ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი
სოციალურ და პოლიტიკურ მეცნიერებათა ფაკულტეტი

მირანდა მუსელიანი

საინფორმაციო უსაფრთხოების ფენომენი 21-ე საუკუნეში- კიბერუსაფრთხოება და მისი განმსაზღვრელი ფაქტორები(ამერიკა - საქართველო)

ნაშრომი შესრულებულია კონფლიქტების ანალიზისა და მართვის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი:ვახტანგ მაისაია

პოლიტიკის მეცნიერებათა დოქტორი

თბილისი

2017

Ivane Javakhishvili Tbilisi State University

Miranda Museliani

Information Security phenomenon of the 21-st century-Cyber Security and it's determinants(Georgia/Usa).

Master Programme in Conflict Analysis and Management of the Faculty of Social and Political Sciences

The thesis is submitted for obtaining the Master's Degree in Conflict Analysis and Management

Head: Vakhtang Maisaia

Doctor of Political Sciences

Tbilisi

2017

ანოტაცია

ნაშრომის თემაა საინფორმაციო უსაფრთხოების ფენომენი 21-ე საუკუნეში-კიბერუსაფრთხოება და მისი განმსაზღვრელი ფაქტორები(ამერიკა -საქართველო).

კვლევის მიზანია:

- ✓ რა ფაქტორები განსაზღვრავს კიბერუსაფრთხოებას საქართველოსა და ამერიკაში.

კვლევის ამოცანებია:

- ✓ კიბერუსაფრთხოების ფენომენის განსაზღვრა.
- ✓ რამდენად არის კიბერუსაფრთხოება განხილული,როგორც საერთაშორისო უსაფრთხოების შემადგენელი ნაწილი.
- ✓ კიბერ ომის ფაქტორი გეოსტრატეგიული დაპირისპირების ფარგლებში.
- ✓ თანამშრომლობის ფორმების გამოკვეთა(როგორ ხდება კიბერუსაფრთხოების ფარგლებში თანამშრომლობა ამერიკა/ საქართველოსთვის).

21-ე საუკუნეში მთელი სამყარო დამოკიდებულია ინტერნეტზე,ინტერნეტ ქსელებზე და მათი საშუალებით კომუნიკაციაზე.ერთი მხრივ ეს ყველაფერი ხელს უწყობს საზოგადოების განვითარებას,თუმცა მეორე მხრივ გამოიწვია დამოკიდებულება მათზე. იქიდან გამომდინარე, რომ ყველაფერი ერთმანეთთანაა კავშირში,გამოიწვია კიბერუსაფრთხოების საკითხის გააქტიურება. ცნობილია,რომ ამერიკა არის უპირველესი სახელმწიფო კიბერუსაფრთხოებაში,ხოლო საქართველო თანდათან იდგამს ფეხს და ვითარდება.ამ ორი სახელმწიფოს განხილვით შევძლებთ დავინახოთ თუ რა არის სუპერ სახელმწიფოს და განვითარებადი სახელმწიფოს კიბერუსაფრთხოება და მისი განმსაზღვრელი ფაქტორები.რისი გაკეთება უწევთ სუპერ და განვითარებად სახელმწიფოს მაქსიმალური დაცული კიბერუსაფრთხოების მისაღწევად,რა პრობლემებს აწყდებიან ისინი და ა.შ. განვიხილავთ ამერიკასა და საქართველოზე განხორციელებულ უდიდეს კიბერ შეტევებს და თითოეული სახელმწიფოს ნაბიჯებს მათ მოსაგვარებლად და გადასაჭრელად.

Annotation

The thesis of the work is „ Information Security phenomenon of the 21-st century-Cyber Security and it's determinants(Georgia/Usa).

The goal of the research is:

- ✓ What factors determine cyber security in Georgia and America.

The objectives of the research are:

- ✓ Determining the phenomenon of cyber security.
- ✓ How much security is considered as a component of international security.
- ✓ The factor of cyber warfare in the geostrategic controversy.
- ✓ Outcome of cooperation (how to cooperate within the cyber security for America / Georgia).

In The 21st century The whole world depends on the Internet, and communication through them. On the one hand it all contributes to the development of society, but on the other the attitude towards them.

It is known that America is the foremost state in cyber security, and Georgia is gradually standing up and develops. By considering these two states we will be able to see what is the super-state and the emerging state cyber security is and its determining factors. What do they have to do to achieve the highest cyber security in a super and developing state, what problems they face, etc. We consider the biggest cyber attacks in America and Georgia and the steps of each state to solve them.

სარჩევი

1.შესავალი.....**6**

1.1გამოკვლევის მეთოდოლოგია.....7

2. საინფორმაციო უსაფრთხოების ზოგადი მიმოხილვა.....9

2.1 რა არის კიბერუსაფრთხოება - არსი, ისტორიული მიმოხილვა და მიმართულებები...11

2.2. კიბერდანაშაული და მისი ტიპოლოგია.....13

2.3. კიბერთავდაცვა და მისი ინსტრუმენტები.....18

3. საქართველოს კიბერ უსაფრთხოების გარემო და მისი ანალიზი.....20

4. ამერიკის შეერთებული შტატების კიბერ უსაფრთხოების რაობა და არსი - მოკლე მიმოხილვა.....25

5. კიბერ საფრთხეების გეოპოლიტიკური ასპექტები: კიბერშეტევები საქართველოსა და ამერიკის შეერთებულ შტატებზე.....28

5.1. 2008 წელს რუსეთის მიერ საქართველოზე კიბერშეტევა.....28

5.2. აშშ-ს კიბერმოწყვლადობის შემთხვევა.....31

5.3. რუსი ჰაკერების მიერ აშშ-ს დემოკრატიული პარტიის დაჰაკვა.....33

5.4. Petya-გლობალური კიბერ ვირუსი- საქართველოს ჭრილში.....36

6. კვლევის ანალიზი.....39

7.დასკვნა.....46

8. უცხო ტერმინთა განმარტება.....47

9.რეკომენდაციები.....49

10.ბიბლიოგრაფია.....50

1. შესავალი

სამაგისტრო ნაშრომის თემაა- საინფორმაციო უსაფრთხოების ფენომენი 21-ე საუკუნეში- კიბერუსაფრთხოება და მისი განმსაზღვრელი ფაქტორები.თემა განხილული იქნება საქართველოსა და ამერიკის შეერთებული შტატების მაგალითზე,რომლის საშუალებითაც ნათლად დავინახავთ განვითარებადი და სუპერ სახელმწიფოს შორის კიბერ უსაფრთხოების საკითხს.

21-ე საუკუნის კონფლიქტების ანალიზი გვიჩვენებს,რომ კიბერუსაფრთხოება არის ყველა ომისა თუ კონფლიქტის განუყოფელი ნაწილი.იგი თავის მხრივს დაკავშირებულია ინფორმაციული ტიპის კონფლიქტთან,რომელიც სწორედ კიბერ შეტევის მიზეზით შეიძლება იყოს გამოწვეული,რამაც შეიძლება ახალი კონფლიქტის კერა წარმოშვას ან არსებულის ესკალაცია გამოიწვიოს.

ნაშრომი განიხილავს კიბერუსაფრთხოების არსს,მის განმსაზღვრელ ფაქტორებს.საინფორმაციო უსაფრთხოების ფენომენს და ამერიკისა და საქართველოს მაგალითზე რეალური კიბერშეტევებს.ასევე, საშუალებას მოგვცემს დავინახოთ კიბერუსაფრთხოების დადებითი ან უარყოფითი მხარეები,რამდენად გახდა იგი საერთაშორისო უსაფრთხოების განმსაზღვრელი ფაქტორი და შეცვალა, თუ არა მან ბოლო ათწლეულის განმავლობაში მსოფლიო.

საუბარია იმაზე თუ რა როლი უჭირავს კიბერუსაფრთხოებას დღევანდელ გეოპოლიტიკურ სივრცეში,რამდენად გადამწყვეტ ფიგურას წარმოადგენს ის სახელმწიფოებისთვის.

განვიხილავ 21-ე საუკუნის მსოფლიოს უდიდეს კიბერ შეტევებს, ვინაიდან რეალური ფაქტების საშუალების განვსაზღვროთ საკითხის არსი.

1.1.გამოკვლევის პროგრამა/მეთოდოლოგია

კვლევის ჩასატარებლად შევარჩიე თვისებრივი სოციოლოგიური კვლევის მეთოდი.გამოვიყენე სიღრმისეული ინტერვიუ ექსპერტებთან და შემთხვევის შესწავლა, მსოფლიოს ყველაზე დიდი კიბერ შეტევების შესასწავლად.შემთხვევის შესწავლა არის თვისებრივი კვლევის მეთოდი და ასევე,ზოგადად,კვლევითი სტრატეგია,რომლის მიზანია ცალკეული ფენომენის ემპირიული შესწავლა რეალურ ცხოვრებისეულ სიტუაციაში სხვადასხვა წყაროების გამოყენებით.გენერალური ერთობლიობას წარმოადგენენ - ექსპერტები. შერჩევის სახე - არაალბათური.ხოლო შერჩევის ტიპი-მიზნობრივი ანუ შეფასებითი,რომლის დროსაც შესასწავლი შემთხვევების შერჩევა ან გარკვეული მიზნით ხდება ანდა ექსპერტთა შეფასებების საფუძველზე. შერჩევის ჩარჩოს წარმოადგენს ის დეპარტამენტები,რომლებიც კიბერუსაფრთხოების მიმართულებით მუშაობენ. ექსპერტებთან გამოყენებული სიღრმისეული ინტერვიუ იყო შედგენილი ნახევრად სტრუქტურირებული კითხვარით,რომელიც უფრო მოქნილი და მოხერხებულია.

მიზნობრივი შერჩევის საფუძველზე შევარჩიე 6 ექსპერტი,რომლებიც მოღვაწეობენ ამ სფეროში, 3-ამერიკელი და 3-ქართველი, იქედან გამომდინარე,რომ ამ ორ ქვეყანას შევეხებით, სწორედ ამიტომაც, მათი აზრი ყველაზე მნიშვნელოვანია,ისინი მუშაობენ ძირითადად ამ ორ ქვეყანაზე, ფლობენ ყველაზე მეტ ინფორმაციას მათ შორის ურთიერთობებზე კიბერუსაფრთხოებასთან დაკავშირებით,იციან თუ რა გეგმები აქვთ სამომავლოდ ამ სფეროში და ა.შ.

ასევე, განვიხილავ სამ უდიდეს შეტევას ამერიკასა და საქართველოზე,რომელიც მსოფლიო ექსპერტების მიერ იქნა აღიარებული.ასევე ერთ კიბერ შეტევას, რომელიც 2017 წლის 27 ივლისს განხორციელდა მთლიანი მსოფლიოს მასშტაბით. ეს არის კიბერ შეტევების მაგალითები,რომლებიც მსოფლიოში არ განმეორებულა და უდიდესი ზარალი მოუტანა ორივე ქვეყანას,როგორც ფინანსურად,ასევე რეპუტაციის მხრივ,ნდობის მხრივ და ა.შ. ამისთვის გამოვიყენე შემთხვევის შესწავლა,რომელიც სიღრმისეულად მოგვცემს საკითხის შესწავლის საშუალებას რეალურ მაგალითებზე და ფაქტებზე დაყრდნობით.ჩემს შემთხვევაში ვიხელმძღვანელე, მოვლენების, როლების და ურთიერთობების შესწავლა - როდესაც შემთხვევის შესწავლა გულისხმობს მოვლენათა დეტალური აღწერას, იგი აგრეთვე მოიცავს მის ახსნას და ინტერპრეტაციას გარკვეულ თეორიებთან მიმართების დადგენის საფუძველზე, თუმცა აუცილებელია ფაქტების და მის შედეგად გაკეთებული დასკვნების ერთმანეთისგან მკაფიოდ გამოცალკევება, სხვა სიტყვებით, ნათლად უნდა ჩანდეს სად არის ფაქტი და სად ავტორისეული ვარაუდი.(განმარტებითი ლექსიკონი/ეროვნ. სასწ. გეგმებისა და შეფასების ცენტრი. - [თბ., 2008]. - 20სმ. [MFN: 76027] ნაწ. 2: განათლების სპეციალისტებისათვის

/ [წიგნზე მუშაობდნენ: სიმონ ჯანაშია და სხვ.]. - [2008]. - 56გვ.. - ბიბლიოგრ.: გვ. 54-56. - ISBN: 978-9941-0-0541-1 (ყველა ნაწ.), ISBN: 978-9941-0-0542-8 (ნაწ. 2) : [ფ.ა.][MFN: 95118]

კვლევის განხორციელების ეტაპები განაწილდება შემდეგნაირად:

- ✓ პირველ ეტაპზე დამუშავდა ამ საკითხთან დაკავშირებით არსებული ლიტერატურა.
- ✓ მეორე ეტაპზე შემუშავდა გეგმა კვლევის განხორციელებისთვის.
- ✓ ექსპერტების მოძება.
- ✓ კითხვარის შემუშავება-რომელიც იყო ნახევრად სტრუქტურირებული.
- ✓ შემდეგი ეტაპია ყველაზე გახმაურებული სამი კიბერ შეტევის შესწავლა შემთხვევის შესწავლის მეთოდის გამოყენება.
- ✓ კვლევის ანალიზი.
- ✓ დასკვნა.
- ✓ რეკომენდაციები.

კვლევის მიზანია:

- ✓ რა ფაქტორები განსაზღვრავს კიბერუსაფრთხოებას საქართველოსა და ამერიკაში.

კვლევის ამოცანებია:

- ✓ კიბერუსაფრთხოების ფენომენის განსაზღვრა.
- ✓ რამდენად არის კიბერუსაფრთხოება განხილული,როგორც საერთაშორისო უსაფრთხოების შემადგენელი ნაწილი.
- ✓ კიბერ ომის ფაქტორი გეოსტრატეგიული დაპირისპირების ფარგლებში.
- ✓ თანამშრომლობის ფორმების გამოკვეთა(როგორ ხდება კიბერუსაფრთხოების ფარგლებში თანამშრომლობა ამერიკა/ საქართველოსთვის).

2. საინფორმაციო უსაფრთხოების ზოგადი მიმოხილვა

საერთაშორისო სტანდარტები, ინფორმაციულ უსაფრთხოებას განსაზღვრავს, როგორც ინფორმაციის კონფიდენციალობის დაცვას,მთლიანობას და ხელმისაწვდომობას (ISO/IEC 27002, 2005,p.1).

ინფორმაციული უსაფრთხოების მიზანია ამა თუ იმ საქმიანობის უსაფრთხოების უზრუნველყოფა,უსაფრთხოების შემაფერხებელი ინციდენტების მინიმუმამდე დაყვანა(Von Solms, 1998).

ასევე ინფორმაციული უსაფრთხოება,შემოკლებით Infosec,არის მოახდინოს არაავტორიზებული დაშვების,ინფორმაციის გამოყენების,გამჟღავნების,შეფერხების,მოდიფიცირების,ჩაწერის ან განადგურების პრევენცია.

Whitman and Mattord (2009) საინფორმაციო უსაფრთხოებას განსაზღვრავენ, როგორც: „ინფორმაციისა და მისი კრიტიკული ელემენტების დაცვას,მათ შორის შედის სისტემები და აპარატურა,რომლებსაც იყენებენ და რომლებიც გადასცემენ ინფორმაციას“(Whitman and Mattord, 2009, p. 8).

სხვადასხვა წყაროები ხაზს უსვამენ ინფორმაციის სამ თვისებას, რომლებიცაა :

- ✓ კონფიდენციალობა - ინფორმაცია რომელიც ხელმისაწვდომია მხოლოდ უფლებამოსილი მხარეებისთვის.
- ✓ მთლიანობა-მონაცემთა არასანქცირებული მოდიფიკაციის თავიდან აცილება.
- ✓ ინფორმაციის ხელმისაწვდომობა-უფლებამოსილი მხარეების მიერ მოთხოვნის შემთხვევაში ინფორმაციის მიღების აუცილებლობა.

მაგრამ, Whitman and Mattord არ შემოიფარგლებიან მხოლოდ ამ სამი მახასიათებლით. ისინი მიუთითებენ, რომ უზრუნველყოს ინფორმაციის კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა, ინფორმაციულ უსაფრთხოებაში ცნობილია,როგორც CIA-ს სამკუთხედი (Central Intelligence Agency, CIA-ცენტრალური სადაზვერვო სააგენტო), იგი ტრადიციულად წარმოადგენდა ინდუსტრიის სტანდარტს.ამ სამი მახასიათებლის დაცვა ყოველთვის მნიშვნელოვანი იყო,თუმცა დღესდღეობის CIA-ს სამკუთხედის მოდელი კომპიუტერული ინდუსტრიის მუდმივ ცვალებად გარემოს ვეღარ შეესაბამება (Whitman and Mattord, 2009, p. 8).აქედან გამომდინარე ისინი ამატებენ ინფორმაციის სიზუსტეს,ნამდვილობას,სარგებლიანობას და ამ მახასიათებლების შემცველი ინფორმაცია უნდა იყოს დაცული.

ზემოაღნიშნულ განმარტებებში რამდენიმე კონცეფცია საჭიროებს უფრო ზუსტ გამოკვლევას.პირველ რიგში უნდა იყოს ნათელი,რომ ინფორმაციული უსაფრთხოება არ არის პროდუქტი ან ტექნოლოგია,იგი არის პროცესი(Mitnick and Simon,2002,p.4). ასევე,Wood-ის მიხედვით ინფორმაციული უსაფრთხოება მკაცრად ტექნიკური საკითხია.თუმცა, იქედან გამომდინარე, რომ კომპიუტერული ტექნიკა და ქსელები მუდმივად ცვალებადია,ინფორმაციის უსაფრთხოების უზრუნველყოფა კომპიუტერებსა და ქსელებში მასთან ერთად უნდა გაფართოვდეს და განვითარდეს.ამ პროცესმა შეიძლება მოითხოვოს გარკვეული პროდუქტების გამოყენება,თუმცა ის პროდუქტები რომელთა ყიდვაც შეუძლებელია, ისინი თითქმის მიუწვდომელია. ორგანიზაციები ქმნიან სპეციალურ ჯგუფებს ინფორმაციული უსაფრთხოების უზრუნველყოფისთვის,ისინი პასუხისმგებლები არიან რისკების მართვაზე, რომლის საშუალებითაც ხდება ინფორმაციული აქტივობების საფრთხეების შემცველობის შეფასება. ორგანიზაციის ღირებულება იმაში მდგომარეობს, რომ მისი ინფორმაცია დაცულია ბიზნეს ოპერაციებში, ეს უზრუნველყოფს როგორც სანდოობის შენარჩუნებას, ასევე კლიენტების ნდობის მოპოვება.

აშშ-ში საინფორმაციო უსაფრთხოების სტრატეგიის გლობალური მიზნებია:

- ✓ ქვეყნის კრიტიკული ინფრასტრუქტურების წინააღმდეგ კიბერნეტიკული შეტევების თავიდან აცილება.
- ✓ კიბერნეტიკული შეტევების წინააღმდეგ ქვეყნის დაცვის დონის ამაღლება.
- ✓ განხორციელებული კიბერნეტიკული შეტევების შემთხვევაში ზარალისა და შედეგების გამოსწორების დროის მინიმიზება.

საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ ძალაში შევიდა 2012 წელს. კანონმა შემოიტანა „კრიტიკული ინფორმაციული სისტემის სუბიექტის“ ცნება, რომელიც განისაზღვრა როგორც ორგანიზაცია, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის, ეკონომიკური და საზოგადოებრივი უსაფრთხოებისთვის. კანონშივე აღნიშნულია, რომ ის შესასრულებლად სავალდებულოა მხოლოდ კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის.საქართველოს კანონში ინფორმაციული უსაფრთხოება განმარტებულია როგორც: „ინფორმაციული უსაფრთხოება – საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას“.

საქართველოში საინფრმაციო უსაფრთხოების სტრატეგიის მიზნებია:

- ✓ ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას
- ✓ დააწესოს საჯარო და კერძო სექტორების უფლება-მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში
- ✓ განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები.

თუ შევადარებთ საქართველოსა და აშშ-ს ინფორმაციული უსაფრთხოების სტტარეგიის მიზნებს გამოიკვეთება ის საერთო მიზნები,რომელიც ამ ორ ქვეყანას გააჩნია მიუხედავად იმისა რომ ერთი უდიდესი და სუპერ განვითარებული სახელმწიფოა ხოლო მეორე პატარა და განვითარებადი.მიზნების არსი ორივე ქვეყნისათვის ერთი და იგივეა,უზრუნველყონ ზარალის შემცირება,კონტროლი და ა.შ. თუმცა, განსხვავებები უფრო მეტია ვიდრე საერთო,მაგრამ საბოლოოდ ინფორმაციული უსაფრთხოების მიზნებს, ერთი მთავარი მიზნისკენ მივყავართ და ეს არის ქვეყნის ინფორმაციული უსაფრთხოების უზრუნველყოფა.

2.1.რა არის კიბერუსაფრთხოება - არსი, ისტორიული მიმოხილვა და მიმართულებები

ასევე სანამ სიღრმისეულად გადავალთ კიბერუსაფრთხოების საკითხის შესწავლაზე უნდა მიმოვიხილოთ, თუ რა არის კიბერ სივრცე.

„კიბერ“- ბერძნული წარმოშობის ზმნაა -“kybereo” ნიშნავს -მართვას, გაძღოლას, გაკონტროლებას. 1940 წლიდან ამერიკელმა მათემატიკოსმა Norbert Wiener-მა(1894-1964) დაიწყო ამ სიტყვის გამოყენება, რათა დაეხასიათებინა კომპიუტერული სისტემა.

უნდა აღინიშნოს რომ კიბერ სივრცეს ერთი კონკრეტული განმარტება არ აქვს.სიტყვა "კიბერ სივრცე" მიანიჭა უილიამ გიბსონმა, რომელმაც გამოიყენა თავის წიგნში „Neuromancer“,1984 წელს.

კიბერ სივრცე არის გარემო სადაც ხდება კომპიუტერული ქსელების კომუნიკაცია,ეს სიტყვა პოპულარული გახდა 1990 წლიდან.იგი ასოცირდება კომპიუტერთან და ინტერნეტის სხვადასხვა კულტურებთან.

Chip Morningstar and F. Randall Farmer-ის თანახმად, კიბერსივრცეში ძირითადად განსაზღვრულია სოციალური ურთიერთქმედება,ვიდრე მისი ტექნიკური

განხორციელება.კიბერსივრცის ძირითადი მახასიათებელი ის არის, რომ ის სთავაზობს გარემოს, რომელიც შედგება მრავალი მონაწილეებისგან, რომლებიც გავლენას ახდენენ ერთმანეთზე და ასევე ექცევიან გავლენის ქვეშ.

ზოგჯერ ინფორმაციულ უსაფრთხოებასა და კიბერ უსაფრთხოებას აიგივებენ და თვლიან რომ ეს ორი ცნება ანალოგიურია,თუმცა თავიდანვე უნდა აღინიშნოს რომ მიუხედავად იმისა რომ ეს ორი ცნება რაღაც მხრივ ფარავს ერთმანეთს,კიბერ უსაფრთხოება სცდება თავად ინფორმაციული უსაფრთხოების საზღვრებს,იგი მოიცავს არა მხოლოდ საინფორმაციო რესურსების დაცვას არამედ სხვა აქტივობებსაც,როგორც ზემოთ აღინიშნა,რიგ შემთხვევებში ინფორმაციულ უსაფრთხოებასა და კიბერ უსაფრთხოებას ურთიერთ ჩანაცვლებად ტერმინებად იყენებენ.თუ ამ ორ ტერმინს ჩავთვლით სინონიმებად,მაშინ კიბერ უსაფრთხოების დასახასიათებლად დასაშვები იქნება თუ გამოვიყენებთ ინფორმაციული უსაფრთხოებისათვის განსაზღვრულ მახასიათებლებს.ამდენად,კიბერ შემთხვევის მაგალითი შეიძლება იყოს ინფორმაციის კონფიდენციალობის,მთლიანობის ან ხელმისაწვდომობის დარღვევა. კიბერ უსაფრთხოების უმრავლესობა დაკავშირებული შეიძლება იყოს მომხმარებელის ან / და ორგანიზაციის საფრთხეებთან.

რაც შეეხება, კონკრეტულად კიბერ უსაფრთხოების განმარტებებს, Merriam Webster-ის ლექსიკონში კიბერუსაფრთხოება განსაზღვრულია, როგორც „ღონისძიებები,რომელიც იცავს კომპიუტერს ან კომპიუტერულ სისტემას არასანქცირებული წვდომისა და თავდასხმისაგან“.

International telecommunications union(ITU) - განსაზღვრავს კიბერ უსაფრთხოებას, შემდეგნაირად: „კიბერუსაფრთხოება არის ერთობლიობა ინსტრუმენტების, პოლიტიკის, უსაფრთხოების კონცეფციის ,რისკის მართვის,ტექნოლოგები და გარანტიები,რომლებიც გამოყენებული იქნება დაიცვა კიბერ გარემო და ორგანიზაციები და ასევე მომხმარებლის აქტივობები. ორგანიზაცია და მომხმარებლის აქტივობები მოიცავს კომპიუტერულ მოწყობილობებს, პირადი, მომსახურება, სატელეკომუნიკაციო სისტემები და ყოველივე ეს ინახება კიბერ გარემოში“.

კიბერუსაფრთხოება მიზნად ისახავს ორგანიზაციის უსაფრთხოების მიღწევას და მისი შენარჩუნების უზრუნველყოფას,ასევე მომხმარებლების აქტივობების შესაბამის დაცვას რისკებისგან.

საჯარო სამსახურები დღითი დღე სულ უფრო მეტად ხდებიან დამოკიდებული ტექნოლოგიების საშუალებით ინფორმაციისა და კომუნიკაციის გამოყენებაზე(ICT-Information and communications technology). რაც უფრო დამოკიდებულნი ვხდებით ICT-

ზე,მით ღრმაა კავშირი კიბერ უსაფრთხოებასთან. ამ მიზეზებიდან გამომდინარე კიბერ უსაფრთხოება წარმოადგენს თანამედროვე სამყაროს ნამდვილ გამოწვევას, რომელთან გამკლავებაც, მხოლოდ სამართალმცოდნეების, უსაფრთხოების ექსპერტებისა და საზოგადოების აქტიური მონაწილეობით არის შესაძლებელი.

კიბერუსაფრთხოება ეროვნული უსაფრთხოების შემადგენელ კომპონენტად და ქვეყნისათვის მეტად მნიშვნელოვან პრიორიტეტად იქცა,ვინაიდან და რადგანაც 50-ზე მეტმა ქვეყანამ ოფიციალურად გამოაქვეყნა დოკუმენტი, რომელიც გარკვეული ფორმით ასახავს მათ ოფიციალურ პოზიციას კიბერივრცეზე, კიბერ დანაშაულზე და/ან კიბერუსაფრთხოებაზე(Klimburg,2012). კიბერუსაფრთხოების უზრუნველოფა რთული ამოცანაა, რომელიც ეყრდნობა დომენურ ცოდნას და მოითხოვს შემეცნებით შესაძლებლობებს,რათა დადგინდეს შესაძლო საფრთხეები დიდი რაოდენობის ქსელური მონაცემებისგან.

2014 წლის სექტემბერში უელსის სამიტზე კიბერუსაფრთხოება ერთ-ერთ მნიშვნელოვან პრიორიტეტად დასახელდა:“ჩვენ ვთანხმდებით,რომ კიბერშეტევებმა შესაძლოა საფრთხის წინაშე დააყენონ ჩვენი ქვეყნების უსაფრთხოება,სტაბილურობა და განვითარება.მათ შეუძლიათ ზიანი მიაყენონ თანამედროვე საზოგადოებას.ამგვარად,ვაცხადებთ,რომ კიბერ თავდაცვა ნატოს ერთიანი თავდაცვის განუყოფელი ნაწილია“-აცხადება ნატოს ყოფილი გენერალური მდივანი, ანდერს ფოგრასმუსენი ნატოს უელსის სამიტზე. (International Business Times, The Three Cyber-Security Challenges Facing Nato, Jarno Limnell, August 13, 2014, Brussels).

2.2.კიბერ დანაშაული და მისი ტიპოლოგია

1969 წელს, ამერიკის თავდაცვის დეპარტამენტმა შექმნა ქსელი ARPANET (Advanced Research Projects Agency Network). თუ თავიდან მხოლოდ 40 კომპიუტერი იყო გამოყენებული ამ ქსელისათვის, 1981 წლისთვის, 200-ზე მეტი კომპიუტერი იყო დაკავშირებული მთელი მსოფლიოს მასშტაბით, ხოლო თუ 2000 წელს ინტერნეტის მომხმარებელთა რაოდენიმა 300 მილიონი იყო 2011 წლის 31 დეკემბრის მონაცემებით ეს რაოდენობა 3 მილიარდს აღწევს.მსოფლიოში ინტერნეტის და კომპიუტერული სისტემების განვითარებასთან ერთად განვითარდა და გამრავალფეროვანდა კომპიუტერული დანაშაული, რომელსაც კიბერ დანაშაული ეწოდება, მას ხშირად 21-ე საუკუნის კრიმინალურ ფორმასაც კი უწოდებენ. იგი ყურადღების ცენტრში თავდაპირველად XX საუკუნის 70-იან წლებში მოექცა.

არ არსებობს კიბერ დანაშაულის ერთი კონკრეტული განმარტება, თუმცა კიბერდანაშაული გულისხმობს ყველა იმ ქმედებას, რომელიც ხორციელდება კიბერსივრცეში

დანაშაულებრივი განზრახვით. ისინი შეიძლება განხორციელდეს, როგორც კონვენციური ისე ახალი საშუალებებით. ინტერნეტის ანონიმური ბუნების საშუალებით, შესაძლებელი მრავალი დანაშაულებრივი ქმედების განხორციელება ყოველგვარი სასჯელის გარეშე, ხოლო შესაბამისი ცოდნის მქონე მხარეები, არაკეთილსინდისიერად იყენებენ მას კიბერსივრცეში დანაშაულებრივი მიზნებისათვის. ეს ქმედებები კი ყოველდღიურად იცვლება და ვითარდება.

კიბერ დამნაშავეები შეიძლება დავყოთ სამ ძირითად ჯგუფად. ესენი არიან:

- ✓ ჰობისტები- ანუ ჰაქტივისტები, როგორებიც არიან დაჯგუფება Anonymous და LulzSec. ისინი არ ცდილობენ თანხის მოპარვას, ისინი ცდილობენ პოლიტიკური მესიჯის მიწოდებას.
- ✓ ორგანიზებული კრიმინალური დამნაშავეები - რომლებიც ყველა საზიანო ქმედებას გარკვეული თანხის მიღების გამო აკეთებენ.
- ✓ კიბერ ჯაშუშები - ადამიანები, რომლებიც ცდილობენ კიბერ საბოტაჟის მოწყობას, როგორც ეს მოხდა 2010 წელს ირანის და 2007 წელს კი ესტონეთის შემთხვევაში ან კიბერ ომის წამოწყებას, რომელიც განხორციელდა 2008 წელს რუსეთის მიერ საქართველოს წინააღმდეგ.

კიბერ დანაშაული ძირითადად დაყოფილია სამ ჯგუფად:

- ✓ პიროვნების წინააღმდეგ მიმართული კიბერ დანაშაული

პიროვნების წინააღმდეგ ჩადენილი კიბერ დანაშაული მოიცავს სხვადასხვა დანაშაულებს, როგორიცაა ბავშვთა პორნოგრაფიის გამოქვეყნება, კიბერ პორნოგრაფია,ფიზიკური პირის შევიწროვება კომპიუტერის გამოყენებით, ტრეფიკინგი, უცენზურო მასალი განაწილება, გამოქვეყნება და გავრცელება, მათ შორის პორნოგრაფიისა და უხამსი ექსპოზიციის შესახებ, წარმოადგენს ერთ-ერთ ყველაზე მნიშვნელოვან კიბერ დანაშაულებს.კიბერ-შევიწროება არის განსხვავებული კიბერ დანაშაული. სხვადასხვა სახის შევიწროვება შეიძლება მოხდეს კიბერსივრცეში, ან კიბერსივრცის გამოყენების საშუალებით,იგი შეიძლება იყოს სექსუალური, რასობრივი, რელიგიური ან სხვა.

პიროვნების წინააღმდეგ მიმართული კიბერ დანაშაულებებია:შეურაცხყოფა ელექტრონული ფოსტით,ცილისწამება,ჰაკინგი,ქსელის გატეხვა,თაღლითობა,ბავშვთა პორნოგრაფია,საფრთხის შემცველი მოქმედებები.

- ✓ საკუთრების წინააღმდეგ მიმართული კიბერ დანაშაული

კიბერ დანაშაულის მეორე კატეგორია არის საკუთრების წინააღმდეგ მიმართულ დანაშაულს წარმოადგენს,რომელიც მოიცავს სხვისი ქონების განადგურება(კომპიუტერის ვანდალიზმი),მავნე ვირუსების ან პროგრამების გამოყენება ვინმეს ქონების გასანადგურებლად,ინტელექტუალური საკუთრების დანაშაული, კომპიუტერული სისტემის ჰაკინგი, ვირუსების გავრცელება,კიბერ გადაკვეთა ანუ საკუთრების ხელყოფა,ინტერნეტ ქურდობა.

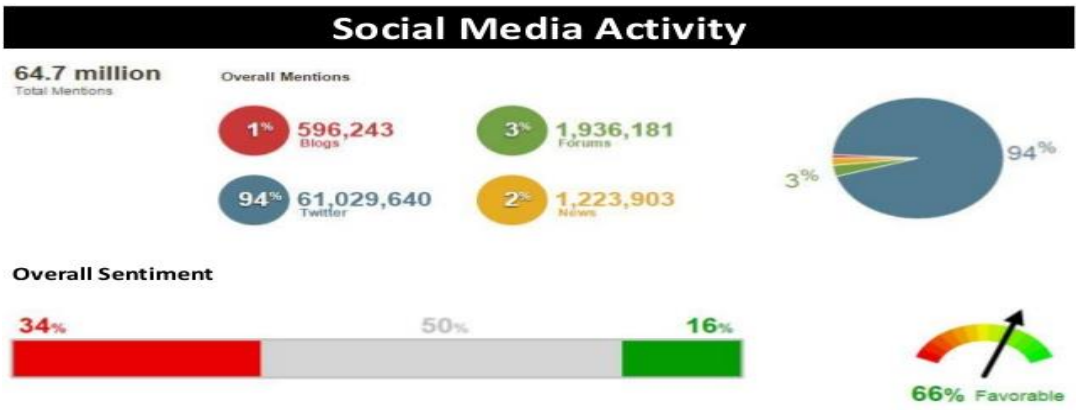
- ✓ სახელმწიფოს წინააღმდეგ მიმართული კიბერ დანაშაული

კიბერ-დანაშაულის მესამე კატეგორია მთავრობასთან დაკავშირებით კიბერ დანაშაულებსაც ეხება.კიბერ ტერორიზმი სწორედ ამ კატეგორიაში შედის,ვინაიდან იგი მიმართულია მთავრობისა და სახელმწიფოს წინააღმდეგ.კიბერ სივცრის ზრდამ გვიჩვენა რომ პიროვნებები თუ დაჯგუფებების საშუალო რაოდენობა საფრთხეს უქმნის მთავრობებს,სახელმწიფოებს თუ ქვეყნის მოქალაქეებს.

როდესაც კიბერ დანაშაულზე ვსაუბრობთ,შეუძლებელია არ შევეხოთ ისეთ აქტუალურ თემას, როგორიც ტერორიზმია. ამ პროცესის ხელშემწყობი ფაქტორია გლობალიზაცია, რომელიც ხელს უწყობს კრიმინალური აქტივობების ზრდას. „უმართავი სივრცეები“ ,რომლებიც ცივი ომის შემდეგ წარმოიშვა, ათვისებულ იქნა ტერორისტებისა და კრიმინალების მიერ, როგორც მათი თავშესაფარი.ტერორიზმის საერთაშორისოდ აღიარებული დეფინიცია 2001წლის 11 სექტემბრამდე არ არსებობდა,თუმცა საბოლოო სახით იგი დღესაც არ არსებობს.დღევანდელი განმარტებით ტერორიზმი არის- „ძალადობის გამოყენება შიშისა და ტერორის კლიმატის შექმნის მიზნით და დასახული პოლიტიკური მიზნების მისაღწევად“(Civil ენციკლოპედიური ლექსიკონი).მიუხედავად ტერორისტული აქტის ჩადენის ტრადიციული მეთოდებისა, კიბერსივრცის განვითარებასთან ერთად ტერორისტების ყურადღება აქტიურად გადმოერთვება კიბერსივრცეში რაც მას ნამდვილ ბრძოლის ველად აქცევს. აღნიშნული კი გლობალურ კრიტიკულ ინფრასტრუქტურას, როგორიცაა მილსადენები, ელექტრო სადგურები, ტრანსპორტი, საკომუნიკაციო სისტემები, საფრთხის წინაშე ჩააგდებს. ამის ნათელი მაგალითი იყო 2010 წელს აღმოჩენილი კომპიუტერული ჭია Stuxnet. ინფორმაციული უსართხოების ექსპერტების განცხადებით, StuxneT იყო პირველი კომპიუტერული ჭია რომელიც აკვირდებოდა ირანის ატომურ ინფრასტრუქტურას, თავისით სწავლობდა მისი გაკონტროლების ხერხებს და კონფიგურაციის შემთხვევაში შეეძლო სხვა კრიტიკული ინფრასტრუქტურების მართვაც. ეს კომპიუტერული ჭია მთელი მსოფლიოს მასშტაბით იყო გავრცელებული და დიდი პოპულარობით სარგებლობდა შავ ბაზარზე, რა დროსაც მოხდა კიბერსივრცეში მისი სხვადასხვა ვარიანტების გავრცელება. აღნიშნულის გამო მისი შემქმნელების დადგენა ფაქტიურად შეუძლებელი გახდა. საინტერესო ის ფაქტი, რომ მისი

აქტივობის ძირითად ზონებს წარმოადგენდნენ ირანი, ინდონეზია, ინდოეთი და პაკისტანი.

„ისლამური სახალიფო - დაეში(ISIS)“, ისევე, როგორც „ალ-კაიდა“ წარმოადგენს ტერორისტულ ორგანიზაციებს, რომლებიც ახლო აღმოსავლეთში ერთიანი ისლამური სახალიფოს შექმნის იდეებით არიან შთაგონებულნი. ძველებურ, ტრადიციულ ხერხებს ტერორიზმისთვის უკვე დიდი ხანია აღარ იყენებენ, 2010 წლიდან ისინი აქტიურად ჩაერთვნენ სოციალურ ქსელებში. ტერორისტები აქტიურად იყენებენ სოციალურ ქსელებს,როგორიცაა Facebook,Twiter,თუმცა ყველაზე გამოყენებადი არის Youtube,სადაც ტერორისტები საკუთარ გვერდს ქმნიან და ამ გვერდს შემდეგ ტერორისტული მიმართვებისათვის იყენებენ და ავრცელებენ ვიდეოებს მხარდემჭერების მოსაპოვებლად. ამის ერთ-ერთი მაგალითია ამერიკელი ჟურნალისტის მკვლელობის ვიდეო,რომელიც გავრცელდა მას შემდეგ რაც ბარაკ ობამამ ისლამსტურ სახელმწიფოს ოფიციალურად გამოუცხადა ომი.



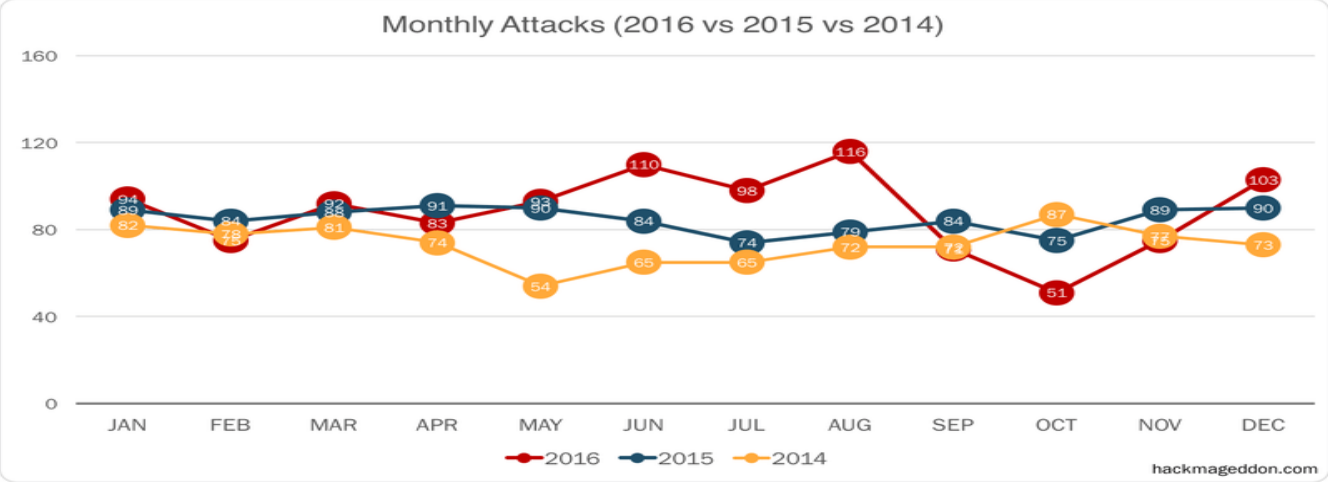
*https://www.slideshare.net/vikashnsingh/isis-50885565

2015-წლის სტატისტიკაში მოცემულია ISIS-ის სოციალური მედიის ანალიზი,სადაც კარგად ჩანს,თუ რომელ ქსელში არიან ისინი ყველაზე მეტად აქტიურები. ეს არის სოციალური მედიის მონიტორინგისა და ანალიზის ანგარიში და არა სადაზვერვო ანგარიში.ანალიზის ანგარიშის შესაქმნელად გამოყენებულია Twitter-ი, ახალი ამბები, News, ფორუმები და ვიდეო საუბრების ბოლო ერთი წლის ისტორიული მონაცემები.

დღევანდელი მდგომარეობით „ისლამურ სახელმწიფოში“ დაახლოებით 12-150000-მდე უცხოური ბოევიკი მოქმედებს, ხოლო ამ რიცხვიდან 100-ზე მეტი არის ამერიკის შეერთებული შტატების მოქალაქე და ეს რიცხვი დღეთი დღე იზრდება.

კიბერ დანაშაულს უდიდესი გავლენა აქვს მსოფლიოზე, რომელშიც ჩვენ ვცხოვრობთ, გავლენას ახდენს ყველა პიროვნებაზე, ორგანიზაციაზე, დაჯგუფებაზე, ოჯახზე, სახელმწიფოზე თუ სხვა. კიბერ დანაშაული ზემოქმედებს დაწყებული იმ უმცირესიდან როგორიცაა-პიროვნება და დამთავრებული იმ უდიდესით, როგორიცაა -მსოფლიო.

Hackmageddon.com-ის მიერ მოწოდებული სამ წლიანი(2014-დან 2016-ის ჩათვლით) ყოველთვიური თავდასხმის გრაფიკი გვიჩვენებს, რომ პირველი დონე 5 თვის განმავლობაში სამივე წელს მსგავსი იყო. 2015 წლის სექტემბრიდან დაიწყეს უფრო თანმიმდევრული აქტივობა, სულ ცოტა დეკემბრამდე, ხოლო 2016 წლიდან ცენტრალურ თვეში კიბერ შეტევების მწვერვალი იყო.



კომპანია „Pierre Audoin Consultants-ის“ 2016წლის კვლევების თანახმად, დანაშაულის 30% კი პერსონალურ ინფორმაციასთან უკანონო წვდომის მოსაპოვებლად არის ჩადენილი . მონაცემების მიხედვით, კიბერდანაშაულის რიცხვის ზრდით ყველაზე მეტად ბიზნესმენები არიან შეშფოთებული და მათი 57% უსაფრთხოების სერვისებს მაქსიმალურად იყენებს.

ამერიკის შეერთებულ შტატებში, 1977 წელს შეიმუშავეს ” ფედერალური კომპიუტერული სისტემების დაცვის შესახებ” კანონპროექტი, რომელიც ითვალისწინებდა სისხლის სამართლებრივ პასუხისმგებლობას კიბერდანაშაულის წინააღმდეგ. კომპიუტერული დანაშაულისაგან მიყენებული ყოველწლიური ზარალი ევროპაში და ამერიკაში შეადგენს რამდენიმე ათეულ მილიარდ დოლარს.
რაც შეეხება საქართველოს, შინაგან საქმეთა სამინისტროს ცნობით: "2011 წლის მარტიდან შინაგან საქმეთა სამინისტრო ჩართულია აღმოსავლეთ პარტნიორობის ეგიდით მიმდინარე პროექტში „თანამშრომლობა კიბერ დანაშაულის წინააღმდეგ“.აღნიშნული პროექტის მიზანია ქართული სამართალდამცავი უწყებების შესაძლებლობების განვითარება კიბერდანაშაულთან ბრძოლის პროცესში“.

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

2.3. კიბერ თავდაცვა და მისი ელემენტები

21-ე საუკუნე ვირტუალური სამყაროს ეპოქაა, რომელიც ჩვენი ცხოვრების განუყოფელი ნაწილია,იგი თავის მხრივ კი ქმნის კიბერ სივრცეს. სახელმწიფოებისთვის უმნიშვნელოვანესია ძლიერი კიბერ სივრცის არსებობა ვინაიდან, მის გარეშე ისინი გარე სამყაროსგან დაუცველები იქნებოდნენ. კიბერ შეტევის განხორციელება მსგავს სახელმწიფოზე მარტივია და მისი განადგურება.კიბერსივრცე და მასთან დაკავშირებული საკითხები არც ისე ახალია თანამედროვეობისთვის.

თანდათან სულ უფრო მტკიცდება, რომ სივრცეზე დაფუძნებული სისტემები არის ძირითადი ხელსაწყოები საერთაშორისო და ეროვნული ურთიერთობებისთვის. შესაბამისად გარე სამყარო სულ უფრო ზრდის კონკურენტობას, კამათსა და დავებს ერთმანეთში. სივრცეზე დაფუძნებული ინფრასტრუქტურა უზრუნველყოფს გლობალური პოზიციონირების, ნავიგაციისა და დროების მონაცემებს. ასევე უზრუნველყოფს გლობალურ საფინანსო ოპერაციებისა და ვაჭრობის სიზუსტეს და ეფექტურობას.

რადგან სივრცეზე დაფუძნებული ინფრასტრუქტურის დამოკიდებულება იზრდება ტექნოლოგიის წინსვლა ბოლო ორი ათწლეულის განმავლობაში მნიშვნელოვნად გაზრდის სივრცის ხელმისაწვდომობის შესაძლებლობას. შედეგად აქტორების ზრდა სივრცეში ცვლის გეოსტრატეგიის ორბიტის სამ პრინციპს.მათი უწყვეტი ნაკადი შეიძლება ითქვას, რომ ამ ორბიტის გადავსებას და დაბინძურებას იწვევს. ახალი აქტორები ცვლიან გეორტრატეგიულ სივრცეს და ყალიბდება ახალი პოლიტიკა 21-ე საუკუნეში.

აქამდე არაერთხელ აღვნიშნეთ,რომ ამერიკა არის მსოფლიოს წამყვანი ქვეყანა სივრცეში, მას თან მისდევს რუსეთის, რომელიც ცდილობს, რომ არაფრით ჩამორჩეს. რაც შეეხება სხვა ქვეყნებს, ფაქტიურად საკმაოდ წარმატებით მიიწევს წინ ჩინეთი, რომელმაც შეიმუშავა მრავალმხრივი სივცრის პროგრამები და მუშაობს შესაძლებლობების გაძლიერებაზე (Robison,2014).

სივრცის აქტივების დაცვა და უსაფრთხოება სასიცოცხლო მნიშვნელობისაა EU-სთვის. მრავალმხრივ დონეზე, EU ცდილობს დაიცვას სივრცეში უსაფრთხოება, საერთაშორისო მოლაპარაკებების გზით(Robinson,2014). 2016 წლის გლობალური სტრატეგია ადასტურებს EU-ს ვალდებულებას, გააძლიეროს მისი სივრცეზე დაფუძნებული სერვისების უსაფრთხოება და ყურადღება გაამახვილოს საპასუხისმგებლო ქცევის პრინციპების

ჩამოყალიბებაზე. უფრო მეტიც, ახლახან ევროპულმა კომისიამ მიიღო ყოველმხრივი სივრცის სტრატეგია ევროპისთვის.

კიბერ თავდაცვაა, როდესაც სახელმწიფოები უზრუნველყოფენ კიბერ უსაფრთხოებას, ხდება კიბერ შეტევების კონტროლი, მისი აღმოჩენა და აღმოფხვრა. თითოეული ქვეყანა ცდილობს, რომ შექმნას მაქსიმალურად ძლიერი კიბერ თავდაცვა, ვინაიდან სწორედ ამაზეა დამოკიდებული მათი მომავალი ურთიერთობები, მათი რეპუტაცია, სამომავლო კავშირები, ეკონომიკა და ქვეყნის ბედი.

კიბერ თავდასხმები გახდა სულ უფრო კომპლექსური და რთული, ორგანიზაციისა და მოწინააღმდეგის მოტივაციის გამო. თანამედროვე თავდასხმები სერიოზულ საფრთხეს უქმნის ეკონომიკასა და ეროვნულ უსაფრთხოებას.კიბერ დანაშაულისგან თავდაცვა ყველა სახელმწიფოს ესაჭიროება, განურჩევლად იმისა სუპერ სახელმწიფოა თუ განვითარებადი. აქედან გამომდინარე ყოველი ქვეყანა ცდილობს, რომ ჰქონდეს მაქსიმალურად განვითარებული და უმაღლესი დონის კიბერ თავდაცვა. ობიექტური რეალობაა, რომ კიბერსივრცეში საიმედო დაცვის შექმნა უკიდურესად რთული ამოცანაა, მასშტაბური კიბერშეტევის თავიდან აცილება და ადექვატური პასუხი კი თითქმის შეუძლებელი; სახელმწიფოები ცდილობენ აქცენტი შემტევ ოპერაციებზე გააკეთონ, რათა ეფექტურად გამოიყენონ კიბერსივრცე მიზნების მისაღწევად.

კიბერ თავდაცვა შეიძება იყოს ორი სახის, ესენია:

- ✓ პასიური თავდაცვა არის აუცილებელი კომპონენტი კარგად დამუშავებული კიბერ თავდაცვის სტრატეგიაში, მაგრამ უკვე აღარ არის საკმარისი დღესდღეობის არსებული რთული და დახვეწილი საფრთხეების გადაწყვეტისთვის.
- ✓ აქტიური კიბერთავდაცვა აღწერს პროაქტიული რეაქციების სპექტრს თავდასხმის დაწყებამდე ან მის დროს,რომელიც მკვეთრად გაუმჯობესებს პრევენციას,გამოვლენას, და რეაგირება ამ რთულ თავდასხმებზე. შედეგად, აქტიური კიბერ-თავდაცვა იზრდება.

ეფექტური და დაბალანსებული კიბერ თავდაცვა უნდა იყოს: უსაფრთხო, ყოველთვის მზადყოფნაში და ელასტიური.

- ✓ უსაფრთხო-ფოკუსირება უნდა მოხდეს ისეთი საკითხების და ქმედებების დაცვაზე,რომლებით უმნიშვნელოვანესი და ძირითადია და ასევე იგი ღირებული უნდა იყოს მოწინააღმდეგე მხარისთვისაც და მისი ოპონენტისთვის.

- ✓ ყოველთვის მზადყოფნაში-ნიშნავს იმას რომ ყოველთვის მზად უნდა იყოს ნებისმიერი კიბერ შეტევის მოგერიებისთვის, ასევე მისი მოგვარებისთვის და ჰქონდეს მუდივი პრაქტიკა კრიტიკული აქტივების, კიბერ შეტევების აღმოჩენისა და წინასწარი პროგნოზისთვის.

- ✓ ელასტიური-შესაძლებელი უნდა იყოს სწრაფად რეაგირება და მოგვარება კიბერ შეტევების, ასევე ნებისმიერი სახის ზარალის მინიმუმამდე დაყვანა, როგორიცაა ეკონომიკური, ასევე რეპუტაცია და სხვა.

მიუხედავად იმისა,რომ ქვეყნები ცდილობენ მაქსიმალურად მაღალი დონის კიბერთავდაცვის შექმნას ჯერ ჯეროვნად ეს ვერცერთმა სახელმწიფომ ვერ მოახერხა, მათ შორის ამერიკამაც კიმისი ჩამოყალიბება, ამის ნათელი მაგალითია არჩევნების დროს დემოკრატიული პარტიის დაჰაკვის მცდელობა, რომელსაც დეტალურად შემდეგ თავში განვიხილავთ. ამას ადასტურებს CIA- ს ამჟამინდელი დირექტორი მაიკ პომპე, რომელიც ოფიციალურად აცხადებს, რომ აშშ-ს მთავრობას არ გააჩნია კიბერ დაცვის პოლიტიკა. ასე რომ, პირველი ნაბიჯი იქნებოდა ადეკვატური პოლიტიკის შემუშავება, რომელიც ეფუძნებოდა კრიტიკული ინფრასტრუქტურის დახვეწილ რისკებზე და მისი ოპონენტების კიბერ შესაძლებლობების კვლევას. უფრო მეტიც, კიბერ-თავდაცვითი შესაძლებლობებისა და კლასიკური კონტრდაზვერვის ოპერაციებთან ერთად კიბერუსაფრთხოების გაერთიანება, ვიდრე ცალკე დომენზე. კიბერთავდაცვა საერთო პასუხისმგებლობაა. შესაბამისად, არასამთავრობო ორგანიზაციებთან ურთიერთობა თავდაცვის სამინისტროსთვის და კიბერუსაფრთხოების ბიუროსთვის მეტად საინტერესო და საჭირო საკითხია. სამწუხაროდ, ამ სფეროში არ არის ფართო სპექტრი. აქ აუცილებლად უნდა იყოს ჩართული როგორც სახელმწიფო სექტორი, ისე არასამთავრობო და კერძო სექტორი. მნიშვნელოვანია თითოეული მოქალაქის, აკადემიური სფეროს წარმომადგენლების და ამ სფეროს ექსპერტების ჩართულობაც.

რა თქმა უნდა, ამ შემთხვევაში ყურადსაღებია საქართველოს კიბერ თავდაცვა. საქართველო, რომელიც ჯერ კიდევ ახლა იწყებს განვითარებას კიბერ უსაფრთხოების სფეროში, მხოლოდ მას შემდეგ დაიწყო კიბერ უსაფრთხოებაზე და კიბერ თავდაცვაზე ზრუნვა, რაც უდიდესი შეტევა საკუთარ თავზე გამოსცადა(2008წლის კიბერ შეტევა,დეტალურად განვიხილავთ სხვა ქვეთავში), სამწუხაროდ მას არ გააჩნია განვითარებული და კარგად აღჭურვილი კიბერ თავდაცვა,რამაც დაგვარწმუნა ვირუს „პეტია-ს“ შემოტევამ (განვიხილავთ ცალკე ქვეთავში).

იმის გათვალისწინებით, რომ ნატოსთვის კიბერუსაფრთხოება ერთ-ერთი მნიშვნელოვანი პრიორიტეტია და შესაბამისად, განსაკუთრებულ აქცენტირებას ახდენს კიბერშესაძლებლობების განვითარებაზე, ალიანსის წევრობის მსურველი ყველა ქვეყანა და მათ შორის საქართველოც, უნდა აცნობიერებდეს, რომ ერთობლივი საიმედო კიბერუსაფრთხოების საწყისი, სწორედ საკუთარი ქვეყნის კიბერთავდაცვაა.

3.საქართველოს კიბერუსაფრთხოების გარემო და მისი ანალიზი

დღესდღეობით საქართველოში, სულ მცირე, 1 მილიონზე მეტი ადამიანი სარგებლობს ინტერნეტით, თუმცა, ჯერ კიდევ არსებობს პრობლემა ინტერნეტის წვდომასთან დაკავშირებით საქართველოს სოფლებში. საქართველოს ეროვნული უშიშროების საბჭო (NSC) წარმოადგენს საქართველოს მთავარ საკონსულტაციო ორგანოს.

ეროვნული უშიშროების საბჭოს ერთ-ერთი პასუხისმგებლობა ქვეყნის უსაფრთხოების პოლიტიკის განსაზღვრაა, მათ შორის ინფორმაციული უსაფრთხოება და კიბერ უსაფრთხოება. ის არის ავტორი საქართველოს უსაფრთხოების კონცეფციის და ასევე მუშაობს ქვეყნის კიბერ უსაფრთხოების კონცეფციაზე.

დღესდღეობით, საქართველოს ინფორმაციული უსაფრთხოების გარემო განვითარების სტადიაზეა. მიმდინარეობს სხვადასხვა კანონების შემუშავება ევროკავშირის რეგულაციებთან და სტანდარტებთან შესაბამისად.

2010 წელს დაიწყო კიბერუსაფრთხოების სფეროს ეტაპობრივი განვითარება.ჩამოყალიბდა საქართველოს იუსტიციის მმართველობაში შემავალი სსიპ.-მონაცემთა გაცვლის სააგენტო,ხოლო შენდეგ უკანასკნელის დაქვემდებარებაში-კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი.

2012 წელს შეიქმნა კიბერდანაშაულთან ბრძოლის ცენტრალური სამმართველო,ხოლო 2014 წელს კიბერუსაფრთხოების ბიურო.

1. საქართველოს იუსტიციის მმართველობა
2. მონაცემთა გაცვლის სააგენტო
3. კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი

2013-2016წელს საქართველოს თავდაცვის სამინისტრომ შეიმუშავა კიბერუსაფრთხოების პოლიტიკა.

„კიბერუსაფრთხოების პოლიტიკა-განმარტავს საქართველოს თავდაცვის სფეროს მიდგომებსა და პრიორიტეტებს კიბერუსაფრთხოების მიმართულებით და განსაზღვრავს

ყველა იმ სტრატეგიულ მიზანს, რომელთა აღსრულებაც განაპირობებს თავდაცვის სფეროს საიმედო, ეფექტურ, სტაბილურ და უსაფრთხო ფუნქციონირებას, რაც თავისთავად ქმნის ეროვნული უსაფრთხოების მყარ საფუძვლებს"-თავდაცვის სამინისტრო.

“ საქართველოს ხელისუფლება პირველად აქვეყნებს საქართველოს კიბერუსაფრთხოების სტრატეგიას. 2008 წლის აგვისტოში რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად აჩვენა, რომ საქართველოს ეროვნული უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე.
საქართველოს კიბერუსაფრთხოების სტრატეგია კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტია, რომელიც ეროვნულ უშიშროების საბჭოსთან არსებული ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტების შემუშავების მაკოორდინირებული მუდმივმოქმედი საუწყებათშორისი კომისიის მიერ შემუშავდა”, – ნათქვამია დოკუმენტში.

ამ დოკუმენტის მიხედვით,კიბერუსაფრთხოების პოლიტიკის პირველი პრიორიტეტული ამოცანებია:

- ✓ განსაზღვროს კიბერსივრცის უსაფრთხოების უზრუნველყოფასთან დაკავშირებული სტრატეგია.
- ✓ საქართველოს შეიარაღებული ძალების ინფორმაციული სისტემების დაცვა პოტენციური კიბერშეტევებისგან, დაზვერვის და რადიო-ელექტრონული ბრძოლის ხერხების და საშუალებების, ფსიქოლოგიური ოპერაციების აქტიური წინააღმდეგობის საშუალებებისა და მეთოდების განვითარება.
- ✓ უსაფრთხო და ადეკვატური ინფორმაციული გარემოს შექმნა, რაც სტაბილური ფუნქციონირებისა და მოქმედების საწინდარია.

2017-2018წლებში საქართველომ მეორედ გამოაქვეყნა კიბერუსაფრთხოების სტრატეგია.

ამ დოკუმენტით საქართველოს კიბერუსაფრთხოების ეროვნული სტრატეგია განსაზღვრავს: „სახელმწიფო პოლიტიკის ძირითად მიზნებს,ძირითად პრინციპებს,აყალიბებს ამოცანებს და მათ შესასრულებლად განსაზღვრავს შესაბამის აქტივობებს“.

საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიზნებია:

- ✓ შეიქმნას უსაფრთხო კიბერსისტემა თავდაცვის სფეროში, მოხდეს ნდობის გენერირება ინფორმაციული ტექნოლოგიების სფეროში, შესაბამისად, გაძლიერდეს ინფრასტრუქტურული შესაძლებლობები თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის.

- ✓ შექმნას და განავითაროს კიბერუსაფრთხოების ისეთი სისტემა,რომელიც ხელს შეუწყობს ინფორმაციული ინფრასტრუქტურის დაცულობას კიბერსაფრთხეების წინაშე და იქნება დამატებითი ფაქტორი ქვეყნის შემდგომი ეკონომიკური და სოციალური განვითარებისთვის.
- ✓ დაინერგოს და განვითარდეს ინფორმაციული ტექნოლოგიების უსაფრთხოების ინციდენტებზე რეაგირების 24/7 მექანიზმები, რომლებიც უზრუნველყოფენ ინფორმაციული და კომუნიკაციების ტექნოლოგიების ინფრასტრუქტურის დაცვას, მოახდენენ საფრთხეებისა და რისკების სწრაფ იდენტიფიცირებას, მათზე რეაგირებას, პრევენციული ზომების გატარებას და საჭიროების შემთხვევაში, კრიზისების მართვას პროგნოზირებადი, პრევენციული, დაცვითი, აღდგენითი მექანიზმების საშუალებით.
- ✓ გაძლიერდეს თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების კრიტიკული ინფრასტრუქტურის დაცვა და გამართული ფუნქციონირების უზრუნველყოფა 24/7 მოქმედი მექანიზმების მიერ ინფორმაციული რესურსების შექმნის, დაუფლების, განვითარების, ოპერირების საუკეთესო პრაქტიკის გამოყენებით.
- ✓ რეგულარულად განხორციელდეს კიბერსივრცეში არსებული და პოტენციური საფრთხეების, რისკებისა და გამოწვევების კვლევა და ანალიზი. საფრთხეების გაცნობიერება და მათი პოტენციური ზემოქმედების შეფასება ხელს შეუწყობს უსაფრთხოების ზომების გაძლიერებას. საფრთხეების ანალიზისა და რისკების კვლევის შედეგების საფუძველზე მოხდეს პრევენციული ზომების შემუშავება და გატარება თანამედროვე გამოწვევების დაძლევის მიზნით.
- ✓ კრიტიკული ინფორმაციული სისტემების მდგრადობის ამაღლება კიბერშეტევებისადმი და კიბერინციდენტებით გამოწვეული შედეგების აღმოფხვრა
- ✓ ეფექტიანი ღონისძიებების გატარება პოტენციური კიბერ ინციდენტების პრევენციის უზრუნველსაყოფად.
- ✓ ხელი შეეწყოს თანამშრომლებს, მონაწილეობა მიიღონ კიბერუსაფრთხოების სფეროსთან დაკავშირებულ სხვადასხვა საგანმანათლებლო ტრენინგებსა და პროგრამებში.
- ✓ 2014-2016 წლების პოლიტიკის განხორციელებისათვის საქართველოს თავდაცვის სამინისტროს მიერ შემუშავებული იქნეს სახელმძღვანელო დოკუმენტები, რომლებიც მნიშვნელოვნად შეუწყობენ ხელს კიბერუსაფრთხოების უზრუნველყოფისათვის საჭირო ინფრასტრუქტურის ეფექტურად დანერგვასა და განვითარებას.

- ✓ შეიქმნას და დამკვიდრდეს კიბერუსაფრთხოებისა და კონფიდენციალობის კულტურა, რაც საშუალებას მისცემს მომხმარებელს, იმოქმედოს ეფექტურად წინასწარ განსაზღვრული წესებით.

ამ მიზნების განსახორციელებლად საქართველოს მთავრობა სარგებლობს შემდეგი პრინციპებით:

- ✓ კიბერუსაფრთხოება როგორც ეროვნული უსაფრთხოების განუყოფელი ნაწილი- რომელზეც დამოკიდებულია სახელმწიფოს ეფექტური განვითარება და იგი არის ეროვნული უსაფრთხოების პოლიტიკის შემადგენელი მიმართულება.
- ✓ ადამიანის უფლებათა განუხრელი დაცვა და პატივისცემა-საქართველოს ხელისუფლება ითვალისწინებს ადამიანის უფლებათა დაცვის პრინციპებს,რომელიც მიესადაგება კიბერუსაფრთხოების პოლიტიკის შემუშავების პროცესს.
- ✓ საქართველოს მთავრობის ერთიანი მიდგომა-კიბერუსაფრთხოების უზრუნველსაყოფად მნიშვნელოვანია სახელმწიფო უწყებებს შორის მაქსიმალური თანამშრომლობა და ისეთი მექანიზმის განვითარება,რომელიც ხელს შეუწყობს კიბერუსაფრთხოების პოლიტიკასთან დაკავშირებით საქართველოს მთავრობის ერთიან მიდგომას და სხვადასხვა სახელმწიფო სტრუქტურებს შორის გამართულ კოორდინირებულ მუშაობას.
- ✓ თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის-კიბერუსაფრთხოების უზრუნველსაყოფად აუცილებელია თანამშრომლობა კერძო და სახელმწიფო სექტორებს შორის.აუცილებელია თანამშრომლობა როგორც ბიზნესს,ასევე არასამთავრობო და აკადემიურ წრეებთან,ვინაიდან კრიტიკული ინფორმაციული ინფრასტრუქტურის ძირითადი ნაწილი თავმოყრილია კერძო სექტორში.
- ✓ აქტიური საერთაშორისო თანამშრომლობა-საქართველოსათვის შეუძლებელია მხოლოდ საკუთარი რესურსებით უზრუნველყოს კიბერუსაფრთხოების სფეროში არსებულ გამოწვევებთან და საფრთხეებთან გამკლავება,სწორედ ამიტომაც მისთვის აუცილებელია თანამშრომლობა საერთაშორისო ორგანიზაციებთან,პარტნიორებთან კიბერუსაფრთხოების სფეროში.
- ✓ ინდივიდუალური პასუხისმგებლობა-თითოეული მოქალაქე,საჯარო დაწესებულება თუ საწარმო ვალდებულია საკუთარი ინფორმაციული უსაფრთხოება ინდივიდუალურად უზრუნველყოს.
- ✓ ადეკვატური ზომები-პროპორციული ზომების მიღება რისკების ანალიზისა და საერთაშორისო რეკომენდაციების შესაბამისად,რომელიც უზრუნველყოფს ინფორმაციის თავისუფალი და შეუზღუდავი წვდომის საშუალებას,ასევე ადამიანის უფლებებისა და სხვა დემოკრატიული პრინციპების დაცვას.

4.ამერიკის შეერთებული შტატების კიბერუსაფრთხოების რაობა და არსი - მოკლე მიმოხილვა

კიბერ უსაფრთხოება ამჟამად და მომავლისთვისაც ერთ-ერთი მნიშვნელოვანი საკითხია ყველა ორგანიზებულ საზოგადოებაში. ვინაიდან, 2009 წელს ამერიკის შეერთებულმა შტატებმა კიბერ უსაფრთხოება დაასახელა „ყველაზე სერიოზულ გამოწვევად ეკონომიკური და ეროვნული უსაფრთხოების გამოწვევებს შორის, 21-ე საუკუნეში ამერიკის ეკონომიკური კეთილდღეობა დამოკიდებული იქნება კიბერ უსაფრთხოებაზე“.

აშშ-ს კიბერუსაფრთხოების სისტემა არის სამ საფეხურიანი.

პირველ დონეში შედიან ფედერალური უწყებები:

- ✓ Department of Defense-თავდაცვის სამინისტრო.
- ✓ Department of Homeland Security, DHS-შიდა უსაფრთხოების სამინისტრო.
- ✓ Office of Cyber Security and Communications-კიბერუსაფრთხოების და კომუნიკაციების ოფისი
- ✓ United States Department of Justice, DOJ-იუსტიციის დეპარტამენტი

მეორე დონეს მოიცავს პირველ დონის სტრუქტურებში შემავალი ჯგუფები/ცენტრები:

- ✓ Cyber Crimes Center-კიბერდანაშაულთან ბრძოლის ცენტრი.
- ✓ National Cyber Security Division, NCSD-კიბერუსაფრთხოების ეროვნული ცენტრი.
- ✓ NSA/CSS Threat Operations Center, NTOC -კიბერსაფრთხეების საოპერაციო ცენტრი.

მესამე დონე არის რეგიონალური და ლოკალური სტრუქტურული ქვედანაყოფები,მათზე კონტროლს ახორციელებენ ზემოთ აღნიშნული ორგანიზაციები.

თეთრი სახლი 2011 წლის 11 სექტემბრის შემდეგ გადაერთო კიბერ უსაფრთხოების თემაზე მუშაობაზე და გამოკვეთა კიბერ უსაფრთხოების სტრატეგია,რომელიც გამოქვეყნდა ამავე წლის მაისში.იგი განიხილავს ამერიკის შეერთებული შტატების პოზიციას კიბერ უსაფრთხოებასთან დაკავშირებულ საკითხებზე და ასევე ამ სფეროში სხვა ქვეყნებთან ურთიერთობებზე.

თავდაცვის დეპარტამენტის მიზანია უხელმძღვანელოს კიბერ სტრატეგიას,რომელიც მოიცავს კიბერ ძალების განვითარებას და კიბერ თავდაცვის გაძლიერებას.იგი ფოკუსირებულია სამ ძირითად ამოცანაზე:

- ✓ დაიცვას ამერიკის შეერთებული შტატები და მისი ინტერესები კიბერ შეტევებისგან
- ✓ უზრუნველყოს ინტერგირებული კიბერ შესაძლებლობები,რათა მხარი დაუჭიროს სამხედრო ოპერაციებს და გაუთვალისწინებელ გეგმებს დამატებითი გარემოებების შემთხვევაში.
- ✓ დაიცვას თავდაცვის დეპარტამენტის ქსელები,სისტემები და ინფორმაცია.

სტრატეგია ფოკუსირებულია 5ძირითად მიზანზე:

- ✓ კომპიუტერული სისტემის,ქსელების და იმ გუნდის განვითარება და გაუმჯობესება,რომლებიც მუშაობენ და პასუხისმგებელნი არიან კიბერ სივცრის ოპერაციებზე.
  2013წლიდან თავდაცვის დეპარტამენტმა დაიწყო კიბერ პერსონალისა და ტექნოლოგიების ინვესტიცია,ანუ ეს ნიშნავს იმას, რომ უზრუნველყოს გუნდის სწავლება და გადამზადება, მისცეს შესაძლებლობების განვითარების საშუალება.ამ მიზნის ძირითადი ამოცანებია:ოპერაციების ტექნიკური შესაძლებლობების და ერთიანი და ინტეგრირებული ოპერატიული პლატფორმის შექმნა,კვლევისა და განვითარების ხელშეწყობა.
- ✓ საინფორმაციო ქსელის,მასში არსებული ინფორმაციის დაცვა და არსებული რისკების/ზარალის შემცირება,შემსუბუქება.
  თავდაცვის დეპარტამენტმა უნდა უზრუნველყოს ყველაზე მნიშვნელოვანი ქსელების და მონაცემების განსაზღვრა, პრიორიტიზირება,ისე ,რომ მისი ოპერაციები ეფექტურად განახორციელოს.ასევე წინასწარი დაგეგმვა და პრაქტიკა ყოველივე ამის შესასრულებლად.ამ მიზნის ძირითადი ამოცანებია:ერთობლივი საინფორმაციო გარემოს, ერთიანი უსაფრთხოების არქიტექტურის შექმნა, რომელიც მიმართულია მომსახურების სპეციფიკური ქსელების და სისტემების დაცვაზე,თავდაცვის გარშემო ფენის დამცავი სისტემის, ანგარიშვალდებულების და საიმედოობის სტანდარტების გაუმჯობესება, კონტრდაზვერვის და IP ქურდობის წინააღმდეგ ბრძოლა მთელი ძალისხმევით.
- ✓ მუდმივი მზად ყოფნა აშშ-ის და მისი ინტერესების მავნე,გამანადგურებელი და დესქტრუქციული კიბერ შეტევებისგან დაცვისთვის.თავდაცვის დეპარტამენტმა უნდა შეიმუშავოს თავისი დაზვერვა, გაფრთხილება და ოპერატიული შესაძლებლობები, რათა შეამსუბუქოს დახვეწილი, ბოროტი კიბერშეტევები.ამ

მიზნის ძირითადი ამოცანებია:დაზვერვისა და გაფრთხილების შესაძლებლობების განვითარება მოსალოდნელი საფრთხეებისგან დასაცავად,იმუშავოს DHS(Departament of Homenland Security)-სთან,რათა განავითაროს უწყვეტი და ავტომატური მექანიზმები ინფორმაციის გაზიარების მიზნით.

- ✓ შექმნას და განავითაროს კიბერ პარამეტრები და გეგმა,რომ შემდგომში შეძლოს მათი გამოყენება კონფლიქტის ესკალაციის გასაკონტროლებლად,ასევე განისაზღვროს კონფლიქტის ბუნების ყველა ეტაპები.მომატებული დაძაბულობის ან მტრობის დროს, პრეზიდენტი უზრუნველყოფილი უნდა იყოს პარამეტრების ფართო სპექტრით კონფლიქტის ესკალაციისთვის კონტროლისთვის. შეერთებულ შტატებში არსებული ხელსაწყოების ნაწილის, შემუშავებული უნდა იყოს ეფექტური კიბერ პარამეტრები და განავითაროს ეს ვარიანტები დეპარტამენტულ გეგმებში. თავდაცვის დეპარტამენტი ხელს შეუწყობს კიბერ შესაძლებლობებს, რათა მიაღწიოს ძირითად უსაფრთხოების მიზნებს მასიმალური სიზუსტით,რათა შეამციროს სიცოცხლის დაკარგვა და ქონების განადგურება.
- ✓ საერთაშორისო პარტნიორებთან და ორგანიზაციებთან ურთიერთობების დაგეგმვა და განხორციელება,რათა გაიზიაროთ მოსალოდნელი საფრთხეები და გაზარდონ საერთაშორისო უსაფრთხოება და სტაბილურობა.ყველა დონის კიბერ უსაფრთხოება მოითხოვს მჭირდო კავშირს და თანამშრომლობას უცხოელ მოკავშირეებთან და პარტნიორებთან.საერთაშორისო თანამეგობრობაში ჩართულობის მიზნით კიბერ სტრატეგიის თავდაცვის დეპარტამენტი ცდილობს დაეხმაროს მათ კიბერ შესაძლებლობებსა თუ კიბერ თავდაცვაში.შესაძლებლო პარტნიორობის განვითარება პრიორიტეტულ რეგიონებზე იქნება ორიენტირებული, მათ შორისაა ახლო აღმოსავლეთი, აზია და ევროპა. DOD(კიბერ უსაფრთხოების თავდაცვის დეპარტამენტი) დარჩება ადაპტაციური და მოქნილი, ვინაიდან საჭიროა ახალი ალიანსებისა და პარტნიორების შეძენა.

5. კიბერსაფრთხეების გეოპოლიტიკური ასპექტები: კიბერშეტევები საქართველოსა და ამერიკის შეერთებულ შტატებზე

5.1.2008 წელს რუსეთის მიერ საქართველოზე კიბერშეტევა

2008 წელს საქართველოსა და რუსეთს შორის მომხდარი შეიარაღებულმა ომმა გასტანა 5 დღეს,თუმცა ასევე ადგილი ჰქონდა რუსეთის მხრიდან არა მხოლოდ შეიარაღებულ, არამედ კიბერ შეტევასაც.შეიქმნა საფრთხე, რომ ქვეყანა აღმოჩნდებოდა ინფორმაციულ ვაკუუმში.კიბერშეტევები თანმიმდევრობით მიმდინარეობდა სხვადასხვა მნიშვნელოვან ობიექტებზე.თავდასხმა მოხდა საგარეო თავდაცვის სამინისტროს ვებ გვერდზე,ასევე დაზიანდა სხვა ელექტრო წყაროები,როგორიცაა საქართველოს ბანკისა და პრეზიდენტის ვებ პორტალები.თავდასხმისთვის გამოყენებული იქნა სხვადასხვა ტექნიკები,როგორიცაა DDOS-გამანაწილებელის გაუქმება და ვებ გვერდების წაშლა/გაუქმება/დამახინჯება.გამოყენებული მეთოდთაგან არცერთი არის ინოვაციური და ახალი თუმცა თავად პროცესი იყო კარგად დაგეგმილი და ორგანიზებული.რუსულენოვანი საიტები როგორიცაა stopgeorgia.ru და სხვები DDOS-ს შეტევებისთვის პროგრამულ ინსტრუციებს სთავაზობდნენ.უნდა აღინიშნოს ისიც რომ, 2008 წელს ინტერნეტ მომხმარებელთა დონე ძალიან დაბალი იყო, 100 ადამიანზე 10 ინტერნეტ მომხმარებელი,რასაც ვერ ვიტყვით რა თქმა უნდა დღესდღეობით.

მკვლევარის Jart Armin-ის განცხადებით, 2008 წლის 7 აგვისტოს შემდეგ მრავალი ქართული ინტერნეტ სერვერი გარე კონტროლის ქვეშ იმყოფებოდა.2008 წლის 9 აგვისტოს საქართველოს ინტერნეტ კავშირის ძირითადი მონაკვეთები გადაიტვირთა და გავრცელდა ინფორმაცია რუსეთსა და თურქეთში დაფუძნებული სერვერების მეშვეობით.

10 აგვისტოს Jart Armin-მა განაცხადა, რომ ქართული საიტები, შესაძლოა, გაყალბებული ყოფილიყო: "გამოიყენეთ სიფრთხილით ნებისმიერი ვებ-გვერდი, რომელიც საქართველოს ოფიციალური წყაროდან გამოჩნდება,რომელზეც უახლესი ამბები არ არის, [როგორიცაა შაბათის, 9 აგვისტოს, ან კვირა, აგვისტო 10], შეიძლება იყოს თაღლითური", - თქვა მან.

2008 წლის 11 აგვისტოს საქართველოს პრეზიდენტის ვებ-გვერდი გაუქმდა და პრეზიდენტ სააკაშვილის ადოლფ ჰიტლერთან ერთად გამოსახული სურათები გამოჩნდა.

რუსმა ჰაკერებმა შეტევები განხორციელეს სამთავრობო, კერძო, საერთაშორისო გვერდებზე, საიდანაც შეიძლებოდა ინფორმაცია გავრცელებულიყო, ასევე მათ თვალთახდვიდან არ გამორჩენიათ არასამთავრობო ორგანიზაციების ოფიციალური საიტებიც. აქედან გამომდინარე ქვეყნის ინფრასტრუქტურის დიდი ნაწილი პარალიზებული აღმოჩნდა.

2008წლის კიბერშეტევამ გვაჩვენა, რომ საქართველოს მთავრობას არ შესწევდა უნარი დაეცვა ინფორმაციული ფუნდამენტი. პირველი კონსტრუქცია რომელიც იყო შემუშავებული, იყო ინფორმაციის გამფილტრავი საშუალება, მას შეეძლო მიეღო და გაეფილტრა რუსული IP-ის ინფორმაცია, თუმცა არც ისე ეფექტური იყო, რადგან ჰაკერები უკვე მზად იყვნენ, რომ მსგავსი თავდაცვა შეიძლება დახვედროდათ,ამიტომ მათ ქვეყნის გარედან დაიწყეს შეტევების განხორციელება. სწორედ ამიტომ, საქართველომ ესტონეთის მთავრობას მიმართა დასახმარებლად და საქართველოში გამოგზავნილ იქნა ექსპრტთა ჯგუფი,რათა შეენარჩუნებინათ თავდაცვა, მათი დახმარებით საქართველოს პრეზიდენტის ვებ გვერდი გადამისამართდა Google-ს ბლოგერების სერვერებზე კალიფორნიაში, თავდაცვის სამინისტროს ვებ გვერდი გადავიდა კერძო კომპანიის სერვერებზე აშშ-ში, საგარეო საქმეთა სამინისტრო კი ესტონეთის სერვერებში.

Korns და Kastenberg აღნიშნავს, რომ საქართველო იყო კიბერ-ჩაკეტილი ,საქართველოს მთავრობამ და მოსახლეობამ ვერ შეძლეს კომუნიკაცია ერთმანეთთან და გარე სამყაროსთან[Tikk, et al., 2008; Grey Goose, 2008; Hollis, 2011; Downing,
2011]. საქართველოს კიბერსივრცე გაყინული იყო, სამოქალაქო საზოგადოებას და კერძო სექტორს არ ჰქონდა გონივრული პასუხი კიბერშეტევებზე, აქ არ იგულისხმება პირდაპირი კონტრშეტევები ან ჩართულობა კიბერ შეტევების შესაჩერებლად, არამედ იმ გზების მოძიება რომლითაც ამ შეტევების დროებითი შეჩერება მაინც მომხდარიყო. ამ შეტევებმა აჩვენა, რომ მხოლოდ სამთავრობო რესურსები არ არის საკმარისი კიბერ სივრცის დასაცავად და კიბერ შეტევებთან გასამკლავებლად, მასში უნდა ჩაერთოს კერძო სექტორიც, რათა მაქსიმალურად იყოს კიბერუსაფრთხოება უსზრუნველყოფილი. მთავრობა შეიძლება იყოს ლიდერი ქვეყნის ინფორმაციული უსაფრთხოების გარემოს ჩამოყალიბებაში, მაგრამ კერძო სექტორისა და სამოქალაქო საზოგადოების მხრიდან თანამშრომლობისა და ინიციატივების გარეშე კიბერ შესაძლებლობების განვითარება სავსეა დაბრკოლებებით.გასაკვირი არ არის რომ 2008 წლის კიბერ შეტევამ უდიდესი გავლენა მოახდინა საქართველოს კიბერ უსაფრთხოების გარემოს შემდგომ ჩამოყალიბებაში.

რუსეთის მიერ საქართველოზე კიბერ შეტევა ბევრი ექსპერტის მიერ აღიარებულია როგორც "ინფორმაციული კიბერ ომი". კიბერ ომი არის "ერი-სახელმწიფოების ქმედებები

სხვა ქვეყნის კომპიუტერების ან ქსელებში შეღწევა ზიანის ან დაზიანების გამომწვევი მიზეზების გამო“-Richard A.Clarck, Cyber War(May 2010).

ამ ქეისსში რუსეთის მხრიდან იყო საერთაშორისო სამართლებრივი დარღვევა და მათ გამოიყენეს ძალა კიბერსივრცეში საქართველოს წინააღმდეგ,თუმცა საბოლოოს რუსეთმა რა თქმა უნდა უარყო საქართველოს მიერ მის მიმართ წაყენებული ბრალდებები.

11 აგვისტოს საქართველომ დაადანაშაულა რუსეთი საქართველოს მთავრობის ვებ-საიტებზე კიბერ ომის დაწყებაში სამხედრო თავდასხმის პარალელურად.საქართველოს საგარეო საქმეთა სამინისტრომ განაცხადა, რომ "რუსეთის მიერ განხორციელებული კიბერ თავდასხმები სერიოზულად უშლის ხელს ბევრ ქართულ ვებსაიტს, მათ შორის საგარეო საქმეთა სამინისტროს საიტსაც“.

კრემლის სპიკერმა ბრალდება უარყო და განაცხადა: "პირიქით, რუსული მედიის და ოფიციალური ორგანიზაციების კუთვნილი ინტერნეტ-საიტები დაზარალდნენ ჰაკერული თავდასხმებით“.

ისრაელის კომპიუტერის საგანგებო სიტუაციების რეაგირების ჯგუფის ყოფილი ხელმძღვანელი გადი ევრონი მიიჩნევდა, რომ ქართული ინტერნეტ ინფრასტრუქტურის თავდასხმები კიბერ-ბუნტი უფრო იყო, ვიდრე კიბერ-ომი. ევრონმა აღიარა, რომ თავდასხმები შეიძლება ყოფილიყო "არაპირდაპირი რუსული (სამხედრო) ქმედება",დამიზნებული თავდამსხმელების მიერ.“"შეეძლოთ შეერჩიათ უფრო სტრატეგიული სამიზნეები ან აღმოეფხვრათ ინფრასტრუქტურა (ქართული ინტერნეტი)".

2009 წლის მარტში უსაფრთხოების მკვლევარებმა დაასკვნეს, რომ რუსეთის GRU და FSB სავარაუდოდ შეასრულეს როლი თავდასხმების კოორდინაციისა და ორგანიზების საქმეში. Stopgeorgia.ru ფორუმი იყო სახელმწიფოს მიერ დაფინანსებული თავდასხმების წინაპირობა.

ამერიკის შეერთებული შტატების კიბერ შეტევების შედეგების ანალიზის განყოფილების წევრმა (US-CCU) John Bumgarner-მა ჩაატარა კვლევა რუსულ-ქართული ომის დროს კიბერშეტებზე.ანგარიშში ნათქვამია, რომ კიბერ-თავდასხმების ორგანიზატორებმა იცოდნენ რუსეთის სამხედრო გეგმები, მაგრამ თავად თავდამსხმელები სამოქალაქო პირები იყვნენ. Bumgarner-ის კვლევამ დაადგინა, რომ ქართული მედიის წინააღმდეგ დაწყებული კიბერ თავდასხმების პირველი ტალღა შეესაბამებოდა სამხედრო ოპერაციებში გამოყენებულ ტაქტიკას. კამპანიაში გამოყენებული კიბერ-თავდასხმის იარაღის უმრავლესობა, როგორც ჩანს, დაწერილი ან მორგებულია გარკვეულწილად კონკრეტულად საქართველოს წინააღმდეგ კამპანიისთვის", - ნათქვამია კვლევაში

ამ შემთხვევის შესწავლით, ნათლად ვხედავთ იმას,რომ საქართველო არ იყო მზად ამ შეტევისთვის და იგი სრულიად უძლური აღმოჩნდა მის წინააღმდეგ საბრძოლველად, როგორც ტექნიკურად, ასევე ფსიქოლოგიურად. საქართველოს არ გააჩნდა შესამაბისად აღჭურვილი უწყებები, ორგანიზაციები, სახელმწიფო თუ კერძო პირები, რომლებიც უზრუნველყოფდნენ ამ კიბერ შეტევასთან გამკლავებას,არ იყვნენ შესაბამისად გადამზადებული კადრები,რომლებსაც ეცოდინებოდათ თუ როგორ უნდა მოქცეულიყვნენ კონკრეტულ შემთხვევაში.

თავდაპირველად, როდესაც გააანალიზეს, რომ საქართველოზე შეტევა განხორიელდა იყო დაბნეულობა,გაურკვევლობა და უიმედობა, რა თქმა უნდა კიბერ შეტევამ გამოიწვია ინფორმაციული ვაკუუმი,რამაც საერთოდ ხელ-ფეხი შეუკრა ჩვენს სახელმწიფოს მოქმედებისგან. თუმცა საბოლოოდ როდესაც ნაბიჯ-ნაბიჯ დაიწყო ჩვენმა ქვეყანამ შეტევისთვის წინააღმდეგობა გაეწია,გამოვიყენეთ ის ელემენტარული რაც გაგვაჩნდა, თუმცა უშედეგო და უსარგებლო აღმოჩნდა შეტევის წინააღმდეგ, ვინაიდან, როგორც აღვნიშნეთ ჰაკერები ამისთვის მზად იყვნენ და ჩვენს მიერ გაწეულ წინააღმდეგობას მათთვის პრობლემა არ შეუქმნია, რომ კვლავ გაეგრძელებინათ ქვეყანაზე შეტევა. მხოლოდ იმის შემდეგ, როცა საქართველო დამოუკიდებლად უძლური იყო წინააღმდეგობა გაეწია რუსეთის მიერ განხოერიელებული კიბერ შეტევისთვის, მან მიმართა დახმარება სხვა უფრო გამოცდილ ქვეყანას, რომლის საშუალებითაც შევძელით კიბერ შეტევის შეჩერება მომხდარიყო.

ვფიქრობ,რომ ამ შეტევის მაგალითზე, საქართველომ საკუთარ თავზე გამოსცადა, რომ როდესაც ომია ყველაფრისთვის უნდა იყო მზად, არა მარტო შეიარაღებლი დაპირისპირებისთვის,არამედ ყველანაირი შეტევისთვის, ეს დამტკიცდა კიდეც შემოთ განხილულ ქეისში. ამან დადებითი შედეგი მოიტანა იმ მხრივ, რომ თუ მანამდე ყურადღებას არ ვაქცევდით, ან კიდევ, ნაკლებად ვითვალისწინებდით კიბერუსაფრთხოების მნიშვნელობას და კიბერ სივრცის დაცვას, 2008 წლის შემდეგ ნათელი გახდა, რომ მხოლოდ შეიარაღება ვერ უზრუნველყოფს ქვეყნის სრულ უსაფრთხოებას და მუშაობა დავიწყეთ იმაზე, რომ გვქონდეს ძლიერი კიბერუსაფრთხოება, კიბერ თავდაცვა, შეძლებისდაგვარად უზრუნველვყოთ კადრების გადამზადება შესაბამის სფეროში სამუშაოდ და სხვა.

5.2. აშშ-ს კიბერმოწყვლადობის შემთხვევა

2014 წელს შეტევა აშშ-ს უმსხვილეს ფინანსურ კონგლომერატზე განხორციელდა. ამ კიბერშეტევის შედეგად, 80 მილიონზე მეტი კლიენტის ანგარიში იყო

კომპრომეტირებული. 2014 წელს JP Morgan Chase-ის ბანკის მონაცემთა გაჟონვის შედეგად, მისი ავტორიტეტი კატასტროფის ზღვარზე აღმოჩნდა.

10 საფინანსო ინსტიტუტის, საინფორმაციო ორგანიზაციების და სხვა კომპანიების, მათ შორის JPMorgan Chase, Fidelity Investments და Wall Street Journal- ის წინააღმდეგ კიბერ შეტევა განხორციელდა.სამმა ადამიანმა მოიპარა ბანკში არსებული პირადი მონაცემები.ამ შეტევების შედეგად, ეჭვმიტანილები ცდილობდნენ ბაზრების გაყიდვას, რომლებიც თითქოსდა კომპანიების მომხმარებლებისთვის მანიპულირებდნენ. მათ ასევე დაიწყეს კიბერ თავდასხმები, რათა გადაიხადონ უკანონო ნარკოტიკების მომწოდებლების, ყალბი პროგრამული უზრუნველყოფის, მავნე დისტრიბუტორების, უკანონო ონლაინ კაზინოებისა და სხვა არაკანონიერი საქმიანობის თანხები.ასევე,დამნაშავეები დაინტერესებულები იყვნენ ინფორმაციით, რომელიც ბანკის მარკეტინგულ მომსახურებასთან იყო კავშირში. შეტევა განხორციელდა 90 სერვერზე, სადაც კლიენტების შესახებ ინფორმაცია ინახებოდა. თითოეული გატეხვის დრო ძალიან მცირე – საათზე ნაკლები იყო. გამოძიების თანახმად(FBI), პირველი შეტევა ბანკის ერთ-ერთი თანამშრომლის პერსონალური კომპიუტერიდან განხორციელდა. მოგვიანებით, აშშ-ს სპეცსამსახურებმა სამი ეჭვმიტანილი – ისრაელის მოქალაქეები დააკავეს. მათ ბრალი ათობით პუნქტში წაუყენეს, მათ შორის – თაღლითობა, უკანონო გზით თანხის მოპოვების მიზნით ფულის გათეთრება, კომპიუტერული სისტემების გატეხვა. ჰაკერებმა მოპოვებული მონაცემები პირადი მიზნებისთვის – ბირჟაზე სათამაშოდ გამოიყენეს. ამის შედეგად, ჰაკერები მილიონობით დოლარით გამდიდრდნენ.

პროკურორების აზრით, ეს იყო მასიური კომპიუტერული შეტევის წრე, რომელიც მიზნად ისახავდა მთელს მსოფლიოში მილიონობით ადამიანის მონაცემების მოპარვას.

"იმ საუკუნეში, როდესაც მნიშვნელოვანი ინფორმაციის დიდი ნაწილი ინახება ციფრულ ფორმატში, პოტენციურად სოციალურად დაუცველი ინტერნეტით ჩართულ მოწყობილობებზე, საზოგადოებრივ-კერძო პრაქტიკა და ინფორმაციის გაზიარება უფრო მნიშვნელოვანია, ვიდრე ოდესმე"-Graham Cluley.

მიუხედავად იმისა,რომ ამერიკის შეერთებული შტატები არის სუპერ სახელმწიფო და მიუხედავად იმისა,რომ იგი დაწინაურებულია ყველა სახელმწიფოსთან შედარებით ბევრ სფეროში, მით უმეტეს უსაფრთხოებაში, ჰაკერებმა მაინც მოახერხეს და შეძლეს ის რომ გაეტეხათ აშშ-ს უმსხვილესი ფინანსური კონგლომერატი. აქედან კარგად ჩანს ერთი რამ, რომ უძლიერესებსაც კი აქვთ თავიანთი სუსტი წერტილი და მათ შეძლეს ამ სისუსტის პოვნა აშშ-ს ფინანსურ კონგლომერატთან დაკავშირებით.

ქვეყანამ და განსაკუთრებით ხალხმა,რომელმაც იზარალა ამ კიბერ შეტევით უდიდესი ზარალი ნახეს, მათ დაკარგეს უზარმაზარი თანხა, თუმცა აქვე გაჩნდა უკვე ნდობის პრობლემა ფიანსურ კონგლომერატზე,ავტორიტეტის განადგურება და ნულამდე დაყვანა, რომელიც თუნდაც არ მიეყენებინა ამ შეტევას ფინანსური ზარალი,საბოლოოდ მაინც გამოიწვევდა ფინანსურ კრიზისს.

ეს შემთხვევა არის მაგალითი იმისა,რომ არცერთი ქვეყანა არ უნდა მოდუნდეს და გვერდზე არ გადადოს თავისი უსაფრთხოების საკითხი,როცა საქმე ეხება ქვეყნის უსაფრთხოებას,რომელიც პარალელურია ეკონომიკური წინსვლის,საზოგადოებრივი განვითარების,პოლიტიკური და საერთაშორისო ურთიერთობების.

5.3.რუსი ჰაკერების მიერ აშშ-ს დემოკრატიული პარტიის დაჰაკვა

აშშ-ს პრეზიდენტობის ყოფილ კანდიდატს Hilary Clinton-ს სახელმწიფო მდივნობის პოსტზე ყოფნისას პირადი ელექტრონული ფოსტის გამოყენებაში ედავებოდნენ. კლინტონს არაერთხელ მოუწია ამ საკითხზე განმარტების გაკეთება. კლინტონის შეცდომა მისმა კონკურენტმა დონალდ ტრამპა სათანადოდ გამოიყენა. მართალია, კლინტონისთვის ოფიციალურად ბრალი არ წაუყენებიათ და სავარაუდოდ, საქმეც მხოლოდ ფეისბუქზე ბოდიშის მოხდით დასრულდებოდა, თუმცა, არჩევნებამდე სულ რაღაც 1 კვირით ადრე FBI-მ განაცხადა, რომ Email-ების საქმეში ახალი დეტალები გამოჩნდა. სკანდალი წინასაარჩევნოდ ხელახლა აგორდა. ბევრი ანალიტიკოსი ვარაუდობს, რომ ამ ფაქტმა შედეგებზე გავლენა იქონია.

თუ ამ ისტორიის მოვლენების ქრონოლოგიას გადახედავთ, ის დაიწყო Hilary Clinton-სა და John Podesta-ს ელექტრონული სკანდალით. მაშინ საიდუმლო ჩანაწერები გავრცელდა „Wikileaks“- ის მეშვეობით და მოიცვა საინფორმაციო ომი იმ დონეზე, რომელიც ამერიკას არასდროს უნახავს. მაგრამ ეს ყველაფერი მოხდა ყველა უსაფრთხოების ზომების იგნორირებით და დაუდევრად მოქმედებით,რითაც საბოლოოდ მათ ჰქონდათ ტონა საიდუმლო მონაცემები. არჩევნებში მონაწილეობისას, აშშ-ს დემოკრატიულმა ეროვნულმა კომიტეტმა (DNC) მიიღო უამრავი ფიშინგ ელფოსტა. ერთ-ერთი მათგანი Hilary Clinton-ის კამპანიის თავმჯდომარეს, John Podesta-ც გაეგზავნა. თანაშემწემ, Charles Delavan-მა John Podesta-ს პირადი ანგარიშისთვის გაგზავნილი შეტყობინება შენიშნა. მან Podesta-ს სთხოვა პაროლის შეცვლა. Delavan-ი მიხვდა რომ ეს შეიძლება ყოფილიყო ელფოსტის ფიშინგი,ამიტომაც გაგზავნა კომპიუტერის ტექნიკოსი მის გამოსასწორებლად.კრემლის ჰაკერები ფლობდნენ Podesta-ს 60000-მდე პირადულ Email-ს. აშშ-ს სადაზვერვო

სამსახურის წარმომადგენლების განცხადებით, მოსკოვმა მიაწოდა ელ-ფოსტა, რომელიც WikiLeaks- ს ეკუთვნოდა. ელექტრონული სკანდალი ოქტომბერში დაიწყო და დომინირებდა საინფორმაციო სივრცეში. FBI-ის დოკუმენტის საფუძველზე,მათთვის გარკვეული დროის განმავლობაში ცნობილი იყო,რომ რუსეთი ფართო მასშტაბით მოქმედებდა და მათ ჰქონდათ სისტემური მცდელობა აშშ-ს პოლიტიკური ორგანიზაციების დაჰაკვის,მათ შორის თეთრი სახლისა და სახელმწიფო დეპარტამენტის. მაგრამ მაღალი დონის დელეგაციის გაგზავნისა და სიგნალის გაზრდის ნაცვლად, FBI-მ მხოლოდ ერთი სპეციალური აგენტი მიიღო. FBI- ის გამოძიების თანახმად, რუსმა ჰაკერებმა DNC- ის კომპიუტერულ სისტემებში თითქმის შვიდი თვის განმავლობაში შეძლეს ყოფნა, სანამ დემოკრატიული ჩინოვნიკები მიხვდებოდნენ თავდასხმის სიმძიმეს და დასახმარებლად მიმართავდნენ გარე კიბერ ექსპერტებს. ბიურომ ბოლო რამდენიმე წელი გაატარა "DUKE"-ს აღმოსაფხვრელად თეთრი სახლის, სახელმწიფო დეპარტამენტის, და მთავრობის ერთ-ერთი საუკეთესო დაცული ქსელის დაუცველი ელექტრონული სისტემებისგან.აგენტმა Adrian Hawkins-მა DNS-ში დანერგა IT helpdesk,მან ტექნიკური მხარდაჭერის ჯგუფის კონტრაქტორ Tamene-ს განუცხადა, რომ DNS-დაჰაკული იყო ჯგუფისგან სახელად "DUKES". Tamene-მ სცადა მოეძებნა ამ ჯგუფის შესახებ რაიმე ინფორმაცია,თუმცა ვერაფერი იპოვა. მას არ შეეძლო ნამდვილი/რეალური ზარის განსხვავება ცრუ ზარისგან.ამიტომაც იგი ფიქრობდა,რომ Hawkins-ის ზარი იყო ერთ-ერთი ეშმაკობა და ყურადღება აღარ მიაქცია ამ ზარს.ეს იყო კიბერ-ჯაშუშური და საინფორმაციო-საბრძოლო კამპანია,რომლის მიზანიც იყო ამერიკის შეერთებული შტატების არჩევნების ჩაშლა,უცხოური ძალაუფლების მიერ პირველი ასეთი მცდელობა იყო ამერიკის ისტორიაში.სადაზვერვო სამსახურმა განაცხადა, რომ ის რაც დაიწყო ინფორმაციის შეგროვებით და გასაჯაროვებით,საბოლოო ჯამში შეიცვალა შესაძლებლობით,რომ ელიც საშუალებას იძლეოდა ზიანი მიაყენოს ერთ-ერთ კანდიდატს, ჰილარი კლინტონს.

ეს შესაძლებელია მომხდარიყო წინასწარი განზრახვით,როგორც ფედერალური ბიუროს გამოძიებამ ოფიციალურად დაადასტურა, მათ გაფრთხილებული ყავდათ DNS - მოსალოდნელი საფრთხის შესახებ და ოფიციალური გამოძიება ინფორმაციის გაჟონვის შემდეგ ჩატარდა.როგორც ჩანს, აშშ ყოველთვის ჰქონდა უზარმაზარი სივრცე/ხარვეზი კიბერ უსაფრთხოებაში,ამასობაში რუსეთი ფართოდ ვითარდება კიბერ შეტევით შესაძლებლობებში და კიბერ უსაფრთხოება გახდა # 1 თემა, მას შემდეგ, რაც დემოკრატებისთვის არჩევნების დაკარგვის მიზეზი გახდა და რუსეთს და ჰაკერებს ადანაშაულებენ იმისათვის, რომ ისინი აგრძელებენ საინფორმაციო ომს.

მონაცემების დარღვევის შემდეგ DNS-მა დაიქირავა CrowdStrike,კიბერ კომპანია.მალევე დადგინდა რომ კიბერ შეტევა განხორციელებული იყო რუსეთიდან და გამოვლენილ იქნა ორი ჯგუფი: „Cozy Bear“ და „Fancy Bear“.

Cozy Bear-მიბმული იყო რუსეთის FSB-ს ჯაშუშურ სააგენტოსთან,რომელმაც თავისი ოპერაცის დაიწყო 2015წელს.

Fancy Bear შეუერთდა თავდასხმებს 2016 წლის მარტში. ჰაკინგის ჯგუფი უკავშირდება GRU- ს, რუსეთის სამხედრო დაზვერვას.ეს იყო Fancy Bear რომელმაც დაჰაკა Podesta-ს ელექტრონული ფოსტის ანგარიში-მოცემულია FBI-ის დოკუმენტში.

Dmitri Alperovitch-მა, CrowdStrike-ის თანადამფუძნებელმა და მთავარმა ტექნოლოგიურმა ოფიცერმა განაცხადა, რომ ეჭვი არ იყო, რომ რუსეთი პასუხისმგებელი იყო: „არ არსებობს იმაზე მეტი დამაჯერებელი რამ,როგორიც ის რომ რუსეთი ამაში ყველაზე მთავარი აქტორია“.

აშშ-ს ცენტრალური სადაზვერვო სააგენტოს (CIA) შეფასებით, რუსეთი აშშ-ს 2016 წლის საპრეზიდენტო არჩევნებში ჩაერია, რათა დონალდ ტრამპს გამარჯვებაში დახმარებოდა.CIA-ს ამ დასკვნის შესახებ ინფორმაცია ოფიციალურმა პირებმა წამყვან გამოცემებს, მათ შორის The Washington Post-სა და The New York Times -ს მიაწოდეს.

The New York Times-ის წყაროს ინფორმაციით, საარჩევნო პერიოდში რუსებმა დემოკრატების ეროვნული კომიტეტის გარდა, რესპუბლიკელების კომპიუტერული სისტემებიც დაჰაკეს, მაგრამ მოპოვებული ინფორმაცია არ გაუვრცელებიათ. სადაზვერვო სამსახურების დასკვნით, რუსებმა WikiLeaks-ს მხოლოდ დემოკრატების დოკუმენტები მისცეს. არჩევნების წინა თვეებში მასობრივად სწორედ დემოკრატების დოკუმენტებმა გაჟონა. თუმცა, მთელი ამ ხნის მანძილზე, რესპუბლიკელები მომხდარს განსხვავებულად ხსნიდნენ და ამბობდნენ, რომ კიბერშეტევის მსხვერპლი პარტიის ინდივიდუალური წევრები ხდებოდნენ და არა მთლიანად ქსელი.

დედამიწაზე ყველა ქვეყანა ვითარდება თავისი კიბერ შესაძლებლობებით და განსაკუთრებით რუსეთი.თუმცა არსებობს კიბერ სივრცეში მოთამაშეები, რომლებიც ჯერ კიდევ არ არის სარადაროზე და შეიძლება უფრო ძლიერი იყოს, ვიდრე ჩვენ ოდესმე გვინახავს.

ერთ-ერთი მაგალითი იმისა,თუ როგორ არ უნდა იყო უყურადღებო,როცა ეს ეხება რეპუტაციას,ქვეყანასთან დაკავშირებულ საქმეს და უნდა აანალიზებდე თუ რამხელა პასუხისმგებლობა აქვს ადამიანს და ჯგუფს დაკისრებული ქვეყნის წინაშე,როდესაც პრეზიდებდობაზე აქვს პრეტენზია.თუმცა შეტევასთან დაკავშირებულმა მცირე

უყურადღებობამაც კი კარგად დაგვანახა,როგორი შედეგი მოიტანა დაზარალებულ პარტიას.

ვფიქრობ,რომ შესაბამისი ყურადღება და შესაბამის დროს რომ გამოეჩინათ ამ საქმესთან დაკავშირებით,შესაძლებელი იქნებოდა მათი დაცვა ამ შეტევისგან.როდესაც შეიმჩნევა ან ხდება კიბერ შეტევა პირველ რიგში უნდა იყოს შესაბამისი ზომები მიღებული:

- ✓ მისი აღმოჩენა
- ✓ დაზუზტება, თუ რა სახის კიბერ შეტევაა
- ✓ შესაბამისი ორგანოების მობილიზება მასთან გასამკლავებლად
- ✓ შესაბამისი საწინააღმდეგო შეტევის შემუშავება
- ✓ დროული მოქმედება კიბერ შეტევის წინააღმდეგ
- ✓ შეძლებისდაგვარად კიბერ შეტევასთან გამკლავება და მისი აღმოფხვრა

ჩემი აზრით, თუ არ იქნება შესრულებული ზემოთ ჩამოთვლილი პუნქტები და თუნდაც ერთ ერთი პუნქტი შეუსრულებელი დარჩება,ალბათ რთული ან შეუძლებელი იქნება კიბერ შეტევასთან გამკლავება.

თუნდაც დემოკრატიული პარტიის დაჰაკვა,რომ განვიხილოთ მაგალითად ამ პუნქტებთან მიმართებაში,ჩემი აზრით მოხდა დაგვიანებული მოქმედება,დაგვიანებით დაზუსტდა ნამდვილად იყო თუ არა შეტევა განხორციელებული ან ვინ იყო რეალური მსხვერპლი,დაგვიანებით ჩაერთვნენ შესაბამისი ორგანოები კიბერ შეტევის წინააღმდეგ და სწორედ ამიტომაც მოხდა ის რაც მოხდა,დემოკრატიული პარტია გახდა ჰაკერების მსხვერპლი,ამ ყველაფერმა კი მათი არჩევნებში წაგება გამოიწვია და ეს ყველაფერი მოხდა ტრამპის სასარგებლოდ.

5.4. Petya-გლობალური კიბერ ვირუსი საქართველოს ჭრილში

უმსხვილესი კომპანიები ასევე რამდენიმე ქვეყნის საჯარო და კერძო კომპანიები გახდნენ კიბერ შეტევის მსხვერპლნი.ვირუსმა სახელად Petya ასობით კომპანიის, ათასობით კომპიუტერში შეაღწია,დაბლოკა ინფორმაცია და უკან დასაბრუნებლად მოითხოვა გამოსასყიდი.ამ შეტევის გამო ყველაზე მეტად დაზარალდა უკრაინა, თუმცა მიუხედავად იმისა,რომ საქართველოში ვირუსს ჯერ არ მოუღწევია საკანონმდებლო ორგანოში შექმნილ შეფერხებას შინაგან საქმეთა სამინისტრო საკუთარი ინიციატივით სწავლობს.მინისტრის მოადგილე შალვა ხუციშვილი ფოთის პორტის მფლობელ კომპანიაზე Maersk-ზე კიბერ თავდახსმის ფაქტს ადასტურებს.

Petya- არის ვირუსი,რომელიც კორპორაციაში ყველაზე სუსტ კომპიუტერს აზიანებს და შემდეგ ქსელით ვრცელდება. სპეციალური მავნე პროგრამების მეშვეობით ხდება კომპიუტერში არსებული ინფორმაციის და მონაცემების შიფრაცია და ამ ფაილების დეშიფრაციისთვის გამოსასყიდი თანხის მოთხოვნა.ამ თანხის გადახდის შემდეგ ფაილები ხელმისაწვდომია და უბრუნდება მესაკუთრეს.თუმცა არის შემთხვევები როდესაც მომხმარებელმა გადაიხადა თანხა,თუმცა შესაძლოა მათ მაინც არ დაუბრუნდეს თავისი ინფორმაცია. „Petya Ransomware"-ის უნიკალურობა ისაა, რომ იგი ფაილებს სათითაოდ არ შიფრავს (როგორც ეს აქამდე არსებული „რანსომვეარების" სახეობებში გვხვდებოდა). ეს უკანასკნელი ტვირთავს კომპიუტერს და შიფრავს მყარი დისკის Master File Table-ს (MFT), რომელიც შეიცავს ჩანაწერებს მყარ დისკზე განთავსებული ყველა ფაილის/დოკუმენტის შესახებ. მათ შორის სახელს, დროს, უფლებების ჩანაწერებს და სხვა. იგი ასევე მყარ დისკზე განთავსებულ "MBR -ს ანაცვლებს საკუთარი მავნე კოდით, რომელსაც უშუალოდ გამოაქვს ეკრანზე გამოსასყიდის ტექსტი და კომპიუტერის მართვის ბერკეტებს არ აძლევს მომხმარებელს.თუმცა,როგორც საქართველოს იუსტიციის სამინისტროს სსიპ „მონაცემთა გაცვლის სააგენტოს" სამთავრობო კომპიუტერულ ინციდენტებზე სწრაფი დახმარების ჯგუფის, CERT-GOV-GE-ს მენეჯერი, დავით ქვათაძემ განაცხადა, Petya ე.წ. Wipper malware-ია."Petya არ გახლავთ Ransomware. ის Wipper malware-ია, რაც იმას ნიშნავს, რომ თუ ის თქვენს კომპიუტერში მოხვდა, ყველაფერს წაშლის. შესაბამისად, გადააგზავნით თუ არა, გამოსასყიდის სახით, 300 დოლარს, მის აღდგენას მაინც ვერ მოახერხებთ. თანაც, ის ელექტრონული ფოსტის მისამართი, სადაც ვირუსისგან დაზარალებულს თანხა უნდა გადაერიცხა, აღარ არსებობს და პროვაიდერმა გათიშა"-განმარტავს დავით ქვათაძე.

ზიანი რომელიც ამ ვირუსის საშუალებით შეიძლება მიადგეს ორგანიზაციებს არის ძალიან დიდი,დაზარალდნენ ისეთი დიდი კომპანიები როგორიცაა Maersk, Fedex, ბანკები, ჯანდაცვის სექტორი, ინფიცირების კერა გამოვლინდა უკრაინასა და რუსეთში და გავრცელდა ევროპაში - კერძოდ, ესპანეთში, საფრანგეთში, დიდ ბრიტანეთში. ვირუსის გავრცელების არეალში ასევე ხვდება ინდოეთიც. დაინფიცირდა უამრავი კომპიუტერი სახელმწიფო სტრუქტურებში, ბანკებში და კორპორაციებში. რუსეთში ასევე დაინფიცირდა 2 უმსხვილესი ნავთობკომპანიის („Роснефть" და „Башнефть") სისტემები, უკრაინაში კი კიევის მეტროპოლიტენისა და ელექტრო მიმწოდებლები კომპანიების („Ukrenergo" და „Kyivenergo") IT ინფრასტრუქტურა. აღნიშნული ვისურის გამო სრულყოფილად ვერ მუშაობენ სარეკლამო გიგანტი ვიპიპი და ფრანგული სამშენებლო მასალების კომპანიები,რუსული ნავთობ კომპანიები ევრაზი და როზნეფტი.

იმის მიუხედავად რომ ეს ვირუსი საქართველოს კონკრეტულად არ შეხებია,და მიუხედავად იმისა რომ სახელმწიფომ არ იცის, რა ტიპის ვირუსია, შესაბამისმა ორგანიზაციებმა მაინც მიიღეს ზომები და Cert-ის მიერ დაიგზავნა შეტყობინებები სხვადასხვა სახელმწიფო უწყებებში,რათა მომზადებულები დახვდნენ აღნიშნულ ვირუსს.პარლამენტის უსაფრთხოების ადმინისტრაციის მიერ მოხდა როგორც ადმინისტრაციის ასევე პარლამენტის თანამშრომლების ინფორმირება,რომ მათ შეეზღუდებოდათ დროებით გარე წყაროებიდან Email-ების მიღების შესაძლებლობა.ასევე ერთ ერთი პრევენციული ზომა რაც იყო მიღებული არის ის,რომ მათ განაახლეს პროგრამული უზრუნველყოფები,თუმცა ეს ზომები მიიღო ზოგიერმა ორგანიზაციამ და არა ყველამ.

სიტუაციური მართვის მენეჯერმა დიმიტრი გუგუნავამ განაცხადა,რომ „როგორც სახელმწიფო,ასევე კერძო სტრუქტურები მოქმედებენ რეაქტიულ რეჟიმში, ვიდრე სტრატეგიულად,რომელიც გულისხმობს რაღაც პრევენციული მექანიზმების შექმნასაც.ეს ირუსი მოსალოდნელია საქართველოშიც გავრცელდეს,რადგან ჩვენ არ ვიცით რა არხებით შეიძლება გავრცელდეს.ჩვენ მივაწოდეთ საზოგადოებას რჩევები რომლის საშუალებითაც შეძლებთ თავი დაიცვათ აღნიშნული ვირუსისგან.“

იუსტიციის სამინისტროს სპეციალისტებმა გასცეს რეკომენდაციები,რომლის საშუალებითაც შესაძლებლობა აქვთ ორგანიზაციებს თავი დაიცვან აღნიშნული ვირუსისგან.ეს რეკომენდაციებია:

საქართველოს იუსტიციის სამინისტროს სსიპ “მონაცემთა გაცვლის სააგენტოს“ სამთავრობო კომპიუტერულ ინციდენტებზე სწრაფი დახმარების ჯგუფი CERT.GOV.GE აღნიშნული შეტევის თავიდან ასაცილებლად გიწევთ რეკომენდაციას:

- ✓ აუცილებელია „ვინდოუსის“ (Windows) სისტემაზე განახლებების დაყენება (ეს არის კრიტიკული ფაქტორი, რომლის უგულებლყოფის შედეგად უამრავი მომხმარებელი ზარალდება);
- ✓ გათიშეთ SMBv1 პროტოკოლი „ვინდოუსის“ თქვენს სისტემაზე და სერვერებზე;
- ✓ რადგან აღნიშნული ვირუსი სხვა სისტემებზე გასავრცელებლად იყენებს WMIC და PSEXEC ხელსაწყოებს, რეკომენდებულია გამორთოთ WMIC-ი (Windows Mnagement Instrumentation Command-Line);
- ✓ ყურადღება გამოიჩინეთ ელ.ფოსტაზე მოსული წერილების მიმართ. დააკვირდით გამომგზავნს, ტექსტს და, რაც ყველაზე მნიშვნელოვანია, მიბმულ დოკუმენტს. ასევე ნუ გადახვალ საეჭვო ბმულებზე;
- ✓ თქვენი ინფორმაციის მაქსიმალური დაცულობისთვის აუცილებელია გადაიტანოთ ეს ინფორმაცია გარე მოწყობილობაზე, რომელიც არ არის თქვენს კომპიუტერთან და ინტერნეტთან შეერთებული;

- ✓ სისტემაზე იქონიეთ ანტი-ვირუსული პროგრამული უზრუნველყოფა (უკანასკნელი განახლებებით).

ჰაკერული თავდასხმების შედეგებზე და პრევენციებზე ნატოს გენერელურმა მდივანმა განაცხადა: „ჰაკერული შეტევის მსხვერპლნი ჯერ მაისში,შემდეგ კი ახლა გავხდით(ივნისი),რაც ჩვენი კიბერ თავდაცვის გაძიერების აუცილებლობას მოწმობს.ჩვენ არა მარტო ალიანსის კიბერ უსაფრთხოების გაძლიერებაზე ვმუშაობთ,არამედ ვეხმარებით მოკავშირეებსაც.უკვე დავიწყეთ კიბერ უსაფრთხოების სამხედრო დომენად ჩამოყალიბებაზე მუშაობა“.

როგორც ცნობილია,ზემოთ აღნიშნულმა ვირუსმა დააზარალა მსოფლიოს უდიდესი კომპანიები,რომელთაც თავიანთი კიბერ თავდაცვა ჰქონდათ,რათა კომპანიები მსგავსი კიბერ შეტევებისგან აერიდებინათ,თუმცა უშედეგოდ.მაგრამ,ახლა გადავხედოთ საქართველოს იუსტიციის სამინისტროს მიერ გაცემულ რეკომენდაციებს. დაგვიცავს კი აღნიშნული რეკომენდაციები ამ უდიდესი ვირუსისგან? ჩემი პასუხია-არა,რადგან ზემოთ აღნიშნული რეკომენდაციები გამოყენებადია ჩვეულებრივი მარტივი კომპიუტერული ვირუსისგან თავის დასაცავად და არა ისეთი მასშტაბური ვირუსისგან, როგორიც Petya გახლავთ.როგორ ფიქრობთ იმ უდიდეს კომპანიებს რომლებზეც შეტევა განხორციელდა არ ექნებოდათ მსგავსი პრევენციის ზომები გათვალისწინებული და მიღებული?რა თქმა უნდა-კი. ამიტომაც ვფიქრობ,რომ ეს შეიძლება ჩაითვალოს იმ ფაქტორად,რომ სახელმწიფომ მიუხედავად იმისა,რომ არ იცის რასთან აქვს საქმე,მოვალეობის მოხდის მიზნით გასცა რეკომენდაციები,რომელიც შესაძლოა სრულიად უსარგებლო აღმოჩნდეს.

6.კვლევის ანალიზი

2017-2018 წლების საქართველოს ეროვნული სტრატეგიის მიხედვით, მთავარი საფრთხე რუსეთის ფედერაცია და რუსული, ორგანიზებული კიბერშეტევები თუ სხვა სახის კიბერ კრიმინალური ქმედებებია. აღსანიშნავია, რომ დოკუმენტში რუსეთი ერთ-ერთ მთავარ საფრთხედ არის მიჩნეული და ნათქვამია, რომ საფრთხის დონე, გასულ წლებთან შედარებით, მომატებულია.საქართველომ ორჯერ შეიმუშავა კიბერუსაფრთხოების პოლიტიკა,პირველი 2014-2016 წელს საქართველოს თავდაცვის სამინისტრომ,ხოლო მეორედ 2017-2018.

ასევე, უნდა აღინიშნოს ის ფაქტიც, რომ საქართველოს კიბერ უსაფრთხოება ორიენტირებული იყო მხოლოდ რუსეთისგან თავდაცვაზე,რომელიც ჩემი აზრით სტრატეგიის დიდი მინუსია, ვინაიდან მხოლოდ ერთი ქვეყნისგან თავდაცვა ვერ შეუქმნის ქვეყანას უსაფრთხოების გარანტიას. თუმცა,ეს შიში გამოწვეულია 2008 წელს მიღებული კიბერ შეტევით,რომელმაც ქვეყნის ინფორმაციული ვაკუუმი გამოიწვია,რომელიც იყო

საერთაშორისო სამართლის დარღვევა რუსეთის მხრიდან,თუმცა ის ფაქტი, რომ საბოლოო დასკვნა და დამამტკიცებელი საბუთი არ არსებობს იმისა რომ ეს რუსეთის მიერ იქნა ჩადენილი და არსებობს მხოლოდ ვარაუდები და ექსპერტების მოსაზრებები,ამიტომაც რუსეთს არანაირი სასჯელი არ მიუღია.

განვითარებადი ქვეყანა,რომელსაც სურს კიბერუსაფრთხოების სფეროში საკუთარი ადგილი დაიმკვიდროს და განვითარდეს,ამ შემთხვევაში ვგულისხმობ საქართველოს,თუმცა პოლიტიკის შემუშავების დროს მხოლოდ ერთ ქვეყანაზე აკეთებს აქცენტს,იგი სხვა ქვეყნებთან მიმართებაში უსუსური იქნება.ჩემი აზრით პოლიტიკა და სტრატეგია ისე უნდა იყოს გათვლილი და შედგენილი,რომ არ იყოს მხოლოდ ერთი ქვეყნისგან თავდაცვაზე ორიენტირებული,არამედ საფრთხე მოსალოდნელია ყველა მხრიდან და საბოლოო ჯამში საიდან მიიღებს ქვეყანა დარტყმას ამის პროგნოზირება შეუძლებელია.

საინტერესოა ის ფაქტი,რომ ისევე როგორც აშშ-ს,ასევე საქართველოს კიბერუსაფრთხოების სტრატეგიას საერთო აქვს ამდენიმე მიზანი,ესენია:

- ✓ ორივე ქვეყანას სურს დაიცვას საკუთარი სახელმწიფო კიბერ შეტევებისგან და თავდახსმებისგან
- ✓ მუდმივად მზადყოფნა და ეფექტიანი ღონისძიებების გატარება პოტენციური კიბერინციდენტების პრევენციის უზრუნველსაყოფად.
- ✓ თანამშრომლობა სახელმწიფო და კერძო უწყებებს შორის,ვინაიდან ამ ორი უწყების თანამშრომლობის გარეშე,თითოეული ცალ ცალკე ვერ გაუმკლავდება კიბერუსაფრთხოების სისტემას.

თუმცა საქართველოს კიბერუსაფრთხოების პირველად შემუშავებულ სტრატეგიაში არაფერი იყო ნათქვამი მისი კომპიუტერული სისტემის,კომპიუტერული ქსელების და იმ გუნდის განვითარება და გაუმჯობესებაზე,რომლებიც მუშაობენ და პასუხისმგებელნი არიან კიბერ სივცრის ოპერაციებზე,კიბერუსაფრთხოებაზე,რომელზე ამერიკის შეერთებული შტატები დიდ ყურადღებას ამახვილებს და უკვე როცა საქართველომ მეორედ შეიმუშავა კიბერუსაფრთხოების სტრატეგია უკვე ჩართული იყო ზემოთ აღნიშნული მიზანი. ვფიქრობ,რომ საქართველომაც უნდა მიაქციოს ამ საკითხს დიდი ყურადღება,ვინაიდან თუ არ იქნება შესაბამისად გადამზადებული კადრები და ორგანოები,მხოლოდ დეპარტამენტების არსებობას აზრი ეკარგება,თუ მისი გამოყენება არ მოხდა საქმისამებრ შესაბამისად.

დღეისათვის,რუსეთის მიერ საქათველოსთან მიმართებით კიბერუსაფრთხოებაში არსებული გარემოებებიდან ირკვევა, რომ:

- ✓ რუსეთის ფედერაციას არ შეუცვლია საკუთარი აგრესიული პოლიტიკა კიბერდომეინში;
- ✓ რუსეთმა უკანასკნელ წლებში მნიშვნელოვნად აამაღლა საკუთარი კიბერშეტევითი შესაძლებლობები;
- ✓ კრემლმა მნიშვნელოვნად დახვეწა კიბერსაშუალებების გამოყენების სპეციფიკა მის მიერვე წარმოებულ ფსიქოლოგიური გავლენის ოპერაციებში;
- ✓ 2008 წელთან შედარებით, მნიშვნელოვნად არის გაზრდილი საქართველოს დამოკიდებულება ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე, რაც, პოტენციური კიბერთავდასხმების შემთხვევაში, მოსალოდნელი ზიანის მასშტაბებს ზრდის.

სახელმწიფო უსაფრთხოებისა და კრიზისების მართვის საბჭოს წარმომადგენელმა ხაზი გაუსვა იმასაც, რომ კიბერუსაფრთხოების სტრატეგიის ფარგლებში, კიბერუსაფრთხოების სფეროში შესაძლებლობების ამაღლების მიზნით, მუშაობა მიმდინარეობს კიბერ რეზერვის შექმნაზე, კიბერკვლევების ლაბორატორიის დაფუძნებასა და სხვა მნიშვნელოვან ღონისძიებებზე,რაც ჩემი აზრით წინ გადადგმული ნაბიჯია საქართველოსთვის.

ექსპერტთა გამოკითხვით გამოიკვეთა შემდეგი საკითხები:

- ✓ განსხვავება კიბერუსაფრთხოებასა და ინფორმაციულ უსაფრთხოებას შორის

ამ თემასთან დაკავშირებით ექსპერტების აზრი ცალსახა იყო,ვინაიდან მათი აზრით ეს ორი გამიჯნულია ერთმანეთისგან,თუმცა ზოგ შემთხვევაში მათ შეიძლება მოიცვან კიდეც ერთმანეთი ან გადაკვეთონ ერთმანეთის გზები.ერთ ერთი ექსპერტის მოსაზრებით:

„ინფორმაციული უსაფრთხოება არის,სახელმწიფოს ეროვნული უსაფრთხოების მნიშვნელოვანი საზრუნავი სექტორი, რომლის ორგანიზების მნიშვნელოვან სტრუქტურებს ქვეყნის სადაზვერვო და კონტრსადაზვერვო სამსახურები წარმოადგენენ“.

მართლაც,რომ ინფორმაციული უსაფრთხოება და კიბერ უსაფრთხოება ალბათ 21-ე საუკუნის უდიდესი საზრუნავია სახელმწიფოებისათვის,ვინაიდან ბოლო დროინდელ კონფლიქტში ყველგან აღმოვაჩენთ კიბერუსაფრთხოების ფენომენის არსებობას და ინფორმაციული უსაფრთხოების მნიშვნელობას.

- ✓ კიბერუსაფრთხოების უზრუნველყოფის კომპონენტები

ამ მხრივ საკმაოდ საინტერესო იყო ის,რომ ექსპერტების მხრიდან გამოიკვეთა კიბერუსაფრთხოების სხვადასხვა კომპონენტები,თუმცა ასევე საინტერესო იყო ის, რომ ერთ-ერთი ექსპერტის მოსაზრებით კიბერუსაფრთხოების უზრუნველყოფის კომპონენტები არ არსებობს 21-ე საუკუნეში.აქვე განვიხილოთ ის კომპონენტები რომლებიც ჩამოთვალეს ესქპერტებმა:

- კიბერსივრცის დაბალანსებული სადაზვერვო და კონტრსადაზვერვო ინფორმაციული აღჭურვისა და სათანადო კონტროლის პროცესი, რომლის მეშვეობითაც შესაძლებელია კიბერსივრცის დაცვა, მათ შორის უცხო სახელმწიფოთა დაზვერვის ობიექტი ქვეყნის სახელმწიფო მოხელეების, მოსახლეობის, კერძო სექტორის სათანადო სასწავლო პროგრამებით აღჭურვის პროცესი.
- ერთის მხარივ, კომპიუტერი, გაშიფვრა და დაცული პირები ან მთავრობა. მეორეს მხრივ, ასევე კომპიუტერი, (ბევრჯერ VPN-ს დამახინჯება, სადაც ცდილობენ ჰაკინგს) და ჰაკერები,რომლებიც ცდილობენ მიიღონ დაცული ინფორმაცია.
- ეროვნული საიდუმლოების დაცვა, ინტელექტუალური საკუთრების დაცვის, ანტი-ჰაკერული ღონისძიებების / ტექნოლოგიების დაცვა.

ფაქტია,რომ მათ მიერ დასახელებული ყველა კომპონენტი არის კიბერუსაფრთხოების უზრუნველყოფის საშუალება,თუმცა ისიც აღსანიშნავია,რომ 21-ე საუკუნეში, მხოლოდ ზემოთ ჩამოთვლილით, საკმაოდ რთულია კიბერუსაფრთხოების უზრუნველყოფა.

- ✓ გეოპოლიტიკის როლი კიბერუსაფრთხოებაში

შეუძლებელია არ შეეხო გეოპოლიტიკა,როდესაც კიბერუსაფრთხოებაზე საუბრობ.ყველაპერი იწყება ქვეყნების მიერ შემუშავებული გეოპოლიტიკით და შესაბამისად ის კავშირშია კიბერუსაფრთხოებასთან.ფაქტია,რომ ექსპერტების აზრით გეოპოლიტიკა მნიშვნელოვან როლს ასრულებს კიბერუსაფრთხოებაში ნებისმიერი ქვეყნისთვის,იგი შეიძლება იცვლებოდეს გეოსტრატეგიული რეგიონების მიხედვით და ასევე მას შეუძლია გავლენა მოახდინოს უცხო ქვეყნების პოლიტიკაზე ან თუნდაც ბიზნესზე.მთავრობები ქმნიან მონაცემებს,რომელიც არის გეოპოლიტიკური სტრატეგიის არსებითი ელემენტი.

„გეოპოლიტიკური ინტერესების შესაბამისად, დაზიანების ობიექტ სახელმწიფოს ან სახელმწიფოთა გაერთიანების წინააღმდეგ დაინტერესებული სადაზვერვო სამსახურები წინასწარ თვლიან კიბერსივრცეში ზემოქმედების მოხდენის მიზნით ძალებისა და საშუალებების, მეთოდებისა და მასშტაბების განსაზღვრას, რომელსაც წინ უსწრებს სათანადო გრიფირების ქვეშსამეცნიერო კვლევები“.

- ✓ კიბერ ომის როლი გეოსტრატეგიული დაპირისპირების ფარგლებში

კიბერუსაფრთხოების როლი გეოსტრატეგიულ კონფროტაციაში ორმაგია,პირველ რიგში არსებობს ცნობილი კიბერ ომი,რასაც მთავრობები აკეთებენ თავიანთი ქვეყნის ინფრასტრუქტურისა და უსაფრთხოების დაცვისათვის.აქვე არის საქმიანობა,რომლეცის მთავრობებმა არ იციან.გარდა ამისა კიბერ ომების განხილვისას,რომლებიც ფარულ ხასიათს ატარებენ,ეს ართულებს გეოსტრატეგიულ ურთიერთობებს,რომელიც ნდობაზეა დამყარებული.თუ ვერ იქნებით ნდობით განწყობილი თქვენი გეოსტრატეგიული მეზობლების მიმართ, ძალიან რთულია, რომ ზოგადად კარგი ურთიერთობები ჰქონდეთ ერთმანეთთან, რაც უფრო დიდ გართულებას შეუწყობს ხელს.

„კიბერ ომი ფსიქოლოგიური ომის შემადგენელია და მის წარმატებით განხორციელებაზეა დამოკიდებული გეოსტრატეგიული დაპირისპირების შედეგი, მათ შორის ფიზიკური ომების მასშტაბების განსაზღვრა და ზოგადად მიზანშეწონილობა“

- ✓ კიბერუსაფრთხოების განმსაზღვრელი ფაქტორები საქართველოში/ამერიკაში

საბოლოო ჯამში,საქართველოში და შეერთებულ შტატებში კიბერუსაფრთხოების ფაქტორები საერთო თემას იზიარებენ და ორივე ქვეყანა ცდილობს საკუთარი სუვერენიტეტის დაცვას.აშშ-სთვის ეს შეიძლება იყოს ჩინელი ან ჩრდილოეთ კორეელი ჰაკერები,რომლებიც ცდილობენ მოიპარონ ფული და გავლენა მოახდინონ კომპანიებზე და მცხოვრებ მოქალაქეებზე.ან თუნდაც რუსი ჰაკერები,რომლებიც ცდილობდნენ კიბერ შეტევა განეხორციელებინათ საპრეზიდენტო არჩევნებზე.საქართველოში ინტერნეტის და ქვეყნის საინფორმაციო სივრცის დიდი ნაწილის დაჰაკვა, ან ახალი ამბების დახურვა.ეს არის ორი განსხვავებული მიზეზი, ისევე როგორც მაგალითები,მაგრამ მაგრამ საბოლოო მიზანი იმ ხალხისაგან, ვინც დაემუქრა აშშ-სა და საქართველოს კიბერ უსაფრთხოებას, ცდილობდნენ ძირი გამოუთხარონ და გაანადგურონ ეს ორი ქვეყანა,დაასუსტონ მათი უსაფრთხოება,გავლენა იქონიონ საერთაშორისო ურთიერთობებზე და ა.შ.

თუმცა, ერთ ერთი ექსპერტი თვლის, რომ საქართველოში კიბერუსაფრთხოების განმსაზრვრელი ფაქტორები არ არსებობს:

„ამერიკაში - სამეცნიერო კვლევებით გამყარებული სადაზვერვო და კონტრსადაზვერვო ოპერატიული კონტროლი და დაგეგმარების პროცესები, საქართველოში.....“

- ✓ საქართველო-აშშ-ს მომავალი ურთიერთობების პერსპექტივები და თანამშრომლობა

გულწრფელად,რომ ვთქვათ ,ეს მთლიანად დამოკიდებულია თუ როგორ განვითარდება სამომავლოდ აშშ-სა და საქართველოს მომავალ ურთიერთობები,თუმცა ძალიან რთულია ამ ყველაფრის ახლა პროგნოზირება.ვაღმოჩნდა,რომ საქართველოს ამ მხრივ მცირე გავლენის მოხდენა თუ შეუძლია,ეს იქნება დამოკიდებული იმაზე,თუ როგორ შეხედავს რუსეთს ტრამპის ადმინისტრაცია.თუ რუსეთ-ამერიკის ურთიერთობები გაიზრდება,ამის გამო შესაძლოა შენარჩუნდეს იგივე მდგომარეობა საქართველოს ურთიერთობებასთან მიმართებაში,ან კიდევ შანსია,რომ ურთიერთობები გაუარესდეს.ხოლო თუ ის ურთიერთობა რომელიც ახლა აქვს საქართველოსა და ამერიკას შენარჩუნება ან კიდევ მომავალში გაიზრდება,კიბერუსაფრთხოებას განვითარების დიდი შანსი აქვს საქართველოში.თუმცა ექსპერტთა აზრით :“ ამ მიმართულებით სასურველია საქართველომ საკუთარი ინტელექტუალური შესაძლებლობებით შექმნას სათანადო ტექნოლოგიები, ქვეყნის სტრატეგიული პარტნიორი სახელმწიფოს ფინანსური მხარდაჭერით“.

- ✓ გახდა თუ არა კიბერუსაფრთხოება საერთაშორისო უსაფრთხოების მთავარ განმსაზღვრელ მიმართულებად

ამ საკითხთან დაკავშირებით ყველას აზრი ერთსულოვანია,ანუ კიბერუსაფრთხოება ერთ-ერთი ყველაზე მნიშვნელოვანი დეტერმინანტია, მონაცემების დაგროვება (მონაცემთა გადამალული ნაციონალური საიდუმლოებები) და სამთავრობო უწყებები, რომლებიც უფრო და უფრო მეტ მონაცემებს იყენებენ მონაცემთა ორიენტირებული ტექნოლოგიით.ბევრი ის ქვეყანა,რომელიც ბევრად წინაა ტექნოლოგიებით,ასევე განვითარებად ქვეყნებში,მთავრობებს აქვთ უამრავი დაცული ინფორმაცია,რომელთა გატეხვასაც ყოველთვის ცდილობენ.ორგანიზაციები,რომლებიც ეძებენ ინფორმაციის თავისუფლებას ყველასათვის,მაგალითად როგორიცაა Wikileaks,ან ანონიმური დაჯგუფებები,რომლებიც იყენებენ ნებისმიერ შესაძლებლობას, რომ გამოამჟღავნონ კერძო ინფორმაცია მსოფლიოსთვის.სამთავრობო და ინდივიდუალურ დონეზე კიბერუსაფრთხოება აუცილებელია, რადგან მას შეუძლია შეინარჩუნოს ჩვენი მთავრობა პირადი ინფორმაციის დაცვაზე, ისევე როგორც ჩვენი პირადი ინფორმაციის დაცვა ოპორტუნისტული ჰაკერებისგან, ქვეყნის შიგნით და გარეთ.

„დიახ, რადგან მაღალტექნოლოგიურ სახელმწიფოებს გააჩნია საშუალებები, სადაზვერვო გადაფარვით სპეცღონისძიებებათა (მათ შორის ფიზიკური ომის) პირობებში საწყის, მიმდინარე და დასკვნით ფაზაში კიბერსივრცის გამოყენების თვალსაზრისით”.

- ✓ შეცვალა თუ არა კიბერუსაფრთხოებამ მსოფლიო ბოლო ათწლეულის განავლობაში

ალბათ,არც ისე რთულია ამ საკითხთან დაკავშირებით ცალსახა პასუხის მოძებნა,ვინაიდან ის რაც 5-10 წლის წინ ზღაპრად ან არარეალობად გვეჩვენებოდა,დღესდღეობით ჩვეულებრივი მოვლენაა კიბერუსაფრთხოების სფეროში.ამიტომაც,კიბერუსაფრთხოებამ მსოფლიო შეცვალა როგორც დადებითად ასევე უარყოფითად. კომპიუტერული სიმძლავრის გაუმჯობესების, ინტერნეტის სიჩქარეების, IP მისამართებით და ინტერნეტის შესახებ უფრო მეტის გაგება, ჩვენი ყოველდღიური დაცვით ინტერნეტში,ამ ყველაფერზე დაყრდნობით, ჩვენი ცხოვრების სტილი იცვლება. ასევე, ჰაკერები, შეიძლება იმყოფებოდნენ რუსეთში, თუმცა მათი IP მისამართი იყოს იოჰანესბურგში, რეიკიავიკთან, სტამბულში, ლონდონში, მადრიდში და შემდეგ ცდილობენ გატეხონ ამერიკული კომპანია.ეს კი უფრო ართულებს ყველაფერს იმ ადამიანებისთვის ვინც კიბერუსაფრთხოების სფეროში მუშაობს და ასევე ეს ნიშნავს იმას რომ ამ ყველაფერმა შეცვალა მსოფლიო.

უარყოფითად შეცვალა იმ მხრივ,რომ იმატა კიბერ შეტევებმა და კიბერ საფრთხეებმა,ქვეყნებს უწევთ მაქსიმალურად გააძლიერონ თავდაცვა უსაფრთხოების შესანარჩუნებლად,თუ ადრე მსგავს რამეზე არც კი იფიქრებდნენ,ახლა ამ საკითხზე გვერდის ავლა ქვეყნის უკუსვლას გამოიწვევს.

დადებითის მხრივ შეცვლა კი არის ის,რომ განვითარდა საზოგადოება ამ სფეროში შეძლებისდაგვარად.რა თქმა უნდა ყველა ქვეყნის კიბერუსაფრთხოება სხვადასხვაგვარია და ათი განვითარების დონეც,თუმცა უნდა აღინიშნოს,რომ კიბერუსაფრთხოება უდიდეს როლს ასრულებს ქვეყნების განვითარებაში იმ მხრივ,რომ იგი გავლენას ახდენს საერთაშორისო ურთიერთობებზე,პოლიტიკაზე,ეკონომიკაზე და სხვა.

7.დასკვნა

საქართველოსა და ამერიკის შეერთებული შტატების კიბერუსაფრთხოების პოლიტიკის განხილვამ გვაჩვენა,რომ ამერიკა მიისწრაფვის იყოს იდეალური და ჰქონდეს იდეალური კიბერუსაფრთხოება,პოლიტიკა,თავდაცვა და ა.შ, ხოლო საქართველო თანდათან სწავლობს, როგორი უნდა იყოს კიბერუსაფრთხოების პოლიტიკა, როგორ უნდა დაიცვას კიბერუსაფრთხოება, ნელ-ნელა ამუშავებს მიდგომებს, აყალიბებს შესაბამის სტრუქტურებს, თუმცა უნდა ვაღიაროთ,რომ კიდევ ბევრის გაკეთება მოგვიწევს რომ ამერიკის შეერთებული შტატების დონემდე მივიდეთ, არამარტო ჩვენ, არამედ სხვა ნებისმიერი ქვეყანას.

კიბერუსაფრთხოება გეპოლიტიკაში ერთ-ერთი მთავარი აქტორია, ვინაიდან სახელმწიფოები სწორედ წინასწარ შემუშავებული გეოპოლიტიკით მუშაობენ, რომელიც დაფუძნებულია კიბერუსაფრთხოებაზე.

კიბერუსაფრთხოება ითვლება 21-ე საუკუნის კონფლიქტების მთავარ მოქმედ აქტორად,რომელმაც შეიძლება გამოიწვიოს კიბერ ომი და თუ მოხდა ამ კიბერ ომის ესკალაცია მაშინ, ის შეიძლება გახდეს მესამე მსოფლიო ომის საფუძველი,ოღონდ ამჯერად არა იარაღის გამოყენებით, არამედ კიბერ დომეინში.

განხილული შემთხვევების შესწავლით და ექსპერტების გამოკითხვით დადასტურდა,რომ კიბერუსაფრთხოება გახდა საერთაშორისო უსაფრთხოების განმსაზღვრელი ფაქტორი და ყველა სახელმწიფო მასზეა დამოკიდებული.

ასევე გამოიკვეთა ის ფაქტი,რომ კიბერუსაფრთხოებამ რადიკალურად შეცვალა მსოფლიო 21-ე საუკუნეში. თითქმის ყველა განვითარებული თუ განვითარებადი სახელმწიფო გადართული ქსელურ სისტემებზე,კომპიუტერულ მომსახურებაზე და კომპიუტერულ სისტემებზე,როცა ადრე ამაზე ფიქრიც კი წარმოუდგენლად ეჩვენებოდა სამყაროს.

საბოლოო ჯამში,მიუხედავად იმისა,რომ ყველა სახელმწიფო ცდილობს ჰქონდეს საუკეთესო და დაცული კიბერუსაფრთხოება, ამ ყველაფრის უზრუნველყოფა შეუძლებელია, ვინაიდან, ისე იცვლება კომპიუტერული სისტემები და ქსელები, ისე ვითარდება ინტერნეტი, რომ ეს ყველაფერი ერთად კიბერუსაფრთხოების სტაბილუობის შესაძლებლობას არ იძლევა.

8.უცხო ტერმინთა განმარტება

- ✓ ინფორმაციული უსაფრთხოება-საერთაშორისო სტანდარტები, ინფორმაციულ უსაფრთხოებას განსაზღვრავს, როგორც ინფორმაციის კონფიდენციალობის დაცვას,მთლიანობას და ხელმისაწვდომბა.
- ✓ კონფიდენციალური ინფორმაცია – ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას, სავარაუდოდ, მოჰყვება კრიტიკული ინფორმაციული სისტემის სუბიექტის ფუნქციებისათვის მნიშვნელოვანი ზიანი და რომლის კონფიდენციალურ ინფორმაციად კლასიფიცირების მიზანია ინფორმაციული აქტივების მართვის წესების უზრუნველყოფა, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას.
- ✓ კიბერსივრცე-კიბერსივცრე არის გარემო სადაც ხდება კომპიუტერული ქსელების კომუნიკაცია,ეს სიტყვა პოპულარული გახდა 1990 წლიდან.იგი ასოცირდება კომპიუტერთან და ინტერნეტის სხვადასხვა კულტურებთან.
- ✓ კიბერუსაფრთხოება-„კიბერ“ -ბერძნული წარმოშობის ზმნაა -“kybereo” ნიშნავს-მართვას,გაძღოლას,გაკონტროლებას.1940 წლიდან ამერიკელმა მათემატიკოსმა Norbert Wiener-მა(1894-1964) დაიწყო ამ სიტყვის გამოყენება,რათა დაეხასიათებინა კომპიუტერული სისტემა.კიბერუსაფრთხოება არის ერთობლიობა ინსტრუმენტების,პოლიტიკის,უსაფრთხოების კონცეფციის ,რისკის მართვის,ტექნოლოგები და გარანტიები,რომლებიც გამოყენებული იქნება დაიცვა კიბერ გარემო და ორგანიზაციები და ასევე მომხმარებლის აქტივობები.
- ✓ International telecommunications union(ITU)- არის გაეროს სპეციალიზებული სააგენტო საინფორმაციო და საკომუნიკაციო ტექნოლოგიების შესახებ.
- ✓ (ICT-Information and communications technology)-საინფორმაციო და საკომუნიკაიო ტექნოლოგიები.
- ✓ კიბერ დანაშაული-კიბერდანაშაული გულისხმობს ყველა იმ ქმედებას, რომელიც ხორციელდება კიბერსივრცეში დანაშაულებრივი განზრახვით.
- ✓ კიბერ თავდაცვა-კიბერ თავდაცვაა, როდესაც სახელმწიფოები უზრუნველყოფენ კიბერ უსაფრთხოებას,ხდება კიბერ შეტევების კონტროლი,მისი აღმოჩენა და აღმოფხვრა.
- ✓ კომპიუტერული ინციდენტი – ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას.

- ✓ კიბერუსაფრთხოების პოლიტიკა-განსაზღვრავს საქართველოს თავდაცვის სფეროს მიდგომებსა და პრიორიტეტებს კიბერუსაფრთხოების მიმართულებით და განსაზღვრავს ყველა იმ სტრატეგიულ მიზანს, რომელთა აღსრულებაც განაპირობებს თავდაცვის სფეროს საიმედო, ეფექტურ, სტაბილურ და უსაფრთხო ფუნქციონირებას, რაც თავისთავად ქმნის ეროვნული უსაფრთხოების მყარ საფუძვლებს
- ✓ კიბერ შეტევა-ჰაკერების მცდელობა დააზიანონ ან გაანადგურონ კომპიუტერული ქსელი ან სისტემა.
- ✓ CIA-Central Intelligence Agency- ცენტრალური სადაზვერვო სააგენტო,წარმოადგენს ამერიკის შეერთებული შტატების ფედერალური მთავრობის სამოქალაქო სადაზვერვო სამსახურს, რომელიც მიზნად ისახავს მსოფლიოს უსაფრთხოების ინფორმაციის შეგროვებას, დამუშავებას და ანალიზს.
- ✓ (NSC)-National Security Council of Georgia-საქართველოს ეროვნული უშიშროების საბჭო,წარმოადგენს საქართველოს მთავარ საკონსულტაციო ორგანოს.
- ✓ ფიშინგი-ფიშინგი არის კიბერთაღლითობის გავრცელებული ფორმა, რომლის მიზანია მსხვერპლს მოტყუების გზით მოპაროს სენსიტიური ინფორმაცია ან მოახდინოს კომპიუტერის კომპრომეტაცია. შეტევის დროს გამოიყენება მეილი, რომელიც იგზავნება კიბერ-კრიმინალების მიერ.
- ✓ კიბერ ომი- ერი-სახელმწიფოების ქმედებები სხვა ქვეყნის კომპიუტერების ან ქსელებში შეღწევის, ზიანის ან დაზიანების გამომწვევი მიზეზების გამო.
- ✓ ჰაკინგი-კიბერ სამყაროში პერსონა რომელსაც შეუძლია გამოიკვლიოს სისტემის სისუსტეები და გამოიყოს მისი მიზნის შესასრულებლად (ცუდი თუ კარგი) არის ცნობილი როგორც ჰაკერი. და ის რითიც არის დაკავებული ამას ჰქვია ჰაკინგი.
- ✓ კიბერუსაფრთხოების ბიურო – საქართველოს თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი (შემდგომ – კიბერუსაფრთხოების ბიურო).
- ✓ DNC- Democratic National Committee- დემოკრატიული ეროვნული კომიტეტი.
- ✓ DNS-ჩვენს ინტერნეტ პროვაიდერს გააჩნია თავისი DNS-ი,უფრო ზუსტად რომ ვთვათ ჩანაწერების წიგნი.

9.რეკომენდაციები

ჩემი აზრით, კიბერუსაფრთხოების მაქსიმალურად განვითარებისთვის და იმისათვის,რომ მაქსიმალურ წარმატებას მიაღწიოს ქვეყანამ კიბერუსაფრთხოებაში აუცილებელია შემდეგი:

- ✓ აუცილებელია მაქსიმალურად მოქნილი, თვალსაჩინო და გამჭირვალე კიბერუსაფრთხოების კონცეფცია, რომელიც მაქსიმალურად წარმოაჩენს საქართველოს ინტერესებს კიბერუსაფრთხოების მხრივ, ასევე კიბერუსაფრთხოებას სხვა ქვეყნებთან მიმართებაში.

- ✓ აუცილებელია ორგანიზებული, განვითარებული და მაქსიმალურად უახლესი ტექნოლოგიით აღჭურვილი ჯგუფი,რომელიც დაიცავს ქვეყანას კიბერ შეტევებისგან, განავითარებს მას კიბერ უსაფრთხოების მხრივ და ხელს შეუწყობს რომ მსოფლიო მასშტაბით მნიშნელოვანი ფიგურა.

- ✓ ისეთი ორგანიზაციების განვითარება, რომელიც მუდმივად იმუშავებს კიბერუსაფრთხოების კონცეფციის დამუშავებაზე და მუდმივ განვითარებაზე.

- ✓ ორგანიზაციების არსებობა,რომელიც მუდმივად თვალყურს ადევნებს კიბერ შეტევების საფრთხეების არსებობას,მის კონტროლს და უზრუნველყოფს მის შესწავლას.

- ✓ დღევანდელი საუკუნე ყველასთვის ცნობილია ინფორმაციულ და კომპიუტერულ საუკუნედ.სწორედ ამიტომაც კიბერუსაფრთხოებაზე მომუშავე ორგანიზაციებმა უნდა უზრუნველყონ ინფორმაციის მაქსიმალური დაცულობა.

- ✓ კიბერუსაფრთხოებასთან მომუშავე ჯგუფს აუცილებლად უნდა შეეძლოთ სწრაფად რეაგირება,მუდმივად განვითარების შესაძლებლობა და მოქნილობა.

- ✓ აიტი აუდიტისა და შემოწმებების კულტურა ორგანიზაციებში.

- ✓ კომპიუტერული განახლებებისა და განახლებული პროგრამების აუცილებლობის დამკვიდრება.

10.ბიბლიოგრაფია

1.https://www.state.gov/r/pa/prs/ps/2017/05/270754.htm

2.http://searchsecurity.techtarget.com/definition/information-security-infosec

3.http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

4. CYBERSECURITY -National Strategy,Roles, andResponsibilities Needto Be Better Defined and More Effectively Implemented- Report to Congressional Addressees- United States Government Accountability Office.(GAO-13-187).

5. The Russian Military and the Georgian War: Lessons and Implications- Ariel Cohen and Robert E. Hamilton(Current Politics and Economics of Russia … ISSN: 1057-2295 Volume 28, Number 1 © Nova Science Publishers, Inc.

6. Cyber War-The Next Threat to National Security and What to Do About It Richard A. Clarke and Robert K. Knake.

7. Protecting Critical Infrastructure-Robert M. Clark *Series Editors:* Simon Hakim · Erwin A. Blackstone · Robert M. Clark

8. 2016 Cybersecurity Report-www.cybersecurityobservatory.com
9. The National Strategy to Secure Syber Space-The White House,Washington.
10. The Department of Defense(DOD) Cyber Strategy-April,2015 .
11. www.elsevier.com/locate/comphumbeh(Computers in Human Behavior 48 (2015) 51–61)
12. FISMA Blog Post Federal Cybersecurity: Administration Releases Annual Report on Agency Cyber Performance By: Grant Schneider
13. Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It Marc Goodman (Doubleday, 2015), 392 pp., index Reviewed by Jay R. Watkins.
14. Federal Information Security Modernization Act of 2014
Annual Report to Congress-Fiscal Year 2016
15. Georgia 2008:legal evaluation according to Georgian and international law -Gvantsa Grigolia
16. Cyber Security Evaluation Tool- National Cybersecurity and
Communications Integration Center
17. საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ- ვებგვერდი, 19/06/2012 სარეგისტრაციო კოდი 140000000.05.001.016807
18. PUBLIC LAW 113–283—DEC. 18, 2014 128 STAT. 3073
19.ინფორმაციის თავისუფლების განვითარების ფონდი-
კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა-პოლიტიკის დოკუმენტი,22აგვისტო,2016.

20. https://www.slideshare.net/vikashnsingh/isis-50885565
21. http://geotimes.ge/blogi/index.php?m=82&post_id=18
22. http://csbd.gov.ge/news.php?news_number=1&news_type=publications&lang=ge
23. http://csbd.gov.ge/news.php?news_number=2&news_type=publications&lang=ge
24. http://netgazeti.ge/technology/22132/
25. http://www.resonancedaily.com/mobile/index.php?id_rub=11&id_artc=29953
26. https://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/
27. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/a-rundown-of-the-biggest-cybersecurity-incidents-of-2016
28. https://en.wikipedia.org/wiki/List_of_cyberattacks
29. https://www.checkmarx.com/2016/09/11/august-2016-hacks-8-largest-hacks-breaches-cyber-incidents/
30. https://idfi.ge/ge/informational-war-of-kremlin-against-georgia-the-necessity-of-having-state-policy-against-propaganda
31. http://cyber.kvira.ge/9981/
32. https://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War#Attacks
33. https://matsne.gov.ge/ka/document/view/1679424
34. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region&region=top-news&WT.nav=top-news&_r=0
35. http://time.com/4600177/election-hack-russia-hillary-clinton-donald-trump/
36. https://www.webpagefx.com/data/cost-of-hackers-in-the-us/
37. http://experti.ge/statiebi1993_sainformacio_omi_pirevli11.htm
38. http://cyber.kvira.ge/17088/
39. http://cyber.kvira.ge/9635/
40. http://geotimes.ge/blogi/index.php?m=82&post_id=18