0-8228-3

წინასიტყვაობა

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი წარმოგიდგენთ ჩვენი ფონდის უფროსი მეცნიერ-თანამშრომლის, კიბერსაკითხების სპეციალისტის, ქალბატონ ხათუნა მშვიდობაძის ნაშრომს – „საქართველოს კიბერბარომეტრი – ანგარიში“. ეს არის საქართველოს უსაფრთხოების, ეკონომიკური განვითარებისა და ევროპაში ინტეგრაციისათვის სასიცოცხლო მნიშვნელობის საკითხის – ჩვენი სახელმწიფოს კიბერუსაფრთხოების – ვრცელი მიმოხილვა. ანგარიშში კარგად არის ნაჩვენები, თუ რამდენს მიაღწია საქართველომ კიბერუსაფრთხოების სფეროში, თუმცა მდგომარეობა ობიექტურადაა შეფასებული და მკაფიოდ არის ჩამოყალიბებული ის მიმართულებები, რომლებიც გაუმჯობესებას საჭიროებენ. რაც ყველაზე მნიშვნელოვანია, ანგარიშში მოცემულია კონკრეტული რეკომენდაციები – თუ რა ნაბიჯები უნდა გადადგას საქართველომ კიბერუსაფრთხოების უზრუნველყოფის მიმართულებით.

საქართველო იყო პირველი ქვეყანა, რომელმაც 2008 წელს ერთდროულად განიცადა როგორც კინეტიკური, ისე კიბერშეტევები. იმ დროს საქართველოში ჯერ კიდევ არ იყო ინტერნეტინფრასტრუქტურა და მისი გამოყენება ისე განვითარებული, როგორც დღეს. ახლა ჩვენ გაცილებით უფრო მეტად ვართ დამოკიდებული ინტერნეტზე, რაც განსაზღვრავს ჩვენს მზარდ ეკონომიკურ განვითარებასა და საერთაშორისო ურთიერთობების ჩამოყალიბებას. რაც მეტად შემოდის ჩვენს ყოფაში ინტერნეტი, მით უფრო მეტი ძალისხმევა გვჭირდება, რომ ეს დიდი სიკეთე არ გახდეს ომის, შპიონაჟისა თუ დანაშაულის იარაღი. მთავრობა, ბიზნესი, სამოქალაქო საზოგადოება და ჩვენი უცხოელი პარტნიორები უნდა გაერთიანდნენ კიბერუსაფრთხოების გასაძლიერებლად. ამ თვალსაზრისით, საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი კვლავაც მოწინავე რიგშია 21-ე საუკუნის უსაფრთხოების გამოწვევებთან გასამკლავებლად – ამის დასტურია ხათუნა მშვიდობაძის წარმოდგენილი ანგარიში – „საქართველოს კიბერბარომეტრი“.

დაბოლოს, მინდა მადლობა გადავუხადო დიდი ბრიტანეთის მთავრობას, კერძოდ, დიდი ბრიტანეთისა და ჩრდილოეთ ირლანდიის გაერთიანებული სამეფოს საელჩოს საქართველოში და დანაშაულის წინააღმდეგ ბრძოლის ბრიტანეთის ეროვნულ სააგენტოს გაწეული მხარდაჭერისთვის. მათ პროექტს აღმოუჩინეს არა მხოლოდ ფინანსური დახმარება, არამედ ითავეს ინტელექტუალური ხელმძღვანელობაც იმ იდეის წარმოსაჩენად, რომ საერთაშორისო თანამშრომლობა განსაზღვრავს ზოგადად კიბერუსაფრთხოების გაუმჯობესებას. დიდ იმედს ვიტოვებთ, რომ ჩვენი და დიდი ბრიტანეთის თანამშრომლობა შემდგომშიც გაგრძელდება.

ეკა მეტრეველი
საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდის აღმასრულებელი დირექტორის მოვალეობის შემსრულებელი

ინტერნეტი სულ უფრო მეტად ერთვება თანამედროვე ცხოვრებაში. ონლაინსივრცეში ინაცვლებს მთავრობა, რომელიც ჩვენს სამსახურში დგას, სამხედროები, რომლებიც ჩვენ გვიცავენ, ეკონომიკა, რომელიც ჩვენ გვეხმარება და გვაძლიერებს და კომუნიკაციების ინდუსტრია, რომელიც ხელს გვიწყობს, რომ შევინარჩუნოთ ურთიერთობები და კავშირები. კიბერსივრცე უდიდეს შესაძლებლობებს გვიშლის, თუმცა მას თან მრავალი რისკიც ახლავს.

ბრიტანეთი ესწრაფვის ისეთ კიბერსივრცეს, სადაც მოქალაქეებს მიეცემათ საშუალება სრულფასოვნად გამოიყენონ მისი შესაძლებლობები – როცა ყოველგვარი მანძილის, დროის, ენობრივი და სხვა კულტურული ბარიერების გარღვევით მოხდება ურთიერთობების დამყარება, ბიზნესის კეთება, მეგობრებისა დ კონტაქტების ქსელის გაზრდა და ამგვარად შეძლებენ მოქალაქეები თავიანთი ცხოვრების გაუმჯობესებას, შესაძლებლობების გაზრდასა და ჩანაფიქრების განხორციელებას. ყოველივე ეს მოითხოვს ეფექტური მექანიზმების შემოღებას, რათა შემცირდეს რისკები და ხელი შეეშალოს თავისუფალი კიბერსივრცის ბოროტად გამოყენებას – ამ სივრცეში სამართალდამცავები ამარცხებენ კრიმინალებს, აქ მოქალაქეებმა იციან, როგორ დაიცვან თავი; კიბერსივრცე არის არა მარტო ეფექტური, არამედ უსაფრთხო საშუალება ბიზნესისთვის; საჯარო ონლაინსერვისები დაცული და მდგრადია, ხოლო იმ გამოწვევების დაძლევა, რომლებიც საფრთხეს უქმნის ეროვნულ ინფრასტრუქტურას, ეროვნულ უსაფრთხოებასა თუ პირად კეთილდღეობას, შესაძლებელია.

„საქართველოს კიბერბარომეტრი – ანგარიში“ ნათლად ასახავს საქართველოს კიბერუსაფრთხოების სურათს. ანგარიშში წარმოდგენილია, თუ რას აკეთებს საქართველო თავისი მოქალაქეების, საქმიანობისა და მნიშვნელოვანი ეროვნული ინფრასტრუქტურის დასაცავად და მოცემულია რეკომენდაციები, რაც საჭიროა გაკეთდეს სამომავლოდ. იმ სფეროში, სადაც ტექნოლოგიების განვითარება სწრაფი ტემპით მიმდინარეობს, ეფექტური რეაგირებისათვის საჭიროა თანმიმდევრული, ფართო და მზარდი ძალისხმევა.

აქვე მინდა პატივისცემა გამოვხატო ხათუნა მშვიდობაძის მიმართ, რომელმაც ორწლიანი თავდაუზოგავი შრომა ჩადო ამ ანგარიშის შესაქმნელად. ასევე მინდა მადლობა გადავუხადო ყველა იმ ადამიანს, რომელთაც თავისი წვლილი შეიტანეს ანგარიშის შექმნის პროცესში, მათი გულწრფელი მისწრაფებისა და მუდმივი ძალისხმევისთვის დაიცვან საქართველოს მოსახლეობა კიბერსივრცეში.

ალექსანდრა ჰოლ ჰოლი

დიდი ბრიტანეთისა და ჩრდილოეთ ირლანდიის გაერთიანებული სამეფოს საგანგებო და სრულუფლებიანი ელჩი საქართველოში

სარჩევი

პროექტის შესახებ

„საქართველოს კიბერბარომეტრი“ არის ანგარიში, რომელიც წარმოადგენს საქართველოში კიბერდანაშაულსა და კიბერსაფრთხეებზე რეაგირებასთან დაკავშირებულ საკითხთა ანალიზს. ანგარიში მოამზადა საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდის საქართველოს უსაფრთხოების ანალიზის ცენტრის კიბერსაკითხების ექსპერტმა ხათუნა მშვიდობაძემ. სამუშაო შესრულდა საქართველოში ბრიტანეთის საელჩოს ძალისხმევითა და დანაშაულის წინააღმდეგ ბრძოლის ბრიტანეთის ეროვნული სააგენტოს ინიციატივით.

ანგარიშის მიზანია გამოავლინოს კიბერსაფრთხეებთან დაკავშირებით ქვეყანაში არსებული პრობლემები და მათზე რეაგირებისა და ბრძოლის ძლიერი და სუსტი მხარეები. ანგარიშში ასახულია საქართველოში ინტერნეტტექნოლოგიებზე დამოკიდებულებისა და ზრდის მაჩვენებელი, კიბერდანაშაულის დონე და ტიპები, სამართალდაცვის შესაძლებლობები, ქმედებები, ინტერნეტთან დაკავშირებული კრიტიკული ინფრასტრუქტურის უსაფრთხოების ზომები, ეკონომიკური და სოციალური პერსპექტივები, შეფასებები და სამომავლო მოქმედებისათვის საჭირო მითითებები. „საქართველოს კიბერბარომეტრი“ არის ერთგვარი გზამკვლევი, რომელიც წარმოადგენს რეკომენდაციების ჩამონათვალს და რომელიც ხელს შეუწყობს ბრიტანეთის მთავრობის ძალისხმევას დაეხმაროს საქართველოს კიბერსაფრთხეებთან გამკლავების საქმეში.

ქვეყნის კიბერუსაფრთხოების მდგომარეობის დასადგენად ჩატარდა საფუძვლიანი კვლევა, რომელიც მოიცავს ინტერვიუებს ადგილობრივ კიბერექსპერტებთან, კერძო ბიზნესისა და სამთავრობო სტრუქტურების იმ წარმომადგენლებთან, რომლებიც პასუხისმგებელი არიან ქვეყნის კიბერუსაფრთხოებაზე.

ანგარიშის მომზადების პროცესში გაწეული დახმარებისათვის დიდ მადლობას მოვახსენებთ ქვემოთ ჩამოთვლილ ყველა პირსა და ორგანიზაციას. ინტერვიუები აღებულია 2014-2015 წლებში და ამდენად, ყველა მოხსენიებულ პირს მითითებული აქვს ამ პერიოდისათვის არსებული თანამდებობრივი მდგომარეობა:

- **ირაკლი წიკლაური**, ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველოს უფროსი, საქართველოს შინაგან საქმეთა სამინისტრო;
- **ტარიელ ალავიძე**, ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველოს ყოფილი უფროსი, საქართველოს შინაგან საქმეთა სამინისტრო;
- **ივანე კაციტაძე**, ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველოს უფროსის მოადგილე, საქართველოს შინაგან საქმეთა სამინისტრო;
- **ოთარ გაბადაძე**, ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველოს უფროსის ყოფილი მოადგილე, საქართველოს შინაგან საქმეთა სამინისტრო;

- **არამ პანიანი**, დეტექტივი, ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველო, საქართველოს შინაგან საქმეთა სამინისტრო;
- **გიორგი პირველი**, გამომძიებელი, ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველო, საქართველოს შინაგან საქმეთა სამინისტრო;
- **შალვა კვინიხიძე**, საერთაშორისო ურთიერთობათა დეპარტამენტის უფროსი, შინაგან საქმეთა სამინისტრო;
- **მარიამ გოგორელიანი**, პროკურორი, შინაგან საქმეთა სამინისტროს გენერალურ ინსპექციაში, ცენტრალური კრიმინალური პოლიციის დეპარტამენტსა და საპატრულო პოლიციის დეპარტამენტში გამოძიების საპროცესო ხელმძღვანელობის დეპარტამენტი, საქართველოს მთავარი პროკურატურა;
- **გიორგი ღიბრაძე**, კრიზისების მართვის ეროვნული ცენტრის დირექტორის მოადგილე, საქართველოს სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო;
- **გიორგი ტიელიძე**, შიდა უსაფრთხოებისა და საჯარო წესრიგის საკითხთა დეპარტამენტის შიდა საფრთხეების ანალიზის სამსახურის უფროსი მრჩეველი, საქართველოს სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო;
- **ირაკლი გვენეტაძე**, თავმჯდომარე, მონაცემთა გაცვლის სააგენტო, საქართველოს იუსტიციის სამინისტრო;
- **ნატა გოდერძიშვილი**, იურიდიული სამმართველოს უფროსი, მონაცემთა გაცვლის სააგენტო, საქართველოს იუსტიციის სამინისტრო;
- **ირაკლი ლომიძე**, ინფორმაციული უსაფრთხოებისა და პოლიტიკის სამმართველოს უფროსი, მონაცემთა გაცვლის სააგენტო, საქართველოს იუსტიციის სამინისტრო;
- **დავით ქვათაძე**, კომპიუტერულ ინცინდენტებზე სწრაფი რეაგირების ჯგუფის ხელმძღვანელი, მონაცემთა გაცვლის სააგენტო, საქართველოს იუსტიციის სამინისტრო;
- **ანდრია გოცირიძე**, კიბერუსაფრთხოების ბიუროს ხელმძღვანელი, საქართველოს თავდაცვის სამინისტრო;
- **ჯემალ ვაშაკიძე**, კომუნიკაციების, IT ტექნოლოგიებისა და ინოვაციების დეპარტამენტის თავმჯდომარის მოადგილე, საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;
- **რამაზ ქვათაძე**, აღმასრულებელი დირექტორი, საქართველოს სამეცნიერო-საგანმანათლებლო კომპიუტერული ქსელების ასოციაცია (გრენა);
- **დავით ტაბატაძე**, სერვისის და პროდუქტების მენეჯერი/CERT ოფიცერი, გრენა;

- **დევიდ ლი**, პრეზიდენტი, მაგთიკომი;
- **ზურაბ ახვლედიანი**, ინფორმაციული უსაფრთხოების ჯგუფის უფროსი, თიბისი ბანკი;
- **ირაკლი ქანდარია**, IT დეპარტამენტის უფროსი, „APM Terminals“, ფოთის საზღვაო პორტი;
- **ნინო სარიშვილი**, საერთაშორისო ურთიერთობებისა და კომუნიკაციების დეპარტამენტის უფროსი, პერსონალურ მონაცემთა დაცვის ინსპექტორის ოფისი.

წინამდებარე ანგარიშში წარმოდგენილი მოსაზრებები ეკუთვნის ავტორს და შესაძლოა არ გამოხატავდეს დანაშაულის წინააღმდეგ ბრძოლის ბრიტანეთის ეროვნული სააგენტოს ან დიდი ბრიტანეთის მთავრობის მოსაზრებებს.

აქვე გვინდა განსაკუთრებული მადლობა მოვახსენოთ ბრიტანეთის საელჩოს წარმომადგენელს, დოქტორ **კრისტოფერ ჯოისს** და ბატონ **კრისტოფერ გოფს** პროექტზე მუშაობის პერიოდში ჩვენთვის გაწეული მხარდაჭერისა და საგულისხმო რჩევებისთვის.

რეზიუმე

მას შემდეგ, რაც ბევრი ჩვენგანის ცხოვრების უდიდესი ნაწილი დამოკიდებული გახდა ინტერნეტტექნოლოგიებზე, ბუნებრივია, ვირტუალურ სამყაროში გადმოინაცვლა სოციალური არსებობის ბნელმა მხარემაც – ნარკოტიკებმა, აზარტულმა თამაშებმა, პროსტიტუციამ, პორნოგრაფიამ, ხულიგნობამ და სხვა მრავალმა დანაშაულმა. ამ თვალსაზრისით გამონაკლისს არც საქართველოს კიბერსივრცე წარმოადგენს, მიუხედავად მისი განსხვავებული მახასიათებლებისა.

გაეროს საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU) მიერ ჩატარებული კვლევის თანახმად, 2014 წელს ინტერნეტით სარგებლობდა ქართველების დაახლოებით 49%. 2014 წლის ოქტომბერში მობილურ ინტერნეტში ჩართული მოსახლეობის რაოდენობა შეადგენდა 1.88 მილიონს. მიუხედავად იმისა, რომ არ არსებობს საქართველოს ოფიციალური ეროვნული სტატისტიკა ელექტრონულ ვაჭრობასა და ონლაინბანკინგში შეღწევადობის შესახებ, ინტერნეტტექნოლოგიებზე დამოკიდებულების მაღალი მაჩვენებელი ერთგვარად განაპირობებს ამ თვალსაზრისით შეღწევადობის ზრდის მაჩვენებელსაც. დღეს უფრო მეტი ადამიანი ფლობს სადებეტო თუ საკრედიტო ბარათებს, ვიდრე უახლოეს წარსულში. საკრედიტო თუ სადებეტო ბარათების მზარდი მოხმარება ბუნებრივად იწვევს ონლაინშესყიდვებისა და ონლაინმიწოდების ინდიკატორის ზრდას. აქედან გამომდინარე, საქართველო უნდა მოემზადოს ფინანსური ონლაინდანაშაულის ზრდასთან საბრძოლველად, რაც თან ახლავს ქვეყნის ეკონომიკურ, კომერციულ განვითარებას და ელექტრონულ კომუნიკაციებზე დამოკიდებულების ზრდას.

კიბერკრიმინალის უკეთ გასაგებად ბრიტანეთის შინაგან საქმეთა სამინისტროსთვის (ანუ ე.წ. British Home Office) მომზადებული ანგარიში განიხილავს კიბერდანაშაულის დიქოტომიას. ბრიტანელები კიბერდანაშაულს ყოფენ ორ კატეგორიად – კიბერდამოკიდებულ დანაშაულად და კიბერშესაძლებელ დანაშაულად. ამერიკელები კი კიბერდანაშაულში მესამე კატეგორიასაც გამოყოფენ – კომპიუტერინციდენტურ დანაშაულს. ასეთ შემთხვევაში კომპიუტერის გამოყენება შესაძლოა ფაქტობრივი დანაშაულისგან პერიფერიულად მოხდეს.

ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულის სამმართველოს წარმომადგენლებმა ჩვენთან საუბრისას განაცხადეს, რომ 2014 წელს საქართველოში რეგისტრირებული კიბერდანაშაულის რაოდენობა დაახლოებით 200 შემთხვევას შეადგენდა. ისეთ პატარა ქვეყანაშიც კი, როგორიც საქართველოა, კიბერდანაშაულის მაჩვენებელი საკმაოდ დაბალია და, სავარაუდოდ, შესაძლოა არასრულყოფილად ასახავდეს კიბერდანაშაულის რეალურ მაჩვენებელს. ამასთანავე, საქართველოში მომხდარი კიბერდანაშაულის უმრავლესობა არ არის არც განსაკუთრებით შემოქმედებითი, არც ტექნოლოგიურად დახვეწილი და არც ძალიან მაღალი რისკების შემცველი. სავარაუდოდ, ალბათ არსებობენ მაღალი ტექნიკური უნარებით დაჯილდოებული ქართველი კიბერკრიმინალები, რომლებმაც იციან რუსული, ინგლისური თუ სხვა ენები და, აქედან გამომდინარე, ისინი შესაძლოა თავიანთ უნარებს იყენებენ კიდეც უფრო სარფიანი მიზნებისათვის. ამასთან, თუკი გავითვალისწინებთ კიბერდანაშაულის ზრდის მსოფლიო ტენდენციას, შეიძლება კიბერდანაშაულის შემთხვევებმა საქართველოშიც უფრო სერიოზული და ხშირი ხასიათი მიიღოს.

ვირტუალურ სამყაროში კიბერდანაშაულთან ერთად ფეხი მოიკიდა კიბერშპიონაჟმა და კიბერომმა და ამ მხრივ არც საქართველოა გამონაკლისი. გასაკვირი არ არის, რომ საქართველოში უპირატესობა უფრო კიბერშპიონაჟისა და კიბერომის წინააღმდეგ ბრძოლას ენიჭება, ვიდრე კიბერკრიმინალის წინააღმდეგ. 2008 წლის შემდეგ საქართველომ ბევრი რამ გააკეთა კიბერუსაფრთხოების შესაძლებლობების გასაუმჯობესებლად, თუმცა ამ მიმართულებით გაცილებით მეტია გასაკეთებელი. კიბერუსაფრთხოებას ჯერ კიდევ ბევრი უყურებს, როგორც ერთ-ერთ რიგით რუტინულ საქმეს, გარდა იმ ადამიანებისა, რომლებიც უშუალოდ არიან დაკავებული ქვეყნის კიბერსივრცის უსაფრთხოების უზრუნველყოფით.

2015 წლის ბოლოსთვის დაგეგმილია კიბერსტრატეგიისა და სამოქმედო გეგმის შუალედური გადახედვა, სადაც აისახება მკაფიო, სპეციფიკური და კონკრეტული მიზნები. ამავდროულად, საქართველო განაგრძობს არსებული კანონების გადახედვის პროცესს, რათა კიდევ უფრო მიუსადაგოს ქართული კანონმდებლობა *ევროპის კონვენციას კიბერდანაშაულის შესახებ*. ეს კი თავისთავად მოითხოვს ცვლილებებისა და განახლების მუდმივ პროცესს. ამ პროცესთან მიმართებით ორი პრობლემა იჩენს თავს. პირველი – სამთავრობო და კერძო სექტორს შორის თანამშრომლობის ნაკლებობა, ხოლო მეორე – კვალიფიციური და პროფესიონალი კადრების დეფიციტი.

საქართველოს სამთავრობო სტრუქტურების ძირითადი კოორდინატორის ფუნქცია აქვს სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოს, რომელიც უშუალოდ პრემიერ-მინისტრს ექვემდებარება. ბოლოს ჩატარებუ-

ლი საკონსტიტუციო რეფორმების შემდეგ სწორედ ამ საბჭოშია თავმოყრილი რეალური პოლიტიკური ძალა. ქვეყნის კიბერუსაფრთხოების თვალსაზრისით ერთ-ერთი დიდი მოთამაშე სამთავრობო სტრუქტურებიდან არის იუსტიციის სამინისტრო, კერძოდ, მისი მონაცემთა გაცვლის სააგენტო (DEA), რომლის დაქვემდებარებაში ასევე შედის კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფი (CERT). მეორე დიდი მოთამაშე შსს-ის ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველოა. კიბერდანაშაულთან ბრძოლის სამმართველო და მონაცემთა გაცვლის სააგენტო დღეისათვის სათანადოდ არიან აღჭურვილი და კიბერსაფრთხეებსაც, არსებული შესაძლებლობებისა თუ რესურსების ფარგლებში, შესაბამისად პასუხობენ, მაგრამ შესაძლოა სამომავლოდ გარკვეული სირთულეები შეექმნათ, რასაც ქვეყანაში კარგად გაწვრთნილი კიბერპროფესიონალების ნაკლებობა გამოიწვევს.

მიუხედავად იმისა, რომ 2008 წლიდან დღემდე საქართველომ მნიშვნელოვანი ნაბიჯები გადადგა კიბერუსაფრთხოების გასაძლიერებლად, კიდევ ბევრია გასაკეთებელი. არსებულ პრობლემასთან ბრძოლა მოითხოვს მიზანმიმართული და თანმიმდევრული კიბერპოლიტიკის გატარებას, რომელიც პრიორიტეტულს გახდის კიბერსაფრთხეებთან ბრძოლას და არსებულ პრობლემატიკას სახელმწიფო დონეზე აიყვანს. კიბერუსაფრთხოების უზრუნველყოფა და კიბერდანაშაულთან ბრძოლა გლობალური პრობლემაა და ამ გამოწვევებთან გამკლავება ასევე მოითხოვს მჭიდრო თანამშრომლობას საერთაშორისო ორგანიზაციებთან და მეგობარ სახელმწიფოებთან.

61-67 გვერდებზე გთავაზობთ ჩვენი დაკვირვებების საფუძველზე შემუშავებულ რეკომენდაციებს.

შესავალი – მსოფლიო კონტექსტი

ვერც ერთმა სხვა ტექნოლოგიურმა მიღწევამ ვერ შეძლო ისეთი გავლენის მოხდენა მსოფლიო საზოგადოებაზე, როგორიც ბოლო 20-25 წლის მანძილზე ელექტრონულად დაპროგრამებული კომპიუტერისა და ფართოდ ხელმისაწვდომი ინტერნეტის ერთობლიობამ. ინტერნეტტექნოლოგიების მსოფლიო მასშტაბით გამოყენება დღითიდღე უდიდესი სისწრაფით იზრდება. მაგალითად, სულ რაღაც შვიდი წლის მანძილზე, რუსეთ-საქართველოს კინეტიკური და კიბერომის შემდეგ, მსოფლიოში ინტერნეტის გამოყენების მაჩვენებელი გაორმაგდა. „ინტერნეტის მსოფლიო სტატისტიკის“ მიხედვით, დაახლოებით სამ მილიარდ ადამიანზე მეტი, მსოფლიო მოსახლეობის 45%, დღეს ინტერნეტის მომხმარებელია.[1] 2006-დან 2012 წლამდე ხელმისაწვდომი გამტარიანობა წამში 6.7 ტერაბაიტიდან[2] 92.1 ტერაბაიტამდე გაიზარდა. ექსპერტების პროგნოზით, 2018 წლისთვის გამტარიანობა წამში 607 ტერაბაიტამდე, ხოლო 2020 წლისთვის წამში 1100 ტერაბაიტამდე გაიზრდება.[3] ეს ნიშნავს, რომ ინტერნეტს სულ უფრო მეტი ადამიანი მოიხმარს.

დღეს, თითქმის ყველა სხვა დარგებთან ერთად, სამთავრობო და სამხედრო ინფრასტრუქტურაც ინტერნეტთან დაკავშირებული კომპიუტერული სისტემებით იმართება. ეს შესაძლებლობების, შედეგიანობისა და კომფორტის უპრეცედენტო საშუალებას იძლევა. ინტერნეტტექნოლოგიები ხელს უწყობს ეკონომიკური კეთილდღეობის ზრდას, ცხოვრების ხარისხის გაუმჯობესებას, ინფორმაციის მარტივად წვდომას და სოციალურ-პოლიტიკურ ურთიერთობებს. მთავრობებს, მაგალითად, შეუძლიათ ინფორმაციისა და სერვისების ონლაინმიწოდება და კრიზისების ონლაინმართვა. ინტერნეტი დღითიდღე იძენს განსაკუთრებულ მნიშვნელობას.

აღსანიშნავია, რომ ინტერნეტის სწრაფი ზრდა მოწყვლადობის ახალ ასპექტებსაც აჩენს. დღეს კიბერსივრცის გამო ქვეყნებს ახალ მნიშვნელოვან საფრთხეებთან უწევთ გამკლავება. როგორც ნატოს სტრატეგიულ კონცეფციაშია აღნიშნული, „კიბერშეტევები გახდა უფრო ხშირი, უფრო ორგანიზებული და უფრო მეტი ზიანის მომტანი მთავრობების, ბიზნესის, ეკონომიკისთვის, აგრეთვე ტრანსპორტირებისა და მიწოდების ქსელებისა და სხვა კრიტიკული ინფრასტრუქტურისთვის; ამგვარი შეტევები საფრთხეს უქმნის ეროვნულ და ევროატლანტიკურ კეთილდღეობას, უსაფრთხოებას და სტაბილურობას“.[4] ეს ეხება ნატოს პარტნიორ ქვეყნებსაც და მათ შორის – საქართველოსაც.

მას შემდეგ, რაც ბევრი ჩვენგანის ცხოვრების დიდი ნაწილი კომპიუტერულმა ტექნოლოგიებმა მოიცვა, სულაც არ არის გასაკვირი, რომ ვირტუალურ სამყაროში გადმოინაცვლა სოციალური არსებობის ბნელმა მხარემაც – ნარკოტიკებმა, აზარტულმა თამაშებმა, პროსტიტუციამ, პორნოგრაფიამ, უგუნურმა ხულიგნობამ და სხვა. ქვემოთ მოცემულია დანაშაულის იმ ტიპების ჩამონათვალი, რომლებიც კომპიუტერული ქსელების გამოყენებით ხდება:

- **ჰაკინგი** – კომპიუტერულ სისტემაში ან ქსელში სუსტი მხარეების მოძიებით არალეგალურად შეღწევა, რაც საფრთხეს უქმნის მონაცემთა კონფიდენციალურობას, მთლიანობასა და ხელმისაწვდომობას.
- **მავნე პროგრამების გავრცელება** სხვადასხვა მიზნის მისაღწევად, რაც საფრთხეს უქმნის მონაცემთა კონფიდენციალურობას, მთლიანობასა თუ ხელმისაწვდომობას.
- **DDoS შეტევა** (distributed denial of service attacks), რის შედეგადაც მფლობელი ან უფლებამოსილი მომხმარებელი კარგავს სისტემის მართვის სადავეებს. თავდამსხმელი ბოტნეტების – დავირუსებული ზომბი კომპიუტერების ქსელის მეშვეობით დიდი რაოდენობის ინფორმაციას ტვირთავს ვებგვერდებსა და სერვერებზე.
- **პირადი მონაცემების ქურდობა**, რაც შესაძლოა გამოიყენონ ფულის მოსაპარად ან გამოსაძალად.
- **კანონის გვერდის ავლით მომხმარებლისთვის კომპიუტერული ქსელით ისეთი წამლების მიყიდვა**, რომელთა გაყიდვაც ჩვეულებრივ გარკვეულ კონტროლს ექვემდებარება.

- **თაღლითობა, „ფიშინგის“ ჩათვლით**, რაც გულისხმობს დამაჯერებელი, ყალბი ელექტრონული გზავნილის გაგზავნას და ინფორმაციის მოპოვებას ინტერნეტთაღლითობის, მოტყუების გზით; საბანკო ინფორმაციის წვდომის მოპოვება მოტყუებით და სხვა.
- **ბავშვთა პორნოგრაფია,** კერძოდ, არასრულწლოვანთა სექსუალური გამოსახულებების ფლობა და გავრცელება; მოზარდთა შერჩევა და სპეციალურად მომზადება სექსუალური ექსპლოატაციისათვის.
- **კიბერდევნა/დაშინება.**
- **კიბერვანდალიზმი,** მონაცემთა შეცვლა ან ხულიგნობის, ან პოლიტიკური თუ სხვა მიზნებისთვის.
- **კიბერშპიონაჟი** – შპიონაჟი უკანონოა თითქმის ყველა ქვეყანაში, თუმცა უმეტეს ქვეყნებში კონტრდაზვერვა წარმოადგენს სამართალდაცვისა და ეროვნული უსაფრთხოების ნაზავს.

ბრიტანეთის შინაგან საქმეთა სამინისტროსთვის მომზადებული ანგარიში კიბერკრიმინალის უკეთ გასაგებად გვთავაზობს კიბერდანაშაულის დიქოტომიას, რომელიც შედგება კიბერდამოკიდებული დანაშაულისა და კიბერშესაძლებელი დანაშაულისაგან.

ამ ანგარიშში წარმოდგენილი განსაზღვრებით, „კიბერდამოკიდებული დანაშაული არის იმ ტიპის დანაშაული, რომლის ჩადენაც შესაძლებელია მხოლოდ კომპიუტერის, კომპიუტერული ქსელების ან სხვა ინფორმაციული და კომუნიკაციური ტექნოლოგიების (ICT) გამოყენებით“. ასეთ დანაშაულთა რიცხვშია ჰაკინგი, მავნე პროგრამების გავრცელდა და DDoS-ის შეტევები.[5] კიბერდამოკიდებული დანაშაული იგივეა, რაც გამიზნული კიბერდანაშაული – ამ ტერმინს უფრო ხშირად იყენებენ აშშ-ში.[6]

კიბერშესაძლებელი დანაშაული კი, ზემოაღნიშნული ანგარიშის მიხედვით, „არის ტრადიციული სახის დანაშაული, რომლის მასშტაბი იზრდება კომპიუტერების, კომპიუტერული ქსელების ან ICT-ის სხვა ფორმების გამოყენებით“.[7] მაგალითად, ქურდობა, თაღლითობა და სექსუალური ექსპლოატაცია ოდითგანვე არსებობს კაცობრიობაში, მაგრამ ინტერნეტტექნოლოგიები ამ სახის დანაშაულის ჩადენის ახალ საშუალებებს იძლევა. შეიძლება ითქვას, რომ კომპიუტერული ტექნოლოგიების ფართოდ გამოყენება და მისი ეფექტურობა ზრდის კიდეც ამ დანაშაულთა მოქმედების ძალასა და მასშტაბებს. კიბერშესაძლებელ დანაშაულს ამერიკული ტერმინოლოგიით ინსტრუმენტული კიბერდანაშაული ჰქვია.[8]

ბრიტანული დიქოტომია იმის საშუალებას გვაძლევს, რომ უკეთ გავიგოთ კიბერდანაშაულის ბუნება. თუმცა წმინდა დიქოტომიური მიდგომა ასევე ხაზს უსვამს იმ ალბათობას, რომ ჩანაწერთა შენახვის სისტემაში შეიძლება კიბერშესაძლებელი დანაშაულის აღრიცხვა არასათანადოდ მოხდეს, რაც, შესაბამისად, კიბერდანაშაულის შემთხვევების არასწორ სტატისტიკას მოგვცემს. არასწორი სტატისტიკა კი, თავის მხრივ, ხელს შეუშლის სამომავლო კვლევებსა და საგამოძიებო საქმიანობას, რაც ერთობ მნიშვნელოვანია ამ სფეროსათვის.

პრობლემის მოსაგვარებლად ლონდონის პოლიციამ, ბრიტანეთის ეკონომიკური დანაშაულის წინააღმდეგ ბრძოლის სამართალდამცავმა ორგანომ და თაღლითობის წინააღმდეგ ბრძოლის ეროვნული დაზვერვის ბიურომ შექმნეს ვებგვერდი სახელწოდებით Action Fraud (თაღლითობა).[9]

ეს ვებგვერდი, როგორც ბრიტანეთის შინაგან საქმეთა სამინისტროს მოხსენებაშია აღნიშნული, „შეტყობინებებს იღებს საზოგადოებისა და ბიზნესის სფეროს წარმომადგენლებისგან ისეთ დანაშაულთა შემთხვევების შესახებ, რომლებიც კლასიფიცირდება შემდეგნაირად: თაღლითობა, კიბერთაღლითობა, კიბერდანაშაული, კომპიუტერული ტექნოლოგიების შემთხვევითი ან მიზანმიმართული გამოყენება. Action Fraud-ი აღრიცხულ შემთხვევებს HOCR-ის [Home Office Counting Rules – ბრიტანეთის შინაგან საქმეთა სამინისტროს აღრიცხვიანობის წესი] საკანონმდებლო დებულებებისა და მოთხოვნების შესაბამისად აფასებს. როდესაც შეტყობინება არ აღირიცხება HOCR-ის მიერ განსაზღვრულ დანაშაულთა მიხედვით, Action Fraud-ი მას ახარისხებს როგორც ინციდენტს, რომელსაც ინფორმაციულობისა და სადაზვერვო მიზნებისთვის ცალკეულად აღრიცხავს.“[10] Action Fraud-ის მეთოდი იძლევა კიბერდანაშაულის აღრიცხვიანობის ბევრად უფრო ფართო სპექტრს, ვიდრე შესაძლებელი იყო ტრადიციული შეტყობინებისა და დაფიქსირების სისტემის საშუალებით.

ამერიკელების მიდგომა ოდნავ განსხვავდება ბრიტანულისგან. ის ეფუძნება კიბერდანაშაულის ტრიქოტომიულ მიდგომას, სადაც მესამე კატეგორიად დამატებულია კომპიუტერინციდენტური (შემთხვევითი) კატეგორია. ასეთ შემთხვევებში კომპიუტერის გამოყენება შესაძლოა თავად დანაშაულისგან პერიფერიულად ხდებოდეს. მაგალითად, კომპიუტერი შესაძლოა ინახავდეს ნარკოტიკის გამსაღებლის კლიენტთა სიას ან ის შეიძლება გამოიყენონ დანაშაულის ჩასადენად საჭირო ინფორმაციის მოძიებისთვის.[11] კომპიუტერული ტექნოლოგიების მოხმარების ზრდა ზრდის მისი ინციდენტური (ანუ დამატებითი, მეორეული დანიშნულებით) გამოყენების მაჩვენებელს ლამის ნებისმიერი სახის დანაშაულში.

უდავოა, რომ დღითიდღე იზრდება სამივე ტიპის კიბერდანაშაულის რიცხვი, რასაც თავისთავად უწყობს ხელს ინტერნეტში ჩართული კომპიუტერების დიდი რაოდენობა. 2013 წლის დეკემბრის ანგარიშში Gartner, ინტერნეტკვლევებზე მომუშავე ერთ-ერთი წამყვანი კომპანია, წერდა, რომ „მომხმარებლები სულ უფრო და უფრო შორდებიან ტრადიციულ პერსონალურ კომპიუტერებს (ნოუთბუკებსა და მაგიდის კომპიუტერებს), რომლებიც სულ უფრო მეტად ხდება საზიარო შინაარის გაცვლის ინსტრუმენტი, ტაბლეტების, ჰიბრიდებისა და მსუბუქი ნოუთბუკების მოქნილობა კი უფრო მეტად შეესაბამება მომხმარებელთა განსხვავებულ და მზარდ მოთხოვნებს“.[12]

EMarketer-ის სტატისტიკა გვიჩვენებს, რომ 2015 წლის ბოლოსთვის სმარტფონის მომხმარებელთა რიცხვი 1.91 მილიარდს მიაღწევს, ხოლო 2016 წელს 2.16 მილიარდი ადამიანი ინტერნეტში სმარტფონების საშუალებით ჩაერთვება.[13] დანაშაული ჯერ ონლაინსივრცეში გაჰყვა ადამიანებს, ახლა კი მობილური მოწყობილობებიდანაც გავრცელდა.[14]

რა თქმა უნდა, კიბერდანაშაული არ მოქმედებს მხოლოდ ინტერნეტისა და სმარტფონების შეღწევის ხარჯზე. ფინანსური კიბერდანაშაულის ზრდა, მაგალითად, ასევე დამოკიდებულია სუფთა შემოსავალისა და ელექტრონული ვაჭ-

რობის ზრდაზე, საკრედიტო ბარათების, ონლაინბიზნესის წარმოების, ონლაინბანკინგის ზრდასა და სხვა მსგავს ფაქტორებზე.

EMarketer-ის პროგნოზით, ბიზნესსა და მომხმარებელს შორის ელექტრონული ვაჭრობა 2015 წელს 1.6 ტრილიონ დოლარს მიაღწევს, 2018 წელს კი – 2.5 ტრილიონ დოლარს. ამ თვალსაზრისით, ჩინეთი პირველ ადგილს იკავებს აბსოლუტური მოცულობის მიხედვით; თუმცა მას დაბალი მაჩვენებელი აქვს თავისი მოსახლეობის მიერ ონლაინშესყიდვების კუთხით. ამ მხრივ ლიდერობს ბრიტანეთი, გერმანია და იაპონია.[15]

აღსანიშნავია, რომ შეერთებულ შტატებს, რომლის მთლიანი შიდა პროდუქტი ერთ სულ მოსახლეზე უფრო მაღალია, ვიდრე ბრიტანეთისა, გაცილებით დაბალი მაჩვენებელი აქვს ელექტრონულ ვაჭრობასა და ონლაინბანკინგში შეღწევადობის თვალსაზრისით. მაგალითად, აშშ-ის ელექტრონული ვაჭრობის მაჩვენებელი დაახლოებით ბრიტანეთის მაჩვენებლის ნახევარია. ეს გამოწვეულია სხვადასხვა სოციოლოგიური ფაქტორით, ძირითად ეკონომეტრიულ ინდიკატორებთან ერთად. რადგანაც კიბერდანაშაული კორელირებს ისეთ აქტივობებთან, როგორიცაა ელექტრონული ვაჭრობა და ონლაინბანკინგი, ამიტომ რთულია კიბედანაშაულით გამოწვეული ფინანსური დანაკარგების ინტერპოლირება გლობალური კალკულაციიდან ეროვნულ კალკულაციაში.

ელექტრონული ვაჭრობის ზრდა 1.6 ტრილიონი დოლარიდან 2.5 ტრილიონ დოლარამდე კიდევ უფრო გაზრდის და მიმზიდველს გახდის ონლაინდანაშაულს. კიბერდანაშაული სულ უფრო მასშტაბურ სახეს მიიღებს. სამწუხაროდ, რთულია კიბერდანაშაულით გამოწვეული მონეტარული ღირებულების სრულად განსაზღვრა. რამდენიმე ანგარიშგასაწევი ორგანიზაციის კვლევები დიდად განსხვავდება ერთმანეთისაგან. განსხვავებებია კიბერდანაშაულის განსაზღვრებებსა და რაოდენობის განსაზღვრასთან დაკავშირებულ მეთოდოლოგიებშიც. ასევე რთულია გარკვეული სახის კიბერდანაშაულით გამოწვეული ფინანსური ზარალის განსაზღვრა. მაგალითად, როგორ უნდა განისაზღვროს ერთი სახელმწიფოს მიერ მეორე სახელმწიფოსგან მოპარული შეიარაღების სისტემის გაუმჯობესებული სქემისა თუ დიზაინის მონეტარული ღირებულება? ამასთან, შემთხვევათა დიდი ნაწილი დაუფიქსირებელი რჩება ინფორმაციის არქონის, რეპუტაციაზე ზრუნვის, ეროვნული უსაფრთხოებისა და კიდევ ბევრი სხვა მიზეზის გამო. დაბოლოს, კვლევის მეთოდოლოგიის არჩევა სხვადასხვა თვალსაზრისისა და მიდგომის საკითხია.

მიუხედავად ყველაფრისა, არიან ორგანიზაციები, რომლებიც ცდილობენ სხვადასხვა მეთოდოლოგიის გამოყენებით კიბერდანაშაულით გამოწვეული ფულადი ზარალის რამენაირად დაანგარიშებას. მაგალითად, *2013 წლის ნორტონის ანგარიში* (Norton Report) კიბერდანაშაულით მიღებული ზარალის წლიურ ოდენობას 113 მილიარდ დოლარად აფასებს. ეს მაჩვენებელი 2012 წელს 110 მილიარდ დოლარს შეადგენდა.[16] გაცილებით უფრო მეტი სიფრთხილით ეკიდება ამ საკითხს მაკაფი (McAfee) და ვაშინგტონის სტრატეგიისა და საერთაშორისო კვლევების (CSIS) ორგანიზაცია, რომლის მეთოდოლოგია დაფუძნებულია საკმაოდ რთულ ეკონომეტრიულ მიდგომაზე. „კიბერდანაშაულითა და კიბერშპიონაჟით გამოწვეული ფინანსური დანაკარგის ზუსტი ოდენობის დადგენა შეუძლებელი ამოცანაა, – აღნიშნულია McAfee-სა და CSIS-ის კვლევაში, – თუმცა შესაძლებელია შემუშავდეს პოტენციური დანაკარგის შედარებით უფრო

ზუსტი საზომი“. მათი მოსაზრებით, შემდგომ კვლევებში კიბერდანაშაულით გამოწვეული დანაკარგის ზღვარი 80 მილიარდი დოლარიდან 400 მილიარდ დოლარამდე იმერყეველებს, რაც, ცხადია, დიდ სხვაობას და საკმაო შეუსაბამობას იძლევა ნორტონის კვლევასთან. შემდგომი კვლევისთვის McAfee-CSIS-ის გუნდი ოთხ ძირითად საკითხს განიხილავს:[17]

- შესაძლებელია თუ არა „დასაშვები ღირებულების“ განსაზღვრისთვის იმდენად ზუსტი ანალოგიების შემუშავება, რომ საშუალება მოგვეცეს კიბერდანაშაულით გამოწვეული დანაკარგი დავადგინოთ? „დასაშვები ღირებულების“ ანალიზის სირთულე ერთგვარ შეუსაბამობას იწვევს უფლებამოსილი პირების მიერ მიღებულ რიგ გადაწყვეტილებებთან. ახალ და ეფექტიან კომპიუტერულ სისტემებზე დამოკიდებულების ზრდის გადაწყვეტილებით ისინი, ხშირ შემთხვევაში, უგულებელყოფენ იმ რისკფაქტორებს, რომლებიც ამ პროცესს ახლავს თან.
- არის თუ არა თავდამსხმელებისთვის მნიშვნელოვანი ტექნოლოგიური მონაპოვარი კიბერსაშუალებით ტექნოლოგიების უკანონოდ მითვისება, რამაც შესაძლოა დაზარალებული ეკონომიკის გრძელვადიანი ხარჯები გამოიწვიოს თუ ჰაკეროზა მხოლოდ უმნიშვნელო გავლენას ახდენს როგორც თავდამსხმელის, ისე მსხვერპლის ეკონომიკურ საქმიანობაზე (უნდა აღინიშნოს, რომ ამან შეიძლება დამანგრეველად იმოქმედოს ცალკეულ კომპანიებზე)?
- ამცირებენ თუ არა კომპანიები ხარჯებს, როგორც ბიზნესის წარმოებისთვის დამახასიათებელი ჩვეული პროცედურის დროს ხდება ხოლმე, თუ სათანადოდ ვერ აფასებენ ზიანისა და ზარალის ნამდვილ მასშტაბებს?
- არის თუ არა ზარალის დოლარის ღირებულებით გაზომვა კიბერშპიონაჟითა და კიბერდანაშაულით მიღებული ზიანის შესაბამისი საზომი და ხომ არ უგულებელყოფს ეს ისეთ არამატერიალურ ხარჯებს, როგორიცაა, მაგალითად, საერთაშორისო სისტემის მიმართ ნდობა ან სამხედრო ძალაზე ზეგავლენა?

2014 წელს McAfee-სა და CSIS -ის კვლევის ავტორებმა წინა წლის ანგარიშის განახლებული ვერსია გამოაქვეყნეს. 2014 წლის ანგარიშის მიხედვით, კიბერდანაშაულით მიღებული წლიური ზარალი 375 მილიარდი დოლარადან 575 მილიარდი დოლარის ფარგლებში მერყეობს. მიუხედავად იმისა, რომ გარეკვეული წინსვლა აქვთ დაანგარიშების თვალსაზრისით, კვლევის ავტორებმა მაინც ვერ შეძლეს მოცემულ ციფრებს შორის არსებული დიდი სხვაობის აღმოფხვრა. ამრიგად, ავტორები შემდეგნაირად აღწერენ იმ სამ მეთოდოლოგიურ მიდგომას, რომელმაც განაპირობა კვლევის შედეგები:

„თუკი ჩვენ გამოვიყენებდით მხოლოდ მაღალი შემოსავლების მქონე ქვეყნების ზარალის/ხარჯის მაჩვენებლებს გლობალური რიცხვის ექსტრაპოლირების მიზნით, მაშინ მივიღებდით საერთო გლობალურ ღირებულებას 575 მილიარდი დოლარის ოდენობით. თუკი ჩვენ გამოვიყენებდით ყველა იმ ქვეყნის (სადაც ინფორმაციის ხელმისაწვდომობა ამ თვალსაზრისით პრობლემას არ წარმოადგენს) ზარალის/ხარჯის სრულ მაჩვენებლებს და ამგვარად მოვახდენდით საერთო გლობალური რიცხვის ექსტრაპოლირებას, ეს მოგვცემდა საერთო გლობალურ ღირებულებას 375 მილიარდი დოლარის ოდენობით. დაბოლოს, მესამე მეთოდოლოგიის თანახმად, თუკი რეგიონული შემოსავლების ხვედრითი წილის შესაბამისად გამოვთვლიდით საერთო მაჩვენებელს, მაშინ მივიღებდით საერთო გლობალურ ღირებულებას 445 მილიარდი დოლარის ოდენობით. აქედან არც ერთი მიდგომა არ არის დამაკმაყოფილებელი, თუმცა სანამ აღრიცხვიანობისა და მონაცემთა შეგროვების მეთოდიკა დაიხვეწება, ამგვარი მიდგომა მოგვცემს საშუალებას მიახლოებით განვსაზღვროთ კიბერდანაშაულითა და კიბერშპიონაჟით გამოწვეული დანაკარგი და მთლიანი ხარჯები“.[18]

ზემოთ მოყვანილი ოთხი კითხვა, მიუხედევად მათ მიმართ არსებული ინტერესისა, ერთგვარ პასუხს სცემს ორ ფუნდამენტურ საკითხს: პირველი – კიბერდანაშაულთან დაკავშირებული ხარჯების გამოთვლა ძალიან რთულია და დოლარის ცალკე აღებული მაჩვენებელი შესაძლოა არც კი იყოს ყველაზე მნიშვნელოვანი საზომი. მეორე – ამ შეკითხვებზე პასუხი ასევე შესაძლოა მოიცავდეს მსოფლიოს მსხვილი ეკონომიკის ქვეყნებში არსებულ სოციალურ-კულტურულ და გარემო ფაქტორებს. ყოველივე ეს კი გლობალური თანხების ინტერპოლაციის ნებისმიერ მცდელობაზე იქონიებს გავლენას ეკონომიკური მაჩვენებლის ლოკალურ დონეზე დაყვანის კუთხით.

პონმონის ინსტიტუტი, რომელსაც აფინანსებს Hewlett Packard-ი, კიბერდანაშაულით გამოწვეული დანაკარგის განსაზღვრისას აბსოლუტურად სხვა მიდგომას ირჩევს. კიბერდანაშაულის მთლიანი გლობალური ან თუნდაც ეროვნული ღირებულების დადგენის ნაცვლად, პონმონის ინსტიტუტი ატარებს სპეციალურ გამოკითხვას სხვადასხვა ქვეყნის გარკვეულ კომპანიებში და წლიური შედეგების მიხედვით ადგენს ტენდენციას. პონმონის ინსტიტუტის 2014 წლის კვლევა მოიცავს 257 კომპანიას ავსტრალიაში, საფრანგეთში, გერმანიაში, იაპონიაში, ბრიტანეთში, შეერთებულ შტატებსა და რუსეთში. ეს უკანასკნელი პირველად შეიყვანეს პონმონის ინსტიტუტის ამ კვლევაში.

ანგარიში აჩვენებს მონაწილე კომპანიების მონაცემებს შორის არსებულ მნიშვნელოვან განსახვავებებს. 2014 წლის ანგარიშის თანახმად, ყველაზე მაღალი საშუალო ღირებულების მაჩვენებელი, 12.7 მილიონი დოლარი, აქვს ამერიკის შეერთებულ შტატებს, ხოლო რუსეთს – ყველაზე დაბალი – 3.3 მილიონი დოლარი. აქვე უნდა აღინიშნოს, რომ წინა წელთან შედარებით ექვსივე ქვეყნის (რუსეთის გამოკლებით) კვლევაში მონაწილე კომპანიების კიბერდანაშაულით

გამოწვეული ხარჯები საგრძნობლად გაიზარდა. მაგალითად, 2.7 პროცენტით იაპონიისთვის და 22.7 პროცენტით ბრიტანეთისთვის. სუფთა პროცენტული ზრდა 2013 და 2014 ფისკალურ წლებს შორის[19] (რუსეთის მაგალითის გამოკლებით) იყო 10.4 პროცენტი.

ცხადია, რომ ორგანიზაციების წინააღმდეგ კიბერდანაშაული მზარდია. პონმონის კვლევით თანახმად, მონაწილე 257 ორგანიზაციის საშუალო წლიურმა კიბერღირებულებამ, 2014 წელს, 7.6 მილიონი დოლარი შეადგინა, 0.5 მილიონი დოლარიდან 61 მილიონი დოლარის ფარგლებში თითოეულ კომპანიაზე.[20]

„ფაქტები მეტყველებს იმაზე, რომ მდგომარეობა გაუმჯობესების ნაცვლად უარესდება, მიუხედავად მთელი იმ რესურსებისა, რასაც კომპანიები კიბერსაფრთხეების წინააღმდეგ ბრძოლისთვის ხარჯავენ“, – ამბობს ლარი პონმონი, ინსტიტუტის ხელმძღვანელი.[21]

შეტევის ტიპების ქვეყნების მიხედვით განსხვავებული მაჩვენებელი ასევე ეწინააღმდეგება გლობალური თუ ცალკეული განვითარებული ქვეყნების მაჩვენებლების ინტერპოლირებას ნაკლებად განვითარებული ქვეყნების მაჩვენებლებში.

ყველა ერთხმად აღიარებს, რომ მსოფლიო კიბერდანაშაული საყურადღებო და მზარდია. ამასთან, კიბერდანაშაულის იმდენი ნაციონალური ვარიაცია იქნება, რამდენი ქვეყანაც არის. ამ საფრთხის მიმართ არც ერთ ქვეყანას არ აქვს გამომუშავებული იმუნიტეტი. კიბერდანაშაულის ტენდენციებს კარგად ასახავს კომპიუტერულ უსაფრთხოებაზე მომუშავე კომპანიების მიერ ჩატარებული უამრავი კვლევა.

კომპიუტერული უსაფრთხოების კომპანია EMC-ის 2015 წლის ანგარიშში გამოყოფილია ოთხი ძირითადი ტენდენცია:

პირველი კიბერკრიმინალი, როგორც საბაზრო მომსახურება, ნელ-ნელა უფრო დაიხვეწება. მაღალი კონკურენციის პირობებში კიბერკრიმინალებმა შესაძლოა უფასო საცდელი სერვისების, გარანტიებისა და, სერვისების განმეორებით გამოყენების შემთხვევაში, ფასდაკლების შეთავაზების ტაქტიკასაც კი მიმართონ.

მეორე მობილურ მოწყობილობებზე თავდასხმების ზრდის საფრთხე. „თუკი მხედველობაში მივიღებთ სმარტფონების მოხმარების ზრდის ტემპს მსოფლიოში, ყურადღება ამ მიმართულებით უფრო გაიზრდება“, – აღნიშნულია ანგარიშში. ანგარიშში ასევე ხაზგასმულია მობილური გადახდის სისტემების მიმართ კიბერთავდასხმის შემთხვევების მოსალოდნელი ზრდაც.

მესამე ფინანსურ ინსტიტუტებზე თავდასხმის შემთხვევების ზრდა, რაც კიბერკრიმინალებისთვის ბევრად უფრო ნოყიერი და მომგებიანი სამიზნეა.

მეოთხე „მოსალოდნელია APT (Advanced Persistent Threat) და მსგავსი თავდასხმების სტრატეგიის გამოყენება რიგი სახელმწიფოებიდან კიდევ უფრო გაიზარდოს რეგიონალური კონფლიქტების დროს. კრიმინალური დაჯგუფებები კი უფრო ინტენსიურად შეეცდებიან სახელმწიფოების მიერ გამოყენებული ტაქტიკის ათვისებასა და გამოყენებას“.[22]

როგორც სმარტფონებისა და სხვა მოწყობილობების მოხმარების ზრდას მოჰყვა კიბერდანაშაულის ზრდა, ისევე მოხდება საგანთა ინტერნეტის [ინგლ. Internet of things (IoT)] ზრდის შემთხვევაშიც. ინტერნეტპროტოკოლის ახალი ვერსიის – IPv6 (ინგლ. Internet Protocol version 6) შემოღებასთან, კომპიუტერული მეცნიერების განვითარებასა და მინიატურიზებასთან ერთად მთელი რიგი ახალი კომპიუტერული ტექნოლოგიები იქმნება, რომელთა უსაფრთხოებაც უკიდურესად მნიშვნელოვანი იქნება. საგანთა ინტერნეტი (IoT) მოიცავს ყველაფერს, რასაც აქვს IP-მისამართი, ხოლო IPv6 იძლევა IP-მისამართების ზრდის უსაზღვროდ დიდ საშუალებას.[23]

ეს საგნები შეიძლება იყოს, მაგალითად, გულის მონიტორები, ბიოჩიპები, მანქანის კომპიუტერები, სახლისა თუ ოფისის თერმოსტატები, სმარტმოწყობილობები და ა.შ. საგანთა ინტერნეტი შესაძლებელს გახდის მაცივრებისა და ტელევიზორების დისტანციურ შეკეთებასა და, ასევე, სხვა მნიშვნელოვანი პროცესების რეალურ დროში მონიტორინგს. საგანთა ინტერნეტს უამრავი უპირატესობა აქვს, თუმცა ის ასევე ზრდის კიბერბოროტმოქმედების არეალს. უკვე დაფიქსირდა ბოტნეტის, დავირუსებული ზომბი კომპიუტერების ქსელში ჩართული სმარტტელევიზორის, აუდიოსპიკერისა (მოსაუბრის) და მაცივრის სპამშეტყობინებების გაგზავნის ერთი შემთხვევა.[24] ეს საშიშროება უკვე დაემუქრა განვითარებულ ქვეყნებს. შესაძლოა საქართველოში მსგავსი რამ ჯერ კიდევ შორეულ პერსპექტივად მიაჩნდეთ, თუმცა დასაშვებია, რომ ამან გაცილებით ადრე იჩინოს თავი, ვიდრე მოსალოდნელია. საგანთა ინტერნეტის ზრდამ შესაძლოა გამოიწვიოს ისეთი ტიპის დანაშაულის ზრდა, როგორიცაა კარდიოსტიმულატორებისა თუ მანქანის კომპიუტერული სისტემების ჰაკინგი.

აღსანიშნავია ისიც, რომ ონლაინსამყაროში, დანაშაულისა და ადამიანური მანკიერების მრავალნაირ ასპექტთან ერთად, თავი იჩინა საუკუნეების მანძილზე ადამიანის არსებობისათვის დამახასიათებელმა ორმა ქმედებამ – შპიონაჟმა და ომმა.

კიბერშპიონაჟის შემთხვევები ლამის ყოველკვირა ხდება. მაგალითად, *Snake-Uroburos-Turla*-ს შპიონაჟურმა კიბერიარაღმა, რომელიც უკრაინის კრიზისს უკავშირდება, დიდი გამოხმაურება ჰპოვა საერთაშორისო პრესაში. ეს შემთხვევა პრესაში გახმაურდა ევრომაიდანის მოვლენების დროს, რასაც უკრაინის ყოფილი პრეზიდენტის, ვიქტორ იანუკოვიჩის, ქვეყნიდან გაქცევა და რუსეთის მიერ ყირიმის დაპყრობა მოჰყვა. თუმცა უნდა აღინიშნოს, რომ *Snake*, საგანგებოდ კიბერშპიონაჟისთვის შექმნილი ეს მრავალფუნქციური კიბერიარაღი, რომლის სამიზნეც უმთავრესად იყო უკრაინა და ლიტვა, უკვე დიდი ხანია, ცნობილ მოვლენებამდე ბევრად ადრე, გამოიყენება ამ ქვეყნების წინააღმდეგ. ამ თვალსაზრისით საინტერესოა კასპერსკის ლაბორატორიის დასკვნაც, რომლის მიხედვითაც *Snake*-ი *Agent.btz*-ის – კიბერშპიონაჟისათვის გამიზნული ადრეული ჭიავირუსის – მონათესავეა, რადგან ამ ორი კიბერიარაღის ხელწერა ძალიან ჰგავს ერთამენთს. *Agent.btz*-ი კი, თავის მხრივ, იმდენად ეფექტური იყო, რომ ამერიკელ ექსპერტებს 2008 წელს წელიწადზე მეტი დასჭირდათ მისგან შეერთებული შტატების მთავრობის კომპიუტერული ქსელის გასაწმენდად. ეს ოპერაცია ცნობილია სახელწოდებით „ბეკშოტ იანკი“ (Backshot Yankee.)[25]

ამრიგად, შპიონაჟი არის დანაშაულის ტიპი, რომელიც არსებობს და ვრცელდება კიბერსივრცეშიც.

საქართველოს მონაცემები

მოსახლეობა: დაახლ. 4.5 მლნ. ადამიანი

დედაქალაქი: თბილისი, დაახლ. 1.2 მლნ. მაცხოვრებლით

მთლიანი შიდა პროდუქტი (IMF-ის მიხედვით): 16.5 მლრდ. აშშ დოლარი

მთლიანი შიდა პროდუქტი ერთ სულ მოსახლეზე (ნომინალური ღირებულებები IMF-ის მიხედვით): 3,700 აშშ დოლარი

მთლიანი შიდა პროდუქტის ზრდა: 4.8%

მთავრობის ელექტრონული პორტალის URL: www. my.gov.ge

მსოფლიო ეკონომიკური ფორუმის მიხედვით ქსელური მზადყოფნის ინდექსით (NRI-Network Readiness Index)**:** მე-60 ადგილი 148 ქვეყნიდან

გაეროს ელექტრონული მმართველობის განვითარების ინდექსით: 56-ე ადგილი 193 წევრი ქვეყნიდან

საინფორმაციო–საკომუნიკაციო ელექტრონული ტექნოლოგიების გამოყენება

(**ICT - Information and Communications Technology**)

2015 წლის „მსოფლიო ეკონომიკური ფორუმის“ *გლობალური საინფორმაციო ტექნოლოგიის ანგარიშის* მიხედვით, 2014 წელს ქსელური მზადყოფნის ინდექსით (NRI – Network Readiness Index) საქართველო 148 ქვეყანას შორის მე-60 ადგილს იკავებს.[26] 2013 წელთან შედარებით, საქართველო 5 პოზიციით დაწინაურდა.[27] NRI ზომავს ქვეყნის ეკონომიკურ მზადყოფნას გამოიყენოს ICT ტექნოლოგიები კონკურენტუნარიანობისა და კეთილდღეობის გასაუმჯობესებლად. კერძოდ, ის აფასებს, თუ როგორია არსებული მდგომარეობა ICT-ის ინფრასტრუქტურის განსავითარებლად; ბიზნესი და მარეგულირებელი გარემო; ინოვაცია და კონკურენციის დონე; ზეგავლენა ეკონომიკურ განვითარებაზე; მოქალაქეების, ბიზნესწრეებისა და სამთავრობო ორგანიზაციების მზადყოფნა; საინფორმაციო ტექნოლოგიების გამოყენებისა და წარმოების დონე ქვეყანაში.

გაეროს საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU) მიერ ჩატარებული კვლევის თანახმად, 2014 წელს ინტერნეტით სარგებლობდა საქართველოს მოსახლეობის დაახლოებით 49%.[28] ამ თვალსაზრისით უფრო დეტალურ ანალიზს ასახავს საქართველოს კომუნიკაციების ეროვნული კომისიის 2014 წლის ოქტომბრის ანგარიში.

ანგარიშის მიხედვით, 2014 წლის ოქტომბრის მონაცემებით, ქვეყანაში არის დაახლოებით ინტერნეტსერვისის პროვაიდერი 100 კომპანია და 603000 აბონენტი.[29] ამ მიმართულებით, აბონენტების რიცხოვნობის მიხედვით, საქართველოში ორი კომპანია ლიდერობს:

- „სილქნეტი“ – 234,542
- „კავკასუს ონლაინი“ – 156,458

ანგარიშის თანახმად, 2014 წელს აბონენტთა რაოდენობის მიხედვით ინტერნეტის მოხმარება, წინა წელთან შედარებით, დაახლოებით 14.4%-ით გაიზარდა – 527,000 ათასიდან 603,000-მდე. კერძოდ, ოპტიკურბოჭკოვანი ინტერნეტის აბონენტთა რაოდენობამ 52.2% შეადგინა, DSL ტექნოლოგიისა – 34.9%, WiFi-ის – 11.5% და WiMax ტექნოლოგიისა – 1.2%. სხვა დანარჩენი ტექნოლოგიების აბონენტთა რაოდენობა 0.1%-ია.

რეგიონებში ინტერნეტკავშირის უფრო მაღალი დონის მისაღწევად ერთ-ერთი გზა შეიძლება მობილური ინტერნეტის განვითარება იყოს. ამასთან დაკავშირებით ანგარიში აჩვენებს, რომ 2014 წლის ოქტომბრის მდგომარეობით მობილური ინტერნეტის მომხმარებელთა რაოდენობა 1.88 მილიონი იყო. აქედან 43% – „მაგთიკომის“, 34% – „ჯეოსელის“ და 23% „ბილაინის“ მომხმარებლები იყვნენ.[30] ამჟამად მობილური ინტერნეტტექნოლოგიებია 2G, 3G და 4G. 2015 წელს ამ კომპანიებმა ქართველ მომხმარებლებს LTE (Long Term Evolution) – მეოთხე თაობის ინტერნეტი შესთავაზეს.

ელექტრონული ვაჭრობა და ონლაინბანკინგი

გასაგებია, თუ რატომ არ არის საქართველო წამყვანი ქვეყნების სიაში ელექტრონული ვაჭრობისა და ონლაინბანკინგის თვალსაზრისით. ამის მიზეზი კარგად ჩანს, თუკი საქართველოში ერთ სულ მოსახლეზე მთლიან შიდა პროდუქტს იმ ქვეყნების მონაცემებთან შევადარებთ, რომლებიც ამ სიებში ლიდერობენ.[31]

ქვეყანა	2014 მშპ ერთ სულ მოსახლეზე აშშ დოლარში
საქართველო	$ 3,700
კანადა	$50,300
გერმანია	$48,600
ნიდერლანდები	$52,000
ბრიტანეთი	$46,000

მიუხედავად ამისა, აღსანიშნავია, რომ საქართველო მისდევს განვითარებული მსოფლიოს ტენდენციას და მისი მთლიანი შიდა პროდუქტი ერთ სულ მოსახლეზე იზრდება. თუკი საორიენტაციოდ ავიღებთ 2008 წელს, რუსეთ-საქართველოს ომის წელს, მას შემდეგ საქართველოს მთლიანი შიდა პროდუქტი ერთ სულ მოსახლეზე დაახლოებით 28%-ით გაიზარდა.[32]

არ არსებობს საქართველოს ეროვნული სტატისტიკა ელექტრონულ ვაჭრობასა და ონლაინბანკინგში შეღწევადობის შესახებ, თუმცა მზარდი ტენდენცია აშკარაა. სულ უფრო მეტი ქართველი ფლობს საკრედიტო და სადებეტო ბარათებს, ონლაინშენაძენების მიწოდება მარტივდება და ყველა დიდ ბანკს აქვს ონლაინბანკინგის შემოთავაზება. აქედან გამომდინარე, საქართველო უნდა მოემზადოს მზარდი ფინანსური ონლაინდანაშაულის წინააღმდეგ საბრძოლველად, რაც თავისთავად მოჰყვება ქვეყნის ეკონომიკურ და კომერციულ განვითარებას.

საინფორმაციო წყაროები

აშშ-ის ეროვნულ-დემოკრატიული ინსტიტუტის 2015 წლის სექტემბრის კვლევის – „საზოგადოების განწყობა საქართველოში“ – მიხედვით, ტელევიზია მოსახლეობის 87%-სთვის ინფორმაციის პირველ წყაროდ რჩება. ინტერნეტი მიიჩნევა რიგით მეორე წყაროდ ქვეყნის პოლიტიკურ, სოციალურ და მიმდინარე საკითხებზე ინფორმაციის მისაღებად.[33] ამ მხრივ, სოციალური მედია ერთ-ერთ მნიშვნელოვან როლს თამაშობს, განსაკუთრებით კი, ფეისბუკი, რომელიც ყველაზე პოპულარულია საქართველოში. 1.22 მილიონი რეგისტრირებული მომხმარებლით ფეისბუკი[34] ქართულ საზოგადოებაში მნიშვნელოვან პლატფორმას წარმოადგენს დისკუსიისა და ინფორმაციის გაცვლისათვის.

ელექტრონული მმართველობა

ელექტრონული მთავრობა საქართველოში განმარტებულია, როგორც „საჯარო ფუნქციების შესრულება ინფორმაციული და საკომუნიკაციო ტექნოლოგიების გამოყენებით".

საქართველოში სახელმწიფო ორგანოებმაც გაზარდეს ინტერნეტტექნოლოგიების მოხმარება. მაგალითად, იუსტიციის სამინისტრომ, ფინანსთა სამინისტროს შემოსავლების სამსახურმა და სხვა დაწესებულებებმა შექმნეს ონლაინსერვისები, რომლებიც საშუალებას აძლევს მოქალაქეებს დარეგისტრირდნენ და ისარგებლონ ონლაინსერვისებით, განაცხადონ პირადობის მოწმობის ასაღებად ან შეავსონ საგადასახადო დოკუმენტაცია. ამასთანავე, ზოგიერთი სახელმწიფო სერვისი უერთდება მობილური აპლიკაციების ბაზარს. მაგალითად, საქართველოს პოლიციამ შექმნა აპლიკაცია, სადაც მომხმარებლებს შეუძლიათ შეამოწმონ მნიშვნელოვანი ინფორმაცია ან გადაიხადონ საგზაო ჯარიმები.[35]

ელექტრონული მმართველობის შესახებ გაეროს მიერ ჩატარებული 2014 წლის კვლევის მიხედვით, საქართველო 56-ე ადგილზეა. ორ წელიწადში ქვეყანა 16 პოზიციით დაწინაურდა: გაეროს 2012 წლის ანგარიშში საქართველო 72-ე ადგილზე იყო.[36] ელექტრონული მმართველობის განვითარების ინდექსი მოიცავს ხელმისაწვდომობის ისეთ მახასიათებლებს, როგორიც არის ინფრასტრუქტურა და განათლების დონე, რომლებიც ასახავს, თუ როგორ იყენებს ქვეყანა საინფორმაციო ტექნოლოგიებს, რომ გაზარდოს მოსახლეობის ხელმისაწვდომობა და ჩართულობა. ელ. მმართველობის საზომია შეფასება, რომელიც აჩვენებს, თუ როგორ იყენებს სახელმწიფო ინტერნეტსა და მსოფლიო ქსელს ინფორმაციის, პროდუქტებისა და სერვისების მიწოდებისთვის. ამასთანავე, ის აფასებს ქვეყანაში ტელეკომუნიკაციისა და ადამიანური კაპიტალის განვითარების დონეს.[37]

საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოსა და ევროკავშირის ტვინინგის პროექტი „ციფრული საქართველო. ელექტრონული საქართველოს სტრატეგია და სამოქმედო გეგმა 2014-2018" მიზნად ისახავს თანამედროვე საინფორმაციო-საკომუნიკაციო ტექნოლოგიების (ICT) დანერგვის ხელშეწყობას ქვეყანაში. შემოთავაზებული ქმედებები მოიცავს უკვე დაწყებულ ინიციატივებსა და სტრატეგიებს. ელექტრონული საქართველოს სტრატეგია არ შემოიფარგლება მხოლოდ იმ აქტივობებით, რომლებსაც ტერმინი „ელექტრონული მმართველობა" მოიცავს და უფრო ფართო მასშტაბებზე ვრცელდება და ხელსაყრელ გარემოს უქმნის ინოვაციურ ბიზნესსექტორსა და ინოვაციურ სამოქალაქო საზოგადოებას. მთავრობამ სტიმული უნდა მისცეს ინოვაციების შემოტანა-დანერგვას საზოგადოებაში, კერძო და სამოქალაქო სექტორებში და ამით ხელი უნდა შეუწყოს მდგრად ეკონომიკურ განვითარებას.

დოკუმენტში გამოყოფილია პრიორიტეტები: ელექტრონული სერვისების განვითარება, ელექტრონული ჩართულობა და ღია მმართველობა; ელ. ჯანდაცვა; საჯარო ფინანსების მართვის სისტემა; ელ. ბიზნესი; საქართველოს ICT რეგიონულ ცენტრად ქცევა; ინფრასტრუქტურული განვითარება; ელ. უსაფრთხოება; ელ. მმართველობისთვის ხელსაყრელი გარემოს შექმნა და ამ მიმართულებით ცნობიერების ამაღლება. დოკუმენტში ნათქვამია, რომ საქართველოს აქვს კარგი სასტარტო პოზიცია, რადგან ICT-ის განვითარების მიმართ მაღალია პოლიტიკური ვალდებულება.[38]

საქართველოს ელ. მმართველობის სტრატეგიის ეფექტურობას და ამ კუთხით ქვეყნის წინსვლას ასახავს ელექტრონული მმართველობის შესახებ გაეროს 2014 წლის კვლევის შედეგებიც, არა მარტო ელ. მმართველობის, არამედ ელ.მოხმარების მიმართულებითაც. ანგარიში აჩვენებს, რომ ელ. სერვისების ხელმისაწვდომობასა და მათ ფაქტობრივ გამოყენებას შორის სხვაობა მნიშვნელოვნად შემცირდა ბოლო ორი წლის განმავლობაში. ანგარიშში ასახული სკალის მიხედვით, წამყვანი პოზიცია უკავია ნიდერლანდებს, რომელსაც 1.0 (ერთი მთელი) ქულა აქვს მინიჭებული. მნიშვნელოვანია საქართველოს პროგრესი ამ თვალსაზრისით. ორი წლის მანძილზე (2012-2014) საქართველოს მაჩვენებელი 0.21-დან 0.59-მდე გაიზარდა.[39]

ICT და ეკონომიკური განვითარება

საქართველოს ICT-ზე დამოკიდებულების ზრდა ხელს უწყობს არა მხოლოდ მთავრობისა და საზოგადოების ჩართვას თანამედროვე ცხოვრებაში, არამედ ქვეყნის ეკონომიკურ ზრდასაც. ამასთანავე, საქართველო დაინტერესებულ მხარეს ICT-ის სფეროში ინვესტირების მიმზიდველ გარემოს სთავაზობს. საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროს გრძელვადიანი სტრატეგია ICT-ის და ინოვაციების სფეროში – *საქართველო 2020* – მიზნად ისახავს მსოფლიო ტოპათეულში მოხვედრას 2020 წლისთვის ქსელური მზადყოფნის ინდექსის გაუმჯობესების კუთხით. ამავე შინაარსის ევროკომისიის კვლევა კი ხაზს უსვამს ICT-ის სექტორის მნიშვნელოვან როლს საქართველოს ეკონომიკაში. კვლევის თანახმად, მისი წილი ~7%-ია ეროვნულ მთლიან შიდა პროდუქტში, რაც მაღალი მაჩვენებელია რეგიონის მიხედვით.[40] ICT-ის განვითარებას მოაქვს შედარებით მაღალი ხელფასები, გადამზადებისა და განვითარების შესაძლებლობები და ეფექტურობის კოეფიციენტის ზრდა.

კიბერდანაშაული

2014 წლიდან საქართველომ კიბერდანაშაულის შესახებ ოფიციალური სტატისტიკის წარმოება დაიწყო. ამ მხრივ უფლებამოსილია საქართველოს შინაგან საქმეთა სამინისტროს საინფორმაციო-ანალიტიკური დეპარტამენტი. მიუხედავად იმისა, რომ არ მოიპოვება 2013 წლის ოფიციალური სტატისტიკა, ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველოს წარმომადგენლებმა ჩვენთან საუბარში განაცხადეს, რომ 2013 წელს მათ გამოიძიეს დაახლოებით 35 მძიმე ხასიათის კიბერდანაშაული. მათ ასევე აღნიშნეს 2013 წელს გამოვლენილი ნაკლებად მძიმე ხასიათის კიბერდანაშაულის შემთხვევები, რომლებიც ჩაიდინეს არაკვალიფიციურმა ჰაკერებმა, ე.წ. სკრიპტკიდებმა. „სკრიპტკიდი“ („Script-kiddies“) დამამცირებელი სახელია, რომელსაც მაღალკვალიფიციური ჰაკერები არაკვალიფიციურ, ნაკლებად დახელოვნებულ ჰაკერებს ეძახიან.

2014 წლის და 2015 წლის პირველი ნახევრის სტატისტიკა, რომელიც ამ ანგარიშშია წარმოდგენილი, მოგვაწოდა საქართველოს შინაგან საქმეთა სამინისტრომ. ქვემოთ მოყვანილი პირველი ცხრილი ასახავს შსს-ის ტერიტორიული და სტრუქტურული დანაყოფების მიერ სისხლის სამართლის კოდექსის 284-ე, 285-ე, 286-ე მუხლებით რეგისტრირებული და გახსნილი კიბერდანაშაულის რაოდენობას 2014 წელსა და 2015 წლის პირველ ნახევარში. სსკ-ის 284-ე მუხლით ისჯება კომპიუტერულ სისტემაში უკანონო შეღწევა, 285-ე მუხლით ისჯება დამაზიანებელი კომპიუტერული პროგრამის შექმნა, გამოყენება ან გავრცელება, ხოლო 286-ე მუხლით ისჯება კომპიუტერული სისტემის ხელყოფა ან/და კომპიუტერული მონაცემის დაზიანება, წაშლა და მოდიფიცირება.[41]

შსს-ის ტერიტორიული და სტრუქტურული დანაყოფების მიერ სსკ-ის 284-ე, 285-ე, 286-ე მუხლებით რეგისტრირებული და გახსნილი დანაშაული

პერიოდი	სსკ-ის 284-ე-286-ე მუხლები		სსკ-ის 284-ე მუხლი		სსკ-ის 285-ე მუხლი		სსკ-ის 286-ე მუხლი	
	სულ რეგის.	გახსნ.	სულ რეგის.	გახსნ.	სულ რეგის.	გახსნ.	სულ რეგის.	გახსნ.
2014 წ.	163	69	144	62	12	7	7	0
2015 წ. (პირველი ნახევარი)	79	22	70	22	3	0	6	0

ქვემოთ მოყვანილი მეორე ცხრილი ასახავს შსს-ის ცენტრალური კრიმინალური პოლიციის დეპარტამენტის მიერ სისხლის სამართლის კოდექსის 284-ე, 285-ე, 286-ე მუხლებით რეგისტრირებული და გახსნილი კიბერდანაშაულის რაოდენობას 2014 წელსა და 2015 წლის პირველ ნახევარში.

ცენტრალური კრიმინალური პოლიციის დეპარტამენტის მიერ სსკ-ის 284-ე, 285-ე, 286-ე მუხლებით რეგისტრირებული და გახსნილი დანაშაული								
პერიოდი	სსკ-ის 284-ე-286-ე მუხლი		სსკ-ის 284-ე მუხლი		სსკ-ის 285-ე მუხლი		სსკ-ის 286-ე მუხლი	
	სულ რეგის.	გახსნ.	სულ რეგის.	გახსნ.	სულ რეგის.	გახსნ.	სულ რეგის.	გახსნ.
2014 წ.	43	5	33	3	5	2	5	0
2015 წ. (პირველი ნახევარი)	25	0	17	0	2	0	6	0

ქვემოთ მოყვანილი მესამე ცხრილი ასახავს შსს-ის ცენტრალური კრიმინალური პოლიციის დეპარტამენტისა და შსს-ის ტერიტორიული და სტრუქტურული დანაყოფების მიერ სისხლის სამართლის კოდექსის სსკ-ის 255 მუხლით რეგისტრირებული და გახსნილი კიბერდანაშაულის რაოდენობას 2014 წელსა და 2015 წლის პირველ ნახევარში. 255-ე მუხლით ისჯება პორნოგრაფიული პროდუქციის უკანონოდ დამზადება ან/და წინასწარი შეცნობით არასრულწლოვნის გამოსახულების შემცველი პორნაგრაფიული პროდუქციის შეძენა, შენახვა, ჩვენებაზე დასწრება, შეთავაზება, გავრცელება, გადაცემა, რეკლამირება, ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ან ასეთი პროდუქციით სარგებლობა.[42]

სსკ-ის 255-ე მუხლით რეგისტრირებული დანაშაული				
	2014 წელი		2015 წ. (პირველი ნახევარი)	
	სულ რეგის.	გახსნ.	სულ რეგის.	გახსნ.
შსს ტერიტორიული და სტრუქტურული დანაყოფების მიერ	9	2	1	1
შსს ცენტრალური კრიმინალური პოლიციის დეპარტამენტის მიერ (მათ შორის)	8	2	1	1

შსს-ის 2014 წლისა და 2015 წლის პირველი ნახევრის მონაცემებში არ აღირიცხება სსკ-ის 255.1 მუხლით ჩადენილი დანაშაული, რომელიც ითვალისწინებს არასრულწლოვნის ჩაბმას პორნოგრაფიული ან პორნოგრაფიული ხასიათის სხვა პროდუქციის უკანონოდ დამზადებასა და გასაღებაში.[43]

შსს-ის მიერ მოწოდებული სტატისტიკა არ ასახავს სსკ-ის შემდეგი მუხლებით ჩადენილ დანაშაულს: 180-ე მუხლი, რომელიც არის თაღლითობა, ანუ მართლსაწინააღმდეგო მისაკუთრების მიზნით სხვისი ნივთის დაუფლება ან ქონებრივი უფლების მიღება მოტყუების გზით; 189-ე მუხლი, რომელიც არის საავტორო უფლებისა თუ რაიმე მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა; 210-ე მუხლი – ყალბი საკრედიტო ან საანგარიშსწორებო ბარათის დამზადება, გასაღება ან გამოყენება. მიზეზი ამისა ის არის, რომ შინაგან საქმეთა სამინისტრომ სულ ახლახან დაიწყო კომპიუტერული ტექნოლოგიების გამოყენებით ჩადენილი რეგისტრირებული და გახსნილი დანაშაულის სტატისტიკური აღრიცხვა. ამისათვის შსს მუშაობს ზუსტი მეთოდოლოგიების შემუშავებისა და აღრიცხვიანობის გაუმჯობესების მიმართულებით. სსკ-ის 324.1 მუხლით ჩადენილი დანაშაულის გამოძიება, რომელიც ეხება კიბერტერორიზმს, ახლადშექმნილი სახელმწიფო უსაფრთხოების სამსახურის კონტრტერორისტული ცენტრის პრეროგატივაა. ეს ცენტრი ადრე შსს-ის დაქვემდებარებაში იყო.

შსს-ის მიერ მოწოდებული მონაცემები სრულად ვერ ასახავს არსებულ მდგომარეობას, რაც შესაძლოა ოთხი ფაქტორით იყოს განპირობებული: პირველი – კიბერდანაშაულის შესახებ ცნობიერების დაბალი დონე როგორც მოსახლეობის, ისე ხელისუფლების იმ წარმომადგენლებისა, რომლებიც უშუალოდ არ მონაწილეობენ ქვეყნის კიბერსივრცის უსაფრთხოებაში. მაგალითად, კიბერშეტევებს მსოფლიოს ახალ ამბებში მნიშვნელოვანი ადგილი უკავია, საქართველოს მედიასივრცეში კი ამაზე თითქმის არაფერს ამბობენ და ეს არც დისკუსიის საგანს წარმოადგენს. ამ სფეროში ცნობიერების დონე საქართველოში არასახარბიელოა. შესაძლოა, ვიღაც კიბერდანაშაულის მსხვერპლი ისე გახდეს და იზარალოს, რომ ამის შესახებ არც კი იცოდეს და ვერც მიხვდეს, თუ როგორ იქცა მსხვერპლად. მეორე – შესაძლოა ზოგიერთი ბანკი ფარავდეს კიდეც დანაკარგებს და რეპუტაციის შელახვის შიშით არ თვლიდნენ საჭიროდ ასეთი შემთხვევების შესახებ სამართალდამცავ ორგანოებში განცხადებას. მესამე – კიბერდამოკიდებული დანაშაულის განსზაღვრისას ძნელია ის სხვა რამეში აგერიოს, თუმცა კიბერშესაძლებელი დანაშაული, მაგალითად, შესაძლოა თავისუფლად დახასიათდეს, როგორც წმინდა თაღლითობა ან ქურდობა. რაც უფრო გაიზრდება კიბერდანაშაულის მოცულობა, მით უფრო უკეთესი შეტყობინებისა და აღრიცხვიანობის სისტემა იქნება საჭირო. დაბოლოს, მიუხედავად იმისა, რომ, მაგალითად, კერძო კომპანიებს კანონით მოეთხოვებათ დანაშაულის შესახებ აცნობონ სამართალდამცავებს, არ არსებობს მექანიზმი, რომელიც შეამოწმებს, დაუმალეს თუ არა კიბერდანაშაული შესაბამის ორგანოებს.

იმის გათვალისწინებით, რომ კიბერდანაშაულის წინააღმდეგ ბრძოლის სამართველოს მიერ აღმოჩენილი შემთხვევების გარდა, შესაძლოა არსებობდეს კიბერდანაშაულის სხვა შემთხვევებიც, ქვემოთ მოყვანილი მაგალითები კარგად ასახავს კიბერდანაშაულის მახასიათებლებსა და ტიპებს საქართველოში.

- **ზიანის მომტანი პროგრამები** – მავნე პროგრამების გამოყენებით თავდამსხმელებმა საფრთხე შეუქმნეს ინფორმაციის ერთიანობასა და ხელმისაწვდომობას ქართულ ნიუსპორტალებზე (droni.ge; pressa.ge; news.ge).
- **აზარტული ონლაინთამაშების საიტზე ჰაკინგი** – დამნაშავემ შეაღწია „აჭარაბეთის“ ვებგვერდის თერთმეტი მომხმარებლის პირად ანგარიშზე და იქ არსებული თანხა, დაახლოებით 3,900 ლარი, საკუთარ ანგარიშზე გადარიცხა. მეორე შემთხვევაში – ჰაკერმა უკანონოდ შეაღწია „ევროპაბეთის“ საიტის მომხმარებლის პირად ანგარიშზე და მოხსნა 3,300 ლარი.
- **სამთავრობო კომპიუტერის გატეხვა** – ქართველი მოზარდი უკანონოდ შევიდა საჯარო სამსახურის ბიუროს ქსელში და ორი დღის განმავლობაში საფრთხე შეუქმნა მონაცემთა კონფიდენციალურობას, მთლიანობას და ხელმისაწვდომობას.
- **კიბერხულიგნობა** – ჰაკერებმა დატოვეს ანიმაციური გამოსახულება და შეტყობინება სახელმწიფო მინისტრის აპარატის ოფიციალურ ვებგვერდზე, რომ საიტის გატეხვა მარტივად ხელმისაწვდომი იყო მათთვის.
- **ჰაკინგი ფეიბოქსის გამოყენებით** – ჰაკერმა შეაღწია საგადახდო მომსახურების პროვაიდერის – „ნოვატექნოლოჯის“ კომპიუტერულ სისტემაში და კომპანიის გადახდის სისტემა www.paybox.ge-ის გამოყენებით მიითვისა „ნოვატექნოლოჯის“ კუთვნილი ნახევარ მილიონზე მეტი ლარი.
- **საკრედიტო ბარათის კლონირება** – ორმა ქართველმა და ექვსმა უკრაინელმა კიბერდამნაშავემ უკანონო გზით დიდი ბრიტანეთის სხვადასხვა ბანკის მომხმარებლის ანგარიშებიდან (1137 პლასტიკური ბარათიდან) £170 000 ფუნტი სტერლინგის ოდენობის თანხა მოხსნა და ონლაინგადახდის საშუალებით ინტერნეტკაზინოს 45 მომხმარებელის ანგარიშზე გადარიცხა.
- **ჰაკინგი და შანტაჟი** – ლატვიელმა ჰაკერებმა საფრთხე შეუქმნეს საბანკო კომპიუტერული სისტემის მონაცემთა კონფიდენციალურობას. ჰაკერები დაუკავშირდნენ ბანკის აღმასრულებელ დირექტორს და მოსთხოვეს თანხა იმისათვის, რომ არ გამოექვეყნებინათ მოპარული ინფორმაცია.
- **ბავშვთა პორნოგრაფია** – ინტერპოლმა მიაწოდა კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველოს ინფორმაცია ქართულ სერვერზე მოზარდის ექსპლოატაციის ამსახველი გამოსახულების გაყიდვის მცდელობის შესახებ. დამნაშავე აღმოჩნდა ბავშვის დედა.
- **ბოტნეტი** – შინაგან საქმეთა სამინისტროს ოპერატიულ-ტექნიკურ დეპარტამენტთან ერთად კიბერდანაშაულის განყოფილებამ აღმოაჩინა ბოტნეტი სამი ათასი ზომბირებული კომპიუტერის შემცველი ქსელით.

- **კიბერშპიონაჟი** – ამერიკული კომპანია *FireEye*-ის 2014 წლის „*APT28*“ – ანგარიშის მიხედვით, სხვა დასავლური ქვეყნების პარალელურად, საქართველოს სამთავრობო საიტები და ოფიციალური პირებიც იყვნენ წლების განმავლობაში რუსული კიბერშპიონაჟის სამიზნეები.
- **თაღლითობა ე.წ სიმბოქსების გამოყენებით** – დამნაშავეებმა ავტორიზაციის გარეშე დაამონტაჟეს ინტერნეტსიგნალის მიმღები სპეციალური მოწყობილობა ე.წ. სიმბოქსი, რომლის მეშვეობითაც საზღვარგარეთიდან განხორციელებული სატელეფონო ზარი, ინტერნეტტრაფიკის გამოყენებით გარდაიქმნებოდა ლოკალურ ზარად და როგორც ქვეყნის შიგნით განხორციელებული ზარი, ისე მიეწოდება საქართველოში მოქმედ კავშირგაბმულობის კომპანიების აბონენტებს. კომპანიების ზარალმა 95,000 ლარი შეადგინა.

შინაგან საქმეთა სამინისტროს წარმომადგენლებმა აღნიშნეს, რომ უკანასკნელი ტიპის დანაშაული ქართულ კიბერსივრცეში ახალი ტენდენციაა.

ისეთი პატარა ქვეყნისთვისაც კი, როგორიც საქართველოა, მიუხედავად იმისა, რომ, სავარაუდოდ, კიბერშემთხვევების შესახებ ინფორმაცია არასრულია, კიბერდანაშაულის საკმაოდ დაბალი მაჩვენებელია. გარდა ამისა, არსებული კიბერდანაშაულის შემთხვევების განხილვისას მნიშვნელოვანია სამ ძირითად ფაქტორს გაესვას ხაზი. პირველი – საქართველოში ჩადენილ კიბერდანაშაულთა უმრავლესობა არ არის განსაკუთრებით შემოქმედებითი. მეორე – ისინი არ არიან ტექნოლოგიურად დახვეწილი (თუმცა შსს-ის წარმომადგენლებმა ჩვენთან საუბრისას ხაზი გაუსვეს კიბერდანაშაულის შემოქმედებითი და ტექნოლოგიური დახვეწის ზრდის ტენდენციას. ეს შენიშვნა არ ეხება საქართველოს წინააღმდეგ მიმართულ მაღალი დონის კიბერშპიონაჟის ფაქტებს) და მესამე – ისინი არ შეიცავენ ძალიან მაღალ ფინანსურ რისკებს – ზედა ზღვარი შეადგენს დაახლობით 620,000 ლარს (£170,000); დანაშაულთა უმეტესობა რამდენიმე ათას ლარს მოიცავს.

ამ ანგარიშში უკვე გაესვა ხაზი კიბერდანაშაულის მთლიანი ღირებულების გლობალური ჯამიდან ინტერპოლირების არაეფექტურობას ლოკალურ მაჩვენებელში. კიბერდანაშაულის ღირებულების დასადგენად შეიძლება საკმაოდ მარტივი გზის გამოყენება – 2014 წელს რეგისტრირებული 200-ზე მეტი დანაშაულით მიღებული ზარალის შეკრება. ეს, მართალია, არ გვიჩვენებს არამატერიალური ფაქტორების ღირებულებას, მაგრამ ამას არც ერთი სხვა მეთოდოლოგია არ იძლევა.

შსს-ის მონაცემების დაბალ მაჩვენებელს შესაძლოა ასევე განაპირობებდეს კერძო კრიტიკული ინფრასტრუქტურების მიმართ მიდგომებიც. ბანკები, მობილური კავშირგაბმულობის კომპანიები და პორტები ცდილობენ უსაფრთხოების საუკეთესო პრაქტიკის დანერგვას და განხორციელებას. თუმცა მათ მოტივაციას უფრო განაპირობებს საერთაშორისო სტანდარტების დაცვისა თუ ინვესტორთა მოლოდინის გამართლების ინტერესი ან პოლიტიკურად მოტივირებული კიბერშეტევების შიში, ვიდრე ზემოაღნიშნული წმინდა კიბერკრი-

მინალის ტიპი. ერთ-ერთმა აღმასრულებელმა დირექტორმა ჩვენთან საუბრისას განაცხადა, რომ მისი კომპანიის კომპიუტერულ სისტემებში წმინდა კიბერკრიმინალის მიზნით უკანონოდ შეღწევის არანაირი შემთხვევა არ დაფიქსირებულა.

ქართველები სხვებზე მეტად ან ნაკლებად პატიოსანი ერი არ არის, საქართველოს წერა-კითხვის ცოდნის თითქმის 100%-იანი მაჩვენებელი აქვს[44] და რუსეთისა და უკრაინის მსგავსად საქართველოც ებრძვის საბჭოთა მემკვიდრეობას – აქ დიდ შესაძლებლობებს ნორმალური დასაქმებისა და ანაზღაურების დაბალი მოლოდინი ახლავს. მხედველობაში თუ მივიღებთ ინტერნეტჩართულობის მაჩვენებელს ქვეყანაში, რაც მოსახლეობის თითქმის ნახევარს წარმოადგენს და ინტერნეტტექნოლოგიებზე დამოკიდებულების ზრდის ტენდენციებს, სავსებით სავარაუდოა, რომ კიბერდანაშაულის მაჩვენებელი გაიზარდოს.

ეს შეიძლება აიხსნას სხვადასხვა ფაქტორის ერთობლიობითაც: საქართველოში პოტენციური ანაზღაურების სიმცირემ, ყველასგან განსხვავებულმა ქართულმა ენამ და სხვაგან უფრო მიმზიდველმა შესაძლებლობამ განაპირობა ალბათ ქვეყანაში კიბერდანაშაულის შედარებით დაბალი მაჩვენებელი. სავარაუდოდ, უნდა არსებობდნენ ნიჭიერი ქართველი კიბერკრიმინალები, რომლებმაც ქართულის გარდა იციან რუსული, ინგლისური და სხვა ენები და რომლებიც საკუთარ შესაძლებლობებს უფრო სარფიანი სამიზნეების წინააღმდეგ იყენებენ. კიბერდანაშაულის ქართული ბაზარი კი ძირითადად ე.წ. სკრიპტკიდებისა და მხოლოდ მცირერიცხოვანი შედარებით ნიჭიერი ჰაკერების მოქმედების არეალად რჩება.

თუ პარალელს გავავლებთ დანაშაულის სხვა სფეროებთან, ქართველმა კიბერკრიმინალებმაც შეიძლება ითანამშრომლონ ორგანიზებული კიბერდანაშაულის რუსულენოვან დაჯგუფებებთან. კრიმინალის სხვა სფეროებში ქართული კრიმინალური დაჯგუფებები, ე.წ. лаврушники – კანონიერი ქურდები – მთელ ევრაზიაში მოქმედებენ, როგორც რუსული კრიმინალის შემადგენელი ნაწილი.[45]

კიბერშპიონაჟი და კიბერომი

კიბერშპიონაჟი და კიბერომი მტკიცედ დამკვიდრდა ვირტუალურ სამყაროში და ამ მხრივ არც საქართველოა გამონაკლისი. საქართველო უკვე იყო კიბერომის ერთ-ერთი სამიზნე, ასევე აღრიცხულია საქართველოს წინააღმდეგ კიბერშპიონაჟის არაერთი შემთხვევა. კიბერშპიონაჟი და კიბერომი, მართალია, განსხვავდება წმინდა კიბერკრიმინალისგან, მაგრამ საქართველოს შემთხვევაში მნიშვნელოვანია ამ სამივე ტიპის სამი მიზეზის გამო გაანალიზება:

პირველი შპიონაჟი დანაშაულია, რომლის კიბერასპექტები შეიძლება შეიცავდეს კიბერდამოკიდებული ან კიბერშესაძლებელი დანაშაულის ფორმებს. ძირითადად ის, რასაც შეიძლება კიბერომი ეწოდოს (თუკი გამოვრიცხავთ ისეთ მავნე პროგრამას, როგორიც, მაგალითად, Stuxnet-ია, რომელსაც ფაქტობრივად ფიზიკური ზარალის მოტანა შეუძლია), შესაძლოა იყოს კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დარღვევის მიზნით კომპიუტერულ ქსელში უკანონო შეღწევის კრიმინალური აქტი. ამგვარი ქმედება მიჩნეული იქნება კიბერდანაშაულად, სანამ არ გამოიკვეთება უცხო ქვეყნის მთავრობის ან რომელიმე სუბნაციონალური ჯგუფის მონაწილეობის ნიშნები, რომლის უკანაც სტრატეგიული მიზნები დგას. მაგალითად, მტრულად განწყობილი ქვეყნის მთავრობებისაგან ინიცირებული კიბერთავდასხმა შესაძლოა განხორციელდეს ელექტრომომარაგების, სატრანსპორტო ან ფიჭური სატელეფონო კომპანიების კომპიუტერულ სისტემებზე, თუნდაც იმ მიზნით, რომ წარმოქმნას ქაოსი, მოახდინოს მოსახლეობის დემორალიზაცია ან თუნდაც ბრძოლის ველი კინეტიკური შეტევისთვის მოამზადოს. აღსანიშნავია, რომ თავიდან ეს იქნებოდა კვალიფიცირებული, როგორც უკანონო შეღწევა კომპიუტერულ სისტემაში, მიუხედავად იმისა, რა აღმოჩნდებოდა შეღწევის საბოლოო მიზანი – კიბერომი, კიბერშპიონაჟი თუ წმინდა კიბერკრიმინალი.

მეორე საქართველოს გეოპოლიტიკური მდებარეობისა და არსებული გამოცდილების გათვალისწინებით, საქართველოს ოფიციალური პირების უმეტესობა შედარებით უფრო მძაფრად აღიქვამს კიბერშპიონაჟისა და კიბერომის საფრთხეებს, ვიდრე წმინდა სახის კიბერდანაშაულს. ეს კარგად ჩანს როგორც *საქართველოს ეროვნული უსაფრთხოების კონცეფციაში*, ისე მაღალი თანამდებობის პირებთან საუბრისას. ქვეყნებს, რომლებიც ცდილობენ საქართველოსთან თანამშრომლობას, უნდა ესმოდეთ საქართველოს მიდგომა და ის საფრთხეები, რომელთა წინაშეც დგას ეს ქვეყანა.

შესაძლოა ვიღაცისთვის საკამათო იყოს, მართლა ჩართულია თუ არა რუსეთის სამთავრობო სტრუქტურები საქართველოს წინააღმდეგ განხორციელებულ კიბერშპიონაჟსა და კიბერშეტევებში, მაგრამ ეჭვს არ იწვევს რუსი კიბერკრიმინალური ჯგუფის ან ჯგუფების მიერ განხორციელებული შეტევები, რომელთა უკანაც მხოლოდ წმინდა პოლიტიკური მოტივი დგას. ეს კი სათანადო ანალიზის საშუალებას გვაძლევს, რომ განვსაზღვროთ, თუ ვის ინტერესებში უნდა შედიოდეს ამ ტიპის კიბერშეტევები.

კიბერშპიონაჟი

2014 წლის ოქტომბერში კიბერუსაფრთხოების საკითხებზე მომუშავე ამერიკულმა კომპანია *FireEye*-მ გამოაქვეყნა ანგარიში სახელწოდებით „APT 28: A Window into Russia's Cyber Espionage Operations." ანგარიში რუსეთის მასობრივი კიბერშპიონაჟის დიდხნიან შემთხვევას ასახავს. კვლევის ავტორები მიიჩნევენ, რომ მიზანმიმართული საფრთხის შემცველი, APT 28-ის სახელით ცნობილი ჯგუფის მიერ განხორციელებული კიბერშპიონაჟი დიდი ალბათობით შესაძლოა ფინანსდებოდეს რუსეთის სამთავრობო სტრუქტურებისგან. ანგარიშის თანახმად, ზემოხსენებული ჯგუფი ახორციელებდა მიზანმიმართულ შპიონაჟს, სულ მცირე, 2007 წლიდან. კიბერშპიონაჟის ამ კამპანიის მთავარ მიზანს წარმოადგენდა „იმ სახის ინფორმაციის მოპოვება, რომელიც მხოლოდ სახელმწიფო ინტერესების საგანი შეიძლებოდა ყოფილიყო". ჯგუფის სამიზნეს წარმოადგენს ამერიკის შეერთებული შტატები, აღმოსავლეთ ევროპის ქვეყნები, ჩრდილოატლანტიკური ხელშეკულების ორგანიზაცია, ევროპის უშიშროებისა და თანამშრომლობის ორგანიზაცია და საქართველოს მთავრობა და ოფიციალური პირები. ამ ტიპის კიბეროპერაცია, ნათქვამია კვლევაში, „მიგვანიშნებს მთავრობის მიერ დაფინანსებულ კიბერშპიონაჟზე, კონკრეტულად კი – იმ მთავრობისა, რომელიც მოსკოვში ზის".[46]

რამდენიმე წლის წინ ქართულმა CERT-მა (კომპიუტერულ საფრთხეებზე სწრაფი რეაგირების ჯგუფი) საერთაშორისო აღიარება მოიპოვა საქართველოს წინააღმდეგ მიმართული კიბერშპიონაჟისათვის შექმნილი Win32/Georbot ვირუსის აღმოჩენისა და მასზე რეაგირების გამო. კიბერშპიონაჟის ამ კონკრეტული შემთხვევის შესახებ დეტალურ ანალიზს გვთავაზობს საქართველოს CERT-ის ანგარიში.[47]

ჯეორბოტი საქართველოში 2011 წლიდან Windows-ის ოპერაციულ სისტემაზე მომუშავე კომპიუტერებში ეძებდა სუსტ მხარეებს ექსპლოატაციის მიზნით. თავდაპირველად ჯეორბოტ-ტროიანი გავრცელდა, "*Watering-hole"-ის* ტიპის შეტევითი სტრატეგიით. *Watering Hole* -ის ტიპის შეტევის სტარტეგია პირველად კომპიუტერული და ქსელური უსაფრთხოების ამერიკულმა კომპანია *RSA Security*-მ განსაზღვრა. ამ შემთხვევაში თავდამსხმელის სამიზნეა გარკვეული ჯგუფი, ორგანიზაცია ან, თუნდაც, რეგიონი. თავდამსხმელი დაკვირვებით ან ინტუიციურად ხვდება, თუ რომელ ვებგვერდებს შეიძლება სტუმრობდეს სამიზნე და რა სახის ინფორმაციით შეიძლება ინტერესდებოდეს

იგი. აინფიცირებს ერთ ან რამდენიმე ასეთ საიტს და შედეგად ინფიცირდება სამიზნე ჯგუფის რამდენიმე წევრის კომპიუტერული სისტემა.

ამ კონკრეტულ შემთხვევაშიც დამნაშავეებმა შეძლეს ქართული ახალი ამბების რამდენიმე პორტალის ინფიცირება *ჯეორბოტ-ტროიანით*. ჰაკერებმა დააინფიცირეს ქართული საინფორმაციო საიტების მხოლოდ ის გვერდები, სადაც განთავსებული იყო ინფორმაცია თავდაცვისა და უსაფრთხოების საკითხების შესახებ. ნებისმიერი მომხმარებლის კომპიუტერული სისტემა, რომელიც შევიდოდა საიტის ამ გვერდებზე, ავტომატურად ხდებოდა ჯეორბოტის მსხვერპლი.

ჯეორბოტის მიზანი იყო კომპიუტერში აღმოეჩინა და მოეპარა ის დოკუმენტები, რომლებშიც გამოყენებული იყო უსაფრთხოებასთან დაკავშირებული სიტყვები – ნატო, სი-აი-ეი, ეფ-ბი-აი, დაზვერვა, ეფ-ეს-ბი, გენერალი, პოლკოვნიკი და ა.შ. მათი აღმოჩენის შემთხვევაში ამ ფაილების გადაწერა ხდებოდა ვირუსის სამართავ სერვერზე.

ჯეორბოტი სრულად აკონტროლებდა ინფიცირებულ კომპიუტერებს. მას შეეძლო ვიდეო და აუდიო მასალის ჩაწერა კომპიუტერში არსებული კამერისა და მიკროფონის საშუალებით; მომხმარებლის კომპიუტერის *სამუშაო დაფის* გადაღება, დოკუმენტების მოპარვა; ნებისმიერი ფაილის გაგზავნა დისკიდან სერვერის მიმართულებით; ქსელში არსებული სხვა კომპიუტერების სკანირება/ინფიცირება. მას შემდეგ, რაც *ჯეორბოტი* აღმოაჩინა საქართველოს CERT-მა და კომუნიკაცია მისი ბრძანებისა და კონტროლის სერვერთან დაიბლოკა, ტროიანის გავრცელება დაიწყო სპამფოსტის საშუალებით. ინფიცირებული კომპიუტერების საერთო რაოდენობა იყო 390, აქედან 70% – საქართველოდან.

საქართველოს CERT-მა მოახდინა საქართველოში ყველა ინფიცირებული IP-ის იდენტიფიცირება და ვირუსული ფაილების ღრმა ანალიზის შედეგად შემუშავდა განეიტრალებისთვის საჭირო ტექნიკური მექანიზმები და გადაეგზავნა დაინფიცირებულ უწყებებს.

საქართველოს CERT-ი თანამშრომლობდა მეგობარი ქვეყნების სამართალდამცავ უწყებებთან, კომპიუტერული საფრთხეების წინააღმდეგ სწრაფი რეაგირების ჯგუფებთან და კომპიუტერული სისტემების უსაფრთხოების ისეთ კომპანიებთან, როგორიცაა Microsoft, ESET, Snort, Cisco და სხვადასხვა ანტივირუსის მწარმოებელ კომპანიებთან დაცვის მექანიზმების შესამუშავებლად.

საქართველოს CERT-მა შექმნა დოკუმენტი ცრუ სახელწოდებით „საქართველო-ნატოს შეთანხმება 2011“. იცოდნენ რა, რომ ამგვარი დოკუმენტი თავდამსხმელის ინტერესს გამოიწვევდა, მას მიება შემტევის შექმნილი ვირუსული ფაილი. კიბერშემტევმა მოიპარა და გადაწერა ცრუ დოკუმენტი და შედეგად თავადვე დაინფიცირდა საკუთარი ვირუსული ფაილით. თავდამსხმელის შეცდომაში შეყვანით შესაძლებელი გახდა შემტევის იდენტიფიცირება. დამნაშავის კომპიუტერზე კონტროლის მოპოვების შედეგად საქართველოს CERT-მა მოიპოვა დამნაშავის მიმოწერა რუს ჰაკერულ ფორუმებზე, რომელიც დახმარებას ითხოვდა გაშიფვრის მექანიზმებისა და ექსპლოიტების შემუშავებაში. ჰაკერის მეტსახელია „ეშკინკოტ 1“. CERT-მა შეძლო დამნაშავის კომპიუტერში არსებული ვიდეოთვალის მეშვეობით მისთვის ფოტოს გადაღება. მიღებული ინფორმაციის საფუძველზე მოხერხდა პიროვნების იდენტიფიცირება. ის რუსეთში მოქმედი ცნობილი ჰაკერია.

ჯეორბოტი იყო კიბერშპიონაჟისთვის შექმნილი ტროიანვირუსი. დაინფიცირებული ქართული კომპიუტერების უმრავლესობა ეკუთვნოდა ქართულ სამთავრობო სტრუქტურებს და კრიტიკული ინფორმაციული ინფრასტრუქტურის ორგანიზაციებს. ასევე რამდენიმე შემთხვევაში დაინფიცირებული იყო საბანკო სექტორის, არასამთავრობო ორგანიზაციებისა და კერძო კომპანიის კომპიუტერები.

კიბერომი

2008 წელს საქართველო იყო პირველი ქვეყანა, სადაც კინეტიკური ომის ფორმების პარალელურად განხორციელდა კიბერშეტევები. ერთწლიანი კვლევის შემდეგ აშშ-ის კიბერკვლევის ჯგუფი – US-CCU – დამოუკიდებელი კვლევითი ინსტიტუტი თავის ანგარიშში წერდა: „შეტევების დიდი ნაწილი, დროის თვალსაზრისით, იმდენად ახლოს იყოს სამხედრო ქმედებებთან, რომ წარმოუდგენელია არ ყოფილიყო მჭიდრო კოორდინირებული თანამშრომლობა რუსეთის სამხედრო სტრუქტურების წარმომადგენლებსა და სამოქალაქო კიბერკრიმინალებს შორის". US-CCU-ის ანგარიშში აღნიშნულია, რომ საქართველოს წინააღმდეგ გამოყენებული ბოტნეტების უმეტესობა ადრეც იყო გამოყენებული სხვა კრიმინალური ქმედებებისთვის. ამერიკის კომპიუტერული უსაფრთხოების მკვლევართა ნაწილმა, რომლებიც ბოტნეტშეტევებს სწავლობენ, აღნიშნეს, რომ აშკარად ჩანდა რუსული ბიზნესქსელის – კიბერკრიმინალური სინდიკატის მონაწილეობის ნიშნები.[48] კიბერშეტევებმა საქართველოში რამდენიმე დღით გათიშა მთავრობის საინფორმაციო და საკომუნიკაციო საშუალებები, ახალი ამბების პორტალები, ფინანსური ტრანზაქციები და ინტერნეტი.

საქართველოზე კიბერთავდასხმების ერთ-ერთი ტაქტიკა იყო ვებგვერდებზე დადებული ინსტრუქციები იმ მოხალისე პირთათვის, რომელთაც სათანადო კომპიუტერული უნარები არ გააჩნდათ, მაგრამ ამ ინსტრუქციების მეშვეობით საშუალება მიეცათ თავიანთი წვლილი შეეტანათ კიბერთავდასხმების განხორციელებაში. ეს სტრატეგია იმდენად ეფექტური იყო, რომ 43 სამიზნე ვებგვერდიდან ზოგს პირვანდელი სახე შეეცვალა და ზოგიც საერთოდ გაითიშა. ამას გარდა 11 ვებგვერდი იმ ბოტნეტების მსხვერპლი გახდა, რომლებიც რუსულ ორგანიზებულ დანაშაულებრივ ჯგუფთან ასოცირდებოდა. სოციალური ქსელები და ამ შეტევისთვის სპეციალურად შექმნილი ვებგვერდები stopgeorgia.ru და stopgeorgia.info (შეაჩერეთ საქართველო) გამოიყენებოდა მოხალისე ჰაკერების შერჩევისა და დაქირავებისთვის. ამ საიტების სერვერები განთავსებული იყო აშშ-ში, გერმანიასა და ლატვიაში. მანამდე კი ამავე სერვერებით სარგებლობდნენ ორგანიზებული დანაშაულებრივი ჯგუფები, კერძოდ კი, რუსული ბიზნესქსელი.[49]

სეკურიტიზაცია და როგორ უყურებს საქართველო კიბერდანაშაულს, კიბერშპიონაჟსა და კიბერომს

სეკურიტიზაციის კონცეფცია (ინგლისური სიტყვიდან Securitization) განსაზღვრავს იმას, თუ რა ხარისხით აღიქვამს ქვეყანა არსებულ საფრთხეებს. სეკურიტიზაციის კონცეფცია შეიმუშავეს და განავითარეს არნოლდ ვოლფერსმა 1952 წელს[50] და ბერი ბუზანმა 1997 წელს.[51] სეკურიტიზაცია არის პროცესი, როდესაც საფრთხე ქვეყნისათვის ეგზისტენციალურ საფრთხედ აღიქმება და პრობლემა არ განიხილება მხოლოდ იურიდიული ან ტექნიკური მნიშვნელობით. მაგალითად, აშშ-მ თავის დროზე მოახდინა საბჭოთა ბირთვული იარაღის საფრთხის სეკურიტიზაცია, ხოლო 2001 წლის 11 სექტემბრის შემდეგ – ტერორიზმის საფრთხის სეკურიტიზაცია.

მიუხედავად საქართველოს 2008 წლის გამოცდილებისა და მიუხედავად იმისა, რომ კიბერსაფრთხეები საქართველოს ეროვნული უსაფრთხოების ერთერთ მთავარ საფრთხედ აღიქმება, საქართველომ დღემდე ვერ შეძლო კიბერსაფრთხის ამ ხარისხში აყვანა.

მაგალითად, ესტონეთის მთავრობამ განსაკუთრებული ყურადღება დაუთმო კიბერუსაფრთხოებას. ესტონეთის პრეზიდენტი ტომას ჰენდრიკ ილვესი მუდამ კიბერუსაფრთხოების მნიშვნელობაზე ლაპარაკობს.[52] მეტიც, ესტონეთმა აშკარად იკისრა პროაქტიური როლი და ჩამოაყალიბა კიბერდაცვის ლიგა. ჩრდილოატლანტიკური ალიანსი მალევე გამოეხმაურა ესტონეთის წინააღმდეგ განხორციელებულ აგრესიულ კიბერთავდასხმებს და ესტონეთის ხელისუფლების ძალისხმევით ტალინში ნატოს კიბერთავდაცვის ცენტრი დაარსდა.

2008 წელს რუსეთის მიერ განხორციელებულმა კიბერშეტევებმა ინტერნეტპოლიტიკის განვითარებისკენ უბიძგა საქართველოსაც. 2008 წლიდან მოყოლებული საქართველომ მრავალი ნაბიჯი გადადგა და გააუმჯობესა თავისი შესაძლებლობები კიბერუსაფრთხოების სფეროში, თუმცა ამ მიმართულებით გაცილებით მეტია გასაკეთებელი. სამწუხაროდ, ზოგადად, გარდა იმ ადამიანებისა, რომლებიც უშუალოდ პასუხისმგებელი არიან ქვეყნის კიბერსივრცის უსაფრთხოებაზე, კიბერუსაფრთხოებას ერთ-ერთ რუტინულ საქმედ მიიჩნევენ.

მიუხედავად იმისა, რომ ოფიციალური განცხადებები და დოკუმენტები კიბერუსაფრთხოებას დიდ უპირატესობას ანიჭებენ, ბიუჯეტი არ შეესაბამება დეკლარირებულ პოლიტიკას. თავის მხრივ, არასაკმარისი ბიუჯეტით აიხსნება ის, რაც აშკარად გამოჩნდა მთავრობის წარმომადგენლებთან საუბრებში, რომ, მაგალითად, საქართველოს სამთავრობო სტრუქტურების ძალიან ბევრი კომპიუტერული სისტემა მუშაობს არალიცენზირებული და მეკობრული პროგრამებით. ამ პრობლემის მოგვარება დიდ ფინანსურ რესურსებს მოითხოვს და, როგორც მთავრობის ერთმა წარმომადგენელმა ჩვენთან საუბრისას აღნიშნა, უფროსი თაობის ხელმძღვანელობას უბრალოდ არ ესმის ამ პრობლემის მნიშვნელობა.

კომპანია Software Alliance BSA-ის 2014 წლის ანგარიში – *გლობალური სოფტის მიმოხილვა* – აფასებს ქვეყნებს არალიცენზირებული კომპიუტერული პროგრამების გამოყენების მიხედვით. ამ ანგარიშში საქართველოს

90%-იანი მაჩვენებლი აქვს არალიცენზირებული პროგრამების გამოყენების მხრივ. ამ მაჩვენებლის კომერციული ღირებულება კი, ანგარიშის მიხედვით, დაახლოებით 40 მილიონი დოლარია.[53]

2014 წლის ევრაზიის თანამშრომლობის ფონდის კვლევის თანახმად, საქართველოში მეკობრული და არალიცენზირებული პროგრამები ფართოდაა გავრცელებული როგორც საჯარო, ისე კერძო სექტორში. ანგარიშში აღნიშნულია, რომ ცენტრალური და ადგილობრივი ხელისუფლების ორგანოებში არსებული 30 ათასი პერსონალური კომპიუტერიდან დაახლოებით 70%-ზე დაყენებული იყო მეკობრული ან არალიცენზირებული პროგრამები. ანგარიშში ნათქვამია, რომ „საქპატენტის“ ინფორმაციით, 2013-2014 წლებში მეკობრული კომპიუტერული პროგრამების საკითხის ირგვლივაც მიმდინარეობდა მოლაპარაკებები საქართველოს მთავრობასა და კომპანია Microsoft-ს შორის, რაც ითვალისწინებდა ლიცენზირებული კომპიუტერული პროგრამების დანერგვას სახელმწიფოს ყველა სტრუქტურაში.[54] მთავრობის ერთ-ერთმა წარმომადგენელმა ჩვენთან საუბრისას ამ საკითხის მოუგვარებლობა ფინანსური რესურსების ნაკლებობით ახსნა.

ინტელექტუალური საკუთრების დაცვა პირდაპირ რელევანტურია ქვეყნის ICT სფეროს განვითარებისა. საქართველო ინტელექტუალური საკუთრების დაცვის კუთხით ცდილობს თავისი კანონმდებლობა საერთაშორისო სტანდარტებს მიუახლოვოს. საქართველოს ინტელექტუალური საკუთრების ეროვნული ცენტრი „საქპატენტი“ არის ის ორგანო, რომელიც საქართველოში ინტელექტუალური საკუთრების პოლიტიკას განსაზღვრავს. საქართველომ რატიფიცირება მოახდინა ამ მიმართულების რიგი საერთაშორისო კონვენციებისა და 2014 წელს ახალი ცვლილებების პროექტი წარადგინა ინტელექტუალური საკუთრების შესახებ კანონებში სავაჭრო ნიშნების, პატენტების, დიზაინისა და საავტორო უფლებების მიმართულებით, რომ უფრო მეტად მიუახლოვდეს საერთაშორისო სტანდარტებს. თუმცა, მიუხედავად ამისა, ეს საკითხი კვლავ რჩება ნაკლებად პრიორიტეტულ მიმართულებად ქვეყანაში.

დაბოლოს, თუკი მხედველობაში მივიღებთ 2008 წლის შემდეგ გადადგმულ ნაბიჯებს და მთავრობის ოფიციალურ პირებთან საუბრებს, იქმნება შთაბეჭდილება, რომ კიბერუსაფრთხოება პრიორიტეტული საკითხია საქართველოში, თუმცა სამთავრობო სტრუქტურებში კიბერუსაფრთხოებაზე მომუშავე ვიწრო წრის მიღმა საკმარისად არ ესმით ეს პრობლემიტიკა და, აქედან გამომდინარე, არ არის საკმარისი დაფინანსება უფრო მასშტაბური კიბერპრობლემის მოსაგვარებლად.

იმ ადამიანების გარდა, ვინც ჩართულია კიბერდანაშაულთან ბრძოლაში – ასეთია ძირითადად შსს-ის კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველო – ინტერესი საქართველოში წმინდა კიბერკრიმინალის წინააღმდეგ ბრძოლის თვალსაზრისით ჩამორჩება პოლიტიკურად მოტივირებული შეტევების წინააღმდეგ ბრძოლის ინტერესს. სამწუხაროდ, ეს ამ საკითხისადმი პროკურატურისა და სასამართლო უწყების მიდგომაზეც აისახა.

დაინტერესებული მხარეები

ონლაინსივრცეში არსებობს სამი ტიპის დაინტერესებული მხარე: მთავრობა, კერძო სექტორი და კერძო პირი. მიუხედავად იმისა, რომ ტრადიციულ დისკუსიაში უსაფრთხოების საკითხებზე ყურადღება გამახვილებულია მთავრობის მნიშვნელოვან როლზე, კიბერუსაფრთხოებას ასევე აქცენტი გადააქვს ბიზნესზე. ბიზნესი დაინტერესებული მხარე სამი მნიშვნელოვანი ფაქტორის გამოა:

პირველი კერძო ბიზნესი ფლობს იმ ინფრასტრუქტურის დიდ ნაწილს, რომელიც უმნიშვნელოვანესია საზოგადოების ეფექტური ფუნქციონირებისთვის და, აქედან გამომდინარე, საზოგადოების უსაფრთხოებისთვის.

მეორე ბიზნესი არის ძალა, რომელსაც შეუძლია *ICT-ის* პოტენციალი ეკონომიკურ განვითარებად გარდაქმნას.

მესამე ბიზნესორგანიზაციები თავადაც *ICT* სერვისების მასშტაბური მომხმარებლები არიან.

დაბოლოს, არ უნდა დავივიწყოთ ინტერნეტის ინდივიდუალური მომხმარებელი. საქართველოში 2.18 მილიონი[55] ინტერნეტმომხმარებლიდან თითოეული დაკავშირებულია სისტემების ამ უკიდეგანო სისტემასთან იმგვარად, როგორც აქამდე არც ერთი ტრადიციული საზოგადოებრივი ცხოვრების ფორმით ყოფილა შესაძლებელი. და მაინც, მიუხედავად იმისა, რომ საქართველოს მოსახლეობის თითქმის ნახევარი ინტერნეტის მომხმარებელია და 1.22 მილიონი ქართველი აქტიურად იყენებს სოციალურ მედიას, კომპიუტერული ტექნოლოგიების, ინტერნეტის და კიბერუსაფრთხოების მნიშვნელობის სათანადოდ აღქმის დონე საკმაოდ დაბალია.

სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო – პრემიერ-მინისტრის კაბინეტი

საქართველოს მთავრობის კიბერუსაფრთხოების თემაზე უწყებათაშორისი კოორდინაცია პრეზიდენტისადმი დაქვემდებარებული ეროვნული უსაფრთხოების საბჭოს ფუნქცია იყო. საკონსტიტუციო ცვლილებების შედეგად ეს ფუნქცია გადაეცა პრემიერ-მინისტრის კაბინეტს. სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო, რომელსაც ხშირად უბრალოდ ეროვნული უსაფრთხოების საბჭოს ან მეორე ეროვნული უსაფრთხოების საბჭოს უწოდებენ, ახლა კოორდინაციას უწევს სხვადასხვა სამთავრობო სტრუქტურას (ერთეულს). საბჭო არის პრემიერ-მინისტრ ირაკლი ღარიბაშვილის საკონსულტაციო საბჭო, რომელიც უშუალოდ მას ექვემდებარება. შესაბამისად, პრემიერ-მინისტრი არის საბჭოს თავმჯდომარე.

საბჭო შედგება შემდეგი მუდმივი წევრებისგან: საბჭოს მდივანი, შინაგან საქმეთა მინისტრი, თავდაცვის მინისტრი, საგარეო საქმეთა მინისტრი და ფინანსთა მინისტრი.[56]

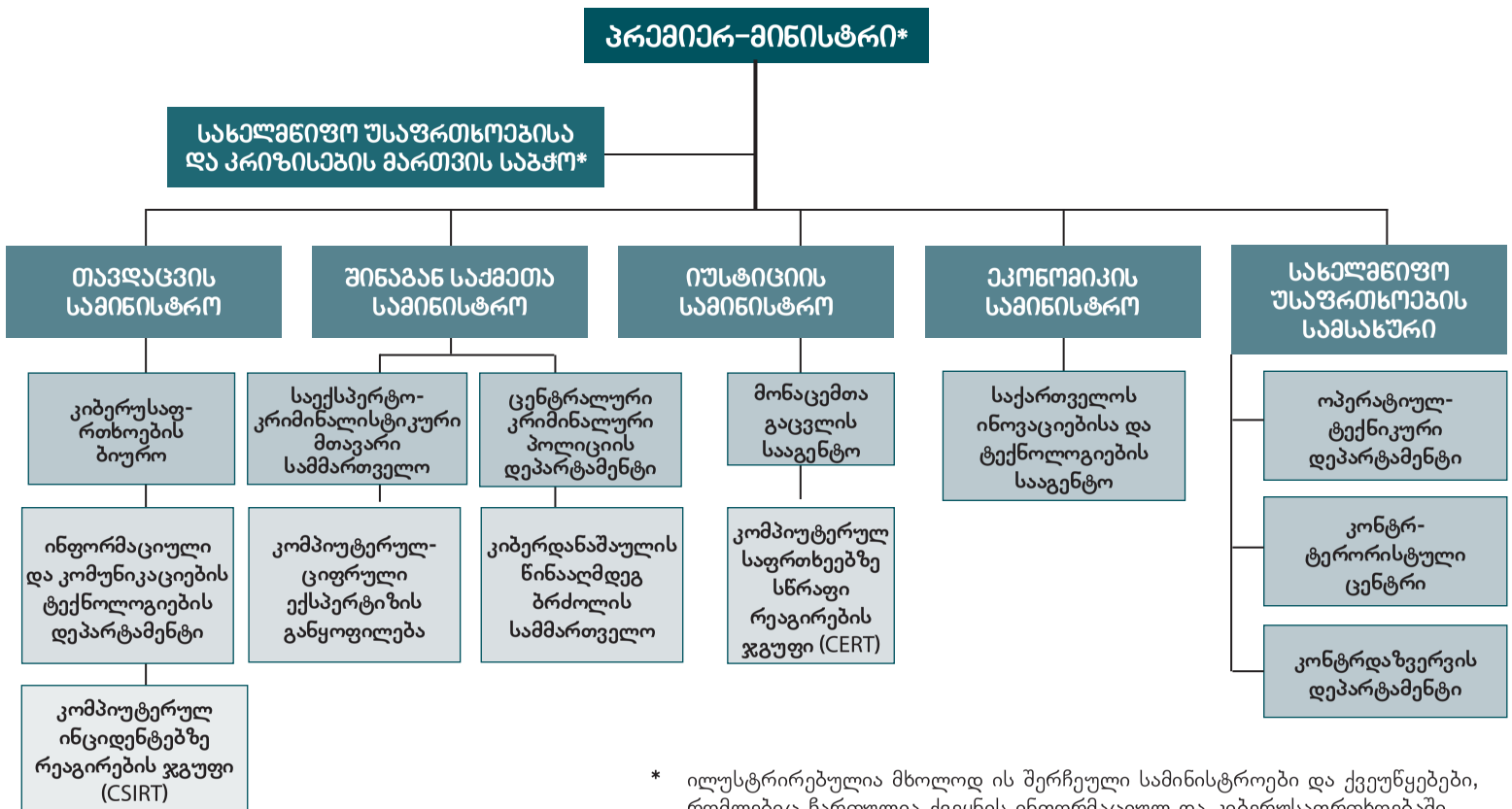
საბჭო კოორდინირებას უწევს ინფორმაციული უსაფრთხოების შესახებ კანონში ცვლილებების ინიცირებას და კრიტიკული ინფორმაციული სისტემის სუბიექტების სიის გადახედვას. საბჭო ასევე კოორდინირებას უწევს კიბერუსაფრთხოების სტრატეგიის გადახედვის პროცესს, რომელიც ამჟამად მიმდინარეობს. საბჭოს მთავარი გამოწვევა ამ მიმართულებით სამთავრობო უწყებებს შორის ეფექტური თანამშრომლობის მიღწევაა.

39-ე გვერდზე წარმოდგენილია საქართველოს მთავრობის კიბერ და ინფორმაციულ უსაფრთხოებაზე პასუხისმგებელი უწყებებისა და ქვეუწყებების სქემა.

იუსტიციის სამინისტრო – მონაცემთა გაცვლის სააგენტო /CERT

ქვეყნის მასშტაბით ინფორმაციულ და კიბერუსაფრთხოებაზე მომუშავე მთავარ ორგანოს წარმოადგენს მონაცემთა გაცვლის სააგენტო (მგს). ეს არის საჯარო სამართლის იურიდიული პირი, რომელიც იუსტიციის სამინისტროს ექვემდებარება. სააგენტო 2010 წლის იანვარში ამოქმედდა. მისი ძირითადი ფუნქციებია ელექტრონული მთავრობის განვითარება, მონაცემთა გაცვლის ინფრასტრუქტურის შექმნა და განვითარება, საინფორმაციო და კიბერსივრცის უსაფრთხოება, ცნობიერების ამაღლება, ICT სტანდარტების განსაზღვრა საჯარო სექტორისთვის და ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება.

სააგენტოს ინიციატივით შეიქმნა კიბერუსაფრთხოების ფორუმი, რომელიც წელიწადში ორჯერ საზოგადოებრივ საწყისებზე აერთიანებს სახელმწიფო და კერძო სექტორის წარმომადგენლებს. ფორუმის მიზანია ინფორმაციული და კიბერუსაფრთხოების საკითხებთან დაკავშირებით იდეებისა და მოსაზრებების გაცვლა.



* ილუსტრირებულია მხოლოდ ის შერჩეული სამინისტროები და ქვეუწყებები, რომლებიც ჩართულია ქვეყნის ინფორმაციულ და კიბერუსაფრთხოებაში.

* საბჭოს შიდაუწყებათაშორისი კოორდინაციის როლი აქვს.

სააგენტოს მოვალეობის მნიშვნელოვანი ნაწილია განსაზღვრული კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფორმაციული უსაფრთხოების უზრუნველყოფა. სააგენტოს ფუნქციებია:

- ცნობიერების ამაღლების თვალსაზრისით საგანმანათლებლო პროგრამების განხოციელება კრიტიკული ინფორმაციული სისტემის სუბიექტების, სხვადასხვა სამთავრობო სტრუქტურების, ადგილობრივი ინტერნეტტექნოლოგიების ორგანიზაციების წარმამადგენლებისა და ფართო საზოგადოებისთვის.
- სამთავრობო უწყებების მხარდაჭერა საინფორმაციო უსაფრთხოების პოლიტიკის მიღებასა და გატარებაში.
- საინფორმაციო უსაფრთხოების სახელმწიფო სტანდარტების და პროცედურების შემუშავება კანონმდებლობისა და რეგულაციების შესაბამისად (ISO 27000-ზე დაყრდნობით).
- საქართველოს კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფის (CERT) მართვა. CERT-მა მუშაობა დაიწყო 2011 წლის იანვარში, მონაცემთა გაცვლის სააგენტოს ბაზაზე. მისი ძირითადი ფუნქციებია:
  - კიბერინციდენტებზე რეაგირება, მათი გაანალიზება და რეკომენდაციების გაცემა;
  - საქართველოს კიბერსივრცის მონიტორინგი და ანალიზი;
  - პენეტრაციის (შეღწევადობის) ტესტის სერვისის მიწოდება წერილობითი კონტრაქტის საფუძველზე;
  - IP მონიტორინგის სერვისის მიწოდება და ინტერნეტქსელში საზიანო ტრაფიკის იდენტიფიკაცია;
  - ბლოკირების (შავ სიაში შეყვანის) სერვისის მიწოდება;
  - საწყისი კოდის სტატიკური ანალიზი და მომსახურების მიწოდება;
  - ზიანის მომტანი პროგრამების აღმოჩენა და ანალიზი;
  - ინციდენტის მართვის ტრენინგის ჩატარება კრიტიკული ინფორმაციული სისტემის სუბიექტის წარმომადგენლებისთვის.

მონაცემთა გაცვლის სააგენტომ განახორციელა ინფორმაციული უსაფრთხოების პოლიტიკის განვითარებისა და განხორციელების ფართომასშტაბიანი პროექტი იუსტიციის სამინისტროში, საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროში, საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროსა და საქართველოს პარლამენტში. მსგავსი პროექტები მიმდინარეობს სხვა სამინისტროებშიც.

კიბერინციდენტს კრიტიკული ინფორმაციული სისტემების სუბიექტებთან აღმოფხვრის მონაცემთა გაცვლის სააგენტო. 2014 წელს გაუშვეს კიბერინციდენტების მართვის განახლებული სისტემა – OTRS. სისტემის

ამუშავების შემდეგ კრიტიკული ინფორმაციული სისტემის სუბიექტებში დაფიქსირდა 350 ინციდენტი. ყველა შეტყობინებულ ინციდენტზე CERT-მა მოახდინა რეაგირება.[57]

საქართველოს CERT-ი ახდენს ნებისმიერი კიბერინციდენტის იდენტიფიცირებას, შეჩერებას და მასზე რეაგირებას. შეფასდება თუ არა ესა თუ ის ინციდენტი, როგორც კიბერსაბოტაჟი, კიბერტერორიზმი ან როგორც წმინდა კიბერკრიმინალი, ეს ცალკე საკითხია, რომელიც უნდა გადაწყვიტოს ცალკეულმა უწყებებმა, რომელთაც ასეთ კანონდარღვევებზე საგამოძიებო იურისდიქცია აქვთ.

საქართველოს CERT-ი თანამშრომლობს მრავალ უცხოელ პარტნიორთან. მათ შორის არიან: *Shadow Server*, *Team Cymru*, *Arbor Networks*, *Network Security Incident Exchange*; *Quarantine Net; Clean MX*. ამ ორგანიზაციებთან თანამშრომლობისა და საკუთარი ძალისხმევის შედეგად, საქართველოს CERT-ი თვეში საშუალოდ 20 ფიშინგის, 30-დან-35-მდე ზიანის მომტანი პროგრამების შემცველი საიტების აღმოფხვრას და 25-30 სახეცვლილი, დაზიანებული ვებგვერდის აღდგენას უზრუნველყოფს.

საქართველოს CERT-მა 2014 წელს მიიღო „CERT“-ის ოფიციალური სავაჭრო ნიშანი. ის შემდეგი საერთაშიროსო ორგანიზაციების წევრია:

- საერთაშორისო ტელეკომუნიკაციების კავშირი (ITU), 2011 წლიდან.
- კომპიუტერულ ინციდენტებზე რეაგირებისა და უსაფრთხოების ჯგუფთა ფორუმი (FIRST), 2013 წლიდან.
- Trusted Introducer (TI) – CERT-ების ევროპული გაერთიანება, 2012 წლიდან.

CERT.GOV.GE ასევე გეგმავს ევროპულ მთავრობათა კომპიუტერულ საფრთხეებზე სწრაფი რეაგირების ჯგუფთა ასოციაციის წევრობას.

პერსონალთან დაკავშირებით უნდა აღინიშნოს, რომ მონაცემთა გაცვლის სააგენტოს ჰყავს ოთხი სერტიფიცირებული ინფორმაციული უსაფრთხოების მენეჯერი (CISM-Certified Information Security Manager) და ორი სერტიფიცირებული ინფორმაციული სისტემის აუდიტორი (CISA-Certified Information System Auditor).

მონაცემთა გაცვლის სააგენტომ საერთაშორისო პროგრამებისა და კონტაქტების მნიშვნელოვანი ქსელი განავითარა. ერთ-ერთია GITI-ის (Georgian IT Innovations) – საერთაშორისო დონის ყოველწლიური კონფერენციის – დაარსება, რომელიც კიბერუსაფრთხოებასა და ინფორმაციული ტექნოლოგიების საკითხებს ეხება. 2014 წლის ნოემბერში ეს კონფერენცია მეშვიდედ ჩატარდა.

მეორე მაგალითია NATO-ს პროგრამის „მეცნიერება მშვიდობისა და უსაფრთხოებისთვის“ (SPS) ფარგლებში დაწყებული ახალი პროექტი, რომელიც კიბერუსაფრთხოების საკითხებში თანამშრომლობის გაუმჯობესებული საშუალებების შემუშავებას და სამხრეთ კავკასიისა და შავი ზღვის აუზის ქვეყნებში რეგიონული კიბერთავდაცვის უზრუნველყოფას გულისხმობს. პირველი რეგიონული სემინარი გაიმართა 2015 წლის ივნისში.[58] ამ პროექტის ფარგლებში სამუშაო შეხვედრები მეორედ გაიმართა ოქტომბერში.

შინაგან საქმეთა სამინისტრო – ცენტრალური კრიმინალური პოლიციის დეპარტამენტი

კიბერდანაშაულის წინააღმდეგ ბრძოლა შინაგან საქმეთა სამინისტროს კომპეტენციას წარმოადგენს. 2012 წლის დეკემბერში შსს-ის ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველო, რომლის მთავარი ფუნქციაა კიბერსივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია. სამმართველოს შექმნა განაპირობა *კიბერდანაშაულის შესახებ ევროპის კონვენციით* აღებულმა ვალდებულებებმა, რაც წევრი ქვეყნისგან მოითხოვს კიბერკრიმინალის წინააღმდეგ ბრძოლის მიზნით სპეციალური სამსახურის შექმნას. სამმართველო ორი განყოფილებისგან შედგება: ტექნოლოგიური კვლევისა და დანერგვის განყოფილება და აკრძალული შინაარსისა და პორნოგრაფიული მასალების გავრცელებასთან ბრძოლის განყოფილება. ამჟამად სამმართველოში 15 თანამშრომელია. სამმართველო ასევე მოიცავს 24/7 კიბერდანაშაულის წინააღმდეგ ბრძოლის საერთაშორისო საკონტაქტო პუნქტს.

შსს-ში აგრეთვე ფუნქციონირებს საექსპერტო-კრიმინალისტიკური მთავარი სამმართველოს კომპიუტერულ-ციფრული ექსპერტიზის განყოფილება, რომელიც ახორციელებს საგამოძიებო მოქმედებების შედეგად მიღებული ციფრული მტკიცებულებების ექსპერტიზას. ოპერატიულ-ტექნიკური დეპარტამენტი, რომელიც ფუნქციონირებდა, როგორც შსს-ის CERT-ი, გადავიდა ახლადშექმნილი სახელმწიფო უსაფრთხოების სამსახურის დაქვემდებარებაში. დეპარტამენტის რესურსი გამოყენებული იყო საჭიროებისას, კიბერდანაშაულის გამოძიების პროცესში. სხვა ალტერნატივა, აუცილებლობის შემთხვევაში, არის ლევან სამხარაულის ეროვნული ექსპერტიზის ბიურო – საჯარო სამართლის იურიდიული პირი, რომელიც შსს-ის დაქვემდებარებაშია. კომპიუტერული ექსპერტიზა ერთ-ერთია იმ უამრავი სერვისიდან, რასაც ეს ბიურო ასრულებს.

შინაგან საქმეთა სამინისტროში შეიმუშავეს სტანდარტული ოპერაციული პროცედურები *ციფრული მტკიცებულებების პირველადი მოპყრობის* შესახებ. მოცემული დოკუმენტები განსაზღვრავს პროგრამული უზრუნველყოფის იმ სახეებსა და ტექნიკურ წესებს, რომელთა მიხედვითაც უნდა განხორციელდეს ციფრული მტკიცებულებების დამუშავება. ამ ეტაპზე მიმდინარეობს აღნიშნული დოკუმენტის საბოლოო სრულყოფა.

შსს-ის აკადემიაში ასევე შეიმუშავეს ტრენინგმოდულები, რომლებიც მოიცავს კიბერდანაშაულთან დაკავშირებულ შემდეგ საკითხებს:

- კიბერდანაშაულის შემთხვევების ანალიზი;
- ელექტრონული მტკიცებულებების ჩხრეკა და ამოღება;
- კიბერდანაშაულის სამართლებრივი ასპექტები;
- კიბერშეტევების ტიპები.

აღსანიშნავია, რომ შსს-მ 2014 წელს დაიწყო კიბერდანაშაულის ცნობადობის კამპანია. შექმნეს მოკლემეტრაჟიანი ფილმების სერია „იდენტიფიკაცია“, რომელიც სხვადასხვა ტიპის დანაშაულებს ეხება. პირველი სერია დაეთმო კიბერდანაშაულის პრობლემატიკას. პროექტი დაფინანსდა საქართველოში აშშ-ის საელჩოს მიერ.

კიბერდანაშაულებთან ბრძოლის მხრივ შსს აქტიურად თანამშრომლობს როგორც ევროპული ქვეყნების სამართალდამცავ სტრუქტურებთან, ასევე აშშ-ის საგამოძიებო ფედერალურ ბიუროსთან.

2014 წელს შსს-მ ბრიტანეთის დანაშაულთან ბრძოლის ეროვნულ სააგენტოსთან ხელი მოაწერა ურთიერთთანამშრომლობის შესახებ მემორანდუმს, რომელიც სხვადასხვა სფეროში (ნარკოდანაშაული, ტრეფიკინგი, კიბერდანაშაული) ორგანიზებულ დანაშაულთან ბრძოლაში თანამშროლობას და ინფორმაციის გაცვლას გულისხმობს.

სამინისტრო აქტიურად თანამშრომლობს საერთაშორისო ორგანიზაციებთან, ჩართულია დონორების მიერ ინიცირებულ სხვადასხვა პროექტში. 2011-2014 წლებში შინაგან საქმეთა სამინისტრო ასევე ჩართული იყო აღმოსავლეთ პარტნიორობის ეგიდით მიმდინარე პროექტში „თანამშრომლობა კიბერდანაშაულის წინააღმდეგ“. ამ პროექტის მიზანი იყო ქართული სამართალდამცავი უწყებების შესაძლებლობების განვითარება კიბერდანაშაულთან ბრძოლის პროცესში.[59]

2012 წლიდან ესტონეთის ხელისუფლების მხარდაჭერით განხორციელდა პროექტი, რომელიც ითვალისწინებდა საქართველოს შინაგან საქმეთა სამინისტროს შესაძლებლობების გაზრდას კიბერდანაშაულის გამოძიებისა და ციფრული მტკიცებულებების ამოღების მიმართულებით. ეს პროგრამა დასრულდა, მაგრამ სამომავლოდ იგეგმება მისი განახლება. 2013 წელს შსს პოლიციის აკადემიაში აშშ-ის საელჩოს ძალისხმევით ამერიკის გამოძიების ფედერალური ბიუროს (FBI) წარმომადგენლებმა კიბერდანაშაულის საკითხებთან დაკავშირებით ტრენინგი ჩაატარეს. 2014 წელს შსს-ის წარმომადგენლები სასწავლო ვიზიტებით, რომლებიც ეხებოდა ორგანიზებულ დანაშაულთან და სხვადასხვა ტიპის კიბერდანაშაულთან ბრძოლას, იმყოფებოდნენ საფრანგეთში, გერმანიაში, პოლონეთსა და ბრიტანეთში. შსს-ის თანამშრომლები ასევე მონაწილეობას იღებენ სხვადასხვა ტრენინგპროგრამაში, რაც ხელს უწყობს მათი კვალიფიკაციის ამაღლებასა და კიბერდანაშულის წინააღმდეგ უფრო ეფექტურ ბრძოლას.

სამინისტროს წარმომადგენლებმა ჩვენთან საუბრისას განაცხადეს, რომ კიბერდანაშაულის ფორმები უფრო და უფრო იხვეწება და, შესაბამისად, მათთან ბრძოლა რთულდება: „იმისთვის, რომ ეფექტურად ებრძოლო ამ პრობლემას, უნდა გქონდეს მაღალი დონის ტექნიკური შესაძლებლობები. მაღალი კვალიფიკაციის უნარების შეძენა შესაძლებელია მხოლოდ მაღალი დონის ტექნიკური ტრენინგების მეშვეობით.“ კერძოდ, საგამოძიებო მოქმედებებში სამმართველოს წარმომადგენლებმა განაცხადეს, რომ მათ ესაჭიროებათ ტრენინგები დასავლური ტაქტიკის, მეთოდებისა და პროცედურების (TTPs) უკეთ შესასწავლად. კერძოდ, კომპიუტერული ექსპერტიზის, მტკიცებულების ამოღების, ტექნიკური ანალიზის, ასევე სხვადასხვა ქვეყნის შესაბამისი სტრუქტურებიდან ინფორმაციის გამოთხოვისა და ექსტრადიციის წესების შესასწავლად.

სახელმწიფო უსაფრთხოების სამსახური

2015 წლის ივლისში, საქართველოს მთავრობის დადგენილებით, შეიქმნა საქართველოს სახელმწიფო უსაფრთხოების სამსახური. სამსახურის საქმიანობის მთავარი მიმართულებებია: საქართველოს კონსტიტუციური წყობილების, სუვერენიტეტის, ტერიტორიული მთლიანობისა და სამხედრო პოტენციალის დაცვა უცხო ქვეყნების სპეციალური სამსახურებისა და ცალკეულ პირთა მართლსაწინააღმდეგო ქმედებისაგან; სახელმწიფო კონსტიტუციური წყობილებისა და სახელმწიფო ხელისუფლების არაკონსტიტუციური, ძალადობრივი გზით შეცვლის გამოვლენა და დაცვის უზრუნველყოფა; ქვეყნის ეკონომიკური უსაფრთხოების უზრუნველყოფა; ტერორიზმთან ბრძოლა; ტრანსნაციონალური ორგანიზებული და საერთაშორისო დანაშაულის წინააღმდეგ ბრძოლა; კორუფციის წინააღმდეგ ბრძოლა; სახელმწიფო საიდუმლოების რეჟიმის დაცვა.

სახელმწიფო უსაფრთხოების სამსახურის შემადგენლობაში შსს-დან გადავიდა ისეთი დანაყოფები, როგორიცაა: კონტრტერორისტული ცენტრი, კონტრდაზვერვის დეპარტამენტი, სახელმწიფო უსაფრთხოების სამსახური, ანტიკორუფციული სააგენტო, სპეციალური ოპერაციების დეპარტამენტი და ოპერატიულ-ტექნიკური დეპარტამენტი.[60] ოპერატიულ-ტექნიკური დეპარტამენტი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143.1 მუხლით, პასუხისმგებელია ფარული საგამოძიებო მოქმედებები განახორციელოს კანონმდებლობით დადგენილი წესის შესაბამისად. აღნიშნული მუხლი ითვალისწინებს სატელეფონო საუბრის ფარულ მიყურადებას და ჩაწერას და ინფორმაციის მოხსნასა და ფიქსაციას კავშირგაბმულობის არხიდან. თუმცა აღნიშნული დეპარტამენტის ახლადშექმნილ სახელმწიფო სტრუქტურაში გადასვლა შსს-ს არ ართმევს ფარული საგამოძიებო მოქმედებების განხორციელების შესაძლებლობას.

პროკურატურა და სასამართლო ხელისუფლება

ბუნებრივია, სამართალდამცავი სისტემის მუშაობისთვის მხოლოდ კიბერდანაშაულთან ბრძოლის ეფექტური პოლიტიკა არ არის საკმარისი; ბრალმდებელსაც და მოსამართლესაც შესაბამისად უნდა ესმოდეთ საკითხის არსი. პროკურატურის და სასამართლო სისტემის მოხელეებისთვის ერთგვარი გამოწვევაა კიბერტექნოლოგიების მზარდ ტემპს მიჰყვნენ. ჩვენთან საუბრისას ამაზე ილაპარაკეს მონაცემთა გაცვლის სააგენტოს და ასევე შსს-ის კიბერდანაშაულთან ბრძოლის სამმართველოს წარმომადგენლებმა. კერძოდ, შსს-ის წარმომადგენლებმა აღნიშნეს, რომ პროკურორებს და მოსამართლეებს სათანადოდ არ ესმით განსახილველი კიბერსაქმეები. როგორც თქვეს, იყო რამდენიმე შემთხვევა, როდესაც მყარი სამხილისა და წარდგენილი მტკიცებულების ამოღების პროცედურის სრული დაცვის მიუხედავად, „საბოლოო განაჩენი არ იყო ადეკვატური, სწორედ იმ მიზეზით, რომ მათ არა აქვთ კიბერსაქმეებზე მუშაობის შესაბამისი ცოდნა და გამოცდილება“.

არსებულ პრობლემასთან გამკლავების მიზნით მონაცემთა გაცვლის სააგენტომ 2014 წლის მარტში პროკურატურის თანამშრომლებს კიბერთემატიკაზე ტრენინგი ჩაუტარა. სწავლება მოიცავდა ისეთ საკითხ-

ებს, როგორიცაა კიბერდანაშაულის ფორმები და მეთოდები, კიბერუსაფრთხოება და კიბერსამართალი. ტრენინგს 10 თანამშრომელი დაესწრო. ერთი-ერთმა ოფიციალურმა პირმა ჩვენთან საუბარისას განაცხადა, რომ „იყო შემთხვევები, როდესაც პროკურატურის რამდენიმე წარმომადგენელი გამოეთიშა სწავლების კურსს, რადგანაც ეს თემა მათთვის მეტისმეტად რთული იყო. ეს არის ის ერთ-ერთი უმთავრესი პრობლემა, რომელიც აუცილებლად უნდა მოგვარდეს“. როგორც ჩანს, ეს არის აქილევსის ქუსლი საქართველოს ძალისხმევისთვის ებრძოლოს კიბერდანაშაულს. პროკურატურის წარმომადგენელმა ჩვენთან საუბრისას აღნიშნა, რომ ზოგიერთ შემთხვევაში რთულია კიბერსაქმეების ტექნიკური მხარის გაგება, რაც გარკვეულწილად რთული გამოწვევის წინაშე გვაყენებს.

თავდაცვის სამინისტრო

2013 წლის 24 დეკემბერს საქართველოს პარლამენტმა კანონში ინფორმაციული უსაფრთხოების შესახებ საქართველოს თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის (შემდგომ – კიბერუსაფრთხოების ბიურო) შექმნასთან დაკავშირებით შესწორება შეიტანა.[61] ბიურო ოფიციალურად 2014 წლის თებერვალში შეიქმნა. მოგვიანებით, იმავე წელს, კანონში შეტანილ იქნა ცვლილებები თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების დამტკიცების შესახებ. თავდაცვის სფეროში კრიტიკული ინფორმაციული სუბიექტების მნიშვნელობის კლასიფიცირებას ადგენს საქართველოს მთავრობა. პროექტი საქართველოს მთავრობას დასამტკიცებლად წარედგინა საქართველოს იუსტიციის სამინისტროსა და საქართველოს თავდაცვისა და შინაგან საქმეთა სამინისტროების ერთობლივი შეთანხმების საფუძველზე.

თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების სია დამტკიცდა საქართველოს მთავრობის #567 დადგენილების საფუძველზე 2014 წლის 29 სექტემბერს.[62] სიაში შედის შემდეგი ორგანიზაციები:

1. საქართველოს თავდაცვის სამინისტრო;
2. საჯარო სამართლის იურიდიული პირი – კიბერუსაფრთხოების ბიურო;
3. საჯარო სამართლის იურიდიული პირი – თავდაცვის სამინისტროს სამხედრო ჰოსპიტალი;
4. საჯარო სამართლის იურიდიული პირი – კადეტთა სამხედრო ლიცეუმი;
5. საჯარო სამართლის იურიდიული პირი – საქართველოს ეროვნული თავდაცვის აკადემია.

ბიუროს მთავარი მისიაა თავდაცვის სფეროში ინფორმაციული და კიბერუსაფრთხოების უზრუნველყოფა, პოტენციური კიბერრისკებისა და საფრთხეების აღმოფხვრა, დროული რეაგირება და ამ მიზნით ეფექტური მეთოდების შემუშავება. ბიურო აქტიურად მუშაობს რელევანტური საკანონმდებლო ჩარჩოს შემუშავების კუთხითაც, რომ უფრო დაუახლო-

ვდეს საერთაშორისო სტანდარტებს. ამასთან, კანონში ასევე ხაზგასმულია, რომ ინფორმაციული უსაფრთხოების პოლიტიკა უნდა პასუხობდეს სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილ მინიმალურ მოთხოვნებს. ამავდროულად, ქვეყნის შიგნით სამთავრობო სტრუქტურებს შორის ეფექტური თანამშრომლობა, საერთაშორისო ორგანიზაციებთან, პარტნიორ ქვეყნებთან ურთიერთობის გაღრმავება ბიუროს მიზნების შემადგენელი ნაწილია.

ბიუროს შემადგენლობაში მუშაობს კომპიუტერულ ინციდენტებზე რეაგირების საკოორდინაციო ცენტრი (CSIRT/CC) და კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი (CSIRT).

ეკონომიკისა და მდგრადი განვითარების სამინისტრო

ეკონომიკის სამინისტროს პროექტის – „ინოვაციური საქართველო 2020“ – მიზანია საქართველოს ეკონომიკის განვითარება ICT ტექნოლოგიების გამოყენებით. აღნიშნული პროექტის ერთ-ერთ მთავარ მიზანს 2020 წლისთვის სწორედ საქართველოს ინფორმაციისა და კომუნიკაციის ინდექსების გაუმჯობესება წარმოადგენს. საქართველოს ინოვაციებისა და ტექნოლოგიების ახლადშექმნილი სააგენტო, რომელიც სამინისტროს შემადგენლობაში ფუნქციონირებს, მიზნად ისახავს ტექნოპარკების, IT ინკუბატორებისა და ინოვაციური ლაბორატორიების დაფუძნებასა და ზოგადად, საქართველოს ICT რეგიონალურ ჰაბად (ცენტრად) ქცევას.

ეკონომიკის სამინისტრო და საქართველოს კომუნიკაციების ეროვნული კომისია პროგრამის – „საქართველო: ინფორმაციისა და კომუნიკაციების პოლიტიკისა და რეგულაციის შემუშავების“ – ფარგლებში თანამშრომლობს ფინეთის მთავრობასა და ევროპის რეკონსტრუქციისა და განვითარების ბანკთან (EBRD). პროგრამის ძირითადი მიზანია მოამზადოს კომპლექსური საპროექტო დოკუმენტაცია საქართველოში ინფორმაციისა და კომუნიკაციების პოლიტიკის შესახებ. EBRD-ის ექსპერტების დახმარებით შემუშავდა დოკუმენტები „ციფრულ მაუწყებლობაზე გადასვლის პოლიტიკა“ და „ციფრული მაუწყებლობის საკანონმდებლო სამოქმედო გეგმა“.

საქართველოს ელექტრონულ საკომუნიკაციო ქსელებში ჩატარდა ფართომასშტაბიანი რეფორმა – შემუშავდა სატელეფონო კოდების ეროვნული ათვლის ახალი სისტემა. ამის შედეგად ამოქმედდა ქალაქებისა და ადმინისტრაციული ცენტრების ახალი სატელეფონო კოდები, ადგილობრივი სატელეფონო ქსელების, მობილური და უსადენო ფიქსირებული სატელეფონო ქსელების ახალი ნუმერაცია.

საქართველოს კომუნიკაციების ეროვნული კომისია

საქართველოს კომუნიკაციების ეროვნული კომისია არის ერთ-ერთი მნიშვნელოვანი სახელმწიფო ინსტიტუტი საქართველოში. მას აქვს ინტერნეტსერვისების მომწოდებელი კომპანიების რეგულირებისა და ზედამხედველობის მანდატი, მათ შორის – ამ კომპანიების უსაფრთხოების წესებზეც. ასევე შეიძლება კომისიის კიბერუსაფრთხოების საკომუნიკაციო პლატფორმად გამოყენება ინტერნეტსერვისის მიმწოდებელ კომპანიებს შორის და, ასევე, კიბერდანაშაულ-თან ბრძოლის სამმართველოსა და საქართველოს CERT-ს შორის.

თანამშრომლობის მექანიზმების გარდა, საქართველოს კომუნიკაციების ეროვნულ კომისიას, როგორც მარეგულირებელ ორგანოს, შეუძლია ხელი შეუწყოს კიბერუსაფრთხოების გაუმჯობესების პროცესს. კერძოდ, ინტერნეტსერვისის მიმწოდებელ კომპანიებში ნებაყოფლობითი კოდექსის ან თუნდაც სავალდებულო პრაქტიკის შემოღებით მოსთხოვოს მათ იქონიონ ინფიცირებული კომპიუტერებისა და ზიანის მომტანი ტრაფიკის შეტყობინების სისტემა და მთავრობისთვის კიბერუსაფრთხოებასთან დაკავშირებული მოსალოდნელი სერიოზული საფრთხეების შეტყობინების მიზნით შესაბამისი ანგარიშგების მექანიზმები შეიმუშაონ.

ამრიგად, ინტერნეტპროვაიდერები შეძლებენ მნიშვნელოვანი წვლილი შეიტანონ ბევრად უსაფრთხო კიბერგარემოს შექმნაში როგორც რიგითი მომხმარებლისთვის, ასევე უფრო მასშტაბური თვალსაზრისით.

პერსონალურ მონაცემთა დაცვის ინსპექტორი

საქართველოში პერსონალურ მონაცემთა დაცვის ინსპექტორის ინსტიტუტი 2013 წლის ივლისში შემოიღეს. ორგანიზაციის შექმნა განაპირობა პერსონალურ მონაცემთა დაცვის შესახებ კანონმა, რომელიც ძალაში შევიდა 2012 წლის მაისში.[63] ამ კანონის მიზანია პერსონალური მონაცემების დამუშავებისას უზრუნველყოს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა. პერსონალურ მონაცემთა დაცვის ინსპექტორი ზედამხედველობას უწევს საქართველოში პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის შესრულებას და ახორციელებს მონაცემთა დამუშავების კანონიერებაზე კონტროლს საჯარო და კერძო დაწესებულებებისათვის. ინსპექტორის მოვალეობებია მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე კონსულტაციის გაწევა, მონაცემთა დაცვასთან დაკავშირებული განცხადებებისა და საჩივრების განხილვა და საქართველოში მონაცემთა დაცვის მდგომარეობისა და მასთან დაკავშირებული მნიშვნელოვანი მოვლენების შესახებ საზოგადოების ინფორმირება.

ამავდროულად, კანონის თანახმად, ინსპექტორს უფლება აქვს განახორციელოს მონაცემთა დამუშავების კანონიერების შემოწმება/ინსპექტირება საჯარო და კერძო დაწესებულებებში. თუკი ინსპექტორი აღმოაჩენს დარღვევებს,

მას უფლება აქვს მოითხოვოს მონაცემთა ნაკლოვანებების გამოსწორება მისივე მითითებული ფორმით და მითითებულ ვადაში, მოითხოვოს მონაცემთა დამუშავების დროებით ან სამუდამოდ შეწყვეტა, მათი დაბლოკვა, წაშლა, განადგურება ან დეპერსონალიზაცია, თუ მიიჩნევს, რომ მონაცემთა დამუშავება ხორციელდებოდა კანონის საწინააღმდეგოდ. მას ასევე უფლება აქვს მონაცემთა დამმუშავებელს ან უფლებამოსილ პირს დააკისროს ადმინისტრაციული პასუხიმგებლობა კანონმდებლობით დადგენილი წესით.

ინტელექტუალური საკუთრების უფლებების დაცვა

საქართველოს ინტელექტუალური საკუთრების ეროვნული ცენტრი – „*საქპატენტი*“ წარმოადგენს საჯარო სამართლის იურიდიულ პირს. საქართველოს კანონმდებლობის თანახმად, „საქპატენტი“ განსაზღვრავს ინტელექტუალური საკუთრების პოლიტიკას. „საქპატენტში“ კონსოლოდირებულია ინტელექტუალური საკუთრების ყველა ძირითადი სფერო: სამრეწველო საკუთრება, საავტორო, მომიჯნავე უფლებები და სხვა. მეორე ორგანიზაცია, რომელიც ამ მიმართულებით მნიშვნელოვან როლს თამაშობს, არის საქართველოს საავტორო უფლებათა ასოციაცია.

კერძო სექტორი

საქართველოს სამეცნიერო-საგანმანათლებლო კომპიუტერული ქსელების ასოციაცია (გრენა)

ორგანიზაცია *გრენა* საქართველოში 1999 წლიდან ფუნქციონირებს. ორგანიზაციაში დასაქმებულია 14 ადამიანი. გრენას პროექტები ხორციელდება უნივერსიტეტებთან მჭიდრო თანამშრომლობით, ევროკავშირის, ნატოს სამეცნიერო პროგრამების, ფონდი „ღია საზოგადოება – საქართველოს“ და საერთაშორისო მეცნიერების და ტექნოლოგიების სამეცნიერო ცენტრის მხარდაჭერით. როგორც კიბერუსაფრთხოების ყველაზე ადრეულმა ორგანიზაციამ საქართველოში, გრენამ ითამაშა მნიშვნელოვანი როლი რუსული კიბერშეტევების შემსუბუქებაში 2008 წლის ომის დროს.

2004 წლიდან გრენას ბაზაზე ფუნქციონირებს Cisco-ს რეგიონული ქსელური აკადემია, რომელიც მსურველებს სთავაზობს შემდეგ კურსებს:

- Cisco Certified Network Associate (CCNA)
- CCNA Security
- Cisco Certified Network Professional (CCNP)

გრენას აქვს დისტანციური სწავლების ცენტრი, რომელიც საშუალებას აძლევს სტუდენტებს სერტიფიცირება გაიარონ ინტერნეტის საშუალებით.

2007 წლიდან გრენა თავისი წევრი ორგანიზაციებისთვის ორი წევრისგან შემდგარ CERT-ს მართავს. CERT-ი დაფუძნდა ნატოს სამეცნიერო პროგრამის მხარდაჭერით. CERT-GE არის ევროპული CERT-ების გაერთიანების წევრი და მჭიდროდ თანამშრომლობს სხვადასხვა ქვეყნის კიბერუსაფრთხოების ორგანიზაციებთან. GRENA CERT-ს აქვს შემდეგი მომსახურება:

- ქსელში უკანონო შეჭრის გამოვლენის სისტემა, რომელიც ამოწმებს ქსელებში შემავალ და გამავალ პაკეტებს.
- ინციდენტის კოორდინაცია – ინციდენტების გამოძიება და აღმოფხვრა სხვადასხვა ქვეყნის CERT-ის ჯგუფებთან თანამშრომლობით.
- სხვადასხვა კიბერსაფრთხის შესახებ ინფორმაციის გავრცელება.
- IP მონიტორინგი და საქართველოს ქსელებში კიბერინციდენტების შესახებ ინფორმაციის მოძიება/გავრცელება.

კრიტიკული ინფრასტრუქტურა

კერძო მფლობელობაში არსებული კრიტიკული ინფრასტრუქტურის შესახებ ინფორმაციის წარმოსადგენად ჩავატარეთ ინტერვიუები ფიჭური და ინტერნეტსერვისის მიმწოდებელ კომპანიებთან, ბანკისა და საზღვაო პორტის წარმომადგენლებთან.

- **მაგთიკომი** ემსახურება მობილური ტელეფონის დაახლოებით 1.7 მილიონ მომხმარებელს და მობილური ინტერნეტის 700,000 აბონენტს, ამავდროულად სატელიტური სამაუწყებლო სისტემის მომხმარებლებს. ორგანიზაცია ასევე ემსახურება 64 იუსტიციის სახლს საქართველოს მასშტაბით.
- **თიბისი ბანკი** არის სრული სერვისის კომერციული ბანკი, რომელიც ფუნქციონირებს, როგორც სააქციო საზოგადოება. ბანკი ემსახურება დაახლოებით 700,000 კლიენტს. მისი სათავო ოფისი, მისი ბიზნესის უმეტეს ნაწილთან ერთად, თბილისშია, თუმცა მას ბიზნესინტერესები აქვს აზერბაიჯანსა და ისრაელში.
- **APM-ტერმინალი** ფუნქციონირებს ფოთის პორტში. კომპანიის სათავო ოფისი არის ჰააგაში, თუმცა მისი მფლობელია დანიური კომპანია Danish Maersk ჯგუფია. APM ამუშავებს 64 ტერმინალს 39 ქვეყანაში. ფოთის პორტი იღებს არა მარტო კონტეინერებს, არამედ გენერალურ ტვირთებს და გადმოტვირთავს 15 ნავმისადგომზე, 2,900 მეტრის სიგრძის ნავსადგომში.

სამივე კომპანიის ბიზნესი შედგება ინფრასტრუქტურისგან, რომელიც ქვეყნისთვის უკიდურესად მნიშვნელოვანია. სამივე კომპანია აცხადებს, რომ

საჭიროების შემთხვევაში მზადაა საქართველოს მთავრობასთან თანამშრომლობისათვის. მათი მოტივაცია კიბერუსაფრთხოების ღონისძიებებთან დაკავშირებით, უპირველეს ყოვლისა, მომდინარეობს მათივე ბიზნესინტერესებიდან – შექმნან უფრო ხელსაყრელი გარემო უსაფრთხოების თვალსაზრისით, რაც განაპირობებს საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანას. სამივე შემთხვევაში კიბერუსაფრთხოებაზე პასუხისმგებელი მათი ინფორმაციული უსაფრთხოების დეპარტამენტები არიან.

ფოთის პორტი პასუხობს ISO 9001-2000 სტანდარტებს. თუკი APM შეინარჩუნებს ეფექტურობას და უსაფრთხოებას, პორტი შეძლებს წელიწადში თავისი გამტარუნარიანობის 25 მილიონი ტონა ტვირთით გაზრდას. კომპიუტერული სისტემა, რომელიც აკონტროლებს პორტის ფუნქციონირებას, დახურულია და დაფუძნებულია არაფართო მოხმარების ოპერატიულ სისტემაზე. ნაკლებად მნიშვნელოვანი სისტემები ჩართულია ინტერნეტსა და ინტერფეისში და დაკავშირებულია საქართველოს საბაჟო სამსახურთან და ოთხ საკონტეინერო ხაზთან. რადგან პორტის ინფორმაციული ტექნოლოგიების მენეჯერების ძირითადი საზრუნავი დახურული სისტემის უსაფრთხოების უზრუნველყოფაა, მათი ზრუნვის ერთ-ერთი მნიშვნელოვანი საგანი შიდა საფრთხეებია. აქედან გამომდინარე, პერსონალთან დაკავშირებით უსაფრთხოების ზომებს სათანადო ყურადღება ექცევა. კომპანიის თითქმის მთელი პერსონალი ვალდებულია გაიაროს კომპიუტერული ტრენინგის სპეციალიზებული კურსი.

თიბისი ბანკი მისდევს ISO-სა და NIST-ის სტანდარტებს. მეტიც, თიბისი ბანკმა 2014 წლის ივნისში ლონდონის საფონდო ბირჟაზე აქციების პირველადი საჯარო შეთავაზება (IPO – Initial Public Offering) განახორციელა, რაც ერთმნიშვნელოვნად საჭიროებს უსაფრთხოების დამატებითი მოთხოვნების შესრულებას. ბანკის ოფიციალურმა წარმომადგენელმა ჩვენთან საუბრისას განაცხადა იმ რისკფაქტორების შესახებ, რაც კომპიუტერული უსაფრთხოების ფუნქციონირებისთვის საჭირო საშუალებების და ტექნიკური უნარების გარედან მოზიდვას, შიდა საფრთხეებსა და მაღალი ტექნიკური უნარების თანამშრომელთა შეზღუდულ რაოდენობას ახლავს. მიუხედავად ამისა, ოფიციალურმა წარმომადგენელმა ჩვენთან საუბრისას აღნიშნა მათი კონტრაქტორების მაღალი ნდობის ხარისხისა და ორგანიზაციაში უსაფრთხოების პროცედურების სათანადოდ უზრუნველყოფის ფაქტის შესახებ. მისი თქმით, მიუხედავად პროფესიონალთა ნაკლებობისა, კარგად არის დაგეგმილი კომბინირებული მუშაობა და საჭიროების შემთხვევაში კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების გუნდის შეკრება.

„მაგთიკომის“ უსაფრთხოების მიდგომა შედარებით კომპლექსურია, რადგანაც აერთიანებს ფიზიკურ უსაფრთხოებას და კიბერუსაფრთხოებას. კომპანია უნდა აკმაყოფილებდეს ITU სტანდარტებს, თუმცა ფიჭური სატელეფონო კომპანიებისათვის ამ სტანდარტების დაცვის მოთხოვნები ნაკლებად მკაცრია. „მაგთიკომის“ სისტემა დახურულია და ის არ იყენებს გარე რესურსებს. ყველაზე დიდი საზრუნავი არის ოპტიკურბოჭკოვანი კაბელის ფიზიკური უსაფრთხოება. „მაგთიკომის“ ოფიციალური წარმომადგენლები ასევე ხაზს უსვამენ სმარტფონებთან დაკავშირებით კიბერდანაშაულის მოსალოდნელი ზრდის საერთო ტენდენციას. სმარტფონების მომხმარებელთა რიცხვი საქართველოში ნახევარ მილონზე მეტს აღწევს და ეს მაჩვენებელი დღითიდღე იზრდება.

ზემოთ წარმოდგენილი მოკლე აღწერა, რა თქმა უნდა, არ ასახავს კიბერუსაფრთხოების სრულ სურათს ზემოაღნიშნულ სამ კომპანიაში, მაგრამ მაინც, მათთან საუბრის შემდეგ რჩება შთაბეჭდილება, რომ ამ კომპანიების ინფორმაციული უსაფრთხოების საკითხი საქმისათვის თავდადებული ადამიანების ხელშია, რომლებიც კარგად უმკლავდებიან ახალ გამოწვევებს.

ამრიგად, იმ სამთავრობო სტრუქტურებისთვის, რომლებიც პასუხისმგებელი არიან ქვეყნის კიბერუსაფრთხოებაზე, მნიშვნელოვანია მომზადდეს ანგარიში იმის შესახებ, თუ კიბერუსაფრთხოების რა ზომებს იღებენ იმ კერძო კომპანიებში, რომლებიც ფლობენ კრიტიკულ ინფრასტრუქტურას. ამასთანავე, მთავრობამ უნდა გამონახოს კერძო კრიტიკული ინფრასტრუქტურის სუბიექტებთან კომუნიკაციისა და მუშაობის ეფექტური გზები.

კონცეფციები, კანონები და გეგმები

ეროვნული უსაფრთხოების კონცეფცია

საქართველოს 2008 წლის გამოცდილების გათვალისწინებით, ახალი *ეროვნული უსაფრთხოების კონცეფციის* ავტორები წერენ:

> „2008 წლის რუსეთ-საქართველოს ომის დროს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ, სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, მიზანმიმართული და მასობრივი კიბერთავდასხმები განახორციელა. ამ კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა... საქართველოსთვის მეტად მნიშვნელოვანია ინფორმაციული სივრცის უსაფრთხოება და ელექტრონული ინფორმაციის დაცულობა. ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერდანაშაულთან ბრძოლას და კიბერსივრცეში დივერსიული აქტებისგან თავდაცვას“.[64]

სტრატეგია ხაზს უსვამს ქვეყნის კიბერუსაფრთხოების საქმეში პარტნიორ ქვეყნებთან თანამშრომლობის მნიშვნელობას.

კიბერუსაფრთხოების სტრატეგია და სამოქმედო გეგმა

კიბერუსაფრთხოების სტრატეგია და სამოქმედო გეგმა ამჟამად გადახედვის პროცესშია. სტრატეგიისა და სამოქმედო გეგმის განახლებული ვარიანტის გამოქვეყნება 2015 წლის ბოლოსთვის იგეგმება. სტრატეგიის გადახედვის

პროცესს ახორციელებს სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოში მუდმივმოქმედი შიდაუწყებათაშორისი კომისია.

2013-2015 წლის უკვე არსებული სტრატეგია და სამოქმედო გეგმა 2013 წლის 17 მაისს, პრეზიდენტის #321 ბრძანებულების საფუძველზე, დამტკიცდა. საქართველოს კიბერუსაფრთხოების სტრატეგია შემუშავდა 2010-2013 წლის *საქართველოს საფრთხეების შეფასების დოკუმენტისა* და *საქართველოს ეროვნული უსაფრთხოების კონცეფციის* საფუძველზე. დოკუმენტი შექმნა საქართველოს ეროვნული უსაფრთხოების საბჭოში მუდმივმოქმედმა შიდაუწყებათაშორისმა კომისიამ, რომელსაც ევალებოდა ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტების შემუშავება/კოორდინაცია.

სტრატეგია მოითხოვს კიბერუსაფრთხოების სისტემის ისეთი ძირითადი პრინციპების შექმნას, რომლებიც არა მარტო გააადვილებს ინფორმაციული ინფრასტრუქტურის დაცვას კიბერსაფრთხეებისგან, არამედ ასევე ხელს შეუწყობს ქვეყნის სოციალურ-ეკონომიკურ განვითარებას. სტრატეგიაში მოცემულია შემდეგი რვა პრინციპი, რომლებიც საჭიროა უკეთ დაცული კიბერსივრცის მისაღწევად: მთავრობის ერთიანი მიდგომა; მთავრობასა და კერძო სექტორს შორის თანამშრომლობა; კვლევა და ანალიზი; ახალი საკანონმდებლო-ნორმატიული ბაზის შექმნა; ინსტიტუციური კოორდინაცია კიბერუსაფრთხოების უზრუნველსაყოფად; საზოგადოების ცნობიერების ამაღლება; საგანმანათლებლო ბაზის ჩამოყალიბება; ტრენინგი და საერთაშორისო თანამშრომლობა.[65]

სტრატეგიისა და სამოქმედო გეგმის გადახედვის პროცესში სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო ორი გამოწვევის წინაშე დგას: 1) მიაღწიოს უწყებათაშორის ეფექტურ კოორდინაციას რაიმე კონკრეტულის მისაღებად და 2) განახლებულ სტრატეგიასა და სამოქმედო გეგმაში ასახოს მკაფიო და კონკრეტული მიზნები.

ევროპის კონვენცია კიბერდანაშაულის შესახებ

2012 წლის 6 ივნისს საქართველომ მოახდინა ევროპის საბჭოს „კიბერდანაშაულის შესახებ კონვენციის“ რატიფიცირება. ამ კონვენციას საქართველომ 2008 წელს მოაწერა ხელი. კონვენცია მოითხოვს როგორც კიბერგამოძიების მიზნით საერთაშორისო თანამშრომლობას, ისე საქართველოს საკანონმდებლო ბაზის ჰარმონიზაციას კონვენციით დადგენილ ნორმებთან. კონვენციის რატიფიცირების დაჩქარებას ხელი შეუწყო „ინფორმაციული უსაფრთხოების შესახებ კანონის“ მიღებამ. აღნიშნული კონვენცია ძალაში შევიდა 2012 წლის 1 ოქტომბერს.[66]

2008–2009 წლებში საქართველოს შინაგან საქმეთა სამინისტრო ჩართული იყო ევროპის საბჭოსა და ევროკომისიის ერთობლივ პროექტში, რომელიც მიზნად ისახავდა კიბერდანაშაულის კონვენციასთან ქართული კანონმდებლობის ჰარმონიზაციას. ამ პროექტის ფარგლებში ცვლილებები შევიდა სისხლის სამართლის კოდექსსა და სისხლის სამართლის საპროცესო კოდექსში.

საქართველო განაგრძობს კანონების გადახედვისა და შესწორების პროცესს, მეტი სიცხადისა და კონვენციასთან უფრო მეტად მისადაგების მიზნით. ეს არის განხილვისა და შესწორების მუდმივი პროცესი. სხვა ქვეყნების

მსგავსად, საქართველომ უნდა მოახდინოს თავისი კანონების ადაპტირება საერთაშორისო შეთანხმებებისა და ახალი ტექნოლოგიების დანერგვის შესაბამისად. საქართველო, რომელმაც დაახლოებით 25 წლის წინ დაიბრუნა დამოუკიდებლობა, მუდმივად ცდილობს მთელი თავისი საკანონმდებლო სისტემის მოდერნიზებას პრაქტიკული გამოცდილების გათვალისწინებითა და მეგობარი ქვეყნების დახმარებით.

კანონი ინფორმაციული უსაფრთხოების შესახებ

კანონი ინფორმაციული უსაფრთხოების შესახებ ეხება იმ იურიდიულ პირებს და სახელმწიფო ორგანოებს, რომლებიც წარმოადგენენ კრიტიკული ინფორმაციული სისტემის სუბიექტებს. 2014-სა და 2015 წელს კანონში რამდენიმე ცვლილება შევიდა. შესაბამისად, კრიტიკული ინფორმაციული სისტემის სუბიექტებისა და მათი კატეგორიზაციიის სპეციალური სია, თავდაცვის სფეროს ჩათვლით, შესაძლოა დამტკიცდეს მხოლოდ საქართველოს მთავრობის ბრძანებულების საფუძველზე. სიას, იუსტიციის სამინისტრო თავდაცვის სამინისტროსთან, შინაგან საქმეთა სამინისტროსთან და ახლადშექმნილი სახელმწიფო უსაფრთხოების სამსახურთან შეთანხმებით, დასამტკიცებლად წარუდგენენ პრემიერ-მინისტრს. თავდაპირველად აღნიშნული სია მტკიცდებოდა საქართველოს პრეზიდენტის ბრძანებულების საფუძველზე, რომელსაც პრეზიდენტის წინაშე დასამტკიცებლად საქართველოს ეროვნული უსაფრთხოების საბჭო წარადგენდა. კიდევ ერთი ცვლილება, რომელიც კანონში შევიდა, უკავშირდებოდა თავდაცვის სამინისტროში საჯარო სამართლის იურიდიული პირის – კიბერუსაფრთხოების ბიუროს შექმნას.

კანონი ადგენს კრიტიკული ინფორმაციული სისტემის სუბიექტების რიგ ვალდებულებებსა და მოთხოვნებს ინფორმაციული უსაფრთხოების პოლიტიკის მიღებასთან დაკავშირებით, რომელიც უნდა შეესაბამებოდეს სტანდარტიზაციის საერთაშორისო ორგანიზაციისა (ISO) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილ ინფორმაციული უსაფრთხოების სტანდარტებს. სიაში არსებული კრიტიკული ინფორმაციის სისტემის სუბიექტებს ასევე მოეთხოვებათ ინფორმაციული უსაფრთხოების ოფიცრებისა და კიბერუსაფრთხოების პერსონალის შერჩევა/დანიშვნა. ამასთანავე, მათ ევალებათ განახორციელონ ინფორმაციული აქტივის აღრიცხვა კრიტიკულობის შესაბამისი კლასის მინიჭების თვალსაზრისით, როგორც კონფიდენციალური, შეზღუდული, არაკლასიფიცირებული ან ღია ინფორმაციული აქტივი. კანონი უფლებამოსილებას ანიჭებს კრიტიკული ინფრასტრუქტურის განსაზღვრულ სუბიექტს, რომ ინფორმაციული სისტემის აუდიტისა და შეღწევადობის (პენეტრაციის) ტესტის ჩატარების მიზნით დაიქირავოს თავისი შერჩეული, შესაბამისი კომპეტენციის მქონე დამოუკიდებელი პირი ან ორგანიზაცია. ტესტის ჩატარების წესს ნორმატიული აქტით ადგენს მონაცემთა გაცვლის სააგენტო. კრიტიკული ინფრასტრუქტურის სუბიექტი ვალდებულია მოახდინოს კომპიუტერული უსაფრთხოების ინციდენტების იდენტიფიცირება და მათზე რეაგირება.

კანონი ასევე განსაზღვრავს საქართველოს CERT-ის, როგორც ეროვნული CERT-ის, უფლებებს და ინტერაქციის დონეს, ასევე – ინფორმაციის გაცვლას კრიტიკული ინფორმაციული სისტემების მფლობელებთან.

CERT-ს არა აქვს სუბიექტების მონაცემებზე წვდომის უფლება მათი ნებართვის გარეშე. ეს იმ შემთხვევაშია შესაძლებელი, თუკი კრიტიკული ინფორმაციის სისტემის სუბიექტი ნებაყოფლობით მისცემს მონაცემთა გაცვლის სააგენტო CERT-ს ამის საშუალებას. თავის მხრივ, კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერი ვალდებულია მიაწოდოს ინფორმაცია CERT-ს კომპიუტერული ინციდენტების შესახებ. თუმცა, სუბიექტის სურვილზეა დამოკიდებული, რამდენად უნდა CERT-ის დახმარება. ნებისმიერ იურიდიულ პირს ან სახელმწიფო ორგანოს, რომელიც არ არის წარმოდგენილი კრიტიკული ინფორმაციული სისტემის სუბიექტების სიაში, შეუძლია ნებაყოფლობით აიღოს ვალდებულება და აამუშაოს კანონმდებლობაში გათვალისწინებული ინფორმაციული უსაფრთხოების მექანიზმები.[67]

ამ კანონის მოქმედება არ ვრცელდება მასმედიაზე, საგამომცემლო, სამეცნიერო, საგანმანათლებლო, რელიგიურ და საზოგადოებრივ ორგანიზაციებსა და პოლიტიკურ პარტიებზე, მიუხედავად იმისა, თუ რამდენად მნიშვნელოვანია მათი საქმიანობა ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.

აღნიშნული კანონი ასევე რეგულირდება რიგი ნორმატიული აქტებით, რომლებიც განსაზღვრავენ და ადგენენ სამართლებრივ ინსტრუმენტებს პრაქტიკული განხორციელებისათვის. დღემდე არსებობს მონაცემთა გაცვლის სააგენტოს მიერ გამოცემული შვიდი ნორმატიული აქტი:

- მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ;
- კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისათვის მინიმალური სტანდარტების დამტკიცების შესახებ;
- ქსელური სენსორის კონფიგურაციის წესების შესახებ;
- ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების შესახებ; ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესის შესახებ და ავტორიზაციის პროცედურებისა და საფასურის შესახებ;
- ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის შესახებ;
- ინფორმაციული აქტივების მართვის წესების შესახებ.

თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს გამოცემული აქვს სამი ნორმატიული აქტი:

- თავდაცვის სამინისტროს საჯარო სამართლის იურიდიული პირის, კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ;
- ინფორმაციული უსაფრთხოების მინიმალური სტანდარტების შესახებ;
- ინფორმაციული აქტივების მართვის წესების შესახებ.

კიბერუსაფრთხოების ბიურო თავდაცვის სფეროში განსაზღვრული კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის სტანდარტებსა და მოთხოვნებს ISO-სა და ISACA-ს მიერ დადგენილი წესების შესაბამისად განსაზღვრავს. ინფორმაციული უსაფრთხოების შესახებ კანონში ცვლილებები განხორციელდა იმ მიზნით, რომ ბევრად ეფექტურად ყოფილიყო შესაძლებელი კრიტიკული ინფორმაციული სისტემის სუბიექტებში კონფიდენციალური და შიდა მოხმარების ინფორმაციის დაცვა.

კრიტიკული ინფორმაციული სისტემის სუბიექტების განახლებული სია, რომელიც პრემიერ-მინისტრის #312 ბრძანებულების საფუძველზე დამტკიცდა 2014 წლის 29 აპრილს:[68]

1. საქართველოს იუსტიციის სამინისტრო;
2. საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო;
3. საქართველოს საგარეო საქმეთა სამინისტრო;
4. საქართველოს ფინანსთა სამინისტრო;
5. საქართველოს შინაგან საქმეთა სამინისტრო;
6. საქართველოს რეგიონული განვითარებისა და ინფრასტრუქტურის სამინისტრო;
7. საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო;
8. საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;
9. საქართველოს პარლამენტი;
10. საქართველოს პრეზიდენტის ადმინისტრაცია;
11. საქართველოს მთავრობის კანცელარია;
12. საქართველოს ეროვნული ბანკი;
13. საქართველოს მთავარი პროკურატურა;
14. თბილისის მერია;
15. საქართველოს ცენტრალური საარჩევნო კომისიის აპარატი;
16. საჯარო სამართლის იურიდიული პირი – „სმარტ ლოჯიქი“;
17. საჯარო სამართლის იურიდიული პირი – სახელმწიფო შესყიდვების სააგენტო;
18. საჯარო სამართლის იურიდიული პირი – სოციალური მომსახურების სააგენტო;
19. საჯარო სამართლის იურიდიული პირი – შეფასებისა და გამოცდების ეროვნული ცენტრი;
20. საჯარო სამართლის იურიდიული პირი – სახელმწიფო სერვისების განვითარების სააგენტო;
21. საჯარო სამართლის იურიდიული პირი – საფინანსო-ანალიტიკური სამსახური;
22. საჯარო სამართლის იურიდიული პირი – საჯარო რეესტრის ეროვნული სააგენტო;
23. საჯარო სამართლის იურიდიული პირი, შემოსავლების სამსახური;

24. საჯარო სამართლის იურიდიული პირი – საქართველოს ფინანსური მონიტორინგის სამსახური;
25. საჯარო სამართლის იურიდიული პირი – სამედიცინო საქმიანობის სახელმწიფო რეგულირების სააგენტო;
26. საჯარო სამართლის იურიდიული პირი – ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრი;
27. საჯარო სამართლის იურიდიული პირი, სამედიცინო მედიაციის სამსახური;
28. საჯარო სამართლის იურიდიული პირი – სამოქალაქო ავიაციის სააგენტო;
29. საჯარო სამართლის იურიდიული პირი – საზღვაო ტრანსპორტის სააგენტო;
30. საჯარო სამართლის იურიდიული პირი – სახმელეთო ტრანსპორტის სააგენტო;
31. საჯარო სამართლის იურიდიული პირი – განათლების მართვის საინფორმაციო სისტემა;
32. სააქციო საზოგადოება „საქართველოს რკინიგზა“;
33. შეზღუდული პასუხისმგებლობის საზოგადოება „საქაერონავიგაცია“;
34. შეზღუდული პასუხისმგებლობის საზოგადოება „საქართველოს აეროპორტების გაერთიანება“;
35. საჯარო სამართლის იურიდიული პირი – განათლების ხარისხის განვითარების ეროვნული ცენტრი;
36. საქართველოს შინაგან საქმეთა სამინისტროს სახელმწიფო საქვეუწყებო დაწესებულება – საქართველოს სასაზღვრო პოლიცია;
37. საჯარო სამართლის იურიდიული პირი – საქართველოს შინაგან საქმეთა სამინისტროს მომსახურების სააგენტო;
38. საქართველოს შინაგან საქმეთა სამინისტროს საჯარო სამართლის იურიდიული პირი – „112“;
39. საჯარო სამართლის იურიდიული პირი – გარემოს დაცვის ეროვნული სააგენტო.

ინფორმაციული უსაფრთხოების შესახებ კანონის მიღებით საქართველომ შეძლო ევროპის კონვენციასთან მიახლოება და მიაღწია იმაზე მეტს, ვიდრე ზოგიერთმა შედარებით დიდმა დემოკრატიულმა ქვეყანამ. აღსანიშნავია, რომ ამ კანონთან დაკავშირებით არსებობს ორი გამოწვევა: პირველი – მთავრობასა და კერძო ორგანიზაციებს შორის ეფექტიანი თანამშრომლობის მიღწევა. ამასთან დაკავშირებით მთავრობის რამდენიმე წარმომადგენელმა ჩვენთან საუბრისას აღნიშნა, რომ კერძო სტრუქტურების მხრიდან თანამშრომლობისათვის მზადყოფნა საკმაოდ დაბალია. მეორე – პროფესიონალი კადრების ნაკლებობა, რაც უპირობოდ საჭიროა კანონის სრული ამოქმედებისათვის. ერთმა ექსპერტმა, რომელმაც არ ისურვა თავისი სახელის გაცხადება, აღნიშნა, რომ:

„საქართველოს ვერც ერთი უნივერსიტეტი ვერ იძლევა კარგ განათლებას კომპიუტერული მეცნიერებისა და კიბერუსაფრთხოების დარგში. არც ერთ უნივერსიტეტს არ შესწევს ამის უნარი. ინფორმაციული უსაფრთხოების შესახებ კანონის ეფექტიანი ამოქმედება არის გამოწვევა – განა ჩვენ გვყავს კიბერუსაფრთხოების დარგის საკმარისი სპეციალისტები, რომლებიც დააკმაყოფილებენ კანონში მოცემულ ყველა მოთხოვნას? ყველა ჩამოთვლილ ორგანიზაციას, რომელთა რიცხვი 39-ია, სჭირდება ამ პრობლემაზე მომუშავე, სულ მცირე, 2-3 პირი. შევძლებთ კი ამას? ამისათვის ჩვენ არ გვაქვს საკმარისი ადამიანური რესურსი“.

სისხლის სამართლის კოდექსი

საქართველოში კიბერდანაშაულის დასჯის საკითხებს არეგულირებს სისხლის სამართლის საპროცესო კოდექსის 25-ე, 27-ე, 32-ე, 35-ე, 38-ე თავები, რომლის მიხედვითაც, სისხლის სამართლის პასუხისმგებლობა ეკისრება პირს კიბერსივრცეში ქვემოთ ჩამოთვლილი უკანონო ქმედების ჩადენის შემთხვევაში:[69]

- კომპიუტერულ სისტემაში უკანონოდ შეღწევა (მუხლი 284);
- დამაზიანებელი კომპიუტერული პროგრამის შექმნა, გამოყენება ან გავრცელება (მუხლი 285);
- კომპიუტერული სისტემის ხელყოფა ან/და კომპიუტერული მონაცემის დაზიანება, წაშლა და მოდიფიცირება (მუხლი 286);
- პორნოგრაფიული პროდუქციის უკანონოდ დამზადება ან/და წინასწარი შეცნობით არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული პროდუქციის შეძენა, შენახვა, ჩვენებაზე დასწრება, შეთავაზება, გავრცელება, გადაცემა, რეკლამირება, ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ან ასეთი პროდუქციით სარგებლობა (მუხლი 255);
- არასრულწლოვნის ჩაბმა პორნოგრაფიული ან პორნოგრაფიული ხასიათის სხვა პროდუქციის უკანონოდ დამზადებასა და გასაღებაში (მუხლი 255.1);
- საავტორო უფლებისა თუ რაიმე მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა (მუხლი 189);
- კიბერტერორიზმი (მუხლი 324.1);
- ყალბი საკრედიტო ან საანგარიშსწორებო ბარათის დამზადება, გასაღება ან გამოყენება (მუხლი 210);
- თაღლითობა, ანუ მართლსაწინააღმდეგო მისაკუთრების მიზნით სხვისი ნივთის დაუფლება ან ქონებრივი უფლების მიღება მოტყუებით (მუხლი 180).

324.1 მუხლში შესწორება შევიდა 2012 წელს, 255-ე და 255.1 მუხლებში – 2013 წელს. 285-ე მუხლში შესწორება შევიდა 2014 წელს, რათა მომხდარიყო მათი შესაბამისობაში მოყვანა ევროპის კონვენციასთან. მთავრობა მომავალშიც გეგმავს არსებული კანონების გადახედვას. ეს შესწორებები შედის კანონისთვის მეტი სიმკვეთრის მინიჭებისა და საქართველოს კანონმდებლობის კონვენციის დადგენილ სტანდარტებთან მიახლოების მიზნით.

ორგანიზებულ დანაშაულთან ბრძოლის სტრატეგია

2013 წელს შინაგან საქმეთა სამინისტრომ შეიმუშავა ორგანიზებულ დანაშაულთან ბრძოლის სტრატეგიის პროექტი, რომელშიც 1.3 ქვეთავი კიბერდანაშაულთან ბრძოლას ეხება. სტრატეგიაში მოცემულია უკვე განხორციელებული ინიციატივების ზოგადი მიმოხილვა და შემდგომი ნაბიჯები, რომლებიც უნდა გადაიდგას კიბერდანაშაულის წინააღმდეგ საბრძოლველად. სტრატეგიაში განხილულია შსს-ის კიბერდანაშაულთან ბრძოლის ძირითადი მიზნები: საზოგადოების ცნობიერების ამაღლება, საკანონმდებლო ბაზის პერიოდული გადასინჯვა, კიბერდანაშაულთან ბრძოლაში ჩართული სააგენტოების (სამთავრობო უწყებების) შესაძლებლობების გაზრდა, თანამშრომლობის გაღრმავება სამართალდამცავ ორგანოებსა და კერძო სექტორს შორის, ასევე თანამშრომლობის გაღრმავება თანამოაზრე ქვეყნებთან და საერთაშორისო ორგანიზაციებთან (OECD, EU, OSCE, NATO, UN, ITU, CoE). აღნიშნული სტრატეგია დაამტკიცა საქართველოს მთავრობამ 2013 წლის ოქტომბერში.[70]

ცვლილებები კანონებში ელექტრონული თვალთვალის შესახებ

2014 წლის სექტემბერში ძალაში შევიდა პერსონალურ მონაცემთა დაცვის შესახებ კანონში განხორციელებული ცვლილებები. ამ ცვლილებების მიხედვით, პერსონალურ მონაცემთა დაცვის ინსპექტორს გაეზარდა უფლებამოსილება, მისი მანდატი გავრცელდა სამართალდამცავი ორგანოების მიერ მონაცემთა დამუშავებაზე და მასვე დაევალა ფარული მიყურადებისა და თვალთვალის კანონთან შესაბამისობის ზედამხედველობაც. კანონის ეს დებულება ეხება სისხლის სამართლის საპროცესო კოდექსის 143.1 ა) მუხლით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებებს, რაც მოიცავს სატელეფონო საუბრის ფარულ მიყურადებას და ჩაწერას.

ზემოაღნიშნულმა ცვლილებებმა შესწორებები გამოიწვია ოპერატიულ-სამძებრო ღონისძიებების შესახებ კანონში, სისხლის სამართლის საპროცესო კოდექსში, ელექტრონული კომუნიკაციების შესახებ კანონში. საკანონმდებლო ცვლილებები არასამთავრობო ორგანიზაციებისა და სამოქალაქო საზოგადოების მხრიდან დიდი განსჯისა და კრიტიკის საგანი გახდა.

ამრიგად, სისხლის სამართლის საპროცესო კოდექსში შეტანილი ცვლილებების მიხედვით, სატელეფონო საუბრის ფარული ჩაწერა/მიყურადების პროცესი ტექნიკურად ხორციელდება ორეტაპიანი ელექტრონული სისტემის მეშვეობით, რომლის თანახმად, საჭიროა ორი სუბიექტის თანხმობა, რათა ტექნიკურად დაიწყოს ფარული საგამოძიებო მოქმედების შესრულება. აქედან

ერთი სუბიექტი არის უფლებამოსილი სამართალდამცავი სტრუქტურები, ხოლო მეორე – პერსონალურ მონაცემთა დაცვის ინსპექტორი, რომელიც სატელეფონო საუბრის ფარული ჩაწერა/მიყურადების პროცესის დასაწყებად ელექტრონულ თანხმობას იძლევა. ორეტაპიანი ელექტრონული სისტემა ნიშნავს იმას, რომ ორივე მხარეს, სამართალდამცავებსა და პერსონალურ მონაცემთა ინსპექტორს, ექნებათ ელექტრონული კომუნიკაციების კომპანიების მონაცემებთან წვდომის ე.წ. „გასაღები“.[71]

კანონში შეტანილი ცვლილებების მომხრეები ხაზს უსვამენ ამ ცვლილებების პოზიტიურ მხარეს. კერძოდ, სატელეფონო საუბრის ფარული ჩაწერა/მიყურადების პროცესის დასაწყებად არა მარტო მოსამართლის განჩინება და პროკურორის მოტივირებული დადგენილებაა საჭირო, არამედ აუცილებელია პერსონალურ მონაცემთა ინსპექტორის ელექტრონული თანხმობა. ოპონენტები მოითხოვენ ე.წ. „გასაღების“ სამართალდამცავი ორგანოების სისტემიდან გასვლას და პროვაიდერი კომპანიებისთვის გადაცემას. ამის საპასუხოდ მთავრობის დოკუმენტში – *საქართველოს მთავრობის კომენტარები არასამთავრობო ორგანიზაციათა კოალიციის ანგარიში* – აღნიშნულია, რომ ე. წ. „გასაღების“ პროვაიდერი კომპანიებისთვის გადაცემით მაქსიმალურად გართულდება პროვაიდერი კომპანიის საქმიანობის კონტროლი. ამ საკითხთან დაკავშირებით დოკუმენტში ასევე ხაზგასმულია შემდეგი გარემოება: „საქართველო არის ოკუპირებული ქვეყანა და მობილური ოპერატორები უცხო ქვეყნის რეზიდენტებია. ასეთი ვითარება პირდაპირ გავლენას იქონიებს უცხოეთის სადაზვერვო ორგანიზაციების შესაძლებლობების გაზრდაზე და ამის პროპორციულად – საქართველოს კონტრდაზვერვითი შესაძლებლობების შესუსტებაზე.“[72]

ე.წ. ორი გასაღები, ანუ ორეტაპიანი ელექტრონული სისტემის გამოყენებით ფარული საგამოძიებო მოქმედების განხორციელება და ელექტრონული თანხმობა არ ვრცელდება ინტერნეტით გადაცემულ მონაცემთა მოპოვებაზე. ამასთან დაკავშირებით ორგანიზაცია *საერთაშორისო გამჭვირვალობა* კრიტიკულ მოსაზრებას გამოთქვამს. ორგანიზაციის თანახმად, „შსს-ს კვლავ რჩება უფლება, შეუზღუდავი რაოდენობის ინფორმაცია მიიღოს ინტერნეტ-პროვაიდერებისაგან, ყოველგვარი გარე კონტროლის გარეშე. ამ შემთხვევაში პერსონალურ მონაცემთა დაცვის ინსპექტორი შემოწმებას ახორციელებს მხოლოდ სასამართლოს, პროკურატურის და ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის მიერ მიწოდებული ინფორმაციის შედარებით და მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებით“. მათ მიაჩნიათ, რომ „კონტროლის ამგვარი მექანიზმი ფორმალური ხასიათისაა, ვინაიდან შსს ინტერნეტპროვაიდერებიდან ინფორმაციის მოპოვების პროცესს იწყებს ყოველგვარი გარე კონტროლის გარეშე. ინსპექტორი შემოწმებისას მხოლოდ სამართალდამცავი ორგანოს კეთილსინდისიერებაზე არის დამოკიდებული: რამდენად სწორ ინფორმაციას მიაწვდის ეს უკანასკნელი“.[73]

საერთაშორისო გამჭვირვალობა ასევე აკრიტიკებს სისხლის სამართლის საპროცესო კოდექსში შეტანილ შემდგომ ცვლილებას, რომლის მიხედვითაც, 143.1 მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული ფარული საგამოძიებო მოქმედებების ჩატარებისთვის სპეციალურ პროგრამულ საშუალებებს შექმნიან სამართალდამცავი ორგანოები. ორგანიზაციას მიაჩნია, რომ ეს დიდი რისკის შემცველი იქნება, რადგან შესაძლებელი

იქნება იმგვარად დაპროგრამება, რომ ინფორმაციის მოპოვება კონტროლის საშუალებების გვერდის ავლით მოხდეს.[74]

143.1 ა და ბ პუნქტები ფარული საგამოძიებო მოქმედებების შემდეგ სახეებს მოიცავს:[75]

ა) სატელეფონო საუბრის ფარული მიყურადება და ჩაწერა;

ბ) ინფორმაციის მოხსნა-ფიქსაცია კავშირგაბმულობის არხიდან, კომპიუტერული სისტემიდან და ამ მიზნით კომპიუტერულ სისტემაში შესაბამისი პროგრამული უზრუნველყოფის საშუალებების ინსტალაცია.

ცვლილებები ასევე შეეხო ელექტრონული კომუნიკაციების შესახებ კანონსაც. ეს კანონი ადგენს საქართველოს ტერიტორიაზე ელექტრონული საკომუნიკაციო ქსელებითა და საშუალებებით საქმიანობის სამართლებრივ და ეკონომიკურ საფუძვლებს, ამ სფეროში კონკურენტუნარიანი გარემოს ჩამოყალიბებისა და რეგულირების პრინციპებს, დამოუკიდებელი ეროვნული მარეგულირებელი ორგანოს (საქართველოს კომუნიკაციების ეროვნული კომისიის) ფუნქციებს, ელექტრონული საკომუნიკაციო ქსელებისა და საშუალებების ფლობის, მათი გამოყენებისა და მომსახურების მიწოდების დროს ფიზიკური და იურიდიული პირების უფლებებსა და მოვალეობებს.[76]

ამ კანონში ახალი ცვლილებების თანახმად, რომელიც ძალაში შევიდა 2014 წლის 30 ნოემბერს, ელექტრონული კომუნიკაციის კომპანიას უნდა ჰქონდეს თავისი ქსელების მეშვეობით განხორციელებული კომუნიკაციის შინაარსის შესახებ ინფორმაციის რეალურ დროში მიწოდების ტექნიკური შესაძლებლობა. ელექტრონული კომუნიკაციების კომპანია ასევე ვალდებულია აღრიცხოს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შესაბამისი სახელმწიფო ორგანოებისთვის გადაცემის ფაქტები და ეს ინფორმაცია უნდა მიაწოდოს პერსონალურ მონაცემთა ინსპექტორს.[77]

ელექტრონული კომუნიკაციების შესახებ კანონში ცვლილებები შევიდა შემდეგ საკითხთან დაკავშირებითაც: ფარული საგამოძიებო მოქმედებებისას სამართალდამცავ სტრუქტურებს კავშირგაბმულობის არხში არსებული მაიდენტიფიცირებელი მონაცემების კოპირებისა და მათი 2 წლის ვადით შენახვის უფლება აქვთ. ამ ინფორმაციის კავშირგაბმულობის არხიდან მოხსნის და ფიქსაციის შემდგომ ფარულ საგამოძიებო მოქმედებებს უფლებამოსილი ორგანო ახორციელებს კოპირებულ მონაცემთა აღნიშნული ბანკებიდან, სასამართლოს განჩინებით ან პროკურორის მოტივირებული დადგენილებით.[78]

კანონის ამ დებულებამ დიდი კრიტიკა გამოიწვია სახალხო დამცველის აპარატის წარმომადგენლების მხრიდან, რადგანაც ეს დებულება უფლებამოსილებას ანიჭებს მონაცემთა ბანკების კოპირებას სასამართლოს განჩინების გარეშე.[79]

სახელმწიფო ორგანოები, რომლებსაც აქვთ ფარული/საგამოძიებო მოქმედებების განხორციელების უფლებამოსილება, არის სახელმწიფო უსაფრთხოების სამსახური და შინაგან საქმეთა სამინისტრო.

სისხლის სამართლის საპროცესო კოდექსის მიხედვით, ფარული საგამოძიებო საქმიანობის განხორციელება შესაძლებელია მოსამართლის განჩინებით. ამასთან, ფარული საგამოძიებო მოქმედება პროკურორის მოტივირებული დადგენილებით შეიძლება ჩატარდეს მოსამართლის თანხმობის გარეშე, გადაუდებელი აუცილებლობისას, როდესაც დაყოვნებამ შეიძლება გამოიწვიოს გამოძიებისათვის ნიშვნელოვანი ფაქტობრივი მონაცემების გა-

ნადგურება ან შეუძლებელი გახადოს ამ მონაცემების მოპოვება. ასეთ შემთხვევაში პროკურორი ვალდებულია ფარული საგამოძიებო მოქმედებების დაწყებიდან არაუგვიანეს 24 საათისა მიმართოს სასამართლოს შუამდგომლობით ჩატარებული ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ. მოსამართლე პროკურორის შუამდგომლობას განიხილავს სასამართლოში მისი წარდგენიდან არაუგვიანეს 24 საათისა.[80]

დასკვნები და რეკომენდაციები

2008 წელს განვითარებული მოვლენების შემდეგ საქართველო აქტიურად ჩაერთო კიბერუსაფრთხოების უზრუნველყოფის საქმეში. მართალია, საქართველოს არ ჰქონდა ისეთი მკვეთრი რეაქცია, როგორიც, მაგალითად, ესტონეთს, მაგრამ ეს საკითხი დადგა ქვეყნის დღის წესრიგში. აღსანიშნავია, რომ 2008 წლის შემდეგ საქართველომ მნიშვნელოვანი ნაბიჯები გადადგა ბევრად უსაფრთხო კიბერგარემოს შესაქმნელად, მაგრამ დღემდე ვერ მოხერხდა ამ საკითხის სეკურიტიზაცია. პრობლემასთან ბრძოლა მოითხოვს თანმიმდევრული და მიზანმიმართული კიბერპოლიტიკის გატარებას, რომელიც საკითხს მნიშვნელოვან სახელმწიფო დონეზე აიყვანს და პრიორიტეტულად აქცევს. საქართველო ცდილობს არ ჩამორჩეს თავის ევროპელ პარტნიორებს და შექმნას და განავითაროს ბევრად უსაფრთხო კიბერგარემო. ამისათვის კი მნიშვნელოვანია საკითხში გათვითცნობიერების დაბალი მაჩვენებლისა და რესურსების ნაკლებობის დაძლევა. დღესდღეობით საქართველოსთვისაც და მთელი მსოფლიოსთვისაც სულ უფრო იზრდება კიბერსაფრთხეების როგორც მოცულობა, ისე ხარისხობრივი მაჩვენებელი, მათ შორის, იზრდება კიბერდანაშაული მობილურ მოწყობილობებზეც.

მონაცემთა გაცვლის სააგენტო და კიბერდანაშაულთან ბრძოლის სამართველო დაკომპლექტებულია საქმის მიმართ პასუხისმგებლობითა და ენთუზიაზმით აღსავსე ადამიანებით. მიუხედავად იმისა, რომ ეს პერსონალი შეესაბამება ძირითად მოთხოვნებს, მათ, კიბერუნარების გაღრმავების მიზნით, მაინც ესაჭიროებათ მაღალი საკვალიფიკაციო პროფესიული სწავლება-ტრენინგები, რათა შეძლონ მომავალში კიდევ უფრო რთულ კიბერსაფრთხეებთან გამკლავება. ამ მიმართულებით ასევე აუცილებელი ფაქტორია ახალი კადრების მოძიება და მომზადება, რადგან ერთ-ერთ მთავარ პრობლემას წარმოადგენს ამ სფეროს სპეციალისტების ნაკლებობა ქვეყანაში.

კიბერუსაფრთხოების პოლიტიკის თვალსაზრისით მნიშვნელოვან როლს თამაშობს პრემიერ-მინისტრის დაქვემდებარებაში არსებული სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭო, რომელმაც საკონსტიტუციო ცვლილებების შემდგომ მნიშვნელოვანი პოლიტიკური ძალაუფლება შეიძინა. საბჭოს განზრახული აქვს ამ კუთხით მკვეთრი ცვლილებების შეტანა და მთავრობის შესაბამის უწყებებთან კოორდინირება. საქართველოში კიბერუსაფრთხოების გარემოს გაუმჯობესებისა და ეფექტურობის გაზრდას მნიშვნელოვნად განაპირობებს ზემოჩამოთვლილი ამ სამი სამთავრობო ერთეულის ერთობლივი ძალისხმევა.

კვლევის შედეგად მოპოვებული ინფორმაცია, უკეთესი კიბერგარემოს შექმნის თვალსაზრისით, შემდეგი რეკომენდაციების გაკეთების საშუალებას იძლევა. განსაკუთრებით პრიორიტეტული რეკომენდაციები შეჯამებულია ქვემოთ მოყვანილ ცხრილში.

- **პასუხისმგებელი სამთავრობო სტრუქტურები და მათი ურთიერთობა კერძო სექტორთან**
  - სახელმწიფო უსაფრთხოების ახალმა საბჭომ ადაპტირებული საუკეთესო პრაქტიკის გამოყენებით უნდა შეიმუშაოს ეფექტური კიბერპოლიტიკა და სხვადასხვა სამთავრობო უწყებასთან ეფექტური კოორდინირება უნდა მოახდინოს.
  - პრიორიტეტულ საკითხად უნდა იქცეს მთავრობასა და კერძო სექტორს შორის ეფექტური პარტნიორობის საუკეთესო პრაქტიკის დანერგვა.
  - მთავრობამ უნდა შეიმუშაოს სამთავრობო კომპიუტერული ტექნიკის საჭიროებისამებრ შეცვლის/განახლების ეფექტური გეგმა და მოახდინოს ლიცენზირებული კომპიუტერული პროგრამებით უზრუნველყოფა. ცხადია, ამ მისიის განხორციელება არა მარტო დიდ ფინანსურ რესურსებთან ან დროის ფაქტორთანაა დაკავშირებული, არამედ ერთგვარ მზადყოფნასა და საკითხის მნიშვნელოვან რანგში აყვანასაც მოითხოვს.
    - « ახალი კომპიუტერული ტექნიკა და პროგრამები უნდა იყოს დაცული შესაბამისი უსაფრთხოების მექანიზმებით.

- **პოლიტიკისა და კანონების გადახედვა**
  - საქართველოს კიბერუსაფრთხოების სტრატეგიასა და სამოქმედო გეგმაში უნდა აისახოს კონკრეტული და მკაფიო მიზნები.
  - უნდა შემუშავდეს და დაინერგოს ეფექტური მექანიზმი, რომელიც სამართლებრივი ბაზის რეგულარულ და მეთოდურ გადახედვას შეუწყობს ხელს. ამ თვალსაზრისით, საკანონმდებლო ცვლილებების შემთხვევაში, მნიშვნელოვანია კონსულტაციების გამართვა კიბერსამართლის ექსპერტებთან პარტნიორი ქვეყნებიდან, ევროსაბჭოდან და ევროკავშირიდან, რაც კიდევ უფრო შეუწყობს ხელს ევროპულ სტანდარტებთან დაახლოების პროცესს. ცვლილებები უნდა განხორციელდეს ახალ ტექნოლოგიებთან შესაბამისობაში.

- არსებობს გარკვეული უხერხულობა საკონსტიტუციო უფლებების დაცვასა და ოპერატიულ სამძებრო ღონისძიებებს შორის. ამ მხრივ საქართველო საჭიროებს დახმარებას სათანადო სამართლებრივი მექანიზმების შესაქმნელად, რათა დაძლიოს ეს პრობლემა.
- მნიშვნელოვანია მალევე შესწორდეს კანონი ინფორმაციული უსაფრთხოების შესახებ და შეიქმნას და დამტკიცდეს იმ მნიშვნელოვანი ინფრასტრუქტურის სია, რომელსაც კერძო სექტორი ფლობს.
  - « ამასთან, უნდა მოხდეს კერძო სექტორის მფლობელობაში არსებული მნიშვნელოვანი ინფრასტრუქტურის კიბერუსაფრთხოების პრაქტიკის შეფასება.

- **კიბერუსაფრთხოებისა და კიბერდანაშაულის შესახებ როგორც ფართო საზოგადოების, ისე საჯარო მოხელეებისა და სამთავრობო სტრუქტურების ხელმძღვანელი პირების ცნობიერების ამაღლება**

  - საზოგადოების ცნობიერების ამაღლების მიზნით დაიგეგმოს და განხორციელდეს სპეციალური პროგრამები, რათა საზოგადოებამ უკეთ გაიგოს, თუ რა რისკების მომტანია კიბერდანაშაული მათთვის და რა სახის საფრთხეების შემცველია ის მოზარდებისთვის. ასევე მნიშვნელოვანია საზოგადოების ცნობიერების ამაღლება პრევენციული ზომებისა და შეტყობინების აუცილებლობის შესახებ. ამისათვის საჭიროა:
    - « სხვა ქვეყნების საუკეთესო პრაქტიკის გათვალისწინება.
    - « კონსულტაციების გამართვა მედიასთან, სასწავლო დაწესებულებებთან და დაინტერესებულ ორგანიზაციებთან, რათა შემუშავდეს ინფორმაციის მიწოდების საუკეთესო გზა საზოგადოების სხვადასხვა ფენისთვის.
  - კომპიუტერული ჰიგიენის მარტივი კურსის შემუშავება და მიწოდება საჯარო მოხელეთათვის.
  - კიბერუსაფრთხოების ძირეულ საკითხებზე მოკლე ბრიფინგებისა და დისკუსიების შემუშავება საქართველოს მაღალი თანამდებობის პირთათვის.

- **კიბერდანაშაულის შეტყობინების მექანიზმი**
  - მას შემდეგ, რაც საზოგადოების ცნობიერების ამაღლების პროგრამა შედეგს გამოიღებს, უნდა დაინერგოს კიბერდანაშაულის შეტყობინების ეფექტური სისტემა, რომელიც სასურველია წარმოადგენდეს თაღლითური საქმიანობისა და კიბერდანაშაულის შეტყობინების პორტალის ისეთ მოდელს, როგორიც ბრიტანეთში შეიმუშავეს.

- **განათლება და ტრენინგი**
  - შემუშავდეს სპეციალური ტრენინგპროგრამები და დახმარება გაეწიოთ შსს-ის წარმომადგენლებს დასავლური პრაქტიკის, ტაქტიკის, ტექნიკის და პროცედურების (TTPs) შესასწავლად. კერძოდ, გამოძიების, კომპიუტერული ექსპერტიზის, მტკიცებულებების ამოღება/მთლიანობის შენარჩუნების, ტექნიკური ანალიზის, მაღალი კვალიფიკაციის უნარების შეძენის, საქმეების (ე.წ. „ქეისების“) ეფექტური მომზადების და ასევე სხვადასხვა ქვეყნის სტრუქტურებიდან/ორგანიზაციებიდან ინფორმაციის გამოთხოვისა და ექსტრადიციის წესების მხრივ. ამასთან დაკავშირებით უნდა აღინიშნოს, რომ შსს-ის თანამშრომლების ტრენინგები საბაზისო ინსტრუქციებს უნდა გასცდეს და დასავლური სტანდარტებით მოხდეს მათი ტექნიკური უნარებისა და შესაძლებლობების გაზრდა.
  - შეიქმნას პროგრამები კვლევით ინსტიტუტებთან და უმაღლეს სასწავლებლებთან ერთად იმისთვის, რომ:
    - « კრიტიკული ინფორმაციული სისტემის ყველა სუბიექტს, რომელიც პასუხისმგებელია საკუთარი ორგანიზაციის ინფორმაციულ უსაფრთხოებაზე, ჰქონდეს შესაბამისი ცოდნა და უნარ-ჩვევები დაკისრებული სამუშაოს შესასრულებლად, ინფორმაციული უსაფრთხოების შესახებ კანონის შესაბამისად.
    - « შეირჩეს ახალი კადრები და სათანადო კვალიფიკაციის მისაღებად ჩაუტარდეთ სწავლება, ინფორმაციული უსაფრთხოების შესახებ კანონის მოთხოვნების შესაბამისად.
  - შინაგან საქმეთა სამინისტროსა და შსს-ის კრიმინალური პოლიციისთვის შემუშავდეს პირველადი რეაგირების სპეციალური ტრენინგპროგრამა, რომელიც შეეხება ციფრული სამხილის ამოღება/შენახვისა და ციფრული სამხილის მთლიანობის შენარჩუნების საკითხებს.

- შემუშავდეს და ჩატარდეს კიბერტრენინგების სპეციალიზებული კურსები პროკურორებისა და მოსამართლეებისთვის.
- შემუშავდეს და ჩატარდეს სემინარების კურსი კიბერდანაშაულის განყოფილებისა და მონაცემთა გაცვლის სააგენტოს თანამშრომლებისთვის ისეთ თემებზე, როგორიცაა ღრმა ქსელში (უხილავი ინტერნეტი) ინფორმაციის მოძიება/კვლევა, ანონიმურობისა და პროაქტიური მეთოდების გამოყენება კიბერდანაშაულისა და მისი ტენდენციების განსაჭვრეტად. მოხდეს შესწავლილი მეთოდების გამოყენება:
  - მაღალი უნარების მქონე კიბერკრიმინალების ტაქტიკის უკეთ გასაგებად;
  - ქართულ კიბერსივრცეში მძიმე და ნაკლებად მძიმე კიბერდანაშაულის ტენდენციების განსასაზღვრად;
  - თანამოაზრე ქვეყნების სამართალდამცავი უწყებებისათვის ეფექტური დახმარების გასაწევად.
- რადგანაც დღეს მობილურ მოწყობილობებზე კიბერთავდასხმები მზარდ საფრთხეს წარმოადგენს, მნიშვნელოვანია ამ მიმართულებით კიბერდანაშაულის წინააღმდეგ ბრძოლის განყოფილებასთან მუშაობა.
- დასავლური პრაქტიკის გათვალისწინებით გაუმჯობესდეს კიბერდანაშაულის შესახებ სტატისტიკური აღრიცხვიანობის მეთოდები.

საქართველოსა და პარტნიორი ქვეყნებისთვის პრიორიტეტული რეკომენდაციების შემაჯამებელი ნუსხა

მიმართულებები	რეკომენდაციების დეტალები
საუკეთესო პრაქტიკის გათვალისწინება	მთავრობათა კიბერუსაფრთხოების საუკეთესო პრაქტიკაზე დაყრდნობით შემუშავდეს სპეციალური სახელმძღვანელო, თანდართული ტრენინგპროგრამებით.
მთავრობის ოფიციალური პირების ცნობიერების ამაღლება კიბერსაკითხებზე	კიბერუსაფრთხოების ძირეულ საკითხებზე შემუშავდეს მოკლე ბრიფინგები და დისკუსიები და მიეწოდოთ საქართველოს მაღალი თანამდებობის პირებს. ასევე შემუშავდეს და მიეწოდოთ მარტივი კომპიუტერული ჰიგიენის კურსები საჯარო მოხელეებს.

ლეგიტიმური კომპიუტერული პროგრამები და ტექნიკა	შემუშავდეს ეფექტური და შესრულებადი გეგმა, რომ სამთავრობო სტრუქტურების კომპიუტერული ტექნიკა აღიჭურვოს ლიცენზირებული კომპიუტერული პროგრამებით. ასევე, საჭიროებისამებრ, გამოიცვალოს კომპიუტერული ტექნიკა.
კიბერუსაფრთხოების სტრატეგია და სამოქმედო გეგმა	სტრატეგია და სამოქმედო გეგმა განახლდეს 2015 წლის ბოლოსთვის და აისახოს მკაფიო, თანმიმდევრული, კონკრეტული და შესრულებადი მიზნები.
სამართლებრივი კონსულტაციები	კიბერსაკითხებთან დაკავშირებული სამართლებრივი ბაზის გადახედვისათვის შემუშავდეს და დაინერგოს საქართველოსა და დასავლელ პარტნიორებს შორის რეგულარული საკონსულტაციო მექანიზმები. ეს ხელს შეუწყობს საკონსტიტუციო უფლებების დაცვასა და სამძებრო ღონისძიებებს შორის არსებული გარკვეული უხერხულობის მოხსნას.
სასამართლო სისტემა და პროკურატურა	შემუშავდეს და მიეწოდოთ სასწავლო ტრენინგპროგრამები მოსამართლეებსა და პროკურორებს.
კერძო საკუთრებაში არსებული კრი ტიკული ინფრასტრუქტურა	შეიქმნას და დამტკიცდეს კრიტიკული ინფორმაციული სისტემის კერძო სუბიექტების ჩამონათვალი.
კიბერუსაფრთხოების მდგომარეობის შეფასება კერძო სექტორში	შეფასდეს კიბერუსაფრთხოების მდგომარეობა და დანერგილი პრაქტიკა იმ კერძო სექტორებში, რომლებიც კრიტიკულ ინფრასტრუქტურას ფლობენ.
საზოგადოების ცნობიერების ამაღლება	საზოგადოების ცნობიერების ამაღლების მიზნით დაიგეგმოს და განხორციელდეს სპეციალური პროგრამები, რათა საზოგადოებამ უკეთ გაიგოს, თუ რა რისკების მომტანია კიბერდანაშაული მათთვის. მნიშვნელოვანია საზოგადოების ცნობიერების ამაღლება პრევენციული ზომებისა და შეტყობინების აუცილებლობის შესახებ.

შსს-ის შესაძლებლობების გაზრდა	შემუშავდეს სპეციალური ტრენინგპროგრამები და დახმარება გაეწიოთ შსს-ის წარმომადგენლებს, რომ შეისწავლონ დასავლური პრაქტიკა, ტაქტიკა, ტექნიკა და პროცედურები (TTPs). კერძოდ, გამოძიების, კომპიუტერული ექსპერტიზის, მტკიცებულებების ამოღება/მთლიანობის შენარჩუნების, ტექნიკური ანალიზის, მაღალი კვალიფიკაციის უნარების შეძენის, საქმეების („ქეისების“) ეფექტური მომზადების და ასევე სხვადასხვა ქვეყნის სტრუქტურებიდან/ორგანიზაციებიდან ინფორმაციის გამოთხოვისა და ექსტრადიციის წესების კუთხით.
პირველადი რეაგირება და პოლიცია	შინაგან საქმეთა სამინისტროსთვის შემუშავდეს პირველადი რეაგირების სპეციალური ტრენინგპროგრამა. ასევე, კრიმინალური პოლიციისთვის – ციფრული სამხილის ამოღება/შენახვისა და ციფრული სამხილის მთლიანობის შენარჩუნების საკითხებზე.

ზემოთ წარმოდგენილი ყველა ჩანაფიქრის განხორციელებისათვის მნიშვნელოვანია შემუშავდეს მკაფიო გეგმა და განისაზღვროს მიზნები. საქართველომ საერთაშორისო პარტნიორებისა და მეგობარი ქვეყნების დახმარებით არა მარტო გაზარდა თავისი კიბერშესაძლებლობები, არამედ სარგებელიც მოუტანა თანამშრომლობის პროცესს. კიბერუსაფრთხოება და კიბერდანაშაული გლობალურ პრობლემას წარმოადგენს. ამდენად, ამ გამოწვევებთან გამკლავება მოითხოვს თანამოაზრე და მეგობარი სახელმწიფოების უფრო მჭიდრო და თანმიმდევრულ საერთაშორისო თანამშრომლობას.

გამოყენებული ლიტერატურა

1. *Internet Usage Statistics, The Internet Big Picture.* Internet World Stats. ნანახია: http://www.internetworldstats.com/stats.htm and Internet World Stats. Internet Growth Statistics. ნანახია: http://www.internetworldstats.com/emarketing.htm
2. 1 ტერაბაიტი ≈ 1,000 გიგაბაიტი.
3. *Brodkin, John, Bandwidth Explodes: As Internet Use Soars, Can Bottlenecks be Averted?* ArsTechnica. May 1, 2012. ნანახია: http://arstechnica.com/business/2012/05/bandwidth-explosion-as-internet-use-soars-can-bottlenecks-be-averted/
4. *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* NATO. November 2010. ნანახია: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf
5. *McGuire, Mike & Dowling,* Samantha, Cyber Crime: A Review of the Evidence. United Kingdom, Home Office. October, 2013. ნანახია: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
6. Brenner, Susan, *Cybercrime: Criminal Threats from Cyberspace.* Santa Barbara, California: Praeger, 2010
7. Mcguire & Dowling
8. Brenner
9. იხ. Action Fraud-ის ვებგვერდი: http://www.actionfraud.police.uk/about-us/who-we-are
10. McGuire & Dowling
11. Brenner
12. *Gartner Says Worldwide Traditional PC, Tablet, Ultra mobile and Mobile Phone Shipments On Pace to Grow 7.6 Percent in 2014.* Gartner.com, January 7, 2014. ნანახია: http://www.gartner.com/newsroom/id/2645115
13. *2 Billion Consumers Worldwide to Get Smart (phones) by 2016.* EMarketer.com. ნანახია:http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694
14. *Mayer, Andre, Smartphones Becoming Prime Target for Criminal Hackers.* CBC News. March 6, 2014. ნანახია: http://www.cbc.ca/news/technology/smartphones-becoming-prime-target-for-criminal-hackers-1.2561126
15. *Retail Sales Worldwide Will Top $22 Trillion This Year.* EMarketer.com. December 23, 2014. ნანახია: http://www.emarketer.com/Article/Retail-Sales-Worldwide-Will-Top-22-Trillion-This-Year/1011765
16. *2013 Norton Report.* Symantec.com. ნანახია: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013
17. *The Economic Impact of Cybercrime and Cyber Espionage,* Center for Strategic and International Studies, July 2013. ნანახია: http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf

18. *Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II.* Center for Strategic and International Studies. June, 2014. ნანახია: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
19. ამერიკული ფისკალური წელი მიმდინარეობს 1 ოქტომბრიდან 30 სექტემბრის ჩათვლით.
20. *2014 Global Report on the Cost of Cyber Crime.* Ponemon Institute. October, 2014. ნანახია: https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf
21. იქვე.
22. *CYBERCRIME 2015 An Inside Look at the Changing Threat Landscape*. EMC. ნანახია: http://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf
23. *Internet of Things (IoT).* Whatls.com. ნანახია: http://whatis.techtarget.com/definition/Internet-of-Things
24. *Hu, Elise, What Do You Do if your Refigerrator Begins Sending Malicious E Mails?* NPR—All Tech Considered. January 16, 2014. ნანახია: http://www.npr.org/blogs/alltechconsidered/2014/01/16/263111193/refrigerator-hacked-reveals-internet-of-things-security-gaps
25. Gostev, Alexander, *Agent.btz: A Source of Inspiration?* Kaspersky Lab SecureList. March 12, 2014. ნანახია: http://www.securelist.com/en/blog/8191/Agent_btz_a_source_of_inspiration.
26. *Dutta, Soumitra, Geiger, Thierry & Lanvin, Bruno,* The Global Information Technology Report 2015. World Economic Forum. ნანახია: http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf
27. *Dutta, Soumitra et.al., The Global Information Technology Report 2013.* World Economic Forum. ნანახია: http://www3.weforum.org/docs/WEF_GITR_Report_2014.pdf
28. *ICT Facts and Figures 2015.* International Telecommunications Union. ნანახია: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
29. *2014 Annual Report.* Georgian National Telecommunications Commission. არ არის დათარიღებული. ნანახია: http://www.gncc.ge/uploads/other/1/1344.pdf
30. იქვე.
31. *GDP per Capita.* The World Bank. არ არის დათარიღებული. ნანახია: http://data.worldbank.org/indicator/NY.GDP.PCAP.CD
32. იქვე.
33. *Thornton, Laura, Public Attitudes in Georgia.* National Democratic Institute, 2015. არ არის დათარიღებული. ნანახია: https://www.ndi.org/files/NDI%20Georgia_April%202015%20Poll_Public%20Issues_ENG_VF_0.pdf.
34. *January 2015 Facebook use in Armenia, Azerbaijan and Georgia* – according to Facebook. Katy Pearce. January, 2015. ნანახია: http://www.katypearce.net/january-2015-facebook-use-in-armenia-azerbaijan-and-georgia-according-to-facebook/
35. *Georgia: Freedom on the Net 2014.* Freedom House. არ არის დათარიღებული. ნანახია: https://freedomhouse.org/report/freedom-net/2014/georgia
36. United Nations E-Government Survey 2014. არ არის დათარიღებული. ნანახია:

http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf

37. იქვე.
38. *Krabina, Bernhard, Liu, Po-Wen.* A Digital Georgia: e-Georgia strategy and action plan 2014-2018. არ არის დათარიღებული. ნანახია: http://www.dea.gov.ge/uploads/eGeorgia%20Strategy.pdf
39. United Nations E-Government Survey 2014
40. *Georgia: ICT Environment, Innovation Policies &International Cooperation.* European Commission, EU- Eastern Europe and Central Asia. არ არის დათარიღებული. ნანახია: http://eeca-ict.eu/images/uploads/pdf/EECA_counires_reports_NEW/ICT-Env_Inno-policies_and_Inter-coop_report_GEORGIA.pdf
41. საქართველოს სისხლის სამართლის კოდექსი, საქართველოს საკანონმდებლო მაცნე, 1999. ნანახია: https://matsne.gov.ge/ka/document/view/16426
42. იქვე.
43. იქვე.
44. *Literacy Rate, Adult Total.* The World Bank. არ არის დათარიღებული. ნანახია: http://data.worldbank.org/indicator/SE.ADT.LITR.ZS
45. *Georgian Organized Crime Blitz in Europe.* In Moscow's Shadows. June 20, 2013. ნანახია: http://inmoscowsshadows.wordpress.com/2013/06/20/georgian-organized-crime-blitz-in-europe/
46. *APT28: A Window into Russia's Cyber Espionage Operations?* FireEye. October 27, 2014. ნანახია: https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html
47. Akhvlediani, Zurab, *Cyber Attacks on Georgian Government Resources.* Data Exchange Agency, May 29, 2012, ნანახია: http://www.slideshare.net/DataExchangeAgency/cyber-attacks-on-georgian-governmental-resources
48. *The US-CCU Report on the Georgian Cyber Campaign.* United States Cyber-Consequences Unit, A US-CCU Special Report. August 2009. სრული ტექსტი იხ.: http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf. შემდგომ ციტირებულია, როგორც US-CCU Report.
49. იქვე.
50. Wolfers, Arnold, *National Security as an Ambiguous Symbol.* Political Science Quarterly 67(4), 1952
51. Buzan, Barry, *Rethinking Security After the Cold War.* Cooperation and Conflict (32), 1997.
52. Stavrides, James, *My Interview with Cyber Expert, Estonian President Toomas Hendrik Ilves.* The Fletcher School. October 9, 2013. ნანახია: http://sites.tufts.edu/fletcherdean/my-interview-with-cyber-expert-estonian-president-toomas-hendrik-ilves/
53. *The Compliance Gap BSA Global Software Survey.* BSA. June 2014. ნანახია: http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf
54. *European Neighboring Policy Action Plan and Eastern Partnership Bilateral and Multilateral Guidelines and their Implementations in the Areas of Trade and Related Fields*

in Georgia. European Partnership Foundation Report. January, 2014. ნანახია: http://www.epfound.ge/files/report_2013___geo.pdf.

55. *Internet live stats. Internet Users by country (2014).* ნანახია: http://www.internetlivestats.com/internet-users-by-country/
56. *Approval of Regulations.* Council for State Security and Crisis Management. January, 2014. ნანახია: http://www.government.gov.ge/files/382_39895_ 502469_ 38060114.pdf
57. 2014 წლის ანგარიში. მონაცემთა გაცვლის სააგენტო. არ არის დათარიღებული. ნანახია: http://www.dea.gov.ge/uploads/DEA_Anual_report_2014_Draft_v1_2.pdf
58. *Enhanced cyber Defence cooperation in the South Caucasus and Black Sea region.* NATO. July 29, 2015. ნანახია: http://www.nato.int/cps/en/natohq/news_121969.htm?selectedLocale=en
59. *Eastern Partnership -Cooperation Against Cybercrime.* Ministry of Internal Affairs. ნანახია: http://police.ge/en/ministry/structure-and-offices/international-relations-department/donor-coordination/proeqtebis-shesakheb/ongoing-projects/eastern-partnership-cooperation-against-cybercrime
60. საქართველოს სახელმწიფო უსაფრთხოების სამსახურის დებულების დამტკიცების შესახებ, საქართველოს საკანონმდებლო მაცნე, 30 ივლისი, 2015. ნანახია: https://matsne.gov.ge/ka/document/view/2930985
61. ინფორმაციული უსაფრთხოების შესახებ კანონის შესწორება, საქართველოს საკანონმდებლო მაცნე, 24 დეკემბერი, 2013 ნანახია: https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2162943
62. საქართველოს მთავრობის #567 დადგენილება თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ, საქართველოს საკანონმდებლო მაცნე, 29 სექტემბერი, 2014. ნანახია: https://matsne.gov.ge/ka/document/view/2521602
63. *Georgian Law on Personal Data Protection.* Legislative Herald of Georgia. Consolidated version. July 8, 2015. ნანახია: https://matsne.gov.ge/en/document/view/1561437.
64. საქართველოს ეროვნული უსაფრთხოების კონცეფცია, საქართველოს მთავრობა, არ არის დათარიღებული. ნანახია: http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx
65. *Cyber Security Strategy.* Legislative Herald of Georgia. May 17, 2013. ნანახია: https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1923932&lang=ge
66. *Convention on Cybercrime.* Council of Europe, Treaty Office. არ არის დათარიღებული. ნანახია: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG
67. *Law of Georgia on Information Security.* Legislative Herald of Georgia. ნანახია: https://matsne.gov.ge/en/document/view/1679424
68. საქართველოს მთავრობის #312 დადგენილება კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ, 24 აპრილი, 2014. ნანახია: https://matsne.gov.ge/ka/document/view/2333175
69. საქართველოს სისხლის სამართლის კოდექსი. საქართველოს საკანონმდებლო

მაცნე, 1999. ნანახია: http://tcc.gov.ge/uploads/kanonebi/sisxlis_samartlis_kodeqsi.pdf

70. *National Strategy for Combating Organized Crime 2013-2014.* Police.ge. არ არის დათარიღებული. ნანახია: http://police.ge/files/OCC/Organized%20Crime%20Strategy-ENG.pdf.
71. *Amendments to the Law on Criminal Procedure Code.* Legislative Herald of Georgia. November 30, 2014. ნანახია: https://matsne.gov.ge/ka/document/view/2593029#DOCUMENT:1.
72. *საქართველოს მთავრობის კომენტარები არასამთავრობო ორგანიზაციათა კოალიციის ანგარიშზე,* საქართველოს მთავრობის ადმინისტრაცია, არ არის დათარიღებული. ნანახია: http://gov.ge/files/323_49254_692246_NGOs2YearProgressReport-CommentsAOG20.05.2015.pdf
73. *Nine threats to your personal life stemming from the new legislation on secret wiretapping, Transparency International.* December 23, 2014. ნანახია: http://www.transparency.ge/en/blog/nine-threats-your-personal-life-stemming-new-legislation-ons-secret-wiretapping
74. იქვე.
75. *საქართველოს სისხლის სამართლის საპროცესო კოდექსი,* საქართველოს საკანონმდებლო მაცნე, 29 სექტემბერი, 2015. ნანახია: https://matsne.gov.ge/ka/document/view/90034
76. *საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ,* საქართველოს კომუნიკაციების ეროვნული კომისია, 19 მაისი, 2011. ნანახია: http://www.gncc.ge/ge/legal-acts/parliament/laws/saqartvelos-kanoni-eleqtronuli-komunikaciebis-shesaxeb-8082.page
77. *„ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონში ცვლილების შეტანის* თაობაზე, საქართველოს საკანონმდებლო მაცნე, 31 ოქტომბერი, 2014. ნანახია: https://matsne.gov.ge/ka/document/view/2457343
78. იქვე.
79. თარხნიშვილი ნინო, *ორი „გასაღები“ ისევ სადავოა,* რადიო თავისუფლება, 31 მარტი, 2015. ნანახია: http://www.radiotavisupleba.ge/content/ori-gasagebi-is-ev-sadavoa/26929588.html
80. *საქართველოს სისხლის სამართლის კოდექსი.* საქართველოს საკანონმდებლო მაცნე.