კავკასიის საერთაშორისო უნივერსიტეტი

კვირკველია ბაჩანა

კომპიუტერული დანაშაული (კიბერტერორიზმის პრობლემა)

(ნაშრომი შესრულებულია მაგისტრის აკადემიური ხარისხის მოსაპოვებლად)

ხელმძღვანელი, სამართლის პროფესორი:
ჭელიძე სერგო

თბილისი
2018 წელი

გამოყენებული აბრევიატურა:

სსკ _ სისხლის სამართლის კოდექსი

სსსკ _ სისხლის სამართლის საპროცესო კოდექსი

ე.წ. _ ეგრეთ წოდებული

ე.ი. _ ესე იგი

გვ - გვერდი

ა.შ. _ ასე შემდეგ

სხვ. _ სხვა

მაგ. _ მაგალითად

იხ. _ იხილეთ

შეად. _ შეადარეთ

თბ. _ თბილისი

წ. _ წელი

წწ. _ წლებში

რედ. _ რედაქტორი

ჟ. _ ჟურნალი

დასახ. ნაშრ. _ დასახელებული ნაშრომი

დასახ. სტატია _ დასახელებული სტატია

გამომც. _ გამომცემლობა

აშშ _ ამერიკის შეერთებული შტატები

გაერო _ გაერთიანებული ერების ორგანიზაცია

ჯანმო _ ჯანმრთელობის მსოფლიო ორგანიზაცია

წმ. _ წმიდა

ჟ. ჟურნალი

ანოტაცია

წინამდებარე ნაშრომში განხილულია კომპიუტერული დანაშულისა და კიბერტერორიზმის ცნება, ზოგადი და სისხლისსამართლებრივი დახასიათება, სამართლებრივი დაცვის მექანიზმები, საკანონმდებლო პრობლემები, ასევე საერთაშორისო ხასიათის ღონისძიებები, კიბერშეტევისა და კიბერტერორიზმის თავიდან ასაცილებლად, ასევე განხილულია სახელმწიფოთა მიერ განხორციელებული ღონისძიებები მოცემულ დანაშაულთან ბრძოლის მიზნით, ასევე შემოთავაზებულია რეკომენდაციები, რაც თანამედროვე მიდგომებით უზრუნველყოფს კიბერტერორიზმის წინააღმდეგ ეფექტურ ბრძოლას.

ტექნოლოგიური განვითარების პარალელურად ვითარდება ასევე კიბერდანაშაულებები. მოცემულ პრობლემაში დიდი მნიშვნელობა ენიჭება არამარტო საერთაშორისო თუ რეგიონალურ დონეზე მიღებულ რეზოლუციებსა და რეკომენდაციებს, ან/და კიბერსაფრთხეებთან მებრძოლ სუბიექტებს, არამედ ასევე პიროვნების ფაქტორს, როგორც ქსელისა და პერსონალური კომპიუტერული მოწყობილობის მომხმარებელს, რაც მაქსიმალურად შეამცირებს რისკებს როგორც გლობალურ, ისე ლოკალურ ინტერნეტ სივრცეში.

Annotation

The present work deals with the notion of computer crimes and cyberterrorism, general and criminal characterization, legal protection mechanisms, legislative problems, also international events, to prevent cyber attacks and cyber terrorism, also discussed the initiatives undertaken by states in order to combat this crime, recommendations are also proposed, which is of modern approaches ensures an effective fight against cyber terrorism.

In parallel to technological development, cybercrime develops as they are active users of each know-how. The problem is of great importance not only to the international and regional levels, resolutions and recommendations, and / or kibersaprtkheeb fighting subjects, but also as a factor in personal computer and network equipment for customers, which in the field of awareness, educational programs d Internet promotion of codes of ethics and the output is a necessary condition for all governments and international organizations, which will reduce the risks of both global and local Internet space.

Contents

შესავალი

არსებობს ტერმინის „კიბერსივრცის“ განმარტების ბევრი ვარიანტი და ყველა მათგანი იძლევა თავისებურ განსაზღვრებას. თუმცა ყველა განმარტებაში აღნიშნულია, რომ „კიბერსივრცე“ წარმოადგენს ინფორმაციულ - ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირის კომპლექსს, რომელიც თავისთან მოიცავს ინტერნეტის გლობალურ ქსელს, კომპიუტერულ სისტემებს, ტელესაკომუნიკაციო ქსელებსა და პროცესორებს.

კიბერსივრცეში დღეს არსებული მდგომარეობა სულ უფრო შემაშფოთებელია, რადგან უსაფრთხოების სფეროს ანალიტიკოსების მიერ ჩატარებული კვლევების მიხედვით, დიდი ქვეყნები თავიანთ პროგრამებს აგებენ კიბერ - ომის წარმოების შესაძლებლობებზე. დღეს უკვე არსებობს სერიოზული მოსაზრებები, რომ კიბერ - ომი და მასთან დაკავშირებული აქტიურობები ადრე თუ გვიან აუცილებლად მოხდება.

კარგად შესრულებული კიბერშეტევა ნებისმიერ ზემოთ მოცემულ სექტორზე გამოიწვევს შიშს, სამოქალაქო პანიკასა და მასიურ არეულობებს. ასევე პარალიზებული იქნება სახელმწიფო სტრუქტურები ყველა დონეზე. ამიტომ, კიბერუსაფრთხოების დარგის ანალიტიკოსები რჩებიან იმ აზრზე, რომ კიბერ - ომმა, მინიმალური დანახარჯებითა და ძალისხმევით, ტრადიციული ომის მსგავსად შეიძლება გამოიწვიოს მასიურად ადამიანთა ფიზიკური განადგურება.

აგრეთვე ნაშრომში მოცემულია წამყვანი ქვეყნების კიბერშესაძლებლობების მიმოხილვა, მათი კიბერუსაფრთხოების პოლიტიკისა და სტრატეგიების მოკლე აღწერილობები, საერთო პრინციპები და რეკომენდაციები. კერძოდ, ნაშრომში განხილულია შეერთებული შტატების, დიდი ბრიტანეთის, ნიდერლანდების სამეფოს, რუსეთისა და ირანის კიბერშესაძლებლობები, მათი კიბერსივრცის დაცვის ორგანიზაციული და სტრუქტურული მოწყობა, რაც შეიძლება მივიჩნიოთ საუკეთესო გამოცდილებად საქართველოს კიბერუსაფრთხოების მოწყობისთვის.

კიბერსივრცეში უსაფრთხოების უზრუნველყოფის სირთულეებს საზღვრები არ გააჩნია. თუმცა ყველა ქვეყანა ცდილობს ეს საკითხი გადაჭრას თავად დამოუკიდებლად, რის გამოც ყველა საჭირო ზომები და ღონისძიებები ხშირ შემთხვევაში არ არის საკმარისი. არსებობს უამრავი სირთულე როგორც კიბერუსაფრთხოების სირთულეების ჩვენეულ გაგებაში, ისე სახელმწიფო პოლიტიკაში და ტექნიკურ შესაძლებლობებში, რომლებიც აუცილებელია მოცემული საკითხების გადასაჭრელად.

მსოფლიოს ქვეყნებისთვის და საქართველოსთვის მეტად მნიშვნელოვანია ინტერნეტ სივრცის უსაფრთხოებისა და ელექტრონული ინფორმაციის დაცულობის უზრუნველყოფა. ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერსივრცეში არასანქცირებული შეღწევის აღკვეთასა და თავდაცვითი ღონისძიებების გაძლიერებას.

ინფორმაციულ ტექნოლოგიებზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულებასთან ერთად იზრდება ის გამოწვევები, რომლებიც საქართველოს ინფორმაციული სივრცის დაცვასთანაა დაკავშირებული. 2008 წლის რუსეთ - საქართველოს ომის დროს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ, სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, მიზანმიმართული და მასობრივი კიბერთავდასხმები განახორციელა. ამ კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა.

საქართველოს მიზანია, შექმნას ინფორმაციული უსაფრთხოების ისეთი სისტემა, რომლის დროსაც ნებისმიერი კიბერთავდასხმის საზიანო შედეგები მინიმუმამდე იქნება შემცირებული და ასეთი თავდასხმის შემდეგ უმოკლეს დროში გახდება შესაძლებელი ინფორმაციული ინფრასტრუქტურის ფუნქციონირების სრული აღდგენა.

კიბერუსაფრთხოების უზრუნველყოფისათვის დიდი მნიშვნელობა ენიჭება საქართველოს მეგობარ ქვეყნებთან თანამშრომლობას და მათი გამოცდილების გაზიარებას. ასევე მნიშვნელოვანია განისაზღვროს საქართველოსთვის სტრატეგიულად პარტნიორი და პოტენციურად მოწინააღმდეგე ქვეყნები.

<u>ნაშრომი განკუთვნილია</u> როგორც მოცემული დარგის სპეციალისტებისთვის და სამართალმცოდნეებისთვის, ისე იმ დაინტერესებული პირებისთვის, რომლებსაც სურთ ამ მიმართულებით შეიძინონ გარკვეული ცოდნა. აგრეთვე, ნაშრომში განხილული საკითხები, დასკვნები და რეკომენდაციები შეიძლება გამოიყენოს, როგორც საკანონმდებლო და აღმასრულებელი ხელისუფლების, ისე კერძო და სამოქალაქო სექტორის წარმომადგენლებმა.

<u>კვლევის საგანს</u> წარმოადგენს ეროვნული უსაფრთხოების კონცეფციის საფუძველზე, კიბერუსაფრთხოების სფეროში საქართველოსთვის პოტენციურად მოწინააღმდეგე და სტრატეგიულად პარტნიორი ქვეყნებისა და ორგანიზაციების განსაზღვრა.

<u>კვლევაში განხილულია</u> არსებული ვითარება; კიბერშეტევის ძირითადი სექტორები და მთავარი მოთამაშე ქვეყნები; პოტენციურად მოწინააღმდეგე და სტრატეგიულად მნიშვნელოვანი ქვეყნებისა და ორგანიზაციების მოკლე აღწერა მოცემული მიმართულებით. **ნაშრომი შედგება** შვიდი თავისაგან. პირველი თავი ეძღვნება კომპიუტერული დანაშაულს. ეს თავი დაყოფილია ორ პარაგრაფად. პირველი პარაგრაფი ეხება კომპიუტერული დანაშაულის ცნებას ხოლო მეორე - კომპიუტერული დანაშაულის დახასიათებას. მეორე თავი მკითხველს აცნობს კომპიუტერული დანაშაულის სისხლისსამართლებრივ დახასიათებას, რომელშიც დეტალურადაა განხილული კომპიუტერული დანაშაულის ჩადენის ხერხები და ინფორმაციის ხელში ჩაგდების მთოდები. მესამე თავი ეთმობა კომპიუტერული დანაშაულის კრიმინოლიგიურ დახასიათებას. რაც შეეხება მეოთხე თავს, მასში განხილულია კიბერტერორიზმის ზოგადი და სისხლისსამართლებრივი დახასიათება, ასევე მოცემულია მეცნიერთა მოსაზრებები კიბერტერორიზმის

ცნებასთან დაკავშირებით. მეხუთე თავში მოცემულია საერთაშორისო და რეგიონალური დონის ღონისძიებები მიმართული კიბერსივრცის დაცვაზე, კერძოდ კიბერდანაშაულთან ბრძოლის ევროპული კონვენცია. მეექვსე თავში განხილულია კიბერტერირიზმის საკანონმდებლო პრობლემატიკა, ხარვეზი და მისი გამოსწორების რეკომენდაციები. ხოლო მეშვიდე თავში დღესდღეობით არსებული გამოწვევები და ის პრობლემები რაც არსებობს ლოკალურ თუ საერთაშორისო დონეზე.

<u>კვლევის მეთოდოლოგიური საფუძველი</u> კვლევისას გამოყენებულია: ისტორიული, ფორმალურ-ლოგიკური, შედარებით-სამართლებრივი და სხვა მეთოდები

<u>სამაგისტრო ნაშრომის სტრუქტურა და მოცულობა</u> ნაშრომი შედგება: ანოტაციის, შესავლის, 7 თავის, 27 პარაგრაფის, დასკვნისა და გამოყენებული ლიტერატურის სიისაგან, ნაშრომის მოცულობა სულ შეადგენს 75 გვერდს.

თავი 1. კომპიუტერული დანაშაულის ზოგადი დახასიათება

1.1 კომპიუტერული დანაშაულის ცნება

ტერმინი „კომპიუტერული დანაშაული“ პირველად გაჩნდა ამერიკულ სამეცნიერო ლიტერატურაში ჯერ კიდევ XX საუკუნის 50-60-იან წლებში, როდესაც განხორციელებულ იქნა კომპიუტერული სისტემის პირველი დანაშაულები. დასავლელი კრიმინოლოგების აზრით, ეს არის ანგარებითი დანაშაულის ჩადენის ყველაზე უნივერსალური საშუალება. როგორც ამერიკელი სპეციალისტები თვლიან, პირდაპირი ეკონომიკური ზიანი, რომელსაც კომპიუტერული დანაშაულები იწვევენ, უკვე ესადაგება იმ მოგებას, რაც კომპიუტერული სისტემის დამკვიდრებას მოჰყვება, ხოლო ამგვარი დანაშაულების მიერ გამოწვეული სოციალური და მორალური ზიანი არც კი ექვემდებარება დათვლას. ამასთან ერთად, უნდა გავითვალისწინოთ, რომ ამ სახის დანაშაულები ხასიათდებიან მაღალი ლატენტურობით: კომპიუტერულ დანაშაულთა მხოლოდ 10-15% შესახებ ხდება ცნობილი, ვინაიდან ორგანიზაციები, რომლებიც დაზარალდნენ ამგვარი დანაშაულების ჩადენის შედეგად, ცდილობენ დამალონ შესაბამისი ინფორმაცია, რადგან ამან შეიძლება გამოიწვიოს მათი რეპუტაციის შელახვა ან განმეორებითი დანაშაულის ჩადენა.[1]

კომპიუტერული დანაშაული ყურადღების ცენტრში პირველად ამერიკის შეერთებულ შტატებში XX საუკუნის 70-იან წლებში მოექცა. დაიწყო ნაციონალურ და საერთაშორისო დონეზე ამ ფენომენის გამოკვლევა. მიღებულ იქნა სპეციალური ნორმები კიბერდანაშაულის მოსაწესრიგებლად.[2] აშშ-ში, ჯერ კიდევ 1977 წელს შეიმუშავეს კანონპროექტი „ფედერალური კომპიუტერული სისტემების დაცვის შესახებ“, რომელიც ითვალისწინებდა სისხლისსამართლებრივ პასუხისმგებლობას ისეთი ქმედებებისთვის, როგორიცაა:

[1] Сибиряков С. Л., криминологическое Характеристика и Профилактика Компьютерных преступлений, Волгоград, 1999, ст. 4;

[2] ზაქაშვილი უ., კიბერტერორიზმი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, გამომცემლობა „მერიდიანი“, თბილისი, 2013წ;

კომპიუტერულ სიტემაში ცრუ მონაცემების შეყვანა, კომპიუტერული მოწყობილობის უკანონო გამოყენება, ფულადი სახსრების მითვისება კომპიუტერული ტექნოლოგიებისა და კომპიუტერული ინფორმაციის მეშვეობით და სხვ. ამ კანონპროექტის საფუძველზე 1984 წლის პქტომბერში მიღებულ იქნა „კომპიუტერული თაღლითობის და კომპიუტერის ბოროტად გამოყენების შესახებ" კანონი. კომპიუტერული დანაშაულის წინააღმდეგ აქტიური რძოლის დასაწყებად კი ამერიკის შეერთებულ შტატებში ექსპერტები გამოყოფენ სამ შემთხვევას, რომლებმაც ცხადი გახადა, რომ ახალი კომპიუტერული და სატელეკომუნიკაციო ტექნოლოგიები დიდ პრობლემებს შეუქმნიდა სამართალდამცავ ორგანოებს. კომპიუტერების მასშტაბური ინტეგრაცია ყოველდღიურ ცხოვრებაში, მარტო ცხოვრების წესის შეცვლას კი არ ნიშნავდა, არამედ შეიცვლებოდა კრიმინალების მიერ დანაშალებრივი საქმიანობის წარმართვის სპეციფიკაც. [3]

როგორც ზემოთ ავღნიშნე, კომპიუტერული დანაშაულები სამართლებრივი რეგულირების სფეროში პირველად მოხვდა XX საუკუნის 70-იან წლებში, როდესაც აშშ-ში 50-60-იან წლებში ჩადენილი ამგვარი ქმედებების მრავალი ფაქტი გამოასკარავდა, რასაც თავის მხრივ მოჰყვა მეცნიერ-კრიმინოლოგებისა და სისხლისსამართლებრივი იუსტიციის ორგანოების მხრიდან ყურადღების მიპყრობა. დაიწყო ამ ფენომენის ინტენსიური გამოკვლევა, როგორც ნაციონალურ, ისე საერთაშორისო დონეზე; სისხლის სამართლის კანონდებლობაში დაიწყო სპეციალიზირებული ნორმების ფორმულირება კომპიუტერულ დანაშაულზე.

საზღვარგარეთის ქვეყნების კანონდებლობის განვითარების ისტორია ამ მიმართულებით გვიჩვენებს, რომ პირველად მსგავსი ნაბიჯი გადაიდგა ამერიკის-არიზონისა და ფლორიდის შტატების საკანონმდებლო კრების მიერ კიდე კიდევ 1978 წელს. მიღებულ კანონს ერქვა „Computer crime act of 1978" და იყო მსოფლიოში პირველი სპეციალური აქტი, რომელიც ადგენდა სისხლისსამართლებრივ პასუხისმგებლობას კომპიუტერული დანაშაულისთვის.

[3] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013 გვ 26;

შემდგომ, პრაქტიკულად აშშ-ის ყველა შტატში მიღებულ იქნა ანალოგიური სპეციალური კანონები. 1984 წელს აღნიშნული საკითხები საკანონმდებლო წესით მოაწესრიგა აშშ-ის ფედერალურმა კანონმდებლობამ.[4]

სისხლის სამართლებრივი კანონმდებლობის მნიშვნელოვანი რეფორმა შემოღებულ იქნა გერმანიაში, სადაც კომპიუტერული ინფორმაციის სფეროში ჩადენილ დანაშაულებზე სისხლისსამართლებრივი პასუხისმგებლობის საკითხი 1986 წლიდან დადგა. 1987 წლის აგვისტოდან განხორციელდა შესაბამისი ცვლილებები გერმანიის სისხლის სამართლის კოდექსში, რითიც დადგინდა პასუხისმგებლობა კომპიუტერული დანაშაულისათვის. 1986 წლის სამეურნეო დანაშაულთან ბრძოლის მეორე კანონით დადგენილ იქნა სისხლის სამართლებრივი პასუხისმგებლობა კომპიუტერული თაღლითობისთვის ჩადენილი საკუთარი თავისთვის ან სხვა პირისთვის სარგებლის მიღების უზრუნველყოფის მიზნით და რომელმაც მიაყენა ქონებრივი ზიანი მონაცემთა დამუშავების პროცესზე ზეგავლენით, არამართლზომიერი პროგრამირების, არასრული ან არასწორი ინფორმაციიც დამუშავების პროცესში-გერმანიის სსკ-ის 263 „ა“ მუხლი, კომპიუტერული შპიონაჟი (თვითნებური-ნებართვის გარეშე-საკუთარი თავისთვის ან სხვისთვის ინფორმაციის შეძენა, რომელიც ინახება ან გადაიცემა ელექტრონული საშუალებების ან მაგნიტური მატარებლის მეშვეობით, ან სხვა უხილავი გზით, თუ ეს ინფორმაცია არ არის განკუთვნილი ამ პირისთვის და სპეციალურად არის დაცული თვითნებური წვდომისგან-გერმანიის სსკ-ის 202 „ა“ მუხლი), კომპიუტერული საბოტაჟი და სხვა დანაშაულები კომპიუტერული ინფორმაციის სფეროში.[5] გერმანიაში კომპიუტერული ინფორმაციის სფეროში ჩადენილ დანაშაულებზე სისხლისსამართლებრივი პასუხისმგებლობის საკითხი 1986 წლიდან დადგა. 1987 წლის აგვისტოდან განხორციელდა შესაბამისი ცვლილებები გერმანიის სისხლის სამართლის კოდექსში, რითიც დადგინდა პასუხისმგებლობა კომპიუტერული დანაშაულისთვის.

---

[4] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, 10;

[5] კაცმანი ა., კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება, ჟურნალი სამართალი, 2000, №2 34-37;

დიდი ბრიტანეთი მრავალი წლის მანძილზე უშედეგოდ ცდილობდა კომპიუტერული დანაშაულის წინააღმდეგ გამოეყენებინა სასამართლო წარმოებაში მიღებული მრავალსაუკუნოვანი გამოცდილება. 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, განადგურება ან კოპირება. [6]

„რუსეთის ფედერაციის სისხლის სამართლის კოდექსში კომპიუტერულ დანაშაულს ეთმობა 28-ე თავი, რომელიც სამი მუხლისგან შედგება. 2015 წელს განხორციელდა ცვლილებები და ამავე წლის 23 მარტიდან იგი ძალაში შევიდა. 272-ე მუხლი 4 ნაწილისგან შედგება. პირველი ნაწილით გათვალისიწნებულია კომპიუტერში შეღწევა და მისი სანქციები. ეს ქმედება უკავშირდება კანონით დაცულ კომპიუტერულ ინფორმაციაში შეღწევას, თუ ამგვარ ქმედებას თან ახლავს განადგურება, ბლოკირება, მოდიფიცირება ან ინფორმაციის კოპირება. მეორე ნაწილით გათვალისწინებულია იმავე ქმედების ჩადენა, რასაც მოჰყვა მნიშვნელოვანი ზიანი, ან ჩადენილ იქნა ანგარებით. მესამე ნაწილი ეხება ამ მუხლის პირველიდ და მეორე ნაწილებით გათვალისწინებული ქმედების ჩადენას ჯგუფის, წინასწარ შეთანხმებული ან ორგანიზებული ჯგუფის მიერ თავიანთი სამსახურეობრივი მდგომარეობის გამოყენებით. [7]

272-ე მუხლს გააჩნია განმარტებითი ორი შენიშვნა:[8] 1). კომპიუტერული ინფორმაციის ქვეშ იგულისხმება ცნობები (მესიჯი, მონაცემები), ელექტრონული სიგნალების ფორმით გადმოცემული, მათი შენახვის საშუალებებისგან დამოუკიდებელად დამუშავება და გადაცემა; 2). მნიშვნელოვან ზიანად ითვლება ზიანი, როდესაც თანხა აღემატება მილიონ რუბლს.

[6] http://www.nato.int/cps/en/natolive/news_52837.htm

[7] Сибиряков С. Л. , криминологическое Характеристика и Профилактика Компьютерных преступлений, Волгоград, 2016 p 18;

[8] სისხლის სამართლის კერძო ნაწილი. წიგნი 2. ლეკვეიშვილი მ., თოდუა ნ. და მამულაშვილი გ., გამომცემლობა ,,მერიდიანი", 2017, 140 გვ;

რუსეთის ფედერაციის სისხლის სამართლის კოდექსის, 273-ე მუხლი უკავშირდება კომპიუტერის საზიანო პროგრამების შექმნას, გამოყენებასა და გავრცელებას. პირველი ნაწილი ეხება ზემოთ ხსენებული ქმედების განხორციელებას, როგორც სხვა კომპიუტერული ინფორმაციის მიზანმიმართულად, ნებართვის გარეშე განადგურებას, ბლოკირებას, მოდიფიცირებას, კოპირებას, ასევე კომპიუტერული ინფორმაციის დაცვის საშუალებების განბლოკვას. მეორე ნაწილი მოიცავს პირველი ნაწილით გათვალისწინებული ქმედების ჩადენას პირთა ჯგუფის მიერ ან ორგანიზებული ჯგუფის მიერ სამსახურებრივი მდგომარეობის გამოყენებით, რაც უთანაბრდება მიყენებულ მნიშვნელოვან ზიანს ან ჩადენილია გამორჩენის მიზნით. მესამე ნაწილი უკავშირდება ამ მუხლის პირველი და მეორე ნაწილით გათვალისწინებული ქმედების ჩადენას, რომელმაც გამოიწვია მძიმე შედეგი ან შეიქმნა ასეთი შედეგის დადგომის საშიშროება.[9]

ბოლო, 274-ე მუხლი კომპიუტერული დანაშაულისა ეხება კომპიუტერული ინფორმაციის შენახვის საშუალებების გადამუშავების ან გადაცემის და საინფორმაციო-სატელეკომუნიკაციო ქსელების ექსპლუატაციის წესის დარღვევას. პირველი ნაწილით გათვალისწინებულია ზემოთ აღნიშნული ქმედების განხორციელება, ასევე ტერმიანელბის მოწყობილობებთან, რამაც გამოიწვია განადგურება, ბლოკირება, მოდიფიცირება, თუნდაც კომპიუტერული ინფორმაციის კოპირება, რის შედეგადაც დადგა მნიშვნელოვანი ზიანი. მეორე ნაწილი უკავშირდება პირველი ნაწილით გათვალისწინებული ქმედების ჩადენას, თუ მან გამოიწვია მძიმე შედეგი ან წარმოიქმნა მისი დადგომის საშიშროება.[10]

გაეროს მიერ მიღებულ იქნა "ინფორმაციული ტექნოლოგიების გამოყენებით ჩადენილი დანაშაულის წინააღმდეგ ბრძოლის შესახებ" რეზოლუციები, რომლებშიც ხაზგასმულია ყველა წევრი სახელმწიფოს მხრიდან საკუთარი საკანონდებლო ბაზის გადახედვის და მისი სრულყოფის

[9] www. docs.cntd.ru/document/9017477

[10] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 1 2 , 2015 მდგ;

აუცილებლობა. 2001 წლის 23 ნოემბერს ქ. ბუდაპეშტში მიღებულ იქნა ევროსაბჭოს კონვენცია „კიბერდანაშაულის შესახებ“.

„კიბერდანაშაულის შესახებ“ კონვენციამ მე-5 მუხლის მიხედვით დასჯადად გამოაცხადა კომპიუტერული სისტემის ფუნქციონირებისთვის საფრთხის შექმნა, რომელიც ჩადენილია კომპიუტერულ მონაცემთა შეყვანის, გადაცემის, დაზიანების, წაშლის და დაფარვის გზით, ხოლო ევროკავშირის ჩარჩო გადაწყვეტილების მე-3 მუხლის მიხედვით კი ყველა მონაწილე სახელმწიფო ვალდებულია მიიღოს საჭირო ზომები, რათა უზრუნველყოს იგივე ქმედების კრიმინალიზაცია. თუმცა, ავსტრიაში დასჯადია ასეთი ქმედება მხოლოდ იმ შემთხვევაში, თუ ის ატარებს მძიმე დანაშაულის ნიშნებს; ჩეხეთი, ესტონეთი და ლიტვა აუცილებელ პირობად მიიჩნევენ ასეთი ქმედებით გამოწვეულ ზიანს. ლატვიელი კანონდებლების აზრით კი საინფორმაციო სისტემაში ჩარევა დანაშაულია მხოლოდ იმ შემთხვევაში, თუ იგი განხორციელდა დაცვის სისტემის განადგურებით ან გამოიწვია დიდი ოდენობის დანაკარგი.[11] 1983 წელს პარიზში ექსპერტების ჯგუფმა ჩამოაყალიბა კომპიუტერული დანაშაულის ცნება: „კომპიუტერული დანაშაული არის კანონით აკრძალული, არაეთიკური ქმედება, რომელიც აფერხებს მონაცემთა ბაზების ავტომატიზებულ მუშაობას ან ინფორმაციის გადაცემას“.[12]

1993 წელს ინტერპოლის მუშაობის ჩარჩოებში ორგანიზებული სემინარის „კრიმინალისტიკა და კომპიუტერული დანაშაული“-ს ფარგლებში კი კომპიუტერული დანაშაულის ცნებამ შემდეგნაირი სახე მიიღო: “სისხლის სამართლით გათვალისწინებული საზოგადოებრივად საშიში ქმედება, რომელშიც

[11] Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448 (Based on article 12 of the Council Framework Decision of 24.02.2005 on attaks against information systems);

[12] Richard W. Aldrich, “CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME”, USAF Institute for National Security Studies USAF Academy, Colorado, April 2000, 10;

მანქანური ინფორმაცია წარმოადგენს დანაშაულებრივი ხელყოფის საშუალებას ან ობიექტს".[13]

მოცემული ცნების მთავარი ნაკლი ისაა, რომ ავტორებმა კომპიუტერული ინფორმაცია წარმოადგინეს, როგორც დანაშაულის ჩადენის საშუალება და ობიექტი. თუმცა არ აღუნიშნავთ, რომ ის შეიძლება კომპიუტერული დანაშაულის საგანიც იყოს.

კიბერ დანაშაულის ერთიანი ცნების შემოღება ბოლო წლებში, არც ერთ ქვეყანას თუ საერთაშორისო ორგანიზაციას უცდია, რადგან რთულია ზოგადა, კიბერდანაშაული მოვაქციოთ რამოდენიმე წინადადებაში, ვინაიდან ცნებაშ უნდა აისახოს კომპიუტერული დანაშაულის ყველა ნიშანი და თავისებურება.[14]

1.2. კომპიუტერული დანაშაულის დახასიათება

კიბერსივრცეში მოისაზრება კომპიუტერული სისტემის მთლიანობა და უსაფრთხოება. კომპიუტერული სისტემა მოწყობილობების, მონაცემებისა და ქსელების ერთობლიობაა, რომლის რღვევისკენაცაა მიმართული კომპიუტერული დანაშაულის ჩადენა. კიბერდანაშაულის ჩადენით შეიძლება ხელყოფილ იქნეს კომპიუტერის ნორმალური ფუნქციონირების მწყობრიდან გამოსვლა, მათი მეშვეობით სხვადასხვა დაწესებულების სერვერში შეღწევა, კონფიდენციალური, პერსონალური ინფორმაციის მითვისება, სხვადასხვა საბანკო ანგარიშებიდან თანხების მოხსნა და სხვა უამრავი მანიპულაცია, რაც აღნიშნული დანაშაულის ჩადენის უსაზღვრო შესაძლებლობით აიხსნება. კომპიუტერული დანაშაული გულისხმობს, როგორც უბრალო/უმნიშვნელო დანაშაულს, რაც შეიძლება პირმა

[13] კაცმანი ა., კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება, ჟურნალი სამართალი, 2000, №2, 58;
[14] სვანაძე ვ., გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, 2015, გვ 56;

უბრალო ინტერესის გამო განახორციელოს, ასევე მასშტაბურ შეტევასაც, რომელსაც შეუძლია მნიშვნელოვანი ზიანის მოტანაც.[15]

კომპიუტერული დანაშაულის სერიოზულ საფრთხედ თავად საზოგადოება ვლინდება, რომელიც უშუალოდ არის კავშირში ტექნოლოგიურ განვითარებასთან და მის ფართოდ გავრცელებასთან. კომპიუტერული სისტემები, ასევე მათი გაერთიანება სხვადასხვა კავშირგაბმულობის სისტემებში, ამყარებს შესაძლებლობას ელექტრონულ სივრცეში შეჭრის მხრივ. აღსანიშნავია, რომ ამგვარი შეღწევის ფორმები ფართოდ არის გავრცელებული და უკავშირდება როგორც წვრილმან, ტრადიციულ ზემოქმედებას, ასევე ისეთი მანიპულაციების განხორციელებას, რომელიც ადამიანის მხრიდან მაღალ მათემატიკურ და ტექნიკურ ცოდნას მოითხოვს. დილეტანტი დამნაშავეებიც კი ახერხებენ, რომ სხვადასხვა კომპიუტერულ სისტემაში შეიჭრან. მიუხედავად იმისა, რომ სახელმწიფოების უმრავლესობას საკმაოდ მოქნილი სისხლის სამართლის კანონები აქვს და ის შესაძლებლობას იძლევა, რომ დასჯილ იქნან ზემოთხსენებული ტიპის სამართალდამრღვევები, სოციალური და ტექნოლოგიური პროცესების ცვლილება წარმოქმნის ახალ-ახალ პრობლემებს, რომელთა ნაწილიც არ ჯდება ჩვეულ, სტანდარტულ საკანონმდებლო სისტემაში. როგორც მსოფლიო დონის პრაქტიკა ცხადყოფს, კომპიუტერული მანიპულაციები არ ემორჩილება (ყველგან არ ემორჩილება) მოქმედ სისხლის სამართლის კანონმდებლობას, ან იურიდიული თვალსაზრისით, ისინი არ შეიძლება დანაშაულად ითვლებოდეს. აქ წამოიჭრება კრიმინალიზაციასთან დაკავშირებული საკითხები. განსახილველი დანაშაულის მარეგილურებელი შესაბამისი ნორმები იძლევა დაპირებას, რაც, თავის მხრივ დაკავშირებულია ყველა ქვეყნის საკანონმდებლო ბაზის ნორმალური განვითარების უზრუნველყოფასთან.[16]

---

[15] სისხლის სამართლის კერძო ნაწილი, წიგნი II, ავტორთა კოლექტივი, მეოთხე გამოცემა, გამომც. „მერიდიანი“ 2012 , გვ 35-40;

[16] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004 გვ 67;

ქვეყნის საზღვრებს გარეთ, სადაც კომპიუტერულმა დანაშაულმა ფართო გავრცელება ჰპოვა, დაგროვილია დიდი გამოცდილება მის წინააღმდეგ საბრძოლველად. კომპიუტერული დანაშაული გავრცელდა საბჭოთა კავშირშიც. ერთ-ერთი პირველი ამგვარი დანაშაული მოხდა 1979 წელს ვილნიუსში, რაც გამოიხატა 78 584 რუსული რუბლის მოპარვაში.[17] შემდეგ მოხდა აღნიშნული დანაშაულის გავრცელება სხვადასხვა ქალაქებში. ხდებოდა თანხების გადატანა ერთი ანგარიშიდან იმ დროს არსებულ ელექტრო კომპლეს „ონეგაზე“. ფულის გადაგზავნა დაეხმარა არაკეთილსინდისიერ თანამშრომლებსაც, რომ ჩაედინათ ქურდობა სამეცნიერო-ტექნიკურ პროგრესზე ზემოქმედებით. საინტერესოა, რომ გამორჩენასთან ერთად წარმოიშვა დანაშაულის ჩადენის ისეთი გზები და საშუალებები, რომლებიც არდე სარგებლის მომტანად სულაც არ ითვლებოდა: მაგ. ფიქტიურ საბანკო ანგარიშზე უმნიშვნელო თანხის გადატანა იმ მიზნით, რომ საბოლოოდ დიდი თანხის დაგროვება მომხდარიყო. ასეთი მანიპულაციის განხორციელება ემყარება იმას, რომ კომპიუტერს შეუძლია წამში ასი ათასობით ოპერაციის განხორციელება მაღალკვალიფიციური ბუღალტერის მსგავსად იმ განსხვავებით, რომ ამ უკანასკნელმა შესაძლოა მთელი დღის განმავლობაში ატაროს იგივე ოპერაციები და საბოლოოდ, მხოლოდ ორი ათასი ოპერაცია განახორციელოს. განსახილველი დანაშაულის კრიმინალიზაციის ფარგლებში უნდა აღინიშნოს „ინფორმაციის ქურდობის“ საკითხი. კომპიუტერული ინფორმაციის გამოყოფის საკითხი განიხილებოდა აუცილებელ წინაპირობად, რაც გააადვილებდა დანაშაულსი ჩამდენთა დასჯას, რადგან, როდესაც კომპიუტერის მეშვეობით ხდებოდა ინფორმაციის არასანქცირებული კოპირება, ის შესაძლოა ქურდობად არც კი დაკვალიფიცირებულიყო, ვინაიდან, ამისთვის ორგანიზაციის ფონდიდან თანხის გატანა უნდა ყოფილიყო სახეზე, რადგან ასეთ დროს რეალურად გატანილი ინფორმაცია შეიძლებოდა ფონდთან კავშირში სულაც არ ყოფილიყო.[18]

[17] Сибиряков С. Л. , криминологическое Характеристика и Профилактика Компьютерных преступлений, Волгоград, 1999 p 11;

[18] батурин Ю. М. Право и политика в компьютерном круге. М., 1987, 126;

რიგი კანონდარღვევები დაკავშირებულია კომპიუტერის ნაწილიდან გამოყოფასთან. ასეთი ტიპის დანაშაულებმა ფართო გავრცელება ჰპოვეს დასავლეთში. ფაქტობრივად, არსებობს ორი ტიპის სახესხვაობა აღნიშნული დანაშაულისა: კომპიუტერის ფიზიკური ნგრევა და პროგრამის გაფუჭება. პირველი ტიპის დანაშაული ხდება საბჭოთა კავშირის სისხლის სამართლის კანონშემოქმედების ნაწილი, თუმცა მსგავსი ტიპის დანაშაულს ადგილი ფაქტიურად არ ჰქონია, რადგან, რადგან შესაბამისი სოციალურ-პოლიტიკური მოტივები მოსახლეობაში არ აღინიშნებოდა. ფსიქიკური აშლილობის ფონიც ნაკლებ აქტიური იყო გამომდინარე „კომპიუტერული ფობიის“ საკითხის დღის წესრიგში არარსებობის გამო, რაც, შესაბამისი ტექნოლოგიური მიღწევების ნაკლებობით იყო განპირობებული, ამიტომ კომპიუტერული დანაშაულის აქტუალობა, სწორედ პროგრამის გაფუჭებასთან არის კავშირში, რომელსაც უფრო ხშირად ახორციელებნ თავად დასაქმებული ადამიანები, რომლებიც უკმაყოფილონი არიან თავიანთი ხელფასით ან ხელმძღვანელობასთან ურთიერთობით ან თანამდებობით და ა.შ. პრობლემა მდგომარეობს იმაში, რომ რეალურად არ არსებობს შემუშავებული მექანიზმი, რომელიც შეძლებდა პროგრამის შექმნის შემდეგ კონტროლი გაეწია მასში ცვლილების და დარღვევის აღმოჩენაზე. კომპიუტერულ დანაშაულთან დაკავშირებული თავდასხმის ობიექტი შეიძლება დავყოთ სამ კატეგორიად: პირველი-თავად კომპიუტერი; მეორე- ობიექტები, რომელზეც, შესაძლოა განხორციელდეს თავდასხმა კომპიუტერის დახმარებით, როგორც ინსტრუმენტისა; მესამე-ობიექტები, რომელთათვისაც კომპიუტერი გამოდის, როგორც დამცავი მექანიზმი. [19]

როდესაც კომპიუტერი ხდება თავდასხმის სამიზნე, აუცილებელია მოხდეს მისი, როგორც სისტემის დათვალიერება და ნაწილების ერთმანეთისგან გამოყოფა. ვიწრო გაგებით, კომპიუტერი ესაა მთავარი ცენტრალური პროცესორი. პრაქტიკაში მისი დამოუკიდებლად გამოყენება არ ხდება პერიფერიული მოწყობილობებისგან. ასევე, ხშირად ის დაკავშირებულია ტერმინალებთან,

[19] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, გვ 26;

რომელთაც შეუძლიათ ჩართონ თავისი თავი და სხვა კომპიუტერები. ნებისმიერი ნაწილი ამ ერთიანი სისტემისა შესაძლოა გახდეს თავდასმის განხორციელების ობიექტი. ოპერაციული სისტემა და მასთან დაკავშირებული პროგრამები შესაძლოა განხილულ იქნეს, როგორც კომპიუტერული სისტემა, ასევე დამოუკიდებელი ობიექტი, რომლისთვისაც კომპიუტერი წარმოადგენს თავშესაფრის მსგავს საშუალებას.[20] კომპიუტერული ტექნიკის განვითარება ართულებს საკითხს, მკაფიოდ იქნეს გავლებული საზღვარი პროგრამულ უზრუნველყოფასა და აპარატულ რეალიზებას შორის. პროგრამულ უზრუნველყოფაზე საფრთხემ შესაძლოა გამოიწვიოს შეცდომები, პროგრამების მოდიფიცირება, მისი კიპორება ან თაღლითობა. კომპიუტერი მაინც წარმოადგენს დამოუკიდებელ საცავს კომპიუტერული ინფორმაციის, მონაცემებისა და პროგრამებისთვის. სხვადასხვა საგნებზე გავლენა და ზემოქმედება შესაძლოა დაიწყოს კოპირებით და დასრულდეს განადგურებით ან ქურდობით.

როგორც ავღნიშნე, კომპიუტერი თავადაც შესაძლოა გახდეს თავდასხმის ობიექტი ან მეორე შემთხვევაში, თვითონვე იყოს საშუალება დანაშაულის ჩადენისთვის. როდესაც კომპიუტერზე ზემოქმედებაზეა საუბარი, აქ კომპიუტერული დანაშაულის შესახებ საუბარი სრულიად ზედმეტია, როგორც განსაკუთრებული ტიპის დანაშაულზე. როდესაც მისი საშუალებით ხდება დანაშაულის ჩადენა, ამან შესაძლოა ზეგავლენა იქონიოს დანაშაულის მაკვალიფიცირებელი ნიშნების შეკრებაზე, თუმცა არსებობს მოსაზრებაც, რომ თავად ფაქტი კომპიუტერული დანაშაულის ჩადენის საშუალებად მისი გამოყენების შესახებ, უკვე წარმოადგენს კვალიფიკაციისთვის საკმარის საფუძველს, რაც, ჩემი აზრით, ნამდვილად არ არის აზრს მოკლებული და უფრო მართებულია, ვიდრე განხილული პირველი შემთხვევა. შემდგომი დეტალიზაცია ტექნიკურ საშუალებებამდე უფრო მეტად მნიშვნელოვანია კრიმინალისტიკისთვის (მაგ: დანაშაულის გახსნის გზები) და სხვ. კომპიუტერული დანაშაულის სპეციფიკიდან გამომდინარე, წარმოიშვა

[20] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012, გვ 34;

საჭიროება, რომ სისხლის სამართლის კანონმდებლობაში განხორციელებულიყო ცვლილებები და იურიდიულ სამეცნიერო ჩარჩოში დარეგულირებულიყო აღნიშნული საკითხები. [21]

მსოფლიო სტატისტიკის მიხედვით, ჩინეთი კიბერდანაშაულის მაჩვენებლით პირველ ადგილზეა. იქ ინტერნეტმომხმარებელთა 83% ამ დანაშაულის მსხვერპლია. შემდეგ მოდის ინდოეთი და ბრაზილია 76%-ით, მათ მოყვება აშშ მსხვერპლის 73%-ით. 2009-2010 წლებში კიბერდანაშაულთა რიცხვი საგრძნობლად გაიზარდა იაპონიაშიც, განსაკუთრებით იმატა ბავშვთა პორნოგრაფიის, მონაცემთა ბაზაზე თავდასხმის და საავტორო უფლებების დარღვევის შემთხვევებმა.[22] კიბერდანაშაულები გახშირდა საქართველოშიც- საავტორო უფლებების დარღვევის ფაქტები და მცდარი იმელიებით მოტყუებული მოქალაქეების რიცხვი გაიზარდა.

გაეროს მონაცემების თანახმად, ეკონომიკური მოგების მიზნით ჩადენილ კომპიუტერულ დანაშაულთა რიცხვი (კომპიუტერული სიყალბე, კომპიუტერული თაღლითობა) მსოფლიოს თითქმის ყველა რეგიონში კიბერდანაშაულთა საერთო რაოდენობის 1/3 შეადგენს. ქვეყნების გარკვეული ნაწილის ანგარიშებში ჭარბობს ისეთი დანაშაულები, როგორებიცაა: „თაღლითობა ელექტრონულ ვაჭრობასა და გადახდების დარგში“, „თაღლითობა ინტერნეტ აუქციონზე-როგორებიცაა „ebay“ (ამერიკის მრავალეროვნული და ელექტრონული ვაჭრობის კომპანია). [23]

[21] Dorothy E. Denning. (23.05.2000). "CYBERTERRORISM". Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html ;

[22] https://ccdcoe.org/tallinn-manual.html;

[23] სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, 2015, გვ 56;

თავი 2. კომპიუტერული დანაშაულის სისხლის სამართლებრივი დახასიათება

2.1. კომპიუტერული დანაშაულის ჩადენის ხერხები – ხელში ჩაგდების მეთოდები, ინფორმაციის ხელში ჩაგდება

პირდაპირი გზით ინფორმაციის ხელში ჩაგდება არის ერთ-ერთი ყველაზე ძველი მეთოდი კომპიუტერული დანაშაულის ჩასადენად. აღნიშნულის განსახორციელებლად მოწყობილობების შეკრება არ წარმოადგენს დიდ სირთულეს და მაღაზიებში ადვილად ხელმისაწვდომია, ამასთანავე, არც ისე დიდ თანხებთანაა დაკავშირებულ: მიკროფონი, რადიომიმღები, დიქტოფონი, მოდემი, პრინტერი. [24]

ინფორმაციის ხელში ჩაგდება შესაძლოა განხორციელდეს ან სატელეფონო არხების მეშვეობით, ან პრინტერის ხაზთან შეერთებით. მთელი ინფორმაცია იწერება. ზოგჯერ ინფორმაციის მიღების მეთოდების დემონსტრირებას ახდენენ თავად კომპანიები, რომლებიც აწარმოებენ ახალ ელექტრო მოწყობილობებს და გააქვთის გამოფენაზე, რათა საზოგადოებას დაანახონ შესაძლებლობანი. [25]

მოსმენისთვის საჭირო ობიექტქები შესაძლოა დაყოფილიქნეს სხვადასხვა სახეებად:

1) კაბელებისა და გაყვანილობების სისტემები. აღნიშნული სხვადასხვა დაფარულ მავთულხლართებს, კაბელებსა და სიხშირეთა ცვლილებებთან არის დაკავშირებული, რომლებიც შესაძლოა გამოყენებულ იქნეს, როგორც ერთჯერადი საუბრის გადასაცემად, ისე მრავალგზის.

2) მიწისზედა მიკროტალღური სისტემები. მრავალარხიანი სისტემები, როგორც სამთავრობო, ასევე ისინი, რომლებიც იმყოფება ჩვეულებრივ

[24] ზაქაშვილი უ., კიბერტერორიზმი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, გამომც. ,,მერიდიანი“, 2013, გვ 23;
[25] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, გამომც. „მერიდიანი“, 2012 , გვ 45-47;

მესაკუთრეთა მფლობელობაში და განკუთვნილია არამხოლოდ ხმასთან დაკავშირებულ ინფორმაციასთან, არამედ სამსახურებრივი ინფორმაციის გადაცემასთან.

3) თანამგზავრთან დაკავშირებული სისტემები. როგორც წესი, მოიცავს მრავალრიცხოვან მიწის ზედაპირზე არსებულ გადამცემ სადგურებს, ისეთებს, რომლებიც კერძო პირებისა და ასევე სახელწიფო ორგანიზაციების საკუთრებაშია.

4) სპეციალური სისტემები დაკავშირებული სამთავრობო კავშირებთან. მაგალითად: ამერიკის შეერთებული შტატების თავდაცვის სამინისტროს კვლევითი ორგანიზაციის კომუნიკაციის არხი: საბრძოლო არხი დაკავშირებული ავტომატური მოწყობილობის მეშვეობით დიალოგის გადაცემასთან და სხვ.[26]

1979 წლიდან ამერიკის შეერთებული შტატების ადმინისტრაციამ შეიუმუშავა სპეციალური სტრატეგია ინფორმაციის უნებართვო მითვისების შესაძლებლობის ზღვრის დაწესებისთვის, რომ მომხდარიყოდიდი ზარალის თავიდან აცილება. მას შემდეგ, რაც მოხდება მაგალითად კანონიერი მომხმარებლების კოდების მოპოვება, უკვე დამნაშავისთვის სირთულეს არ წარმოადგენს ნებისმიერი მსხვილი თანხის ხელში ჩაგდება. ერთ ასეთ შემთხვევას ადგილი ჰქონდა კალოფორნიის შტატში, სადაც ბანკის თანამშრომელმა ყოველგვარი სირთულისა და რაიმე საშუალების გამოყენების გარეშე განახორციელა კოდების ხელში ჩაგდება, მიუხედავად იმისა, რომ მათი ცოდნა არ შედიოდა აღნიშნული თანამშრომლის კომპეტენციაში. რამოდენიმე დღის განმავლობაში ამ პიროვნებამ საკუთარ ანგარიშზე გადარიცხა საკმაოდ სოლიდური თანხა და მიიმალა. საბოლოოდ იგი დაკავებულ იქნა. [27]

ელექტრო სიგნალების გარდამქმნელი მოწყობილობები, რომლებიც ყველა კომპიუტერშია ჩამონტაჟებული და წარმოადგენს მონაცემების ეკრანზე გადმოტანის საშუალებას, მნიშვნელოვნად ზრდის ამ მოქმედებას და ამ გზით მის

[26] http://www.nato.int/cps/en/natolive/news_52837.htm;
[27] Richard W. Aldrich, "CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME", USAF Institute for National Security Studies USAF Academy, Colorado, April 2000;

ირგვლივ მიმოფანტავს მონაცემებეს. ტალღები, რომლებიც წარმოიშობა ეკრანის მეშვეობით, იჭრებიან მინის გავლით. როგორც კი აღნიშნული სიგნალები მიიღება და გადაეცემა სხვა კომპიუტერს, შესაძლებელი ხდება გამოსახულება დაბრუნდეს, რომელიც ჩნდება წინამორბედი კომპიუტერიდან, რისთვისაც უნდა მივმართოთ კონკრეტულ ნაწილს თითოეული კომპიუტერის შემთხვევაში ინდივიდუალურად. აქედან გამომდინარე, კომპიუტერები განსხვავდებიან ერთმანეთისგან მათი „ხმის“ მიხედვით, რაც თავის მხრივ დამოკიდებულია ნაწილებზე და სხვა ტექნიკურ მახასიათებლებზე, რომლებიც განსხვავებული აქვთ ერთი სერიული წარმოების მოწყობილობებსაც კი. ამიტომ, ეკრანის გამოსხივების ჩვენების შესწავლით, შესაძლებელია მონაცემების შედარება უმარტივესი ტექნიკური საშუალებების გამოყენებით, რაც ხელმისაწვდომია თითოეული ადამიანისთვის. იმისათვის, რომ მოვიპოვოთ საიმარ საკითხებთან დაკავშირებული ინფორმაცია, საბანკო საიდუმლოებები ან სამეცნიერო კვლევების შედეგები, საჭორია მხოლოდ საორიენტაციო ანტენის ქონა, რომელიც ნებისმიერ რადიომოყვარულს აქვს, ასევე ტელევიზორებსაც, რომლებშიც აუცილებელია რამოდენიმე დიოდის ჩამაგრება. [28]

ინფორმაციის ქურდები, რომლებიც როგორც წესი, ადმინისტრაციული შენობებიდან მოშორებით ჩერდებიან მსუბუქ ან სატვირთო ავტომანქანებში, ხელთ აქვთ გადამცემი, მიმღები მოწყობილობა, რაც ეხმარება მათ ამგვარი გზით ზედმეტი ყურადღების მიპყრობის გარეშე შეიტყონ მონაცემები, რომლებიც ინახება კომპიუტერში და გამოიყენება სამუშაო პროცესში. პრაქტიკული ექსპერიმენტების ჩატარების დროს შესაძლებელი ხდებოდა ისეთი მონაცემების მიღება, რომლებიც ერთდროულად რამოდენიმე ტერმინალის ეკრანის მეშვეობით გამოჰქონდათ.[29] აღნიშნული ტერმინალები ერთმანეთისგან მოშორებით იყო განლაგებული და მონაცემების მიღება მათგან ხდებოდა ეკრანზე ამ ინფორმაციის გამოტანით ყოველ მომდევნოზე მისი წინამორბედიდან. ექსერტთა აზრით,

[28] კაცმანი ა., კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება, ჟურნალი სამართალი, 2000, №2 34-37;

[29] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, გამომც. „მერიდიანი“, 2012 , გვ 45-47;

თეორიულად შესაძლებელია ერთდროულად 50 ტერმინალიდან მოხდეს მონაცემთა გაქრობა. თუ, ქურდების მიერ თავიანთ სატელევიზიო მიმღებთან მოხდება ასევე ვიდეომაგნიტოფონის შეერთება, შესაძლებელია მთელი ინფორმაციის ერთად თავმოყრა, შემდეგ კი, მათი მშვიდად გაანალიზება. ამგვარი გზით მოხდა მონაცემთა მოპარვა ამერიკის შეერთებული შტატების არმიიდან, რომლებიც ს.რ.უ. (სღ) თანამშრომლებმა აღმოაჩინეს ქალაქ სან-დიეგოს სამალავში.

ე.წ. „ხოჭო“ მონტაჟდება კომპუტერებში, როგორც მიკროფონი, რათა განხორციელდეს კომპიუტერთან მომუშავე თანამშრომლების საუბრების ხელში ჩაგდება. ეს მარტივი მეთოდი გამოიყენება ძირითადად იმისათვის, რომ მოხდეს ინფორმაციის მიღება კომპიუტერის სისტემის მუშაობასთან, თანამშრომლებთან, უსაფრთხოების ზომებისა და სხვა საკითხებთან დაკავშირებით.[30]

ნარჩენებისგან გაწმენდა - ინფორმაციის მიღების აღნიშნული მეთოდი მდგომარეობს მონაცემთა ძიებაში, რომელთაც ტოვებენ მომხმარებლები კომპიუტერთან მუშაობის შემდეგ. ზემოთ ხსენებული პროგრამით ხდება „სანაგვე ყუთში“ ჩაყრილი ინფორმაციის შეგროვება, მათი დახარისხება საჭირო და გამოუსადეგარი ინფორმაციის სახეებად. არსებობს მოსაზრება, რომ კომპიუტერის მუშაობის შემდეგ, ოპერაციული მეხსიერება ყოველთვის არ “წულდება” (ბოლოს შესრულებული მუშაობა არ იშლება). სხვა მომხმარებელი მხოლოდ თავისი ინფორმაციის მცირედ ნაწილს ჩაწერს და შემდეგ მშვიდად კითხულობს წინამორბედ ჩანაწერებს, საიდანაც არჩევს მისთვის საჭიროს. ასეთი გზით შეიძლება აღმოჩენილ იქნეს პაროლები, მომხარებელთა სახელები და ა.შ. პრაქტიკული თვალსაზრისით, მიმაჩნია საკმაოდ ჭკვიანურ მეთოდად, რომლის გამოყენებაც ბევრი დამნაშავისთვის დამანაშაულის ჩადენის საკმაოდ იოლ და ნაკლებად შეუმჩნეველ საშუალებას წარმოადგენს. [31]

[30] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012 გვ 34;

[31] ზაქაშვილი უ., კიბერტერორიზმი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, გამომც. ,, მერიდიანი“, 2013, გვ 23;

თავი 3. კომპიუტერული დანაშაულის კრიმინოლოგიური დახასიათება

3.1. კომპიუტერულ დანაშაულთა კრიმინოლოგიური დახასიათების მნიშვნელობა

ქართულ იურიდიულ მეცნიერებაში ფაქტობრივად არ არსებობს რაიმე განზოგადებული მონაცემები კომპიუტერული დანაშაულის კრიმინოლოგიური დახასიათების ელემენტების ფორმირებისათვის.

უკეთესად საქმე არც ყოფილ მოკავშირე რესპუბლიკებშია. როგორც რუსეთის ფედერაციაში ჩატარებულმა კვლევებმა აჩვენეს, რომ გამოკითხულ რესპოდენტთა

55% ამ კატეგორიებზე საერთოდ არაფერი იცის, 39% ნაწილობრივ იცნობს კომპიუტერული დანაშაულის ჩამდენ პირთა კრიმინალისტიკური დახასიათებას მაგრამ არაიურიდიული წყაროებიდან, საიდანაც 66% მოდის მასობრივი ინფორმაციის საშუალებებზე, 28% კი კინო- და ვიდეოფილმებიდან (ძირითადად უცხოური წარმოების)[32]

არადა რესპოდენტებად გამოდიოდნენ შინაგან საქმეთა ორგანოების საქალაქო და რაიონული განყოფილებების და სამმართველოების უფროსები და მათი მოადგილეები (საგამოძიებო განყოფილებების უფროსები), რომლებთაც პირველ რიგში უნდა ფლობდნენ სამეცნიერო ინფორმაციას იმაზე, რასთანაც უნდა ჰქონდეთ საქმე თავიანთ უშუალო პრაკტიკულ საქმიანობაში.[33]

რა თქმა უნდა ასეთი მდგომარეობას დამაკმაყოფილებლად ვერ ჩავთვლით. ამიტომ ვფიქრობთ, როგორც სამეცნიერო ისე პრაკტიკული თვალსაზრისიდან აქტუალურია დანაშაულებრივ ქმედებათა ამ კატეგორიის კრიმინოლოგიური დახასიათების პრობლების დამუშავება.

---

[32] http://www.melik.narod.ru/#_2_1;

[33] სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული,2015, გვ 56;

კომპიუტერული ინფორმაციის სფეროში არსებული დანაშაულები ახალი ხილია ჩვენ რეალობაში. ამ დანაშაულთა გამოძიების სამამულო პრაკტიკა ნულოვანია, ვინაიდან მხოლოდ უკანასკნელ წლებში პროგრამულ-ტექნიკური საშუალებების განვითარების და მოსახლეობის ე.წ. „კომპიუტერული განათლების“ დონის გაზრდის შედეგად ინფორმაციული სისტემები დაინერგა ისეთ დარგებში, როგორიცაა ბუღალტრული აღრიცხვა, ეკონომიკური გამოთვლები, პლანირება და ა.შ.

კომპიუტერული ინფორმაციის სფეროში განხორციელებულ დანაშაულთა საზოგადოებრივი საშიშროება სულ უფრო და უფრო აშკარა ხდება.

მოცემულ სფეროში შეიმჩნევა სამართლებრივი რეგლამენტაციის ნაკლებობა და ის ფაქტი, რომ გამომძიებლებს არ გააჩნიათ ცოდნა თანამედროვე ინფორმაციულ ტექნოლოგიებზე მნიშვნელოვან წილად ხელს უწყობს ამ ტიპის მართლსაწინააღმდეგო ქმედებების მაღალ ლატენტურობას და დაუსჯელობის სინდორმის დათესვას.[34]

ერთმანეთისაგან განასხვავებენ კომპიუტერული დანაშაულის შემდეგ კრიმინოლოგიურ ჯგუფებს: ეკონომიური კომპიუტერული დანაშაულები,კომპიტერული დანაშაულები მიმართულნი პირადი უფლებების და კერძო სფეროს ხელშეუხებლობის წინააღმდეგ, კომპიუტერული დანაშაულები საზოგადოებრივი და სახელმწიფო ინტერესების წინააღმდეგ.[35]

ყველაზე უფრო სახიფათო და გავრცელებულია – ეკონომიური კომპიუტერული დანაშაულები – რომლებიც მოიცავენ კომპიუტერულ თაღლითობას (სხვის ხარჯზე არამართლზომიერი გამდიდრება ავტომატიზირებული ინფორმაციული სისტემების მართლსაწინააღმდეგო გამოყენების შედეგად), კომპიუტერული ეკონომიკური შპიონაჟი და პროგრამების ქურდობა, კომპიუტერული საბოტაჟი, მომსახურებათა და „კომპიუტერული დროის“ ქურდობა, ავტომატიზერებულ ინფორმაციულ სისტემაში თვითნებური შეღწევა, ტრადიციული ეკონომიური დანაშაულები, ჩადენული კომპიუტერების

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

[35] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3, 2012, გვ 23;

მეშვეობით. ეკონომიური კომპიუტერული დანაშაულები ყველაზე ხშირად ხორციელდება ანგარებითი მოტივებით იმ ორგანიზაციების თანამშრომლების მიერ, სადაც გამოიყენება კომპიუტერები, მაგრამ შეიძლება განხორციელებულ იქნეს სხვა პირების მიერ, ღია კომპიუტერული სისტემების (საბანკო ავტომატი და ა.შ.) ბოროტად გამოყენების შედეგად ან სისტემაში არამართლზომიერი შეღწევის შედეგად. კომპიუტერული თაღლითობები (კომპიტერულ მატარებლებზე არსებული საბანკო ანგარიშების არამართლზომიერი გამოყენება, უკანონო შემოსავლების მიღება ხელფასის, სოციალური დახმარებების, ჰონორარების სახით ავტომატიზირებული ინფორმაციული სისტემების „მოტყუების“ შედეგად და ა.შ.), პროგრამების ქურდობა („კომპიუტერული მეკობრეობა“), კომპიუტერული სისტემისაგან მომსახურების არამართლზომიერი მიღება (კომპიუტერული დროის ქურდობა) ფართოდ არის გავრცელებული დასავლეთის ქვეყნებში და შეადგენს კომპიუტერული დანაშაულების მნიშვნელოვან ნაწილს. [36]

პირადი უფლებების და კერძო სფეროს ხელშეუხებლობის წინააღმდეგ მიმართული დანაშაულები უფრო ხშირად გამოიხატება კომპიუტერულ სისტემაში პირის შესახებ არასწორი და არაკორექტული მონაცემების შეტანით, სწორი მონაცემების არამართლზომიერი შეგროვებით, კომპიუტერულ მატარებლებზე არსებული ინფორმაციის გახმაურებით (მაგალითად, საბანკო საიდუმლოების გახმაურება, კლიენტების ბაზებით ვაჭრობა და ა.შ.

სახელმწიფოს და საზოგადოების ინტერესების წინააღმდეგ მიმართული დანაშაულები მოიცავენ დანაშაულებს სახელმწიფო და საზოგადოებრივი უსაფრთხოების წინააღმდეგ, საზღვარგარეთ ინფორმაციის გადაცემის წესების დარღვევას, თავდაცვითი სისტემების მუშაობის დეზორგანიზაციას, ავტომატიზირებული ინფორმაციული სისტემების ბოროტად გამოყენებას არჩევნებზე ან საპარლამენტო გადაწყვეტილებების გაყალბების მიზნით.[37]

[36] გორაშვილი გ., ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები, გამომც. „უნივერსალი“, 2010, გვ 62;

[37] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, 2004, გვ 65;

თავი 4. კიბერტერორიზმი

4.1. კიბერტერორიზმის ზოგადი და სისხლისსამართლებრივი დახასიათება

„მრავალი რევოლუციური ტექნოლოგიის მსგავსად, კომპიუტერული ტექნოლოგიები თავის თავსში უზარმაზარ პოტენციალს ატარებენ როგორც პროგრესისთვის, ისე ბოროტად გამოყენებისთვის - ქსელური ინფორმაციის ხელყოფა, კომპიუტერული მეკობრეობა, ელექტრონული ჯაშუშობა, პორნოგრაფიის გავრცელება და სხვ“.[38] „საბრძოლო იარაღმა დროთა განმავლობაში უდიდესი ევოლუცია განიცადა. სატევარი, შუბისპირი, მშვილდი, ისარი, ხმალი, ფარი, მუზარადი, ზარბაზანი... მერე ტანკი, ავტომატი, ტყვიამფრქვევი და ბირთვული იარაღიც. გაუმჯობესდა იმდენად, რომ კომპიუტერის კლავიატურითაც შესაძლებელი გახდა არანაკლები ზიანის მიყენება მოწინააღმდეგისათვის. გაჩნდა ახალი ტერმინები, როგორიცაა: კიბერტერორიზმი, კიბერ ომი, კიბერ თავდასხმა“.[39] „ტერორიზმის გარშემო ერთგვარი აზრთა სხვადასხვაობა არის, რის გამოც რთულია იგი კონკრეტული დეფინიციით განვსაზღვროთ. თავად ტერორისტებზე ამგვარი გამონათქვამიც კი არსებობს: „ერთისთვის ტერორისტი, სხვისთვის თავისუფლებისათვის მებრძოლია.“ ეს სიტყვები ჟერარდ სეიმურმა 1975 წელს, თავის წიგნში „ჰარის თამაშში“ მოიხსენია.

აშშ-ს გამოძიების ფედერალური ბიუროს (Federal Bureau of Investigation - FBI) მიხედვით კი ტერორიზმი არის: „ძალისა და სისასტიკის უკანონო გამოყენება ადამიანების ან მათი საკუთრების წინააღმდეგ, მთავრობის იძულებისათვის, საზოგადოების ან და მისი რომელიმე სეგმენტის დასაშინებლად და გამყარებულია პოლიტიკური ან სოციალური მიზნებით.“

38 ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“, 2017, გვ 281;
39 ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 , 2012, გვ122;

ამერიკის შეერთებული შტატების მთავრობის დეპარტამენტის პოზიცია ტერორიზმის შესახებ შემდეგნაირად არის ჩამოყალიბებული: "წინასწარ დაგეგმილი, პოლიტიკურად მოტივირებული სისასტიკე, ჩადენილი სამოქალაქო სამიზნეებზე, ქვენაციონალური ჯგუფის ან საიდუმლო აგენტების მიერ, რომელიც საზოგადოების დაშინებას ემსახურება."[40]

„ტერორისტულმა აქტებმა ქუჩიდან ვირტუალურ სივრცეში გადაინაცვლა. თუ ჩვეულებრივი ტერორისტები ხელყუმბარებითა და ავტომატებით იბრძვიან, კიბრტერორისტები ომს ვირტუალურ სივრცეში აწარმოებენ. ჩვენი ცხოვრება სულ უფრო და უფრო დამოკიდებული ხდება კომპიუტერზე. ყველა სტრატეგიულად მნიშვნელოვან ობიექტზე მოქმედებენ კომპიუტერები - მეტროპოლიტენი, სამოქალაქო ავიაცია, ელექტრომომარაგება, რადიო, ტელევიზია, და სხვ. აღნიშნული ობიექტების სერვერების მწყობრიდან გამოყვანით, განვითარებულ სახელმწიფოთა სხვადასხვა ინფრასტრუქტურები დიდ მატერიალურ ზარალს განიცდიან, რომ აღარაფერი ვთქვათ ადამიანთა მსხვერპლზე."[41] „დღეს სახელმწიფოებს და, განსაკუთრებით, განვითარებულ ქვეყნებს უწევთ ახალ, უფრო რთულ საფრთხეებთან გამკლავება. კიბერმზვერავებმა, კიბერჯარისკაცებმა, კიბერტერორისტებმა, ერთი ან რომელიმე ძალის, იდეოლოგიის მხარდამჭერმა ჯგუფებმა ვირტუალურ სამყაროში დაიდეს ბინა.

კიბერსაფრთხეები არა მარტო ტექნოლოგიურად განვითარებულ ქვეყნებს, არამედ ნაკლებად განვითარებულ ქვეყნებსაც ემუქრება. პოტენციური სამიზნე ქვეყნები კიბერუსაფრთხოებას სერიოზულად უდგებიან. ქვეყნები, თავისი კულტურული, სოციალური, ეკონომიკური, გეოგრაფიული და პოლიტიკური მდგომარეობის შესაბამისად აყალიბებენ კიბერპოლიტიკას. ეძებენ ეფექტურ გზებს, ქმნიან და ცვლიან სტრატეგიულ დოკუმენტებს, ტაქტიკას და მიდგომის მეთოდებს.

---

40 პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, 2012, 45;

41 ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი" , 2017, გვ 281

ყოველდღიურად ხდება კიბერდანაშაული ინდივიდების, სხვადასხვა ბიზნესისა თუ მთავრობის წინააღმდეგ. კიბერომი უკვე წარმოადგენს საფრთხეს, რომლის წინააღმდეგაც ეროვნული უსაფრთხოების ექსპერტები ეძიებენ უფრო ეფექტურ, თანმიმდევრულ სტარტეგიებსა და საერთაშორისო შეთანხმებებს. [42]

კიბერთავდასხმები შესაძლოა იყოს სპეცოპერაციებისა და საჰაერო თავდასხმების ეკვივალენტური. სპეციალური დანიშნულების რაზმების ან საჰაერო ძალების გაწვრთნისა და აღჭურვისათვის საჭირო ფინანსურ და ადამიანურ რესურსებთან შედარებით ჰაკერები, კომპიუტერები და ბოტნეტები თუ სხვა სახის კიბერ და ინფორმაციული იარაღის შექმნა გაცილებით მცირე დროსა და სახსრებს მოითხოვს. ამან შესაძლოა საფრთხე შეუქმნას ქვეყნის კრიტიკულ ინფრასტრუქტურას, ეკონომიკას და მოსახლეობის ფსიქოლოგიურ მდგომარეობას. [43]

კიბერკრიმინალურმა დაჯგუფებებმა და კიბერდამნაშავე ქვეყნებმა შესაძლოა მცირედი დანახარჯებით განახორციელონ სამიზნე ქვეყნის ეკონომიკისა და მისი მნიშვნელოვანი ინფრასტრუქტურის დესტაბილიზაცია. ექსპერტები დღემდე დაობენ იმასთან დაკავშირებით, თუ როგორი განსაზღვრება უნდა მიეცეს კიბერშეტევებს - როგორც კრიმინალური ქმედება თუ როგორც საომარი ქმედება?

მსოფლიოში ისეთი ბერკეტის არსებობისას, როგორიც ინტერნეტია, კომპიუტერული უნარებით აღჭურვილი აქტიური ადამიანებისგან ხშირად ყალიბდებიან კარგად გაწვრთნილი ჰაკტივისტები, ჰაკერ-ტერორისტები და ჰაკერ-მებრძოლები და ისინი მთელ მსოფლიოში არიან გაბნეული“.[44]

„ფაქტობრივად, ტერორისტულ ორგანიზაციებმა უახლოესი კომპიუტერული ტექნოლოგიები ტერორისტულმა აქტის ჩდენის საშუალებად

[42] http://www.chebucto.ns.ca/Current/HalifaxSummitG7/;
[43] Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448 (Based on article 12 of the Council Framework Decision of 24.02.2005 on attaks against information systems);
[44] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, 5-6;

აქციეს და ამით აღნიშნული დანაშაული უფრო საშიშ მოვლენად ექცა მსოფლიოს. კიბერტერორიზმი არის თანამედროვე ეპოქის სწრაფი ტექნოლოგიური განვითარებისა და წინსვლის შედეგი. მოგეხსენებათ, ტექნოლოგიის განვითარებას ყოველთვის თან ახლავს ჰაკერების დიდი ინტერესი, მოახდინონ ჰაკერული ცოდნის დემონსტრირება ანუ კიბერტერორის განხორციელება. მოქმედების მექანიზმი კი შემდეგშია: დათქმულ დროს, ასეულ ათასობით კომპიუტერიდან ხდება გასატეხი სერვერიდან ინფორმაციის ერთდროული მოთხოვნა. სერვერი ვერ ძლებს და იჭედება“.[45]

„უნდა აღინიშნოს, რომ კიბერ საფრთხეები ემუქრება არა მხოლოდ ღია სისტემას, არამედ ასევე საშიშროებას ქმნის დახურული სისტემისთვისაც. არც დახურული სისტემები - ქსელები, რომლებიც პირდაპირ არ არიან დაკავშირებული ინტერნეტთან - არიან სრულად დაცული. ამას სტაქსნეტის და ვიკილიქსის მაგალითებიც ცხადყოფს: ერთმა - ჭია ვირუსმა, რომელმაც გაანადგურა ათასი ცენტრიფუგა ნათანზის ბირთვულ ელექტროსადგურზე, და მეორემ - აშშ-ის არმიის ყოფილი რიგითი ჯარისკაცის ბრედლი მენინგის მიერ ვებგვერდ „ვიკილიქსისათვის“ ათიათასობით აშშის სახელმწიფო საიდუმლო დოკუმენტის გადაცემით - უდიდესი საფრთხის წინაშე დააყენა ამერიკის სახელმწიფო უსაფრთხოება. ინტერნეტი არ არის ერთადერთი გზა კომპიუტერულ სისტემებში შესაღწევად, თუმცა ეს არის ფართო და გახსნილი გზა“.[46]

„ეტიმოლოგიურად „კიბერტერორიზმი“ ორი სიტყვისაგან - „კიბერ“ და „ტერორიზმისაგან“ შედგება. წინსართი „კიბერ“ ნიშნავს კიბერნეტიკულ სივრცეს, ვირტუალურ სივრცეს, ანუ კომპიუტერის მეშვეობით, მოდელირებულ სივრცეს, რომელშიც ინახება ინფორმაცია პირების, ფაქტების, მოვლენების, პროცესების,

[45] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012, 123;
[46] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, გვ 6;

ნივთების შესახებ მათემატიკური, სიმბოლური ან ნებისმიერი სხვა სახით და მოძრაობის პროცესშია ლოკალური ან გლობალური კომპიუტერული ქსელით“.[47]

„ტერმინი - „კიბერტერორიზმი“, ინფორმაციული ტექნოლოგიების ლექსიკონში 1997 წელს გაჩნდა, როდესაც ფედერალური გამოძიების ბიუროს აგენტმა მარკ პოლიტმა განსაზღვრა ტერორიზმის აღნიშნული სახეობა როგორც „სამოქალაქო მიზნების მიმართ, წინასწარ განსაზღვრული პოლიტიკურად მოტივირებული შეტევები ინფორმაციულ, კომპიუტერულ სისტემებზე, კომპიუტერულ პროგრამებსა და მონაცემებზე, სუბნაციონალური დაჯგუფებების ან საიდუმლო აგენტების მხრიდან, გამოხატული ძალადობით“[48]

„ცნობილი ექსპერტი დოროთი დენინგი კიბერტერორიზმს განსაზღვრავს როგორც „ხელისუფლების ორგანოების იძულებითი დაყოლიების მიზნით პოლიტიკური ან სოციალური მიზნების მისაღწევად კანონსაწინააღმდეგო შეტევას ან შეტევის განხორციელების საფრთხეს კომპიუტერებზე, ქსელსა ან მასში არსებულ ინფორმაციაზე“ [49]

„ტერმინი „კიბერტერორიზმი“ პირველად 1980 წელს კალიფორნიის უსაფრთხოები სადადაზვერვის ინსტიტუტის მეცნიერ თანამშრომელმა ბარი კოლინმა გამოიყენა ტერორისტული ორგანიზაციების მიერ კიბერსივრცის აქტიურად გამოყენების აღსანიშნავად. მოგვიანებით,აშშ-ის კიბერტერორიზმის ერთ-ერთი წამყვანი ექსპერტი, ჯორჯთაუნის უნივერსიტეტის პროფესორი დოროთი დენინგი ინტერნეტში საქმიანობის კლასიფიკაციის შემდეგ ასპექტებს გამოყოფს: „აქტივიზმი“ და „კიბერტერორი“. კიბერტერორიზმი წარმოადგენს ტერორიზმისა და კიბერსივრცის შერწყმას. ის მოიცავს პოლიტიკურად მოტივირებულ ჰაკერულ ოპერაციებს,რომელთა მიზანია პოლიტიკური თუ

[47] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“ , 2017, გვ 281;

[48] Larry J. Siegel (2008) Criminology- Cyber crime and technology - Cyber terrorism: Cyber Crime With Political Motives . pp № 449;

[49] Dorothy E. Denning. (23.05.2000). "CYBERTERRORISM". Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html;

ეკონომიკური ხასიათის დამანგრეველი შედეგების მიღწევა. დენინგის ამგვარი კლასიფიკაცია გამყარებულია „Computer Emergency“ ჯგუფის სტატისტიკური კვლევითი მონაცემებით. ამ მონაცემების მიხედვით, 2001 წელს დაფიქსირებულია ქსელებზე შეტევის 52 685 შემთხვევა, რომელსაც შეეძლო აშშ-ის ინფრასტრუქტურის პარალიზება. ეს ციფრი ორჯერ მეტია 2000 წლის მონაცემებთან შედარებით. მას შემდეგ ინციდენტების რაოდენობა კატასტროფულად მატულობს, საკრედიტო ბარათების სკანირებით დაწყებული და სხვა სახის კომპიუტერული შეტევით დამთავრებული“.[50]

„ტერორისტები კიბერსივრცეს იყენებენ შემდეგი მიზნებისათვის[51]:

- ინტერნეტის საშუალებით პოტენციურ სამიზნეებზე შეაგროვონ ინფორმაცია მდებარეობის და მახასიათებლებისგანსასაზღვრად;

- ტერორისტულ მოძრაობათა მხარდაჭერისათვის ფინანსური რესურსების შესაგროვებლად;

- ტერორისტული მოძრაობების შესახებ დეტალური ინფორმაციის შემცველი ვებგვერდების შესაქმნელად, რაც მოიცავს დაჯგუფებების მიზნების, ამოცანების, პროტესტის გამოხატვის ფორმების და დაჯგუფებებთან დაკავშირებული სხვა სახეობის შემცველ ინფორმაციას. რითაც ტერორისტული მოძრაობები ცდილობენ ტერორისტების მხარდამჭერ ჯგუფებზე სინერგიულ ზემოქმედებას, რაც გულისხმობს აღნიშნულ ჯგუფებზე გავლენის მოხდენას მართვის არაკლასიკური, ქვეცნობიერი მეთოდების გამოყენებით;

- ფინანსური ინსტიტუტებისგან ფულის გამოძალვისთვის, რათა მათ თავი აარიდონ კიბერტერორიზმის აქტებს და არ დაკარგონ რეპუტაცია;

- ინტერნეტის ფართო აუდიტორიის გამოსაყენებლად უკვე დაგეგმილი ან სამომავლო მოქმედებების, ან განხორციელებულ ტერაქტებზე პასუხისმგებლობის

[50] გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008, 67;

[51]Tropina Tatyana Lvovna (2005) - Cybercriminality: concept, a condition, criminally-legal measures of struggle from http://www.crime.vl.ru/index.php?p=986&more=1&c=1&tb=1&pb=1;

აღების თაობაზე ინფორმაციის გასავრცელებლად, აგრეთვე, მსგავსი შინაარსის ელექტრონული წერილების მასობრივად დასაგზავნად;

- ინტერნეტის გამოყენება ინფორმაციულ-ფსიქოლოგიური ზემოქმედებისთვის, „ფსიქოლოგიური ტერორიზმის“ ინიცირებისათვის. ინტერნეტის საშუალებით საზოგადოებაში შიშისა და პანიკის დასანერგად ან დეზინფორმირების გზით ადამიანების შეცდომაში შესაყვანად. აგრეთვე, ტერორისტული ორგანიზაციები აქტიურად იყენებენ ინტერნეტის მსოფლიო ქსელს სხვადასხვა ჭორის და მათ შორის საგანგაშო ინფორმაციის გასავრცელებლად;

- ტერორისტულ საქმიანობაში სათანადო პოტენციალის და გამოცდილების მქონე პიროვნებების ჩასართავად, რომელთათვისაც ცნობილი არ უნდა იყოს მათი საქმიანობის ნამდვილი მიზანი. მაგალითად, კომპიუტერული ხულიგნების დაყოლიება, რომელთათვის უცნობია, თუ რას ემსახურება მათი სამომავლო საქმიანობა;[52]

- ელექტრონული ფოსტით ან ელექტრონული შეტყობინებების „დაფებით“ დაშიფრულ შეტყობინებათა გასაცვლელად;

- ტერორისტული შინაარსის ვებგვერდების განსათავსებლად, სადაც საუბარია ფეთქებად ნივთიერებებსა თუ საშუალებებზე, შხამებზე, მომწამვლელ გაზებსა და მათი დამოუკიდებლად მიღება–დამზადების ინსტრუქციებზე“.[53]

„სად გადის ზღვარი ჰაკერის მიერ ჩადენილ მარტივ ხულიგნობასა, სამთავრობო დაფინანსების კიბერ ოპერაციებსა და კიბერ ომებს შორის? ეს დღესდღეობით კიბერ სივრცის ერთ-ერთი ყველაზე აქტუალური კითხვაა, რადგან კიბერ შეტევა შეიძლება გახდეს საპასუხო სამხედრო აგრესიის მიზეზი. დღეს ამერიკის შეერთებული შტატების თავდაცვის დეპრატამენტმა უკვე მიიღო ინიციატივა, რომლის მიხედვითაც იგი სახელმწიფოს წინააღმდეგ

[52] Сибиряков С. Л. , криминологическое Характеристика и Профилактика Компьютерных преступлений, Волгоград, 1999 p 11;

[53] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012, 170;

განხორციელებულ სამთავრობო კიბერ შეტევას, კონვენციური სამხედრო მოქმედებებით უპასუხებს. ასევე გასათვალისწინებელია ჩრდილოატლანტიკური ალიანსის პოტენციალიც, რომელიც მსგავსი სცენარებით ყოველწლიურ სამხედრო სწავლებებსაც მართავს – Nato Cyber Coalition. ამ რეალობაში კიბერ აქტივობები განსაკუთრებულ საფრთხეს ატარებს, რომელმაც შეიძლება კოლოსალური მასშტაბების სამხედრო მოქმედებები გამოიწვიოს. მაგალითად, თუ შეტევა განხორციელდა ალიანსის წევრი სახელმწიფოს მიმართ, მოსალოდნელია რომ გამოყენებულ იქნება ვაშინგტონის შეთანხმების მეხუთე პუნქტი, რომლის მიხედვითაც წევრი სახელმწიფოს მიმართ განხორციელებული შეტევა ითვლება შეტევად ალიანსის წევრ-სახელმწიფოებზე“.[54]

„ინტერნეტის საომარ მოქმედებებში გამოყენება თანამედროვე მეთოდია და მასში ხშირად არიან ჩართული რიგითი მოქალაქეები თუ კიბერსაომარი საშუალებებით შეიარაღებული ან ნაწილობრივ შეიარაღებული მებრძოლები. ასეთ განვითარებას სამი სახის შედეგი აქვს: პირველი - სხვადასხვა ჯგუფი, რომლებიც სახელმწიფოს სახელით არ მოქმედებენ. მეორე - სახელმწიფო ძალები გადადიან მოქმედების ახალ სტრატეგიებზე და ქმნიან ან იყენებენ კიბერმებრძოლთა ჯგუფებს და მესამე - ინტერნეტის მეშვეობით იწყება ახალი სახის მებრძოლთა ტიპის ჩამოყალიბება, რასაც ინდივიდუალური კიბერმებრძოლები ეწოდება. ზოგიერთი ქვეყნის მთავრობას არა მხოლოდ შემწყნარებლური დამოკიდებულება აქვს კიბერკრიმინალური დაჯგუფებების მიმართ, არამედ ქირაობს კიდეც მიზანში ამოღებული ქვეყნების წინააღმდეგ“.[55]

„ყურადსაღებია ტერმინი „ქსელური ომი“ რომელიც დევიდ რონფელდმა და ჯონ არკრილამ შემოიტანეს. დევიდ რონფელდის განსაზღვრებით ომის ეს სახეობა - „წარმოადგენს საზოგადოებრივი კონფლიქტის ერთ-ერთ სახეს, რომელიც წარმოებული კომუნიკაციის საშუალებების გამოყენებით მიმდინარეობს

[54] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, გამომცემლობა ,,სანი“, თბ., 2012, 46;
[55] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, გვ 7;

ინტერნეტის მეშვეობით“.[56] ჯონ არკრილას განმარტებით კი, „ქსელური ომი“ - „სოციალურ დონეზე, ტრადიციული საომარი ძალის გამოყენების გარეშე, კონფლიქტების წარმოების ახალი ხერხია, როდესაც პროტაგონისტები (მთავარ როლში მყოფი ადამიანები) იყენებენ ორგანიზაციის ქსელურ ფორმებს და მასთან დაკავშირებულ დოქტრინებს, სტრატეგიებს და ტექნოლოგიებს, რომლებიც შეესაბამება ინფორმაციული საზოგადოებას ეპოქას.“[57]

„ინფორმაციული ომის განსაზღვრების ძირითად ცნებებს წარმოადგენს netwar და cyber war. ორივე კონფლიქტის წარმოების ერთგვარ ფორმაა, რომლის დროსაც შესაძლებელია გამოიყენონ კიბერტერორიზმის მეთოდები დასაშუალებები. netwar – კიბერსივრცეში კონფლიქტის წარმოებაა სოციალურ დონეზე, ხოლო cyber war - კიბერსივრცეში კონფლიქტის წარმოებაა სამხედრო დონეზე. მათ შორის განსხვავება კიბერსივრცეში კონფლიქტის წარმოების ფორმა და მიზანია“.[58]

„აგრეთვე, საყურადღებოა სამომავლო ტერორისტული ოპერაციების დაგეგმვის და მათი განხორციელების მიზნით, ტერორისტული ორგანიზაციების და კიბერდამნაშავეთა დაჯგუფებებს შორის აქტიური თანამშრომლობა. კიბერდამნაშავეებს გააჩნიათ ის ტექნიკური უნარჩვევები და პოტენციური შესაძლებლობები, რაც საჭიროა კიბერსივრცეში ტერორისტული ოპერაციების ჩასატარებლად და კინეტიკურ სფეროში ჩასატარებელი ტერორისტული ოპერაციების ტექნიკური მხარდაჭერისთვის. ამიტომაც, ტერორისტული დაჯგუფებების მხრიდან არსებობს დაინტერესება გამოიყენონ კიბერდამნაშავეები ტერორისტული საქმიანობისთვის. მრავალი ტერორისტული დაჯგუფება თუ ორგანიზაცია დღეს უფრო მეტად ორიენტირებულია კიბერსივრცეში ტერორისტული აქტების განხორციელებისკენ. აღნიშნულს განსაზღვრავს რამდენიმე მნიშვნელოვანი ფაქტორი, მათ შორის: კიბერსივრცეში ჩატარებული

[56]Arquilla J. and Ronfeldt D. (1993) - CYBERWAR IS COMING!: Both Netwar and Cyberwar Are Likely – pp. № 27;

[57] Arquilla J. and Ronfeldt D. (2001) Networks And Netwars- THE ADVENT OF NETWAR (REVISITED): Defi ning Netwar pp. № 6;

[58] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012, 172.

ოპერაციების დაბალი ბარიერი, ადამიანური რესურსების ეფექტიანი გამოყენება ოპერაციის ფარულობა. და მობილობა“.[59]

„კიბერტერორიზმი წარმოადგენს კიბერშეტევის ერთ-ერთ სახეს. მისი ნათელ მაგალითად შეიძლება დავასახელოთ პოლიტიკური მოტივაციის მქონე კიბერშეტევა, რომელიც იწვევს სიკვდილიანობას ან სხეულის დაზიანებას, აფეთქებას ან მნიშნველოვან ეკონომიკურ დანაკლისს. შეტევა, რომ მივიჩნიოთ კიბერტერორიზმად, ის უნდა ატარებდეს პიროვნების ან ქონების წინააღმდეგ მიმართულ ძალადობის სახეს, ან უნდა იწვევდეს შიშისათვის საკმარის საფუძველს.

4.2. კიბერტერორიზმი საქართველოს სისხლის სამართლის კოდექსის მიხედვით

საქართველოს კანონდებლობით კიბერტერორიზმი განმარტებულია, როგორც კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას, ჩადენილი მოსახლეობის დაშინების ან ხელისუფლების ორგანოებზე ზემოქმედების მიზნით. კიბერტერორიზმის კლასიკური დეფინიციის მიხედვით ის წარმოადგენს კრიმინალურ ქმედებას, რომლის დროსაც გამოიყენება კომპიუტერული და ტელესაკომუნიკაციო საშუალებები და მიზანი კრიტიკული ინფრასტრუქტურის მწყობრიდან გამოყვანაა. კიბერტერორირზმს შედეგად შეიძლება მოჰყვეს ადამიანთა მსხვერპლი, მატერიალური დანაკარგი და მრავალი სხვა პრობლემა“.[60]

„კოდექსის ძველი რედაქციით კიბერტერორიზმი შემდეგნაირად იყო განმარტებული: „კიბერტერორიზმი, ესე იგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების

[59] იხილეთ იქვე, 167გვ.

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.“ 2012 წლის 2 მარტის ცლილებების შემდეგ კი მუხლი ჩამოყალიბდა შემდეგნაირად: „კიბერტერორიზმი, ესე იგი 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“. [61]

,,კოდექსის ძველი რედაქციის შესაბამისად კიბერტერორიზმის დაცვის უშუალო ობიექტი იყო სახელმწიფოს ინტერესი (სტრატეგიული, პოლიტიკური ან ეკონომიკური) დამატებითი ობიექტი კი შეიძლება ყოფილიყო ადამიანის სიცოცხლე, ჯანმრთელობა, ქონება. მიუხედავად იმისა, რომ 3241 მუხლის ახალ რედაქციაში სახელმწიფოს სტრატეგიულ და სხვა ინტერესზე მითითებას აღარ ვხვდებით, დანაშაულის უშუალო ობიექტი იგივე დარჩება, რადგან ხელისუფლების ორგანოზე ზემოქმედება მიმართულია სწორედ სახელმწიფო სტრატეგიულ და სხვა ინტერესების წინააღმდეგ. დამატებით ობიექტთან დაკავშირებითაც შეიძლება იგივე ითქვას‘‘. [62]

„საქართველოს სისხლის სამართლის კოდექსის 324[1]-ე მუხლის მიხედვით, კიბერტერორიზმისაგან სისხლისსამართლებრივი დაცვის უშუალო ობიექტია სახელმწიფოს ინტერესი (სტრატეიული, პოლიტიკური ან ეკონომიკური), დამათებითი ობიექტი შეიძლება იყოს ადამიანის სიცოცხლე, ჯანმრთელობა, ქონება.

[61] ზაქაშვილი უ., კიბერტერორიზმი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, გამომც. ,,მერიდიანი“ თბ., 2013 გვ23;

[62] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, გვ 26

კიბერტერორიზმის ობიექტური მხარე გამოიხატება კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლებაში, მის გამოყენებაში ან გამოყენების მუქარაში, რაც ქმნის მძიმე შედეგის განხორციელების საშიშროებას.

324^1-ე მუხლის დისპოზიციაში საუბარია კომპიუტერული ინფორმაციის დაუფლებაზე, მის გამოყებნებაზე ან გამოყენების მუქარაზე. საფრთხე - „მძიმე შედეგის განხორციელების საშიშროება“ - რაც შეიძლება შეიქმნას აღნიშნული მოქმედების განხორციელებით სხვდასხვა ხასიათის შიძლება იყოს, მაგალითად, ტრანსპორტის მუშაობის ბლოკირება, შფერხება ენერგომომარაგეაში, მასობრივი განადგურების იარაღის დამზაების ტექნოლოგიის ხელში ჩაგდება, სხვადასხვა სტრატეგიული დანიშნულების ობიექტების მუშაობის დეზორგანიზაცია და სხვა.[63]

324^1-ე მუხლის პირველი ნაწილით გათვალისწინებული შმადგენლობა კონკრეტული საფრთხის შემქმნელი დელიქტის სახით არის ჩამოყალიბებული. ისჯება თავისთავად კანონში მითითებული მოქმედების ჩადენა - კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის განხორციელების საშიშროებას.

324^1-ე მუხლის მე-2 ნაწილი პასუხისმგებლობის დამამძიმებელ გარემოებად ითვალისწინებს ადამიანის ადამიანის სიკვდილს ან სხვა მძიმე შედეგს, პირველი ნაწილით გათვალისწინებული ქმედების ჩადენის შედეგად.[64]

მძიმე შედეგი შეფასებითი ნიშანია და საქმის კონკრეტული გრემოების მხედველობაში მიღებით უნდა შეაფასოს სასამართლომ. მძიმე შედეგი შეიძლება გამოიხატოს სტრატეგიული ობიექტის მუშაობის პარალიზებაში, ხელისუფლების ორგანოთა მუშაობის დეზორგანიზაციაში, დიდ ქონებრივზიანში და ა.შ.

---

[63] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012 გვ 23;

[64] სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, ავტორთა კოლექტივი, გამომც. „მერიდიანი“ თბ., 2012 გვ 24;

კიბერტერორიზმის ამსრულებელი შეიძლება იყოს ნებისმიერი შერაცხადი ფიზიკური პირი 14 წლის ასაკიდან, ასევე იურიიული პირი.

სუბიექტური მხრივ კვალიფიკაციისათვის განმსაზღვრელი მნიშვნელობა აქვს მიზანს - მოსახლეობის დაშინება ან/და ხელისუფლების ორგანოზე ზემოქმედება. კიბერტერორიზმის მოტივი სხვადასხვა შეიძლება იყოს, პოლიტიკურით დაწყებული და რელიგიური ფანატიზმით დამთავრებული. ის კვალიფიკაციაზე გავლენას არ მოახდენს. სახეზეა პირდაპირი განზრახვით ჩადენილი დანაშაული“.[65]

„თანამედროვე მსოფლიოში კიბერდანაშაულის წინააღმდეგ ბრძოლა უკვე საერთაშორისო პრობლემად იქცა და თავისი მნიშვნელობით საერთაშორისო ტერორიზმსაც გაუტოლდა. ტრანსნაციონალური კომპიუტერული დანაშაულის და კიბერტერორიზმის წინააღმდეგ ბრძოლის ეფექტიანი მეთოდების შემუშავება წარმოადგენს მსოფლიო კიბერსივრცის უსაფრთხოების უზრუნველყოფის ძირითადი ელემენტია. სწორედ ამიტომ, კიბერსივრცის უსაფრთხოების კვლევა მსოფლიოში მრავალი ქვეყნის მუშაობის პრიოტეტულ მიმართულებად იქცა.[66]

ესტონეთში 2007 წლის 27 აპრილს დაწყებული კიბერშეტევები, რომლებიც 3 კვირის განმავლობაში გრძელდებოდა, წარმოადგენდა სახელმწიფოს წინააღმდეგ მიმართული კიბერშეტევების პირველ და უპრეცენდენტო შემთხვევას. შეტევის სამიზნედ იქცა როგორც სახელმწიფო, აგრეთვე კერძო სექტორის ინტერნეტ ინფრასტრუქტურა. აღნიშნული მოვლენა გახდა ესტონეთისა და ჩრდილოატლანტიკური ალიანსის წევრი ქვეყნებისათვის კიბერუსაფრთხოების სფეროში რიგი ღონისძიების გატარების საფუძველი, რათა სამომავლოდ სავალალო შედეგებისგან თავი აერიდებინათ და მოეხდინათ კიბერშეტევებით მიღებული დანაკარგების მინიმიზება. ამ მიზნით, ესტონეთში შეიქნმა ჩრდილოატალნტიკური ალიანსის წევრი ქვეყნების კიბერუსაფრთხოების ცენტრი,

[65] სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, ავტორთა კოლექტივი, გამომც. „მერიდიანი“ თბ., 2017, 282-283;

[66] http://ec.europa.eu/research/fp6/index_en.cfm;

რომელმაც შეიმუშავა კადრების მომზადების ახალი პროგრამა და დაიწყო თანამედროვე დაცვის საშუალების შექმნა და მათი განვითარება“.[67]

4.3 კანონმდებლობა კიბერდანაშაულზე და ზოგადი პოლიტიკა

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.[68]

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

[67] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012, 173-174;

[68] სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, ავტორთა კოლექტივი, გამომც. „მერიდიანი“ თბ., 2012 , გვ 45-47;

შორის ონლაინ), (სსკ– მუხ. 255, ნაწ.2), ინტელექტუალური საკუთრების უფლების დარღვევა და კიბერ საშუალებებით ჩადენილი ტერორიზმი. (სსკ. მუხ.3241).

გარდა ამისა, 2012 წელს მიღებულ იქნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“, რომელიც აწესებს ინფორმაციული უსაფრთხოების ზოგად სტანდარტებს საჯარო და კერძო სექტორისთვის.[69] აღნიშნული საკანონმდებლო აქტის საფუძველზე, საქართველოს პრეზიდენტმა დაამტკიცა „კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხა“. ამ ეტაპზე ნუსხაში შედიან მხოლოდ ის სახელმწიფო დაწესებულებები, რომელთა გამართული ფუნქციონირება სასიცოცხლო მნიშვნელობას მქონეა საქართველოსთვის.[70]

2013 წლის მაისში საქართველოს პრეზიდენტმა ხელი მოაწერა საქართველოს კიბერ უსაფრთხოების სტრატეგიას 2013–2015 წლებისთვის, რომელიც წარმოადგენს კიბერ უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ მთავარ დოკუმენტს. სტრატეგიას გააჩნია სამოქმედო გეგმა, სადაც დეტალურად გაწერილია დაგეგმილი ღონისძიებები, ისევე ის სახელმწიფო უწყებები, რომლებიც უშუალოდ პასუხისმგებელნი არიან სამოქმედო გეგმით განსაზღვრული ვალდებულებების შესრულებაზე.[71]

საქართველოს მთავრობა მიიჩნევს, რომ საქართველოში კიბერტერორიზმის საფრთხე და მისგან მოსალოდნელი ზიანის მასშტაბები იზრდება. ამის შესახებ საქართველოს მთავრობის მიერ დამტკიცებულ კიბერუსაფრთხოების 2017-1018 წლების ეროვნული სტრატეგიაში წერია. სტრატეგიის მიხედვით, თანამედროვე პერიოდში ტერორისტულ დაჯგუფებებს მნიშვნელოვანი რესურსები აქვთ და ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებს აქტიურად იყენებენ საკუთარი საქმიანობის მხარდაჭერისთვის. „აღნიშნულის ნათელი დადასტურებაა ტერორისტული ორგანიზაციის ,,ისლამური სახელმწიფო“, რომელიც

[69] http://dea.gov.ge/uploads/legal_acts/8/Inf._Security;
[70] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm;
[71] გორაშვილი გ., ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები, გამომც. „უნივერსალი“, თბ., 2010 , გვ 62;

რეგულარულად ახორციელებს კიბერშეტევებს ანტიტერორისტული კოალიციის წევრი სახელმწიფოების კრიტიკული ინფორმაციული სისტემების წინააღმდეგ", - წერია დოკუმენტში.

სტრატეგიის მიხედვით, ქვეყნისთვის მთავარი საფრთხე რუსეთის ფედერაციის მიერ ორგანიზებული კიბერშეტევები და კიბერსაშუალებებით ჩადენილი დანაშუალებია.[72]

[72] კაცმანი ა., კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება, ჟურნალი ,,სამართალი", 2000, №2 34-37;

თავი 5. კიბერსაფრთხეების წარმოშობის წყაროები და სახეობები. - კიბერსაფრთხეებთან მებრძოლი სუბიექტები

„კიბერსივრცის“ ტერმინის განსაზღვრების ბევრი ვარიანტი არსებობს. თითოეული მათგანი იძლევა თავისებურ განმარტებას. თუმცა ყველა განმარტებაში განსაზღვრულია, რომ „კიბერსივრცე“ ეს არის ინფორმაციული და ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირში არსებული კომპლექსი, სადაც შედის გლობალური ინტერნეტისა და ტელეკომუნიკაციის ქსელები, კომპიუტერული სისტემები, ასევე ჩართული პროცესორები, სერვერები და მაკონტროლირებელი მოწყობილობები, რომლებიც გამოიყენება მრეწველობის სხვადასხვა დარგში. [73]

ახალი ტექნოლოგიების განვითარებასთან ერთად იზრდება საფრთხეები, რომლებიც დიდ ზიანს აყენებს კიბერსივრცეს და მის მომხმარებელს. სახელმწიფოს და სახელისუფლებო ორგაონოებს პირველ რიგში ადარდებთ ეროვნული უსაფრთხოების უზრუნველყოფა, კრიტიკული ინფორმაციისა და ინფორმაციული ინფრასტრუქტურის დაცვა როგორც უცხო სახელმწიფოს, ისე არასამთავრობო სუბიექტებისა და დაჯგუფებების მხრიდან ხელყოფისგან, რათა თავიდან იქნას აცილებული ინფორმაციის მოპარვა ან/და გადაცემა, ქსელის დაზიანება ან/და საერთოდ განადგურება. სახელმწიფოს უსაფრთხოების რეალურ საფრთხეს წარმოადგენს კიბერშეტევები, რომლებიც მიმართულია ისეთი სასიცოცხლო მნიშვნელობის მქონე ინფრასტრუქტურის განადგურებისკენ, როგორებიცაა სატელეკომუნიკაციო ქსელების, ენერგოგენერირებისა და ნავთობ გადამამუშავებელი სიმძლავრეების სისტემები, ასევე ელექტრომომარაგების, საფინანსო, ჯანდაცვისა და სატრანსპორტო სისტემები. [74]

ქვემოთ განხილულია კიბერსაფრთხეები და მათი სახეობები, რომლებიც ემუქრება კიბერსივრცეს და ზოგადად ინფორმაციული ინფრასტრუქტურის

[73] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, გამომცემლობა ,,სანი“ თბ., 2012, გვ 49;
[74] Arquilla J. and Ronfeldt D. (2001) Networks And Netwars- THE ADVENT OF NETWAR (REVISITED): Defi ning Netwar pp. № 6 p 23

სისტემების მთლიანობას. ასევე ნაჩვენებია წარმოშობის ის წყაროები, საიდანაც მომდინარეობს მოცემული კიბერსაფრთხეები. ნაშრომის მეორე ნაწილში განხილულია ის საერთაშორისო და რეგიონალური დონის სუბიექტები, რომლებიც ებრძვიან კიბერსაფრთხეებს და ცდილობენ დაიცვან კიბერსივრცე და ინფორმაციული ინფრასტრუქტურის სისტემები კიბერდამნაშავეთა ხელყოფისგან. [75]

5.1 საერთაშორისო და რეგიონალური დონის ღონისძიებები მიმართული კიბერსივრცის დაცვისკენ

„კიბერდანაშაულთან ბრძოლისა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პროცესში დიდი მნიშვნელობა ენიჭება არამარტო ეროვნულ პოლიტიკას, სტრატეგიასა თუ სხვა სახის ქმედით ზომებს, არამედ ასევე თანამშრომლობას საერთაშორისო და რეგიონალურ დონეზე. მსგავსი თანამშრომლობა კიბერსივრცის დაცვის სფეროში ითვალისწინებს და მოიცავს საერთაშორისო და რეგიონალურ კონვენციებს, ფორუმებს, ორგანიზაციებსა და ალიანსებს, შეხვედრებსა და დისკუსიებს, ერთობლივ რეზოლუციებს, გადაწყვეტილებებსა და რეკომენდაციებს, დირექტივებს.[76]

ევროპის საბჭოს მიდგომა შემდეგია - 2001 წლის 23 ნოემბერს ბუდაპეშტში ხელი მოეწერა კიბერდანაშაულთან ბრძოლის ევროპულ კონვენციას (CETS 185)[77], რომელიც ძალაში შევიდა 2004 წლის 1 ივლისს. კონვენცია მომზადდა ევროპის საბჭოს ფარგლებში კანადის, შეერთებული შტატების, იაპონიისა და სამხრეთ აფრიკის რესპუბლიკის მონაწილეობით. დღესდღეისობით ეს კონვენცია არის მოცემულ სფეროში ერთადერთი აღიარებული იურიდიული დოკუმენტი, რომელიც მიღებულია საერთაშორისო დონეზე და ის არის ღია ყველა დაინტერესებული ქვეყნისთვის. ასევე საინტერესოა კონვენციაზე დამატებით

[75] გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008, გვ 15

76 პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012 გვ 49;

77 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

მიღებული პროტოკოლი (CETS 189)[78] კომპიუტერულ ქსელებში ქსენოფობიისა და რასიზმის ნიადაგზე ჩადენილი დანაშაულების შესახებ, რომელსაც ხელი მოეწერა 2003 წლის იანვარში და ძალაში შევიდა 2006 წლის მარტის თვეში.[79]

კონვენცია ხელმომწერ ქვეყნებს ავალდებულებს შექმნან სამართლებრივ - ნორმატიული ბაზა აუცილებელი კიბერდანაშაულის პრობლემის ეფექტური გადაწყვეტისთვის. ასევე ყველა ხელმომწერი ქვეყანა თავის თავზე იღებს ერთმანეთისთვის დახმარების აღმოჩენას კიბერდამნაშავეთა სამართლებრივი დევნისა და ინციდენტების გამოძიების საკითხში. ევროპული კონვენცია არის ერთერთი პირველი საერთაშორისო დოკუმენტი, სადაც განსაზღვრულია და კლასიფიცირებულია კიბერდანაშაული. კერძოდ, შემოსულია ინტერნეტ სივრცეში 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 ეფექტური გამოძიების ინსტრუმენტები და მათთან ბრძოლა. კონვენციის მოქმედფება ვდრცელდება ყველა დანაშაულზე, რომელიც ჩადენილია კომპიუტერულ სისტემებში, ასევე ელექტრონული საშუალებებით შეგროვილი ნებისმიერი მტკიცებულებები.[80]

კონვენცია წარმოადგენს სტანდარტულ დოკუმენტს, რომელიც წარმოადგენს საერთაშორისო კანონმდებლობის ძალზედ მნიშვნელოვან შემადგენელ ნაწილს. მასში მოცემულია იურიდიული და ტექნიკური ნორმების ოპტიმალური კომპლექსი, რომელიც შეიძლება გამოყენებულ იქნას ამ სფეროში საერთაშორისო თანამშრომლობის გაფართოებაზე დამატებითი შეთანხმებების დამუშავების მიზნით. გამომდინარე, რომ კიბერდანაშაულს, კიბერტერორიზმსა

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

79 სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, ავტორთა კოლექტივი, გამომც. „მერიდიანი“ თბ., 2012 გვ 45-47

80 ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012 , გვ 23;

და კიბერომს გააჩნიათ ბევრი საერთო ნიშანი და მახასიათებელი, კონვენცია ნებისმიერ კიბერშეტევაზე, მიუხედავად მათი მოტივაციისა, ითვალისწინებს, რომ მასზე ხელმომწერმა ქვეყნებმა პასუხისმგებელი უწყებების მოთხოვნაზე უნდა დააკავონ და გადასცენ ყველა კიბერდამნაშავე სამართალდამცავ ორგანოებს, მიუხედავად იმისა, განიხილებიან თუ არა ისინი საკუთარ ქვეყნებში როგორც დამნაშავეები, ტერორისტები ან კიდევ პატრიოტები“.[81]

2012 წლის 6 ივნისს საქართველომ მოახდინა ევროპის საბჭოს “კიბერდანაშაულის შესახებ კონვენციის” რატიფიცირება. ამ კონვენციას საქართველომ 2008 წელს მოაწერა ხელი, თუმცა კონვენცია მოითხოვს არა მარტო საერთაშორისო თანამშრომლობას კიბერსაგამოძიებო მოქმედებების ჩატარების მიზნით, არამედ საქართველოს კანონმდებლობის ჰარმონიზაციას კონვენციით დადგენილ ნორმებთან. კონვენციის რატიფიცირების დაჩქარებას ხელი შეუწყო „ინფორმაციული უსაფრთხოების შესახებ კანონის“ მიღებამ. აღნიშნული კონვენცია ძალაში შევიდა 2012 წლის 1 ოქტომბერს”. “2013 წლის 17 მაისს საქართველოს პრეზიდენტმა ხელი მოაწერა საქართველოს კიბერუსაფრთხოების სტრატეგიას და კიბერუსაფრთხოების სტრატეგიის სამოქმედო გეგმას. დოკუმენტი მოუწოდებს სახელმწიფო უწყებებს გამართული, კოორდინირებული მუშაობისაკენ და სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის მექანიზმების შემუშავებისაკენ. დოკუმენტი ასევე ხაზს უსვამს საერთაშორისო თანამშრომლობის აუცილებლობას და საგანმანათლებლო ბაზის ჩამოყალიბებას. სამოქმედო გეგმა განსაზღვრულია 2015 წლის ჩათვლით”.[82]

5.2 კიბერსაფრთხეების წარმოშობის წყაროები და სახეობები

[81]სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, თბ., 2015, გვ 152-154;

[82] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, გვ 12;

კიბერდანაშაულთან ბრძოლის ერთერთ მთავარ პრობლემას წარმოადგენს ის ფაქტი, რომ ხშირად ძალზედ რთულია ზუსტად დაადგინო არამარტო უშუალო შემსრულებლები, არამედ მათი ადგილსამყოფელი ან ის ქვეყანა, საიდანაც განხორციელდა შეტევა. ამიტომ, დამნაშავეს ან დამნაშავეთა ჯგუფს შეუძლია ადვილად დამალოს არამარტო თავისი მონაწილეობა კიბერშეტევის ორგანიზებაში, არამედ თავისი თავი დააფიქსიროს როგორც ქსელის სხვა მომხმარებლად ან საერთოდ დარჩეს ანონიმურად. [83]

კიბერსაფრთხეების წარმოშობის წყაროებს წარმოადგენენ როგორც სახელმწიფო და კერძო სექტორის წარმომადგენლები, ისე სხვადასხვა სახისა და ნიშნით შექმნილი ორგანიზაციები და ფიზიკური პირები. შეერთებული შტატების კონტროლის პალატის მასალების მიხედვით, კიბერსაფრთხეების წარმოშობის წყაროები შეიძლება დავაკვალიფიციროთ შემდეგნაირად, კერძოდ: **სახელმწიფო** - უცხოეთის ქვეყნების სადაზვერვო სამსახურები კომპიუტერულ ტექნოლოგიებს იყენებენ ინფორმაციის შეგროვებისა და ჯაშუშობისთვის. მსგავსი ქმედებები სადაზვერვო სამსახურების მხრიდან შეიძლება მიმართული იყოს როგორც მეგობარი, ისე მოწინააღმდეგე ქვეყნების მიმართ, ან არასახელმწიფო სუბიექტების წინააღმდეგ. სახელმწიფო თავისი სადაზვერვო სამსახურების გამოყენებით, ახორციელებს კიბერშეტევებს პოტენციური მოწინააღმდეგე სახელმწიფოების მიმართ დეზინფორმაციის, დესტაბილიზაციის, დაშინების ან ფართომასშტაბიანი კიბერომის წარმოების მიზნით.[84] ასევე საყურადღებოა ის გარემოება, რომ ხშირად ხდება პიროვნების უსაფრთხოებისა და უფლებების დარღვევა. კერძოდ, სახელმწიფოს სპეციალურმა სამსახურებმა შეიძლება მიმართონ ისეთ ქმედებებს, რომელთა გამოყენებითაც ხდება მოქალაქეთა პერსონალური მონაცემების გადაჭერა, მოპარვა და გამოყენება. მსგავსი ქმედებები ხშირ შემთხვევაში ხდება სასამართლოს შესაბამისი ორგანოების სანქციისა და სწორი დემოკრატიული კონტროლის გარეშე; **კორპორაციები, კომპანიები** - დაკავებულნი არიან

[83] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81;
[84] Richard W. Aldrich, "CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME", USAF Institute for National Security Studies USAF Academy, Colorado, April 2000 ;

სამრეწველო/კორპორაციული ჯაშუშობითა და/ან დივერსიული საქმიანობით, რაშიც ისინი ხშირად იყენებენ ჰაკერებსა და ორგანიზებულ დამნაშავეთა ჯგუფებს. კომპანიების, კორპორაციებისა და კერძო სექტორის სხვა წარმომადგენლებს ასევე შეუძლიათ დაარღვიონ ადამიანის უფლებები პიროვნების პერსონალური მონაცემების შეგროვებისა და ანალიზის გზით, ან ზოგ შემთხვევაში მოცემული მონაცემების სახელმწიფო ორგანოებთან ან სხვა დაინტერესებულ პირებთან გაცვლით; **ჰაკერები** - იყო დრო როცა ჰაკერების მხრიდან ქსელებში არასანქცირებული შეღწევა ან პროგრამების გატეხვა დაკავშირებული იყო ჰაკერთა საზოგადოებაში ავტორიტეტის მოპოვებასთან ან წვრილმან ჰულიგნობასთან. დღესდღეისობით სურათი კარდინალურად არის შეცვლილი, კერძოდ ჰაკერთა უმრავლესობის ქმედება ატარებს კრიმინალურ ხასიათს.[85] ადრე თუ ჰაკერებისთვის ქსელის გატეხვისათვის საჭირო იყო კომპიუტერული ტექნოლოგიების სფეროში სპეციალური უნარ - ჩვევების ცოდნა, როცა ამჟამად საკმარისია ინტერნეტიდან შესაბამისი ინსტრუქციებისა და პროტოკოლების გადმოქაჩვა და მათი გამოყენება შერჩეულ საიტზე კიბერშეტევის ორგანიზებისთვის. ამის გამო, კიბერშეტევის განხორციელება მომხმარებლისთვის გახდა უფრო ადვილად ხელმისაწვდომი. ჰაკერთა მომსახურეობით სარგებლობენ არამარტო კორპორაციები და კომპანიები, არამედ სადაზვერვო ან სხვა სახის სპეციალური სამსახურებიც; **ჰაკტივისტები** - ტერმინი „ჰაკტივიზმი“ (hacktivism) წარმოიშვა ორი სიტყვის „Hack“ და “Activism” შეერთებით და ის აღნიშნავს სოციალური პროტესტის გამოხატვის ახალ მოვლენას, რომელიც წარმოადგენს თავისებურ სინთეზს რაღაცის მიმართ გამოხატული პროტესტის სოციალური აქტიურობისა და ჰაკერობის, რომელიც მიმართულია გარკვეული ვებ - გვერდების ან საფოსტო სერვისების წინააღმდეგ. თავიანთი პოლიტიკური მიზნების მისაღწევად, ჰაკტივისტები მიისწრაფვიან დააზიანონ ან საერთოდ მწყობრიდან გამოიყვანონ ზოგიერთი ვებ - გვერდი; **კიბერ დივერსანტები ქსელის უკმაყოფილო მომხმარებელთა რიცხვიდან** - ზოგადად, უკმაყოფილო მომხმარებლები

[85] Dorothy E. Denning. (23.05.2000). "CYBERTERRORISM". Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html ;

წარმოადგენენ სერიოზულ საფრთხეს, ვინაიდან ისინი კარგად იცნობენ სისტემის მუშაობის პრინციპებს და შეუძლიათ თავიანთი ეს ცოდნა გამოიყენონ დესტრუქციული მიზნებისთვის. მაგალითად, სისტემის დასაზიანებლად ან კონფიდენციალური ინფორმაციის მოსაპარად. შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) მონაცემებით, სისტემის მომხმარებლებისა და გარე წყაროების მხრიდან კიბერშეტევის ორგანიზების შესაძლებლობის ერთმანეთთან შეფარდება შეადგენს 2:1; **ტერორისტები** - ცდილობენ ინფრასტრუქტურის მნიშვნელოვანი ობიექტები გამოიყვანონ მწყობრიდან, საერთოდ გაანადგურონ ან გაომიყენონ თავიანთი მიზნებისთვის. მათი ქმედება სერიოზული საფრთხის ქვეშ აყენებს ქვეყნების ეროვნულ უსაფრთხოებას, იწვევს ადამიანთა მასიურ მსხვერპლს, ასუსტებს ეკონომიკას, ასევე ზიანს აყენებს საზოგადოების მორალურ მდგომარეობასა და ამცირებს მათ სანდოობას ხელისუფლების მიმართ. ყველა ტერორისტული ორგანიზაცია და დაჯგუფება არ ფლობს საკმარის ცოდნასა და ტექნიკურ საშუალებებს ეფექტური კიბერშეტევის განხორციელებისთვის, თუმცა არსებობს თეორიული დაშვება, რომ მათ მიიღონ მსგავსი ცოდნა და შესაძლებლობა, ან დახმარებისთვის მიმართონ ორგანიზებული დანაშაულის წარმომადგენლების მომსახურებას; **ბოტნეტი** - ინტერნეტ - ბოტი ბოტნეტში წარმოადგენს პროგრამას, რომელიც ფარულად არის დაყენებული მსხვერპლის/ობიექტის კომპიუტერულ მოწყობილობაში, რაც დამნაშავეს/ბოროტმოქმედს საშუალებას აძლევს დავირუსებული კომპიუტერის რესურსების გამოყენებით, შეასრულოს გარკვეული ქმედებები. ჰაკერების ეს სახეობა თავისი პროგრამებით ავირუსებენ კომპიუტერების დიდ რაოდენობას, რომელთა რესურსებსაც შემდეგ იყენებენ კიბერშეტევის კოორდინირებისთვის, ასევე „სპამის“ გასაგზავნად, ფიშინგისთვის და სხვა მავნე ქმედებისთვის. მსგავსი სახის ქსელები წარმოადგენენ არალეგალური ვაჭრობის ობიექტს; **ფიშერები** - ეს არის ფიზიკური პირები ან პატარა დაჯგუფებები, რომლებიც იყენებენ ფიშინგის ტექნოლოგიებს პერსონალური რეკვიზიტების მოპარვისა და ფასიანი ინფორმაციების გადაყიდვის მიზნით. თავიანთი მიზნების მისაღწევად ფიშერები ხშირად იყენებენ „სპამებს“ და ჯაშუშურ პროგრამებს; **სპამერები** - ფიზიკური ან

იურიდიული პირები, რომლებიც მასიურად აგზავნიან არამოთხოვნილ ელექტრონულ ფოსტას დაფარული ან მცდარი ინფორმაციით, რომლის მიზანია ფიშინგითა და ჯაშუშური პროგრამების გამოყენებით კონკრეტულ ორგანიზაციებზე კიბერშეტევის განხორციელება; **ჯაშუშური და მავნე პროგრამების შემქმნელები** - ფიზიკური ან იურიდიული პირები, რომლებსაც გააჩნიათ დანაშაულებრივი ზრახვები კომპიუტერების მომხმარებლებზე კიბერშეტევის განსახორციელებლად; **პედოფილები** - ეს კატეგორია სულ უფრო აქტიურად იყენებს ინტერნეტს საბავშვო პორნოგრაფიის გასავრცელებლად, ასევე სოციალური ქსელებისა და ინტერნეტ ჩათების გამოყენებით, პოტენციური მსხვერპლების გასაცნობად.

როგორც წესი, ზემოთ მოცემულ კიბერსაფრთხეების წარმოშობის წყაროების ყველა სახეობას, გამომდინარე დასახული ამოცანის გადაჭრისა და მიზნის მისაღწევად, აქტიურად იყენებს არამარტო კრიმინალური სამყარო, არამედ ასევე სახელმწიფო სადაზვერვო ან სხვა სახის სპეციალური სამსახურები. [86]

5.3 კიბერსაფრთხეებთან მებრძოლი სუბიექტები

კიბერსაფრთხეებთან ბრძოლის ერთერთ მთავარ პრობლემას წარმოადგენს ის ფაქტი, რომ ინფორმაციული და საკომუნიკაციო ქსელების უმეტესობა არის კერძო სექტორის საკუთრებაში, როცა მათ უსაფრთხოებაზე პასუხისმგებლობა ეკისრება სახელმწიფოს. უნდა აღინიშნოს, რომ პროცესში კერძო სექტორის მონაწილეობა გაცილებით ართულებს ქსელების დაცვასა და მათი უსაფრთხოების უზრუნველყოფას. ორივე ჯგუფს, სახელმწიფოს და კერძო სექტორს გააჩნიათ სხვადასხვა ინტერესები და მიზნები, რაც ამცირებს კიბერსივრცის დაცვის ეფექტურობას. [87]

[86] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012 , გვ 49;
[87] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81;

ეს პროცესი კიდევ უფრო რთულდება, როცა საკითხი იღებს გლობალურ ხასიათს, რომლის გადაწყვეტაში დიდი როლი ენიჭება საერთაშორისო ნორმებსა და არსებულ სუბიექტებს. ამ უკანასკნელებმა შეიძლება შეასრულონ გარკვეული კატალიზატორის როლი მოცემულ პროცესში, მიმართული როგორც ეროვნული, ისე საერთაშორისო სამართლებრივი ბაზის სრულყოფისა და ჰარმონიზაციისკენ, სადაც იგულისხმება კიბერდამნაშავეთა სამართლებრივი დევნა, მონაცემთა შენახვა და დაცვა, ასევე ქსელის უსაფრთხოების უზრუნველყოფის პრინციპები და კიბერშეტევებზე ოპერატიული რეაგირება. აგრეთვე უნდა აღინიშნოს, რომ საკითხისადმი მსგავსი მიდგომით შესაძლებელია ინფორმაციულ სისტემებში სუსტი და მოწყვლადი ადგილები, ასევე სახელმწიფო და კერძო სექტორის სუბიექტებს შორის პარტნიორობა კიბერდამნაშავეობასთან ბრძოლის საკითხში.

საერთაშორისო დონეზე კიბერსაფრთხეებთან ბრძოლის თაობაზე მიღებულია ისეთი მნიშვნელოვანი სამართლებრივი აქტები, როგორებიცაა გაეროს გენერალური ასამბლეის 2000 წლის 4 დეკემბრის №55/63 და 2001 წლის 19 დეკემბრის №56/121 რეზოლუციები „დანაშაულებრივი მიზნებით ინფორმაციული ტექნოლოგიების გამოყენებასთან ბრძოლა“, 2008 წლის 1 – 2 აპრილს, სტრასბურგში მსოფლიო კონფერენციაზე “თანამშრომლობა კიბერდანაშაულის წინააღმდეგ” მიღებული დოკუმენტი „კიბერდანაშაულობასთან ბრძოლის სფეროში სამართალდამცავი ორგანოებისა და ინტერნეტ - პროვაიდერების ერთობლივი მუშაობის ძირითადი პრინციპები“. რეგიონალურ დონეზე უნდა აღინიშნოს ევროსაბჭოს რეკომენდაციები №R[89]9 “კომპიუტერულ დანაშაულებთან ბრძოლა”.[88]

კიბერდანაშაულობასთან ბრძოლის ერთერთ ძირითად სუბიექტად მოიაზრება ქსელის მომხმარებელი. ამიტომ აუცილებელია მათი ჩართვა საგანმანათლებლო ღონისძიებებში, რომლებიც დაეხმარება მომხმარებელს უფრო კარგად გაერკვნენ

[88] გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008 , გვ 15;

ისეთ საკითხში, როგორიცაა კომპიუტერული მაქინაციები, პირადი რეკვიზიტების მოპარვა, ინტერნეტში არსებული დანაშაულებები, ინტერნეტის ეთიკა და სხვა. [89]

ქვემოთ მოცემულია ზოგიერთი ძირითადი სუბიექტი, რომლებიც მონაწილეობენ კიბერსაფრთხეებთან ბრძოლაში, კერძოდ, საერთაშორისო და რეგიონალური ორგანიზაციები:

- ✓ აზია - წყნარი ოკეანის ეკონომიკური თანამშრომლობის სამუშაო ჯგუფი ტელეკომუნიკაციებსა და ინფორმაციებში;
- ✓ ქსელებისა და ინფორმაციული უსაფრთხოების ევროპული სააგენტო;
- ✓ ნატო - ს კიბერნეტიკული დაცვის მოწინავე მეთოდების გაერთიანებული ცენტრი206;
- ✓ სამხრეთ - აღმოსავლეთის ქვეყნების ასოციაცია;
- ✓ ეკონომიკური განვითარებისა და თანამშრომლობის ორგანიზაცია208;
- ✓ კომპიუტერულ ქსელებში საგანგებო სიტუაციებზე ოპერატიული რეაგირების ჯგუფი;
- ✓ ინტერნეტის მართვის ფორუმი;
- ✓ ელექტროკავშირის საერთაშორისო გაერთიანება;
- ✓ ინტერნეტის საზოგადოება;
- ✓ სახელებისა და ნომრების მინიჭების ინტერნეტ - კორპორაცია;
- ✓ სამოქალაქო ინიციატივა ინტერნეტ - პოლიტიკა „მერიდიანი“;
- ✓ დიდი რვიანის ლიონის ჯგუფი, მაღალი ტექნოლოგიების სფეროში დანაშაულებების ქვეჯგუფი, გაერო, ევროსაბჭო. [90]

[89] ზაქაშვილი უ., კიბერტერორიზმი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, გამომც. ,,მერიდიანი“, 2013 , გვ 23;

[90] გორაშვილი გ., ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები, გამომც. „უნივერსალი“, თბ., 2010, გვ 62;

5.4 კიბერუსაფრთხოების სფეროში არსებული ორგანიზაციული სტრუქტურების მოკლე აღწერა. საქართველოში არსებული სუბიექტები

ბოლო ათწლეულში ინტერნეტ - სივრცის და მასთან დაკავშირებული პროცესების სწრაფმა განვითარებამ, ასევე მომხმარებელთა რაოდენობის მოკლე დროში კოლოსალურმა ზრდამ, გამოიწვია ახალი სახელმწიფო სუბიექტების შექმნისა და განვითარების საჭიროება. ყველა ქვეყანა ცდილობს მაქსიმალურად ეფექტური, მოქნილი და დახვეწილი ისეთი ორგანიზაციული სტრუქტურის ჩამოყალიბებას, რომელიც მაქსიმალურად უზრუნველყოფს კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას, გაატარებს ეფექტურ ღონიძიებებს მიმართულს კიბერუსაფრთხოების უზრუნველყოფაზე, ასევე მაქსიმალურად დაიცავს პიროვნების პერსონალურ ინფორმაციას და არსებულ მონაცემთა ბაზებს.[91] პირველ რიგში, ყველა ქვეყნის ხელისუფლება მოცემულ საკითხს განიხილავს როგორც ეროვნული უსაფრთხოების ერთერთ მნიშვნელოვან შემადგენელ ნაწილს, და შესაბამისად მსგავსი სუბიექტების დიდი ნაწილი იმყოფება თავდაცვის და შინაგან საქმეთა სამინისტროების, ან სადაზვერვო, უშიშროების ან სხვა სპეციალური სამსახურების კურატორობის ქვეშ.

მსგავს სუბიექტებს გააჩნიათ არსებობის მოკლე ისტორია. ფაქტიურად, არ არსებობდა არავითარი გამოცდილება და ყველა ქვეყანა ინდივიდუალურად ავითარებდა მოცემულ საკითხს. შეიძლება ითქვას, რომ კიბერუსაფრთხოების სფეროში სახელმწიფო თუ კერძო სუბიექტების შექმნა და მათი მომავალი განვითარება ეფუძნება იმ პრეცედენტებს, რომლებიც წარმოიშვა ინტერნეტ - სივრცეში და უკავშირდება ზოგადად, კიბერსივრცის დაცვის აუცილებლობას. ამიტომ, მოცემული სფეროს პარალელურად მუდმივად მიმდინარეობს სახელმწიფო თუ კერძო სექტორის სუბიექტების ორგანიზაციული სტრუქტურის განვითარების პროცესი.[92]

---

[91] სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, თბ., 2015, გვ 56;

[92] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm;

ნაშრომში განხილულია საქართველოში არსებული ის სუბიექტები, რომლებიც პასუხისმგებელნი არიან კომპიუტერული ქსელებისა და კიბერსივრცის, ასევე პერსონალური მონაცემების დაცვაზე და ებრძვის კიბერდანაშაულს როგორც ლოკალურ ისე საერთაშორისო დონეზე.[93]

საქართველოში არ არსებობს ერთიანი ორგანო, რომელიც კოორდინაციას გაუწევს ქვეყნის კიბერსივრცის დაცვასა და უზრუნველყოფს კიბერუსაფრთხოებასთან დაკავშირებულ ღონისძიებებს სამინისტროებსა და უწყებებს შორის.[94] განხორციელებულმა საკონსტიტუციო ცვლილებებმა და უშიშროების საბჭოს ალტერნატიული ორგანოს უსაფრთხოებისა და კრიზისების მართვის საბჭოს შექმნამ გამოიწვია მოცემული საკითხის დროებით ღიად დატოვება. კერძოდ, უშიშროების საბჭომ, რომელმაც თავის დროზე შეიმუშავა კიბერუსაფრთხოების სტრატეგია, და რომლის ფარგლებშიც უნდა ყოფილიყო კიბერსივრცის დაცვის საკითხებზე მომუშავე უწყებათაშორისი კომისია, თავისი ფუნქციები მოცემულ სფეროში გადასცა უსაფრთხოებისა და კრიზისების მართვის საბჭოს, სადაც ჯერჯერობით ამ მიმართულებით წინსვლა არ არის. მიუხედავად ამისა, კანონში „ინფორმაციული უსაფრთხოების შესახებ“ განსაზღვრულია კიბერუსაფრთხოებაზე პასუხიმგებელი და მაკოორდინირებელი სახელმწიფო ორგანო. კერძოდ, კანონის მე - 3 თავში „კიბერუსაფრთხოების უზრუნველყოფა“ ვკითხულობთ, რომ „საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, ასევე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ სხვა, მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE. მოცემული ჯგუფის მოვალეობებში შედის კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა, კომპიუტერული ინციდენტების ანალიზი, აღრიცხვა, მათი დროული გამოვლენა, რეაგირება და კოორდინაციის უზრუნველყოფა და სხვა. ასევე,

[93] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012, გვ 49;
[94] http://www.nato.int/cps/en/natolive/news_52837.htm;

ჯგუფი პასუხისმგებელია მოცემულ სფეროში ცნობიერების ამაღლებაზე, საგანმანათლებლო პროცესზე და სხვა.[95]

საქართველოში კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვაზე, კიბერუსაფრთხოებით ღონისძიებების უზრუნველყოფასა და კიბერდანაშაულთან ბრძოლას წარმართავს იუსტიციის, თავდაცვისა და შინაგან საქმეთა სამინისტროები, რომლებსაც განსაზღვრული აქვთ და მოქმედებენ თავიანთი კომპეტენციის ფარგლები. კერძოდ: [96]

- მოცემული სამინისტროებიდან ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემებისა და სუბიექტების დაცვაზე პასუხისმგებელია იუსტიციის სამინისტროს სსიპ „მონაცემთა გაცვლის სააგენტო“, სადაც ასევე გაერთიანებულია ზემოთ ნახსენები კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE. სააგენტო ასევე განსაზღვრავს ინფორმაციული უსაფრთხოების პოლიტიკას, კოორდინაციასა და მონიტორინგს უწევს სამინისტროებსა და უწყებებში ინფორმაციული უსაფრთხოების მიმართულებით გასატარებელ ყველა ღონისძიებას.
- 2014 წლის თებერვალში თავდაცვის სამინისტროს ფარგლებში შეიქმნა სსიპ „კიბერუსაფრთხოების ბიურო“, რომლის მიზანია კიბერდანაშაულთან ბრძოლის ერთიანი სახელმწიფო პოლიტიკის განხორციელება, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა, ბიუროს კომპეტენციას მიკუთვნებული სფეროს მარეგულირებელი კანონმდებლობის შემუშავება და სრულყოფა და კანონმდებლობით დადგენილი სხვა საქმიანობის განხორციელება. ბიუროს ძირითადი საქმიანობა წარიმართება ინფორმაციული და კომუნიკაციების ტექნოლოგიების დეპარტამენტის

[95] სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, 2015, გვ 56;

[96] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 54-61;

მიერ, რომლის სტრუქტურული ერთეულებია: პროექტების მართვის სამმართველო; კომპიუტერულ ინციდენტებზე რეაგირების საკოორდინაციო სამმართველო CSIRT/CC); კომპიუტერულ ინციდენტებზე რეაგირების სამმართველო (CSIRT); კომპიუტერულ ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილება;

- ინტერნეტ - სივრცეში კიბერდანაშაულების გამოვლენას, აღკვეთას, მოკვლევით და საგამოძიებო საქმიანობას, ასევე საჭიროების შემთხვევაში დაკავებას, ახორციელებს შინაგან საქმეთა ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველო. გარდა ამისა, შინაგან საქმეთა სამინისტროში საექსპერტო–კრიმინალისტიკური მთავარი სამმართველოს შემადგენლობაში ჩამოყალიბდა კომპიუტერულ–ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც უშუალოდ ახორციელებს ციფრული მტკიცებულებების პირველად მოპყრობასა და მათ შემდგომ ექსპერტიზას. სამინისტროს შემადგენლობაში ასევე ფუნქციონირებს ოპერატიულ - ტექნიკური დეპარტამენტი, რომელიც ახორციელებს სამინისტროში ინოვაციური ინფორმაციული ტექნოლოგიების, ციფრული სატელეკომუნიკაციო სისტემების დანერგვას და ოპერირებას, აღნიშნულ სფეროებში სხვა სახელმწიფო დაწესებულებების კონსულტირებას, სამინისტროსა და მისი სტრუქტურული ქვედანაყოფების სატელეკომუნიკაციო უზრუნველყოფას და კანონმდებლობით დადგენილი წესის შესაბამისად, საგამოძიებო ღონისძიებების განხორციელების შედეგად მოპოვებული ციფრული მტკიცებულებების საექსპერტო - კრიმინალისტიკურ გამოკვლევას. [97]

საქართველო აქტიურად მიისწრაფვის ევროინტეგრაციისკენ, ქვეყანა ცდილობს გახდეს ევროკავშირისა და ჩრდილოეთ ალიანსის სრულუფლებიანი წევრი, ხელი მოეწერა ასოცირების ხელშეკრულებას. ყოველივე ეს ნიშნავს, რომ

[97] გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008, გვ 15;

ქვეყანა თავის თავზე იღებს ყველა იმ ვალდებულებას, რაც უზრუნველყოფს არამარტო საქართველოს უსაფრთხოებას, არამედ ევროკავშირის როგორც ცალკეული წევრი ქვეყნებისა ისე მთლიანად ევროკავშირის უსაფრთხოების შესაბამისი ნორმების დაცვას, სადაც ასევე იგულისხმება კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა.[98] ეს არის ქვეყნისთვის სერიოზული გამოწვევა, რადგან საქართველომ უნდა შექმნას ეროვნული კანონმდებლობა, წესრიგში მოიყვანოს და საერთაშორისო სტანდარტებს შეუსაბამოს ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემისა და ცალკეული სუბიექტების დაცვა, გაზარდოს საერთაშორისო თანამშრომლობა და რისკების შემცირების მიზნით, უნდა მოახდინოს საზოგადოების ცნობიერების ამაღლება და საგანმანათლებლო სისტემის შემუშავება. მოცემულ სფეროში აქტუალური და აუცილებელი ხდება საქართველოს სუბიექტების, ევროკავშირის წევრი და სხვა ქვეყნების ანალოგიურ სუბიექტებთან ინტეგრაციის პროცესის სწორი მიმართულებით წარმართვა, მათი ცოდნისა და გამოცდილების გაზიარება, რაც ხელს შეუწყობს კიბერუსაფრთხოების სფეროში ქვეყნის ორგანიზაციულ სტრუქტურული სუბიექტების განვითარებას, მათ საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანას, კოორდინირებული მუშაობის ამაღლებასა და ეფექტური ღონისძიებების გატარებას კრიტიკული ინფორმაციული ინფრასტრუქტურისა და პერსონალური თუ სხვა სახის მონაცემთა დაცვის მიმართულებით.[99]

[98] გორაშვილი გ., ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები, გამომც. „უნივერსალი“, თბ., 2010, გვ 62;
[99] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, 2004, გვ 77-81;

თავი 6. საქართველო და ახალი გამოწვევები კიბერსივრცეში

გასული წლის 13 ივნისს, თეირანში ირანსა და რუსეთს შორის მიღწეულ იქნა შეთანხმება კიბერუსაფრთხოების სფეროში თანამშრომლობის შესახებ, რომელიც ორიენტირებული იქნება მოცემულ დარგში სადაზვერვო ინფორმაციის გაცვლაზე, საფრთხეების წინააღმდეგ ურთიერთმოქმედებასა და საერთო თავდაცვაზე.

ბოლო ერთ თვეში, ეს არის რუსეთის მიერ მიღწეული თანამშრომლობის მეორე შეთანხმება. მანამდე, 8 მაისს რუსეთმა ჩინეთთან მოაწერა ხელი თანამშრომლობის თორმეტპუნქტიან ხელშეკრულებას, სადაც ერთი მოზრდილი პუნქტი დათმობილი აქვს კიბერუსაფრთხოების სფეროში ურთიერთობას.[100]

რუსეთის მხრიდან კიბერუსაფრთხოებაში მსგავსი გააქტიურება საერთაშორისო დონეზე არის პირდაპირი პასუხი, მიმდინარე წელს შეერთებული შტატების მიერ ახალი კიბერუსაფრთხოების სტრატეგიის მიღებაზე. სტრატეგიაში პირველად იქნა დაკონკრეტებული ქვეყნები, საიდანაც შეერთებული შტატები უნდა მოელოდნენ კიბერ საფრთხეებს. ასეთ ქვეყნებად სტრატეგიაში დასახელდა რუსეთი, ჩინეთი, ირანი და ჩრდილოეთ კორეა. ამის გათვალისწინებით, კიბერუსაფრთხოების მიმართულებით, უნდა ველოდოთ რუსეთსა და ჩრდილოეთ კორეას შორის თანამშრომლობის დაწყების ახალ ეტაპს. ფაქტიურად, შეიძლება ითქვას, რომ კიბერუსაფრთხოების სფეროში იქმნება ახალი „კოალიცია“, სადაც გაერთიანებულ ქვეყნებს გააჩნიათ საერთო ინტერესები მიმართული შეერთებული შტატების, ისრაელისა და ზოგადად, დასავლეთისა და მისი მოკავშირეების წინააღმდეგ.[101]

დარგის აღიარებული ექსპერტები მიიჩნევენ, რომ საფრთხეები ელექტრონული მმართველობის განვითარების პარალელურად, კიდევ უფრო გაიზრდება. იგივე ექსპერტები პროგნოზირებენ კიბერუსაფრთხოების ახლო

[100] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, გამომც. „მერიდიანი“ 2012, გვ 45-47;

[101] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012 , გვ 34;

მომავალს, კერძოდ, გაციფროვნების პროცესი გაგრძელდება სულ უფრო მეტი ინტენსივობით და ის შეაღწევს ჩვენი ცხოვრების ყველა ასპექტში და ჩვენი საზოგადოების ფუნქციებში. ადამიანები სულ უფრო და უფრო დამოკიდებულები გახდებიან ციფრულ მომსახურებასა და სხვადასხვა სახის ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე, რაც ხელს შეუწყობს საზოგადოებრიობის როგორც მოქალაქეების, ისე მედია საშუალებების ინტერესს კიბერუსაფრთხოების მიმართ. მომავალში თანამედროვე საზოგადოება გახდება სულ უფრო მოწყვლადი, რადგან რთულია ერთმანეთთან დაკავშირებული და დამოკიდებული სისტემების სრულად აღქმა და დაცვა. გაიზრდება გლობალური და შიდა საზოგადოებრივი დამოკიდებულებები, რაც კიბერუსაფრთხოების გამოწვევებს სულ უფრო გლობალურ ხასიათს აძლევს და ამდენად, არსებობს კიბერ საფრთხეებზე საერთაშორისო რეაგირების აუცილებლობა. ახალი ტექნოლოგიური ინოვაციები ძირითადად მოდის კერძო სექტორიდან და ეს პროცესი სულ უფრო მზარდი იქნება, რაც ერთი - ორად ზრდის ასევე უსაფრთხოების უზრუნველყოფის საჭიროებას. იქვე, ამის პარალელურად არის ახალი ტექნოლოგიები, რომლებიც უზრუნველყოფენ კიბერუსაფრთხოებას და მიუხედავად ამისა, კიბერ სივრცეში გაიზრდება გამალებული შეიარაღების პროცესი.[102]

კიბერდანაშაულებები კვლავ იქნება გამოწვევა საზოგადოებისთვის და ეკონომიკური დანაკარგები სულ უფრო გაიზრდება, რაც სხვა მხრივ ხელს შეუწყობს სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობის განვითარებას.[103] კიბერ შესაძლებლობების კონცეფციას გავლენა ექნება საერთაშორისო პოლიტიკაზე და ძალაუფლებისთვის გლობალურ ბრძოლაზე, რაც ასევე შეუწყობს ხელს კიბერ სივრცეში გამალებული შეიარაღების პროცესის გაზრდის ტენდენციას. სავსებით შესაძლებელია, რომ ახლო მომავალში მოხდება გლობალური კიბერ კატასტროფა, რაც მთლიანად შეცვლის ჩვენს მიდგომას არამარტო კიბერუსაფრთხოების, არამედ მთლიანად კიბერსივრცეში

[102] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012, გვ 23;
[103] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012, გვ 49;

საერთაშორისო თანამშრომლობის მიმართ. კიბერის ახალ ეპოქაში გამარჯვებული იქნება ის, ვინც შეძლებს საბაზრო ეკონომიკის გათვალისწინებით უსაფრთხოების საკითხების კომპლექსურ გადაწყვეტას; გააჩნიათ საუკეთესო ტალანტების მობილიზების შესაძლებლობა; და შესწევთ ადაპტაციის უნარი და ყოველგვარი ძალისხმევის გარეშე იმუშაონ მრავალეროვან გარემოში. ფაქტიურად, კიბერუსაფრთხოება გახდა საგარეო პოლიტიკის შემადგენელი ნაწილი და ის სულ უფრო აქტიურ როლს თამაშობს საერთაშორისო ურთიერთობების საკითხში. საინტერესოა ამ მხრივ რა მდგომარეობაა საქართველოში?[104]

უკვე 2008 წლის აგვისტოს ომის შემდეგ, როცა რუსეთის მხრიდან მოხდა მასირებული კიბერ შეტევა ქვეყნის ინფრასტრუქტურაზე, სამთავრობო ვებ-გვერდებზე. ქვეყანა დადგა სერიოზული პრობლემის წინაშე, იყო საფრთხე, რომ საქართველო მოქცეულიყო ინფორმაციულ ვაკუუმში. მიღებული ცუდი გამოცდილების გათვალისწინებით, ხელისუფლებამ დაიწყო კიბერუსაფრთხოების სფეროს განვითარებაზე ფიქრი. კერძოდ, იუსტიციის სამინისტროში შეიქმნა სსიპ - მონაცემთა დაცვის სააგენტო, განისაზღვრა კრიტიკული ინფორმაციული ინფრასტრუქტურის სუბიექტები, რომელთა დაცვა დაევალა მონაცემთა გაცვლის სააგენტოს, შეიქმნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“ და „კიბერუსაფრთხოების სტრატეგია“, ასევე თავდაცვის სამინისტროში ახალი შექმნილია სსიპ - კიბერუსაფრთხოების ბიურო, რომელიც პასუხისმგებელია თავდაცვის სფეროში კიბერუსაფრთხოებითი ღონისძიებების გატარებაზე. ასევე შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში არსებობს კიბერდანაშაულთან ბრძოლის სამმართველო, და ბოლოს რაც ასევე მნიშვნელოვანია შეიქმნა კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი მთავარი დოკუმენტი – საქართველოს

[104] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81;

კიბერუსაფრთხოების 2013-2015 წლების სტრატეგია. აქვე შეიძლება ავღნიშნოთ ორგანიზაცია „გრენას“ დადებითი როლი და საქმიანობა ამ მიმართულებით.[105]

მიუხედავად ამისა, კიბერუსაფრთხოების სფეროს მიმართულებით ქვეყანაში არსებობს სერიოზული პრობლემები, რაც პირველ რიგში უკავშირდება საჭირო საკანონმდებლო ბაზის არ არსებობას, რომელიც დაარეგულირებს უკვე არსებული თითოეული სუბიექტის - მონაცემთა გაცვლის სააგენტოს, კიბერუსაფრთხოების ბიუროსა და შსს კიბერდანაშაულთან ბრძოლის სამმართველოს ურთიერთ კოორდინირებულ საქმიანობას, განსაზღვრავს თითოეული სუბიექტის მოქმედების ფარგლებსა და დამატებით ვალდებულებებს, ასევე რაც ყველაზე მნიშვნელოვანია კანონმდებლობაში უნდა იყოს განსაზღვრული კერძო სექტორის, ინტერნეტ მომწოდებლების ვალდებულებები და მათთან ყველა ზემოთნახსენები სახელმწიფო სუბიექტის კოორდინირებული მუშაობის კონკრეტული ასპექტები. სხვათა შორის, მოცემულ დარგში სახელმწიფოსა და კერძო სექტორს შორის მუშაობა წარმოადგენს დიდ პრობლემას არა მარტო ჩვენთან, არამედ ბევრ წამყვან ქვეყანაში. სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობა აუცილებელი პირობაა კიბერ სივრცის დაცვის უზრუნველყოფისთვის. ერთის მხრივ სახელმწიფო ეროვნული უსაფრთხოების უზრუნველყოფიდან გამომდინარე, ვალდებულია დაიცვას ქვეყნის მთლიანი ინფრასტრუქტურა არასანქცირებული შეღწევისგან, მაგრამ არ ფლობს ყველა საჭირო რესურსს, ვინაიდან რესურსის დიდი ნაწილი არის კერძო სექტორის მფლობელობაში.[106] ეს საბაზრო ეკონომიკის პირობებში ნორმალური და აუცილებელი მოვლენაა. მეორეს მხრივ, კერძო სექტორს არ გააჩნია არავითარი სამართლებრივი ვალდებულებები ითანამშრომლოს სახელმწიფოსთან და გამოაყენებინოს მის ხელთ არსებული რესურსი. აქ ისევ და ისევ მივდივართ საჭირო საკანონმდებლო ბაზის არარსებობის პრობლემასთან და შესაბამისად არც კერძო სექტორს არ გააჩნია არავითარი ვალდებულებები. აქ ძირითადად საუბარია ინტერნეტ

[105] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, გვ 26;

[106] ზაქაშვილი უ., კიბერტერორიზმი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, გამომც. ,,მერიდიანი“, 2013 , გვ 23;

პროვაიდერებზე, რომელთა მფლობელობაშიც არის ქსელები, რომლებიც თავის მხრივ ინტერნეტით უზრუნველყოფენ სამთავრობო სტრუქტურებს, სტრატეგიული დანიშნულების ობიექტებს, კერძო მომხმარებლებს, სამრეწველო ობიექტებსა და მსხვილ კომპანიებს, მათშორის მსხვილ ბანკებს, დიპლომატიურ და სხვა უცხოურ მისიებსა თუ წარმომადგენლობებს.[107]

ასევე დიდი მნიშვნელობა ენიჭება საზოგადოების ცნობადობის ამაღლებასა და დარგის აკადემიურ დონეზე განვითარებას, რაც ჩვენთან ფაქტიურად არ ხორციელდება. საზოგადოების ცნობადობის ამაღლება და დარგის აკადემიურ დონეზე განვითარება, რაც ასევე გულისხმობს სამეცნიერო-კვლევითი და ანალიტიკური საქმიანობის წარმოებას, გაცილებით ამცირებს კიბერსივრციდან მომდინარე საფრთხეებს. აქვე ცალკე გამოვყოფდი საჭირო პროფესიული კადრებისა და სპეციალისტების არარსებობას. მაგალითად, ქვეყანას არ ჰყავს კიბერ-ანალიტიკოსები, არ არის კიბერ სამართლის დარგის სპეციალისტები, არ გვყავს კრიპტოგრაფები, რაც კიბერ თავდაცვითი საქმიანობის განვითარებისთვის აუცილებელ პირობას წარმოადგენს.[108]

მსოფლიო საზოგადოება დადგა ახალი კიბერ საფრთხის წინაშე, რაც მომდინარეობს ისლამური ჰაკერული ჯგუფებიდან და დაჯგუფებებიდან. უახლოეს მომავალში იგივე საფრთხის წინაშე აღმოჩნდება საქართველოც, რომლის საგარეო პოლიტიკა მიმართულია ევროპულ ინსტიტუტებში ინტეგრაციისკენ, ქვეყანა უნდა გახდეს ევროკავშირისა და ჩრდილოეთ ატლანტიკური ალიანსის წევრი, საქართველომ ხელი მოაწერა ევროპასთან ასოცირების ხელშეკრულებას, სადაც ერთერთ პუნქტად ჩადებულია უსაფრთხოების საკითხების უზრუნველყოფა. ყოველივე ეს გამოიწვევს, ქვეყანაში დასავლური კომპანიების, ახალი მისიებისა და წარმომადგენლობითი ოფისების გახსნას. ეს პროცესი სულ უფრო გაიზრდება, რაც თავის მხრივ, ჩვენი ქვეყნის მიმართ კიდევ უფრო ზრდის საფრთხეებს ისლამური ფუნდამენტალიზმის მხრიდან, რის პარალელურადაც

[107] Arquilla J. and Ronfeldt D. (2001) Networks And Netwars- THE ADVENT OF NETWAR (REVISITED): Defi ning Netwar pp. № 6 p 23;
[108] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm;

იზრდება კიბერ საფრთხეებიც. მაგალითისთვის, 2015 წლის იანვარიდან დღემდე განხორციელდა რამოდენიმე კიბერშეტევა, რომელიც მოდიოდა ისლამური ჰაკერული დაჯგუფებებისგან. აქ აღსანიშნავია მიმდინარე წლის 10 იანვარს ფრანგულ კომპანია "კარფურის" საქართველოს ფილიალის ვებ-გვერდზე განხორციელებულ კიბერ შეტევას, რომელიც განახორციელა "ახლო აღმოსავლეთის კიბერ არმიამ".[109] სხვათა შორის, იმ პერიოდში განხორციელდა საკმაოდ მასიური კიბერ შეტევა ფრანგულ კომპანიებსა და მათ წარმომადგენლობით ოფისებზე მთელს მსოფლიოში, სადაც ასევე ფიგურირებდა "კარფურის" საქართველოს ფილიალი. ეს ფაქტი ყურადღებას იმსახურებს და ის უნდა განვიხილოთ, როგორც პრეცედენტი ჩვენი ქვეყნისთვის, რომელსაც მომავალშიც ექნება ადგილი, და ეს არ შემცირდება, პირიქით უფრო გაიზრდება. ასევე ამა წლის 16 აპრილს ისლამური ჰაკერული დაჯგუფება "ელ მოჰაჯირის" მიერ განხორციელდა თავდასხმა "საქართველოს მოსამართლეთა ერთობის" ვებ-გვერდზე.

გარდა ამისა, დასავლეთის პრესა და ექსპერტები სულ უფრო ხშირად წერენ, რომ რუსეთი "ჰიბრიდული ომების" შემადგენელი ელემენტების გამოყენებას, უკრაინის შემდეგ იწყებს ბალტიისპირეთის ქვეყნებისა და პოლონეთის წინააღმდეგ. აქ საუბარია მიზანმიმართულ კიბერ შეტევებსა და "საინფორმაციო ომზე". არ უნდა გამოვრიცხოთ ასევე ახლო მომავალში მსგავსი ქმედებები საქართველოს წინააღმდეგ, თუმცა მანამდე ჩვენი ქვეყნის მიმართ განხორციელდა სხვა კიბერ შეტევები.[110] მაგალითისთვის, ამერიკული ავტორიტეტული ორგანიზაცია "FireEye"-ს კვლევისა და ანალიზის მიხედვით, 2008 – 2014 წლებში რუსეთის მხრიდან მუდმივად ხორციელდებოდა კიბერ შეტევები, რომელთა ობიექტები იყო საქართველოს საგარეო და შინაგან საქმეთა და თავდაცვის სამინისტროები, ასევე სხვადასხვა საინფორმაციო სააგენტოები. კიბერ შეტევების

[109] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012, გვ 34;
[110] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012, გვ 49;

ხასიათი იყო ჯაშუშური და მიზნად ისახავდა დასავლურ ინსტიტუტებთან დაკავშირებით ქვეყნის მიზნებისა და ამოცანების შესახებ ინფორმაციის მოპარვას.

კიბერუსაფრთხოების ელემენტების განხილვა უნდა მოხდეს ეროვნული უსაფრთხოების დონეზე, მიმდინარე და ახალი საფრთხეები აუცილებლად გათვალისწინებული და ასახული უნდა იყოს ეროვნული უსაფრთხოების კონცეფციაში.[111]

6.1 კიბერუსაფრთხოების უზრუნველყოფის მნიშვნელობა

კიბერსივრცე ქმნის ერთიან კომპლექსურ გარემოს მასში შემავალი ინფორმაციული და კომუნიკაციების ტექნოლოგიების მოწყობილობებითა და ქსელებით, რაც საშუალებას აძლევს საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისს, შეიარაღებული ძალების გენერალური შტაბის სტრუქტურულ ქვედანაყოფებსა და სამინისტროში შემავალ საჯარო სამართლის იურიდიულ პირებს განახორციელონ სხვადასხვა ტიპის კომუნიკაცია, ძალებისა და საშუალებების მართვა.

მომავალში კიბერსივრცე კიდევ უფრო კომპლექსური და მასშტაბური გახდება, გაიზრდება სახელმწიფო სტრუქტურების დამოკიდებულება ინფორმაციულ ტექნოლოგიებზე, რაც განაპირობებს ახალი რისკებისა და საფრთხეების წარმოქმნას. სწორედ აქედან გამომდინარე, აუცილებელია კიბერუსაფრთხოების ისეთი მოქნილი მექანიზმების შექმნა, რომლებიც ეფექტურად უპასუხებენ ახლად წარმოქმნილ გამოწვევებს.კიბერუსაფრთხოების უზრუნველყოფის მნიშვნელოვან ნაწილს, აგრეთვე წარმოადგენს ახალი

[111] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81;

კიბერშეტევებისადმი ინფორმაციული სისტემების მდგრადობის ამაღლება, პრევენციული ღონისძიებების შემუშავება და გატარება.[112]

კიბერუსაფრთხოება მოიცავს საქართველოს თავდაცვის სამინისტროს საქმიანობის ყველა იმ სფეროს, სადაც გამოიყენება ინფორმაციული ტექნოლოგიები, იქნება ეს სამხედრო/თავდაცვითი ოპერაციების დაგეგმვა, სამხედრო წვრთნების წარმოება, ლოგისტიკური მხარდაჭერა თუ სხვა, რათა უზრუნველყოფილი იქნეს ინფორმაციის მთლიანობა, ხელმისაწვდომობა და დროული გაზიარება.[113]

კიბერსივრცეში ადგილი აქვს მიზანმიმართული, შემთხვევითი, ბუნებრივი ხასიათის ინციდენტებს. ინფორმაციული ტექნოლოგიები შესაძლებელია გამოყენებული იქნეს არამართებული ან/და კანონ საწინააღმდეგო მიზნებისათვის სხვადასხვა წყაროს მიერ. მიზანმიმართულმა კიბერშეტევამ შესაძლოა მნიშვნელოვნად შეაფერხოს კრიტიკული ინფორმაციული სისტემების გამართული ფუნქციონირება, საფრთხე შეუქმნას ქვეყნის თავდაცვისუნარიანობას და უსაფრთხოებას.[114]

[112] გორაშვილი გ., ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები, გამომც. „უნივერსალი“, თბ., 2010, გვ 62;

[113] **საქართველოს** კანონი ინფორმაციული უსაფრთხოების შესახებ. გვ 14

[114] http://dea.gov.ge/uploads/legal_acts/8/Inf._Security;

თავი 7. კიბერტერორიზმის საკანონმდებლო პრობლემები

„კანონმდებელმა უცნაური გადაწყვეტილება მიიღო, როცა კიბერტერორიზმი და ტერორისტული აქტი ერთმანეთისგან განასხვავა დანაშაულის მიზნით. კერძოდ, ტერორისტული აქტი შეიძლება უცხო ქვეყნის ხელისუფლების ორგანოზე ან საერთაშორისო ორგანიზაციაზე ზემოქმედების მიზნით განხორციელდეს, კიბერტერორიზმი კი მხოლოდ მოსახლეობის და ხელისუფლების ორგანოზე ზემოქმედების მიზნით. რთულია ამ მოსაზრებას მოუძებნო ლოგიკა. მით უფრო მაშინ, რომ კომპიუტერული დანაშაულის ერთ-ერთი მთავარი სირთულე სწორედ ისაა, რომ არაა შეზღუდული სახელმწიფო საზღვრებით და მარტივია მისი ჩადენა მაგალითად, საქართველოში შინიდან გაუსვლელად, სხვა სახელმწიფოს წინააღმდეგ. განვიხილოთ კაზუსი:[115]

ბ. კრაკოვსკიმ, რომელიც იყო საქართველოს მოქალაქე და ცხოვრობდა ქ. თბილისში, შეაღწია აეროპორტის კომპიუტერულ სისტემაში და მონაცემთა გადაცემის პროცესზე გავლენით შეძლო, თბილისის მიმართულებით მფრინავ შვედეთის მთავრობის საკუთრებაში არსებულ ავია-ეკიპაჟისთვის არასწორი კოორდინატების მიწოდება, რამაც ამ თვითმფრინავისტვის ავია-კატასტროფა გამოიწვია. მოგვიანებით, ინტერნეტში გავრცელდა ბ. კრასოვსკის მიმართვა, სადაც იგი იმუქრებოდა, რომ თუ შვედეთის ელისუფლება არ გაათავისუფლებდა მის მოკავშირე პატიმრებს, მომავალში შვედეთის საკუთრებაში არსებულ სხვა თვითმფრინავებსაც ჩამოაგდებდა. ზემოაღნიშნული დანაშაულის შინაარსი შეესაბმება 324[1]-ე მუხლის მე-2 ნაწილით აღწერილ ქმედებას. სახეზე გვაქვს კანონით დაცული კომპიუტერული ინფორმაციის მართსაწინააღმდეგო დაუფლება და მისი გამოყენება. კერძოდ, ბ. კრაკოვსკიმ კომპიუტერულ ისტემაში უნებართვო შეღწევის გზით მოიპოვა ისეთი კომპიუტერული მონაცემი, რომლის გამოყენებითაც შეძლო მონაცემთა გადაცემის პროცესზე გავლენის მოხდენა და

[115] სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, თბ., 2015, გვ 56;

შვედეთის მთავრობის საკუთრებაში არსებულ თვითმფრინავის ეკიპაჟს მიაწოდა არასწორი კოორდინატები, რამაც არათუ შქმნა მძიმე შედეგის დადგომის საფრთხე, არამედ ეს შედეგი დადგა კიდეც, რადგან თვითმფრინავმა განიცადა ავია-კატასტროფა და დაიღუპნენ ადამიანები. მიუხედავად ამისა, სახეზე კიბერტერორიზმი მაინც არ გვაქვს, რადგან დამნაშავის მიზანი არ იყო არც მოსახლეობის დაშინება და არც საქართველოს ხელისუფლებაზე ზემოქმედების მოხდენა. ბ. კრასიოვსკის მიზნად ჰქონდა დასახული შვედეთის მთავრობაზე ზეგავლენის მოხდენა. [116]

შედეგად ვიღებთ უცნაურ ვითარებას: გამოდის, რომ ბ. კრასოვსკიმ ჩაიდინა 324[1] მუხლში აღწერილი ქმედება, რომლის მიზანი იყო კოდექსის 323-ე მუხლით გათვალისწინებული უცხო ქვეყნის ხელისუფლების ორგანოზე ზემოქმედების მოხდენა.

გაუგებარია, კანონმდებელმა კიბერტერორიზმი რატომ ჩაკეტა ერთი ქვეყნის საზღვრებში და დანაშაულია მიზნად მხოლოდ მოსახლეობის დაშინება და ხელისუფლების ორგანოზე ზემოქმედების მოხდენა დააწესა, მაშინ როცა ტერორისტული აქტი, პირიქით სრულყოფილად გამოხატავს ამ დანაშაულის ბუნებას და არ კმაყოფილდება მხოლოდ ქვეყნის შიდა ინტერესებით და დანაშაულის მიზნად მიუთითებს, როგორც უცხო ქვეყნის ხელისუფლების ორგანოსა, ასევე საერთაშორისო ორგანიზაციაზე ზემოქმედებას. [117]

აქედან გამომდინარე, კომპიუტერული მონაცემის გამოყენებით ჩადენილი ნებისმიერი დანაშაულის მხოლოდ ერთ სახელმწიფოს ფარგლებში განხილვა გაუმართლებელია.

[116] გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008, გვ 15;

[117] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012, გვ 23;

მოცემული მსჯელობის საფუძველზე შეიძლება დავასკვნათ, რომ კიბერტერორიზმის მუხლი შეიცავს ხარვეზებს და პრაქტიკაში რთული იქნება მისი გამოყენება. [118]

„იურიდიული დეფინიციის არარსებობის პირობებში, როგორც დოქტრინაში, აგრეთვე, ოფიციალურ ნორმატიულ აქტებში, ხშირია ტერირიზმის აღრევა სხვა სოციალურ სამართლებრივ მოვლენებთან. განსაკუთრებით ხშირია ომის, პარტიზანული ბრძოლის, ეროვნულ-გამათავისუფლებელი მოძრაობის, დეკოლონიზაციის პროცესების ტერორიზმთან გაიგივება“[119] - აღნშნავს გ. გორაშვილი. დავამატებ, რომ გარდა ჩამოთვლილისა, ტერორიზმის კომპიუტერულ დანაშაულში აღრევაც არასწორია: კიბერტერორიზმი, არის ტერორისტული აქტი, ჩადენილი კომპიუტერულ სისტემაში შეღწევის და კომპიუტერული მონაცემების უნებართვო გამოყენების გზით. ამდენად, ჩემი აზრით, კომპიუტერული მონაცემის დაუფლება შეგვიძლია განვიხილოთ ტერორიზმის ჩადენის ხერხად და არა დამოუკიდებელ დანაშაულად, რადგან კოდექსის 323-ე მუხლის მიხედვით ტერორისტული აქტია აფეთქება, ცეცხლის წაკიდება, იარაღის გამოყენება ან სხვა ქმედება, რომელიც ქმნის ადამიანის სიცოცხლის მოსპობის, მნიშვნელოვანი ქონებრივი ზიანის ან სხვა მძიმე შედეგის განხორციელების საშიშროებას ჩადენილი მოსახლეობის დაშინების ან ხელისუფლების ორგანოზე ზემოქმედების მიზნით და არა აქვს მნიშვნელობა, როგორ იქნება ეს ქმედება ჩადენილი, რა გზით, რა ხერხით: დამნაშავე კომპიუტერს გამოიყენებს, თუ ასაფეთქებელ ნივთიერებას, ამით დანაშაულის არსი არ შეიცვლება.[120]

კანონმდებელმა კომპიუტერული მონაცემების საშუალებით ჩადენილი ტერორისტული აქტი კიბერტერტორიზმად ჩათვალა. ამ ლოგიკით გამოდის, რომ დანაშაული ჩადენის ხერხის მიხედვით, უნდა დავყოთ ტერორისტული აქტის

[118] Arquilla J. and Ronfeldt D. (1993) - CYBERWAR IS COMING!: Both Netwar and Cyberwar Are Likely – pp. № 27 p 18;
[119] გორაშვილი გ., ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები, გამომც. „უნივერსალი“, თბ., 2010, გვ 59;
[120] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm;

სახეობები და გარდა, კიბერტერორიზმისა, მივიღებთ: ტერორისტულ აქტს აფეთქებით, ტერორისტულ აქტს ავტომატის სასხლეტზე ხელის გამოკვრით ან ტერორისტულ აქტს „მოლოტოვის“ კოქტეილის გამოყენებით. შესაძლებელია კიდევ უფრო გავაფართოვოთ ფანტაზია და ვისაუბროთ ტერორისტულ აქტზე სხვა სახელმწიფოს ტერიტორიაზე შეღწევით. [121] ეს მიდგომა არ უნდა იყოს სწორი და დასაბუთებული. ჩემი აზრით, 324[1]-ე მუხლში ხაზგასმულია მხოლოდ კანონით დაცული კომპიუტერული ინფორმაციის დაუფლების, მისი გამოყენების ან გამოყენების მუქარის გზით ჩადენილი ტერორისტული აქტი. ვფიქრობ ამ უკანასკნელს გულისხმობს 323-ე მუხლში მითითებული „სხვა ქმედება“. თუმცა, ეს მსჯელობა არ გამორიცხავს იმ გარემოებას, რომ კიბერტერორიზმისთვის სისხლისსამართლებრივ პასუხისმგებლობას ცალკე მუხლი ადგენს. ამ შემთხვევაში არსებული რედაქცია სერიოზულ დახვეწას საჭიროებს.

გარდა ზემოაღნიშნულისა, კიბეტერორიზმის მუხლი სხვა კითხვებსაც ბადებს. მაგალითად, განვიხილოთ დამამძიმებელი გარემოებები. 324[1]-ე მუხლის მე-2 ნაწილი ითვალისწინებს ადამიანის სიკვდილს, ან სხვა მძიმე შედეგს. მძიმე შედეგი შესაძლოა გამოიხატოს სტრატეგიული ობიექტის ფუნქციონირების შეფერხებაში, დაზიანებაში, ქონებრივ ზიანში და ა.შ. აქედან გამომდინარე იბადება კითხვა: თუ ტერორისტული აქტისთვის დამამძიმებელი გარემოებაა მისი ჩადენა ჯგუფურად და არაერთგზის, რატომ არ უნდა იყოს იგივე დამამძიმებელი გარემოება კიბერტერორიზმისთვის?[122]

ყოველივე ზემოაღნიშნულის გათვალისწინებით მიმაჩნია, რომ კოდექსში 324[1]-ე მუხლის მოცემული სახით არსებობა არის კანონმდებლობის ხარვეზი და იგი საჭიროებს მთელ რიგ ცვლილებას“.[123]

---

[121] Сибиряков С. Л. , криминологическое Характеристика и Профилактика Компьютерных преступлений, Волгоград, 1999 p 11;

[122] სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, თბ., 2015, გვ 56;

[123] ზაქაშვილი უ., კიბერტერორიზმი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, გამომც. „საუნჯე“, თბ., 2013, გვ 157-160;

კიბერტერორიზმის ბუნებიდან გამომდინარე რთულია მივაკუთვნოთ ის კონკრეტულ კომპიუტერულ დანაშაულს, რადგან მისი ჩადენა შესაძლებელია ყველა იმ ხერხისა და მეთოდის გამოყენებით, რაც გამოიყენება სხვადასხვა კომპიუტერული დანაშაულის ჩადენისას.[124] ერთ-ერთი მთავარი ნიშანი რაც განასხვავებს ამ ქმედებას სხვა კიბერშეტევებიგან ეს არის მოტივი და მიზანი, კერძოდ მოსახლეობის დაშინება და ხელისუფლების ორგანოებზე ზემოქმედება და ასევე უფრო მძიმე შედეგი, სხვა კიბერშეტევებისგან განსხვავებით, რაც შეიძლება გამოიხატოს ადამიანის სიცოცხლის მოსპობაშიც. ზოგადად რთულია არა მარტო კობერტერორიზმის არამედ ტერორიზმის ცნების განსაზღვრაც. უფრო სწორი იქნება თუ ვიტყვით რომ კიბერტერორიზმი ესაა ტერორისტული ხასიათის კიბერშეტევა. შეაძლოა უბრალო კომპიუტერილი დანაშაულიც, როგორიცაა კომპიუტერულ სისტემაში უნებართვო შეღწევა, მისი გამოყენება ან ხელყოფა დაკვალიფიცირდეს კიბერტერორიზმად თუ მან მძიმე შედეგი გამოიწვია.

რაც შეეხება ავტორის პოზიციას, სავსებით შესაძლებელია კობერტერორიზმის განვიხილოთ როგორც ტერორისტული აქტის ჩადენის ერთ ერთი ხერხი, ასევე ვეთანხმები იმ მოსაზრებას, რომ აღნიშნულ ნორმას აქვს ხარვეზი იმ კუთხით, რომ დამამძიმებელ გარემოებად არ აქვს მითითებული მისი ჩადენა ჯგუფურად და არაერთგზის.[125] აღნიშნული საკანონმდებლო ხარვეზის აღრმოფხვრის ერთ-ერთი საშულება არის ზუსტი კრიტერიუმების განსაზღვრა ტერორიზმსა და კიბერანაშაულს შორის, რადან შესაძლოა უბრალო ჰაკერმა კიბერსივრცეშსი მეღწევთ მოიპოვოს ინფორმაცია როგორც კონკრეტულ პირზე და სახელმწიფო საიდუმლოებაზე, ასევე გამოიწვიოს როგორც კონკრეტული ცალკეული პირების ისე მთლიანი მოსახლეობის დაშინება და დესტაბილიზაცია. ასევე საჭიროა გადაიდგას ქმედითი ნაბიჯები კანონმდებლობის სრულყოფისაკენ. აუცილებელია სახელმწიფოს მხრიდან ქმედითი ღონისძიებებუს განხორციელება, კერძოდ სათანადო ფროფესიონალი კადრების მოზადება, საზოგადოების ცნობიერების და და განათლების ამაღლება ამ სფეროში, ასევე კომპიუტერული

[124] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm;
[125] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199;

სისტემების თანამედროვე პროგრამებით აღჭურვა, რაც დაიცავს მათ ნებისმიერი სახის კიბერშეტევისაგან. [126]

7.1 საკანონმდებლო ინიციატივა და მისი აუცილებლობის მნიშვნელობა საქართველოსთვის

წინამდებარე პოლიტიკის აღსრულებისა და განხორციელებისათვის საჭირო კომპონენტია საკანონმდებლო ბაზის დახვეწა.[127] ინფორმაციული ტექნოლოგიების სფეროში საქართველოს თავდაცვის სამინისტრომ უნდა განსაზღვროს შესაბამისი ნორმატიული აქტების შემუშავების საჭიროება, უზრუნველყოს არსებული კანონმდებლობის საერთაშორისო ნორმებთან შესაბამისობაში მოყვანა და ამით განავითაროს და გააძლიეროს სამართლებრივი ჩარჩოები. ასევე, წინამდებარე პოლიტიკის გათვალისწინებით, საჭიროა განხილულ იქნეს საქართველოს კანონმდებლობაში, მათ შორის „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილებების შეტანის საკითხი.[128]

საქართველოს თავდაცვის სამინისტრომ უნდა გააცნობიეროს ამ ღონისძიებების პრიორიტეტულობა და ხაზი გაუსვას ისეთი ინიციატივების საჭიროებას, რომლებიც ქმნიან მყარ სამართლებრივ საფუძვლებს პოლიტიკის განხორციელებისა და თავდაცვის სამინისტროს კიბერუსაფრთხოების უზრუნველყოფისთვის.

კიბერუსაფრთხოება უნდა გახდეს საქართველოს თავდაცვის სამინისტროს მიერ ორგანიზებული სამხედრო წვრთნების შემადგენელი კომპონენტი. ძალზე მნიშვნელოვანია კიბერუსაფრთხოების წვრთნების რეგულარულად ორგანიზება და წარმოება, რაც მოიცავს, როგორც ტექნიკურ, ასევე ოპერატიულ ასპექტებსა და სტრატეგიული გადაწყვეტილებების მიღების პროცედურებს.აღნიშნული

[126] Larry J. Siegel (2008) Criminology- Cyber crime and technology - Cyber terrorism: Cyber Crime With Political Motives . pp № 449 p 25;

[127] გორაშვილი გ., ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები, გამომც. „უნივერსალი“, თბ., 2010;

[128] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ. გვ 14;

წვრთნების სისტემატურად განხორციელება უზრუნველყოფს არსებული და პოტენციური საფრთხეების დასაძლევად მზადყოფნის შეფასებას.[129]

შეუძლებელია კიბერუსაფრთხოების უზრუნველყოფა და განვითარება იზოლირებულად განხორციელდეს. დასახული ამოცანის ეფექტურად შესრულება შესაძლებელია მხოლოდ იმ შემთხვევაში, თუკი უზრუნველყოფილი იქნება მჭიდრო კოლაბორაცია საერთაშორისო და ადგილობრივ დონეზე. აქედანგამომდინარე, სახელმწიფომ უნდა განავითაროს ორმხრივი და მრავალმხრივი ურთიერთობები და აქტიურად დაუჭიროს მხარი ევროპული და ჩრდილო-ატლანტიკური ხელშეკრულების ორგანიზაციების რეკომენდაციებს, რაც ხელს შეუწყობს კიბერუსაფრთხოების უზრუნველყოფისათვის საჭირო ამოცანების შესრულებას. საქართველოს თავდაცვის სამინისტრომ ხელი უნდა შეუწყოს ინფორმაციული ტექნოლოგიების უსაფრთხოების ინციდენტებზე რეაგირების ადგილობრივ ჯგუფებს, დაამყარონ ურთიერთობა უცხო ქვეყნების კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფებთან, რათა მოხდეს ახალი სტანდარტების, მიდგომებისა და პრინციპების ადგილობრივ დონეზე დანერგვა საქართველოს კანონმდებლობის შესაბამისად.აგრეთვე, მნიშვნელოვანია თანამშრომლობის გაღრმავება საერთაშორისო ორგანიზაციებთან სამართლებრივი კუთხით. კიბერუსაფრთხოება დინამიკური სფეროა, იცვლება შეტევების ტიპი, თავდამსხმელთა მიზნები და მოტივები, და ხშირ შემთხვევაში, ძალიან რთული ხდება, განისაზღვროს, რომელი სამართლებრივი ნორმა არეგულირებს კიბერინციდენტის კონკრეტულ შემთხვევას.[130] კიბერუსაფრთხოების მიმართულებით მრავალმხრივ ფორმატში თანამშრომლობა გაზრდის ინფორმაციული და კომუნიკაციების ტექნოლოგიების სტაბილურიდა უსაფრთხო სისტემის შექმნის, განვითარების და ქვეყანაში მისი ამოქმედების შესაძლებლობებს.[131]

---

[129] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81;

[130] გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008, გვ 15;

[131] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013 , გვ 26;

დასკვნა

დღეს კიბერტერორიზმი, მსოფლიოს გლობალურ პრობლემად იქცა. სხვადასხვა სახის კიბერშეტევები, უფრო და უფრო ფართო მასშტაბებს ღებულობენ და კომპიუტერული ტექნოლოგიების განვითარებასთან ერთად პროგრესს განიცდიან. კიბერტერორიზმი ძირს უთხრის როგორც სახელმწიფოს ისე მოსახლეობის მშვიდობას კეთილდღეობას. მრავალი ქვეყანა აქტიურადაა ჩართული კიბერტერორიზმის წინააღმდეგ ბრძოლაში და ეძებს მისი თავიდან აცილების გზებსა და სტრატეგიებს.[132] კიბერტერორიზმისგან თავის დასაცავად საჭიროა სახელმწიფოთა მხრიდან ერთიანი ძალისხმევა, ურთიერთდახმარება, ერთმანეთში პრაქტიკისა და გამოცდილების გაზირება, რათა შემუშავებულ იქნეს მასთან ბრძოლის ეფექტური, როგორც სამართლებრივი, ისე ტექნიკური მექანიზმები. „კიბერტერორიზმი სერიოზულ საფრთხეს წარმოადგენს კაცობრიობისათვის, ამასთანავე, სიახლის გამო მისი საშიშროების ხარისხი ბოლომდე არ არის შესწავლილი და გაცნობიერებული.[133] გამოცდილება, რომელიც უკვე გააჩნია მსოფლიო საზოგადოებას ამ სფეროში, ნათლად მოწმობს ნებისმიერი სახელმწიფოს დაუცველობას. მით უფრო, რომ კიბერტერორიზმს არ აქვს სახელმწიფო საზღვრები, კიბერტერორისტს ფაქტიურად შეუძლია დაემუქროს პრაქტიკულად დედამიწის ნებისმიერ წერტილში განთავსებულ საინფორმაციო სისტემას.

ვირტუალური ტერორისტის აღმოჩენა და განეიტრალება საკმაოდ რთული საქმეა, იმის გამო, რომ იგი საკმაოდ უმნიშვნელო კვალს სტოვებს. მით უფრო რთულია ბრძოლა ტერორიზმთან ინტერნეტის გლობალური ქსელის გამოყენებით".[134] „ტერორიზმთან ბრძოლის ერთ-ერთი აპრობირებული ხერხია

---

[132] http://www.chebucto.ns.ca/Current/HalifaxSummitG7/;

133 სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, თბ., 2015, გვ 56;

მსგავსი ფაქტების მასმედიის მხრიდან ნაკლები აფიშირება, რადგან ხშირად ტერორისტები ამა თუ იმ ტერაქტს ახორციელებენ საზოგადოებრივი აზრის, ყურადღების მიპყრობის მიზნით და თუ მათი ნამოქმედარი და მოთხოვნები არ გადაიცემა ტელევიზიით, არ გაშუქდება პრესით, მაშინ ტერორისტული ორგანიზაციებისათვის ტერაქტების ჩადენა ყურადღების მიქცევის მიზნით, აზრს დაკარგავს. ამგვარ ტაქტიკას გასულ საუკუნეში საკმაო წარმატება მოჰყვა, როდესაც ლათინური ამერიკის სახელმწიფოებში ხელისუფლებამ ამ ქვეყნებში მოქმედ ტერორისტულ ორგანიზაციებთან ბრძოლაში ეს ხერხიც გამოიყენა".[135] „დადგა დრო, როცა კიბერტერორიზმით დაინტერესდეს არა მარტო სამხედრო ორგანიზაციები, არამედ საერთაშორისო თანამეგობრობა. მათ შორის, გაერო რათა შემუშავებული და მიღებული იქნეს საერთაშორისო კონვენცია კიბერტერორიზმის წინააღმდეგ ბრძოლის პოლიტიკური, ორგანიზაციული და სამართლებრივი ღონისძიებათა გატარების თაობაზე“.

„უდავოდ მისასალმებელია ჩვენს ქვეყანაში კიბერ დანაშაულთან ბრძოლის მხრივ გატარებული ქმედითი ღონისძიებები, კერძოდ ის, რომ საქართველო გახდა ევროპის საბჭოს კიბერდანაშაულის შესახებ კონვენციის წევრი, რითიც ჩვენმა სახელმწიფომ კიდევ ერთი დიდი ნაბიჯი გადადგა კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლაში; ასევე ეტაპობრივად მიმდინარეობს ტრენინგები და კონფერენციები კიბერდანაშაულის თემაზე, რაც უშუალოდაა მიმართული კიბერ კრიმინალის მზარდი მასშტაბების აღსაკვეთად და ცნობიერების ასამაღლებლად. სწორედ ამ მიზანს ემსახურება საქართველოში კიბერ დანაშაულთან მიმართებით გამკაცრებული საკანონმდებლო ნორმებიც.[136]

დღევანდელი მდგომარეობით, საკანონმდებლო სივრცეში არსებული ყველა მექანიზმი მეტ-ნაკლებად ეფექტურია იმისათვის, რომ კიბერ შეტევების შემთხვევები დროულად იქნეს გამოძიებული. აქვე აღსანიშნავია სხვადასხვა კანონში განხორციელებული ცვლილებებიც. თუმცა სრული სურათის დასანახად პრაქტიკა ითამაშებდა დიდ როლს, რომელიც ჯერჯერობით მწირი მოცულობით

გვაქვს საკანონმდებლო ბაზაში“.[137] “აუცილებელია როგორც სამთავრობო, ასევე ბიზნესორგანიზაციებს შორისთანამშრომლობის გაღრმავება, საგანმანათლებლო პროგრამების ფართოდ განხორციელება და საზოგადოებრივი ცნობიერების

მნიშვნელოვანია მაღალი სტანდარტების შეტევების პრევენციის სენსორული სისტემების დანერგვა, ფართო მასშტაბის კიბერკონტრდაზვერვის გეგმისა და თავდაცვითი სტრატეგიების შემუშავება. ამ თვალსაზრისით პრიორიტეტულია უწყებათაშორისი კოორდინაცია და კომუნიკაცია. მნიშვნელოვანია ქვეყნის შიგნით საკანონმდებლო ბაზის არა მარტო შემუშავება, არამედ აღსრულება. ამ პრობლემასთან გამკლავება ასევე საჭიროებს მჭიდრო საერთაშორისო თანამშრომლობას.”[138]

საქართველო აქტიურად მიისწრაფვის ევროინტეგრაციისკენ, ქვეყანა ცდილობს გახდეს ევროკავშირისა და ჩრდილოეთ ალიანსის სრულუფლებიანი წევრი, ხელი მოეწერა ასოცირების ხელშეკრულებას. ყოველივე ეს ნიშნავს, რომ ქვეყანა თავის თავზე იღებს ყველა იმ ვალდებულებას, რაც უზრუნველყოფს არამარტო საქართველოს უსაფრთხოებას, არამედ ევროკავშირის როგორც ცალკეული წევრი ქვეყნებისა ისე მთლიანად ევროკავშირის უსაფრთხოების შესაბამისი ნორმების დაცვას, სადაც ასევე იგულისხმება კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა.[139] ეს არის ქვეყნისთვის სერიოზული გამოწვევა, რადგან საქართველომ უნდა შექმნას ეროვნული კანონმდებლობა, წესრიგში მოიყვანოს და საერთაშორისო სტანდარტებს შეუსაბამოს ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემისა და ცალკეული სუბიექტების დაცვა, გაზარდოს საერთაშორისო თანამშრომლობა და რისკების შემცირების მიზნით, უნდა მოახდინოს საზოგადოების ცნობიერების ამაღლება და საგანმანათლებლო სისტემის შემუშავება.

---

[138] სისხლის სამართლის კერძო ნაწილი. წიგნი 2. ლეკვეიშვილი მ., თოდუა ნ. და მამულაშვილი გ., გამომცემლობა ,,მერიდიანი“, თბ. 2017, გვ 145;

მოცემულ სფეროში აქტუალური და აუცილებელი ხდება საქართველოს სუბიექტების, ევროკავშირის წევრი და სხვა ქვეყნების ანალოგიურ სუბიექტებთან ინტეგრაციის პროცესის სწორი მიმართულებით წარმართვა, მათი ცოდნისა და გამოცდილების გაზიარება, რაც ხელს შეუწყობს კიბერუსაფრთხოების სფეროში ქვეყნის ორგანიზაციულ სტრუქტურული სუბიექტების განვითარებას, მათ საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანას, კოორდინირებული მუშაობის ამაღლებასა და ეფექტური ღონისძიებების გატარებას კრიტიკული ინფორმაციული ინფრასტრუქტურისა და პერსონალური თუ სხვა სახის მონაცემთა დაცვის მიმართულებით. [140]

[140] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm;

გამოყენებული ლიტერატურა:

1. საქართველოს კონსტიტუცია, თბილისი, 1995 წლის 24 აგვისტო.
2. საქართველოს სისხლის სამართლის კოდექსი, 2009 წელი.
3. სისხლის სამართლის კერძო ნაწილი. წიგნი 2. ლეკვეიშვილი მ., თოდუა ნ. და მამულაშვილი გ., გამომცემლობა ,,მერიდიანი", თბილისი 2017
4. ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, გამომც. „მერიდიანი" თბ., 2012
5. კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004
6. კაცმანი ა., კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება, ჟურნალი სამართალი, 2000, №2
7. პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012
8. მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013
9. ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა", ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012
10. ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი" №3 თბ., 2012
11. გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში", ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008
12. ზაქაშვილი უ., კიბერტერორიზმი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, გამომც. თბ., 2013
13. სვანაძე ვ. გოცირიძე ა., კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები, ნაშრომების და სტატიების კრებული, თბ., 2015
14. გორაშვილი გ., ეთნიკურ-სეპარატისტული ტერორიზმის განვითარების საფრთხე საქართველოში და მისი პროფილაქტიკის გზები, გამომც. „უნივერსალი", თბ., 2010
15. საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ.

უცხოენოვანი სამეცნიერო ლიტერატურა

1. Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448 (Based on article 12 of the Council Framework Decision of 24.02.2005 on attaks against information systems)
2. Richard W. Aldrich, "CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME", USAF Institute for National Security Studies USAF Academy, Colorado, April 2000
3. Larry J. Siegel (2008) Criminology- Cyber crime and technology - Cyber terrorism: Cyber Crime With Political Motives . pp № 449

4. Dorothy E. Denning. (23.05.2000). "CYBERTERRORISM". Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
5. Tropina Tatyana Lvovna (2005) - Cybercriminality: concept, a condition, criminally-legal measures of struggle from http://www.crime.vl.ru/index.php?p=986&more=1&c=1&tb=1&pb=1
6. Arquilla J. and Ronfeldt D. (1993) - CYBERWAR IS COMING!: Both Netwar and Cyberwar Are Likely – pp. № 27
7. Arquilla J. and Ronfeldt D. (2001) Networks And Netwars- THE ADVENT OF NETWAR (REVISITED): Defi ning Netwar pp. № 6
8. Сибиряков С. Л. , криминологическое Характеристика и Профилактика Компьютерных преступлений, Волгоград, 1999
9. батурин Ю. М. Право и политика в компьютерном круге. М., 1987

ინტერნეტ მასალა

1. www. docs.cntd.ru/document/9017477
2. www.melik.narod.ru/#_2_1
3. http:// conventions.coe.int/Treaty/en/Treaties/Html/185.htm
4. http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm
5. http://www.nato.int/cps/en/natolive/news_52837.htm
6. https://ccdcoe.org/tallinn-manual.html
7. https://www.ciret.org/conferences/paris-2000/
8. http://www.chebucto.ns.ca/Current/HalifaxSummitG7/
9. http://ec.europa.eu/research/fp6/index_en.cfm
10. https://www.enisa.europa.eu/
11. http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=1&CL=ENG
12. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
13. http://dea.gov.ge/uploads/legal_acts/8/Inf._Security
14. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199