გორის სახელმწიფო სასწავლო უნივერსიტეტი

სოციალურ მეცნიერებათა, ბიზნესის და სამართალმცოდნეობის ფაკულტეტი

კიბერდანაშაული, კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში

სამაგისტრო ნაშრომი შესრულებულია სოციალურ მეცნიერებათა ბიზნესისა და სამართალმცოდნეობის ფაკულტეტზე სამართლის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად.

ხელმძღვანელი: **მალხაზ ლომსაძე**

სამართლის დოქტორი, ასოცირებული პროფესორი

სტუდენტი: **თამარ ჩოჩიშვილი**

გორი, საქართველო

2019 წელი

რეზიუმე

XXI საუკუნეში ადამიანთა შორის კომუნიკაცია ძირითადად ინტერნეტ სივრცის მეშვეობით ხორციელდება, შესაბამისად საზოგადოება იმდენად დამოკიდებული გახდა კომუნიკაციის ამდაგვარ საშუალებებზე, რომ მათ გარეშე ვერც კი წარმოუდგენიათ ცხოვრება. საზოგადოების ამგვარმა დამოკიდებულებამ განაპირობა ისეთი დანაშულებრივი ქმედებების მომრავლება როგორიცაა კიბერ დანაშაული/კიბერტერორიზმი, სწორედ ამიტომაც გადავწყვიტე წინამდებარე ნაშრომის შექმნა და იმ მნიშვნელოვანი საკითხების განხილვა, რაც დღევანდელი მსოფლიოს გლობალურ პრობლემად იქცა.

ნაშრომი შედგება სამი ნაწილისგან - შესავალი, ძირითადი ნაწილი და დასკვნა, იგი მოიცავს სამ თავს, რომელშიც კიბერდანაშაულის/კიბერტერორიზმის ცნების საბაზისო საკითხებთან ერთად განხილულია საერთაშრისო თანამშრომლობის მნიშვნელობა, ამ კუთხით არსებული პოლიტიკური მიმართულებები, შექმნილი საკანონმდებლო რეგულაციები და მის საფუძველზე არსებული პრობლემები, ასევე საქართველოს მიდგომები და სტრატეგიები კიბერდანაშაულთან / კიბერტერორიზმთან ბრძოლის წინააღმდეგ და დეფინიციები.

ნაშრომის მიზანია, კიბერდანაშაულის და მასთან დაკავშირებული საკითხების სამართლებრივ ჭრილში განხილვა და ანალიზი.

Abstract

In the XXI century communication between people is mainly exercises via Internet, accordingly society became so dependent on these means of communication, that it cannot imagine life without them. This kind of attitude of society has led to an increase in criminal acts, such as cybercrime and cyberterrorism is why I decided to create this research and discuss those important issues that became a global problem of present-day world.

The research consists of three parts - the introduction, the main part and the conclusion, it contain three chapters and where the importance of international cooperation, political trends existing in this area, created legislative regulations and problems existing on its basis, approaches and strategies of Georgia in the fight against cybercrime / cyberterrorism and definitions of how the financing of terrorism is executed by such means of criminal acts, as cybercrime is discussed alongside the basic issues of concept of cybercrime / cyberterrorism.

The purpose of this research is to review terrorism as a global problem and related issues in legal context and analyze.

ნაშრომში გამოყენებული შემოკლებანი

ა. შ. - ასე შემდეგ

ე.წ. - ეგრეთ წოდებული

იხ. - იხილეთ

გვ. - გვერდი

ე.ი. - ესე იგი

სხვ. - სხვა

აშშ - ამერიკის შეერთებული შტატები

ჟურნ.- ჟურნალი

გამომც. - გამომცემლობა

ეგმ . - ელექტრო გამომთვლელი მანქანა

შსს - შინაგან საქმეთა სამინისტრო

გაერო - გაერთიენებული ერების ორგანიზაცია

ეუთო - ევროპის უშიშროებისა და თანამშრომლობის ორგანიზაცია

თბ. - თბილისი

სარჩევი

შესავალი

ძველად, ადამიანები კომუნიკაციისათვის სხვადასხვა საშუალებებს იყენებდნენ, როგორებიცაა ზეპირი გადაცემა, წერილობითი სახის ინფორმაციის მიმოცვლა, ფოსტა, სატელეფონო კავშირი, ტელეგრაფი და ა.შ. ინტერნეტის შექმნამ კი საგრძნობლად გაამარტივა კომუნიკაცია, კერძოდ, ადამიანს მიეცა საშუალება დროის უმოკლეს მონაკვეთში მიიღოს ან/და გაცვალოს სხვადასხვა სახის ინფორმაცია მეგობრებთან, ოჯახის წევრებთან, ბიზნეს პარტნიორებთან - დაამყაროს კომუნიკაცია მისთვის მოსახერხებელი ფორმით, სასურველ დროს და მსოფლიოს ნებისმიერ წერტილში. სწორედ აღნიშნული სიმარტივის გამო, საზოგადოების უმეტესი ნაწილი კომუნიკაციის ამდაგვარ/ახალ საშუალებებზე იმდენად დამოკიდებული გახდა, რომ მის გარეშე კომუნიკაციის წარმოდგენაც კი უჭირთ. ასევე მსოფლიოში არსებული თითქმის ყველა თანამედროვე მსხვილი თუ წვრილი ორგანიზაცია (კორპორაცია, კომპანია, საწარმო, ფირმადა ა.შ) მისი საქმიანობის რეალიზაციას, სწორედ ინტერნეტ კომუნიკაციის და საერთაშორისო ქსელების მეშვეობით ახორციელებს. შესაბამისად, ბუნებრივია, რომ მათი საქმიანობის შესახებ თუ სხვა მნიშვნელოვანი ინფორმაცია მათ მიერვე შექმნილი ან/და შესყიდული პროგრამების საშუალებით ელექტრონულ სისტემებში ინახება, რომლის დაცულობა სასიცოცხლოდ მნიშვნელოვანია მათთვის.

XXI საუკუნეში, ტექნოლოგიური განვითარების შედეგად, ყველაფერი დამოკიდებულია კომპიუტერულ სისტემებზე. ნებისმიერ სფეროში გამოიყენებენ, ნიშვნელოვან ინფორმაციებს ინახავენ კიბერსივრცეში. აღნიშნულიდან გამომდინარე გაიზარდა რისკები ვირტუალურ სივრცეში უკანონოდ შეღწევასთან დაკავშირებით. კიბერდამნაშავეები სხვადასხვა პროგრამების გამოყენებით მოიპოვებენ ისეთ მნიშვნელოვან ინფორმაციებს, როგორიცაა მაგალითად ონლაინ საკრედიტო ბარათების პაროლები [1] ,

[1] პაროლი - იგივე კოდური სიტყვა, ფრაზა.

სხვადასხვა სახის სოციალური ქსელების პაროლები, ონლაინ მიმოწერის დეტალებიდა ა. შ.

მნიშვნელოვანია, რომ მრავალი ქვეყნის და ორგანიზაციის მუშაობაში, როგორც უკვე ავღნიშნე, განსაკუთრებული ადგილი უკავია კომპიუტერული სისტემებისა და ინტერნეტის გამოყენებას, შესაბამისად მათი მუშაობის შეფერხება ან რაიმე სახის დაზიანება, სერიოზულ უარყოფით გავლენას მოახდენს მათი საქმიანობის პროცესზე, რასაც აღნიშნული ორგანიზაცია, კომპანია თუ სახელმწიფო სტრუქტურა ახორციელებს. უამრავი შემთხვევაა, როდესაც კომპიუტერული სისტემების დაზიანებამ, სერიოზული ეკონომიკური ზიანი და ზოგჯერ მუშაობის სრული შეფერხება გამოიწვია, რომლითაც გარკვეული სარგებელი მიიღეს გარეშე პირებმა -კონკურენტმა ორგანიზაციებმა, გარკვეულმა დაჯგუფებემა და ა.შ.

სამაგისტრო ნაშრომის მიზანი:

წარმოდგენილ ნაშრომში განვიხილავ კომპიუტერული დანაშაულის სამართლებრივი მოწესრიგების პრობლემას საქართველოში და მოქმედი კანონმდებლობის შესაბამისობას ,,კიბერდანაშაულის შესახებ“ ევროპის საბჭოს კონვენციასთან. ასევე ნაშრომის კვლევის მიზანია კიბერდანაშაულის სისხლისსამართლებრივი მოწესრიგების პრობლემების წარმოჩენა და მათი სრულყოფის გზების დასახვა.

თემის აქტუალობა. უწინ მსოფლიო ფილმებში ვხედავდით ჰაკერებს და ისინი ზღაპრის გმირები გვეგონა. დღეს ტერმინი ,,კიბერდანაშაული“ აღარავის უკვირს. საზოგადოებისათვის რთულია გაარკვიოს ვინ არის უბრალო თაღლითი, რომელიც კომპიუტერული ტექნიკის საშუალებით 100 დოლარიანებს ბეჭდავს და ვინ გენიოსი, რომელსაც შეუძლია ნებისმიერი კომპიუტერული დაცვითი სისტემის გადალახვა. მათ ყველას ,,ჰაკერებს“ უწოდებენ. ჩნდება კითხვა, რა შეიცვალა XX საუკუნის 70-იანი წლებიდან ანუ კომპიუტერული დანაშაულის ჩასახვის დღიდან ,,კიბერდანაშაულის შესახებ“ ევროსაბჭოს 2001 წლის 23 ნოემბრის კონვენციის მიღებამდე? პასუხი მარტივია - შეიცვალა კომპიუტერული დანაშაულის შინაარსი, გაფართოვდა მისი

საზღვრები და გაიზარდა საფრთხე, უფრო მრავალფეროვანი გახდა მისი ჩადენის ხერხი.

კომპიუტერული დანაშაულის საკითხის შესწავლის დაწყებამდე ვცადე გამერკვია, რამდენად აქტუალური შეიძლება იყოს ეს პრობლემა საქართველოსთვის. დღეს განვითარებად ქვეყნებში აქტიურად მიმდინარეობს სახელმწიფო და კერძო სექტორის კომპიუტერებით და ინტერნეტით უზრუნველყოფა. უკანასკნელ წლებში აღნიშნულ პროცესში საქართველოც აქტიურად ჩაება. ეს კი ჰაკერებისთვის ქმნის ნოყიერ ნიადაგს კრიმინალური საქმიანობის დაწყებისთვის. აღნიშნულს ხელს უწყობს და ასეთ სახელმწიფოებში უსაფრთხოების ერთიანი სისტემის არარსებობა, მაღალი ტექნოლოგიების სფეროში სამართალდამცავი ორგანოების ნაკლები კომპეტენტურობა და ზოგადად, კიბერდანაშაულის ლატენტურობის მაღალი ხარისხი. ეს უკანასკნელი სერიოზულ პრობლემას წარმოადგენს განვითარებული ქვეყნების სამართალდამცავი ორგანოებისათვისაც. საქართველოს მასშტაბით საკითხის აქტუალობის დასაბუთების მიზნით მივმართე შსს-ს ადმინისტრაციას და გამოვითხოვე გამოძიების ოფიციალური სტატისტიკა.[2] გაირკვა, რომ, 2006 წლიდან 2014 წლის ჩათვლით სულ 551 დანაშაულია რეგისტრირებული, აქედან გახსნილია 150 საქმე, ხოლო 2015 წლიდან - 2018 წლამდე დარეგისტრირებულია 2311 დანაშაული აქედან გახსნილია 481 საქმე. გამოდის, რომ კომპიუტერული დანაშაულის პრობლემა საქართველოში პრაქტიკულად არ არსებობს ან თუ არსებობს, ძალიან უმნიშვნელო პრობლემებს ქმნის.

თუმცა მე ვთვლი, რომ საკითხის აქტუალობა ნაკლებადაა დამოკიდებული ოფიციალური სტატისტიკის შედეგზე, ვინაიდან კომპიუტერული დანაშაულის მაღალი ლატენტური ხასიათი არ იძლევა სრულ შესაძლებლობას მისი გამოვლენისა და გამოძიებისთვის.

კვლევის მეთოდი: ნაშრომში გამოყენებულია, საქართველოს სისხლის სამართლის კოდექსი მუხლების შედარებით - სამართლებრივი ანალიზი

[2] იხ. შსს წერილი NMIA9 19 00715722 20.03.2019 წ.

ევროპის საბჭოს კონვენციის და ზოგიერთი საზღვარგარეთის ქვეყნების კანონმდებლობასთან მიმართებით. გარდა ამისა, გამოყენებულია, ისტორიული, ანალიტიკური, კონკრეტულ - სოციოლოგიური, დოგმატური და სხვა მეთოდები. ასევე, გამოყენებულია სამართლებრივი სტატისკიტის მონაცემები სასამართლო შესწავლისა და განზოგადების გზით.

კვლევის თეორიული საკითხები: კვლევისას გამოყენებულია კომპიუტერული დანაშაულის შესახებ შექმნილი საერთაშორისო სახელმძღვანელოები, მონოგრაფიები, სტატიები. ნაშრომი ეყრდნობა ს. ცარნის, კ. ალექსანდერის, კ. შულმანის, ნ. კარჩევსკის, მ. გერკეს, პ. ვერდელიოს, ე. მევიოლდის, თ. წერეთლის, ალ. კაცმანის, გ. მამულაშვილის, მ. ლეკვეიშვილის, მ. ცაცანაშვილის, გ. ნაჭყებიას და სხვათა ნაშრომებს და მოსაზრებებს.

ნაშრომის სტრუქტურა: ნაშრომი შედგება შესავლის და სამი თავისგან. I თავი განსაზღვრავს კიბერდანაშაულის ცნებას, სამართლებრივ ისტორიას და საინფორმაციო ტექნოლოგიების არსს. II თავში მიმოვიხილავ კიბერბულინგს, კიბერბულინგის კატეგორიებს, კიბერბულინგს საქართველოში და კიბერთაღლითობას. III თავში მიმოვიხილავ კიბერტერორიზმს, როგორც კიბერდანაშაულის ერთ-ერთ სახეს, ევროპის ქვეყნების გამოცდილებას კიბერტერორიზმის შესახებ, კიბერდანაშაულთან ბრძოლის სისხლისსამართლებრივ ღონისძიებათა საერთაშორისო და ეროვნულ კანონმდებლობას.

I თავი

კიბერდანაშაულის ცნება და სამართლებრივი კვლევის ისტორია

რატომ არის კომპიუტერული დანაშაული ძალიან მნიშვნელოვანი? პირველ რიგში იმიტომ, რომ როგორც ისტორია გვასწავლის კრიმინალები ხშირად ბოროტად იყენებენ ახალ ტექნოლოგიებს სარგებლის მისაღებად ან სხვებისთვის ზიანის მისაყენებლად. ავტომობილი ამის შესანიშნავი მაგალითია. ავტომობილი შეიქმნა კანონმორჩილი ადამიანების ტრანსპორტირებისათვის, მაგრამ მალე ის გადაიქცა ხვადასხვა დანაშაულის

საგნად (მაგ. მანქანის ქურდობა, მანქანის გაქურდვა), საშუალებად (მაგ. ბანკის ძარცვისას კართან მდგარი მანქანა) და იარაღად (მაგ. ავტოსაგზაო შემთხვევა, როდესაც დამნაშავე მიიმალება). კომპიუტერის შემთვევაშიც აშკარად იგივე მეორდება[3].

კომპიუტერული დანაშაული ყურადღების ცენტრში პირველად აშშ-ში XX საუკუნის 70 - იან წლებში მოექცა. ნაციონალურ და საერთაშორისო დონეზე დაიწყო ამ ფენომენის გამოკვლევა. მიღებულ იქნა სპეციალური ნორმები კიბერდანაშაულის მოსაწესრიგებლად. აშშ-ში ჯერ კიდევ 1977 წელს შეიმუშავეს კანონპროექტი ,,ფედერალური კომპიუტერული სისტემების დაცვის შესახებ“, რომელიც ითვალისწინებდა სისხლისსამართლებრივ პასუხისმგებლობას ისეთი ქმედებისთვის, როგორიცაა კომპიუტერულ სისტემაში ცრუ მონაცემების შეყვანა, კომპიუტერული მოწყობილობის უკანონო გამოყენება, ფულადი სახსრების მითვისება კომპიუტერული ტექნოლოგიების და კომპიუტერული ინფორმაციის მეშვეობით და სხვა. ამ კანონპროექტის საფუძველზე 1984 წლის ოქტომბერში მიღებულ იქნა ,,კომპიუტერული თაღლითობის და კომპიუტერის ბოროტად გამოყენების შესახებ“ კანონი. კომპიუტერული დანაშაულის წინააღმდეგ აქტიური ბრძოლის დასაწყებად კი აშშ-ში ექსპერტები გამოყოფენ სამ შემთხვევას, რომლებმაც ცხადი გახადა, რომ ახალი კომპიუტერული და სატელეკომუნიკაციო ტექნოლოგიები დიდ პრობლემებს შეუქმნიდა სამართალდამცავ ორგანოებს. საყოველთაო კომპიუტინგი (კომპიუტერების მაშტაბური ინტეგრაცია ყოველდღიურ ცხოვრებაში) მარტო ცხოვრების წესის შეცვლას კი არ ნიშნავდა, არამედ შეიცვლებოდა კრიმინალების მიერ დანაშაულებრივი საქმიანობის წარმართვის სპეციფიკაც. მაგალითისთვის მოვიყვან სამივე **შემთხვევას:**

1. 1986 წელს კალიფორნიის უნივერსიტეტის ასტრონომს დაევალა არასასიამოვნო, მაგრამ აშკარად მცირე მნიშვნელობის პრობლემის გადაჭრა უნივერსიტეტის კომპიუტერულ ლაბორატორიაში. უნივერსიტეტი ამუშავებდა ორ საბუღალტრო პროგრამას, რომელიც აღრიცხავდა კომპიუტერების

[3] იხ.scott charney, kent alekander, types of computer crime, 25.11.2005 http://www.crime-research.org/articles/types-of-computer-crime/2

გამოყენებას და არეგისტრირებდა მათ მომხმარებლებს. ვინიდან ამ პროგრამით ხდებოდა თანხებთან დაკავშირებით ერთი და იგივე ინფორმაციის დაფიქსირება, მათი შედეგიც ერთნაირი უნდა ყოფილიყო. თუმცა გაურკვევლი მიზეზით სხვაობამ 75 აშშ დოლარი შეადგინა.

გამოძიების ფედერალურმა ორგანოებმა უარი განაცხადეს საქმის გამოძიებაზე იმ მოტივით, რომ 75 დოლარიანი დანაკარგი უმნიშვნელო იყო, მაგრამ ასტრონომმა კლიფორდ სტოლმა თავად დაიწყო გამოძიება. ის წერდა ჰაკერის მოქმედებებს და მუშაობდა როგორც ადგილობრივ ასევე უცხოურ სატელეფონო კომპანიებთან, რათა დაედგინა თავდასხმის წყარო. აღმოჩნდა, რომ გერმანელ ჰაკერ მარკუს ჰესს აფინანსებდა რუსეთის სახელმწიფო უსაფრთხოების კომიტეტი, რათა გაემჟღავნებინა აშშ-ს სამხედრო საიდუმლოება. ამრიგად, ეს იყო მნიშვნელოვანი გაკვეთილი როგორც სამართალდამცავი ორგანოების, ასევე დაზვერვის სამსახურისთვის.

პირველ რიგში, ცხადი გახდა, რომ ქსელური ინფორმაცია არ იყო დაცული მასში უნებართვო შეღწევისაგან და მეორე - ფინანსური ზარალი ყოველთვის არ განსაზღვრავს ხელყოფის სერიოზულობას და ინფორმაცია კიბერდანაშაულის შესახებ არ უნდა შემოწმდეს მხოლოდ ფინანსური ზარალის მიხედვით.

2. მეორე შემთხვევა დაკავშირებული იყო კომპიუტერულ ვირუსთან ე.წ. მორისის მატლთან (Morris worm). 1988 წელს ქორნელის უნივერსიტეტის სტუდენტმა რობერტ მორისმა შექმნა პროგრამა ინტერნეტის მეშვეობით კომპიუტერში შესაღწევად. მას შემდეგ რაც კომპიუტერული ვირუსი შეაღწევდა სამიზნე კომპიუტერში იგი დაიკავებდა კომპიუტერის მეხსიერებას, რაც გამოიწვევდა კომპიუტერის გამორთვას. სანამ კომპიუტერული ვირუსი გაუვნებელყოფილი იქნა, მან დააზიანა დაახოებით 62 00 კომპიუტერი და გამოიწვია 98 მილიონ დოლარზე მეტი ზარალი.

3. მესამე მაგალითი ეხება 1989 წლის თავდასხმას კომპანია ,,ბელსაუსზე“, რომელიც განხორციელდა სიკვდილის ლეგიონის სახელით ცნობილ ჰაკერთა

ჯგუფის მიერ. მათთვის შესაძლებელი გახდა ადგილობრივ სატელეფონო სისტემაში ცვლილებების შეტანა და მონაცემების განადგურება.[4]

მიუხედავად იმისა, რომ ამერიკელი გამომძიებლები განხილულ დანაშაულს წარმატებით გაუმკლავდნენ, აუცილებელი გახდა კომპიუტერული დანაშაულის შესახებ საკანონმდებლო ინიციატივის მომზადება, რომელსაც მხარი დაუჭირა ამერიკის გენერალური პროკურორის ეკონომიკური დანაშაულის საბჭომ. უკვე 1991 წლის სექტემბერში კი იუსტიციის დეპარტამენტის გენერალურ სასარჩელო განყოფილებაში შეიქმნა კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლის განყოფილება.

ჩემი აზრით, ზემოთმოყვანილი აზრით, ზემოთმოყვანილი მაგალითი არის სახელმძღვანელო შემთვევა მსოფლიოს სხვადასხვა სახელმწიფოსთვის კიბერდანაშაულის წინააღმდეგ ბრძოლაში და ასევე, ცალსახად მიმაჩნია, რომ საქართველომ ამ საკითხებში ყოველთვის განსაკუთრებული ყურადღება უნდა მიაქციოს უცხოურ გამოცდილებას.

დიდი ბრიტანეთი მრავალი წლის მანძილზე უშედეგოდ ცდილობდა კომპიუტერული დანაშაულის წინაღმდეგ გამოეყენებინა სასამართლო წარმოებაში მიღებული მრავალსაუკონოვანი გამოცდილება, თუმცა უშედეგოდ. 1990 წლის აგვისტოში ძალაში შევიდა კანონი ,,კომპიუტერული ტექნოლოგიის არასანქცირებული გამოყენების შესახებ“, რომლითაც დასჯადად გამოცხადდა კომპიუტერში ან მასში დაცულ ინფორმაციაში ან/და პროგრამაში წინასწარ განზრახული უკანონო შეღწევა, ასევე ამ ინფორმაციის ბლოკირება, მოდიფიცირება, განადრურება ან კოპირება[5].

[4] იხ.scott charney, kent alekander, types of computer crime, 25.11.2005 http://www.crime-research.org/articles/types-of-computer-crime/2 (სამივე კაზუსი განხილულია მოცემულისტატიის საფუძველზე)

[5] საქართველოს სისხლის სამართლის კოდექსი მასში შეტანილ ცვლილებამდე შიცავდა მსგავსი შინაარსის დანაშაულებრივ ქმედებას, კერძოდ სისხლის სამართლის კოდექსის ძველი რედაქციის 284-ე მუხლის მიხედვით დასჯადი იყო: ,,კანონით დაცულ კომპიუტერულ ინფორმაციასთან, ე.ი მანქანა მატარებელზე, ელექტრო გამომთვლელ მანქანაზე (ეგმ-ზე) ეგმ-ის სისტემაში ან მათ ქსელში ასახულ ინფორმაციასთან არამართლზომიერი შეღწევა, რამაც ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან მოპოვება ან /და ეგმ-ის სისტემის ან მათი ქსელის მოშლა გამოიწვია, ასევე მობილური მოწყობილობის საერთაშორისო იდენტიფიკატორის შეცვლა.

გერმანიაში კომპიუტერული ინფორმაციის სფეროში ჩადენილ დანაშაულებზე სისხლისამართლებრივი პასუხისმგებლობის საკითხი 1986 წლიდან დადგა. 1987 წლის აგვისტოდან განხორციელდა შესაბამისი ცვლილებები გერმანიის სისხლის სამართლის კოდექსში, რითიც დადგინდა პასუხისმგებლობა კომპიუტერული დანაშაულისთვის. 1993 წელს მსგავსი ცვლილებები განიცადა **პოლანდიის** სისხლის სამართლის კოდექსმა და დანაშაულად გამოაცხადა კომპიუტერში არასანქცირებული შეღწევა, კომპიუტერული საბოტაჟი, ვირუსების გავრცელება და სხვ.

ბოლო წლებში კომპიუტერული დანაშაული აღიარებულია საერთაშორისო ხასიათის დანაშაულად და მის წინააღმდეგ ბრძოლა წარმოადგენს მრავალი საერთაშორისო ორგანიზაციისთვის პრიორიტეტულ მიმართულებას.

გაერო-ს მიერ მიღებული იქნა ,,ინფორმაციული ტენოლოგიების გამოყენებით ჩადენილი დანაშაულის წინააღმდეგ ბრძოლის შესხებ“ რეზოლუციები, რომლებშიც ხაზგასმულია ყველა წევრი სახელმწიფოს მხრიდან საკუთარი საკანონმდებლო ბაზის გადახედვის და მისი სრულყოფის აუცილებლობა.

ეკონომიკური განვითერებისა და თანამშროლობის ორგანიზაცია 1983 წლიდან სწავლობს და ამზადებს შესაბამის რეკომენდაციებს, რათა საერთაშორისო დონეზე მსგავს დანაშაულებრივ შემთხვევებზე განხორციელდეს ანალოგიური სისხლისსამართლებრივი პასუხისმგებლობის დაკისრება.

დიდი რვიანის ქვეყნებს შექმნილი აქვთ საკონტროლო პუნქტების მუდმივმოქმედი ქსელი, რომელსაც კომპიუტერულ დანაშაულთან დაკავშირებით წამოჭრილი პრობლემების გამო შეუძლია მიმართონ საერთაშორისო თანამშრომლობის პროცესის მონაწილე ყველა წევრმა. მნიშვნელოვან დოკუმენტს წარმოადგენს **ეუთო-ს** მიერ მიღებული გადაწყვეტილება: ორგანიზაცია წევრ-სახელმწიფოებს აძლევს რეკომენდაციას შეუერთდნენ ევროსაბჭოს მიღებულ კონვენციას ,,კიბერდანაშაულის შესახებ“ და ,,დიდი რვიანის“ ქვეყნების მიერ მუდმივმოქმედ ქსელს, რომლის მიზანია

კვირაში შვიდი დღე ოცდაოთხი საათი მოკავშირე სახელმწიფოებისთვის ინფორმაციის მიწოდება და კომპეტენციის ფარგლებში სათანადო დახმარების [6] აღმოჩენა.

საერთაშორისო აქტებიდან საქართველოსთვის ყველაზე მნიშვნელოვან დოკუმენტს წარმოადგენს **ევროსაბჭოს კონვენცია** ,,კიბერდანაშაულის შესახებ", რომელიც მიღებულ იქნა 2001 წლის 23 ნოემბერს ქ. ბუდაპეშტში[7] ევროსაბჭოს 41 წევრი სახელმწიფოს მიერ. აღნიშნული დოკუმენტი წარმოადგენს მსოფლიოს მასშტაბით ერთ-ერთ პირველ სერიოზულ მცდელობას კიბერდანაშაულის წინააღმდეგ ბრძოლაში: ნაციონალური უსაფრთხოების დასაცავად, ერთიანი სტრატეგიის ჩამოყალიბებისათვის და ურთიერთთანამშრომლობისთვის. მას, გარდა ევროპული ქვეყნებისა, ხელი მოაწერეს კანადამ, იაპონიამ, სამხრეთ აფრიკამ, [8] აშშ-მ. საინტერესოა, რომ 2008 წლის აპრილში რუსეთის ფედერაციამ უარი თქვა კონვენციის ხელმოწერაზე, ხოლო ამავე წლის ივლისში კონვენციას ხელი მოაწერა აზებაიჯანმა [9] . კონვეცია განსაზღვრავს ექსტრადიციის და ორმხრივი დახმარების პრინციპებს. ევროსაბჭოს წევრ ქვეყნებიდან კონვენციის რატიფიცირება და შესაბამისად კონვენციაში მოცემული ქმედებების კრიმინალიზაცია და სხვა პრინციპების მოქმედება ეროვნული კანონმდებლობის დონეზე განხორციელდა მას შემდეგ სახელმწიფოებში ალბანეთი, სომხეთი, ბოსნია, ბულგარეთი, ხორვატია, კვიპროსი, დანია, ესტონეთი, ფინეთი, საფრანგეთი, გერმანია, უნგრეთი, ისლანდია, იტალია,

[6] აღნიშნული ვალდებულება სახელმწიფოებს ,,კიბერდანაშაულის შესახებ" ევროსაბჭოს კონვენციის რატიფიცირების შემთხვევაში ისედაც უჩნდებათ, ხოლო ევროკავშირის საბჭოს N2005/222 ჩარჩო გადაწყვეტილების თანახმად მუდმივი ქსელის შექმნის ვალდებულება ევროკავშირის ყველა წევრ - ქვეყანას გააჩნია.

[7] ევროსაბჭოს კონვენცია საქართველოსთვის მნიშვნელოვანი გახდა მას შემდეგ, რაც 2009 წლის 1 ივნისიდან 2010 წლის 31 მაისამდე, ევროსაბჭოს ორგანიზებით საქართველოში განხორციელდა ,,კიბერდანაშაულის პროექტი საქართველოში", რომლის ფარგლებშიც ევროსაბჭოს კონვენციის მოთხოვნების შესაბამისად მომზადდა საკანონმდებლო ცვილებების პროექტი. იგი მოგვიანებით სრულად იქნა ასახული საქართველოს სისხლის სამართლის კოდექსში და სისხლის სამართლის საპროცესო კოდექსში.

[8] იხ. http://en.wikipedia.org/wiki/convention_on_cybercrime

[9] იხ. http://www.today.az./news/society/46054.html

ლიტვა, ლატვია, მოლდოვა, ნიდერლანდები, ნორვეგია, რუმინეთი, სერბეთი, სლოვაკეთი, სლოვენია, მაკედონია, უკრაინა[10].

დღეის მდგომარეობით კონვენცია ,,კიბერდანაშაულის შესახებ“ წარმოადგენს ერთ-ერთ უმთავრეს დოკუმენტს და გარანტიას მსოფლიოს სახელმწიფოთა ნაციონალური უსაფრთხოების დასაცავად ურთიერთ თანამშრომლობისთვის კომპიუტერული დანაშაულის წინააღმდეგ ბროლაში, საკანონმდებლო ბაზის დახვეწისა და ყველა სახელმწიფოს წინაშე დასმული ყველაზე სწრაფად განვითარებადი გამოწვევა - კომპიუტერული დანაშაულის მავნე შედეგის შემცირებისათვის.

1.1 საინფორმაციო ტექნოლოგიები და დანაშაული

მეორე მსოფლიო ომის შემდეგ, მსოფლიოში დაიწყო მძლავრი საზოგადოებრივი მოძრაობა ადამიანების თანასწორუფლებიანობის, ზოგადსაკაცობრიო იდეალების, ადამიანის ძირითადი უფლებებისა და თავისუფლების, აგრეთვე ყოველი ადამიანის უზრუნველყოფილი ცხოვრების დასამკვიდრებლად. მაშინვე აღინიშნა, რომ ეს პროცესი მოითხოვს დაუშრეტელი პოლიტიკური ნების გამოვლენასა და შესაბამისი საკანონმდებლო ბაზის ფორმირებას, რამაც თავისუფლების გარდა, უნდა მისცეს ადამიანს თავისი ფიზიკური და ინტელექტუალური პოტენციალის სრულად გამოვლენის საშუალება. მაგრამ ძალზე მოკლე ხანში გაირკვა, რომ მხოლოდ პოლიტიკურ ნებასა და საკანონმდებლო ბაზას არ მოაქვს სასურველი შედეგი, აუცილებელია მესამე კომპონენტი - საინფორმაციო ინფრასტრუქტურა, რომელიც უზრუნველყოფს ადამიანთა გათვითცნობიერებას მიმდინარე პროცესებში, მათ ინფორმირებას ხელისუფლების ქმედებათა შესახებ და საზოგადოებრივი დოვლათის შექმნა - განაწილების გამჭვირვალობას[11]. აქედან გამომდინარე, დაიწყო პრესის, რადიოსა და ტელევიზიის, კავშირგაბმულობისა და მონაცემთა ბაზების განვითარების ყოველმხრივი ხელშეწყობა. მაგრამ არც

[10] იხ. http://conventions.coe.int/treaty/commun/cherchesig.asp?NT=185&CM=&DF=CL=ENG
[11] იხ. http://www.nplg.gov.ge

ამან უზრუნველყო სრულყოფილი დემოკრატიის ჩამოყალიბება და ყოველი ადამიანის უზრუნველყოფილი ცხოვრება.

მიუხედავად იმისა, რომ დასახული მიზნები სრულად ვერ იქნა მიღწეული, ბიძგი მიეცა მოულოდნელ და ახალ ფენომენს - შეიქმნა საზოგადოებრივი ფენა, რომელიც დაკავებული იყო ინფორმაციის მოპოვება - დამუშავებითა და გავრცელებით. ამ ფენამ საბოლოოდ გამოიწვია ინფორმაციის მოპოვება - დამუშავებისა და საინფორმაციო ტექნოლოგიების წარმოების მძლავრი ინდუსტრიის შექმნა, რომელმაც უზრუნველყო ინფორმაციის ფართო მასშტაბიანი მიმოცვლა - გავრცელება და საფუძველი ჩაუყარა მეცნიერება ტევადი ტექნოლოგიების განვითარებასა და ციფრული ეკონომიკის ფორმირებას.

მე-20 საუკუნის მეორე ნახევარში მსოფლიო საინფორმაციო - საკომუნიკაციო ინფრასტრუქტურის განვითარებამ (უპირველეს ყოვლისა, გლობალურმა კომპიუტერულმა ქსელებმა და საინფორმაციო ბანკებმა, თანამგზავრულმა, ოპტიკურ - ბოჭკოვანმა და ფიჭურმა კავშირმა) ბიძგი მისცა მსოფლიო საინფორმაციო ინფრასტრუქტურისა და სივრცის ჩამოყალიბებას და შესაბამისად შექმნა საერთო- საინფორმაციო გარემოს ფორმირების წინაპირობები, რამაც წარმოქმნა როგორც დადებითი, ასევე უარყოფითი ფენომენები[12].

მსოფლიო საინფორმაციო გარემოს ფორმირება წარმოადგენს გლობალიზაციისა და ინტეგრაციის ერთ - ერთ უმნიშვნელოვანეს საფუძველს, კერძოდ, ინფორმაციის მიმოცვლის არნახულმა ტემპებმა და მოცულობებმა:

✓ პოლიტიკურ ასპექტში - გამოიწვია საერთაშორისო ინსტიტუტების ჩამოყალიბება;

✓ ეკონომიკურ ასპექტში - გამოიწვია ფართო მომსახურების მძლავრი ინდუსტრიისა და „სამომხმარებლო საზოგადოების“ ფორმირება;

✓ სამეცნიერო - ტექნიკურ ასპექტში - გამოიწვია მეცნიერებატევადი ტექნოლოგიების შექმნა - განვითარება

[12] იხ. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

დღეისათვის საინფორმაციო საზოგადოების ფორმირების კრიტიკული ამოცანები - საინფორმაციო სივრცის ფორმირება და საზოგადოებისათვის მისი ხელმისაწვდომობის უზრუნველყოფა ტექნოლოგიური თვალსაზრისით, ეფუძნება ინტერნეტ ტექნოლოგიების გამოყენებას. ერთი მხრივ, ინტერნეტ - ქსელის საკვანძო კომპიუტერებზე - სერვერებზე ინფორმაციის განთავსება (ვებ-გვერდების სახით) მონაცემთა დიდი მასივების წარმოდგენისა და ცენტრალიზებულად მართვის საშუალებას იძლევა (თანამედროვე მძლავრი მონაცემთა ბაზების მართვის სისტემების გამოყენებით), ხოლო მეორე მხრივ, ინფორმაციის თავისუფალი მიმოქცევა, რომლის საშუალებასაც ინტერნეტი იძლევა, უზრუნველყოფს სერვერებზე განთავსებული საინფორმაციო მასივების იოლად ხელმისაწვდომობას მომხმარებელთა შეუზღუდავი რაოდენობისათვის, ნებისმიერი ადგილიდან და ნებისმიერ დროს.

ზემოაღნიშნული მოვლენების დადგომამ, გამოიწვია ისეთი დანაშაულებრივი ქმედებების ჩადენა, რომელიც მხოლოდ დღევანდელ თანამედროვეობაში გვევლინება, რასაც ადგილი ვერ ექნებოდა მსოფლიოს არსებობის იმ საუკუნეებში, რა დროსაც არ არსებობდა ინტერნეტ სივრცე. სწორედ ასეთ, ახლად შექმნილ დანაშაულებრივ ქმედებას წარმოადგენს კიბერ (კიბერნეტიკულ) დანაშაული, სამართლებრივი დეფინიციის მიხევით კი იგი, წარმოადგენს ნებისმიერი მართლსაწინააღმდეგო ქმედებას, რომელიც ჩადენილია კომპიუტერული სისტემის გამოყენებით კიბერსივრცეში.

საქართველოს სისხლის სამართლის კოდექსში კიბერდანაშაულს **XXXV თავი** ეძღვნება (284-ე - 286-ემუხლები).[13]

კიბერდანაშაულის სახეებად კანონი განიხილავს:

- ✓ კომპიუტერულ სისტემაში უნებართვო შეღწევას;
- ✓ კომპიუტერული მონაცემების ან/და კომპიუტერული სისტემის უკანონოდ გამოყენებას;
- ✓ კომპიუტერული მონაცემების ან/და კომპიუტერული სისტემის ხელყოფას;

[13] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი. წიგნი მე-2 გამომცემლობა „მერიდიანი“ 2012 წ.

ამასთან, კანონი განმარტავს, რომ კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის, პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკრო პროცესორით, აგრეთვე მობილური ტელეფონი). **კომპიუტერული** მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას. **უნებართვო** გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენიპირისათვის[14].

საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლის თანახმად, დანაშაულია კომპიუტერულ სისტემაში უნებართვო შეღწევა და იგი ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით იმავე ვადით. თუ ქმედებამ გამოიწვია მნიშვნელოვანი ზიანი ან თუ იგი ჩადენილია წინასწარი შეთანხმებით ჯგუფის მიერ, სამსახურებრივი მდგომარეობის გამოყენებით ან ამგვარი ქმედებისათვის ნასამართლევი პირის მიერ, იგი ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე.

საქართველოს სისხლის სამართლის კოდექსის 324[1] მუხლის თანახმად, დანაშაულია აგრეთვე კიბერტერორიზმი ესეიგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას, ჩადენილი მოსახლეობის დაშინების ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით. ეს დანაშაული ისჯება თავისუფლების აღკვეთი თვადით. ათიდან თხუთმეტ წლამდე. თუ იგივე ქმედება გამოიწვევს ადამიანის სიცოცხლის მოსპობას ან სხვა მძიმე შედეგს, იგი ისჯება თავისუფლების

[14] საქართველოს სისხლის სამართლის კოდექსი

აღკვეთით ვადით თორმეტიდან ოც წლამდე ან უვადო თავისუფლების აღკვეთით. ამ მუხლით გათვალისწინებული ქმედებისათვის სისხლისსამართლრივი პასუხისმგებლობა გათვალისწინებულია ასევე იურიდიული პირისათვის და იგი ისჯება ლიკვიდაციით ან საქმიანობის უფლების ჩამორთმევით დ აჯარიმით[15]. არანაკლებ საინტერესოა, კიდევ ერთი დანაშაულებრივი ქმედება - კიბერქურდობა, რომელიც სახეზეა, როდესაც საავტორო უფლების დარღვევით ხდება ინტერნეტიდან სხვადასხვა ინფორმაციის გადმოწერა. უმეტეს შემთხვევაში ვებ - გვერდებით სთავაზობენ მომხმარებელს პირატულ მასალას.

ამჟამად ინტერნეტი ვითარდება იმგვარად, რომ მოხდეს ისეთი მომსახურებების მხარდაჭერა, როგორიცაა მაგალითად, აუდიო და ვიდეო ფართოზოლოვანი ნაკადების გადაცემა. საერთო სარგებლობის ქსელის არსებობა (როგორიცა აინტერნეტი) და მძლავრი, ხელმისაწვდომი პორტატიული კომპიუტერული და საკომუნიკაციო ტექნიკა (როგორიცაა პორტატიული კომპიუტერები, ორმხრივი პეიჯერები, პერსონალური ციფრული თანაშემწეები, ფიჭური ტელეფონები) წარმოშობს მობილური კომპიუტერული და საკომუნიკაციო ტექნოლოგიების განვითარების ახალ პარადიგმას[16].

ამ ევოლუციას მოაქვს ახალი შესაძლებლობები - ინტერნეტ ტელეფონია, ინტერნეტ ტელევიზია. ტექნოლოგიების შემდგომი განვითარება საშუალებას იძლევა დაიხვეწოს ფასებისა და ტარიფების სისტემა, აგრეთვე შეიქმნას ქსელური ტექნოლოგიების ახალი თაობა სხვადასხვა მახასიათებლითა და მოთხოვნებით, ფართო ზოლოვანი საკაბელო კავშირიდან დაწყებული და თანამგზავრული კავშირით დამთავრებული. დაშვების ახალი რეჟიმები და მომსახურების ახალი ფორმები წარმოშობენ ახალ შესაძლებლობებს, რომლებიც თავის მხრივ სტიმულს მისცემენ თავად საქსელო ინფრასტრუქტურის ევოლუციას.

[15] საქართველოს სისხლის სამართლის კოდექსი
[16] იხ. http://www.nplg.gov.ge

2012 წელს მიღებულ იქნა კანონი "ინფორმაციული უსაფრთხოების შესახებ", რომელიც აწესებს ინფორმაციული უსაფრთხოების ზოგად სტანდარტებს საჯარო და კერძო სექტორისთვის. აღნიშნული საკანონმდებლო აქტის საფუძველზე, საქართველოს პრეზიდენტმა დაამტკიცა „კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხა“. 2013 წლის მაისში საქართველოს პრეზიდენტმა ხელი მოაწერა "საქართველოს კიბერუსაფრთხოების სტრატეგიას 2013 – 2015 წლებისთვის", რომელიც წარმოადგენს კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ მთავარ დოკუმენტს.

ელექტრონული სერვისების და საინფორმაციო ტექნოლოგიების განვითარებასთან ერთად საქართველოს კიბერსივრცეში დანაშაული მუდმივად იზრდებოდა, თანამედროვე ტექნოლოგიების განვითარებამ ბიზნესის წარმოება უფრო ეფექტიანი და ხელმისაწვდომი გახადა. კომპანიებს გაუადვილდათ მომხმარებლისთვის პროდუქციისა და მომსახურების შეთავაზება, თუმცა, კიბერსივრცეზე მზარდ დამოკიდებულებასთან ერთად, გაიზარდა კიბერდანაშაულის საფრთხეც. ინტელექტუალური საკუთრება და კომერციულად სენსიტიური ინფორმაცია ორგანიზებული დანაშაულებრივი ჯგუფებისთვის მიმზიდველი სამიზნეებია. თანამედროვე პერიოდში კიბერდანაშაულის საკმაოდ გავრცელებული შემთხვევებია: ონლაინ თაღლითობა, კომპიუტერულ სისტემასთან უნებართვო წვდომა, კომპიუტერული სისტემისა და მონაცემის უნებართვოდ გამოყენება და ა.შ. კიბერდანაშაულის ერთ - ერთ შემწყობ ფაქტორს კერძო სექტორის დაბალი ცნობიერება წარმოადგენს. კიბერსივრცეს არ გააჩნია საზღვრები. კიბერდანაშაულთან ბრძოლის ერთ - ერთი მიზანია, ხელი შეუწყოს საქართველოში კერძო სექტორის კიბერსივრცეში გამართულ ფუნქციონირებას, ელექტრონული ტრანზაქციების უსაფრთხო განხორციელებასა და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებელ განვითარებას. დასაცავი ინფრასტრუქტურის უდიდეს ნაწილს ფლობს და ოპერირებს კერძო სექტორი[17].

[17] იხ. http://police.ge/files

ამრიგად, ვინაიდან კიბერდანაშაულმა დიდი ზიანი შეიძლება მიაყენოს ბიზნესს. აუცილებელია კერძო სექტორმა დაიცვას კომერციულად სენსიტიური ინფორმაცია, ინტელექტუალური საკუთრება, მომხმარებელთა მონაცემები და სხვ.

II - თავი

კიბერბულინგი

ბულინგი (ინგ.Bullying) დაშინებას, ჩაგვრას, დატერორებას ნიშნავს. ის შეიძლება განიმარტოს, როგორც წინასწარგანზრახული, აგრესიული და ნეგატიური ქმედება, რომელიც მიმართულია სხვათა საზიანოდ. მას ყოველთვის ჰყავს სამიზნე, რომელზედაც ადამიანი ან ადამიანთა ჯგუფი ძალის დემონსტრირებას ცდილობს. „ბულინგი ვლინდება ფიზიკური და ფსიქოლოგიური ჩაგვრის სხვადასხვა ფორმით. ეს შეიძლება იყოს სისტემატიური დაცინვა (მსხვერპლის გარეგნობის ან პიროვნული მახასიათებლების), მსხვერპლის ნივთების დაზიანება, ფულის ან პირადი ნივთების გამოძალვა, აბუჩად, მასხრად აგდება, დამცირება.“[18]

ავსტრალიის „ეროვნული ცენტრი ბულინგის წინააღმდეგ” გამოყოფს ბულინგის შემდეგ ტიპებს:

- ✓ **ფიზიკურიბულინგი** - მოიცავს ფიზიკურ შეურაცხყოფას (დარტყმა, ხელი კვრა, ფეხის კვრა, სხეულის დაზიანება). ავსტრალიაში ყოველწლიურად 60.000-მდე ბავშვი ხდება აღნიშნული ტიპის ბულინგის მსხვერპლი, ამიტომ მნიშვნელოვანია ავსტრალიის გამოცდილების გაზიარება ზოგადად ბულინგის წინააღმდეგ ბრძოლაში, რადგან კიბერბულინგის საწყისი შესაძლებელია სწორედ რეალური ცხოვრებიდანაც მოდიოდეს.
- ✓ **ვერბალურიბულინგი** - მოიცავს სიტყვიერ შეურაცხყოფას (დამცინავი სახელით მიმართვა, ჰომოფობიური, რასისტული ან სხვა ნიშნით გამოთქმული განცხადებები და სხვა).
- ✓ **სოციალური ბულინგი** - სხვისი სოციალური რეპუტაციის შელახვა ან/დადამცირება.

[18] იხ. http://www.education.ge/index.php?do=definition/view&id=1891

✓ **კიბერ ბულინგი** - ხორციელდება ციფრული ტექნოლოგიების გამოყენებით ინტერნეტში. (მობილურით, კომპიუტერით, სოციალური მედიით და ა.შ.) სწორედ კიბერბულინგი არის აღნიშნული თავის კვლევის საგანი

2.1 კიბერბულინგის კატეგორიები

ავსტრალიის ფედერალური პოლიცია გვთავაზობს კიბერბულინგ [19] კატეგორიას:

1. **აალებადი** - შეიძლება დაიწყოს ორ პიროვნებას შორის და როგორც ალი ისე მოედოს სხვებსაც და ჩაითრიოს. აღნიშნული ძირითადად ხდება სოციალურ ქსელებში, საჯარო განცხადებაზე და კომენატრების შემდეგ. რა დროსაც ურთიერთსაპირისპირო აზრის გაჩენისათანავე შეიძლება დისკუსიაში მონაწილე პირები გაიყონ 2 ან მეტ ჯგუფად და დაიწყოს ღია დაპირისპირება მათ შორის;
2. **შევიწროება, შეწუხება** სიძულვილის ენით საუბარი, შეწუხება, განხორციელებული ჩათში მიწერით, იმეილით და ა.შ. ამ დროს ერთი პირი ახორციელებს მეორის მიმართ ისეთ ქმედებებს, რომელიც იწვევს ამ პირის სიმშვიდის დარღვევას. ეს შეიძლება გამოიხატოს პირად შეურაცხყოფაშიც
3. **ცილისწამება** - განზრახ არასწორი, მცდარი ინფორმაციის გავრცელება პირზე, მისი რეპუტაციის შელახვის მიზნით
4. **მოტყუება** - ვინმეს მოტყუება, რომ ხარ სხვა პიროვნება. მაგალითად ყალბი მომხმარებლის დარეგისტრირება სოციალურ ქსელში, რომელიც ვითომ წარმოადგენს მსხვერპლის ახლობელს. აღნიშნული შეიძლება გამოყენებული იქნას პირისგან რაიმე ინფორმაციის გამოსატყუებლად და შემდგომ მის წინააღმდეგ გამოსაყენებლად, ბულინგის განსახორციელებლად;
5. **სხვა ადამიანის განსახიერება** - საკუთარი მონაცემების გაყალბება, საკუთარ თავზე განსხვავებული ბიოგრაფიის მოგონება, პირთან დაასახლოვებლად. მოტყუების კატეგორიისგან განსხვავებით, ამ შემთხვევაში ბულინგის

[19] იხ. http://www.afp.gov.au/~/media/afp/pdf/c/cyber-bullying-no-crops.pdf

განმახორციელებელი არ ცდილობს მსხვერპლის ნაცნობის როლი მოირგოს, არამედ ქმნის ლეგენდას საკუთარ თავზე და ისე შედის კონტაქტში. აღნიშნულის მიზანიც არის მსხვერპლის შესახებ ისეთი ინფორმაციის მოპოვება, რომლის საშუალებითაც მოახდენს მასზე ბულინგის განხორციელებას;

6. **გარიყვა** - ვინმეს დაიგნორება ან უფლების ჩამორთმევა, რომ ვერ შეძლოს ონლაინ ჯგუფში აქტივობის განხორციელება

7. **კიბერ მიყოლა** - ერთგვარი გადაკიდება ინტერნეტში კონკრეტულ პიროვნებაზე. აღნიშნული არ მოიცავს პირად მიმოწერაში გადაკიდებას, უბრალოდ იგივე აქტივობას ახორციელებს პირი, რასაც სხვა. მაგალითად სოციალურ ქსელში ყველგან დააკომენტარებს, სადაც ეს პიროვნება დაწერს რამეს.

2.2 კიბერბულინგი საქართველოში

„კიბერ-გადაკიდებას (კიბერბულინგს), როგორ ცდანაშაულის ცალკე სახეს, არ იცნობს საქართველოს კანონმდებლობა, თუმცა საქართველოს სისხლის სამართლის კოდექსი ითვალისწინებს სისხლის სამართლებრივ პასუხისმგებლობას თვითმკვლელობამდე მიყვანისათვის, რომელიც გამოიწვია მსხვერპლისადმი განხორციელებულმა მუქარამ, მისი პატივის ან ღირსების სისტემატურმა დამცირებამ. ეს დანაშაული ისჯება თავისუფლების შეზღუდვით ვადით სამ წლამდე ან თავისუფლების აღკვეთით ვადით ორიდან ოთხ წლამდე“[20].

ჩემი აზრით ზემოთ აღნიშნული საკითხი პრობლემას წარმოადგენს, რადგან თუ კიბერბულინგმა არ გამოიწვია პირის თვითმკვლელობამდე მიყვანა, მანამდე სამართალდამცავი ორგანოს წარმომადგენლებს არ შეუძლიათ მოქმედება.

ზოგიერთი იურისტი მიიჩნევს, რომ ინტერნეტში გადაკიდება, ადამიანის შეურაცხყოფა არ უნდა იყოს დასჯადი. მაგალითად “netgazeti.ge-თან” მიცემულ

[20] იხ. http://pog.gov.ge/res/docs/statistika/cybercrime.pdf

ინტერვიუში[21]საიას ყოფილი თავმჯდომარე, იურისტი კახა კოჟორიძე აცხადებს, რომ ინტერნეტში შეურაცხყოფა არ უნდა დაკვალიფიცირდეს წვრილმან ხულიგნობად. მისი აზრით თუ სამართალდამცავი ორგანოები ამაზე რეაგირებას დღეს დაიწყებენ, მაშინ გამოდის, რომ კანონი განჭვრეტადი არ ყოფილა. ანუ კანონი არ არის ისე ჩამოყალიბებული, რომ ის რიგითმა ადამიანმა გაიგოს და მიხვდეს, რომ ინტერნეტში გინება აკრძალულია. ჩემი აზრით აღნიშნულ შემთხვევაში სამართალდამცავ ორგანოებს შეუძლიათ მაინც იმოქმედონ ადმინისტრაციულ სამართალდარღვევათა კოდექსის 166 -ე მუხლის მიხედვით, რაც გულისხმობს შემდეგს: **წვრილმანი ხულიგნობა** – „საზოგადოებრივ ადგილებში ლანძღვა - გინება, მოქალაქეებზე შეურაცხმყოფელი გადაკიდება და სხვა ამგვარი მოქმედება, რომელიც არღვევს საზოგადოებრივ წესრიგსა და მოქალაქეთა სიმშვიდეს, – გამოიწვევს დაჯარიმებას 100 ლარის ოდენობით ან, თუ საქმის გარემოებებისა და დამრღვევის პიროვნების გათვალისწინებით ამ ზომის გამოყენება არასაკმარისად იქნება მიჩნეული, – ადმინისტრაციულ პატიმრობას 15 დღემდე ვადით“[22].

ამ შემთვევაში შეიძლება პრობლემად იკვეთებოდეს თუ რას ნიშნავს საზოგადოებრივი ადგილი. ჩემი აზრით საზოგადოებრივი ადგილი ეს არის ნებისმიერი სივრცე, სადაც იკრიბება საზოგადოება. ეს შეიძლება იყოს ქუჩა, ტრანსპორტი, სკვერი და აგრეთვე ინტერნეტ სივრცეც, რადგან აქაც იკრიბება საზოგადოება, აქვთ ჩვეულებრივი ურთიერთობა: პირადი მიმოწერა, ჯგუფური მიმოწერა. ანუ ადამიანებს აქვთ ერთმანეთთან კონტაქტი, იკრიბებიან სხვადასხვა ვებგ-ვერდზე, ფორუმებზე, სოციალურ ქსელებში და ა.შ. შესაბამისად შეგვიძლია, რომ ინტერნეტ სივრცე, სადაც ხდება საზოგადოების შეკრება და იქმნება საზოგადოებრივი სივრცე, მივიჩნიოთ საზოგადოებრივ ადგილად. აღნიშნულიდან გამომდინარე ჩემი აზრით სამართალდამცავ ორგანოებს შეუძლიათ ინტერნეტში შეურაცხყოფის შემთვევაში იმოქმედონ ადმინისტრაციულ სამართალდარღვევათა კოდექსის 166-ე მუხლის მიხედვით.

[21] იხ. http://netgazeti.ge/news/35133/

[22] საქართველოს ადმინისტრაციულ სამართალდარღვევათ აკოდექსის 166-ე მუხლი.

მეორე არგუმენტად კოჟორიძე აღნიშნავს, რომ ეს მუხლი მიღებულია მანამ, სანამ ინტერნეტში ასეთი პრობლემა გაჩნდებოდა, შესაბამისად მისი მიზანი არ იყო ინტერნეტში შეურაცხყოფის პრობლემის დარეგულირება. აგრეთვე აღნიშნავს, რომ სიტყვის და გამოხატვის თავისუფლების შესახებ კანონის მე-9 მუხლში წერია, თუ რა შემთხვევაში შეიძლება დარეგულირდეს სიტყვის და გამოხატვის შინაარსი.

„კანონით შეიძლება დაწესდეს სიტყვისა და გამოხატვის შინაარსობრივი რეგულირება, თუ ეს ეხება:

ა) ცილისწამებას;

ბ) უხამსობას;

გ) პირის პირშეურაცხყოფას ;

დ) დანაშაულის ჩადენისკენ წაქეზებას;

ე) მუქარას;

ვ) პერსონალურ მონაცემებს, სახელმწიფო, კომერციულ ან პროფესიულ საიდუმლოებას;

ზ) რეკლამას, ტელეშოპინგს ან სპონსოროზას;

თ) სამხედრო მოსამსახურის, ადმინისტრაციული ორგანოს, აგრეთვე მისი თანამდებობის პირის, წევრის ან თანამშრომლის სიტყვისა და გამოხატვის თავისუფლებას;

ი) თავისუფლება აღკვეთილიან თავისუფლება შეზღუდული პირის სიტყვისა და გამოხატვის თავისუფლებას;

2. შინაარსობრივი რეგულირება შეიძლება განხორციელდეს მხოლოდ თვალსაზრისობრივად ნეიტრალური, არადისკრიმინაციული შეზღუდვის სახით“[23].

აქ წერია, რომ კანონით შესაძლოა დაწესდეს სიტყვისა და გამოხატვისათვის შინაარსობრივი რეგულირება, თუ ეს ეხება პირისპირ შეურაცხყოფას. აღნიშნულ შემთხვევაში კოჟორიძე მიიჩნევს, რომ ინტერნეტში განხორციელებული შეურაცხყოფა არ არის პირისპირ შეურაცხყოფა.

[23] საქართველოს კანონი სიტყვისა და გამოხატვის თავისუფლების შესახებ, მუხლი 9.

შეურაცხყოფა - „პიროვნების პატივისა და ღირსების განზრახ დამცირება, გამოხატული უწესო ფორმით. შეურაცხყოფის დროს დამნაშავე აკნინებს სხვის პატივსა და ღირსებას სიტყვიერი ძალადობის მეშვეობით (გინება, სალანძღავი სიტყვა), რაც შეეხება პირის ზნეობრივ თუ გონებრივ თვისებებს, ფიზიკურ თავისებურებას თუ საქმიანობას, მნიშვნელობა არა აქვს, შეესაბამება თუ არა ნათქვამი სინამდვილეს“[24]. აღნიშნულიდან გამომდინარე, როდესაც მაგალითად სოციალურ ქსელში ერთი პიროვნება მიაყენებს მეორეს შეურაცხყოფას, გამოდის, რომ მოხდა პიროვნების პატივისა და ღირსების განზრახ დამცირება. ამ დროს საქმე გვაქვს პირისპირ შეურაცხყოფასთან და აგრეთვე ადმინისტრაციულ სამართალდარღვევათა კოდექსის 166-ე მუხლის მიხედვით თუ ვიმსჯელებთ, ამ შემთხვევაში საქმე გვაქვს წვრილმან ხულიგნობასთან და სამართალდამცავ ორგანოებს შეუძლიათ იმოქმედონ, რადგან პირისპირ შეურაცხყოფა ინტერნეტში იგივე მოქალაქეზე გადაკიდებაა აღნიშნული მუხლის მიხედვით, რაც არღვევს მოქალაქეთა სიმშვიდეს. აგრეთვე თუ მაგალითად რომელიმე სოციალურ ქსელში, საჯარო განცხადებაზე ერთმა პიროვნებამ მიაყენა მეორეს შეურაცხყოფა, ამ შემთვევაში არამხოლოდ შეურაცხყოფილის უფლებები დაირღვა, არამედ მთლიანი საზოგადოებისრადგან როგორც ზემოთ აღვნიშნე სოციალური ქსელი და იქ დადებული ნებისმიერი საჯარო ინფორმაცია, რომელსაც თვალყურს ადევნებს საზოგადოება, არის საზოგადოებრივი ადგილი. შესაბამისად აღნიშნული ქმედება დაკვალიფიცირდება როგორც წვრილმანი ხულიგნობა: საზოგადოებრივ ადგილას ლანძღვა-გინება.

კიბერბულინგზე საუბრისას მნიშვნელოვანია ცალკე გამოვყოთ ბავშთა მიმართ განხორციელებული ბულინგი. „რადიო თავისუფლებასთან“ მიცემულ იტერვიუში [25] კავშირ "საფარის" სამედიცინო დირექტორი სოფო ტაბაღუა განმარტავს, რომ ბავშვთა მიმართ კიბერბულინგი, ტრადიციული ბულინგის მსგავსად, აგრესიას, ძალადობას და ჩაგვრის გავრცელებას უწყობს ხელს. კიბერსივრცეში მაღალია ანონიმურობა, შესაბამისად გამოხატვის გზებიც უფრო

[24] იხ. http://www.nplg.gov.ge/gwdict/index.php?a=term&d=5&t=2599
[25] იხ. http://www.radiotavisupleba.ge/content/normad-kceuli-dzaladoba/25154835.html

აგრესიული ხდება და მსხვერპლისთვის უფრო მძიმე გადასატანი ხდება ბულინგი, შეიძლება უფრო სერიოზული ფსიქოლოგიური ტრავმაც მიიღოს ბავშვმა. „ბავშვის უფლებათა კომიტეტის N13 ზოგად კომენტარში, რომელიც ეხება ბავშვის უფლებას, დაცული იყოს ნებისმიერი სახის ძალადობისგან, აღნიშნულია, რომ ბავშვის მიმართ ძალადობა, როგორც ფიზიკური, ასევე, ფსიქოლოგიური, ხშირად, გამოხატულია თავად ბავშვებს შორის ბულინგით. აღნიშნული ზიანს აყენებს ბავშვის ფიზიკურ და ფსიქოლოგიურ კეთილდღეობას, ასევე, უარყოფითად აისახება ბავშვის განვითარებაზე, განათლებასა და საზოგადოებაში ინტეგრაციაზე“ [26] . ყოველივე ზემოთ აღნიშნულიდან გამომდინარე ბავშვთა წინააღმდეგ მიმართული ბულინგი კიდევ უფრო მძიმე შედეგებს იწვევს, რადგან ბავშვის ფსიქიკა უფრო მყიფეა და შეიძლება რადიკალურ გზებს მიმართონ, საკუთარ თავს რაიმე დაუშაონ. ამიტომ მნიშვნელოვანია შესაბამისი ღონისძიებების გატარება, რათა მოხდეს აღნიშნული დანაშაულის გამოვლენა და აღკვეთა.

კიბერბულინგი თავისი არსიდან გამომდინარე სპეციფიურია, რადგან კიბერ სივრცის გამოყენებით ხორციელდება. თუმცა ჩემი აზრით ძირითადად კიბერბულინგის საწყისი მოდის რეალური ცხოვრების ბულინგიდან. მაგალითად: თუ ბავშვი არის სკოლაში ბულინგის მსხვერპლი, აქედან გამომდინარე შეიძლება შემდგომ მასზე ბულინგი განხორციელდეს კიბერ სივრცის გამოყენებითაც: სოციალურ ქსელში მოხდეს მასზე ისეთი ინფორმაციის გავრცელება, რომელიც გამოიწვევს მსხვერპლ ბავშვში ფსიქოლოგიურ ტრავმას და შეიძლება რაკიდალურ შედეგებამდე მიიყვანოს. მაგალითად თუ რეალურ ცხოვრებაში უშუალოდ ჩაგრავენ მას, შეიძლება მოხდეს აღნიშნულის ვიდეო გადაღება და შემდგომ სოციალურ ქსელში გავრცელება.

რეკომენდაციები:

- ✓ კიბერსივრცის კონტროლი ბულინგისგან დასაცავად საკმაოდ რთულია თუ ის პირადი მიმოწერით ხორციელდება. მაგალითად სკოლის მოსწავლეებში

[26] საქართველოს სახალხო დამცველის ანგარიში, 2015 წელი, გვ.919.

ბულინგის განმახორციელებელი მსხვერპლს წერს პირად ჩატში. ამ შემთხვევაში მნიშვნელოვანია, რომ ბავშვი იყოს ინფორმირებული და შესაბამის ადამიანებს მიაწოდოს ინფორმაცია აღნიშნულთან დაკავშირებით. ასეთ დროს მნიშვნელოვანია მანდატურთა სამსახურის ჩართვა. ისინი აქტიურად უნდა თანამშრომლობდნენ ბავშვებთან სკოლებში და უნდა ახდენდნენ ბულინგის ფაქტების გამოვლენას, შემდგომი აღკვეთისათვის. შეიძლება ითქვას მანდატური უნდა იყოს ოპერატიული თანამშრომლის უნარ-ჩვევებით აღჭურვილი, რომ ადვილად შევიდეს კონტაქტში ბავშვთან, რომელიც გულჩათხრობილია, არავის უსმენს, არავის ენდომება და მოიპოვოს შესაბამისი ინფორმაცია მისგან.

✓ შ.ს.ს აკადემია აქტიურად უნდა ახდენდეს მანდატურების გადამზადებას, რათა უფრო ეფექტურად ებრძოლონ ბულინგს სკოლაში.

✓ რაც შეეხება საჯაროდ განხორციელებულ კიბერბულინგს, აქ უნდა მოხდეს სამართალდამცავი ორგანოების ჩართვა იმ კუთხით, რომ დროულად მოხდეს ისეთი სახის ინფორმაციის დაბლოკვა ან ამოღება შესაბამისი ინტერნეტ სივრციდან, რომელიც შეიცავს ბულინგის ნიშნებს. ანუ მაგალითად თუ რომელიმე სოციალურ ქსელში (მაგალითად „Facebook.com") ან ვიდეო პორტალზე (მაგალითად „Youtube.com") გავრცელდა ისეთი სახის ინფორმაცია, რომელიც შეიცავს ბულინგის ნიშნებს და მიმართულია შესაბამისი პირის მიმართ, უნდა მოხდეს ასეთი ინფორმაციის დაბლოკვა, წაშლა, ხოლო გამავრცელებლის მიმართ გატარდეს შესაბამისი ღონისძიებები.

2. 3 კიბერთაღლითობა

,,ევროპის საბჭოს 2001 წლის კომპიუტერული დანაშაულის შესახებ კონვენციის მე-8 მუხლი" ავალდებულებს ხელმომწერ სახელმწიფოებს, მიიღონ შესაბამისი საკანონმდებლო და სხვა სახის ზომები, რომლებიც მოახდენს შემდეგ ქმედებათა კრიმინალიზაციას:

✓ კომპიუტერული მონაცემის ნებისმიერი ფორმით შეყვანა, შეცვლა, წაშლა ან გადამალვა;

✓ კომპიუტერული სისტემის ფუნქციონირებაში ნებისმიერი სახით ჩარევა, თაღლითური ან სხვა არაკეთილსინდისიერი განზრახვით საკუთარი ან სხვისი ფინანსური/ეკონომიკური მოგების/სარგებლის უნებართვოდ მიღების მიზნით.[27]

კიბერ სივრცეში თაღლითები იყენებენ ფიშინგს, რაც ნიშნავს შემდეგს: „(ინგლისურად phishing:fishing - თევზაობა) — ინტერნეტ თაღლითობის დანაშაულებრივი ფორმა, რომლის მიზანია თაღლითური გზით მომხმარებელს გამოსძალოს პირადი საიდენტიფიკაციო მონაცემები, მაგალითად პაროლი, საკრედიტო ბარათის ან საბანკო ანაგარიშის ნომერი და სხვა კონფიდენციალური ინფორმაცია“[28]. ანუ ამ დროს ხდება მომხმარებლის პირადი მონაცემების, იდენტიფიკაციის ქურდობა.

ფიშინგის გამოყენების გავრცელებული ხერხები:[29]

ფიშინგ წერილი - ამ დროს მსხვერპლს ელ. ფოსტის მისამართზე მიდის ყალბი წერილი სხვადასხვა ორგანიზაციიდან, მაგალითად ბანკიდან, რომლის მომხმარებელიც არის და სთავაზობს პირადი მონაცემების განახლებას წერილშივე შეთავაზებული ყალბი ვებ გვერდის გამოყენებით. თუ მომხმარებელი გადავა აღნიშნულ ლინკზე და შეავსებს მონაცემებს, ინფორმაციას ავტომატურად მიიღებს დანაშაულებრივი ქმედების ჩამდენი პირი.

ფიშინგ ვებ გვერდი - ამ შემთხვევაში პირი გადადის ვებ გვერდზე, რომლის დასახელებაც გავს რეალურ ვებ გვერდს. ახდენს ავტორიზაციას, რა დროსაც ხდება ინფორმაციის გადაცემა თაღლითისთვის.

ვებ მისამართის მანიპულაცია - აღნიშნულ შემთვევაში ფიშერი (ფიშინგის განმახორციელებელი) მსხვერპლს მიწერს ვებ მისამართს რეალური დასახელებით, მაგრამ ლინკზე გადასვლის შემდეგ იცვლება სახელწოდება და მომხმარებელი აღმოჩნდება თაღლითის მიერ დამზადებულ გვერდზე.

---

[27] ევროპის საბჭოს კონვენცია კომპიუტერული დანაშაულის შესახებ, ბუდაპეშტი, 23.11.2001 მუხლი 8

[28] იხ. http://dea.gov.ge/?web=0&action=article&article_id=8&lang=geo

[29] იხ. http://www.phishing.org/phishing-techniques/

ფიშინგის ყველაზე ხშირ სამიზნეს წარმოადგენენ ბანკები, საფინანსო ორგანიზაციები, ელექტრონული აუქციონები და ინტერნეტ მაღაზიები. ვინაიდან თაღლითებს სურთ მოიპოვონ ინფორმაცია, რომელიც იძლევა ფულთან წვდომის საშუალებას. აგრეთვე პოპულარულია ელექტრნული ფოსტის მონაცემების მოპარვა, რათა შემდგომში გამოიყენონ სპამის და ვირუსების გასავრცელებლად.

2013 წლისათვის საგადასახადო ბარათების რაოდენობამ ევროკავშირში მიაღწია 760 მილიონ ერთეულს, რაც გულისხმობს 1.5 ერთეულ ბარათს ერთ სულ მოსახლეზე. უნაღდო ანგარიშსწორების ზრდამ გამოიწვია ახალი კიბერ თავდასხმის მეთოდების ზრდა და ამასთან საპირისპირო ზომების შემუშავება ბარათების ინდუსტრიაში კლიენტებისა და ბიზნესის დასაცავად[30]. ზემოთ აღნიშნულიდან გამოდინარე აშკარა ხდება თუ რამდენად სახიფათო გახდა კიბერ სივრცის გამოყენებით ჩადენილი თაღლითობა. ქართულ რეალობაში გვაქვს ფიშინგ ვებ გვერდების შექმნის შეთხვევები, ძირითადად ინტერნეტ ტოტალიზატორების გამოყენებით. მაგალითად თაღლითი ქმნის ინტერნეტ სათამაშო საიტის „adjarabet.com-ის“ მსგავსი სახელწოდების ვებ გვერდს, ოღონდ ამატებს ერთ ასოს - „i“-ს. რის შედეგადაც ვიღებთ შემდეგ სახელწოდებას “adjiarabet.com”. შექმნილი ყალბი მისამართი გავს ნამდვილს, ამიტომ შეიძლება მომხმარებელი შევიდეს შეცდომაში და გამოიყენოს აღნიშნული ყალბი საიტი. მოახდენს ავტორიზაციას და საკუთარ ინფორმაციას გადასცემს თაღლითს.

საქართველოს სისხლის სამართლის კოდექსი არ ითვალისწინებს ფიშინგის (იდენტიფიკაციის ქურდობის) შესაბამის მუხლს. აღნიშნული დანაშაულის შემთხვევაში პირის ქმედება დაკვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284-ე და 177-ე მუხლებით.[31] რაც გულისხმობს კომპიუტერულ სისტემაში უნებართვო შეღწევას და ქურდობას, ესე იგი სხვისი მოძრავი ნივთის ფარულ დაუფლებას მართლსაწინააღმდეგო მისაკუთრების მიზნით.

[30] ევროპოლისყოველწლიურიანგარიში, 2015 წელი.
[31] იხ. http://pog.gov.ge/res/docs/statistika/cybercrime.pdf

ფიშინგთან საბრძოლველად მთელი რიგი ღონისძიებებია გატარებული ორგანიზაციების მიერ. შეიქმნა ფიშინგ საიტების სია, რომელსაც აქტიურად იყენებს ისეთი ინტერნეტ ბრაუზერები, როგორებიცაა: "Internet Explorer", "Google Chrome", "Opera" და სხვა. შეიქმნა სპეციალური სერვისი რომელიც ფილტრავს ფიშინგ საიტებს[32] ფიშინგის წინააღმდეგ საბრძოლველად შეიქმნა სპეციალური სამუშაო ჯგუფი: „Anti Phishing Working Group", რომელიც აერთიანებს როგორც სამთავრობო და სამართალდამცავ ორგანოებს, ისე არასამთავრობო ორგანიზაციებს. გაერთიანებულია 1800 ზე მეტი ინსტიტუცია[33].

აღნიშნული ჯგუფის სამუშაო მოიცავს შემდეგ აქტივობებს:

- ✓ კონფერენციების გამართვა და შესაბამისი პროფესიონალების მოწვევა ფიშინგის წინააღმდეგ ბრძოლის ხერხების დახვეწასა და განვითარებისთვის.
- ✓ შესაბამისი ღონისძიებების ჩატარება, რათა შეკრებილი იქნას პროფესიონალები მთელი მსოფლიოდან და ერთობლივი ჯგუფი დაკომპლექტდეს კიბერდანაშაულის წინააღმდეგ ბრძოლისთვის.
- ✓ საზოგადოების ცნობიერებისა და განათლების დონის ამაღლება, რათა არ გახდნენ კიბერდანაშაულის მსხვერპლი

რეკომენდაციები:

- ✓ სამართალდამცავი ორგანოების აქტიური თანამშრომლობა საერთაშორისო ორგანიზაციებთან, პირველ რიგში ზემოთ აღნიშნულ „Anti Phishing Working Group"-თან. სადაც გაერთიანებულია მთელი რიგი ჯგუფები პროფესიონალებისა. შესაბამისად მნიშვნელოვანია მათი გამოცდილების გაზიარება, რომელიც დაგვეხმარება ფიშინგის წინააღმდეგ ბრძოლაში, ახალი ხერხების გაცნობასა და განვითარებაში.
- ✓ სამართალდამცავები უნდა გადიოდნენ მუდმივ გადამზადებას და აქტიურად იღებდნენ მონაწილეობას მოწინავე ქვეყნების: ა.შ.შ.-ს და ევროპის ქვეყნების მიერ ჩატარებულ ღონისძიებებში კიბერთაღლითობის წინააღმდეგ ბრძოლაში.

[32] ი.ხ http://dea.gov.ge/?web=0&action=article&article_id=8&lang=geo
[33] ი.ხ http://www.antiphishing.org/about-APWG/

- ✓ ასევე შესაძლებელია შემდგომ უკვე საქართველოშიც, მსგავსი ღონისძიებების განხორციელება და ერთგვარი კურსის ჩატარება სამართალდამცველებისათვის. ამისათვის აქტიურად უნდა ჩაერთოს შ.ს.ს აკადემია, რომელიც მოაწყობს შესაბამის ღონისძიებას და მოიწვევს პროფესიონალებს მოწინავე ქვეყნებიდან, ლექცია-სემინარების ჩასატარებლად.
- ✓ საზოგადოების ცნობიერების ამაღლება, რათა არ გახდნენ ფიშინგის ან კიბერ თაღლითის მიერ გამოყენებული სხვა ხერხის მსხვერპლი. აღნიშნულთან დაკავშირებით შეიძლება შ.ს.ს-მ წამოიწყოს ერთგვარი კამპანია, ჩაიწეროს ვიდეო რგოლები და გავრცელდეს როგორც ინტერნეტ სივრცეში, ისე ტელევიზიით.

III თავი

კიბერტერორიზმი

სანამ უშუალოდ კიბერტერორიზმზე გადავალ, მნიშვნელოვანია განვიხილოთ რა არის ზოგადად ტერორიზმი, რა სახის დანაშაულთან გვაქვს საქმე. აღნიშნული სიტყვა ყოველ ადამიანში შიშის გრძნობას აღძრავს, ეს სიტყვა დაკავშირებულია უარყოფით მოვლენასთან. საინტერესოა განვიხილოთ ტერორიზმის ისტორიული ცვალებადობა და ტერორისტული მეთოდების გამოყენება დროსთან მიმართებაში.

კაცობრიობის ისტორიაში ტერორისტული ქმედების ნიშნები მრავლად მოიძებნება. ძალადობრივი მეთოდებით მიზნის მიღწევის მცდელობა საზოგადოების განვითარების ყველა ეტაპს ახასიათებდა. „პოლიტიკოსებისა და პოლიტოლოგების ნაწილის აზრით, ყველა ტერორისტული აქტის პირველწყარო და საფუძველი სოციალური მოტივებია“[34]. ტერორიზმი პირველ რიგში იწვევს შიშს და პანიკას. ის გამოიყენება საზოგადოების დაშინებისათვის. არსებობს ტერორიზმის რამდენიმე სახე. მათგან დღეს ყველაზე დიდ პრობლემას წარმოადგენს რელიგიური მოტივებით განხორციელებული ტერორისტული აქტები. სწორედ რელიგიური ექსტრემისტები იწირავენ

[34] ნ.ლომიძე „გლობალური საფრთხეები და ეროვნული უსაფრთხოების პრობლემები საქართველოში“ თბილისი 2013, გვ. 65

ყველაზე დიდი რაოდენობით უდანაშაულო მსხვერპლს. ისლამური ხალიფათის ჩამოყალიბების შემდეგ კიდევ უფრო წინა პლანზე წამოიწია აღნიშნულმა პრობლემამ. ისინი რელიგიური ნიშნით, მათგან განსხვავებული, სხვა მრწამსის ადამიანებს ხოცავენ მხოლოდ იმიტომ, რომ სხვა ღმერთის სწამთ. ისინი გამოდიან მოწოდებებით მათი რელიგიური მხარდამჭერების მიმართ, რომ ფიზიკურად გაანადგურონ ნებისმიერი ადამიანი, ვისი რწმენაც არ არის მათი რწმენის თანხვედრაში.

ტერორიზმი ვლიდება სხვადასხვა ფორმით განხორციელებულ ტერორისტულ ქმედებებში. ყველაზე გავრცელებული ფორმებია[35]:

- ✓ **დივერსია**, თავდასხმა და მკვლელობა - ცეცხლსასროლი თუ ბიოლოგიური იარაღის გამოყენებით სრულიად უდანაშაულო, მშვიდობიანი მოსახლეობის ფიზიკური განადგურება;
- ✓ **გატაცება** - ჩინოვნიკებისა და ხელისუფლების წარმომადგენლების გატაცება, საზოგადოების ფართო ფენების ყურადღების მისაქცევად, აგრეთვე ფინანსური და სხვა მოთხოვნილებების დასაკმაყოფილებლად
- ✓ **შენობა-ნაგებობების დაუფლება** - ძირითადი სამიზნეებია საელჩოები და ადმინისტრაციული შენობები
- ✓ **ჰაიჯეკინგი** - სატრანსპორტო საშუალებების გატაცება;

სწორედ ამ უკანასკნელს - კიბერტერორიზმს განვიხილავ აღნიშნული თავის ფარგლებში, რომელიც ძირითადად გამოიყენება მუქარისა და ძალადობის შემცველი ინფორმაციის გასავრცელებლად, სახელმწიფო სტრუქტურების ონლაინ ბაზებზე შეტევით, სახელმწიფო საიდუმლოების მოსაპოვებლად, სახელმწიფოს დეზორგანიზაციისთვის და საზოგადოების დაშინებისათვის. ტერორისტები ძალადობის ან ძალადობის მუქარის გამოყენებით შიშსა და პანიკას თესავენ საზოგადოებაში. ყველა ტერორისტული აქტი, მათ შორის კიბერტერორიზმი შეიცავს ძალადობას ან მუქარას. მისი მიზანია ფართო საზოგადოებაზე ხანგრძლივი ფსიქოლოგიური ზეგავლენის მოხდენა, რასაც საკმაოდ წარმატებით ახორციელებენ კიბერსივრცის

[35] ჯ.გახოკიძე - „ეროვნულიუსაფრთხოებისძირითადიპრობლემები“, თბილისი 2007 წელი, გვ.168

გამოყენებით სხვადასხვა ტერორისტული ორგანიზაციები, დღეს კი განსაკუთებით ისლამური ხალიფატი.

3.1 კიბერტერორიზმი, როგორც კიბერდანაშაულის ერთ-ერთი სახე

შემდგომი კვლევისათვის მნიშვნელოვანია დავადგინოთ თუ რით განსხვავდება ერთმანეთისგან ეს 2 ცნება და არის თუ არა კიბერტერორიზმი კიბერდანაშაულის ერთ-ერთი სახე.

„კიბერტერორიზმი განისაზღვრება, როგორც დანაშაულებრივი ქმედება, რომელიც მიმართულია მთლიანი საზოგადოების წინააღმდეგ. ხოლო კიბერდანაშაულის სამიზნეა კონკრეტული ჯგუფი ან ინდივიდი"[36]. აქედან გამომდინარე შეგვიძლია გავმიჯნოთ ეს ორი ცნება მისი მიზნიდან გამომდინარე. კიბერტერორიზმის დროს დანაშაულებრივი ქმედება მიმართულია მთლიანად საზოგადოების წინააღმდეგ, მას სურს შიშის დათესვა სახელმწიფოში, მისი დესტაბილიზაცია და განადგურება. ხოლო კიბერდანაშაულს აქვს კონკრეტული მიზანი, გარკვეული სარგებლის მიღების სურვილი, რის შედეგადაც ზიანდება კონკრეტულ პირთა ჯგუფი ან ინდივიდი. ამ უკანასკნელის დროს, დანაშაულის ჩამდენ პირს არ სურს ზიანი მიადგეს მთლიან საზოგადოებას, ის არ მოქმედებს სახელმწიფოს წინააღმდეგ, არ სურს მისი დესტაბილიზაცია.

ეს ორი ცნება გამიჯნულია საქართველოს სისხლის სამართლის კოდექსითაც. კიბერტერორიზმი წარმოდგენელია სსკ-ის XXXVIII, ტერორიზმის თავში. რაც გულისხმობს: კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლებას, მის გამოყენებას ან გამოყენების მუქარას, რაც ქმნის მძიმე შედეგის საშიშროებას, ჩადენილი მოსახლეობის დაშინების

[36] იხ.http://cyber.laws.com/cyber-terrorism

ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით. აღნიშნულიდან გამომდინარე კიბერტერორიზმი განისაზღვრება როგორც ტერორიზმის ერთ - ერთი სახე.

კიბერდანაშაული განსაზღვრულია სსკ-ის XXXV, კიბერდანაშაულის თავის მიხედვით. რაც გულისხმობს კომპიუტერულ სისტემაში უნებართვო შეღწევას; კომპიუტერული პროგრამის ან/და სხვა მოწყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარ უზრუნველყოფას; კომპიუტერული მონაცემის უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვას.

ყოველივე ზემოთ აღნიშნულიდან გამომდინარე კიბერტერორიზმს და კიბერდანაშაულს აქვთ საერთო და განმასხვავებელი ნიშნები. ისინი განსხვავდებიან დანაშაულის მიზნიდან გამომდინარე: კიბერტერორიზმის დროს კიბერტერორისტის მიზანია სახელმწიფოს დეზორგანიზაცია, საზოგადოებაში შიშისა და პანიკის დათესვა. თავისი მოქმედებით კიბერტერორისტი ზიანს აყენებს მთლიან საზოგადოებას. ხოლო კიბერდანაშაული მოიცავს ყველა იმ დანაშაულებრივ ქმედებას, რომელიც მიმართულია კონკრეტული პირის ან პირთა ჯგუფის წინააღმდეგ. კიბერდამნაშავე მოქმედებს კონკრეტული პირის და პირთა ჯგუფის მიმართ, რათა მიიღოს გარკვეული სარგებელი, მაგალითად სხვისი საბანკო ანგარიშის გატეხვა და მისგან საკუთარ ანგარიშზე თანხის გადატანა. ამ დროს საქმე გვაქვს კიბერდანაშაულთან, რადგან დანაშაულის ჩამდენ პირი მოქმედებს კონკრეტული პირის მიმართ, რომლისგანაც იპარავს თანხას. ამ ქმედებით იგი ზიანს აყენებს ერთ კონკრეტულ პიროვნებას და არა მთელ საზოგადოებას. კიბერტერორიზმის დროს კი კიბერტერორისტი ახორციელებს ისეთ ქმედებას, რომელიც ზიანს აყენებს მთელ საზოგადოებას. მაგალითად 2015 წლის ნოემბერში, ისლამური სახელმწიფოს მიერ ქართულ ენაზე გავრცელებული კადრები ინტერნეტით, რომელიც შეიცავდა მუქარას ქართველი ერის მიმართ,

ეროვნული და რელიგიური კუთვნილებიდან გამომდინარე, იმუქრებოდნენ ჩვენი ფიზიკური განადგურებით. აღნიშნულმა ინტერნეტ მიმართვამ გამოიწვია შიში საზოგადოებაში, რაც დაკვალიფიცირდება როგორც კიბერტერორიზმი, რადგან მან გამოიწვია მთლიანი მოსახლეობის დაშინება და გავრცელებული იყო კიბერსივრცის გამოყენებით.

3.2 კიბერდანაშაულთან ბრძოლის სისხლისსამართლებრივ ღონისძიებათა ანალიზი საერთაშორისო და ეროვნულ კანონმდებლობათა მიხედვით

კიბერ დანაშაულის საკითხების მთავარ მარეგულირებელ საერთაშორისო დოკუმენტს წარმოადგენს ევროპის საბჭოს 2001 წლის კონვენცია კიბერ დანაშაულის შესახებ, რომლის რატიფიცირებაც საქართველომ 2012 წელს მოახდინა. აღნიშნული დოკუმენტი განსაზღვრავს კიბერ სივრცეში ჩადენილ იმ მართლსაწინააღმდეგო ქმედებებს, რომლის დასჯადად გამოცხადება ევალება კონვენციის ყველა წევრ სახელმწიფოს. ამასთანავე, კონვენცია წევრ ქვეყნებს ავალდებულებს შექმნან კიბერ დანაშაულთან ბრძოლის შიდა ეროვნული სპეციალიზირებული დანაყოფები, რომლებიც ასევე შეასრულებენ 24/7 საერთაშორისო საკონტაქტო პუნქტის უფლებამოსილებებს. საქართველოში კიბერდანაშაულის დასჯადობის საკითხებს არეგულირებს სისხლის სამართლის კოდექსის (სსკ) XXXV თავი, რომლის თანახმადაც სისხლის სამართლის პასუხისმგებლობას იწვევს კიბერსივრცეში ჩადენილი შემდეგი ქმედებები: კომპიუტერულ სისტემაში უნებართვო შეღწევა (მუხ.284), კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება, კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა. აღნიშნულთან ერთად, დანაშაულს წარმოადგენს ბავშვთა პორნოგრაფიის ხელმისაწვდომობის უზრუნველყოფა ნებისმიერ ფორმით (მათ შორის ონლაინ), (სსკ– მუხ. 255, ნაწ.2), ინტელექტუალური საკუთრების უფლების დარღვევა და კიბერ საშუალებებით ჩადენილი ტერორიზმი. (სსკ. მუხ.324[1]).

გარდა ამისა, საქართველოში 2012 წელს მიღებულ იქნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“, რომელის მიზანია ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედებით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება-მოვალეობები ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები[37]. მისი მოქმედება ვრცელდება, ყველა იურიდიულ პირსა და სახელმწიფო ორგანოზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტები არიან. ხსენებული კანონის მოქმედება ასევე ვრცელდება ისეთ ორგანიზაციასა და უწყებაზე, რომლებიც კრიტიკული ინფორმაციული სისტემის სუბიექტს ექვემდებარებიან, ან ამ სუბიექტთან დაკავშირებული არიან დასაქმების, სტაჟირების, სახელშეკრულებო ან სხვა ურთიერთობით და რომლებიც უზუნველყოფენ ინფორმაციული აქტივის წვდომას ასეთი ურთიერთობის ფარგლებში[38].

სწორედ აღნიშნული საკანონმდებლო აქტის საფუძველზე, არსებობს „კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხა“, რომლის შედგენისას, მხედველობაში მიღებულ იქნა ისეთი კრიტერიუმები, როგორიცაა: ინფორმაციული სისტემის შეფერხების, ან მწყობრიდან გამსვლის სავარაუდო შედეგების სიმძიმე და მასშტაბი; სავარაუდო ეკონომიკური ზარალის სიმძიმე სუბიექტებისთვის ან/და სახელმწიფოსათვის; ინფორმაციული სისტემის მიერ გაწეული მომსახურების აუცილებლობა საზოგადოების ნორმალური ფუნქციონირებისათვის; ინფორმაციული სისტემის მომხმარებელთა რაოდენობა; სუბიექტის მატერიალური მდგომარეობა და სავარაუდო ხარჯების ოდენობა, რომლებიც მისთვის ხსენებული კანონიდან გამომდინარე ვალდებულებების დაკისრებას მოჰყვება.

მნიშვნელოვანია, რომ ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონის მოქმედება არ ვრცელდება მასმედიაზე, გამომცემლობათა რედაქციებზე, სამეცნიერო, საგანმანათლებლო, რელიგიურ დასაზოგადოებრივ ორგანიზაციებსა და პოლიტიკურ პარტიებზე, მიუხედავად

[37] საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“ მუხლი 1
[38] საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“

იმისა, თუ რამდენად მნიშვნელოვანია მათი საქმიანობა ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისულების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთის. მითითითებული საკანონმდებლო აქტის III თავი ეძღვნება კიბერუსაფრთხოების უზრუნველყოფას, მათ შორის კიბერუსაფრთხოების პრიორიტეტულ სააფრთხეების სახეებს, როგორიცაა:

- ✓ კიბერშეტევა, რომელიც საფრთხეს უქმნის ადამიანთა სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას;
- ✓ კიბერშეტევა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული სისტემების წინააღმდეგ;
- ✓ კიბერშეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურსებს ან/და საკუთრების უფლებას;
- ✓ სხვა ნებისმიერი ქმედება, რომელიც, მისი ხასიათიდან, მიზნიდან, წყაროდან, მოცულობიდან ან რაოდენობისან ამ მისი აღკვეთისთვის საჭირო რესურსების ოდენობიდან გამომდინარე, კრიტიკული ინფორმაციული

სისტემის ნორმალური ფუნციონირებისთვის საკმარისი საფრთხის შემცველია. თავის მხრივ, კანონი აკეთებს განმარტებას კიბერშეტევის შესახებ, კერძოდ კი, კიბერშეტევა არის ქმედება, როდესაც ელექტრონული მოწყობილობა, ან/და მასთან დაკავშირებული ქსელი, ან სისტემა გამოიყენება კრიტიკულ ინფორმაციულ სისტემაში შემავალი სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების, ან ინფორმაციის უკანონოდ მოპოვების გზით.

მსოფლიოს ქვეყნები ერთიანდებიან, რათა უფრო აქტიურად ებრძოლონ მსოფლიოში გავრცელებულ ტერორიზმს. ამ მხრივ არც კიბერტერორიზმის ფეროა განსხვავებული და მრავალი ქვეყანა აქტიურადაა ჩართული კიბერტერორიზმის წინააღმდეგ ბრძოლაში. 2001 წლის 23 ნოემბერს, ბუდაპეშტში მიიღეს კონვენცია, კომპიუტერული დანაშაულის შესახებ, რომლის რატიფიცირება საქართველომ 2012 წელს მოახდინა. კონვენცია წევრ ქვეყნებს ავალდებულებს, „მიიღოს ისეთი საჭირო საკანონმდებლო და სხვა

ზომები, რომლებიც ეროვნული კანონმდებლობით მოახდენს მთლიან კომპიუტერულ სისტემაზე ან მის ნაწილზე უნებართვო შეღწევის კრიმინალიზაციას, თუ ეს ქმედება წინასწარ განზრახვითაა ჩადენილი“[39].

ასევე ევროკავშირში შექმნილია ორგანო სახელწოდებით „საერთაშორისო მრავალმხრივი პარტნიორობა კიბერსაფრთხეების წინააღმდეგ“ (International Multilateral Partnership Against Cyber Threats), რომელიც შეიქმნა 2011 წელს და აერთიანებს ევროკავშირის წევრ ქვეყნებს.

შინაგან საქმეთა სამინისტრომ ასევე მნიშვნელოვანი ნაბიჯები გადადგა კიბერდანაშაულთან ბრძოლის მიმართულებით საკუთარი შესაძლებლობების ამაღლების მიზნით. 2008 – 2009 წლებში შსს ჩართული იყო ევროპის საბჭოსა და ევროპული კომისიის ერთობლივ პროექტში, რომელიც მიზნად ისახავდა კიბერდანაშაულის კონვენციასთან ქართული კანონმდებლობის ჰარმონიზაციას. აღნიშნული პროექტის ფარგლებში ცვლილებები შევიდა სისხლის სამართლის კოდექსში, სისხლის სამართლის საპროცესო კოდექსში, „ოპერატიული – სამძებრო საქმიანობის შესახებ“ და „ელექტრონული კომუნიკაციების შესახებ“ კანონებში.

2011 წლის მარტიდან შინაგან საქმეთა სამინისტრო ჩართულია აღმოსავლეთ პარტნიორობის ეგიდით მიმდინარე პროექტში „თანამშრომლობა კიბერდანაშაულის წინააღმდეგ“. აღნიშნული პროექტის მიზანი იყო ქართული სამართალდამცავი უწყებების შესაძლებლობების განვითარება კიბერდანაშაულთან ბრძოლის პროცესში.

2012 წლიდან ესტონეთის ხელისუფლების მხარდაჭერით ხორციელდება პროექტი, რომელიც ითვალისწინებს საქართველოს შინაგან საქმეთა სამინისტროს შესაძლებლობების ამაღლებას კიბერდანაშაულის გამოძიებისა და ციფრული მტკიცებულებების ამოღების მიმართულებით. მნიშვნელოვანია, რომ ევროპელი პარტნიორების გარდა, საქართველოს შინაგან საქმეთა

[39]იხ. ბოძაშვილილ. ნ, კორეხიძე „კიბერსივრცის სამართალი“, 2012 წ. (ნაშრომში გამოყენებული წიგნის ოფიციალური ელ - ვერსია გამოქვეყნებულია საიტზე www.lit.ge რომელშიც გვერდები მითითებული არ არის)

სამინისტრო ეფექტურად თანამშრომლობს აშშ გამოძიების ფედერალურ ბიუროსთან კიბერდანაშაულთან ბრძოლის სფეროში[40].

ამდენად, საქართველოში ისევე როგორც, მსოფლიოს სხვა მოწინავე სახელმწიფოებში, შექმნილია ინფორმაციული უსაფრთხოების პოლიტიკა, რომელიც ემსახურება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს. აღნიშნული კი, ამ კუთხით სასიცოცხლოდ მნიშვნელვანია, საერთაშორისო თანამშრომლობისთვის და შესაბამისად კიბერდანაშაულის კონტროლისა და პრევენციისთვის.

3. 3 2001 წლის 23 ნოემბრის კონვენცია კიბერდანაშაულის შესახებ

კიბერუსაფრთხოების სახელმწიფო პოლიტიკა (NCSS - National Cyber Security Strategy) არის საშუალება, რომელიც ემსახურება სახელმწიფოს ინფორმაციული სისტემებისა და მთლიანად ინფრასტრუქტურის უსაფრთხოებისა და სანდოობის გაზრდის შესაძლებლობას, რომელიც ამავდროულად მაქსიმალურად ამცირებს რისკებს. კიბერუსაფრთხოების სტრატეგიაში გამოიყენება პრობლემისადმი მაღალი დონის მიდგომა, კერძოდ: გამოიყოფა სახელმწიფოს მთელი რიგი მიზნები, ამოცანები და პრიორიტეტები, რომლებიც აუცილებელია მოცემული დროის მონაკვეთში მისაღწევად. ფაქტიურად, სტრატეგია ეს არის მოდელი, რომელიც საშუალებას იძლევა კიბერუსაფრთხოების საკითხების მოგვარებას ქვეყნის შიგნით[41].

2001 წლის 23 ნოემბერს ბუდაპეშტში ხელი მოეწერა კიბერდანაშაულთან ბრძოლის ევროპულ კონვენციას, რომელი ცძალაში შევიდა 2004 წლის 1 ივლისს. კონვენცია მომზადდა ევროპის საბჭოს ფარგლებში კანადის, შეერთებული შტატების, იაპონიისა და სამხრეთ აფრიკის რესპუბლიკის მონაწილეობით. დღესდღეისობით კონვენცია არის მოცემულ სფეროში ერთადერთი აღიარებული იურიდიული დოკუმენტი, რომელიც მიღებულია

[40] იხ. http://police.ge/ge/projects/kiberdanashauli/saertashoriso-tanamshromloba-kiber-danashaultan-brdzolashi

[41] იხ. /dea.gov.ge/uploads/legal_acts/1/monacemta%20gacvlis%20saaagento_geo.pdf

საერთაშორისო დონეზე და ის არის ღია ყველა დაინტერესებული ქვეყნისთვის, რომელიც კიბერდანაშაულის მთავარ მარეგულირებელ საერთაშორისო დოკუმენტს წარმოადგენს კონვენცია ხელმომწერ ქვეყნებს ავალდებულებს შექმნან სამართლებრივ - ნორმატიული ბაზა აუცილებელი კიბერდანაშაულის პრობლემის ეფექტური გადაწყვეტისთვის. ასევე ყველა ხელმომწერი ქვეყანათავის თავზე იღებს ერთმანეთისთვის დახმარების აღმოჩენას კიბერდამნაშავეთა სამართლებრივი დევნისა და ინციდენტების გამოძიების საკითხში. ევროპული კონვენცია არის ერთ - ერთი პირველი საერთაშორისო დოკუმენტი, სადაც განსაზღვრულია და კლასიფიცირებულია კიბერდანაშაული. კერძოდ, შემოსულია ინტერნეტსივრცეში არასანქცირებული შეღწევისა და რესურსების არაკანონიერი გადაჭერის განსაზღვრება, კომპიუტერულ სისტემებსა და ინფორმაციის მატარებელზე არაკანონიერი ჩარევა, მოწყობილობის არასამართლებრივი გამოყენება, კომპიუტერული მაქინაციები. კონვენციის მოქმედება ასევე ვრცელდება საბავშვო პორნოგრაფიასა და საავტორო უფლებების დარღვევაზე. დოკუმენტში განსაზღვრულია კომპიუტერული დანაშაულების ეფექტურიგამოძიების ინსტრუმენტები და მათთან ბრძოლა. კონვენციის მოქმედება ვდრცელდება ყველა დანაშაულზე, რომელიც ჩადენილიაკ ომპიუტერულ სისტემებში, ასევე ელექტრონული საშუალებებით შეგროვილი ნებისმიერი მტკიცებულებები[42]. დოკუმენტი განსაზღვრავს კიბერსივრცეში ჩადენილი მმართლსაწინააღმდეგო ქმედებებს, რომლის დასჯადად გამოცხადება ევალება კონვენციის ყველა წევრ ქვეყანას[43].

2001 წლის კონვენცია კიბერდანაშაულის არის პირველი საერთაშორისო ხელშეკრულება, რომელიც ეხება კომპიუტერული ქსელების მეშვეობით, განსაკუთრებით საავტორო უფლებების დარღვეევას, კომპიუტერთან დაკავშირებულ თაღლითობას და ქსელის უსაფრთხოების დარღვევას. იგი ასევე შეიცავს მთელი რიგ უფლებამოსილების დავალდებულებების მინიჭებას

[42] იხ. http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=1&CL=ENG

[43] პრეზიდენტის ბრძანებულება „კიბერდანაშაულის შესახებ“ კონვენციის დამტკიცების თაობაზე N 450

სახელმწიფოსთვის, კომპიუტერული დანაშაულის წინააღმდეგ ეფექტური ბრძოლის განხორციელებლად.

კონვენციის მთავარი ამოცანაა, განახორციელოს საერთო კრიმინალური პოლიტიკა, რომელიც მიზნად ისახავს საზოგადოების დაცვას კიბერდანაშაულისწინააღმდეგ, განსაკუთრებით შესაბამისი კანონმდებლობის მიღებისა და საერთაშორისო თანამშრომლობის ხელშეწყობით.

აღნიშნული კონვენციის ყველა მონაწილე სახელმწიფო ვალდებულია მიიღოს ისეთი საჭირო საკანონმდებლო და სხვა ზომები, რომლებიც ეროვნული კანონმდებლობით მოახდენს მთლიან კომპიუტერულ სისტემაზე ან მის ნაწილზე უნებართო შეღწევის კრიმინალიზაციას, თუ ეს ქმედება წინასწარ განზრახვითაა ჩადენილი. მონაწილე სახელმწიფომ შეიძლება მოითხოვოს, რომ დანაშაულის ჩადენის პირობად ჩაითვალოს უსაფრთხოების ზომების დარღვევა კომპიუტერული მონაცემების ან სხვა არაკეთილსინდისიერი განზრახვით, ან სხვა კომპიუტერულ სისტემასთან კავშირში, რომელიც შეერთებულია მეორე კომპიუტერულ სისტემასთან.

კონვენციის მონაწილე სახელმწიფოები ვალდებულები არიან მოახდინონ ეროვნული კანონმდებლობის დონეზე კომპიუტერული მონაცემების უნებართვოდ გამოყენების, დაზიანების წაშლის, გაუარესების კრიმინალიზაცია.

3. 4 2012 წლის საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ

2008 წლის აგვისტოს ომის დროს საქართველოზე განხორციელებულმა კიბერშეტევებმა დღის წესრიგში მწვავედ დააყენა მნიშვნელოვანი ინფორმაციული ინფრასტრუქტურების უსაფრთხოების საკითხი. დაიწყო შესაბამის საკანონმდებლო ბაზაზე მუშაობა. ერთ-ერთი საერთაშორისო ანალიტიკური ფონდის მონაცემებით კიბერშეტევა ჯერ კიდევ 2008 წლის 18 ივლისს დაფიქსირდა [44] , ხოლო 8 აგვისტოდან ფართო მასშტაბიანი

[44] იხ. http://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf.

ინტერნეტშეტევები განხორციელდა სამხრეთ ოსეთის სახელისუფლო და მედიასაიტებზე[45].

საქართველომ კიბერუსაფრთხოების პოლიტიკის განვითარების მიმართულებით გარკვეულ წარმატებებს მიაღწია. ეს გამოიხატებოდა კანონის „ინფორმაციული უსაფრთხოების შესახებ“, კიბერუსაფრთხოების სტრატეგიისა და სამოქმედო გეგმის დროულად შემუშავებასა და შესაბამისი სუბიექტების შექმნაში. კერძოდ, საქართველოს კიბერუსაფრთხოების პოლიტიკის უფრო დეტალურად განხილვისას აღმოვაჩენთ, რომ 2013 წლის მაისში გამოქვეყნდა საქართველოს კიბერუსაფრთხოების სტრატეგია, რომელიც წარმოადგენს „ეროვნული უსაფრთხოების მიმოხილვის“ პროცესის ფარგლებში შექმნილის კონცეპტუალური და სტრატეგიული დოკუმენტების პაკეტის ნაწილს. შესაბამისად, აღნიშნული სტრატეგია ეფუძნება „საქართველოს საფრთხეების შეფასების 2010 – 2013 წლების დოკუმენტს“ და „საქართველოს ეროვნული უსაფრთხოების კონცეფციას“. სტრატეგიაში ვკითხულობთ, რომ „საქართველოს კიბერუსაფრთხოების სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს სამოქმედო გეგმებს და ამოცანებს. სტრატეგიაზე დაყრდნობით, საქართველოს ხელისუფლება გაატარებს ღონისძიებებს, რომლებიც ხელს შეუწყობს სახელმწიფო ორგანოების, კერძო სექტორისა და სამოქალაქო საზოგადოების კიბერსივრცეში დაცულად ფუნქციონირებას, ელექტრონული ოპერაციების უსაფრთხო განხორციელებას და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებლად მოქმედებას“. სტრატეგიის მთავარი მიზანია კიბერსივრცის ან სხვა ქმედებების საზიანო შედეგები და რისკები მაქსიმალურად იქნას შემცირებული და უმოკლეს დროში მოხდეს დაზიანებული ინფორმაციული ინფრასტრუქტურის სრული აღდგენა. ყოველივე ამას ემატება კრიტიკული

[45] იხ. http://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf

ინფორმაციული სისტემების მდგრადობისა და დაცულობის ამაღლება, ასევე დროულიპ რევენცია[46].

კანონი საქართველოს ინფორმაციული უსაფრთხოების გარემოში რადიკალური ცვლილებების საფუძველი გახდა. მისი მთავარი თემა ე.წ. კრიტიკული ინფორმაციული ინფრასტრუქტურადამისი დაცვა. თავის მხრივ კიკრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხაში შედიან მხოლოდ სამთავრობო დაწესებულებები.

ინფორმაციული უსაფრთხოების მხრივ, სამოქალაქო და სამხედრო სფეროები გაყოფილი უნდა იყოს. კომპეტენციათა აღრევამ, შესაძლოა, სამართლებრივი პრობლემები გამოიწვიოს. თუ სამოქალაქო ობიექტებზე კიბერთავდასხმა ხორციელდება და მათ სამხედრო უწყება პასუხობს, ეს, შესაძლოა, სამხედრო აგრესიად ჩაითვალოს – კიბერუსაფრთხოების მხრივ საერთაშორისო სამართლის აქტების სიმწირე მრავალფეროვანი ინტერპრეტაციის საშუალება იძლევა. თეორიული სამართლებრივი პრობლემების წარმოშობა სამოქალაქო და სამხედრო კიბერსფეროების გამიჯვნის ერთადერთი მიზეზი არ არის. ინფორმაციული უსაფრთხოების მენეჯმენტისა და კონკრეტულ საფრთხეებზე პასუხისთვისაც დომენების გაყოფა უფრო ეფექტურია[47].

ამგვარად, საქართველომ ხსენებული კანონის მიღებით შექმნა ინფორმაციული უსაფრთხოების გარკვეული პოლიტიკა, რომელიც ემსახურება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის საფეროში დადგენილ საერთაშორისო სტანდარტებს.

3.5 ა.შ.შ. კიბერტერორიზმის წინააღმდეგ

აშშ-ს კიბერტერორიზმის ერთ-ერთი წამყვანი ექსპერტი, ჯორჯთაუნის პროფესორი დოროთი დენინგი ინტერნეტში საქმიანობის კლასიფიკაციის სამ ასპექტს გამოყოფს:[48]

[46] იხ. http://www.dcaf.ch/Project/Horizon-2015
[47] იხ. http://www.first.org/
[48] Dorothy E.Denning, “Activism,Hacktivism, and Cyberterrorissm: The Internet as a tool for influencing foreing policy”, chapter eight

✓ **აქტივიზმი** - კიბერსივრცის ლეგიტიმური, ნორმალური, კანონიერი გამოყენება საკუთარი იდეების პროპაგანდისა თუ სხვა ღონისძიებების განხორციელების მიზნით, რომელიც მოიცავს ინფორმაციის მოძიებას, ვებ გვერდებზე განთავსებას, ელ-პუბლიკაციების გავრცელებას, ინტერნეტ რესურსების გამოყენებას.

✓ **ჰაქტივიზმი** - აქტივიზმისა და ჰაკერობის ნაზავი. იგი მოიცავს უკანონო კიბერ ოპერაციებს, რომელთა დროს გამოიყენება ჰაკერული ტექნიკა სამიზნეების (ძირითადად ვებ გვერდების) წინააღმდეგ. მისი მიზანია საიტების ნორმალური ფუნქციონირების ხელის შეშლა და არა დამანგრეველი ზიანის მიყენება. ანუ ამ შემთხვევაში საქმე გვაქვს კიბერდანაშაულთან და არა კიბერტერორიზმთან

✓ **კიბერტერორი** - ტერორიზმისა და კიბერსივრცის შერწყმა. ის მოიცავს პოლიტიკურად მოტივირებულ ჰაკერულ შეტევებს, რომელთა მიზანია დამანგრეველი შედეგების მიღწევა: სახელმწიფო ეკონომიკის მოშლა, სახელმწიფო სტრუქტურების სერვერებზე შეტევა, ისეთი ინფორმაციის გავრცელება, რომელიც ზიანს მიაყენებს მთლიანად საზოგადოებას, დათესავს შიშს და პანიკას.

ამერიკის შეერთებული შტატები შეიძლება ითქვას N1 მებრძოლი სახელმწიფოა ზოგადად ტერორიზმის წინააღმდეგ. 2001 წლის ტერაქტების შემდეგ კიდევ უფრო გაამძაფრა ბრძოლა ა.შ.შ.-ს სახელმწიფომ. გამოძიების ფედერალური ბიუროს განცხადებით ტერორიზმი შტატებისთვის წარმოადგენს მთავარ საფრთხეს. შესაბამისად მათ გაატარეს მთელი რიგი ღონისძიებები სახელმწიფოს თავდაცვის უნარიანობის გაზრდისათვის, შეიმუშავეს გეგმები მის წინააღმდეგ საბრძოლველად. აღნიშნულიდან გამომდინარე მნიშვნელოვანია ა.შ.შ.-ს გამოცდილების გააზრება, გაზიარება და შემდგომი განვითარება, დახვეწა, რათა უფრო ეფექტური და შედეგიანი იყოს კიბერტერორიზმის წინააღმდეგ ბრძოლა.

ზემოთ თქმულიდან გამომდინარე, ტერორიზმის წინააღმდეგ ბრძოლა ავტომატურად გულისხმობს მისი ერთ-ერთი სახის - კიბერტერორიზმის

წინააღმდეგ ბრძოლასაც. ა.შ.შ.-ში კიბერსივრცეს, ტერორიზმის კუთხით, დიდ მნიშვნელობას ანიჭებდნენ ჯერ კიდევ გასული საუკუნის მიწურულს. პრეზიდენტი კლინტონი და შემდგომ ჯორჯ ბუში, 2001 წლის ტერაქტებამდეც დიდ ყურადღებას აქცევდნენ კიბერუსაფრთხოებას და მის მნიშვნელობაზე საუბრობდნენ სხვადასხვა მოხსენებებში, როგორც კონგრესის წინაშე აგრეთვე წინასაარჩევნო კამპანიის წარმოებისას. 2014 წელს კი ობამამ განაცხადა, რომ კიბერტერორიზმი არის ქვეყნის ყველაზე დიდი პრობლემა.

2001 წლის 9/11-ის შემდგომ, ტერორიზმის საფრთხის გაზრდის გამო კიდევ უფრო გამძაფრდა ბრძოლა კიბერტერორიზმის წინააღმდეგ. შეიქმნა სხვადასხვა პროგრამები და მიიღეს ახალი კანონმდებლობა. თეთრ სახლში დაარსდა კიბერ სივრცის უსაფრთხოების ოფისი, ხოლო საკანონმდებლო დონეზე მიიღეს 2001 წლის „პატრიოტის აქტის“ 814-ე სექცია, რომელიც შეეხება კიბერტერორიზმს. 2003 წელს კი შეიმუშავეს „კიბერუსაფრთხოების სტრატეგია,“ რომელიც განახლდა 2011 წელს.

3.6 ევროპის ქვეყნები კიბერტერორიზმის წინააღმდეგ

ევროპის ქვეყნები დღეს განსაკუთრებული საფრთხის წინაშე აღმოჩნდნენ ტერორიზმთან მიმართებაში, რასაც ბოლო დროს განვითარებული მოვლენები ადასტურებს. 2015 წლის პარიზის ტერაქტებმა მთელი მსოფლიო შეძრა. ერაყიდან და სირიიდან წამოსულმა მიგრანტებმა საფრთხე კიდევ უფრო გაზარდეს, რადგან სავარაუდოა, რომ მათ რიგებში შეიძლება ბევრი ტერორისტია, რომლებიც შემდგომ ტერორისტულ აქტებს განახორციელებენ ევროპის კონტინენტზე. 2015 წლის 13 ნოემბრის პარიზის ტერაქტების შემდეგ ტერორიზმის საშიშროების უმაღლესი დონე თითქმის 1 თვის განმავლობაში შენარჩუნებული იყო ბელგიის დედაქალაქში. რამდენიმე დღის განმავლობაში პარალიზებული იყო მეტრო, სკოლები, ცენტრალური ქუჩები. ძებნა იყო გამოცხადებული 10 მდე ადამიანზე. აღნიშნულიდან გამომდინარე ევროპის ქვეყნებს მართებს მეტი სიფრთხილე და მნიშვნელოვანი ღონისძიებების

გატარება ტერორიზმის წინააღმდეგ, მათ შორის რა თქმა უნდა კიბერტერორიზმის კუთხითაც.

ევროპამ კიბერტერორიზმის წინააღმდეგ საბრძოლველად აქტიური მოქმედებები რეალურად 2005 წლიდან დაიწყო, როდესაც ევროპის საბჭომ მიიღო ვარშავის 16 მაისის კონვენცია ტერორიზმის აღკვეთის შესახებ. 2006 წლიდან ევროპის საბჭოს პრიორიტეტად განისაზღვრა კიბერტერორიზმის პრობლემა და მსჯელობის საგანი გახდა ექსპერტთა კომიტეტისთვის (CODEXTER58). 2007 წელს კი შეიქმნა მონაცემთა ბაზა კიბერტერორიზმის შესახებ. ზემოთ აღნიშნული მოქმედებების განხორციელების მიუხედავად დღეს აშკარაა, რომ ევროპის ქვეყნებს კიდევ უფრო მეტი აქვს გასაკეთებელი კიბერტერორიზმის წინააღმდეგ საბრძოლველად, რადგან კიბერ სივრცეს არ აქვს საზღვრები და უფრო დიდ პრობლემას წარმოადგენს სახელმწიფოებისთვის, საზოგადოების უსაფრთხოებისათვის და მნიშვნელოვანი ინფრასტრუქტურის დაცვისთვის.

3.7ექსპერტთა კომიტეტი

ექსპერტთა კომიტეტი ტერორიზმის შესახებ (Committee of Experts on Terrorism - CODEXTER) არის მთავრობათაშორისი ექსპერტთა კომიტეტი, რომელიც შეიქმნა 2003 წელს ევროპის საბჭოს მინისტრთა კომიტეტის მიერ, ტერორიზმის წინააღმდეგ მიმართული ქმედებების კოორდინაციისათვის. CODEXTER-ი ატარებს პლენარულ სხდომებს წელიწადში ორჯერ, რომელშიც მონაწილეობენ ექსპერტები ევროპის საბჭოს წევრი ქვეყნებიდან და საერთაშორისო ორგანიზაციების წარმომადგენლები. მათ შეიმუშავეს ევროპის საბჭოს 1977 წლის 27 იანვრის კონვენცია ტერორიზმის პრევენციის შესახებ.[49]
ევროპის საბჭო ანვითარებს სამართლებრივ სტანდარტებს ტერორისტული აქტების პრევენციისა და აღკვეთისათვის, ადამიანის უფლებებისა და კანონის უზენაესობის დაცვითა და პატივისცემით. საბჭო აგრძელებს მუშაობას, რომ გაზარდოს საერთაშორისო თანამშრომლობა ტერორიზმის წინააღმდეგ.

[49] http://www.coe.int/t/dlapil/codexter/about_en.asp

ევროპის საბჭო ანვითარებს სამართლებრივ სტანდარტებს ტერორისტული აქტების პრევენციისა და აღკვეთისათვის, ადამიანის უფლებებისა და კანონის უზენაესობის დაცვითა და პატივისცემით. საბჭო აგრძელებს მუშაობას, რომ გაზარდოს საერთაშორისო თანამშრომლობა ტერორიზმის წინააღმდეგ.

2014-2015 წლებისთვის, კომიტეტმა დაადგინა 4 პრიორიტეტი:

1. სპეციალური საგამოძიებო ტექნიკა
2. რადიკალიზმი, უცხოელი ტერორისტები და მათი მომზადების შესახებ ინფორმაცია.
3. მარტო მოქმედი ტერორისტები
4. საკანონმდებლო ბაზის ხარვეზები და საერთაშორისო სამართლებრივი ინსტრუმენტები.

2015 წლის 22 ოქტომბერს ევროპის საბჭოს მიერ მიღებული იქნა დამატებითი ოქმი ტერორიზმის აღკვეთისა და პრევენციისათვის, რომელშიც გაწერილია გეგმა, თუ როგორ უნდა ებრძოლონ ექსტრემიზმს და რადიკალიზმს.

3.8 მონაცემთა ბაზა

კიბერტერორიზმის მონაცემთა ბაზა შეიცავს სახელმწიფოთა წვლილს, რომელიც წარდგენილია ექსპერტთა კომიტეტის (CODEXTER) მიმართ. აღნიშნულ ბაზაში წარმოდგენილია 32 ქვეყანა და მათი ხედვები კიბერტერორიზმის წინააღმდეგ ბრძოლაში. მათ შორის ერთ-ერთია საქართველო[50]

ექსპერტთა კომიტეტის მიერ სახელმწიფოების მიმართ დასმულია შემდეგი 5 კატეგორიის კითხვა:

ა) ეროვნული პოლიტიკა - არის თუ არა შემუშავებული ეროვნული პოლიტიკა კიბერდანაშაულისა და კიბერტერორიზმის შესახებ?

ბ) სამართლებრივი ჩარჩო - არის თუ არა დასჯადი კიბერსივრცის გამოყენება ტერორისტული მიზნებისთვის და თუ არის რა სახის (ადმინისტრაციული, სისხლისსამართლებრივი თუ სამოქალაქო სამართლებრივი)?

[50] ი.ხ http://www.coe.int/t/dlapil/codexter/cyberterrorism_db.asp

გ) საერთაშორისო თანამშრომლობა - აღწერილი უნდა იყოს სახელმწიფოს მიერ ზოგადი ხედვა საერთაშორისო თანამშრომლობასთან დაკავშირებით.

დ) ინსტიტუციური ჩარჩო - სახელმწიფოს მიერ ჩამოთვლილი უნდა იყოს დაწესებულებები, რომლებიც ახორციელებენ ბრძოლას კიბერტერორიზმის წინააღმდეგ.

ე) სტატისტიკური ინფორმაცია -იმ დანაშაულების სტატისტიკური აღწერა, რომელიც განხორციელდა კიბერსივრცის გამოყენებით.

3.9 საქართველო კიბერტერორიზმის წინააღმდეგ

საქართველო დღეს განსაკუთრებით დიდი პრობლემის წინაშე აღმოჩნდა ზოგადად ტერორიზმის კუთხით. ჯერ კიდევ დამოუკიდებლობის გამოცხადებისთანავე „ქვეყნის სპეციფიკიდან გამომდინარე გამოიკვეთა ორი საფრთხე: ერთი - საერთაშორისო ტერორიზმი და მეორე- ეთნიკური ტერორიზმი. პირველ მათგანს განაპირობებდა ჩვენი ქვეყნის გეოგრაფიული მდებარეობა, მეორეს კი - მემკვიდრეობით მიღებული საბჭოური ნაციონალური პოლიტიკის მიერ ღრმად „ჩამარხული“ ნაღმები.“[51]

ზემოთ აღნიშნულ პრობლემას 21-ე საუკუნეში მიემატა ახალი პრობლემა ტერორიზმის კუთხით - კიბერტერორიზმი. ტერორიზმის აღნიშნული მეთოდით ბრძოლა სახელმწიფოების წინააღმდეგ ეფექტური იარაღია ნებისმიერი ტერორისტისათვის, რადგან კიბერსივრცეს არ გააჩნია საზღვრები და შეიძლება ინტერნეტით ისეთი ინფორმაციის გავრცელება, რომელიც საზოგადოების თითოელ წევრამდე მიაღწევს და დასთესს შიშისა და დაუცველობის გრძნობას. აღნიშნულ მეთოდს აგრეთვე იყენებენ საქართველოს მოქალაქეობის მქონე ტერორისტები, რომლებიც ისლამური ხალიფატის რიგებში იბრძვიან რელიგიური მოტივებით. ისინი ავრცელებენ ძალადობისა და მუქარის შემცველ ინფორმაციებს, რომელიც ნერგავს შიშს საზოგადოებაში.

კიბერტერორიზმის წინააღმდეგ ბრძოლაში საქართველო აქტიურად არის ჩართული:

[51] ჯ. გახოკიძე - „ეროვნული უსაფრთხოების ძირითადი პრობლემები“, თბილისი 2007 წელი, გვ.172

1. 2006 წელს საქართველოს სისხლის სამართლის კოდექსში შევიდა ცვლილება კიბერტერორიზმის შესახებ;

2. 2012 წელს მიღებული იქნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“;

3. თანამშრომლობა საერთაშორისო ორგანიზაციებთან;

4. 2015 წელს თავდაცვის მინისტრმა მიიღო გადაწყვეტილება კიბერრეზერვის შექმნის შესახებ, რომლის მიზანიც იქნება კიბერტერორიზმისგან სახელმწიფოს დაცვა.

საქართველოს სისხლის სამართლის კოდექსში 2006 წელს, ტერორიზმის თავში შესული ცვლილების, 324^1 მუხლის მიხედვით:

1. კიბერტერორიზმი, ესე იგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას და ხელყოფს საზოგადოებრივ უსაფრთხოებას, სახელმწიფოს სტრატეგიულ, პოლიტიკურ ან ეკონომიკურ ინტერესს, ჩადენილი მოსახლეობის დაშინების ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით ისჯება თავისუფლების აღკვეთით ვადით ათიდან თხუთმეტ წლამდე.

2. იგივე ქმედება, რამაც ადამიანის სიცოცხლის მოსპობა ან სხვა მძიმე შედეგი გამოიწვია, – ისჯება თავისუფლების აღკვეთით ვადით თორმეტიდან ოც წლამდე ან უვადო თავისუფლების აღკვეთით.

შენიშვნა: ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ლიკვიდაციით ან საქმიანობის უფლების ჩამორთმევით და ჯარიმით“[52]. თუმცა ამ შემთხვევაში გამოყოფოლია მიზანი: უნდა არსებობდეს ტერორისტული საქმიანობის განხორციელების აშკარა, პირდაპირი დაარსებითი საფრთხე. რაც რეალურად პრობლემას წარმოადგენს, რადგან თუ პირს აქვს ტერორისტული იდეები და ამას საჯაროდ აცხადებს, თან ქადაგებს და მოუწოდებს სხვებსაც ჩაერთონ ტერორიზმში, გამოდის, რომ სამართალდამცავებს არ შეუძლიათ იმოქმედონ ამ მუხლის მიხედვით, თუ არ

[52] საქართველოს სისხლის სამართლის კოდექსი, მუხლი 324^1

არსებობს ტერორისტული საქმიანობის განხორციელების აშკარა, პირდაპირი და არსებითი საფრთხე. რამაც რეალურად დღეს სავალალო მდგომარეობა შექმნა. მაგალითისათვის: ერთ-ერთი აჭარელი მუსლიმი ჯერ კიდევ საქართველოში ყოფნის პერიოდში აქტიურად ავრცელებდა ინტერნეტში მიმართვებს, რომელიც შეიცავდა ძალადობას და მუქარას ქართველი ქრისტიანების მიმართ. სამართალდამცავებს მის მიმართ არ გაუტარებიათ არანაირი ღონისძიება და დღეს ის ისლამური ხალიფატის რიგებში იბრძვის.

ყოველივე ზემოთ აღნიშნულიდან გამომდინარე, საჭიროა კანონმდებლობის დახვეწა, რათა უფრო ეფექტურად და დროულად ვებრძოლოთ აღნიშნულ დანაშაულს. მნიშვნელოვანია კიბერტერორიზმის წინააღმდეგ ბრძოლაში მოწინავე სახელმწიფოების გამოცდილების გაზიარება, მათი კანონმდებლობის განხილვა და ქართულ რეალობაზე მორგება.

რეკომენდაციები:

კიბერტერორიზმის წინააღმდეგ საბრძოლველად მნიშვნელოვანია მთელი რიგი ღონისძიებების გატარება. რადგან კიბერტერორიზმი ხორციელდება კიბერ სივრცეში, რომელსაც არ გააჩნია საზღვრები, კიდევ უფრო ართულებს მასთან ბრძოლას. მნიშვნელოვანია განისაზღვროს მასთან ბრძოლის ხერხები და მათი ერთობლივად გამოყენების ეფექტურობის განსაზღვრა. საერთაშორისო პრაქტიკიდან გამომდინარე, რომელიც განვიხილე კიბერტერორიზმის თავში, ქვემოთ შემოგთავაზებთ რამდენიმე რეკომენდაციას, რომელიც ჩემი აზრით უმნიშვნელოვანესია, რათა დროულად და ეფექტურად მოხდეს კიბერტერორიზმის აღკვეთა:

- ✓ **კანონმდებლობა** - პირველ რიგში მნიშვნელოვანია საკანონმდებლო ბაზის სრულყოფა, რათა სამართალდამცავებმა კანონის ფარგლებში, დროულად და ეფექტურად მოახდინონ კიბერტერორიზმის წინააღმდეგ ბრძოლა. რადგან კიბერ სივრცესთან გვაქვს საქმე, რომელსაც არ გააჩნია საზღვრები, მნიშვნელოვანია, რომ სხვადასხვა ქვეყნის სამართალდამცავ ორგანოებს ჰქონდეთ უფრო თავისუფალი მოქმედების საშუალება ერთმანეთის კონტროლირებად ტერიტორიებზე.

✓ **საზოგადოების თვითშეგნების ამაღლება** - აღნიშნული საკითხი საკმაოდ გრძელვადიანია და შეიძლება რამდენიმე თაობის გამოცვლაც დაჭირდეს. მნიშვნელოვანია ისეთი ღონისძიებების გატარება, რომელიც მიმართული იქნება საზოგადოების სხვადასხვა ფენების მოქალაქეობრივი თვითშეგნების ასამაღლებლად. აღნიშნული მეთოდი არა მხოლოდ კიბერტერორიზმის, არამედ ზოგადად ტერორიზმის წინააღმდეგ საბრძოლველად არის მნიშვნელოვანი. საჭიროა ლექციების ჩატარება საზოგადოების ისეთი ნაწილისათვის, რომელიც სახელმწიფოში წარმოადგენს უმცირესობას და მათგან შეიძლება წამოვიდეს ტერორიზმის საფრთხე. ასეთია დღეს საქართველოში წარმოდგენილი მუსლიმების ნაწილი, რომელთაგან ხალხი მიდის ისლამურ ხალიფატში საბრძოლველად. ხდება მათი გადაბირება არასწორი აზროვნების შედეგად. ჰგონიათ, რომ საქართველოში ქრისტიანები მათ დაჩაგვრას ცდილობენ და შურისძიების მიზნით ეწერებიან ისლამური ხალიფატის რიგებში. მნიშვნელოვანია ასეთი ხალხის გათვიცნობიერება, მოქალაქეობრივი თვითშეგნების ამაღლება, რათა მიხვდნენ, თუ რაიმე პრობლემა შეექმნებათ, მიმართონ სახელმწიფო აპარატებს და არაძალადობრივი გზებით მოაგვარონ მათი პრობლემები. აგრეთვე გააცნობიერონ თუ რა საშინელებაა ტერორიზმი.

✓ **კომპიუტერული** სისტემის დაცვა - კომპიუტერული უსაფრთხოების დაცვა შესაბამისი პროგრამების მეშვეობით. აღნიშნულთან დაკავშირებით მნიშვნელოვანია მაღალი დონის IT სპეციალისტების მომზადება, რომლებიც დროულად და ეფექტურად შეძლებენ კიბერშეტევის განხორციელების შემთხვევაში დაზიანებული სისტემის აღდგენას. აგრეთვე ისინი ყოველდღიურად უნდა ხვეწდნენ დაცვის სისტემებს, რათა კიბერტერორისტებს გაურთულდეთ ან საერთოდ ვეღარ გატეხონ სახელმწიფო აპარატის კიბერ ბაზები, რომელიც სახელმწიფოსთვის მნიშვნელოვან ინფორმაციებს ინახავს.

✓ **სამართალდამცავი ორგანოების ჩართვა** - კიბერტერორიზმი არ არის მხოლოდ თავდაცვის სამინისტროს ან საქართველოს უსაფრთხოების სამსახურის გადასაჭრელი პრობლემა. აღნიშნულ დანაშაულთან ბრძოლაში

შესაძლებელია თითოეული სტრუქტურის ჩართვა. მაგალითად რაიონული განყოფილებები აქტიურად უნდა იყოს ჩართული ზოგადად ტერორიზმის წინააღმდეგ ბრძოლაში. უბნის ინსპექტორს უნდა ჰქონდეს ამომწურავი ინფორმაცია მის უბანში მცხოვრებ პირებზე. შესაბამისად მას ექნება ინფორმაცია ისეთი ადამიანის შესახებ, რომელსაც რადიკალური შეხედულებები აქვს და იხრება ტერორიზმისაკენ. შესაბამისად შეიძლება პრევენციული ღონისძიებების გატარება ასეთი პიროვნების გამოვლენის შემთხვევაში.

3.10 საერთაშორისო თანამშრომლობა

კიბერდანაშაული ხორციელდება კიბერ სივრცის გამოყენებით, რაც ზრდის აღნიშნული დანაშაულებრივი ქმედების ჩამდენის მოქმედების ფარგლებს. აღნიშნულიდან გამომდინარე კიბერდანაშაული არ არის ერთი რომელიმე ქვეყნის პრობლემა, არამედ მთელი მსოფლიოს პრობლემაა. ამიტომ მნიშვნელოვანია საერთაშორისო თანამშრომლობის კიდევ უფრო გააქტიურება. პირველი ნაბიჯები საერთაშორისო თანამშრომლობისათვის კიბერდანაშაულის წინააღმდეგ ბრძოლაში გადაიდგა 2001 წელს, როდესაც მიიღეს ევროპის საბჭოს კონვენცია „კიბერდანაშაულის შესახებ“.

ევროპის საბჭოს 2001 წლის „კიბერდანაშაულის შესახებ“ კონვენციის მე-3 თავი ეხება საერთაშორისო თანამშრომლობას. აღნიშნული კონვენციის 23-ე მუხლის მიხედვით ხელმომწერი სახელმწიფოები ვალდებული არიან კომპიუტერულ სისტემებსა და მონაცემებთან დაკავშირებულ დანაშულთა გამოძიებისა და დევნის, აგრეთე დანაშაულთან კავშირში მტკიცებულებათა ელექტრონული ფორმით შეგროვების მიზნით, ფართოდ ითანაშმრომლონ ერთმანეთთან. კონვენციის მე-3 თავი განსაზღვრავს შემდეგ ვალდებულებებს სახელმწიფოების მიმართ:

- ✓ ექსტრადიციის შემთხვევაში შესაბამისი მოქმედებების გატარების წესი მონაწილე სახელმწიფოებს შორის;
- ✓ ორმხრივ დახმარებასთან დაკავშირებული პრინციპები;

✓ ინფორმაციის გაზიარება სახელმწიფოებს შორის. აღნიშნული მდგომარეობს შემდეგში: ერთ სახელმწიფოს შეუძლია მეორეს გაუზიაროს ისეთი ინფორმაცია, რომელიც შეიძლება არ მოუთხოვია მეორე სახელმწიფოს, მაგრამ ინფორმაციის გამცემი სახელმწიფო თვლის, რომ შეიძლება დაეხმაროს აღნიშნული მასალები სხვა სახელმწიფოს;

✓ საერთაშორისო ხელშეკრულებათა არარსებობის შემთხვევაში ორმხრივი დახმარების მოთხოვნა და შესაბამისი პროცედურები;

✓ კომპიუტერულ მონაცემთა შენახვა, დაჩქარებული დაცვა და გადაცემა;

✓ სადღეღამისო/მუდმივი ქსელის ფუნქციონირება. ყველა წევრი სახელმწიფო ვალდებულია, დანიშნოს საკონტაქტო პირი, რომელთან დაკავშირებაც შესაძლებელი იქნება 24 საათის განმავლობაში, კვირაში 7 დღე. რათა უზრუნველყოფილი იქნეს კომპიუტერულ სისტემებსა და მონაცემებთნ დაკავშირებულ დანაშაულთა გამოძიება ან დევნა, ან მტკიცებულებების ელექტრონული ფორმით შეგროვებისთვის საჭირო შესაბამისი დახმარების გაწევა. საქართველომ აღნიშნული კონვენციის რატიფიცირება მოახდინა 2012 წელს, რის შედეგადაც ავიღეთ ვალდებულება მოგვეხდინა ზემოთ ჩამოთვლილი და სხვა ვალდებულებების შესრულება. ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო, რომელიც ახორციელებს კონვენციით დაკისრებულ ვალდებულებებს, მასვე დაევალა 24/7 მუდმივი ქსელის შესრულების ფუნქცია. [53] აგრეთვე ჩამოყალიბდა კომპიუტერულ-ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც ახორციელებს უშუალოდ ციფრული მტკიცებულებების პირველად მოპყრობასა და მათ შემდგომ ექსპერტიზას.

ევროპოლი გვთავაზობს საერთაშორისო თანამშრომლობის პრინციპებს:[54]

✓ **ოპერატიული თანამშრომლობა** - მოიცავს შესაბამის მოქმედებებს, რომელიც უნდა გაატარონ მოკავშირე სახელმწიფოების სამართალდამცავმა ორგანოებმა.

[53] საქართველოს მთავარი პროკურატურა, ანალიტიკური სამმართველო, "ინფორმაცია კიბერდანაშაულის შესახებ", გვ. 10

[54] https://www.gccs2015.com/sites/default/files/documents/GCCS2015_discussion_paper_on_improving_international_cooperation.pdf

აღნიშნულში იგულისხმება შეთანხმებული კოორდინაცია, ინფორმაციის გაცვლა და შესაბამისი სამართლებრივი რეგულირება.

✓ სტრატეგიული თანამშრომლობა - პოლიტიკური რეგულირება სახელმწიფოების მიერ, შესაბამისი პრევენციული ღონისძიებების გატარება, სასწავლო ღონისძიებების განხორციელება, პრობლემების კვლევა და შემდგომი განვითარება

✓ პარტნიორობა - წევრი და მოკავშირე სახელმწიფოების სამართალდამცავი ორგანოების კოორდინაცია კიბერდანაშაულის წინააღმდეგ ბრძოლაში. რადგან კიბერ სივრცეს არ გააჩნია საზღვრები, ევროპოლი ვერ შემოიფარგლება მხოლოდ ევროპის ქვეყნებით, მნიშვნელოვანია სხვა სახელმწიფოთა სამართალდამცავებთან მჭიდრო კავშირი

კიბერდანაშაულის წინააღმდეგ ბრძოლაში აქტიურად არის ჩართული ინტერპოლი - კრიმინალური პოლიციის საერთაშორისო ორგანიზაცია. ინტერპოლის წევრია 120 ქვეყნის ოფიციალური საპოლიციო ორგანოები. 67 აღნიშნულიდან გამომდინარე მნიშვნელოვანია ინტერპოლის წევრ სახელმწიფოებთან აქტიური თანამშრომლობა კიბერდანაშაულის წინააღმდეგ ბრძოლაში და ერთიანი სამოქმედო გეგმის შემუშავება, რადგან კიბერდანაშაული თითოეული სახელმწიფოსთვის თანაბარმნიშვნელობითი უნდა იყოს, კიბერ სივრცის ფართო საზღვრებიდან გამომდინარე.

2014 წელს ინტერპოლმა ჩამოაყალიბა ინოვაციების გლობალური კომპლექსი სინგაპურში, რომლის მიზანიც არის ხელი შეუწყოს საერთაშორისო თანამშრომლობას კიბერდანაშაულის წინააღმდეგ ბრძოლაში. აღნიშნულ კომპლექსში სამუშაოდ ინტერპოლი იწვევს ინტერნეტ უსაფრთხოების სპეციალისტებს, მათი გამოცდილებიდან გამომდინარე, რათა თანამედროვე მიღწევების გამოყენებით და მაღალი ცოდნით ეფექტურად ებრძოლონ კიბერდანაშაულს[55]. საქართველო ინტერპოლის წევრია 1993 წლიდან. დღეს საქართველოს ინტერპოლის ეროვნული ცენტრალური ბიურო აქტიურად თანამშრომლობს ინტერპოლის გენერალურ სამდივნოსთან. ძირითადად

[55] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

თანამშრომლობა მოიცავს სამართალდამრღვევების წინააღმდეგ გატარებულ ღონისძიებებს, შესაბამის ცირკულარზე დასმის კუთხით.

რეკომენდაციები:

- ✓ მნიშვნელოვანია, რომ გარდა ინტერპოლის საქართველოს ეროვნული ცენტრალური ბიუროსა, ინტერპოლთან ურთიერთობაში აქტიურად იყოს ჩართული ცენტრალური კრიმინალური პოლიციის კიბერდანაშაულთან ბრძოლის სამმართველო, რათა სამართალდამცავებმა მიიღონ შესაბამისი ცოდნა და გამოცდილება, აგრეთვე საკუთარი გამოცდილება გაუზიარონ სხვა ქვეყნის წარმომადგენლებს.
- ✓ ჩვენმა სამართალდამცავებმა უნდა მიიღონ აქტიური მონაწილეობა ნებისმიერ ღონისძიებაში, რომელიც ჩატარებული იქნება რომელიმე საერთაშორისო ორგანიზაციის მიერ კიბერდანაშაულის წინააღმდეგ ბრძოლაში.
- ✓ მიუხედავად იმისა, რომ კიბერ სივრცეს არ გააჩნია საზღვრები და კიბერდანაშაული თითოეული ქვეყნის პრობლემაა და ყველამ ერთად უნდა ებრძოლოს, ჩემი აზრით მაინც მნიშვნელოვანია, რომ რეგიონალურ დონეზე თანამშრომლობა ცალკე საფეხურზე განვიხილოთ. ანუ შეიძლება ჩვენს მეზობელ სახელმწიფოებთან ერთად ცალკე გავატაროთ სხვადასხვა ღონისძიებები კიბერდანაშაულის წინააღმდეგ ბრძოლაში. ძირითადად აზერბაიჯანთან და თურქეთთან, რომლებიც დღეს ჩვენი სტრატეგიული პარტნიორებია.
- ✓ **კიბერტერორიზმის** კუთხით საერთაშორისო თანამშრომლობა კიდევ უფრო მნიშვნელოვანია, რადგან როგორც კიბერ სივრცეს, ისე ტერორიზმს არ გააჩნია საზღვრები და თითოეული ქვეყნის პრობლემაა. ტერორისტები თავისუფლადმოქმედებენ, სახელმწიფოების წარმომადგენლებს კი არ აქვთ დაშვება ერთმანეთის სისტემაზე, ამიტომ უფრო რთულად არის საქმე და რამდენიმე ნაბიჯით ჩამორჩებიან კიბერტერორისტებს. სახელმწიფოთაშორისი კავშირი შეიძლება ითქვას არ არის ეფექტური და დროული, ამიტომ მნიშვნელოვანია რამე საერთო სისტემის შექმნა, რომლის მეშვეობითაც

მოკავშირე სახელმწიფოთა სამართალდამცავებს შეეძლებათ უფრო თავისუფალი მოქმედებების გატარება ერთმანეთის ტერიტორიებზე.

დასკვნა

ყოველივე ზემოთ ხსენებულიდან გამომდინარე, თანამედროვე საერთაშორისო მდგომარეობა არ იძლევა რაიმე დამამშვიდებელ პროგნოზებს, იმასთან დაკავშირებით, რომ ახალ ათასწლეულში, საერთაშორისო თანამეგობრობა შეძლებს აღკვეთოს ძალადობა. ძალადობა და მისი გამოყენების მუქარა კვლავ აქტუალური იქნება. დღესდღეობით ტერორიზმი თავისი განსხვავებული ფორმებით გახდა ჩვეულებრივი მოვლენა იმ ქვეყნებშიც, რომლებიც ადრე მიიჩნეოდნენ სტაბილურობისა და სამოქალაქო თანხმობის მოდელებად. დასავლეთის ექსპერტების აზრით, საერთაშორისო თანამეგობრობის მიმდინარე ძალისხმევა უძლურია ბოლო მოუღოს ტერორიზმს და მით უფრო, აღმოფხვრას მისი გამომწვევი მიზეზები. ტერორიზმის წინააღმდეგ ბრძოლას ართულებს სხვა საკითხებთან ერთად, საინფორმაციო, ენერგიისა და ფინანსური სისტემების გლობალიზაცია. ამიტომაც იგი შედის გლობალური პრობლემების რიცხვში, რომელიც დგას კაცობრიობის წინაშე.

მსოფლიოს ყველა წამყვანი ანალიტიკოსის კვლევები და არსებული მსოფლიო გამოცდილება ნათლად აჩვენებს, რომ საკუთარი კიბერ სივრცის დაცვაში მთავარი როლი ენიჭება მოცემული მიმართულებით საკანონმდებლო ბაზის მომზადებას და დახვეწას, ასევე საზოგადოებაში ცნობიერების ამაღლებას, საგანმანათლებლო და აკადემიური საქმიანობის წარმოებასა და საერთაშორისო ურთიერთობების გაღრმავებას.

დამნაშავე სამყარო ისეთია, როგორის საშუალებასაც მას აძლევს სახელმწიფო“ – ეს ფრაზა ჯონ კრამნიკს ეკუთვნის. მართლაც, დღესდღეობით მრავალი სახელმწიფო ცდილობს რომ საკუთარ ქვეყანაში მაქსიმალურად უზრუნველყოს გლობალური ქსელის ეფექტური კონტროლი, რაც მისასალმებელია. მეორე მხრივ კი საჭიროა ქვეყნებს შორის თანამშრომლობის

გაღრმავება კიბერტერორიზმის წინააღმდეგ ბრძოლისა და კიბერუსაფრთხოების გამყარების კუთხით.

წამყვანი ქვეყნების გამოცდილება აჩვენებს, რომ კიბერ სივრცის დაცვა არ არის დამოკიდებული მხოლოდ ტექნოლოგიურ მიღწევებზე, რადგან ხშირ შემთხვევაში ახალი ტექნოლოგიები ადვილად მისაწვდომია დამნაშავე ჰაკერული ჯგუფებისთვის და დაჯგუფებებისთვის. კიბერუსაფრთხოების სფეროში სულ უფრო დიდი როლი ენიჭება საერთაშორისო და რეგიონალური დონის ურთიერთობებს, გამოცდილების გაზიარებას, კვლევასა და ანალიზს, საზოგადოებაში ცნობადობის ამაღლებასა და სათანადო საკანონმდებლო ბაზის არსებობას.

დღეს კიბერტერორიზმს შეუძლია დიდი ზიანის მოტანა, რადგან მის დანაშაულებრივ არსენალში კლავიატურაა, როგორც ასაფეთქებელი საშუალება. კიბერტერორიზმი, როგორც უკვე ავღნიშნე, არის კიბერ სივრცისა და ტერორიზმის ერთობლიობა, რომელიც ითვალისწინებს ინფორმაციის გამოყენებას იარაღის, მეთოდის, სამიზნის სახით ტერორისტული მიზნის მისაღწევად. ამიტომაც, იგი არ არის მხოლოდ მომავლის საფრთხე იგი უკვე რეალური შედეგებით გვევლინება და ამიტომ სამართლებრივი მექანიზმები ამ კუთხით უნიფიცირებას ითხოვს.

ამრიგად, სახელმწიფოთა ხელისუფლებამ, კერძო და სამოქალაქო სექტორებმა, და ზოგადად, მთელმა საზოგადოებამ უნდა გააცნობიეროს და გაითავისოს, რომ ინტერნეტ/კიბერ სივრცე არის ქვეყნის ეროვნული ინფრასტრუქტურის მნიშვნელოვანი შემადგენელი ნაწილი, რომლის უსაფრთხოების უზრუნველყოფა და დაცვა პირდაპირ კავშირშია როგორც თითოეული მოქალაქის პერსონალური მონაცემების და ვირტუალურ სივრცეში პირადი უსაფრთხოების, ისე მთლიანად ეროვნული უსაფრთხოების უზრუნველყოფის თემასთან, ტერორიზმი სამართლიანადაა მიჩნეული თანამედროვეობის გლობალურ პრობლემად ამიტომაც, სასიცოცხლოდ მნიშვნელოვანია სამთავრობო ორგანოების შესაბამისი ქმედებები მისი კონტროლისა და აღკვეთისთვის.

კვლევის პროცესში გამოიკვეთა შემდეგი პრობლემები:

✓ ქართულ რეალობაში სამართალდამცავი ორგანოები არ ატარებენ შესაბამის პრევენციული ხასიათის ღონისძიებებს. ძირითადად ჩართული არიან გამოძიების ეტაპზე. აქედან გამომდინარე მნიშვნელოვანი იყო შემეთავაზებინა პრევენციული ხასიათის რეკომენდაციები, რათა უფრო ეფექტური გახდეს სამართალდამცავი ორგანოები და მეტი ფუნქცია შეითვისოს, დანაშაულის შემდგომი პრევენციისთვის.

✓ კიბერბულინგის განხილვისას გამოჩნდა, რომ სამართალდამცავი ორგანოები არ ახდენენ შესაბამის რეაგირებას ინტერნეტ სივრცეში განხორციელებულ შეურაცხყოფის ფაქტებზე, თუ ამ ქმედებამ რაიმე მძიმე შედეგი არ გამოიწვია. აღნიშნულთან პრობლემას წარმოადგენს აგრეთვე საზოგადოებრივი ადგილის განმარტება.

✓ რაიონული განყოფილებების წარმომადგენლები, კერძოდ უბნის ინსპექტორები არ ახორციელებენ თავიანთ სამოქმედო ტერიტორიაზე ეფექტურ სამუშაოებს, დანაშაულის პრევენციის მიზნით. არ აქვთ ამომწურავი ინფორმაცია მათ რაიონში მცხოვრები პირების შესახებ.

✓ კიბერსივრცეში განხორციელებული ზოგიერთი ქმედება, მაგალითად კიბერბულინგი, კიბერსივრცის ფარულობიდან გამომდინარე შეიძლება ლატენტური დარჩეს, რასაც ხელს უწყობს თავად მსხვერპლი.

✓ მოსახლეობის დაბალი ცნობიერება კიბერდანაშაულის ზოგიერთი ხერხის შესახებ. მაგალითად ფიშინგის ან სპამის შემთხვევა, როდესაც მომხმარებელი თავისი გულუბრყვილობით და ინფორმაციის ნაკლებობით გადასცემს თავის პირად მონაცემებს კიბერდამნაშვეს. ტექნოლოგიების განვითარებასთან ერთად იხვეწება კიბერდანაშაულის განხორციელების ხერხებიც. შესაბამისად მნიშვნელოვანია სამართალდამცავი ორგანოების წარმომადგენლების შესაბამისი მომზადება. ზემოთ აღნიშნული პრობლემების გადასაჭრელად კვლევის პროცესში წარმოვაჩინე შესაბამისი რეკომენდაციები, კერძოდ:

✓ კიბერბულინგის განხორციელებისას, როდესაც ერთი პიროვნება მეორეს აყენებს შეურაცხყოფას, გამოდის, რომ მოხდა პიროვნების პატივისა და ღირსების განზრახ დამცირება. შესაბამისად საქმე გვაქვს წვრილმან ხულიგნობასთან და სამართალდამცავმა ორგანოებმა უნდა გაატარონ შესაბამისი ღონისძიება სამართალდამრღვევის მიმართ.

✓ ინტერნეტ სივრცე, სადაც იკრიბება საზოგადოება არის საზოგდოებრივი ადგილი, ამიტომ აღნიშნულ სივრცეში ლანძღვა-გინება, მოქალაქეებზე შეურაცხმყოფელი გადაკიდება და სხვა ამგვარი მოქმედება, რომელიც არღვევს საზოგადოებრივ წესრიგსა და მოქალაქეთა სიმშვიდეს, უნდა მოექცეს სამართალდამცველთა ყურადღების ცენტრში

✓ რაიონული განყოფილების თანამშრომლები, კერძოდ უბნის ინსპექტორები და ოპერ თანამშრომლები აქტიურად უნდა იყვნენ ჩართული მოქალაქეებთან ურთიერთობაში, რათა მაქსიმალურად ამოიღონ ინფორმაცია მათ სამოქმედო ტერიტორიაზე მცხოვრები და სისტემატიურად მყოფი პირების შესახებ. უნდა მოხდეს დანაშაულთან კავშირში პირების გამოვლენა და დანაშაულებრივი ქმედების აღკვეთა.

✓ სამართალდამცავ ორგანოებს აქტიური ურთიერთობა უნდა ჰქონდეს სხვადასხვა დანაშაულის მსხვერპლთან. აღნიშნული ყველაზე ეფექტურია ბულინგთან მიმართებაში. თუ ადამიანი რეალურ ცხოვრებაში ბულინგის მსხვერპლია, დიდია ალბათობა, რომ მასზე კიბერბულინგიც განხორციელდეს. შესაბამისად მნიშვნელოვანია სამართალდამცავი ორგანოების ინფორმირება შემდგომი მოქმედებებისთვის.

✓ მნიშვნელოვანია მოქალაქეთა ცნობიერების ამაღლება, რათა არ გახდნენ კიბერდანაშაულის მსვერპლი. ამისათვის შეიძლება სამართალდამცავი ორგანოები ჩართული იყოს საგანმანათლებლო კუთხით. მაგალითად შ.ს.ს-მ შესაძლებელია ერთგვარი კამპანია დაიწყოს კიბერდანაშაულის წინააღმდეგ განათლების სამინისტროსთან ერთად და სკოლებიდან დაიწყოს კიბერდანაშაულის წინააღმდეგ ბრძოლა, ბავშვების განათლებით და მათი ცნობიერების ამაღლებით.

✓ შ.ს.ს აკადემიამ უნდა მოახდინოს სამართალდამცავთა შესაბამისი გადამზადება კიბერდანაშაულის წინააღმდეგ ბრძოლის კუთხით. ამისთვის შეიძლება შესაბამისი სასწავლო პროგრამების მომზადება და სპეციალისტების მოწვევა კიბერდანაშაულთან მებრძოლი მოწინავე სახელმწიფოებიდან, ლექცია-სემინარების ჩასატარებლად და თავიანთი გამოცდილების გასაზიარებლად.

✓ მნიშვნელოვანია აქტიურად ვიყოთ ჩართული საერთაშორისო თანამშრომლობაში. უნდა ვითანამშრომლოთ ნებისმიერ ქვეყანასთან, ვისაც სურვილი აქვს კიბერდანაშაულის წინააღმდეგ ეფექტური ღონისძიებების გატარების. ჩვენი სამართალდამცავები უნდა ესწრებოდნენ საერთაშორისო ღონისძიებებს, რომელსაც ატარებს საპოლიციო ორგანიზაციები და მოწინავე სახელმწიფოები. რაც შეიძლება მეტი ინფორმაცია უნდა მივიღოთ კიბერდანაშაულის წინააღმდეგ ბრძოლაში სიახლეების შესახებ, გავიზიაროთ მოწინავე სახელმწიფოების გამოცდილება და გავატაროთ შესაბამისი ღონისძიებები საქართველოშიც.

ბიბლიოგრაფია

ნორმატიული აქტები:

1. საქართველოს სისხლის სამართლის კოდექსი
2. საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“
3. 2001 წლის ევროსაბჭოს კონვენცია „კიბერდანაშაულის შესახებ“
4. 2005 წლის 16 მაისის კონვენცია „დანაშაულებრივი გზით მიღებული შემოსავლების გათეთრების, მოძიების, ამოღებისა და კონფისკაციის და ტერორიზმის დაფინანსების შესახებ“
5. პრეზიდენტის ბრძანებულება „კიბერდანაშაულის შესახებ“ კონვენციის დამტკიცების თაობაზე N 450
6. საქრთველოს კიბერუსაფრთხოების სტრატეგია, დანართი N 2
7. საქართველოს სისხლის სამართლის კოდექსი (13.04.2016 მდგომარეობით);

8. ადმინისტრაციულ სამართალდარღვევათა კოდექსი (27.05.2016 მდგომარეობით);
9. ევროპის საბჭოს კონვენცია კომპიუტერული დანაშაულის შესახებ, ბუდაპეშტი, (23.11.2001);

სამეცნიერო ლიტერატურა:

1. ავტორთა კოლექტივი „სისხლის სამართლის კერძო ნაწილი“ წიგნი II, გამომცემლობა „მერიდინაი“ თბილისი 2012 წ.
2. ავტორთა კოლექტივი „ორგანიზებული დანაშაული “ თბილისი 2002 წ.
3. ავტორთა კოლექტივი „მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ ტრენინგის სახელმძღვანელო,“ ევროსაბჭო, სტრასბურგი, 2010 წ.
4. ბოძაშვილი ლ. კორეხიძე ნ. „კიბერსივრცის სამართალი“, 2012 წ.
5. გორაშვილი გ. “ეთნიკურ - სეპარატისტული ტერორიზმის გზები“ გამომცემლობა “უნივერსალი თბილისი 2010 წ
6. გორაშვილი გ. ტერორიზმი და მისი იმანენტური კრიმინოლოგიური ნიშნები ჟურნალი ადამიანი და კონსტიტუცია 2004 N 2
7. კაცმანი ა. სადისერტაციო ნაშრომი „კომპიუტერული დანაშაული“ თბილისი 2004 წ.
8. კაცმანი ა. კომპიუტერული სანაშაულის სისხლისმართლებრივი და კრიმინალისტიკური დახასიათება“ ჟრნალი სამართალი 2000 წ. N 2
9. ლანცავა გ. „კომპიუტერული დანაშაული“ ჟურნალი “მართლმსაჯულება“ 2008 წ. N 2,
10. მაღრაძე მ. გელაშვილი ა. სისაური ვ. „ტერორიზმი და ფაქტორები, რომლებიც მოქმედებენ პიროვნების ტერორისტად ჩამოყალიბებაზე“ მონოგრაფია, თბილისი 2016 წ.
11. წერეთელი თ. ტყეშელიძე გ. „მოძღვრება დანაშაულზე“ გამომცემლობა „მეცნიერება“ თბილისი 1969 წ.

ელექტრონული წყაროები:

1. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
2. https://www.gccs2015.com/sites/default/files/documents/GCCS2015_discussion_paper_on_improving_international_cooperation.pdf
3. http://www.coe.int/t/dlapil/codexter/cyberterrorism_db.asp
4. http://www.coe.int/t/dlapil/codexter/about_en.asp
5. http://www.first.org/
6. http://www.dcaf.ch/Project/Horizon-2015
7. http://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf.
8. http://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf
9. http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=1&CL=ENG
10. http://police.ge/ge/projects/kiberdanashauli/saertashoriso-tanamshromloba-kiber-danashaultan-brdzolashi
11. http://cyber.laws.com/cyber-terrorism
12. http://www.antiphishing.org/about-APWG/
13. http://pog.gov.ge/res/docs/statistika/cybercrime.pdf
14. http://dea.gov.ge/?web=0&action=article&article_id=8&lang=geo
15. http://dea.gov.ge/?web=0&action=article&article_id=8&lang=geo
16. http://www.phishing.org/phishing-techniques/
17. http://www.radiotavisupleba.ge/content/normad-kceuli-dzaladoba/25154835.html
18. http://www.nplg.gov.ge/gwdict/index.php?a=term&d=5&t=2599
19. http://pog.gov.ge/res/docs/statistika/cybercrime.pdf
20. http://netgazeti.ge/news/35133/
21. http://www.afp.gov.au/~/media/afp/pdf/c/cyber-bullying-no-crops.pdf
22. http://police.ge/files
23. http://www.education.ge/index.php?do=definition/view&id=1891
24. https://www.ncab.org.au/bullying-advice/bullying-for-parents/types-of-bullying/
25. http://www.nplg.gov.ge

26. http://en.wikipedia.org/wiki/convention_on_cybercrime
27. http://www.today.az./news/society/46054.html
28. http://conventions.coe.int/treaty/commun/cherchesig.asp?NT=185&CM=&DF=CL=ENG
29. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
30. http://www.crime-research.org/articles/types-of-computer-crime/2