კავკასიის საერთაშორისო უნივერსიტეტი

ოთარი ჭოხონელიძე

ევროკავშირის როლი კიბერუსაფრთხოების განვითარების საქმეში: გამოწვევები და მათთან ბრძოლის სტრატეგიები

საერთაშორისო ურთიერთიერთობებისა და საერთაშორისო უსაფრთხოების სამაგისტრო პროგრამა

სამაგისტრო ნაშრომი შესრულებულია სოციალურ მეცნიერებათა მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

სამაგისტრო ნაშრომის ხელმძღვანელი:

სოციალურ მეცნიერებათა დოქტორი, სრული პროფესორი

ვალერი მოდებაძე

თბილისი 2018 წელი

ანოტაცია

კიბერსივრცე ადამიანების ცხოვრების ნაწილი გახდა, მასზე დამოკიდებული ხდება ფაქტობრივად ყველაფერი, რაც კომფორტულს ხდის ამა თუ იმს სერვისის, ტექნოლოგიის და ა.შ. გამოყენებას. რაც დრო გადის ყველა სფერო ხდება ინფორმაციულ ტექნოლოგიებზე დამოკიდებული, შესაბამისად ნებისმიერ სერვისს, ტექნოლოგიებს, ბიზნესებს, ორგანიზაციებს და ა.შ. ყველაფერს რაც მუშაობს ქსელთან დაკავშირებული, ჭირდება დაცვა კიბერშეტევებისგან, პროგრამული გაუმართავობისგან ან უბრალოდ ადამიანური ფაქტორისგან, სწორედ ამისთვის არსებობს კიბერუსაფრთხოება, რომლის მიზანია უსაფრთხო გახადოს ნებისმიერი სახის ოპერაცია ინტერნეტ თუ შიდა ქსელებში.

ნაშრომში განხილულია კიბერუსაფრთხოება დაწყებული ინტერნეტის საწყისიდან, როგორ ვითარდებოდა, რა მომენტიდან გახდა საჭირო და აქტუალური, ასევე აღწერილია კიბერ საფრთხეების ტიპები. წარმოდგენილია შესაბამისი მაგალითები იოლად აღქმის მიზნით. მასალა გათვლილია როგორც გაცნობითი მიზნისთვის ასევე ანალიზისთვის. გავეცნობით ინფორმაციული ომის არსს, მის ტიპებს და ამ მხრივ ევროპაში არსებულ მდგომარეობას.

ძირითადი აქცენტი გავლებულია ევროკავშირზე და მის მიერ გატარებულ კიბერ პოლიტიკაზე. სრული ანალიზია ევროპაში არსებულ განვლილ და დღევანდელ მდგომარეობაზე კიბერუსაფრთხოების კუთხით. წარმოდგენილია და განხილულია ევროკავშირის და ევროკავშირის ქვეყნების სტრატეგიები და პროექტები.

ძირითად მიზანს წარმოადგენს სრული მასალის ანალიზის შედეგად რეკომენდაციების და ალტერნატიული გზების შემუშავება.

Annotation

Cyberspace has become a part of people's lives, actually everything depends on it, which makes it convenient to use service, technology, etc. As time goes, as time passes, all areas are going to depend on information technologies. Therefore any kind of service, technology, businesses, organizations, etc. Everything that works on the network requires protection from cyber-attacks. Software malfunction or just a human factor, that is why exists cyber-security, the aim of which is to make safe any kind of operation in the Internet or internal networks.

The paper deals with cyber-security starting from the beginning of the Internet, How was it evolved from what moment it became necessary and actual. The types of cyber threats are also described. Presented relevant examples for easy understanding. The material is intended for an introductory purpose as well as for analysis. We will take a look at the essence of the information war, the types and the situation in Europe in this regard.

The main focus is on the EU and its cyber policy. It is a complete analysis of the past and current situation in Europe in terms of cyber-security. There are presented and discussed

The strategies and projects of EU and EU countries.

The main goal is to develop recommendations and alternative ways as a result of analysis of the full material.

European Union role in cyber-security development: Challenges and strategies to combat them

Otari Tchokhonelidze

შინაარსი

შესავალი

კიბერუსაფრთხოება, კიბერდანაშაული, კიბერტერორიზმი, კიბერთავდასხმა ეს ის ტერმინებია რომლებიც რამდენიმე ათეული წლის წინ ფანტასტიკის სფეროს წარმოადგენდა. ინტერნეტის შექმნამ და გავრცელებამ სრულად შეცვალა არსებული რეალობა, მან სრული რევოლუცია მოახდინა თითქმის ყველა სფეროში, თუ კი ინტერნეტს გარკვეული კატეგორია საწყისში სკეპტიკურად უყურებდა, დღესდღეობით ყველა თანხმდება რომ ეს არის დიდი ნაბიჯი ნებისმიერი სფეროს განვითარებისკენ. რაც დრო გადის ყველა ტექნოლოგია ნელნელა ხდება ინტერნეტზე დამოკიდებული, სხვადასხვა სერვისები, მათ შორის სახელმწიფო სერვისებიც ხდება ონლაინში და ეს ყველაფერი ძალიან პრაქტიკულია, თუმცა ინტერნეტზე დამოკიდებულებამ წარმოაჩინა მეორე მხარეც, რაც უფრო განვითარდა ეს სფერო, გამოჩნდნენ ადამიანები რომლებმაც შეისწავლეს მისი სუსტი მხარეებიც, აღმოჩნდა რომ შესაძლებელი იყო ინტერნეტის საშუალებით მასზე დაკავშირებულ სხვადასხვა კომპიუტერულ მოწყობილობებში შეღწევა კომპიუტერული თავდასხმების (კიბერშეტევების) შედეგად, კიბერსაფრთხეების აქტუალობამ გამოიწვია მის წინააღმდეგ ბრძოლის საჭიროება, კიბერშეტევებისგან თავდაცვას ეწოდება კიბერუსაფრთხოება. რაც დრო გადის კიბერუსაფრთხოება უფრო აქტუალური ხდება, მიუხედავად იმისა რომ ამ სფეროში მრავალი განვითარებული ქვეყანა დაიხვეწა,

ისინიც კი ვერ უზრუნველყოფენ სრულ დაცვას, მითუმეტეს მესამე მსოფლიოს ქვეყნები. ევროკავშირში კიბერუსაფრთხოების განვითარებას დიდ ყურადღებას უთმობენ, ეს თემა მუდმივ აქტუალურია, უფრო მეტიც მისი აქტუალობა იმატებს დროის გასვლასთან ერთად, იქედან გამომდინარე რომ კომპიუტერული ტექნოლოგიების განვითარებასთან ერთად არა მარტო კიბერუსაფრთხოების მეთოდები ძლიერდება, არამედ კიბერთავდასხმის მეთოდებიც. მიუხედავად იმისა რომ ევროკავშირი აქტიურად ცდილობს ამ საკითხის მოგვარებას, შემუშავებული აქვს სხვადასხვა სტრატეგიები და პროექტები, საბოლოო გეგმა მაინც ვერ შეადგინეს ჯერ კიდევ, ევროკავშირში სხვადასხვა კონფერენციებზე კიბერსაფრთხეებს გამოყოფენ როგორც ყველაზე აქტუალურ საფრთხეს, სწორედ ამიტომ ეს თემა ძალიან აქტუალურია და პრაქტიკული გეგმის შემუშავება ყველაზე პრიორიტეტულია.

აღნიშნული კვლევის კითხვებს წარმოადგენს:

- რამ გამოიწვია კიბერუსაფრთხოების სფეროს შექმნა და განვითარება?
- რა სახის კიბერსაფრთხეები არსებობს და როგორია მათ წინააღმდეგ ევროკავშირის პოლიტიკა?
- არის თუ არა კიბერუსაფრთხოების სახელმწიფო სტრატეგიები და ევროკავშირის სტრატეგია ეფექტური პრაქტიკაში?
- რა მეთოდებით შეიძლება ამ სფეროს გაძლიერება?

კვლევაში გამოყენებული თვისობრივი კვლევის მეთოდების: ისტორიული ანალიზის, დესკრიფციული ანალიზის, კონტენტ ანალიზის, SWOT ანალიზის და case study-ს შესწავლის საფუძველზე კვლევის მიმდინარეობისას გამოიკვეთა ისეთი ამოცანები როგორებიცაა:

- პირველი კიბერსაფრთხეების და კიბერუსაფრთხოების წინაპირობის მიმოხილვა.

- კიბერსაფრთხეების ანალიზი და კიბერუსაფრთხოების გამოწვევების წარმოჩენა.
- ევროკავშირის წევრი ქვეყნების და ევროკავშირის კიბერუსაფრთხოების სტრატეგიების მიმოხილვა.
- ევროკავშირის კიბერსივრის მომავალი გამოწვევების წარმოჩენა და რეკომენდაციების შემუშავება.

კვლევის მეთოდოლოგია მოიცავს „ძალთა ბალანსის თეორიას“ , „კიბერშეტევების თეორიას“ (Rui Zhuang Alexandru G. Bardas Scott A. DeLoach Xinming Ou), „კიბერუსაფრთხოების მეცნიერების თეორიას“ (D, McMorrow).

საკითხის კვლევისას დასმული კითხვებისა და ამოცანების შესწავლის შემდეგ, რომელიც მიღწეულ იქნა საკვლევი მეთოდების, ანალიზისა და კვლევის მეთოდოლოგიის ხარჯზე გამოიკვეთა **თემის ჰიპოთეზა:**

საფრთხეები კიბერსივრცეში მსოფლიოსთვის სრულიად ახალი გამოწვევაა, მისი განვითარება დაიწყო კიბერსივრცის შექმნიდანვე, რაც წლები გადიოდა გამოჩდნა საჭიროება დაარსებულიყო კიბერუსაფრთხოების კუთხით ინსტრუმენტები, სტრატეგიები, უნარჩვევების და ცნობიერების ჩამოყალიბება. ციფრული სამყაროს განვითარებამ გამოიწვია ყველა სფეროს მასთან დაკავშირება, დღესდღეობით ეს კავშირი იმდენად მჭიდროა, ერთი მეორეს გარეშე წარმოუდგენელი ხდება.

კიბერუსაფრთხოების ჩამოყალიბების და საბოლოო ფორმის მიცემის საჭიროება უდაოა, არ არსებობს სფერო რომელსაც არ ჭირდება კიბერ საფრთხეებისგან დაცვა, რომლებშიც პირველ რიგში იგულისხმება კიბერშეტევები, თუმცა ასევე არსებობს პროგრამული უზრუნველყოფის „ბაგები“ და ასევე ადამიანური ფაქტორიც.

მსგავსი პრობლემების ფონზე რამდენიმე ამოცანა დგას ევროკავშირის წინაშე, ეს არის კიბერუსაფრთხოების მაქსიმალური განვითარება, რაც უნდა მოხდეს რაც შეიძლება სწრაფად, წინააღმდეგ შემთხვევაში ვერ დაეწევიან ტექნოლოგიურ განვითარებას, კიბერუსაფრთხოების განვითარებაში არამარტო პროგრამული და ტექნიკური კუთხით დაცვა იგულისხმება, არამედ აუცილებელია უნარების მუდმივი

გაძლიერება, ხოლო ყველა სახელმწიფო სექტორებში და ყველა პიროვნებაში კიბერუსაფრთხოების კუთხითცნობიერების ამაღლება.

ნაშრომში განხილული იქნება პირველადი საფრთხეები და პირველადი დაცვის საშუალებები, კიბერსაფრთხეების სხვადასხვა ფორმები, კიბერდაპირისპირებების ფორმები. მოყვანილი იქნება კონკრეტული მაგალითები სხვადასხვა მოტივაციით გაკეთებული შეტევების. წარმოვაჩენ ინფორმაციული ომის რაობას, ინფორმაციული წყაროების გამოყენებას ტერორისტული ორგანიზაციების მიერ და ასევე რუსეთ-ევროკავშირის ინფორმაციულ დაპირისპირებას.

ნაშრომში ძირითადი აქცენტი კეთდება ევროკავშირის გამოწვევებზე, შესაბამისად განხილული იქნება ცალკე ევროკავშირის კიბერუსაფრთხოების კუთხით მომუშავე სააგენტოები: ევროკავშირის ინფორმაციის და ქსელების უსაფრთხოების სააგენტო - ENISA, ევროპის კიბერდანაშაულის ცენტრი - EUROPOL/EC3, ევროპის თავდაცვის სააგენტო - EDA. განვიხილავ ევროკავშირის ქვეყნების სახელმწიფო კიბერუსაფრთხოების სტრატეგიებს რომლების ოფიციალურად არის გამოქვეყნებული 2018 წლის ივნისის ჩათვლით. ბევრი ვიფიქრე მომეყვანა რამდენიმე მაგალითი თუ ევროკავშირის ქვეყნების ყველა არსებული სტრატეგია, თუმცა ვინაიდან ამ ნაშრომის მიზნებია გაცნობითი სახის ქონა და ასევე ანალიზი, ყველა ქვეყნის მაგალითი შეიძლება გამოსადეგი იყოს, მოყვანილი იქნება ეროკავშირის წევრი ქვეყნების სახელმწიფო კიბერუსაფრთხოების სტრატეგიების მხოლოდ ძირითადი მომენტები.

ცალკე განიხილება ევროკავშირის კიბერუსაფრთხოების სტრატეგია, რომელსაც წესით უნდა მოერგოს ყველა წევრი ქვეყნების სტრატეგიები, თუმცა დღევანდელი მდგომარეობით ფიზიკურად არ არსებობს ერთი კონკრეტული მოდელი.

ბოლო თავი მიეძღვნება მიმდინარე და სამომავლო კიბერსაფრთხეებს და პრაქტიკულ რეკომენდაციებს.

ნაშრომის საბოლოო მიზანია ამ ყველა სტრატეგიების და ამოცანების ფონზე წარმოვაჩინოთ როგორია მდგომარეობა პრაქტიკაში, რეალურია თუ არა დასახული მიზნებით გამოწვევების აღმოფხვრა და რაც მთავარია ალტერნატიული სტრატეგიების განხილვა რეკომენდაციების სახით.

სამაგისტრო ნაშრომის შესრულებისას მასალები და წყაროები შეირჩა შემდეგი კრიტერიუმებით:

- საიმედოობა (ოფიციალური წყაროები)
- კომპეტენტურობა
- საერთაშორისო (ევროკავშირის) წყაროებზე ძირითადი აქცენტის გადატანა

ნაშრომში გამოყენებული ლიტერატურიდან შეიძლება განვიხილოთ შემდეგი ნამუშევრები:

1) **The history of cyber security — everything you ever wanted to know**

ტექსტში განხილულია კიბერუსაფრთხოების საწყისები, დაწყებული ნულიდან, თუ რამ გამოიწვია კიბერუსაფრთხოების საჭიროება და როგორ ვითარდებოდა ის.

2) **ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები და რეკომენდაციები. საქართველოს კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები (კრებული) - ვლადიმერ სვანაძე**

ეს ერთადერთი ქართულ ენაზე შესრულებული მასალაა, რომელიც ჩავთვალე ღირებულად ნაშრომში გამოსაყენებლად, ეს არის მოზრდილი კრებული, რომელიც ზოგად დონეზე განიხილავს კიბერუსაფრთხოებას როგორც ევროკავშირში ისე საქართველოში.

3) **Strategic Defence for Russia's Undeclared Information War on Europe - Salome Samadashvili**

კიდევ ერთი ქართველის მიერ შესრულებული მასალა ინგლისურ ენაზე, რომელიც ძალიან გამომადგა ინფორმაციულ ომზე წერისას.

4) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

ეს არის ევროკავშირის კიბერუსაფრთხოების სტრატეგია, რომელიც პირდაპირ კავშირშია ამ ნაშრომში და მის ყველა ასპექტში იყო გამოსადეგი.

I თავი - კიბერსაფრთხეები, კიბერუსაფრთხოება და ინფორმაციული ომი როგორც მისი შემადგენელი ნაწილი

თანამედროვე ცხოვრებაში ისეთი ტერმინები როგორებიცაა: კიბერუსაფრთხოება, კიბერსივრცე, კიბერტერორიზმი და ა.შ. ყველას სმენია, მაგრამ სულ რამდენიმე ათეული წლის წინ ეს სფერო საერთოდ არ არსებობდა. მეტიც, რამდენიმე ათეული წლის წინ პრაქტიკულად გამოყენებადი კომპიუტერებიც არ არსებობდა, ასე რომ ეს მიმართულება ჯერ კიდევ ახალგაზრდაა და სწორედ ახლა მიმდინარეობს მისი განვითარება.

1970-80 წლების დასაწყისშიც ხდებოდა „კომპიუტერული დანაშაულები“, მაგრამ ეს შემოიფარგლებოდა ძირითადად, კომპიუტერულ მოწყობილობებთან პირადი ურთიერთობისას თუ კი ვინმე ნახავდა/წაიკითხავდა ისეთ რამეს რაც არ უნდა

ენახა/წაეკითხა. მართალია ინტერნეტის შექმნის პირველი მცდელობები ჯერ კიდევ 60-ანი წლების დასაწყისში დაიწყო, თუმცა როგორც ასეთი ჩამოყალიბება დაიწყო 80-ანი წლების დასაწყისში და 1985 წელში შეიძლება ითქვას უკვე ჩამოყალიბებული ქსელის სახე მიიღო.

კიბერუსაფრთხოების წარმოშობის საწყისი მიზეზად შეიძლება ჩაითვალოს ჯერ კიდევ 1971 წელს მომხდარი ფაქტი, როდესაც გერმანელი ჰაკერი ბობ ტომასი (Bob Thomas) მიხვდა რომ ქსელის (ARPANET რომელიც ინტერნეტის ერთგვარი წინაპარია) საშუალებით შესაძლებელი იყო პროგრამის გავრცელება, რომელიც დაძვრებოდა არფანეტის ქსელში და ყველგან ტოვებდა გარკვეულ კვალს, ეს იყო ტექსტი: "I'M THE CREEPER: CATCH ME IF YOU CAN." – „ მე ვარ მხოხავი: დამიჭირე თუ შეგიძლია". ეს იყო პირველი ვირუსი. რეი ტომლინსონმა (Ray Tomlinson) ნახა ეს

იდეა, მოეწონა, ცოტა შეცვალა რომ პროგრამას შეძლებოდა გამრავლება, სწორედ ასე მივიღეთ პირველი გამრავლებადი ტიპის „ჭია" – "Worm" ვირუსი, ვირუსის სახეობა

რომელიც ყველაზე გავრცელებულია ინტერნეტში. მალევე მან დაწერა კიდევ ერთი პროგრამა

სახელად „Reaper" - მკვლელი, რომლის მიზანიც იყო Creeper-ის მოძებნა და მისი წაშლა/განადგურება. ეს იყო პირველი ანტივირუსი. ამავე ადამიანმა შექმნა ელექტრონული ფოსტა - Email.[1]

1985 წლიდან შესაძლებელი გახდა ნელნელა ქსელი მსურველებზე გავრცელებულიყო, ინფორმაციული გაცვლების მიზნით, ფაქტობრივად ინტერნეტის საწყისთან ერთად გამოჩნდნენ ადამიანები რომლებმაც დაინახეს მისი სისუსტეებიც და ამის სათავისოდ გამოყენება დაიწყეს. მაგალითად რუსები ერთერთი პირველები

[1] First computer virus of Bob Thomas - Georgi Dalakov

იყვნენ ვინც დაინახეს კიბერ სივრცის პოტენციურ თავდასხმის იარაღად გამოყენების შესაძლებლობა და ადრეულ წლებშივე დაიწყეს შესაბამისი კვლევები და ექსპერიმენტები.

პირველ რიგში ჰაკერობა გულისხმობდა ინფორმაციის მოპარვას. 1986 წელს გერმანელმა ჰაკერმა მარკუს ჰესმა გატეხა სერვერი კალიფორნიაში ბერკლიში, საიდანაც გატეხა 400მდე სამხედრო კომპიუტერი, მისი მიზანი იყო ინფორმაცია მიეყოდა KGB-თვის, თუმცა მას საბოლოოდ მიაგნეს, როდესაც ასტრონომმა კლიფორდ სტოლმა შეამჩნია საეჭვო მოქმედებები.

1988 წელს რობერტ მორისს გაუჩნდა იდეა გაეზომა ინტერნეტი, ამისთვის მან დაწერა პროგრამა/ვირუსი ჭია (worm,) სადაც მან დაუშვა შეცდომა, ეს ვირუსი იმდენად გავრცელდა მოიცვა სრულად ინტერნეტი და სერიოზული ზიანი მიაყენა მას, ინტერნეტი ძალიან შენელდა. ეს იყო ადამიანი რომელიც პირველად დაჯარიმდა ინტერნეტში მოქმედების გამო.[2]

1.1 კიბერდანაშაულები სახეები და მათი მოქმედების მეთოდები

კომპიუტერული და მობილური ქსელების საიმედო და გამართული მუშაობა არის ძალიან მნიშვნელოვანი ფაქტორი როგორც სახელმწიფოსთვის, ასევე მოქალაქეთათვის, მან შეიძლება ნებისმიერ მიმართულებაზე იქონიოს გავლენა, როგორიცაა სახელმწიფო ეკონომიკა, მოქალაქეთა ეკონომიური მდგომარეობა, სახელმწიფო და კერძო სერვისების მუშაობა და ა.შ. ქსელების გამართული

[2] The history of cyber security — everything you ever wanted to know

https://www.sentinelone.com/blog/history-of-cyber-security/

ფუნქციონალურობის დარღვევა შეიძლება გამოწვეული იყოს მრავალი ფაქტორით: კიბერშეტევები, მოწყობილობების ფიზიკური დაზიანება, პროგრამული უზრუნველყოფის მუშაობის დარღვევა, ადამიანის დაშვებული შეცდომები და ა.შ.

მრავალი მიზეზი შეიძლება იყოს თუ რა მიზეზით დაირღვა ქსელების გამართული მუშაობა და ეს ნათლად გვაჩვენებს თუ რამდენად მრავალფეროვანი და იოლია მისი მდგომარეობიდან გამოყვანა, შესაბამისად სახელმწიფოში ქაოსის გამოწვევა. ეს ნათელი მაგალითია რამდენად დამოკიდებულია დღევანდელი ადამიანი კომპიუტერულ ქსელებზე.

ტერმინი კიბერუსაფრთხოება საკუთარ თავში მოიცავს უამრავი სახის საფრთხეს და ასევე უამრავი სახის საფრთხის გადაწყვეტის მეთოდს. კიბერუსაფრთხოების საფრთხეების გადაწყვეტასნ ჭირდება კომპლექსური პრობლემების განხილვა.

კიბერსივრცის შექმნამ ახალი გამოწვევები და პოტენციური საფრთხეები გააჩინა, ეს ჯერ კიდევ ახალგაზრდა მაგრამ საფრთხის მომცველი სფეროა, სადაც კრიმინალური აქტების აღმოფვრა საკმაოდ რთულია. კომპიუტერულ ქსელებში კრიმინალური მოქმედების ადგილი შეიძლება იყოს როგორც ე.წ. ბნელი ქსელი (Dark NET), რომელზე შეღწევაც ხდება პროექტი ტორის (TOR) საშუალებით, ასევე სოციალური ქსელებიც, როგორებიცაა: Facebook, Twitter, Instagram და ა.შ.

ევროკავშირის სასამართლო გაერთიანების (Eurojust) 2011 წლის ანგარიშის თანახმად: "ტერმინი კიბერდანაშაული მოიცავს ორი სახის კრიმინალურ ქმედებას: ინტერნეტის გამოყენება „ტრადიციული" დანაშაულებისთვის როგორებიც არის თაღლითობა, გაყალბება, სექსუალური შეურაცხყოფის მომცველი მასალის გამოქვეყნება და ა.შ. და მეორეს მხრივ ინტერნეტის გამოყენება ელექტრონული დანაშაულებისთვის, ინფორმაციული სისტემების დემობილიზაციისა და დაზიანების მიზნით."

საჭიროა აღინიშნოს რომ ე.წ. „ბნელი ქსელის“ (Dark NET) შესახებ ცოტას თუ სმენია, მაგრამ ინტერნეტში არსებობს ადგილი ამ სახელით ცნობილი, რომელზეც ვერ შეხვალთ ჩვეულებრივი ბრაუზერების საშუალებით Chrome, Microsoft edge, Opera, Firefox etc. ამ ქსელში შეღწევა ხდება პროექტი ტორის საშუალებით, ბნელ ქსელში არ არსებობს საიტების სტანდარტული მისამართები რომლებსაც ზეპირად დაიმახსოვრებთ, ეს უბრალო სიმბოლოების გროვაა, ამ ქსელში ფაქტობრივად შეუძლებელია ვინმეს იდენტიფიკაცია, დაფიქსირება, სწორედ ამიტომ ეს ქსელი იქცა კრიმინალისთვის სამოთხედ, აქ თქვენ შეძლებთ ნებისმიერი ნარკოტიკული საშუალების ყიდვას, იარაღები, პედოფილია, ყველაფერი რაც არალეგალურია გვხვდება აქ, ხოლო გადახდა ხდება კრიპტოვალუტა ბიტკოინის საშუალებით რაც კიდევ უფრო დაშიფრულს ხდის ნებისმიერ ტრანზაქციას.

Europol-ის თანახმად: „ინტერნეტ ტექნოლოგიების განვითარებამ გამოიწვია მრავალი პრაქტიკული დანაშაულების განხორციელების გაიოლება, გარდა კიბერდანაშაულებისა: საბანკო ბარათების გაყალბება, ბავშვების შეურაცხყოფის მასალების გაყიდვა და აუდიო და ვიზუალური პირატობა. ამ ყველაფერს დაემატა გაიოლებული ნარკოტიკების შექმნა და გაყიდვა, ტრეფიკინგის მსხვერპლების იოლი მოძიება, არალეგალური იმიგრაციის საბუთების დამზადება, ცხოველებით არალეგალური ვაჭრობა და უამრავი სხვადასხვა კრიმინალური ქმედების გაიოლება. ასევე ინტერნეტი ფართოდ გამოყენებადია კრიმინალური დაჯგუფებების მიერ ფულის გასათეთრებლად.“

ყველაზე ხშირად გამოყენებული ონლაინ სივრცის დანაშაულების ტერმინებია: კიბერშეტევა, კიბერტერორიზმი, კიბერომი, კიბერდანაშაული. კიბერდანაშაულები შეიძლება განხორციელდეს როგორც ცალკეული პიროვნებისგან ასევე ორგანიზებული ჯგუფისგან, მეთოდები და ტიპები სხვადასხვა შეიძლება იყოს: ჭიები,

ვირუსები, ტროას ცხენები, ლოგიკური ბომბები. მათ შორის სხვაობა მდგომარეობს მეთოდსა და მიზანში.

შეტევები ხორციელდება DDOS (distributed denial-of-services) საშუალებით, რაც მდგომარეობს სამიზნეზე დიდი რაოდენობით მონაცემებით შეტევაზე, არ აქვს მნიშვნელობა შეტევას 1 ადამიანი ანხორციელებს თუ ადამიანთა დაჯგუფება, ნებისმიერ შემთხვევაში ის ხდება მრავალი კომპიუტერის გამოყენებით, შეტევის მიზანია სამიზნე კომპიუტერზე წვდომა შეუწყდეს მის მფლობელებს, ხოლო შემადგენელ ვირუსებში შეიძლება ჩაპროგრამებული იყოს კონკრეტული მიზნები.

ყველაზე საშიში ვირუსებია ლოგიკური ბომბები, რომლებსაც არ ჭირდებათ სერვერთამ კავშირი, ისინი ძალიან პატარა ზომის არიან და მათო აღმოჩენა ძალიან რთულია.

იქედან გამომდინარე რომ თავდასხმები ხდება ერთდროულად უამრავი კომპიუტერიდან ე.წ. botnet-ების, ანუ უამრავი კომპიუტერების ქსელია გაერთიანებული, პლუს ვირტუალური კომპიუტერები, რომლებიც ყველა ერთიანად ესხმის თავს სამიზნეს, აქედან გამომდინარე ძალიან რთულდება თავდამსხმელის აღმოჩენა. ასეთ თავდასხმებს შეუძლიათ უდიდესი ზიანის მიყენება, ინფორმაციის მოპარვა. თანხის მოპარვა, სისტემის განადგურება და ა.შ.

ინფორმაციული ტექნოლოგიების და ქსელების საწყის წლებში თავდასხმები ხორციელდებოდა არაორგანიზებულად, სხვადასხვა ვირუსებით რომლებიც Random-ით (შემთხვევითობის პრინციპით) ახორციელებდა თავდასხმებს. დროტა განმავლობაში ტექნოლოგიების და პროგრამული უზრუნველყოფის დახვეწასთან ერთად იხვეწება ვირუსული პროგრამებიც, რის შედეგადაც უკვე მიზანმიმართულედ შეიძლება კონკრეტულ კომპანიაზე, ორგანიზაციაზე და ა.შ. კონკრეტული მიზნებით თავდასხმა, რაც კიდევ უფრო სახიფათოს ხდის მას.

კიბერდანაშაული - ონლაინ კრიმინალურ ქმედებებს შორის ყველაზე გავრცელებული და ყველაზე მეტი დანაშაულის მომცველია. კიბერდანაშაული არის კანონდამრღვევი ქმედებების გამხორციელება ინტერნეტ ქსელის საშუალებით. კიბერდანაშაულებში შედის:

პირდაპირი და არაპირდაპი თავდასხმები ონლაინ არასასურველი ინფორმაციის გავრცელებით, ან სპამებით ელეტრონული ფოსტისა და სოციალური ქსელების საშუალებით, რომლებიც ხშირ შემთხვევაში კომპიუტერულ ვირუსებს შეიცავენ.

ბავშვთა პორნოგრაფიის გავრცელება, რაც მთელი მსოფლიოს მასშტაბით კანონით დასჯადია, თუმცა ინტერნეტის რთულად კონტროლირებადობის გამო ეს მაინც ხერხდება, განსაკუთრებით ფიქსირდება ფაქტები დარქ ნეტში.

არალეგალური ფინანსების გათეთრება ინტერნეტის საშუალებით ცნობილი პრაქტიკაა კრიმინალურ სამყაროში. კიბერ ქურდობა, რაც გულისხმობს ნებისმიერი სახის ქურდობა სხვადასხვა მეთოდების გამოყენებით.

კიბერვანდალიზმი - როდესაც კიბერ თავდასხმა პირდაპირ მიმართულია კონკრეტული სერვერის, ბაზის, საიტის დაზიანებისკენ.

კიბერტერორიზმი - ეს არის ტერორიზმის ვირტუალური სახეობა რომელსაც ახორციელებს ადამიანი ან ორგანიზებული ადამიანთა ჯგუფი (ჰაკერები,) ეს ხდება კომპიუტერების საშუალებით. კომპიუტერული ტერორიზმიც კიბერდანაშაულის სახეობაა, თუმცა ეს არის ორგანიზებული დანაშაული რომლის მიზანია სამიზნეს ზიანი მიაყენოს.

კიბერტერორიზმის მიზნები შეიძლება განსხვავდებოდეს, ეს იყოს მიზანმიმართული ზიანის მიყენება, საბანკო სისტემაზე, სახელმწიფო სისტემასა და ქსელებზე, კონკრეტული ადამიანთა ჯგუფების წინააღმდეგ მიმართული ეთნიკური, რელიგიური ან რაიმე სხვა ნიშნით.

კიბერტერორიზმის ერთერთი პირველი შემთხვევა მოხდა ჯერ კიდევ 1996 წელს, როდესაც ჰაკერმა რასისტული ტექსტის გავრცელების მიზნით შეტევა განახორციელა მასაჩუსეცის ინტერნეტის სერვისის პროვაიდერზე, თუმცა მან ვერ მოახერხა მათი სახელით მსოფლიოში გაევრცელებინა რასისტული ტექსტი, რის შემდეგაც სერვერი დააზიანა და დატოვა ტექსტი: „თქვენ აუცილებლად ნახავთ ნამდვილ ინტერნეტ ტერორიზმს, გპირდებით.“

ხშირ შემთხვევაში ის რაც შედის კიბერტერორიზმის დეფინიციაში, რეალურ ტერორიზმთან დაკავშირება რთულია, იქედან გამომდინარე რომ ხშირ შემთხვევაში კიბერთავდასხმის მიზნები გაურკვეველი რჩება, ხოლო ზიანის მიყენება კონკრეტული მიზნის და იდეოლოგიის გარეშე არ შედის სტანდარტული ტერორიზმის დეფინიციაში. ამიტომ რთულია კიბერტერორიზმის ზუსტი მნიშვნელობის აღწერა და ყველა სხვადასხვაგვარად აღიქვამს მას, მაგალითად თუ კი ცივი ომის დროს დაპირისპირებული მხარეები ერთმანეთზე კიბერ შეტევებს ანხორციელებენ, ეს შეიძლება აღქმული იქნას როგორც კიბერტერორიზმიც, კიბერომიც და უბრალოდ კიბერთავდასხმაც.

კიბერომი - არის პოლიტიკური ნიშნით დაპირისპირება მხარეებს შორის, რომელიც ითვალისწინებს ოპონენტის ფინანსურ ინსტიტუტებზე, სამხედრო ქსელზე ან სამთავრობო ინსტიტუტებზე თავდასხმას, მიზანი შეიძლება იყოს პოლიტიკური, ფინანსური ან სამხედრო მოგების მიღება.

წელს მიუნიხის უსაფრთხოების კონფერენციაზე სამხედრო ექსპერტებმა და ევროპის თავდაცვის მინისტრებმა კითხვაზე თუ რა სახის საფრთხე არის ყველაზე საშიში დღევანდელი მდგომარეობით, ფაქტობრივად მსგავსი პასუხები გასცეს, რომ ეს არის კიბერთავდასხმები.

გერმანიის თავდაცვის მინისტრის ურსულა ვონ დერ ლეიენის განცხადებით მიუხედავად იმისა რომ ძალიან რთულია მათი რეაქტიული თვითმფრინავების ფიზიკური განადგურება, სამაგიეროდ იოლია მათი კიბერ შეტევით დაზიანება.

მიუნიხის კონფერენციის ძირითადი თემა იყო კიბერ უსაფრთხოება და განხილვა მიდიოდა იმ საკითხზე რომ სამხედრო ტექნიკა სრულად დაფუძნებულია კომპიუტერულ ტექნიკაზე. ესტონეთის თავდაცვის მინისტრმაც გამოთქვა აზრი რომ ნებისმიერი იარაღის განეიტრალებაა შესაძლებელი საკმაოდ იოლად.

IT უსაფრთხოების ექსპერტის სანდრო გეიკენის აზრით იქამდე სანამ სამხედრო ტექნიკის კიბერუსაფრთხოება მივა სათანადო დონემდე რომ მათი განეიტრალება არ ხდებოდეს იოლად კიდევ 6-7 წელია საჭირო.[3]

1.2 კიბერთავდასხმების სოციალურ-ტექნოლოგიური განზომილებები

დენი, წყალი, ჯანმრთელობის სფერო, ფინანსები, ტრანსპორტი, კვება ყველაფერი იქნება ეს მოწოდება თუ შექმნა გარკვეულწილად კომპიუტერიზებული და ურთიერთდაკავშირებულია. სერვისებამდე და ინფორმაციებამდე წვდომა გაიოლებული და კომფორტულია, მაგრამ ამ ყველაფერიმა შექმნა ასევე ახალი ადგილი კრიმინალური ქმედებისთვის, სადაც კრიმინალების აღმოჩენა რთული ან შეუძლებელია. ადამიანურმა კონფლიქტებმა რეალური სამყაროდან გადაინაცვლა ვირტუალურში.

კიბერსამყარო (კიბერსივრცე) არის მასიური სოციალურ-ტექნოლოგიური სისტემათა სისტემა, სადაც ადამიანები ასრულებენ წამყვან როლს.

[3] cybersecurity. Threats, calls, solutions - Zgoba Artem, Moscow, Dmitry Markelov, St. Petersburg, Pavel Smirnov, PhD., St. Petersburg

კიბერთავდასხმების აღმოსაჩენად ან შესაჩერებლად არსებობს სპეციალური პროგრამული უზრუნველყოფები, თუმცა ისინი არ არის სრულყოფილი და სანდო, მათ შეუძლიათ კომპიუტერული ალგორითმების და მათი ქმედების ამოცნობა, თუმცა არ შეუძლიათ ადამიანური ფაქტორის ამოცნობა. იმას რომ მსგავსი თავდაცვითი მექანიზმები არ ამართლებს მოწმობს ისიც რომ კიბერუსაფრთხოება აქტუალური თემაა და სავარაუდოდ ახლო მომავალშიც ასე იქნება. თუ კი ინტერნეტის შექმნის საწყის წლებში კიბერშეტევების მიზნები იყო ფინანსური მოგება, ინფორმაციის მოპარვა და ზოგადად წვრილმანი ან პირადული მიზეზები. დღესდღეობით უფრო და უფრო იმატებს კიბერშეტევების სოციალური, პოლიტიკური, ეკონომიკური და კულტურული კონფლიქტები. რეალურ სამყაროში თავდასხმების პრევენცია ხდება მომდევნო ნაბიჯების ამოცნობით, ეს ხერხდება თავდამსხმელთა იდეოლოგიის და მიზნების ცოდნიდან გამომდინარე. კიბერსივრცეში ეს რთული საკითხია, იქედან გამომდინარე რომ მსგავსი შეტევების განხორციელებისას ხშირ შემთხვევაში თავდამსხმელები ინკოგნიტოდ რჩებიან და რადგან რთული ამოსაცნობია რა მიზნები ამოძრავებთად და ფაქტობრივად შეუძლებელია დადგენა თუ რა იდეოლოგიის მომხრეები არიან, მათი შემდეგი ნაბიჯის ამოცნობა ფაქტობრივად შეუძლებელი ხდება.

კიბერშეტევები შეიძლება ხდებოდეს უამრავი მოტივით, მაგრამ გარდა სტანდარტული უბრალო მოტივებისა გამოსაყოფია ფართო მასშტაბიანი მოტივები როცა მიზეზი შეიძლება იყოს პოლიტიკური, სოციალური, რელიგიური და ა.შ.

მიუხედავად იმისა რომ შეუძლებელია კონკრეტული კიბერ შეტევით დადგინდეს მოტივი და იდეოლოგია, არსებობს მეთოდი რომ ნაწილი მათგანის იდენტიფიკაცია მაინც მოხდეს, ეს არის კიბერ შეტევების შესწავლის მეთოდი, მოგროვება ყველა მათგანის, ურთიერთდაკავშირება სხვადასხვა კუთხით, იდენტიფიცირება რომლებია

ერთიდაიგივე ჯგუფების მიერ და მათი სამიზნეების ანალიზით მეტი ინფორმაციის მიღება შემდგომი პრევენციისთვის.

პოლიტიკურად მოტივირებული კიბერშეტევებს - ახორციელებენ კიბერკრიმინალები რომლებიც პოლიტიკურად არიან მოტივირებულები. ისინი შეიძლება იყვნენ პოლიტიკური ექსტრემისტული დაჯგუფების წევრები რომლებიც კიბერსივრცეს იყენებენ პროპაგანდის გასავრცელებლად, პოტენციური მტრების ვებსაიტებსა და სერვერებზე თავდასასხმელად, თანხის მოპარვა საკუთარი პოლიტიკური იდეოლოგიის დასაფინანსებლად ან კიბერსივრცის გამოყენება ფიზიკურ სამყაროში სამოქმედო გემის შესამუშავებლად.

პოლიტიკური კიბერშეტევების მოტივაცია შეიძლება დაიყოს ორ ნაწილად ესენია: პოლიტიკური ქმედებების წინააღმდეგ მიმართული, ან კანონების და ღია დოკუმენტების წინააღმდეგ მიმართული.

პოლიტიკური ქმედებების წინააღმდეგ მიმართული პოლიტიკური კიბერშეტევები -

1998 წლის ივნისში ინდოეთის ატომურ კვლევით ცენტრზე მოხდა მასობრივი კიბერშეტევა ერთდროულად ამერიკის შეერთებული შტატებიდან, დიდი ბრიტანეთიდან, ნიდერლანდებიდან და ახალი ზელანდიიდან, მიზანი იყო ატომური კვლევების გაპროტესტება. ჰაკერებმა გაანადგურეს სერვერის მასალები და დატოვეს ტექსტი.

1998 წლის ოქტომბერში შეტევა განხორციელდა მექსიკის პრეზიდენტის ერნესტო ზედილოს ვებსაიტზე, მიზანი იყო გენოციდის, კოლონიზაციის და რასიზმის პროტესტი.

1999 წლის ივნისში გერმანიაში დიდი რვიანის (ახლანდელი დიდი შვიდეული) წინააღმდეგ მიმართული პროტესტის ნიშნად გერმანიის სხვადასხვა კომპანიებზე და სტრუქტურებზე გამხორციელდა ძალიან დიდი რაოდენობით კიბერშეტევები, კანადიდან, ისრაელიდან, ინდონეზიიდან და გერმანიიდან.

1999 წელს სერბეთში, კოსოვოს ომის დროს, სერბებმა განახორციელეს კიბერშეტევები ამერიკის შეერთებული შტატების და ნატოს წინააღმდეგ, მიზანი იყო ნატოს და იუგოსლავიის მიმართ პროტესტი. ასევე მათ გამოიყენეს ინტერნეტი ინფორმაციული ომისთვის და ავრცელებდნენ სხვადასხვა ვიზუალურ და ინფორმაციულ მასალებს.

2008 წლის დეკემბერში პეკინში სამიზნე გახდა საფრანგეთის საელჩო, მას თავს დაესხნენ ჩინელი ჰაკერები, როგორც კი საფრანგეთის პრეზიდენტი ნიკოლას სარკოზი და დალაილამა შეხვდნენ ერთმანეთს.

კანონმდებლობის ან ღია დოკუმენტების წინააღმდეგ განხორციელებული კიბერშეტევები -

1995 წელს საფრანგეთის სამთავრობო ვებსაიტებზე მიმართული კიბერშეტევა, რომელიც მიმართული იყო საფრანგეთის ატომური და სოციალური პოლიტიკის გასაპროტესტებლად. კიბერშეტევის ავტორებმა გააღვივეს პროტესტის გრძნობა მოქალაქეებში, რომლებმაც ყველამ ერთდროულად გახსნა საფრანგეთის სამთავრობო ვებსაიტი, რითაც გამოიწვია სერვერის გადატვირთვა და ის მიუწვდომელი იყო რამდენიმე საათი.

2001 წლის მარტში სამხრეთ კორეის და იაპონიის ჰაკერები თავს დაესხნენ იაპონიის განათლების სამინისტროს ვებსაიტს, მათი მხრიდან კონტროვერსიული ისტორიული წიგნების გამოშვების გამო.

ფიზიკური ძალადობის წინააღმდეგ მიმართული კიბერშეტევები -

1999 წელს ბელგრადში ჩინეთის საელჩოს შემთხვევითი დაბომბვის გამო პროტესტის ნიშნად ჩინელმა ჰაკერებმა კიბერშეტევები განახორციელეს ამერიკის შეერთებული შტატების სახელმწიფო ვებსაიტებზე.

1999 წელს ჩინეთსა და ტაივანს შორის პოლიტიკურმა დაპირისპირებამ გამოიწვია კიბერომი, ჩინელებმა საკუთარი კონტროლის ქვეშ მოაქციეს ზოგიერთი ტაივანური

სამტავრობო ვებსაიტი, ხოლო ტაივანელებმა ჩინურ სამთავრობო ვებსაიტებზე ანტიკომუნისტური მესიჯები დატოვეს.

2000 წლის ნოემბერში პალესტინელი ჰაკერები თავს დაესხნენ კომპანიას "Lucent technology" რომელიც ბიზნესს აწარმოებდა ისრაელში, რამაც გამოიწვია კიბერომი ებრაელებსა და პალესტინელებს შორის.

2007 წლის აპრილში ესტონეთის სერვერებზე განხორციელდა DOS კიბერშეტევები მსოფლიოს დაახლოებით მილიონი კომპიუტერიდან ბოტების საშუალებით, რამაც გამოიწვია სრულად კიბერ სერვერების ჩამოშლა, ესტონეთმა ბრალი დადო რუსეთს, თუმცა რუსეთმა იუარა მისი ჩარევა ამ საკითხში.

სახელმწიფო ტერიტორიებთან დაკავშირებული კიბერშეტევები -

2000 წელს ინდოეთის სამთავრობო ვებსაიტებზე განხორციელდა კიბერშეტევები პაკისტანის ჰაკერების მხრიდან, ქაშმირის კონფლიქტის გასაპროტესტებლად.

2008 წლის აგვისტო, რუსეთ-საქართველოს ომი ცხინვალის ტერიტორიისთვის, რუსეთმა განახორციელა მასობრივი კიბერშეტევები სრულად საქართველოს კიბერსოვრცის წინააღმდეგ, რამაც საქართველოს კიბერ სივრცე ერთგვარ ვაკუუმში მოაქცია და სრულად ჩაახშო ის.

მსგავსი მაგალითები უამრავია და დროთა განმავლობაში იმატებს, რადგან კიბერუსაფრთხოების დონე ჯერ კიდევ ძალიან დაბალზეა მსოფლიო მასშტაბით.

კიბერშეტევების ეკონომიკური შედეგები - დღესდღეობიტყველაფერი ინტერნეტის საშუალებით ხდება, მათ შორის ბიზნესიც იმართება ინტერნეტში და არამარტო, არის მრავალი ბიზნესი რომელიც სრულად ინტერნეტში ოპერირებს და არ გააჩნია ფიზიკური მისამართი, ასეთი ტიპის ბიზნესებია: ელექტრონული ფოსტა (Email), ღრუბელი (Cloud), ფაილების ატვირთვა ჩამოტვირტვა და სხვა უამრავი სერვისი, რომლებსაც ჭირდება მუდმივი მონიტორინგი. ყველა მსგავს სერვიის ჭირდება

თავდაცვა კიბერშეტევებისგან, მსგავსი თავდასხმები ხშირ შემთხვევაში ეკონომიკურად აზარალებს მომხმარებლებს.

ეკონომიკური ზარალი შეიძლება დადგეს სხვადასხვა სახის, ყველაზე მარტივი შემთხვევა ეს შეიძლება იყოს სერვერებიდან პირდაპირი თანხის მოპარვა. ინფორმაციის მოპარვა რომელიც შეიზლება ფასეული იყო და საიდუმლო. ასევე ეკონომიკური შედეგი დგება მხოლოდ იმ ფაქტითაც რომ კიბერუსაფრთხოების უზრუნველყოფა ფინანსებთანაა დაკავშირებული და პრევენციისთვის მაინც იხარჯება გარკვეული თანხები.

კიბერსივრცე სულ უფრო იჭრება ადამიანთა ცხოვრებაში, ეს ეხება ყველა სფეროს, ადამიანების სოციალური ცხოვრება სრულად ინაცვლებს ვირტუალურში, შესაბამისად ყველა სახის კონფლიქტი ხდება იქ, იქნება ეს რასობრივი, ეთნიკური, რელიგიური, სოციალური, პოლიტიკური, ეკონომიკური, რამე სხვა სახის კონკრეტულ ჯგუფს მიკუთვნებულ ადამიანებს შორის თუ პირადული, კიბერსივრცე იქცა ადგილად სადაც თანამედროვე ადამიანი ცხოვრობს, იქნება ეს სოციალური კავშირები, ბიზნესი, გართობა, კონფლიქტი, მომსახურების მიღება, ყველაფერი ხდება აქ, რასაც როგორც აღვნიშნეთ გარდა კომფორტულობისა ბევრი უარყოფითი მხარეც აქვს.[4]

1.3 ინფორმაციული ომი - ახალი გამოწვევა ევროპისთვის

ინფორმაციული ომის სახელიდანვე გამომდინარეობს რომ ომი ხდება ინფორმაციის საშუალებით, ინფორმაციის გავრცელების ძირითადი წყარო არის ინფორმაციული ტექნოლოგიები, სწორედ აქ ერთვება კიბერუსაფრთხოება,

[4] Dimensions of cyber-attacks - Robin Gandhi, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, And Phillip Laplante

რომელმაც უნდა უზრუნველყოს ინფორმაციული ომის სხვადასხვა შემადგენელი ნაწილებისგან თავდაცვა.

თანამედროვე მსოფლიოში ინფორმაციული ომი უფრო დიდ იარაღად იქცა ვიდრე ფიზიკური, ოდითგანვე ინფორმაციული ომის მოგება ხშირ შემთხვევაში გულისხმობდა ფიზიკური ომის მოგებასაც, ამის ნათელი მაგალითია მეორე მსოფლიო ომი, სადაც მიუხედავად იმისა რომ საბჭოთა კავშირმა გერმანიაზე ადრე შექმნა საკონცენტრაციო ბანაკები, არ ინდობდა ებრაელებსაც, მაგრამ იმდენად სწორად გათვალა ინფორმაციის გავრცელების მეთოდები და თუ რა უნდა გაევრცელებინა, რომ დღემდე როდესაც ვახსენებთ საკონცენტრაციო ბანაკს ასოცირდება გერმანიასთან.

ოცდამეერთე საუკუნე ინფორმაციული ტექნოლოგიების საუკუნეა, იმდენად განვითარდა ტექნოლოგიები რომ რეალურ დროში მსოფლიოს ნებისმიერი წერტილის შესახებ ინფორმაცია ცნობილია ნებისმიერი დაინტერესებული პიროვნებისთვის. აქედან გამომდინარე ინფორმაციით მანიპულირება გადამწყვეტ როლს ასრულებს საზოგადოებრივი აზრის ჩამოყალიბებაში, შესაბამისად ეფექტური პოლიტიკის გატარებაში.

ინფორმაციული ომი შეიძლება მოიცავდეს ((Reisman & Antoniou, 1994)

- ტაქტიკური ინფორმაციის მოგროვება
- ინფორმაციის სიზუსტის გადამოწმება
- პროპაგანდის და დეზინფორმაციის გავრცელება, ოპონენტის ცუდად წარმოსაჩენად და მანიპულაციისთვის.
- ოპონენტის მიერ მოპოვებადი ინფორმაციის დამახინჯება, შეცდომაში შეყვანა.
- ოპონენტისთვის ინფორმაციის მოპოვებაზე ხელის შეშლა

ინფორმაციულ საუკუნეში ინფორმაციული ომი უფრო იოლი და აქტუალური გახდა, შესაბამისად ზოგიერთი სახელმწიფოს მთავრობა მილიარდობით დოლარს ხარჯავს სპეციალურ სამსახურებში, რომლებიც პოტენციურ ინფორმაციულ საფრთხეებს დაადგენენ და პრევენციას მოახდენენ, ან მოქმედ საფრთხეებს დაადგენენ და შეაჩერებენ.

თუ კი აქამდე ინფორმაციული ომისთვის ტელე, რადიო და წერითი მედია გამოიყენებოდა, ახლა უკვე ძირითადი წყაროა ინფორმაციული ტექნოლოგიები, კიბერშეტევები და განსაკუთრებით სოციალური მედია.

კიბერშეტევები გამოიყენება სხვადასხვა მიზნებით, ესენია საიდუმლო ინფორმაციის მოპოვება, ასევე ინფორმაციის მოპოვებაზე ხელის შეშლა, ინფორმაციულ ვაკუუმში მოქცევა, ოპონენტის ქსელების დაზიანება, ჩახშობა და ა.შ.

უფრო ფართო მასშტაბით ინფორმაციული ომის საშუალებად გამოიყენება სოციალური მედია და სოციალური ქსელები, როგორებიცაა Facebook, Instagram, Twitter,

სოციალური მედიის მოხერხებულობა გაავრცელო ინფორმაცია, ფოტო-ვიდეო მასალა და ა.შ. გარდა ამისა მისდამი იოლი წვდომა საზოგადოების ყველა ფენისთვის, გახდა საფუძველი რომ სოციალურ მედიას მოეპოვებინა მონოპოლია სხვა მედია საშუალებების წინააღმდეგ. სოციალური მედია საზოგადოებას სთავაზობს ყველანაირად კომფორტულ პლატფორმას, რომელზეც ინფორმაცია ვრცელდება იოლად, იაფად და რაც მთავარია დიდი სისწრაფით. ნებისმიერი მომხდარი ფაქტი მსოფლიოს მასშტაბით წამიერად ხდება ცნობილი სოციალური მედიის საშუალებით, იდება უამრავი ფოტო-ვიდეო მასალა, რის გამოც მას კონკურენციას ტელევიზია, რადიო და მითუმეტეს ბეჭდვითი მედია კონკურენციას ვერ გაუწევს.

კონფლიქტი ისრაელსა და პალესტინას შორის ჯერ კიდევ ინტერნეტამდე დაიწყო, თუმცა დღეს აქტიურად მიმდინარეობს ინფორმაციული ომი ამ ორ დაპირისპირებულ

მხარეს შორის, ისინი აქტიურად ავრცელებენ სოციალურ მედიაში ვიზუალურ მასალებს, სადაც წარმოჩენილია დრამატული მასალები, საკუთარი ინტერესების დაცვის მიზნით. ორივე მხარე განსაკუთრებით აქტიურია ტვიტერზე, სადაც ისრაელის მხარეს ნახევარ მილიონამდე გამომწერი ყავს ხოლო პალესტინის მხარეს 18000, ისინი აქტიურად ავრცელებენ სხვადასხვა ინფორმაციას დღეში რამდენიმეჯერ.

სწორედ ხელმისაწვდომობიდან გამომდინარე იოლი ხდება სოციალურ მედიაში ე.წ. fake news დეზინფორმაციის გავრცელება, სხვადასხვა სამსახურები, დაჯგუფებები, ორგანიზაციები გამიზნულად ავრცელებენ დეზინფორმაციას ოპონენტების წინააღმდეგ, სოციალური მედია გახდა ომის ალტერნატიული არენა, სადაც იარაღი სიტყვები და მასალებია, მას პოტენციურად შეუძლია გამოიწვიოს რეალური ომიც და არა მარტო, აქ გავრცელებულმა მასალებმა შეიძლება გამოიწვიოს პროტესტის გრძნობა რამაც საზოგადოება შეკრას და გამოიყვანოს ქუჩაში.

სოციალურ მედიას ფეისბუქს, ტვიტერს, ინსტაგრამს აქვს ტრენდების ფუნქცია, ეს არის ალგორითმი რომელიც სრულად პლატფორმაზე აანალიზებს ყველაზე ხშირად გამოყენებულ ფრაზებს, სიტყვებს, ჰეშთეგებს და ქმნის სიას სადაც ტრენდები დაწყობილია რიგითობის მიხედვით, საიდანაც იოლად შეიძლება ვნახოთ ყველაზე პოპულარული თემები მიმდინარე დროს. ამ ფუნქციის დადებითი მხარეების გარდა დიდი მინუსი აქვს, ეს არის ის რომ სხვადასხვა დაჯგუფებებს ეძლევათ საშუალება ბოტების გამოყენებით ხელოვნურად იმეორონ ერთიდაიგივე თემები და ხელოვნურად შეიყვანონ ტრენდებში პროპაგანდა.[5]

გავრცელებული პროპაგანდის შესაბამისად ქმნიან დეზიფორმაციულ ნიუსებს (Fake news), მემეებს, ვიზუალურ მასალებს, ეს ყველაფერი ხელს უწყობს გავრცელებული პროპაგანდის ლეგიტიმაციას.

[5] Social Media as a Tool for Information Warfare - Aylin Manduric

სხვადასხვა სოცალური საშუალებები ემსახურება სხვდასხვა მიზნებს, შესაბამისად მათი გამოყენება დეზინფორმაციისთვის სხვადასხვა სახით ხდება, ფეისბუქი უფრო შიდა სოციალური პლატფორმაა, რომელიც აკავშირებს ოჯახებს, ნათესავებს, მეგობრებს, აქ გავრცელებული ინფორმაციების უმრავლესობაც უფრო პირადული სახისაა, ასევე ფეისბუქზე მიუხედავად იმისა რომ არსე-ბობს ტრენდების ფუნქცია, ის არ არის გამოსაჩენ ადგილას, ამიტომ ნაკლებ პოპულარულია. რაც შეეხება ტვიტერს ეს არის მიკრო ბლოგი, რომელზეც ერთ ჯერზე მაქსიმუმ 140 სიმბოლოს გამოქვეყნება შეიძლება. აქ ნაკლებ შეხვდებით პირადულ და ოჯახურ სიტუაციას, ეს პლატფორმა აკავშირებს მთელ მსოფლიოს და განიხილება უფრო ზოგადი საკითხები, პოლიტიკა, შოუ ბიზნესი, ტექნიკური სიახლეები და მრავალი სხვა. ტვიტერზე დაწერილ ტვიტს თუ კი ის ტრენდული გახდება უამრავი ადამიანი ნახულობს, პასუხობს აზიარებს და ა.შ. ამიტომაც იდეალური პლატფორმაა პროპაგანდისთვის.

იქედან გამომდინარე რომ ტვიტერი იდეების გავრცელების პლატფორმაა და ინფორმაცია სწრაფად ვრცელდება, მას აქტიურად იყენებენ მაგალითად ჟურნალისტები და აკადემიკოსები. თუმცა მისი გამოყენება დაიწყეს სხვადასხვა ტერორისტულმა ორგანიზაციებმაც. ალქაიდა ადრე ამჯობინებდა საიტების შექმნას და საკუთარი სიტყვის ამ გზით გავრცელებას, თუმცა საბოლოოდ ტვიტერზე გადავიდნენ, ამ გზით სწრაფი წვდომა აქვთ როგორც მომხრეებთან ისე მტრებთან, ისინი აქტიურად იყენებენ სხვადასხვა მეთოდებს რომ გაგზავნილი მესიჯი ტრენდში აღმოჩნდეს და მაქსიმალურად გავრცელდეს.

ევროკავშირისთვის გარდა სხვადასხვა ტერორისტული ორგანიზაციებისა, ყველაზე დიდ საფრთხედ მოიაზრება რუსეთის ფედერაცია, განსაკუთრებით კიბერ სივრცეში, სადაც რუსული პროპაგანდა განსაკუთრებით აქტიურია.

რუსეთისთვის პროპაგანდის გზით ბრძოლა ახალი არ არის, იქ ჯერ კიდევ საბჭოთაკავშირის დროს ისწავლებოდა ცალკე მიმართულება „სპეც-პროპაგანდა.“

მაგრამ პუტინის დროის რუსეთში განსაკუთრებით გააქტიურდა ეს მეთოდები, ინფორმაციული ტექნოლოგიების განვითარებას რუსეთი აქტიურად იყენებს სათავისოდ, დეზინფორმაციის და პროპაგანდის გასავრცელებლად.

ანტიდასავლური პროპაგანდა რუსეთის ინფორმაციული ომის შემადგენელი ნაწილია, ისინი წარმოაჩენენ ევროკავშირს და ზოგადად დასავლეთს როგორც ტრადიციების წინააღმდეგ მიმართულ ქვეყნებს, ევროპა გამოყავთ გარყვნილების ბუდე. ამით ისინი წარმოაჩენენ საკუთარ უპირატესობას და აჩვენებენ თითქოს მათი ვალია სახელმწიფოს კონსერვატორული ღირებულებები დაიცვან.

რუსეთში მკაცრად კონტროლდება არასამთავრობო ორგანიზაციების არსებობა და ფაქტობრივად მინიმუმამდეა დაყვანილი ევროპიდან დაფინანსებული მსგავსი ორგანიზაციები.

ევროკავშირი ყოველთვის ერთი ნაბიჯით უკან არის როდესაც საქმე ეხება რუსეთის პროპაგანდას და დეზინფორმაციას, ამის მიზეზი მდგომარეობს არა იმაში რომ რუსეთია ძლიერი ან ევროპა სუსტი, არამედ ამ ორ მხარეს შორის პოლიტიკურ ხედვებს შორის განსხვავებაში. რუსეთში მსგავსი მეთოდებით ბრძოლა მიღებულია ხოლო ოპონენტის აზრის დაბლოკვა სხვადასხვა მეთოდებით მათი პოლიტიკის ნაწილია. განსხვავებით რუსეთისგან ევროპაში ერთერთი მთავარი ფასეულობაა სიტყვის თავისუფლება, აქედან გამომდინარე ვერც დეზინფორმაციის კონტროლი ხერხდება. რუსეთის აქტიური ინფორმაციული ომის გამო სხვა გზა არ რჩება ევროკავშირის ქვეყნებს რაიმე ნაბიჯები უნდა გადადგან, ერთერთი პირველი იყო დიდი ბრიტანეთის კანონი, რომელიც გულისხმობს ინტერნეტ ტროლების რომლებიც აშკარად ზიანის მომტანია პენიტენციურ დაწესებულებაში 6 თვით მოთავსებას. ასევე მუშავდება ევროკავშირის სხვადასხვა ქვეყნებში შესაბამისი კანონმდებლობები.

იმისთვის რომ ევროკავშირმა წინააღმდეგობა გაუწიოს რუსეთის მხრიდან დეზინფორმაციას, ჭირდება კრეატიული და სერიოზული მიდგომა, სხვადასხვა

კანონმდებლობების შემუშავებით, რომელიც თავის მხრივ არ დაარღვევს ევროპულ ფასეულობებს.[67]

[6] Information Warfare as a Geopolitical Tool - Tomáš Čižik
[7] Strategic Defence for Russia's Undeclared Information War on Europe - Salome Samadashvili

I I თავი - ევროკავშირის მიერ გატარებული პოლიტიკა კიბერუსაფრთხოების კუთხით

ევროკავშირი მსოფლიოში წამყვანი სუბიექტია კიბერუსაფრთხოების კუთხით აქტიურობის, შემუშავებული სტრატეგიების და პროექტების მხრივ, ევროკავშირის სხვადასხვა კონფერენციებსა და შეხვედრებზე ხშირ შემთხვევაში ძირითად თემას წარმოადგენს კიბერუსაფრთხოება, მეტიც ევროკავშირში კიბერთავდასხმა ყველაზე აქტუალურ პრობლემად მიიჩნევა და ცდილობენ. ამ თემას კურირებს სპეციალური სააგენტოები: „ევროკავშირის ქსელების და ინფორმაციის უსაფრთხოების სააგენტო“– ENISA, ევროპის კიბერდანაშაულის ცენტრი - EUROPOL/EC3, ევროპის თავდაცვის სააგენტო - EDA.

ასევე არის არამომგებიანი (Non-profit,) თვითდაფინანსებადი ორგანიზაციები კიბერუსაფრთხოების კუთხით.

ის რომ ამხელა ყურადღება ეთმობა კიბერუსაფრთხოების თემას, ნათელს ხდის თუ რამდენად სერიოზულად უდგება ევროკავშირი ამ თემას.

2.1 ევროკავშირის კიბერუსაფრთხოების სტრატეგია და რეფორმის გეგმა

ევროკავშირის ქვეყნების კიბერუსაფრთხოების სახელმწიფო სტრატეგიებს თუ შევადარებთ ნათლად ჩანს მათი არაერთგვაროვნება, ზოგიერთი მათგანის ძირითადი მომენტები ემთხვევა, თუმცა მაინც დიდი განსხვავებებია, როგორც სტრატეგიის პუნქტებში, ასევე დოკუმენტის ზომაში, 1 გვერიდან დაწყებული 40 გვერდს ზემოთ დოკუმენტებიც არის. მეტიც ისინი დაფუძნებულია სხვადასხვა ფასეულობებზე.

ზოგიერთის დოკუმენტი იმდენად პატარაა გამოხატავს მათ არასერიოზულობას, გარდა ამისა მაგალიტად ლატვიის კიბერუსაფრთხოების სტრატეგიის დოკუმენტი სხვა ფორმატშია დაწერილი და შემდეგ არალიცენზირებული პროგრამით არის გადაყვანილი Pdf ფორმატში.

ეს ყველაფერი ნათლად გამოხატავს თუ როგორი ჩამოუყალიბებელია კიბერუსაფრთხოების სფერო, აქ არ არის საუბარი რომ ყველას საერთო სტრატეგია უნდა ქონდეს, თუმცა რადგან ისინი არიან ერთი კავშირის წევრები რომლებსაც აკავშირებთ არამხოლოდ რეგიონი არამედ ფასეულობების, საჭიროა მათი სტრატეგიები ეფუძნებოდეს ერთ ძირითად სტრატეგიას, როგორც კანონები ეფუძნება კონსტიტუციას.

ევროკავშირს აქვს ოფიციალური დოკუმენტი, რომელიც არა იმდენად სტრატეგია არამედ უფრო ხედვაა ევროკავშირის კიბერუსაფრთხოების სტრატეგიის, ასევე არსებობს გეგმა რეფორმის მიზნით.

ბოლო ორი ათწლეულის განმავლობაში ინტერნეტის და კონკრეტულად კიბერსივრცის განვითარებამ უზარმაზარი გავლენა იქონია სოციუმის ყველა ნაწილზე. ყოველდღიური ცხოვრება, ფუნდამენტალური უფლებები, ეკონომიკა, ზოგადად ყველა სფერო დამოკიდებული დახდა ინფორმაციულ და საკომუნიკაციო სისტემებზე. ღია კიბერსივრცემ გამოიწვია პოლიტიკური და სოციალური ჩართულობა მსოფლიოს მასშტაბით. ინტერნეტმა ზღვრები წაშალა ქვეყნებს, თემებს, მოქალაქეებს შორის. ინტერნეტი გახდა თავისუფლების წყარო, სადაც ყველას აქვს გამოხატვის თავისუფლება, ის დემოკრატიის ერთგვარ საყრდენად მოგვევლინა.

იმისთვის რომ კიბერსივრცემ განაგრძოს ღია და თავისუფალი ინფორმაციის გაცვლის საშუალების როლი, საჭიროა ევროპის ფასეულობები და კანონები გავრცელდეს ინტერნეტ სივრცეშიც. მართალია კიბერუსაფრთხოების უზრუნველყოფა და ადამიანების უფლებების დაცვა ფუნდამენტალურია, თუმცა

კიბერსივრცის შემთხვევაში ეს გამოწვევაა, რადგან რთულია დაადგინო ზღვარი უფლების დაცვასა და ცენზურას შორის. თუმცა რაც შეეხება კიბერშეტევებს და ვირუსებს ეს ცალსახად დანაშაულია და აღმოსაფხვრელია, ამისთვის საჭიროა სახელმწიფოებმა იმუშაონ და გამართონ კიბერსივრცე. თუმცა არის კიდევ ერთი წინაღობა, ეს არის ის რომ კერძო სექტორს უჭირავს დომინანტური ადგილი კიბერსივრცეში და რთულია ისეთი პოლიტიკის გატარება რომ არავინ დააზიანოს.

კიბერსივრცე იქცა ეკონომიკური ზრდის ხერხემლად, ყველა სახის ფინანსური ოპერაციები, ფინანსური სექტორები დამოკიდებულია ინტერნეტზე. ინტერნეტ სერვისების სრულად გამოყენებით თეორიულად ევროკავშირს შეუძლია მთლიანი შიდა პროდუქტის 500 მილიარდიანი ზრდა წელიწადში, თუმცა სამწუხაროდ 2013 წლის კვლევების თანახმად ყოველი მესამე ადამიანი ევროპაში არ ენდობა ინტერნეტს ფინანსების კუთხით. ევროკავშირის ფარგლებში საშუალოდ 10დან ერთი ადამიანი მაინც გახდა ონლაინ თაღლითობის მსხვერპლი.

ბოლო წლებში მიუხედავად მზარდი ინტერნეტ სერვისებისა, კომფორტისა და ზოგადად მრავალი დადებითის რაც მოაქვს ინტერნეტს, უამრავი საფრთხეც გამოჩნდა და ის არათუ იკლებს არამედ პირიქით საკმაოდ დიდი სისწრაფით იმატებს, იქნება ეს გამიზნული თუ შემთხვევითი. საფრთხეებს შეიძლება ქონდეს სხვადასხვა საწყისები: კრიმინალური, პოლიტიკური, ტერორისტული, სახელმწიფოების მიერ დაფინანსებული, ისევე როგორც ბუნებრივი მოვლენების ან შემთხვევითობის სახით.

ევროკავშირის ეკონომიკაზე უკვე ზემოქმედებს კიბერდანაშაულები კერძო პირების და კერძო სექტორის წინააღმდეგ. მეთოდები სხვადასხვაა, სისტემაში შეღწევა, ინფორმაციის მოპარვა, ან ჩვენს მიერ უკვე განხილული მეთოდის Ransom ვირუსების საშუალებით ფულის გამოძალვა.

ევროკავშირის გარეთ ზოგიერთი ქვეყანა ინტერნეტს იყენებს არასათანადოდ, მოქალაქეთა კონტროლისთვის, აწესებენ ცენზურას, აკონტროლობენ კონტენტს და

ა.შ. ევროკავშირის გადაწყვეტილებით ინტერნეტი უნდა იყოს დემოკრატიული და სიტყვის და გამოხატვის თავისუფლებას უნდა მიენიჭოს პრიორიტეტი.

ამ ყველაფრიდან გამომდინარე გახდა აქტუალური კიბერუსაფრთხოება, სწორედ ამიტომ მსოფლიოს მასშტაბით სხვადასხვა ქვეყნები ადგენენ კიბერუსაფრთხოების სახელმწიფო სტრატეგიებს. რომელთა ევროპულ ნაწილსაც უკვე გავეცანით, თუმცა ამჯერად გავეცნობით კონკრეტულად ევროკავშირის კიბერუსაფრთხოების სტრატეგიას.

ევროკავშირის კიბერუსაფრთხოება ეყრდნობა ევროკავშირის უსაფრთხოების ფუნდამენტურ კანონებს, დემოკრატიული მიდგომა უნდა იყოს კიბერსივრცეშიც. ინტერნეტი განიხილება როგორც ადამიანის უფლება, ყველას უნდა ქონდეს შესაძლებლობა შევიდეს ინტერნეტში და დაცული იყოს იქ. კიბერსივრცეს არ აკონტროლებს რაიმე კონკრეტული სტრუქტურა, აქ არიან დაინტერესებული მხარეები, რომელთაგან უმრავლესობა კერძო სექტორიდანაა, სწორედ ისინი ადგენენ წესებს. ევროკავშირი ადასტურებს ინტერნეტში კერძო სექტორის დომინანტობის აუცილებლობას დემოკრატიული მიზნით და აპირებს ხელი შეუწყოს მათ.

ევროკავშირი თვლის რომ კიბერსივრცის უსაფრთხოების პასუხისმგებლობა უნდა გადანაწილდეს ყველა სექტორზე და კერძო პირებზეც. ევროკავშირმა უნდა უზრუნველყოს თავისუფლება და დაცულობა ინტერნეტში, ყველა პირის სარგებელისთვის.

ევროკავშირი გამოყოფს 5 სტრატეგიულ პრიორიტეტს:

- კიბერმდგრადობის უზრუნველყოფა.
- კიბერდანაშაულების კუთხით რადიკალური ცვლილებები.
- კიბერდაცვის პოლიტიკის და შესაძლებლობების განვითარება,

სტანდარტულ უსაფრთხოებასა და თავდაცვის პოლიტიკაზე დაფუძნებით.

- სამრეწველო და ტექნოლოგიური რესურსების განვითარება კიბერუსაფრთხოებისთვის.
- თანმიმდევრული საერთაშორისო კიბერსივრცის პოლიტიკის ჩამოყალიბება ევროკავშირისთვის და ევროკავშირის ფასეულობებზე ხელშეწყობა.

კიბერმდგრადობის მიღწევა:

პირველ რიგში ევროკავშირის საჯარო ხელისუფლებისა და კერძო სექტორის შეთანხმებული მოქმედება, რის შედეგადაც ერთობლივად ეფექტურად შეძლებენ კიბერსაფრთხეების წინააღმდეგ ბრძოლას. გამოცდილების გაზიარება და საერთო პოლიტიკის შექმნა აუცილებელია ამ საკითხში, წინააღმდეგ შემთხვევაში ევროპა გახდება იოლი სამიზნე კიბერდანაშაულისთვის. სწორედ ამ მიზნებისთვის, შუამავალი როლის შესასრულებლად შეიქმნა „ევროპის ქსელების და ინფორმაციის უსაფრთხოების სააგენტო“ (European Network and Information Security Agency “**ENISA**”) 2004 წელს.

ცნობიერების ამაღლება:

სწორედ იმაზე დაფუძნებით რომ კიბერუსაფრთხოება უნდა იყოს საერთო პასუხისმგებლობა, აუცილებელია ამ კუთხით ცნობიერების ამაღლება, ყველა მომხმარებელმა უნდა იცოდეს კიბერსაფრთხეების შესახებ და შესაბამისად მისი ყველა ქმედების პასუხისმგებელი უნდა იყოს. ENISA-ს დაევალა ცნობიერების ამაღლების კუთხით მუშაობა, პუბლიკაციების დადება, ექსპერტების სემინარების ორგანიზება და საჯარო-კერძო სექტორების თანამშრომლობის გაძლიერება. ევროპოლი, ევროჯასთი და სახელმწიფო მონაცემების დაცვის ხელისუფლებაც აქტიურად მუშაობენ ამ კუთხით.

ევროკავშირში სამი სააგენტო მუშაობს აქტიურად კიბერუსაფრთხოების კუთხით, ესენია: ევროკავშირის ინფორმაციის და ქსელების უსაფრთხოების სააგენტო - ENISA, ევროპის კიბერდანაშაულის ცენტრი - EUROPOL/EC3, ევროპის თავდაცვის სააგენტო - EDA. ამ სააგენტოებს ყავთ მენეჯმენტის ბორდები, რომლებშიც წარმოდგენილია სხვადასხვა ქვეყნების წარმომადგენლები.

ეს კიბერუსაფრთხოების სტრატეგია არის ევროკავშირის ხედვა თუ როგორ შეიძლება კიბერსივრცეში საფრთხეებზე გამკლავება, ძირითადი მესიჯია ყველა სექტორის თანამშრომლობა გამოიწვევს ეფექტურ კიბერუსაფრთხოებას.[8]

კიბერუსაფრთხოების რეფორმა:

ევროკავშირის მიზანია გააძლიეროს კიბერუსაფრთხოების წესები რომ დაუპირისპირდეს ზრდად კიბერსაფრთხეებს და ინიციატივა ხელში აიღოს. 2017 წლის 19-20 ოქტომბერს ევროპის კონსულმა დააყენა საკითხი ევროკავშირის კიბერუსაფრთხოების საერთო მიდგომების მიღების შესახებ. ეს რეფორმა ევროკომისიის მიერ იქნა შემოტავაზებული სექტემბერში.

მიზნებია:

- კიბერუსაფრთხოების უფრო ძლიერი სააგენტოს შექმნა.
- ევროკავშირის ფართო კიბერუსაფრთხოების სერტიფიცირების სქემის წარმოდგენა.
- ქსელების და ინფორმაციის უსაფრთხოების დირექტივების სწრაფი განხორციელება.

ევროპის ლიდერები კიბერუსაფრთხოების რეფორმას მიიჩნევენ ერთერთ უმთავრეს მიზნად.

რეფორმა საჭირო გახდა საფრთხეების დიდი სისრაფით ზრდადობის გამო, მსოფლიოში ათობით მილიარდი მოწყობილობა უკავშირდება ქსელს, საფრთხეები კიდევ როგორც პროგრამული შეცდომების, ასევე ვირუსების და კიბერშეტევეის სახით სულ უფრო მატულობს.

რაც შეეხება ცნობიერების ამაღლებას, ევროპელების 51% თვლის რომ არ არის საკმარისად ინფორმირებული ამ საკითხში, ხოლო კომპანიების 69%-ს ელემენტარული ცოდნაც არ აქვთ კიბერ საფრთხეების კუთხით.

[8] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

ერთერთი წარმოდგენილი რეფორმაა ასევე კიბერუსაფრთხოების სერტიფიცირების სქემა, რომელიც წარმოადგენს გარკვეულ წესებს როგორც პროგრამულ ისე ტექნიკურ დონეზე.

ევროკომისია არ თვლის ENISA-ს საკმარისად ეფექტურად, და სურვილი აქვს ბევრად ძლიერი სააგენტო შექმნას რომ უფრო ეფექტურად იბრძოლოს კიბერსაფრთხეების წინააღმდეგ.[9]

2.2 ევროკავშირის ქვეყნების სახელმწიფო კიბერუსაფრთხოების სტატეგიები

ევროკომისიის შეხვედრებზე საკმაოდ ხშირად განიხილება კიბერუსაფრთხოების საკითხი, მას ხშირ შემთხვევაში აღნიშნავენ როგორც სახელმწიფო მნიშვნელობის სტრატეგიულ პრობლემას, რომელიც საზოგადოების ყველა ფენას და სახელმწიფოს ყველა სექტორს ეხება. კიბერუსაფრთხოების სახელმწიფო სტრატეგია არის საშუალება ამ კუთხით ქვეყნის შიგნით მოგვარდეს ეს პრობლემა, სტრატეგია ეს ის ინსტრუმენტია რომელიც პირველადი ნაბიჯია კონკრეტული მოქმედებებისკენ გადადგმული. ევროკავშირში წევრ ქვეყნებს სახელმწიფო კიბერუსაფრთხოების სტრატეგიის კუთხით კონსულტაციას უწევს ENISA, ისევე როგორც მთლიანად ევროკავშირის საერთო პოლიტიკის შემუშავებას.

ევროკავშირის ქვეყნებს ისევე როგორც ინდივიდუალური კანონმდებლობები, სხვადასხვა საკითხებში სტრატეგიებიც სხვადასხვა აქვთ, კიბერუსართხოების კუთხით ეს სხვაობები უფრო აშკარაა, რადგან ეს სფერო ჯერ კიდევ ჩამოუყალიბებელია და ყველა ტავისებურად ცდილობს გაუმკლავდეს, ENISA-ს როლი ამ მხრივ ამჟამად მხოლოდ კონსულტაციების დონეზეა.

[9] Reform of cyber security in Europe - http://www.consilium.europa.eu/en/policies/cyber-security/

პირველი სახელმწიფო კიბერუსაფრთხოების სტრატეგია ამერიკის შეერთებულ შტატებს ეკუთვნის, სწორედ აქ დაიწყეს პირველად კიბერსაფრთხეების რეალურ პრობლემად აღქმა.

პირველად ევროკავშირში კიბერუსაფრთხოების გეგმის შემუშავება გერმანიამ დაიწყო, რასაც მოყვა სხვა ევრო ქვეყნების მხრიდანაც იგივე ქმედებები, თუმცა პირველი კიბერუსაფრთხოების სახელმწიფო სტრატეგია ევროპაში გამოაქვეყნა ესტონეთმა 2008 წელს. [10]

დაბლა მოკლედ მიმოხილულია ევროკავშირის ქვეყნების მიერ გამოქვეყნებული ყველა სახელმწიფო კიბერსტრატეგია, რომელიც გამოქვეყნებულია 2018 წლის ივნისის ჩათვლით.

ავსტრია (2013)

ტექნოლოგიურმა რევოლუციამ ფეხი მოიკიდა ყველა სფეროში და ყველა განვითარებული ქვეყანა ცდილობს კიბერსივრცის სიკეთეები გამოიყენოს საკუთარი ტექნოლოგიური, ეკონომიკური, სოციალური, კულტურული, სამეცნიერო და პოლიტიკური განვითარებისთვის. ტექნოლოგიურმა განვითარებამ და ინტერნეტმა სრულად შეცვალა ყველა სფერო, უფრო კომფორტული გახადა ისინი. ავსტრიის მოსახლეობის ¾ რეგულარულად იყენებს ინტერნეტს, მათ შორის ნახევარი ყოველდღიურად.[11]

ავსტრიის კიბერუსაფრთხოების სტრატეგია არის ყოვლისმომცველი აქტიური კონცეპტი კიბერსივრცის დასაცავად და ვირტუალურ სამყაროში ადამიანების

[10] ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები და რეკომენდაციები. საქართველოს კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები (კრებული) - ვლადიმერ სვანაძე

[11] ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები და რეკომენდაციები. საქართველოს კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები (კრებული) - ვლადიმერ სვანაძე

უსაფრთხოების შესაქმნელად, ისე რომ არ დაირღვეს ადამიანთა უფლებები. ასევე მიზანია ამ კუთხით ავსტრიის მოქალაქეების ცნობიერების ამაღლება.

კიბერუსაფრთხოების კუთხით ავსტრიის სტრატეგიული მიზნებია:

- ინფორმაციის გაცვლის ხელმისაწვდომობა, საიმედოობა, კონფიდენციალურობა შესაძლებელია მხოლოდ დაცულ, საიმედო და სტაბილური კიბერსივრცის პირობებში. ამასთან კიბერსივრცე უნდა იყოს მზად ცვლილებებისთვის და გადაეწყოს შესაბამისად, რომ შენარჩუნდეს ძირითადი ჩამოთვლილი მიზნები.
- კიბერუსაფრთხოების უზრუნველყოფისთვის ავსტრია ვალდებულებას იღებს უზრუნველყოს კიბერსაფრთხეებისგან დაცულობა და ითანამშრომლოს კერძო სექტორთან.
- ლეგალური აქტივი „კიბერუსაფრთხოების“ სახით დაცულია ავსტრიის ხელისუფლების მიერ, არასამთავრობო ორგანიზაციებთან პარტნიორობით.
- ცნობიერების ამაღლების მეთოდით ავსტრია ქმნის „კიბერუსაფრთხოების კულტურას.“
- კიბერუსაფრთხოებაზე საუბრის და სხვადასხვა ორგანიზაციებთან პარტნიორობის ფონზე, ახალი ინიციატივები ამ კუთხით მხარდაჭერილია და აქტიურად განიხილება. შესაბამისად ავსტრია ბიზნესისთვის სანდო ადგილად მიიჩნევა.
- ავსტრია აქტიურად მიიღებს მონაწილეობას საერთაშორისო და განსაკუთრებით ევროპის კიბერუსაფრთხოების განვითარების სტრატეგიებში, ინფორმაციის გაცვლის მეთოდით და პარტნიორობით.
- ავსტრიაში ინტერნეტ-ხელისუფლება დაცულია და განუწყვეტლივ ვითარდება. როგორც დედაქალაქში ისე პროვინციებში დროთა განმავლობაში ინტერნეტუსაფრთხოება განვითარდება.

- ყველა ავსტრიული საწარმო უზრუნველყოფს საკუთარი ვირტუალური სივრცის უსაფრთხოებას, ისევე როგორც დასაქმებულების ვინაობას და უსაფრთხოებას.
- ავსტრიელმა მოქალაქეებმა უნდა იცოდნენ კიბერსივრცეში პირადი პასუხისმგებლობა და თუ როგორ დაიცვას საკუტარი ონლაინ აქტივობები.

ბელგია (2014)

ბელგიაში შემუშავდა სპეციალური კანონმდებლობა კიბერდანაშაულების წინააღმდეგ. კანონმდებლობა შეეხო ონლაინ კომუნიკაციას, ონლაინ ხელმოწერებს და სერტიფიცირებას, საინფორმაციო საზოგადოებას, პირადი ცხოვრების და პერსონალური მონაცემების დაცვას.

ბელგიაში ოფიციალურად მოქმედებს კიბერ ინციდენტების აღმოჩენის და აღმოფხვრის სტრუქტურა. ცალკეა გამოყოფილი ონლაინში ბავშვთა დაცვის ინსტიტუტი. ასევე მოქმედებს ცალკეული ვებგვერდი ონლაინ ბავშვთა პორნოს გავრცელების დასარეპორტებლად.

ბულგარეთი (2016)

ბულგარეთს საკუთარი კიბერუსაფრთხოების სტრატეგია 9 პუნქტად აქვს დაყოფილი:

1. სახელმწიფო მდგრადი კიბერუსაფრთხოების სისტემის ჩამოყალიბება, ცნობიერების ამაღლება და კოორდინირებული პრევენცია.
2. ქსელის და ინფორმაციის უსაფრთხოება როგორც კიბერმდგრადობის ფუნდამენტი.
3. ინფორმაციულ ტექნოლოგიებზე დამოკიდებული ინფრასტრუქტურის დაცულობის გაუმჯობესება.
4. სახელმწიფოს, ეკონომიკას და მოსახლეობას შორის უკეთესი თანამშრომლობა.

5. სამართლებრივი და მარეგულირებელი ხელშეკრულება.
6. კიბერდანაშაულების წინააღმდეგ ბრძოლა.
7. კიბერთავდაცვა. (იგულისხმება როგორც ვირტუალური ისე ფიზიკური)
8. ცნობიერების ამაღლება, განათლება და ინოვაციები.
9. საერთაშორისო თანამშრომლობა: EU, NATO, OSCE, UN, ITU, ICANN და რეგიონალური მეზობლები.

ხორვატია (2015)

ხორვატიას მოზრდილი დოკუმენტი აქვს ამ თემაზე, თუმცა ჩვენ გამოვყოფთ ცალკე სტრატეგიებს.

1. სისტემური მიდგომა და ნაციონალური კანონმდებლობის განვითარება.
2. კიბერსივრცის მდგადობის, საიმედოობის და უსაფრთხოების განვითარების მიზნით სპეციალური ღონისძიებების გატარება.
3. ინფორმაციის გაზიარების უფრო საიმედო მექანიზმების შემუშავება.
4. უსაფრთხოების ცნობიერების ამაღლება.
5. სასწავლო პროგრამების განვითარებაზე ხელშეწყობა.
6. ონლაინ სერვისების განვითარებაზე ხელშეწყობა.
7. კვლევის და განვითარების ხელშეწყობა.
8. საერთაშორისო თანამშრომლობაზე სისტემური მიდგომა.

ჩეხეთის რესპუბლიკა (2011)

- კიბერუსაფრთხოების კუთხით ყველა სახის სტრუქტურების, პროცესების და თანამშრომლობის ეფექტურობა და გაფართოება
- აქტიური საერთაშორისო თანამშრომლობა

- სახელმწიფო კრიტიკული ინფორმაციული ინფრასტრუქტურის და მნიშვნელოვანი ინფორმაციული სისტემების დაცულობა.
- კერძო სექტორთან თანამშრომლობა.
- კვლევა და განვითარება / მომხმარებელთა ნდობა
- სწავლა, ცნობიერების ამაღლება და ინფორმაციული სოციუმის განვითარება.
- ჩეხეთის პოლიციის დახმარება კიბერდანაშაულთან ბრძოლაში.
- კიბერუსაფრთხოების კანონმდებლობის შემუშავება და ევროკავშირის რეგულაციების შემუშავებაში მონაწილეობა.

კვიპროსის რესპუბლიკა (2013)

კვიპროსის რესპუბლიკა საკუთარი კიბერუსაფრთხოების სისტემის განვითარებისთვის მკაცრად ითვალისწინებს ევროკავშირის ზოგად მითითებებს და რჩევებს. მათი სტრატეგია გულისხმობს ელექტრონული ბიზნესის პლატფორმის განვითარებას და ხელშეწყობას, ინფორმაციული სოციუმის განვითარებას, ნდობის მოპოვებას როგორც მოქალაქეებში ისე ონლაინ ბიზნესებისთვის, უსაფრთხო ელექტრონული სისტემის ჩამოყალიბებას, კიბერსაფრთხეებზე ეფექტურ რეაგირებას, კრიტიკული ინფრასტრუქტურების დაცულობის განვითარებას.

დანია (2018)

ისევე როგორც მთელ მსოფლიოში, დანიაშიც აქტიურად და სწრაფად ვითარდება ინფორმაციული ტექნოლოგიები, შესაბამისად უფრო და უფრო მეტი სფერო უერთდება ინტერნეტს, საზოგადოება და ბიზნესები ხდება ინტერნეტის შესაძლებლობებზე დამოკიდებული.

დანია ერთერთი ყველაზე ტექნოლოგიური სახელმწიფოა მსოფლიოში, ინფორმაციული ტექნოლოგიების განვითარება სახალხო სექტორის განვითარების და ბიზნესების კონკურენტუნარიანობის გაზრდის გასაღებია.

მოქალაქეები ინტერნეტის საშუალებით ამყარებენ კონტაქტს როგორც სახელმწიფო სერვისებთან ასევე ბიზნესებთან, დაცული საშუალებებით რომელიც პირად ინფორმაციას პატივს ცემს.

ნდობა სრულად არის დამყარებული კობერსივრცის დაცულობაზე, როგორც შიდა ისე გარე კიბერშეტევებისგან.

2018 წელს დანიამ 1.5 მილიარდი ჩადო კიბერუსაფრთხოებასა და ინფორმაციულ დაცულობაში. ამ წლების განმავლობაში დანია წარმოადგენს 25 ინიციატივას, რომლებიც მიმართული იქნება კიბერ სექტორში ყველაზე კრიტიკული მხარეების განვიტარებისკენ.

კიბერსაფრთხეების სრულად აღმოფხვრა შეუძლებელია, თუმცა დანიის მთავრობა იღებს პასუხისმგებლობას უზრუნველყოს საკუთარი მოქალაქეების დაცულობა ინტერნეტში.

ესტონეთი (2014)

კიბერუსაფრთხოების უზრუნველყოფის პრინციპები:

- კიბერუსაფრთხოება სახელმწიფო უსაფრთხოების ნაწილია. ის უზრუნველყოფს სოციუმის, სახელმწიფოს, ეკონომიკის და ინოვაციების ფუნქციონალურობას.
- კიბერუსაფრთხოება მოქალაქისთვის ფუნდამენტალური უფლებებით, ინდივიდუალური თავისუფლებით და პერსონალური ინფორმაციის დაცვით არის გარანტირებული.
- კიბერუსაფრთხოება უზრუნველყოფილია პროპორციულობის ბაზაზე, კიბერსაფრთხეების გათვალისწინებით.
- კიბერუსაფრთხოება უზრუნველყოფილია კერძო და სახალხო სექტორთან თანამშრომლობით.
- კიბერუსაფრთხოების საწყისია ინდივიდუალური პასუხისმგებლობა.

- განსაკუთრებული მნიშნელობის არის ისეთი სახის კიბერსაფრთხეები რომლებიც შეიძლება რეალურ სამყაროში გავრცელდეს რაიმე სახით.
- კიბერუსაფრთხოება მხარდაჭერილია საერთაშორისო კვლევებით.
- კიბერუსაფრთხოება უზრუნველყოფილია საერთაშორისო თანამშრომლობით. ასევე ესტონეთი ხელს უწყობს მსოფლიო კიბერუსაფრთხოების განვითარებას.

ფინეთი (2013)

როგორც პატარა, ერთიან და ქმედით ქვეყანა ფინეთს დიდი შანსები აქვს ავანგარდში ჩაუდგეს კიბერუსაფრთხოებას. მათ აქვთ ვრცელი საბაზისო ცოდნა და ძლიერი ექსპერტიზა, დიდი ტრადიციები სახალხო სექტორთან ახლო თანამშრომლობაში, რომელიც დაფუძნებულია ნდობაზე, ასევე შიდა სექტორული თანამშრომლობა.

ფინეთის ხედვა კიბერუსაფრთხოების კუთხითგამოიყურება ასე:

- ფინეთს შეუძლია უზრუნველყოს კიბერსაფრთხეებისგან სასიცოცხლო მნიშვნელობის ფუნქციების დაცვა ნებისმიერ სიტუაციაში.
- მოსახლეობას, მთავრობას და ბიზნეს სექტორს შეუძლია ინტერნეტში ეფექტურად იმუშაოს უსაფრთხოების წესების დაცვით.
- 2016 წლისთვის ფინეთი იქნება წამყვანი ქვეყანა კიბერსაფრთხეებთან ბრძოლის კუთხით.

საფრანგეთი (2015)

საფრანგეთს გამოყოფილი აქვს 5 სტრატეგიული ამოცანა:

1. სახელმწიფო საინფორმაციო სისტემების და კრიტიკული ინფრასტრუქტურის დაცვა და უსაფრთხოების უზრუნველყოფა.
2. ელექტრონული ნდობა, კონფიდენციალურობა და პირადი ინფორმაციის დაცვა, კიბერდაცულობა.

3. ცნობიერების ამაღლება, ტრენინგები და განათლების განვითარება.

4. ელექტრონული ბიზნესის ხელშეწყობა, ინტერნეტ დანაშაულების კონტროლი.

5. ევროპასთან თანამშრომლობა, კიბერსტრატეგიის ავტონომია, კიბერსივრცის სტაბილურობა.

გერმანია (2011)

გერმანიის ფედერაციის სტრატეგია დაფუძნებულია მიმდინარე საფრთხეებსა და კრიტიკული ინფრასტრუქტურის დაცულობის გეგმაზე. გერმანია 10 პუნქტზე ამახვილებს ყურადღებას:

1. კრიტიკული ინფორმაციული სტრუქტურების დაცვა.

2. ინფორმაციული ტექნოლოგიების სისტემების დაცვა.

3. საჯარო ადმინისტრირების სექტორში ინფორმაციული ტექნოლოგიური უსაფრთხოების გაძლიერება.

4. სახელმწიფო კიბერრეაგირების ცენტრი

5. სახელმწიფო კიბერუსაფრთხოების საბჭო.

6. კიბერსივრცეში კრიმინალის ეფექტური კონტროლი.

7. ეფექტური კოორდინირებული მოქმედება კიბერუსაფრთხოების ევროპასა და მსოფლიოში უზრუნველსაყოფად.

8. საიმედო და სანდო ინფორმაციული ტექნოლოგიების გამოყენება.

9. ფედერალური ხელისუფლების ორგანოებში პერსონალის განვითარება.

10. კიბერშეტევების წინააღმდეგ ინსტრუმენტები.

საბერძნეთი (2017)

A. უსაფრთხო და სტაბილური კიბერსივრცის განვიტარება და დამკვიდრება, სახელმწიფო, ევროკავშირის და საერთაშორისო კანონების,

პრაქტიკის და სტანდარტების გათვალისწინებით, ისე რომ დაცული იყოს მოქალაქეებისა და ბიზნეს სექტორის ძირეული უფლებები.

B. კიბერსაფრთხეების წინააღმდეგ ბრძოლის შესაძლებლობების უწყვეტი განვითარება, კრიტიკული ინფრასტრუქტურების პრიორიტეტულობით.

C. ეროვნული კიბერუსაფრთხოების სტრუქტურის ინსტიტუციური დაცვა, კიბერშეტევების და კიბერსაფრთხეების მინიმიზირების მიზნით.

D. სახალხო და კერძო სექტორის უსაფრთხოების კულტურის განვითარება.

უნგრეთი (2013)

უნგრეთის კიბერსივრცის უსაფრთხოება შედის უნგრეთის სახელმწიფო ინტერესებში. ასევე თავისუფალი, დემოკრატიული და უსაფრთხო კიბერსივრცის ფუნქციონირება, კანონების გათვალისწინებით. უნგრეთის კიბერსივრცის უსაფრთხოება და თავისუფლება უზრუნველყოფილია კერძო, სახალხო და ბიზნეს სექტორთან თანამშრომლობით, ყველა მათგანის პასუხისმგებლობით.

ირლანდია (2015)

ირლანდიის კიბერუსაფრთხოების სტრატეგიის კუთხით დასახული ამოცანებია:

- კრიტიკული საინფორმაციო ინფრასტრუქტურის და მნიშვნელოვანი ეკონომიკური სექტორების მდგრადობის და სიმტკიცის განვითარება, განსაკუთრებით საჯარო სექტორში.
- საერთაშორისო პარტნიორებთან და ორგანიზაციებთან ჩართულობის გაგრძელება, კიბერსივრცის უსაფრთხოების, თავისუფლების და ბიზნეს სექტორის განვიტარების უზრუნველსაყოფად.
- ბიზნესების და კერძო პირების პირადი ქსელების, მოწყობილობების და ინფორმაციის დაცულობის პასუხისმგებლობის, ცნობიერების ამაღლება, მათი ამ საკითხებში ხელშეწყობა და ტრენინგი.

- კიბერსაფრთხეების წინააღმდეგ შესაბამისი კანონმდებლობის შემუშავება.
- მარეგულირებელი ხელშეკრულების უზრუნველყოფა, პერსონალური ან სხვა ინფორმაციის მფლობელებისთვის, რომელიც იქნება ძლიერი, პროპორციული და სამართლიანი.
- საჯარო ადმინისტრირების და კერძო სექტორის შესაძლებლობების გაზრდა კიბერინციდენტების მართვის მხრივ.

იტალია (2013)

სახელმწიფო კიბერუსაფრთხოების სტრატეგიის ხელშეკრულება და შესაბამისი სახელმწიფო გეგმა, ორივე გათვალისწინებულია პრემიერ მინისტრის 2013 წლის 24 იანვრის განკარგულებაში რომელიც მოიცავს სტრატეგიულ მითითებებს კიბერუსაფრთხოების უზრუნველყოფის კუთხით. მიზანია სახელმწიფო მზადყოფნაში ყოფნა კიბერსივრცეში მიმდინარე და მომავალი გამოწვევებისთვის. იმის გათვალისწინებით რომ ტექნოლოგიების განვიტარებას მოსდევს ახალი საფრთხეები და დღევანდელი მდგომარეობით არ არის ეფექტური.

ლატვია (2014)

კიბერუსაფრთხოების პოლიტიკის მიზანია საიმედო კიბერსივრცის უზრუნველყოფა, უსაფრთხო, საიმედო სერვისებისთვის რაც მნიშვნელოვანია სახელმწიფოსა და სოციუმისთვის.

კიბერსაფრთხეების წინააღმდეგ ბრძოლა შესაძლებელია თუ კი სისტემატურად მოხდება კიბერუსაფრთხოების სისტემის განვითარება და უნარების გაუმჯობესება.

კიბერსაფრთხეების წინააღმდეგ ეფექტური ბრძოლისთვის საჭიროა სახელმწიფოს შიდა და საერთაშორისო დონის თანამშრომლობა.

კიბერსაფრთხეების შემცირება შესაძლებელია თუ კი მონაწილეობას მიიღებს ყველა სექტორი, როგორც სახელმწიფო, ისე კერძო და საჯარო.

კიბერუსაფრთხოების პოლიტიკა უნდა შემუშავდეს ისე რომ გათვალისწინებული იყოს პიროვნების ფუნდამენტალური უფლებები და თავისუფლებები.

ლიეტუვა (2011)

1. სახელმწიფო საინფორმაციო რესურსების უსაფრთხოების უზრუნველყოფა.
2. კრიტიკული საინფორმაციო სტრუქტურების ეფექტური მუშაობის უზრუნველყოფა.
3. ლიეტუვას მოქალაქეებისთვის და ადამიანებისთვის ვინც ლიეტუვაში ჩერდებიან კიბერუსაფრთხოების უზრუნველყოფა.

ლუქსემბურგი (2018)

1. სახელმწიფოს შიდა თანამშრომლობის გაძლიერება.
2. საერთაშორისო თანამშრომლობის გაძლიერება.
3. ელექტრო ინფრასტრუქტურის საიმედოობის გაზრდა.
4. კიბერდანაშაულის წინააღმდეგ ბრძოლა.
5. ინფორმაციის მიწოდება, ტრენინგი და ცნობიერების ამაღლება.
6. სტანდარტების, ნორმების, სერთიფიკატების შემუშავება საინფორმაციო კრიტიკული ინფრასტრუქტურებისთვის.
7. თანამშრომლობის გაძლიერება აკადემიურ და კვლევით სფეროსთან.

მალტა (2016)

- კიბერდანაშაულთან ბრძოლა.
- სახელმწიფო კიბერუსაფრთხოების გაძლიერება.
- კიბერსივრცის დაცვა.
- კიბერუსაფრთხოების შესახებ ცნობიერების ამაღლება და განათლება.
- სახელმწიფო ხელშეკრულების შემუშავება კიბერუსაფრთხოების კუთხით.

- სახელმწიფო და საერთაშორისო თანამშრომლობა.
- სახელმწიფო საინფორმაციო ინფრასტრუქტურის დაცვა კიბერსაფრთხეებისგან.
- მოხმარებელთა კიბერსივრცის უსაფრთხოების უზრუნველყოფა.

ნიდერლანდები (2018)

- ნიდერლანდები კიბერშეტევებისადმი სტაბილურია და და იცავს საკუთარ საციცოხლო მნიშვნელობის ინტერესებს საინფორმაციო სფეროში.
- ნიდერლანდები ებრძვის კიბერდანაშაულს.
- ნიდერლანდები ნერგავს კიბერუსაფრთხოების სერვისებს და პროსუქტებს კონფიდენციალურობის დასაცავად.
- ნიდერლანდები ქმნის კოალიციებს კიბერ თავისუფლებისთვის, უსაფრთხოებისთვის და მშვიდობისთვის.
- ნიდერლანდებს აქვს საკმარისი ცოდნა კიბერუსაფრთხოების კუთხით რომ ამ მხრივ შემოიღოს/შექმნას ინოვაციები.

პოლონეთი (2017)

პოლონეთის ძირითადი მიზანია უზრუნველყოს მაღალი დონის უსაფრთხოება კერძო,საჯარო სექტორებისთვის და პიროვნებებისთვის, მნიშვნელოვანი ინფორმაციული სერვისების გამოყენებისას.

პოლონეთი გადადგამს კონკრეტულ მიზანმიმართულ ნაბიჯებს კიბერინციდენტების პრევენციის მიზნით. მნიშვნელოვნად გააძლიერებს კიბერსაფრთხეების წინააღმდეგ ბრძოლის საშუალებებს. სახელმწიფო პოტენციალს გაზრდის კიბერუსაფრთხოების კუთხით და საერთაშორისო დონეზე სახელს მოიხვეჭს კიბერუსაფრთხოების განვითარებაში.

პორტუგალია (2015)

პორტუგალიის კიბერუსაფრთხოების სქემა 6 პუნქტისგან შედგება:

1. კიბერსივრცის უსაფრთხოების სტრუქტურა.
2. კიბერდანაშაულთან ბრძოლა.
3. კიბერსივრცის და სახელმწიფო ინსფრასტრუქტურის დაცვა.
4. სწავლა, ცნობიერების ამაღლება და პრევენცია.
5. კვლევა და განვითარება.
6. თანამშრომლობა.

რუმინეთი (2011)

რუმინეთის მიზანია უზრუნველყოს ნორმალური და შემცირებადი რისკები კიბერსივრცეში, ცოდნის, შესაძლებლობების და მექანიზმების გაუმჯობესებით.

1. კონცეპტუალური, მოქმედი და ორგანიზებული კანონმდებლობის შექმნა კიბერუსაფრთხოების უზრუნველსაყოფად.
2. სახელმწიფო რისკების მენეჯმენტის განვითარება და ქმედითი ნაბიჯების გადადგმა კიბერუსაფრთხოებაში.
3. კიბერსფეროში უსაფრთხოების კულტურის განვითარება და ხელშეწყობა.
4. საერთაშორისო თანამშრომლობის განვითარება კიბერუსაფრთხოებაში.

სლოვაკეთი (2015)

- სახელმწიფო კიბერსივრცის დაცვა.
- კიბერუსაფრთხოებისკუთხით ცნობიერების ამაღლება.
- შიდა სახელმწიფო თანამშრმლობა.
- საერთაშორისო თანამშრომლობა.
- კიბერუსაფრთხოების უზრუნველყოფისას ადამიანების ფუნდამენტური უფლებების გათვალისწინება.

სლოვენია (2016)

- სისტემური რეგულაციების გაძლიერება კიბერუსაფრთხოებაში.
- კიბერსივრცეში მოქალაქეთა დაცვა.
- ეკონომიკაში კიბერუსაფრთხოება.
- კრიტიკული ინფრასტრუქტურის სტაბილურობის უზრუნველყოფა.
- საჯარო უსაფრთხოების და კიბერდანაშაულთან ბრძოლის უზრუნველყოფა.
- თავდაცვითი კიბერშესაძლებლობების განვითარება.
- დაცული ონლაინ ოპერაციების და მნიშვნელოვანი ინფრასტრუქტურების სტაბილური მუშაობის უზრუნველყოფა.
- საერთაშორისო ტანამშრომლობის დახმარებით კიბერუსაფრთხოების გაძლიერება.

ესპანეთი (2013)

- ტელეკომუნიკაციის სისტემების, რომლებიც გამოიყენება ხელისუფლების წაწმომადგენლების მიერ, უსაფრთხოების უზრუნველყოფა.
- ბიზნეს სექტორის და კრიტიკული ინფრასტრუქტურის სატელეკომუნიკაციო საშუალებების უსაფრთხოების უზრუნველყოფა.
- კიბერტერორიზმის აქტივობების აღმოჩენის, პრევენციის, მოქმედების, ანალიზის, აღდგენის, კვლევის განვითარება.
- კიბერსივრციდან მომავალი საფრთხეების შესახებ ცნობიერების ამაღლება.
- კიბერუსაფრთხოების ამოცანების შესახებ ინფორმაციის, უნარჩვევების მოპოვება.

შვედეთი (2017)

მთავრობის მიზანია შექმნას ძლიერი პლატფორმა რომელიც გრძელვადიან პერსპექტივაში იმუშავებს კიბერუსაფრთხოების უზრუნველსაყოფად. მთავრობის

მიზანია ამ სფეროს ყველა ნაწილის ცალკეული ამოცანების დასახვა და ყველა მათგანის გადაჭრა. ამოცანების გადაჭრის მიზნით შეიქმნება სპეციალური კომისიები და სამსახურები.

იქედან გამომდინარე რომ უსაფრთხოების გამოწვევების ერთხელ და საბოლოოდ გადაწყვეტა შეუძლებელია, იმ მიზეზებიტ რომ ციფრული ტექნოლოგიები განუწყვეტლივ ვითარდება, სტრატეგია უნდა იყოს მოქნილი და ეგრებოდეს კიბერსივრცის ცვლილებებს. შვედეთის მთავრობა გეგმავს პირველი მსგავსი პრაქტიკა დაამყაროს 2018 წელს.

დიდი ბრიტანეთი (2016)

- ჩვენი მოქმედებები და პოლიტიკა იქნება დაფუძნებული ჩვენი ხალხის დასაცავად და კეთილდღეობისთვის.
- კიბერთავდასხმას მივიღებთ ისე როგორც რეალურ თავდასხმას და პასუხიც იქნება შესაბამისი.
- ჩვენ ვიმოქმედებს საერთაშორისო და სახელმწიფო კანონების გათვალისწინებით და იგივეს ველით სხვისგანაც.
- ჩვენ დავიცავთ ჩვენს ძირეულ ფასეულობებს რაც გულისხმობს დემოკრატიას, კანონმორჩილებას, თავისუფლებას, ღია მთავრობებს და ინსტიტუტებს, ადამიანის უფლებებს და გამოხატვის თავისუფლებას.
- ჩვენ დავიცავთ დიდი ბრიტანეთის მოქალაქეების კონფიდენციალურობას.
- კიბერსივრცის დასაცავად ვითანამშრომლებთ ყველა სექტორთან.
- სახელმწიფო იღებს პასუხისმგებლობას საერთაშორისო დონეზე, მაგრამ ბიზნესები და მოქალაქეები პასუხისმგებლები არიან საკუთარ ნაბიჯებზე.
- საჯარო სექტორში პასუხისმგებლობა ეკისრებათ შესაბამის წარმომადგენლებს.

- არ დავუშვებთ არანაირ რისკს კიბერსაფრთხეებისგან თავის ასარიდებლად.
- ვითანამშრომლებთ იმ ქვეყნებთან ვინც იზიარებს ჩვენს ხედვებს.
- გავაანალიზებთ კიბერუსაფრთხოების მოქმედებას არამარტო ტექნიკურ მხარეში არამედ პროგრამულშიც, უსაფრთხოების უზრუნველყოფის მიზნით.[12]

2.3 ევროკავშირის ინფორმაციის და ქსელების უსაფრთხოების სააგენტო - ENISA და სხვა სააგენტოები

ევროკავშირის ქსელების და ინფორმაციის უსაფრთხოების სააგენტო (ENISA) არის ევროპის ქსელებისა და ინფორმაციის უსაფრთხოების ცენტრი. ENISA მუშაობს სხვადასხვა ჯგუფებთან ერთად, რომ შეიმუშაოს რჩევები და რეკომენდაციები ინფორმაციის უსაფრთხოების კუთხით.

ENISA ტერიტორიულად მდებარეობს საბერძნეთში, ჰერაკლიონში კრეტაზე, ხოლო მისი სათაო ოფისი მდებარეობს ათენში. მას შემდეგ რაც ENISA დაარსდა 2004 წელს, ის აქტიურად უზრუნველყოფს ევროკავშირში ქსელების და ინფორმაციის უსაფრთხოებას და ამ კუთხით ცნობიერების ამაღლებაზეც აქტიურად მუშაობს.

ENISA-ს მუშაობა მოიცავს კიბერუსაფრთხოების ლექციების ჩატარებას, ნაციონალური კიბერუსაფრთხოების სტრატეგიების შემუშავებას, პროგრამული უზრუნველყოფის დანერგვას და ქსელებისა და ინფორმაციის უსაფრთხოების კუთხით კანონმდებლობების შემუშავებაშიც იღებს მონაწილეობას.

ENISA-ს მიზანია კიბერუსაფრთხოების კუთხით ცნობიერების ამაღლება, ევროკავშირის მოქალაქეების, მომხმარებლების და სახალხო ორგანიზაციების

[12] National Cyber Security Strategies (NCSSs) Map - https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

სასარგებლოდ. ENISA მიზნის მისაღწევად მიკერძოების გარეშე დაეხმარება და შეასრულებს საკუთარ მისიას ევროპის ყველა ქვეყანაში. ENISA ევროკავშირის ყველა წევრ ქვეყანას სთავაზობსმასთან დაკავშირების საშუალებას კონსულტაციების მიზნით.

ENISA-ს სტრატეგიები და სტრატეგიული ამოცანებია:

ENISA-ს მიერ გამოცემული დოკუმენტი რომელიც მოიცავს მის სტრატეგიებს 2016-2020 წელში:

- **ექსპერტიზა.** ევროპის მხარდაჭერა და მომზადება ქსელების და ინფორმაციის უსაფრთხოების კუთხით. შედარებით, ანალიზით და ექსპერტიზით, კიბერუსაფრთხოების ძირითად პრობლემურ საკითხებზე, რომლებიც პოტენციურად შეიძლება შეეხოს ევროკავშირს, ტექნოლოგიების განვითარების გათვალისწინებით.
- **პოლიტიკა.** კიბერუსაფრთხოების ევროპის პრიორიტეტულ საკითხად ქცევაზე ხელის შეწყობა. ევროკავშირის შესაბამის ინსტიტუტებზე და ევროპის ქვეყნებზე დახმარება ამ კუთხით კანონმდებლობების შემუშავებაში.
- **შესაძლებლობები.** ევროპის ქვეყნებზე ხელშეწყობა მათი კიბერუსაფრთხოების შესაძლებლობების გაზრდის მიზნით. მათი სახმარება ამ კუთხით გაძლიერების მიზნით,
- **თანამეგობრობა.** ევროპული ქვეყნების ქსელების გაერთიანების დასწრაფება. ევროპის ქვეყნებს შორის თანამშრომლობის გაძლიერებით,
- **გარემოს შექმნა.** ENISA-ს გავლენის გაზრდა. მენეჯმენტის გაუმჯობესებით და დაინტერესებულ ქვეყნებთან წვდომის გაზრდა როგორც ევროპაში ისე მსოფლიოში.

ტექნოლოგიური განვითარების სწრაფი ტემპის გამო, კიბერსაფრთხეების რაოდენობაც სწრაფად იმატებს ევროპაში, იქედან გამომდინარე რომ ყველა ეკონომიკური თუ სოციალური აქტივობა დღესდღეობით კომპიუტერიზებულია,

ტექნოლოგიური სოციუმის ზრდას აუცილებლად უნდა მოსდევდეს ინფორმაციული და ქსელების დაცვის მეთოდების ზრდა, რომ მივიღოთ სტაბილური გარემო.

ENISA-ს 2016 წლის მონაცემებით კიბერსაფრთხეების რაოდენობა ყოველწლიურად დიდი რაოდენობით მატულობს და ისინი განიცდიან ევოლუციას, რის შედეგადაც უფრო დიდი საფრთხის შემცველები ხდებიან, კიბერშეტევები სულ უფრო შედეგიანები ხდება, ხოლო კიბერუსაფრთხოების მეთოდები ვერ ეწევა განვითარების სისწრაფით, შესაბამისად ვერ ნარჩუნდება სტაბილურობა.

შეჯიბრში ჰაკერებსა და დამცველებს შორის, ჰაკერები ყოველთვის 1 ნაბიჯით წინ არიან, თუმცა არის რაღაც ცვლილებებიც:

- დამცველებმა განავიტარეს საკუთარი შესაძლებლობები, კიბერსაფრთხეების საკუთარი სერვერებისკენ მიმართვით და მათი შესწავლით.
- დამცველებმა მიაგნეს დეანონიმიზაციის მეთოდს, რის შედეგადაც შეუძლიათ ჰაკერის იდენტიფიცირება დარქ ნეტშიც.
- დამცველებმა ისწავლეს რომ თავდაცვა მედალის მხოლოდ ერთი მხარეა და დაიწყეს შეტევის მეთოდის გამოყენება თავდასაცავად.
- ჰაკერებმა ფართო საზოგადოებისთვის ხელმისაწვდომი გახადეს ვირუსის კოდი რომ განევითარებინათ შესაძლებლობები.
- ჰაკერებმა დიდი შრომა და ინვესტიციები ჩადეს საკუთარი მომგებიანი პროდუქტების განვითარებაში.

ENISA-ს შექმნა გამოიწვია ევროკავშირის ქვეყნების არაერთგვაროვანმა პოლიტიკამ კიბერუსაფრთხოების კუთხით, ყველა მათგანმა იცის ამ სფეროს აუცილებლობა, მაგრამ არ იყო ურთიერთშეთანხმებული ქმედებები, მისი მიზანია მათ შორის შეასრულოს შუამავალის როლი, რათა მიიღონ საერთო სტანდარტები, ასევე გაუწიოს დახმარება და კონსულტაციები ყველა მათგანს ცალკეულად. ENISA

ფინანსდება ევროკავშირის ბიუჯეტიდან, ფინანსების მიზნობრიობას აკონტროლებს დანიშნული ბორდი.

ENISA კომუნიკაციის ძირითად საშუალებად იყენებს მედიას, იქედან გამომდინარე რომ ევროკავშირი მრავალ ქვეყანას მოიცავს, და მათ ევალებად ყოველ მათგანზე კონსულტაციები, როცა საქმე ეხება ახალ აღმოჩენებს, კვლევებს თუ რჩევებს, ის ენდობა მედიას როგორც ინფორმაციის სწრაფ გამავრცელებელს. სააგენტოში მუშაობს 60 მუდმივ მომუშავე მაღალი დონის სპეციალისტი, ევროპის 27 სხვადასხვა ქვეყნიდან, გარდა ამისა მუშაობს რამდენიმე დროებითი დაქირავებული სპეციალისტიც.

ENISA-ს საფრთხეებს შორის განსაკუთრებულ კიბერსაფრთხეების მაგალითებად მოყვანილი ყავს 2 კონკრეტული ვირუსი, რომლებსაც საერთაშორისო ინტერესიდან გამიმდინარე უფროდ დეტალურად განვიხილავთ: 2017-ში კიბერინციდენტების რაოდენობამ იმატა, განსაკუთრებული ყურადღება მიიპყრო ორმა ინციდენტმა სახელწოდებებით: Wannacry და Notpetya.

ENISA აქტიურად თანამშრომლობს ევროკავშირის ქვეყნებთან და უწევს კონსულტაციებს, მსგავსი სიტუაციების პრევენციის მიზნით.[13][14]

ევროპის კიბერდანაშაულის ცენტრი შეიქმნა 2013 წელს ევროპოლის მიერ, რომ გაეძლიერებინა კანონმდებლობის აღსრულების სქემა კიბერსივრცეში დანაშაულების წინააღმდეგ მოქალაქეების, მთავრობების და ორგანიზაციების კიბერდანაშაულისგან დაცვის მიზნით.

ევროპის კიბერდანაშაულის ცენტრი ყოველ წელს აქვეყნებს ანგარიშს: „ინტერნეტის ორგანიზებული კრიმინალის საფრთხეების შეფასება.“ რომელიც არის ძირითადი სტრატეგიული ანგარიში, კიბერდაშაულების განვითარების ძირითადი აღმოჩენების და საგანგაშო საფრთხეების შესახებ.

[13] About ENISA - https://www.enisa.europa.eu/about-enisa/mission-and-objectives
[14] ENISA PROGRAMMING DOCUMENT 2018–2020 - ნოემბერი 2017

სააგენტოს ყავს 2 სტრატეგიული ჯგუფი:

- ურთიერთობის და მხარდაჭერის, რომელიც ადგენს თანამშრომლობებს და კოორდინაციას უწევს პრევენციას და ცნობიერების ამაღლებას.
- სტრატეგია და განვითარება, რაც ითვალისწინებს:
  - სტრატეგიულ ანალიზს
  - პოლიტიკის ფორმულირებას.
  - სტანდარტიზებული ტრენინგების განვითარებას.

ევროპის კიბერდანაშაულის ცენტრი ძირიტად აქცენტს აკეტებს შემდეგ საკითხებზე:

- კიბერდამოკიდებული კრიმინალი
- ონლაინში ბავშვების სექსუალური ექსპლუატაცია
- ფინანსური თაღლითობა

სააგენტოს მენეჯმენტი განსაზღვრავს სააგენტოს პოლიტიკას, ადგენს თუ როგორ უნდა მიაღწიოს მიზანს, თანამშრომლობს სხვადასხვა სააგენტოებთან.

ევროპის თავდაცვის სააგენტო - EDA გარდა სხვა საკითხებისა აქტიურად მუშაობს კიბერუსაფრთხოების კუთხითაც. სააგენტო ეხმარება ევროკავშირის ქვეყნებს სამხედრო კიბერთავდაცვის კუთხით. გარდა ამისა მუშაობს კიბერუსაფრთხოების კუთხით ცნობიერების ამაღლებაზე.

კიბერუსაფრთხოება აქტუალური თემაა როგორც სამხედრო ისე საჯარო სფეროში, აქედან გამომდინარე სამხედრო სფეროზე ორიენტირებული სააგენტო მუშაობს საჯარო კუთხითაც.

III თავი - ევროკავშირში კიბერუსაფრთხოების მიმდინარე და სამომავლო გამოწვევები - ევრო-კიბერუსაფრთხოება პრაქტიკაში

ევროკავშირი აქტიურად განიხილავს კიბერუსაფრთხოების თემას უკვე მრავალი წელია, დგინდება ახალი სტრატეგიები, ხდება სტრატეგიის რეფორმები, აქვეყნებენ ანგარიშებს და მოქმედებს სხვადასხვა სააგენტოები ამ კუთხით, ამ ყველაფრის მიუხედავად ევროკავშირი მესამე მსოფლიოს ქვეყნების შემდეგ ერთერთი ყველაზე პრობლემურია ამ კუთხით, ვერცერთმა ცვლილებამ ვერ მოიტანა რეალური შედეგი, მეტიც კიბერსაფრთხეების რაოდენობა მატულობს, ეს ხდება მსოფლიო მასშტაბით, თუმცა როდესაც ევროკავშირს აქვს პრეტენზია იყოს წამყვანი ამ კუთხით, მას უსწრებენ ჩინეთიც, ამერიკის შეერტებული შტატებიც და ზუსტად არ არის დადგენილი მაგრამ შესაძლოა რუსეთიც კი.

3.1 ახალი და პოტენციური კიბერსაფრთხეები

რაც დრო გადის კიბერსაფრთხეები უფრო მრავალფეროვანი და კომპლექსური ხდება, თუ კი დროთა განმავლობაში მოიძებნა გზები უბრალო საფრთხეების წინააღმდეგ ბრძოლისთვის, ყოველთვის ჩნდება ახალი, უფრო რთული და საშიში საშუალებები.

Wannacry და Notpetya ეს არის ვირუსების ტიპი რომლების მოქმედებაც გასხვავდება სხვებისგან, ისინი ბლოკავენ სამიზნე კომპიუტერებს და მათ ბლოკი ეხსნებათ იმ შემთხვევაში თუ გადაიხდიან კონკრეტულ თანხას, ამ სახის კიბერშეტევის სახელწოდებაა: “Ransomware.”

ეს მეთოდი არ იქნებოდა ისე ცნობილი, რომ არა ეს ორი კიბერშეტევა სახელებით Wannacry და Notpetya.

Wannacry-ს თავდასხმის შედეგად მხოლოდ ინგლისში 80ზე მეტ ჯანმრთელობის დაცვის ორგანიზაციაში დაიბლოკა კომპიუტერები, რამაც გამოიწვია 20000 მიღების გაუქმება, 600 ოპერაციის გაუქმება, 5 საავადმყოფო საერთოდ შეცერდა რადგან ვეღარ მიიღებდა ახალ პაციენტებს.

ეს კიბერშეტევა არ იყო პირველი მსგავსი ტიპის შეტევა, ეს ხდებოდა მანამდეც, თუმცა დიდხანს ვერ გაძლო, რადგან ბანკში გადარიცხული თანხის მიგნება იოლი აღმოჩნდა. ამ შემთხვევაში კი ამ შეტევის განახლებული ვერსია გამოიყენეს, 2 ახალი ინოვაციის გამოყენებით მათი მიგნება შეუძლებელი გახდა, ესენია დაშიფრვა და კრიპტოვალუტა ბიტკოინი.

ადრეული მსგავსი ტიპის ransomware (Ransom - გამოსყიდვა) ვირუსებისგან პრევენცია იოლი იყო, იქედან გამომდინარე რომ მომხმარებელის ის უნდა გაეხსნა რომ დაინფიცირებულიყო, ეს ხდებოდა მეილით მოტყუებით და ა.შ. თუმცა Wannacry-მ შეცვალა სიტუაცია, Wannacry გახდა პირველი worm ტიპის ვირუსი რომელიც მსგავსი სისტემით მოქმედებდა, ამ ტიპს ეწოდა ransomworm, განსხვავება კი მდგომარეობდა მისი გავრცელების შესაძლებლობაში, ამ შემთხვევაში აღარიყო საჭირო ის მომხმარებელს თავად გაეხსნა, worm-ის უპირატესობა მდგომარეობს იმაში რომ მას შეუძლია საკუთარი თავის გამრავლება, ასევე ის დაძვრება სხვადასხვა კომპიუტერებსა და სერვერებზე, სწორედ აქედან გამომდინარეობს მისი სახელი worm - ჭია.

მიუხედავად ჭიის ტიპის ვირუსის შესაძლებლობებისა, მისი სუსტი მხარე არის ადვილად მიგნებადობა და ამოცნობა, ხოლო უსაფრთხოების პროგრამული უზრუნველყოფების განვითარების შედეგად worm ტიპის ვირუსები დიდი ხანია აღარ გამოჩენილა, სანამ არ გამოჩნდა Wannacry, აქედან შეგვიძლია დავასკვნათ თუ რამხელა შრომაა ჩადებული ამ ვირუსში. Wannacry-ს საბედისწერო მომენტი გახდა, როდესაც ინკოგნიტო ჰაკერთა ჯგუფმა მაიქროსოფთს მიუთითა ვინდოუსის სუსტ

წერტილზე, რასაც Wannacry იყენებდა გავრცელებისთვის, რის შემდეგაც მაიქროსოფთმა გამოუშვა სპეციალური patch (პაჩი-დანამატი) და ამოავსო ხვრელი.

მალე გამოჩნდა ახალი ვირუსი Notpetya რომელიც ვრცელდებოდა უკრაინაში ფართოდ გამოყენებადი გატეხილი პროგრამის საშუალებით, მიუხედავად ამისა მან დაიპყრო ფარმაცევტული კომპანია. მიუხედავად მცირე მასშტაბისა, დესტრუქციულობის მხრივ Notpetya-ს უფრო დამანგრეველად მიიჩნევენ ვიდრე Wannacry-ს, იქედან გამომდინარე რომ, ამ ტიპის ვირუსების აზრი მდგომარეობს ფინანსურ მოგებაში, რის შემდეგაც კომპიუტერზე წვდომას უბრუნებენ პატრონს, თუმცა Notpetya სრულად ანადგურებდა კომპიუტერში არსებულ ინფორმაციას, მისი აღდგენის შესაძლებლობის გარეშე.

ვინდოუსში არსებული სუსტი მხარეები ნელნელა ამოივსო და თითქოს მორჩა ამ ტიპის ვირუსის გავრცელება, თუმცა გამოჩნდა ახალი ტიპის ვირუსი, რომელიც სხვა საშუალებით ვრცელდება, გავს ransomware ვირუსს, თუმცა განსხვავებული მეთოდით მოქმედებს, თუ კი ransomware ვირუსი ბლოკავდა კომპიუტერს, doxware ვირუსი თანხის გადაუხდელობის შემთხვევაში არსებულ ინფორმაციას ხდის საჯაროს და ავრცელებს ინტერნეტის საშუალებით.[15]

მონაცემთა ბაზებში შეღწევა და ინფორმაციის მოპარვა არ არის ახალი საფრთხე, თუმცა ის დღესაც ისევე აქტუალურია როგორც წინა წლებში.

“Anthem” არის ამერიკის მომხმარებელთა რაოდენობით მეორე ჯანმრთელობის დამზღვევი კომპანია, რომლიდანაც მოიპარეს 78.8 მილიონი მიმდინარე და ყოფილი მომხმარებლების მონაცემთა ბაზები, რომელშიც შედიოდა მათი სახელი და გვარები, დაბადების თარიღები, მისამართები, სოციალური უსაფრთხოების ნომრები და სამედიცინო ისტორიები. ამ გარღვევის ზუსტი ზარალი ჯერ არ არის დადგენილი, თუმცა სავარაუდოდ 100 მილიონ დოლარზე მეტია.

[15] WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017 - https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

2016 წლის ბოლოს მოიპარეს კომპანია „Uber-ის“ მონაცემთა ბაზები, რომელშიც შედიოდა 57 მილიონი უბერის მომხმარებელის ინფორმაცია და ასევე 600 000 უბერის მძღოლის. ინფორმაციის მოპოვება მოხდა github-ის საშუალებით, სადაც საერთოდ არ უნდა ყოფილიყო მსგავსი მონაცემები.

ბოლო დროს ყველაზე გახმაურებული შემთხვევა მოხდა 2017 წლის 29 ივლისს, როდესაც მოიპარეს Equifax საკრედიტო ანგარიშგების სააგენტოს მონაცემთა ბაზები, სრული ინფორმაცია ფაქტობრივად ამერიკის შეერთებული შტატების მოქალაქეთა ნახევარზე. [16]

ამ ფაქტებმა ნათელი გახადა რომ ასეთი დიდი კომპანიებისა და სააგენტოების ბაზებიც კი არ არის დაცული, ზედმეტია საუბარი პატარა კომპანიებზე, შესაბამისად ეს საფრთხე აქტუალობას არ კარგავს და ისევ დგას დღის წესრიგში 2018 წელსაც.

ასევე მიმდინარე საფრთხეა კრიპტოვალუტების მაინინგი, რაც უფრო აქტიურად ხდება მაინინგი, უფრო მეტი ჰაკერი ინტერესდება სერვერებში შეღწევით და კრიპტოვალუტების მოპარვით. არის უფრო ჭკვიანური საშუალებებიც, როდესაც მოწყობილობებში უჩუმრად შეღწევით ამ მოწყობილობებს იყენებენ მაინინგისთვის პირადი მოგებისთვის.

დღესდღეობით უამრავი კიბერსაფრთხეა აქტუალური, რომლებიდანაც ზოგიერთი ახალია, თუმცა ბევრი ძველიც დღემდე მიმდინარე პრობლემად რჩება, ხოლო კიბერუსაფრთხოება ჯერ კიდევ სტრატეგიებით შემოიფარგლება.

3.2 ევროკავშირი და ხელოვნური ინტელექტი

ხელოვნური ინტელექტი (Artificial Inteligence – AI) ეს არის ნეირონული ქსელური სისტემაზე დაფუძნებული ალგორითმი, რომელსაც გააჩნია შესწავლის უნარი. AI-ს სუსტი ვერსია, ანუ ხელოვნური ინტელექტი რომელიც დაპროგრამებულია 1 კონკრეტული მიმართულებისთვის უკვე მრავალი წელია არსებობს, საწყისისტვის ეს იყო ჭადრაკის მოტამაშე კომპიუტერი, რომელსაც შესაძლო სვლების გათვლით და

[16] The 17 biggest data breaches of the 21st century - https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

ალბათობის დაანგარიშებით შეეძლო მრავალი ნაბიჯით წინ ეფიქრა და ისე გაეკეთებინა სვლა, მართალია დასაწყისში მას ამარცხებდნენ მაღალი დონის მოჭადრაკეები, თუმცა პროცესორების გაძლიერებამ გამოიწვია პროცესების მართვის სიმრავლის და სისწრაფის მატება, რის შედეგადაც ხელოვნურმა ინტელექტმა აჯობა ადამიანს ჭადრაკში.

ჭადრაკი მხოლოდ დასაწყისი იყო, ნელნელა ალგორითმის გამოყენება დაიწყეს სატელეკომუნიკაციო მოწყობილობებში. სმარტფონებში ხელოვნური ინტელექტი მოგვევლინა პირადი დამხმარეს (Personal asistent) როლში, მათ შორის კომპანიებმა თავიანტი ასისტენტები გამოუშვეს, ყველაზე ცნობადებია Apple – Siri, Google – google now, Microsoft – Cortana. მათი ფუნქციონალი მინიმუმიდან დაიწყო და ნელნელა აუმჯობესებენ, მათ შეუძლიათ დარეკვა, მუსიკის ჩართვა, ინტერნეტში ძიება, მოკლე ტექსტური შეტყობინების წაკითხვა და უამრავი სხვა ფუნქცია რომელიც ივსება ყოველ განახლებაზე, მათ შორის არის ისეთი ფუნქციაც როგორიც არის ანეგდოტის მოყოლა.

დაწყებული ასეთი ფესვებით, AI-გამოუნახეს სულ უფრო მეტი ფუნქციონალი, მანქანის მართვა, სხვა ტექნიკის მართვა, რობოტების მართვა და ა.შ.

ამ ყველაფრის მიუხედავად დღესდღეობით არსებული ხელოვნური ინტელექტი არის ე.წ. სუსტი ხელოვნური ინტელექტი, რაც გულისხმობს რომ მას არ აქვს რეალური ინტელექტი, მას აქვს მინიჭებული კონკრეტული ფუნქცია, რომელსაც გამოთვლების საშუალებით სწორად აკეთებს ან აუმჯობესებს კიდევაც.

მიუხედავად ამისა პოტენციურ საფრთხეს წარმოადგენს სუსტი ხელოვნური ინტელექტიც კი. მაგალითისთვის თუ კი ხელოვნური ინტელექტი მართავს მძიმე ტექნიკას, რაკეტებს და ა.შ. მსგავსი რამ საშიშია თუ კი ის ჩავარდება არასწორი ადამიანის ხელში. არსებობს მეორე ვარიანტიც, იქედან გამომდინარე რაც მეტი ესმის სუსტ ხელოვნურ ინტელექტს, მან შეიძლება ბრძანება აღიქვას პირდაპირი გაგებით, მაგალითათ მანქანის მართვისას უთხრათ რომ ძალიან სწრაფად მიგიყვანოთ

დანიშნულების ადგილამდე და მან ბრძანებიდან გამომდინარე უგულვებელყოს საგზაო წესები და პირდაპირი გადაჭრით ყველაფრის მიუხედავად გადაწყვიტოს თქვენი ადგილზე სწრაფად მიყვანა.

რაც შეეხება რთულ ხელოვნურ ინტელექტს, მისი არსებობის ზოგადი შესაძლებლობა, ან დაშვების შემთხვევაში სავარაუდო დრო თუ რამდენი იქნება საჭირო მის შექმნამდე წარმოადგენს კონტროვერსიულ თეორიებს. პირველ რიგში ეჭვქვეშ აყენებენ ზოგადად მისი არსებობის შესაძლებლობას, იქედან გამომდინარე თუ რამდენად რთულია ადამიანის ტვინი და რა რთული ალგორითმი, ქსელები და მოწყობილობები იქნება საჭირო რომ ხელოვნური ინტელექტი მიუახლოვდეს და გადაუსწროს რეალურ ინტელექტს, ჯერ კიდევ ფანტასტიკის სფეროს თვლიან. თუმცა წლების გასვლასთან ერთად აზრი იხრება იქითკენ რომ ეს ადრე თუ გვიან შესაძლებელი იქნება. კამათი არის დროის ფაქტორზეც, თუმცა იმის გათვალისწინებით რომ ასეთის არსებობის შემთხვევაში შესაბამისი სტრატეგიის შემუშავებას დაჭირდება ათწლეულები, თვლიან რომ დროა დაიწყონ მზადება, ვინაიდან ზოგიერთი თეორეტიკოსის აზრით ეს შეიძლება უკვე 60-70 წელშიც განხორციელდეს.

რა არის საფრთხე თუ კი მოგვევლინება ადამიანზე განვითარებული ხელოვნური ინტელექტი? პასუხი საკმაოდ მარტივია: ადამიანი დედამიწაზე ბატონობს არა იმიტომ რომ ყველაზე ძლიერია, ან ყველაზე სწრაფია ან ყველაზე გამძლე, არამედ იმიტომ რომ ყველაზე ჭკვიანია. აქედან მოდის მარტივი დასკვნა, თუ კი ადამიანი აღარ იქნება ყველაზე ჭკვიანი არსება დედამიწაზე, ხომ არ იქნება სავარაუდო შესაბამისი მოვლენების განვითარება?![17]

ევროკავშირის პოლიტიკა AI-ს კუთხით მთლიანად თავდაცვითია, მის სტრატეგიაში პირველ რიგში განხილულია AI-სგან მომავალი პოტენციური საფრთხეები და

[17] Benefits & risks of artificial intelligence - Max Tegmark

მხოლოდ ამის შემდეგ განიხილება მისი შესაძლო დადებითი მხარეები. მაშინ როცა ჩინეთი, რუსეთი და ამერიკა აქტიურად მუშაობენ ხელოვნური ინტელექტის განვითარებაში, ჩინეთი მოწინავეა ამ საკითხში, და ის დიდ წარმატებას წინასწარმეტყველებს უკვე 2030 წლისთვის.

გარდა ამისა ევროკავშირის სტრატეგია უფრო ფორმალობას გავს ვიდრე სტრატეგიას, მას არ აქვს კონკრეტული სამუშაო გეგმა ამ კუთხით, რაც მის როლს კიბერუსაფრთხოების საკითხში კითხვის ნიშნის ქვეშ აყენებს.

3.3 ევროკავშირის კიბერუსაფრთხოება პრაქტიკაში - სამოქმედო გეგმა

მიუხედავას ევროკავშირის აქტიური მცდელობებისა დაიკავოს ადგილი მსოფლიო კიბერუსაფრთხოების განვითარების კუთხით, ის კარგავს პოზიციებს, მისი კიბერუსაფრთხოების სტრატეგია უფრო ფორმალობას გავს ვიდრე რაიმე რეალურ გეგმას, განსხვავებით ჩინეთისა და ამერიკის შეერთებული შტატებისა, სადაც ამ კუთხით საკმაოდ წარმატებული შედეგები აქვთ და უწყვეტად განაგრძობენ წინსვლას. ევროკავშირის მთავარი სისუსტეები მისი პოლიტიკური და კიბერ სისუსტეა. პირველ რიგში ევროკავშირის პრობლემაა მისი წევრი ქვეყნების შეუთანხმებლობა კიბერუსაფრთხოების პოლიტიკის გატარებაზე, როგორც უკვე გამოჩნდა ნაშრომში, მათი სახელმწიფო კიბერუსაფრთხოების სტრატეგიები მკვეტლად განსხვავდება, ამასთან არცერთი მათგანია საკმარისად ძლიერი სტრატეგია რომ დომინანტის პოზიცია დაიჭიროს. ევროკავშირის კიბერუსაფრთხოების სტრატეგია არ შეიცავს არანაირ რეალურ სამოქმედო გეგმას, რაც პირდაპირ გამორიცხავს კიბერსაფრთხეების წინააღმდეგ ეფექტურობას, თუ კი არ შემუშავდება კონკრეტული სამოქმედო გეგმა და არა ფორმალური სტრატეგიები, ევროკავშირის ერთადერთ

იმედად რჩება წევრი ქვეყნების თანამშრომლობა, რაც ასევე არ ასახავს ნათელ მომავალს, წევრი ქვეყნების ბანალური სტრატეგიებიდან გამომდინარე.

ევროკავშირის პრობლემა არა მხოლოდ ფორმალურ სტრატეგიებშია, არამეს ევროკავშირის წევრ ქვეყნებს შორის არ არსებულ კოლექტივიზმშიც, მათ არათუ კიბერუსაფრთხოების სტრატეგიის კუთხით აქვთ სრულიად განსხვავებული ხედვები, არამედ ზოგადად კიბერუსაფრთხოების დეფინიციის აღქმაშიც კი.

კი აქვს ზოგიერთ ევროპულ ქვეყანას კონკრეტული ხედვები ამ კუთხით, თუმცა საერთო ჯამში ისინი ცალკე აღებულად არ ჩანან, გარდა ამისა შეუთანხმებლობა თავისას შვება. მაგალითისთვის ევროკავშირში ინფორმაციულ ტექნოლოგიებში და კიბერუსაფრთხოებაში ყველაზე განვიტარებულ ქვეყანად შეიძლება მოვიაზროთ ესტონეთი, და კი მის სტრატეგიაში შედის კონკრეტული პუნქტები მათ შორის წევრ ქვეყნებს შორის თანამშრომლობა, თუმცა ეკონომიკურად და პოლიტიკურად უფრო ძლიერ ქვეყანას როგორიც არის დიდი ბრიტანეთი სულ სხვა ხედვა აქვს და ის თანამშრომლობის შესაძლებლობას უშვებს მხოლოდ ერთეულ ქვეყნებთან.

2017 წელს ევროკავშირმა განაახლა კიბერუსაფრთხოების სტრატეგია რომელიც მიიღო 2013 წელს, ახალი სტრატეგიის მიზანი იყო უფრო მეტად მოეცვა ეს სფერო, მიუხედავად ამისა არც აქ მომხდარა ძირეული ცვლილებები, სტრატეგიაში წერია სტანდართული ფრაზები რომ კიბერსივრცე უნდა იყოს დაცული, უსაფრთხო, თავისუფალი, მაგრამ არსად წერია თუ როგორ გეგმავს ამის გაკეთებას.

ჩინეთი საკუთარ კიბერუსაფრთხოების სამოქმედო გეგმას აფუძნებს საკუთარ კვლევებს ხელოვნურ ინტელექტზე, ისინი უკვე არიან მოწინავე ქვეყანა ამ კუთხით და მათი პროგნოზების თანახმად ძალიან სწრაფად გეგმავენ განვითარებას. ამერიკის შეერთებული შტატების კიბერუსაფრთხოება ეფუძნება სამხედრო მხარეს, და უფრო აქტიურ სამხედრო კიბერუსაფრთხოების პოლიტიკას ატარებს. რუსეთის ფედერაცია თავის მხრივ ავტორიტარულ რეჟიმში კიბერუსაფრთხოებასაც ავტორიტარიზმზე

აფუძნებს, ცენზურით, და კიბერსივრცის კონტროლით, რაც შეიძლება არ ემთხვევა დემოკრატიული ქვეყნების ღირებულებებს, თუმცა ესეც ერთგვარი მუშა სტრატეგიაა სამოქმედო გეგმით. ევროკავშირის სტრატეგიას რაც შეეხება არც ძველი და არც ახალი არ არის დაფუძნებული არანაირ კონკრეტულ სამოქმედო გეგმაზე, მხოლოდ და მხოლოდ შეიცვალა ის რომ პოლიტიკური დებატების დონეზე კიდევ უფრო აქტიურად განიხილება კიბერუსაფრთხოების თემა.

იმისათვის რომ ევროკავშირმა მიიღოს რეალური მოქმედი კიბერუსაფრთხოების სტრატეგია, რამდენიმე რეალური ნაბიჯის გადადგმაა საჭირო:

- პირველ რიგში აუცილებელია ევროკავშირის მხრიდან მოხდეს თავიანთი სტრატეგიის უუნარობის აღიარება.
- უნდა შემუშავდეს ახალი კიბერუსაფრთხოების სტრატეგია, არა რეფორმის სახით, არამედ სრულად ნულიდან დაიწეროს, რომლის მიზანიც იქნება სამოქმედო გეგმის შექმნა და თან ისეთი სტრატეგიის შედგენა, რომელიც შეასრულებს ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სახელმწიფო სტრატეგიებისთვის კონსტიტუციის როლს, ანუ მასზე უნდა დაფუძნდეს შემდეგ შესაბამისად ყველა წევრი ქვეყნის სტრატეგიები.
- ახალ სტრატეგიაზე თავიანთის დაფუძნება უნდა გახდეს მოთხოვნა წევრი ქვეყნების მიმართ ან მოწოდების სახით მაინც და უნდა მოხდეს წევრ ქვეყნებს შორის თანამშრომლობის გაძლიერება.
- იმის მაგივრად რომ დაიწუნონ არსებული კიბერუსაფრთხოების სააგენტოები და იფიქრონ კიდევ ახლების შექმნაზე, უნდა გაიზარდოს ამ სააგენტოების დაფინანსება უფრო ეფექტური ნაბიჯებისთვის და მათი ნაბიჯები უნდა შეესაბამებოდეს ახალ სტრატეგიას და კონკრეტული მითითებებით, შუამავლის როლის შეთავსებიტ დაეხმარონ ყველა წევრ ქვეყანას სტრატეგიების შემუშავებაში.

- უნდა განიხილოს და დადგინდეს კიბერუსაფრთხოების დეფინიცია უფრო ფართოდ და ღრმად და არა ზედაპირულად.

საბოლოო ჯამში ევროკავშირს აქვს პოტენციალი დაიკავოს ადგილი კიბერუსაფრთხოების სფეროში, თუ კი ეს კავშირი გახდება ნამდვილი კავშირი არამხოლოდ ადამიანის შესახებ ფასეულობებით, არამედ კიბერუსაფრთხოების კუთხითაც, უნდა მოხდეს პრიორიტეტების დალაგება, მეტი წონა მიეცეს ამ კუთხით ისეთ ქვეყნებს რომლებსაც მეტი გამოცდილება აქვთ ამ საქმეში, მაგალითად ესტონეთს, და არა ქვეყნებს რომლებსაც უბრალოდ პოლიტიკურად უფრო დიდი წონა აქვს.

დასკვნა

ამ ნაშრომში განვიხილე ევროკავშირის პოლიტიკა კიბერუსაფრთხოების კუთხით ყველა ასპექტში რის შედეგადაც საიდანაც შეიძლება დავასკვნათ:

რამ გამოიწვია კიბერუსაფრთხოების სფეროს შექმნა და განვითარება?

მე-20 საუკუნე გახდა ტექნოლოგიური რევოლუციის საუკუნე, სწორედ აქედან დაიწყო ძალიან სწრაფი განვითარება ინფორმაციულმა ტექნოლოგიებმა. ინფორმაციული ტექნოლოგიების განვიტარებასთან ერთად განვითარდა ქსელები, სადაც გაჩნდა პირველი კიბერსაფრთხეები, სწორედ ეს იყო საწყისი წერტილი როცა ჩაისაცა კიბერუსაფრთხოების ჩანასახი. რაც მეტი დრო გადიოდა და ვითარდებოდა ქსელები, უფრო მეტ საფრთხეებს ვხვდებოდით კიბერსივრცეში, დროთა განმავლობაში რაც ქსელებზე დამოკიდებულება გაიზარდა ხმამაღლა დაიწყეს ამ თემაზე საუბარი და აქტიურად დაიწყეს კიბერსაფრთხეების წინააღმდეგ ბრძოლა, აქედან დაწყებული შეიძლება ჩავთვალოთ რომ კიბერუსაფრთხოებას ჩაეყარა საფუძველი და მას შემდეგ პარალელურად ვითარდებიან როგორც კიბერსაფრთხეები ისე კიბერუსაფრთხოებაც.

რა სახის კიბერსაფრთხეები არსებობს და როგორია მათ წინააღმდეგ ევროკავშირის პოლიტიკა?

კიბერსაფრთხეები არსებობს უამრავი სახის, უამრავი მიზეზით და საშუალებით. პირველ რიგში უნდა გამოვყოთ სახეები, კიბერსაფრთხე შეიძლება იყოს გამიზნული კიბერშეტევის სახით, შეიძლება იყოს პროგრამული უზრუნველყოფის შეცდომის მიზეზით და ასევე ადამიანური ფაქტორის მიზეზით. კიბერშეტევების მოტივაცია შეიძლება იყოს სხვადასხვაგვარი, მას შეიძლება ქონდეს პოლიტიკური სახე, მაგალითისთვის კონკრეტული გადაწყვეტილებისთვის საბოტაჟის მოწყობის მიზნით განხორციელებული კიბერშეტევები, ან საერთოდ კიბერომი როდესაც

დაპირისპირებულ მხარეებს შორის მიმდინარეობს კიბერშეტევები, მაგალითად სახელმწიფოებს შორის კონფლიქტის გამო.

ევროკავშირი საკმაოდ აქტიურად საუბრობს კიბერუსაფრთხოებაზე, მას ხშირად მიიჩნევენ ყველაზე აქტუალურ საფრთხედ, მოქმედებს სხვადასხვა სააგენტოები ამ კუთხით, რომლებსაც ევალებათ შუამავლობა ევროკავშირის წევრ ქვეყნებს შორის, ტრენინგები, პუბლიკაციები და ა.შ.

არის თუ არა კიბერუსაფრთხოების სახელმწიფო სტრატეგიები და ევროკავშირის სტრატეგია ეფექტური პრაქტიკაში?

ევროკავშირი როგორც ზოგადი კანონმდებლობის მხრივ, ასევე კიბერუსაფრთხოების კუთხით არ ავალდებულებს წევრ ქვეყნებს მიიღონ მსგავსი კანონები და სტრატეგიები, შესაბამისად ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სახელმწიფო სტრატეგიები მკვეთრად განსხვავდება. ზოგიერთის სტრატეგია ძირითად მომენტებში ემთხვევა, თუმცა ერთიანობაში საერთოდ არ ჩანს ერთი კონკრეტული მოდელი. თვითონ ევროკავშირის კიბერუსაფრთხოების სტრატეგია ძალიან ზოგადია და მიუხედავად გატარებული რეფორმისა ასეთივე დარჩა, მისი სტრატეგია უფრო ფორმალობაა ვიდრე რაიმე სახის გეგმა. შესაბამისად არც სახელმწიფო სტრატეგიები არც ევროკავშირის სტრატეგია არ არის ერთი პოლიტიკით მოტივირებული, არ ამოძრავებთ ერთი მიზნები, ევროკავშირს ფიზიკურად არ გააჩნია კიბერსაფრთხეების წინააღმდეგ კონკრეტული სამოქმედო გეგმა, რომელსაც დაეყრდნობა. ხედვების ასეთი განსხვავებებიდან და სამოქმედო გეგმის არ ქონიდან გამომდინარე ევროკავშირი კიბერუსაფრთხოების კუთხით პრაქტიკაში ძალიან სუსტი და არაეფექტურია, მას ამ კუთხით უსწრებს როგორც ჩინეთი და ამერიკის შეერთებული შტატები, ასევე რუსეთიც.

რა მეთოდებით შეიძლება ამ სფეროს გაძლიერება?

ევროკავშირის კიბერუსაფრთხოების გასაძლიერებლად საჭიროა კიბერუსაფრთხოების სტრატეგიის უფრო მოცულობითი სრული ვერსიის შექმნა და ევროკავშირის წევრი ქვეყნებისთვის მოთხოვნის ან მოწოდების სახით წარდგენა, რომ მას დაეფუძნოს წევრი ქვეყნების სახელმწიფო სტრატეგიები. ევროკავშირის წევრი ქვეყნებისთვის აქტიური კონსულტაციების გაწევა შესაბამისი სააგენტოების საშუალებით, ხოლო მათი დაფინანსების გაზრდა, რაც გარდა ეფექტურობის გაზრდისა იქნება იმის მაჩვენებელი თუ რამდენად მნიშვნელოვანია ეს სექტორი. წევრი ქვეყნებისთვის მოწოდება აქტიური თანამშრომლობისკენ, კიბერუსაფრთხოებისთვის საჭიროა მჭიდრო კოლექტივიზმი, ურთიერთ პრაქტიკის გაზიარება და რაც მთავარია ამ საკითხში გარკვეული ქვეყნებისთვის ამ კუთხით მეტი პოლიტიკური წონის მიცემა.

გამოყენებული ლიტერატურა

1) ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები და რეკომენდაციები. საქართველოს კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები (კრებული) - ვლადიმერ სვანაძე

2) Brief History of the Internet - Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff (1997)

3) Benefits & risks of artificial intelligence - Max Tegmark

4) Commanding the Trend: Social Media as Information Warfare - Lt Col Jarred Prier, USAF

5) CYBERSECURITY. THREATS, CALLS, SOLUTIONS - Zgoba Artem, Moscow, Dmitry Markelov, St. Petersburg, Pavel Smirnov, phd., St. Petersburg

6) Cyber-security in the European Region: Anticipatory Governance and Practices - Tine Højsgaard Munk 2015

7) Dimensions of cyber-attacks - Robin Gandhi, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, And Phillip Laplante

8) Europe's AI delusion - BRUNO MAÇÃES

9) First computer virus of Bob Thomas - Georgi Dalakov

10) Information Warfare as a Geopolitical Tool - Tomáš Čižik

11) Information Warfare - New Security Challenge for Europe. Tomáš Čižik

12) Moving beyond the European Union's weakness asa cyber-security agent - Krzysztof Feliks Sliwinski

13) Social Media as a Tool for Information Warfare - Aylin Manduric

14) Strategic Defence for Russia's Undeclared Information War on Europe - Salome Samadashvili

15) Types of information warfare and examples of malicious programs of information warfare - Dragan Z. Damjanović

16) What is cyber terrorism? – Jane mccallion

17) About ENISA - https://www.enisa.europa.eu/about-enisa/mission-and-objectives

18) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

19) Cyber Defence - https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence

20) European cybercrime centre - EC3 - https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

21) Enisa programming document 2018–2020 - https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020

22) National Cyber Security Strategies (ncsss) Map - https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

23) Reform of cyber security in Europe - http://www.consilium.europa.eu/en/policies/cyber-security/

24) The 17 biggest data breaches of the 21st century - https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

25) The history of cyber security — everything you ever wanted to know - Https://www.sentinelone.com/blog/history-of-cyber-security/

26) Wannacry, Petya, notpetya: how ransomware hit the big time in 2017 - https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

გამოყენებული აბრევიატურების ნუსხა

EU – European union

Email – Electronic mail

DDOS - Distributed denial of services

ENISA - European Network and Information Security Agency

EDA - European Defence Agency

PDF – Portable document format

AI – Artificial intelligence