Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 37-44 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

საარჩევნო კიბერდანაშაული: არსი და ძირითადი ფორმები

ELECTORAL CYBERCRIME : ESSENCE AND BASIC FORMS

ნინო ბოჭოიძე - ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი (პოლიტიკის მეცნიერების ბაკალავრის მე-3 კურსის სტუდენტი)
Nino Bochoidze- Ivane Javakhishvili Tbilisi State University (Bachelor in Political Science – Junior)

ანოტაცია: 21-ე საუკუნეში განსაკუთრებით დიდი აქტუალურობითა და გლობალურობით გამოირჩევა საერთაშორისო ტერორიზმის საკითხი. პრობლემას არ აქვს საზღვრები და ის მთელი მსოფლიოსთვის მთავარი გამოწვევაა,რომლის წინააღმდეგ ბრძოლა მხოლოდ ერთიანი ძალისხმევითაა შესაძლებელი. ტერორიზმის ერთ-ერთ სახედ შეიძლება ჩაითვალოს „ტექნოლოგიური ერის“ ახალი პრობლემა- კიბერდანაშაული.

ინტერნეტი დღეს არის ყველაზე სწრაფად მზარდი ტექნოლოგია და ამავდროულად ერთ-ერთი ყველაზე საფრთხის შემცველი გამოგონება,რომელიც კაცობრიობას გააჩნია. რთულია ზუსტად განსაზღვრო კიბერდანაშაულის დეფინიცია, გამომიდნარე მისი კომპლექსური სტრუქტურისა და მრავალფეროვანი ფორმების. ფართოდ რომ განვმარტოთ,კიბერდანაშაული,ეს არის ყველა სახის სისხლისსამართლებრივი დანაშაული ,რომელიც ჩადენილია საკომუნიკაციო ან საინფორმაციო ტექნოლოგიების გამოყენებით,ან მათ მიმართ. კიბერდანაშაულის საკმაოდ ფართო სპექტრია ჩვენს ირგვლივ გაშლილი და ყოველდღიურად ადამიანები ვხდებით ძალიან ხშირი ინტერნეტ თავდასხმის მსხვერპლი,რაც თანამედროვე „ციფრული საზოგადოებისთვის“ მნიშვნელოვანი პრობლემაა.

კიბერდანაშაულის ერთ-ერთი ქვესახეობაა, შეიძლება ასეც ითქვას, საარჩევნო კიბერდანაშაული. ჩემ მიერ შერჩეული საკვლევი თემა, კიდევ უფრო დიდი გამოწვევაა მსოფლიოსთვის. ცალკეული სახელმწიფოები აქტიური პოლიტიკით ებრძვიან ინტერნეტ-დანაშაულს,რომლის რადიკალური ფორმაა საარჩევნო კიბერდანაშაული. ძირითადად სიტყვის ეტიმოლოგიური გაგებიდან, ცხადია, მისი დეფინიცია თავსატეხს არ წარმოადგენს,თუმცა საარჩევნო კიბერდანაშაული და მის ფორმებთან ეფექტური ბრძოლა,ნამდვილად რთულია. ისეთი ქვეყნებისთვის,როგორებიცაა ამერიკის შეერთებული შტატები, დიდი ბრიტანეთი, ევროპის მოწინავე სახელწმიფოები- მათთვის კიბერუსაფრთხოების პრობლემა ბევრად უფრო ადრე დადგა,ვიდრე საქართველოსნაირ განვითრებად ქვეყნებში. საარჩევნო კიბერდანაშაული ხელს უშლის დემოკრატიულ განვითარებას, თავისუფალ და თანასწორ არჩევნებს და ზიანს აყენებს სახლემწიფო უსაფრთხოებას. ის,რომ საარჩევნო კიბერდანაშაული დღეს ძალიან გავრცელებული ფორმაა, დასტურდება როგორც უცხოეთის (აშშ-ს ელექტრონული არჩევნები),ასევე საქართელოს მაგალითით.

საკვაძო სიტყვები: *საარჩევნო კიბერდანაშაული, არჩევნები,ეროვნული უსაფრთხოება, პოლიტიკა, კიბერ თავდასხმები.*

ABSTRACT: The issue of international terrorism is especially relevant in the 21st century. The problem has no borders and it is a major challenge for the whole world, which can be fought only through joint efforts. One of the forms of terrorism can be considered a new problem of the "technological nation" - cybercrime.

Nowadays, The Internet is the fastest growing technology and at the same time one of the most dangerous inventions that mankind has. It is difficult to define the definition of cybercrime precisely, given its complex structure and variety of forms. To put it broadly, cybercrime is all types of criminal offenses committed

using, or in relation to, communication or information technology. There is a wide range of cybercrime around us and every day we become victims of very frequent internet attacks, which is a significant problem for the modern "digital society".

One of the sub-types of cybercrime is electoral cybercrime. The research topic I have chosen is an even bigger challenge for the world than it seems. Individual states are actively pursuing and fighting against cyber and internet crime- the radical form of which is electoral cybercrime. Basically from the etymological understanding of the word, it is clear that its definition is not a puzzle, although electoral cybercrime and its effective fight against its forms are really difficult. For countries such as the United States, the United Kingdom, and advanced European states, the problem of cybersecurity has arisen much earlier than in developing countries like Georgia. Electoral cybercrime hinders democratic development, free and fair elections, and undermines national security. The fact that electoral cybercrime is a very common form today is evidenced by the example of both foreign (US e-elections) and Georgia.

KEYWORDS: *Electoral Cybercrime, Elections, National Security, Politics, Cyber-attacks*.

კვლევის მიზანი,ამოცანა,პრობლემა,კითხვა:

ჩემი მცირე **კვლევის მიზანია** განვსაზღვრო რა არის საარჩევნო კიბერდანაშაული და როგორია მისი ძირითადი ფორმები. ვნახავთ თუ რამდენად ეფექტურია საარჩევნო კიბერდანაშაულის წინააღმდეგ ბრძოლის პრევენციული ღონისძიებები. არანაკლებ მნიშვნელოვანია საზოგადოების ცნობიერების დონე საარჩევნო კიბერდანაშაულთან მიმართებით,აქ ჩვენ შევეხებით ინდივიდების დამოკიდებულებას საარჩევნო სისტემების მიმართ და უსაფრთხოების ნორმების დაცვას. ამგვარად, ვნახავთ როგორ ხდება საარჩევნო კიბერთავდასხმის მომზადება,განხორციელება, აღმოფხვრა და მისთვის თავის არიდება.

კვლევის ამოცანაა საარჩევნო კიბერდანაშაულის შესახებ კვლევებისა და სტატიების გაცნობა თუ როგორ ხორციელდება საარჩევნო კიბერთავდასხმა (მომზადება), გავაანალიზებთ საზოგადოების ცნობიერების დონეს (საარჩევნო კიბერდანაშაულის შესახებ) და აღმოვაჩენთ რა ბერკეტებს ფლობს სახელწმიფო საარჩევნო კიბერდანაშაულის აღმოსაფხვრელად.

კვლევის მთავარი პრობლემა არის 21-ე საუკუნეში საარჩევნო კიბერდანაშაულთან ბრძოლის გზების სიმწირე და საზოგადოების ცნობიერების დონე,რაც გამოიხატება არაინფორმულობაში. ბევრი ადამიანისთვის უცნობია თუ რატომ უნდა იყოს მათი პირადი მონაცემები დაცული,ვისგან და რა სარგებელი შეიძლება მიიღოს დამნაშავემ ინფორმაციის მოპარვით. პრობლემის არსი ღრმაა,ვინაიდან საარჩევნო კიბერდანაშაული შედის იმ სისხლის სამართლებრივ დანაშაულთა რიცხვში,რომელიც რთულად გამოსაძიებელი და საკმაოდ მზარდი პრობლემაა.

საკვლევი კითხვა: რა არის საარჩევნო კიბერდანაშაული, როგორია მისი ძირითდი ფორმები და რამდენად ეფექტურია საარჩევნო კიბერდანაშაულის წინააღმდეგ პრევენციული ღონისძიებები?

ჰიპოთეზა:

საარჩევნო კიბერდანაშაული თავისი არსითა და ფორმით არის მნიშვნელოვანი გამოწვევა და კომპლექსური სტრუქტურის მქონე პრობლემა. ის თავისი ხასიათითა და მასშტაბურობით ზიანს

აყენებს ცალკეული ქვეყნის ეროვნულ და საერთშორისო უსაფრთხოებასა. საარჩევნო კიბერდანაშაული არის რთულად კონტროლირებადი დანაშაული,რომლის წინააღმდეგ ბრძოლაც მოითხოვს ერთობას და ს საერთშორისო საზოგადოების ურთიერთთანამშრომლობას.

კვლევის მეთოდოლოგია:

ჩემს კვლევაში ვიყენებ თვისობრივი კვლევის მეთოდს,ვინაიდან ჩემი საკვლევი თემა თეორიულია და მოითხოვს ემპირიულ მასალაზე დაყრდნობით კონცეპტუალური დასკვნების გაკეთბას. კვლევას საფუძვლად უდევს სხვადასხვა ექსპერტის კვლევის, სტატიების, პოლიტიკის სტრატეგიული გეგმების კონტენტ ანალიზი. პირველ ეტაპზე მოძიებულ იქნა საერთაშორისო კვლევითი დოკუმენტები საკვლევ თემასთან დაკავშირებით,მოხდა მათი სიღრმისეული შესწავლა და საბოლოოდ კვლევის დასასრულს,გაანალიზებული კონტენტის საფუძველზე დასკვნის გაკეთბა.

თემის მიმოხილვა:

სარჩევნო კიბერდანაშაულის არსი და რისკები

საარჩევნო კიბერდანაშაული თავისი ხასიათითა და გავრცელების არეალით საკმაოდ ხშირი და მრავლისმომცველია. მისი არსია სწორედ თავდასხმის განხორციელება პოლიტიკურად ყველაზე მნიშვნელოვან მოვლენაზე-არჩევნებზე. კიბერთავდასხმის მიზანია მოიპოვოს ფარულად ინფორმაცია, გამოიყენოს ის ბოროტოად და მიაყენოს ზიანი კონკრეტული ქვეყნის ეროვნულ უსაფრთხოებას, პარტიას,პოლიტიკურ ფიგურას ან ყველაზე რადიკალური ფორმით, გამოიწვიოს ქვეყნების დაპირისპირება. როგორც წესი მთავარი მიზანი საარჩევნო კიბერდანაშაულისთვის არის არა კიბერსივრცის ხელყოფა,არამედ მოსახლეობის დაშინება ან ზემოქმედება ხელისუფლების ორგანოზე. რა თქმა უნდა, თავდასხმის რისკები ყოველდღიურად იზრდება,თუმცა საერთაშორისო საზოგადოება თანხმდება,რომ ჯერ კიდევ არ დგას გლობალიზებულ ერაში ის მომენტი,როდესაც ქვეყნები ციფრულად დაიწყებენ კომუნიკაციას, შესაბამისად ეს კიდევ უფრო გაზრდის თავდასხმების რაოდენობას და შესაძლოა ქსელური კავშირებით ერთი სახელწმიფო შეიჭრას მეორე სახლემწიფოს სუვერენიტეტში, მოიპოვოს საჭირო ინფორმაცია და „გაქრეს“ კიბერსივრცეში ისე,რომ მისი კვალის მიგნებას ვერავინ შეძლებს. თითქოს წარმოუდგენელია როგორ ხდება ჩვენს რეალობაში ამგვარი რთული დანაშაულის ჩადენა და შემდეგ მისი იდენთიფიკაცია,თუმცა ყველაფერი დამოკიდებული არის რისკებზე და მათ სწორად გათვლაზე. დემოკრატიას ყველაზე დიდ ზიანს არალეგიტიმურად ჩატარებული არჩევნები აყენებს. საარჩევნო კიბერთავდასხმა სწორედ იმიტომაა კომპლექსური დანაშაული, რომ ქმედების განხორციელებისას გათვლილია ყველა მოსალოდნელი რისკი. სამწუხაროდ დღეს მსოფლიოს უმრავლეს ქვეყანაში ჯერ კიდევ არ დგას საკითხი კიბერუსაფრთხოების გაძლიერების პოლიტიკის კუთხით,რაც თავის მხრივ ზრდის საფრთხეებს,რომლებთან ბრძოლაც დიდ ძალისმხევას მოითხოვს. პირველ რიგში, საარჩევნო კიბერთვდასხმისას მთავარი სამიზნე ყოველთვის არის საარჩევნო სისტემები. ვირტუალური მმართველობა კიდევ უფრო ზრდის რისკებს მოსალოდნელი თავდასხმებისას. აღსანიშნავია ის კიბერ-რისკები,რომლებიც უკავშირდება მატერიალურ ზიანს, ორგანიზაციების რეპუტაციის განადგურებას, ტექნოლოგიური წარუმატებლობის გამო შეფერხებებს,ასევე ეს ტერმინი გულისხმობს დეზინფომაცის გავრცელებას, საარჩევნო ადმინისტრაციებიდან ქსელური

უსაფრთხოების შესახებ ინფრმაციის მოპარვას, სუსტი პროგრამული უზრუნველყოფის გამოაშკარავებას და კიდევ ბევრ სხვა დამაზიანებელ ქმედებას. საბოლოო ჯამში, რისკები დაკავშირებულია როგორც კონკრეტულ ადამიანებთნ,ასევე აბსტრაქტულ მოვლენებთნ და ყველაზე მთვარ,უკონტროლო ინტერნეტთან და ონლაინ-სივრცესთან. ჩვენ უნდა შევძლოთ ძლიერი კიბერუსაფრთხოების პოლიტიკით და მოქნილი მექანიზმებით ამ საფრთხეების აღმოფხვრას და პრევენციას,მაგრამ არ უნდა დაგვავწიყდეს,რომ ყველა დიდი კიბერთავდასხმის უკან დგას ადამიანთა ჯგუფი, რომელიც სარგებლობს ავტორიტეტით,აქვს წვდომა მნიშვნელოვან ინფორმაციაზე და ხშირად ისინი არიან პოლიტიკური სპექტრის წარმომადგენლები,რომლებიც მიზანმიმარულად მოქმედებენ სამიზნის წინააღმდეგ. რაც შეეხება შემსრულებლებს,ისინი არიან უბრალო ჰაკერები კარგი ცოდნისა და გამოცდილების მქონე ადამიანები,რომლებიც უბრალოდ დავალებებს ასრულებენ.

საარჩევნო კიბერდანაშაული,როგორც პოლიტიკური დანაშაული

საარჩევნო კიბერთავდასხმა დანაშაულია,რომლის მოტივიც შეიძლება იყოს ანგარება, შურისძიება, პოლიტიკური და ა.შ. ის განიხილება პოლიტიკურ დანაშაულად,ვინაიდან თავისი არსით წარმოადგენს იდეოლოგიურად მოტივირებულ ქცევას,რომელიც იურიდიულად შეიძლება განისაზღვროს როგორც დანაშაულებრივი ქმედება.პოლიტიკურად მოტივირებული კომპიუტერული დანაშაული სტაბილურად იზრდება 1980-იანი წლების ბოლოდან[1]. საფრთხე ექმნებათ როგორც ერ-სახელმწიფოებს,ასევე პოლიტიკური დღისწესრიგის მქონე პირებსა და ჯგუფებს.საარჩევნო კიბერდანაშაული არსებითად მოტივირებულია პოლიტიკურად და მას შეუძლია ზიანი მიაყენოს, არა მხოლოდ პოლიტიკას,არამედ ეკონომიკას, ტექნოლოგიურ სფეროს, მედია საშუალებებსა და უსაფრთხოების მიზნებს. მიუხედავად იმისა,რომ კიბერთვდასხმა ითვლება პოლიტიკურ დანაშაულად, ჩვენთვის რთულია ვისაუბროთ მასთნ ბრძოლის გზებზე იგივე სტრატეგიით,როგორცაა ეს შესაძლებელია სხვა პოლიტიკურ დანაშაულთან ბრძოლისას. ძალზე რეალურია კიბერ ომისა და კიბერ ჯაშუშობის საფრთხე, რომელიც მჭიდროდაა დაკავშირებული საარჩევნო კიბერთვდასხმებთან.ამ საფრთხეების რაოდენობრივი შეფასება რთულია,ვინაიდან თავდასხმის ჭეშმარიტი წყაროს დადგენა ზოგჯერ შეუძლებელია რადგან თავდამსხმელთა უმეტესობა საკუთარ თავსა და მათ სამიზნეს შორის კავშირების ჯაჭვს იყენებს. მაგალითად, სადმე ევროპაში "ჰაკერმა" შეიძლება გამოიყენოს კომპიუტერის სისტემა ჩინეთში, გაერთიანებული სამეფოს სისტემაზე შეტევისთვის. ყურადსაღებია, ის ფაქტიც,რომ რთულია მოტივების ჩამოყალიბება ონლაინ შეტევებში,სწორედ ამიტომ არჩევნებზე თავდასხმა თავისთვად გულისხმობს პოლიტიკურ დამნაშავეობას,ვინაიდან ის პირდაპირააა მიმართული სახემწიფოში მიმდინარე პოლიტიკური მოვლენისაკენ. საარჩევნო ადმინისტრაციების მთავარი მიზანია მანიპულირების რისკების მართვა და მოსალოდნელი საფრთხეების თავიდან აცილება,რომელსაც ახორციელებენ აუდიტისა და კონტროლის

[1] Anderson,K, (29 sep,2008) „**How do we tackle political cyber-crime?“** https://www.computerweekly.com/opinion/How-do-we-tackle-political-cyber-crime?fbclid=IwAR1TO7nq7A-lKv_-7SQJzzpvYjiw1cEguaykCTudVWxHps7hQkAJdiDFkMk

ღონისძიებებით.მაშინ როდესაც მსოფლიო ქვეყნების უმრავლესობას პრაქტიკაში აქვთ არჩევნების „ქაღალდებით“ ჩტარება, დღეს თნდათანობით იზრდება ტექნოლოგიური რესურსის გამოყენება,რომელიც თავის მხრივ საფუძველია დიდი კიბერშეტევებისა. გავრცელებულია არასწორი წარმოდგენა,რომ მხოლოდ ის ქვეყნები ხდებიან კიბერთავდასხმის მსხვერპლნი,რომლებსაც ელექტრონული ხმის მიცემის სისტემა აქვთ, თუმცა ყველა არჩევნები დამოკიდებულია ინფორმაციისა და საკომუნიკაციო ტექნოლოგიის ინსტრუმენტებზე.ბევრი ექსპერტი საუბრობს სწორედ ელექტრონულ სისტემასა და ქაღალდების სისტემის სხვაობა-უპირატესობებზე და თვლიან,რომ წარმატების გასაღები იქნება კიბერუსაფრთხოება, „ქაღალდის ბილიკები“, რისკების შემზღუდავი აუდიტი და უწყებათშორისი კომუნიკაცია.

კიბერთავდასხმების ფორმები არჩევნებში

არჩევნებზე თავდასხმა შესაძლოა განხორციელდეს რამდენიმე ფორმით. არსებობს წინა საარჩევნო პროცესზე თავდასხმის ფორმა,რომლის დროსაც თავდამსხმელების მოტივი და მიზანია წინასწარი წვდომის მიღება და შემდეგ პოლიტიკური ამინდის შეცვლა,რაც იწვევს არჩევნების გაჭიანურებას ან საერთოდ გაუქმებას. მეორე ფორმა ესაა უშუალოდ არჩევნების მიმდინარეობისას თავდასხმის განხორციელება,რომელიც მიმართულია კონკრეტულად ერთი პარტიის ან პოლიტიკური ფიგურის დეგრადაციისკენ. ძირითდად მეორე ფორმა ყველაზე გავრცელებულია და ვხვდებით მის კერძო სახეებსაც,როდესაც თვდასხმები ხორციელდება პოლიტიკურ კამპანიებზე, პარტიების საინფორმაციო და საკომუნიკაციო მედია-პლატფორმებზე და ის ყველაზე ხანგრძლივ მუშაობას მოითხოვს დამნაშავის მხრიდან,რათა მიაღწიოს მიზანს. მესამე ძირითდი ფორმა გახლავთ არჩევნებზე თვდასხმა,მისი შედეგების გამოქვეყნების,ე.ი. დასრულების შემდეგ. ეს ფორმა გამოირჩევა განსაკუთრებული სიმწვავით,რადგან კიბერშეტევა გავლენას ახდენს არა მხოლოდ არჩევნებში მონაწილე კანდიდანტებზე,არამედ მთლიან ელექტორატზე. განსაკუთრებულს მგრძნობელობას იწვევს საარჩევნო კიბერშეტევები საზოგადოებაში.რთულია სახელმწიფოსთის ახსნას მიზეზები და მიზნები თავდასხმებისა, რომლის თვიდან აცილებაზე პასუხსიმგებელი თავადაა. თითოეული ჩვენგანი შესაძლოა ისე გავხდეთ კიბერთავდასხმის მსხვერპლი,რომ ეს ვერც გავაანალიზოთ,მაგრამ როდესაც საქმე დემოკრატიულ ღირებულებებზე დაფუძნებულ ფარულ კენჭისყრას ეხება, საზოგადოება ვერ ეგუება პირადი ინფორმაციის თაღლითური მოპოვების ფაქტს. არსებობს თვდასხმის საჰაერო განხორციელების პრაქტიკა რომელიც ეფექტურად მუშაობს დეზინფორმაციის გავრცელებასთნ ერთად. რაც უფრო მარტივია საარჩევნო ინფრასტრუქტურა,მით უფრო ადვილია თვდასხმა მასზე. შეტევის განხორციელება სივრცეში განუსაზღვრელია შეიძლება ითქვას, ვინაიდან თანაბრად მოსალოდნელია როგორც ქვეყნის შიგნიდან თვდასხმა,ასევე სხვა სახელწმიფოებიდან. ბევრი მკვლევარი საუბრობს მომავალი არჩევნების საფრთხეებზე,რომლებიც მომდინარეობს კიბერსივრციდან და ეხება ინფორმაციის გასაჯაროვებას. მაგალითისთვის შეგვიძლია გავიხსენოთ სულ ახლახანს მომხდარი კიბერთვდასხმა რუსეთის მხრიდან საქართველოს სააარჩევნო სიებზე.[2] ამერიკული გამოძიების თანახმად, საქართველოს მოსახლეობის პირადი ინფორმაცია მოპარულ და განთვსებულ იქნა საერთშორისო მონაცემთა უცხოური ბაზის პორტალზე,სადაც ერთდროულად ასეულობით ქვეყნის უსაფრთხოების სამსახურს აქვს წვდომა და შეეძლოთ გასაჯაროვებული ინფორმაციის

[2] Cimpanu, C. (March 30,2020 -- 02:07 GMT (03:07 BST) **“Personal details for the entire country of Georgia published online”** https://www.zdnet.com/article/personal-details-for-the-entire-country-of-georgia-published-online/

მოპარვა და რა თმა უნდა საჭიროებისამებრს გამოყენება. დიდი კიბერშეტევის მსხვერპლი იყო 2016 წლის არჩევნები ამერიკის შეერთეული შტატები,რომელსაც მსოფლიოში ყველაზე ძლიერი კიბერუსაფრთხოების პოლიტიკა აქვს და სწორედ მისი მაგალითით დასტურდება ჩემი ჰიპოთეზა,რომ ისეთ ძლიერ საფრთხესთნ ბრძოლა,როგორიც საარჩევნო სისტემებზე კიბერთვდასხმებია, მარტო რთულია და მოითხოვს საერთაშორისო საზოგადოების ურთიერთთანამშრომლობას.სწორედ ამას გულისხმობს უწყებათშორისი კომუნიკაცია,რაც აშშ-ს მთავარი ბერკეტია კიბერუსაფრთხოების გაძლიერებისთვის.2017 წლის ივნისში შეერთებული შტატების მასშტაბით, 100-მა საარჩევნო ექსპერტმა კონგრესს მიმართა ღია წერილით აღნიშნა, რომ მრავალი იურისდიქცია „არასათანადოდ იყო მომზადებული, რათა გაუმკლავდეს კიბერუსაფრთხოების რისკების ზრდას“[3]. ეს ნიშნავს,რომ ბევრ პრობლემას და გამოწვევას აწყდება მსოფლიოში ყველა სახელმწიფო როდესაც საქმე ეხება კიბერსივრცეს.

საარჩევნო კიბერუსაფრთხოება(უსაფრთხოების დაცვის მექანიზმები) საფრთხე და პრევენცია

როდესაც ჩვენ ვსაუბრობთ საფრთხეებზე და მათ მიერ გამოწვეულ ზიანზე,აუცილებელია პარლელურად განვიხილოთ კიბერუსაფრთხოების მნიშვნელობა და ის მექანიზმები,რომლითაც შესაძლებელია რისკების თავიდან აცილება და უსაფრთხოების უზრუნველყოფა. ყველაზე მთავარი,როდესაც საქმე ეხება საარჩევნო კიბერთავდასხმას,არის თავდამსხმელსა და სამიზნეს შორის ურთიერთკავშირის დადგენაა. შემდეგი ნაბიჯი არის შესაბამისი სტრუქტურებისა და სახლმწიფო აპარატების მხრიდან რისკების სწორი შეფასება,რასაც მოჰყვება საბრძოლო სტრატეგიის შემუშავება. ცნობილია,რომ იდენტური კიბერშეტევა არ არსებობს,ვინაიდან არ არსებობს იდენტური ქსელი,შესაბამისად თითოეული შეტევის ფაქტს სჭირდება კონკრეტული დეტალური გამოძიება. საბოლოო ნაბიჯი არის პრობლემის აღმოფხვრა, მოქნილი ბერკეტებით ბრძოლა და ყველაზე რადიკალური ფორმა არის კონტრშეტევა. რაც შეეხება,კონტრშეტევას, ის პრაქტიკაში ჯერ არ განხორციელებულა,ქმედების კვალიფიკაცია არ მომხდარა როგორც-კონტრშეტევა,თუმცა აშშ-ს კიბერუსაფრთხოების პოლიტიკა ითვალისწინებს მსგავს ღონისძიებებსაც.

საარჩევნო სისტემის ქსელური უსაფრთხოება გულისხმობს „ონლაინ“ და „ოფლაინ“ მდგომარეობაში პროგრამული უზრუნველყოფის თანაბარ სიძლიერეს. ყველაზე გახშირებული თავდასხმები მაინც ხდება პირად ინფორმაციულ ბაზებზე და საჯარო მედია პლათფორმებზე, საიდანაც უფრო მარტივია ინფორმაციის აღება და ბოროტად გამოყენება ვიდრე პირადი მონაცემებით მანიპულირება. დღეს უკვე ბევრი დიდი ორგანიზაცია და კორპორაცია იბრძვის კიბერსივრციდან მომავალი საფრთხეების წინააღმდეგ,ისინი თანამშრომლობენ ცალკეული სახლემწიფოების უსაფრთხოების სამსახურებთნ და ქმნიან ერთგვარ ვაკუუმ სისტემას რათა კანონიერად დაიცვან ის,რასაც „ჰაკერები“ უკანონოდ ართმევენ. საერთაშორისო სამართალი,რომელიც აწესრიგებს კიბერსამართალს და იცავს საერთაშორისოდ ყველა ქვეყნის ეროვნული სამართლის მიერ აღიარებულ ნორმებს,ითვალისწინებს კიბერთავდასხმების წინააღმდეგ მიმართულ პრევენციურ ღონისძიებებს.მინდა სტრუქტურის რთული აგებულების

[3] National Election Defense Coalition (June 21,2017) **“Election Integrity Open Letter to Congress,”** https://www.electiondefense.org/election-integrity-expert-letter

გასააზრებლად მოვიყვანო "FIREEYE"-ის ექსპერტთა კვლევა[4] მაგალითად და მოკლედ განვიხილო თუ რა კონკრეტული ნაბიჯებია იმისთის,რომ არჩევნებზე კიბერთავდასხმა იქნას თავიდან აცილებული და საფრთხეები განეიტრალებული. პირველ რიგში, ექსპერტები გამოყოფენ სამ ძირითად დაუცველ კატეგორიას,რომლებიც ყველაზე ხშირად ხდებიან ამგვარი თვდასხმების სამიზნეებში. პირველი ეს არის ძირითადი საარცევნო სისტემები,მეორე -საარჩევნო ადმინისტრატორები და ბოლოს საარცევნო კამპანიები,რომლებშიც თავის მხრივ იგულისხმება (პარტიები,სოც.მედიის პლათფორმები,საინფორმაციო ორგანიზაციები,დონორი ჯგუფები...). თვდაცვის მექანიზმები კი ასე გამოიყურება- პირველი ნაბიჯი არის საარცევნო ინფრასტრუქტურის კრიტიკული შეფასება, შემდეგი ნაბიჯია ხარვეზების გამოვლენა და ხმის მიცემის გეგმის ტესტრიება,შემდეგი ეტაპია საარცევნო ინფრასტრუქტურის მოდერნიზება,რაც გულისხმობს უსაფრთხოების პროგრამულ გაუმჯობესებას და ბოლო ნაბიჯი არის არსებული ტექნოლოგიური კავშირების მუდმივი განახლება.არსებობს რადიკალური გზით ამ პრობლემის გადაჭრის საშუალებაც,რაც პირდაპირ მოიაზრებს საარჩევნო სისტემების შეცვლას, ინფორმაციის ნაკლებ საჯაროობას და ტექნოლოგიების როლის შემცირებას საარჩევნო ინფრასტრუქტურაში. ევროპის მოწინავე ქვეყნბში ფიქრობენ,რომ არჩევნების ელექტრონული სისტემით ჩატარება ყველაზე დიდი საფრთხის შემცველია,მაშინ როდესაც აშშ-ში ეს პრაქტიკა უკვე წლებს ითვლის და ის მაინც დემოკრატიის უპირობო ნიმუშია.

დასკვნა

ამრიგად, მინდა ჩემი მსჯელობა შევაჯამო და ვთქვა,რომ საარჩევნო კიბერდანაშაული ნამდვილად არის ერთ-ერთი ყველაზე კომპლექსური სტრუქტურის მქონე დანაშაული,რომლის წინააღმდეგ ბრძოლაც მოითხოვს სიფრთხილეს და ძალების კონსტრუირებას ერთობლივად. ბუნებრივია,საფრთხეები ზრდადი ფუნქციაა და შესაბამისად მისი პრევენცია პირდაპირპროპორციულად უნდა მოხდეს.მე მიმაჩნია,რომ ეროვნულ დონეზე სახელმწიფოები სისხლის სამართლის კოდექსით ვერ დაარეგულირებენ მსგავსს კიბერშეტევებს,გარდა ამისა საერთაშორისო სამართალი ყოველთვის ვერ უმკლავდება ქსელურ თავდასმხებს და საჭიროა კიბერუსაფრთხოების გაძლიერება,აშშ-ს მრავალწლიანი პრქტიკის გაზიარება და რაც ყველაზე მთავარია საზოგადოების ცნობიერების დონის ამაღლება,რადგან მაშინაც კი,როდესაც თავს უსაფრთხოდ ვგრძნობთ,ვიღაცები დაკავებულები არიან ჩვენს შესახებ ინფორმაციის მოპოვებით,დამუშავებითა და სწორ დროს ,სწორ ადგილას გამოყენებით.

ბიბლიოგრაფია:

1. Anderson,K, (29 sep,2008) „**How do we tackle political cyber-crime?"** https://www.computerweekly.com/opinion/How-do-we-tackle-political-cyber-crime?fbclid=IwAR1TO7nq7A-lKv_-7SQJzzpvYjiw1cEguaykCTudVWxHps7hQkAJdiDFkMk
2. Cimpanu, C. (March 30,2020 -- 02:07 GMT (03:07 BST) **"Personal details for the entire country of Georgia published online"** https://www.zdnet.com/article/personal-details-for-the-entire-country-of-georgia-published-online/
3. National Election Defense Coalition (June 21,2017) **"Election Integrity Open Letter to Congress,"** https://www.electiondefense.org/election-integrity-expert-letter

[4] Seen (29 April,2020) "**Cyber threats and elections: understanding the security risk".** https://vision.fireeye.com/editions/06/06-cyber-threats-and-elections.html?fbclid=IwAR1j9LtiMEtFkCZcAOJqbGu62IzyLY_mqLTI5Y-kvAl4JtLbaKTq0cNF5Vc#

4. Seen (29 April,2020) "**Cyber threats and elections: understanding the security risk".** https://vision.fireeye.com/editions/06/06-cyber-threats-and-elections.html?fbclid=IwAR1j9LtiMEtFkCZcAOJqbGu62IzyLY_mqLTI5Y-kvAl4JtLbaKTq0cNF5Vc#
5. Jakobsson, M. and Ramzan, Z. (Apr 23,2008) **"Cybercrime and Politics: The Dangers of the Internet in Elections"** https://www.informit.com/articles/article.aspx?p=1190114&ranMID=24808&fbclid=IwAR0tnKJGmtgqfK5AeoT1L892KBPN2SGCA_yhndhK7SO0nIQjCggGvkWPaFQ
6. Rafter,D. (Seen – may 3,2020) **"2020 election cybersecurity: Protecting U.S. elections against cybercrime"** https://us.norton.com/internetsecurity-emerging-threats-2020-election-cybersecurity.html?fbclid=IwAR0HoTAl4coxa8nmkX8ts9cbuoIhugSKiSxDmhRPffcPZHPWm4oImbk107Q
7. Fidler, D.P (2016**) "The U.S. Election Hacks, Cybersecurity, and International Law"** DOI: https://doi.org/10.1017/aju.2017.5
8. Ivanova, A.X. (September,2019) **"Online voting as an element of cybersecurity of megacities" https://www.researchgate.net/publication/339143499_Online_voting_as_an_element_of_cybersecurity_of_megacities?fbclid=IwAR0Yq9SaLkOWcP4fJdhgL6mau9c_GO5_C-it-5dkTrTYkoozEKXttiRSiLY**
9. Morris, D. Baccio, M. Klein,D. Nixon. A. (April 28,2020) **"Cyber Threats to Elections"** Webinar **https://www.brighttalk.com/webcast/574/387719/cyber-threats-to-elections?fbclid=IwAR2YFZ2dCFoeq5Phfmu4c1MNV9rB03KyOMLsK--cx2A1dlVTrsd1X6-_fTo**
10. Thomas,D. (October 26,2017) **"Protecting elections from cyberattacks"** **https://www.raconteur.net/technology/protecting-elections-from-cyberattacks**
11. Staak.S.V. and Wolf,P. (seen April 30,2020) **"Cybersecurity in Elections" (Models of Interagency Collaboration) https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf?fbclid=IwAR3EPnVTRkIm6rwncCm1uL-llPeHqmXYPgRpE6OYa1EJaAisWQcP7RQXb_s**
12. Seen (May 2,2020) **National Counterintelligence and Security Centre- "Foreign Threats to U.S. elections ,election security information needs"** **https://www.odni.gov/files/ODNI/documents/DNI_NCSC_Elections_Brochure_Final.pdf**
13. Agawu, E. A. (April 3, 2018) **"How to Think About Election Cybersecurity: A Guide for Policymakers." https://www.newamerica.org/cybersecurity-initiative/policy-papers/how-to-think-about-election-cybersecurity/**
14. Hawkins, D. (June 5, 2018) **"The Cybersecurity 202: Voters' Distrust of Election Security Is Just as Powerful as an Actual Hack, Officials Worry"-** *Washington Post* **https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/05/the-cybersecurity-202-voters-distrust-of-election-security-is-just-as-powerful-as-an-actual-hack-officials-worry/5b1567091b326b08e883912f/%3futm_term%3d.7a03e7805651**