კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები

(კრებული)

ვლადიმერ სვანაძე

საქართველოს საზოგადოებრივ საქმეთა ინსტიტუტის დოქტორანტი, სოციალურ მეცნიერებათა სადოქტორო პროგრამა, კიბერუსაფრთხოების პოლიტიკა

2015

სარჩევი

წინასიტყვაობა

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

წინამდებარე კრებულში მოცემულია ის ნაშრომები, რომლებიც გადმოცემს კიბერსივრცის უსაფრთხოების უზრუნველყოფისა და მისი მაქსიმალური დაცვის საკითხებს. კერძოდ, კრებულში გაეცნობით იმ საფრთხეებს, რომლებიც არსებობს კიბერსივრცეში, ამ საფრთხეების წარმოქნის წყაროებსა და მათ სახეობებს. ასევე საერთაშორისო და რეგიონალურ დონეზე განხორციელებულ იმ ღონისძიებებს, რომლებიც მიმართულია კიბერსივრცის დაცვაზე. გარდა ამისა კრებულში მოცემულია ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების პოლიტიკისა და სტრატეგიების მოკლე აღწერილობები, საერთო პრინციპები და რეკომენდაციები. ასევე ზოგიერთი ქვეყნის იმ ორგანიზაციულ - სტრუქტურული ერთეულების მოკლე აღწერილობა, რომლებიც ანხორციელებენ აუცილებელ ღონისძიებებს მიმართულს კიბერსივრცის დაცვასა და კიბერუსაფრთხოების უზრუნველყოფაზე. ყოველივეს ფონზე განხილულია საქართველოს კიბერუსაფრთხოების სტრატეგია, პოლიტიკა და სუბიექტები. აქვე აღსანიშნავია, რომ კრებულში განხილულია სოციალური ქსელებისა და მათი დაცვის საკითხები, როგორც ეროვნული უსაფრთხოების ერთერთი შემადგენელი და მნიშვნელოვანი ნაწილი. იქვე მოცემულია დემოკრატიულობის ის საკითხები, რომლებიც უკავშირდება სოციალური ქსელების გამოყენებას.

არსებობს ტერმინის „კიბერსივრცის“ განმარტების ბევრი ვარიანტი და ყველა მათგანი იძლევა თავისებურ განსაზღვრებას. თუმცა ყველა განმარტებაში აღნიშნულია, რომ „კიბერსივრცე“ წარმოადგენს ინფორმაციულ - ტექნოლოგიური ინფრასტრუქტურის

ურთიერთკავშირის კომპლექსს, რომელიც თავისთან მოიცავს ინტერნეტის გლობალურ ქსელს, კომპიუტერულ სისტემებს, ტელესაკომუნიკაციო ქსელებსა და პროცესორებს.

ბოლო ორ ათწლეულში ჩვენ გავხდით ე. წ. „ინფორმაციული აფეთქების“ უნებლიე მოწმეები, როცა პრაქტიკულად არავის არ შეუძლია გვერდი აუაროს ინფორმაციულ ქსელებზე დაშვებასა და მის გამოყენებას, იქნება ეს პირადი საყოფაცხოვრებო თუ პროფესიულ დონეზე. ამის გარდა, გლობალური ქსელების მიმართ არსებულ მზარდ ინტერესს თან ახლავს მისი უსაფრთხოების უზრუნველყოფის ადეკვატური ზომები. ეს გამოწვეულია იმ ფაქტით, რომ თავდაპირველად ინტერნეტი იქმნებოდა სამეცნიერო მონაცემების გაცვლის მიზნით, თუმცა დღეს ეს სურათი კარდინალურად არის შეცვლილი და ამჟამად ინტერნეტის გლობალური ქსელი წარმოადგენს მსოფლიო ეკონომიკის მხარდამჭერ ერთერთ ძირითად საშუალებას. აღსანიშნავია ის გარემოება, რომ ინტერნეტის კონსტრუქციული თუ დესტრუქციული მიზნებით გამოყენებისა და მისი ფუნქციონირების საკმაოდ სწრაფად მზარდი პროცესი წინ უსწრებს ინფრასტრუქტურის რეფორმირებისა და უსაფრთხოების უზრუნველყოფის ძალისხმევას. თავის მხრივ კიბერუსაფრთხოება ანუ ინტერნეტის გლობალური ქსელის უსაფრთხოება მოიცავს საკითხის გადაჭრის გლობალურ მასშტაბს, თუმცა ამ მიმართულებით არსებული ღონისძიებების დიდი ნაწილი ხორციელდება ცალკეული ქვეყნებისა და მათი ეროვნული უსაფრთხოების პოლიტიკის დონეზე, რაც არ არის საკმარისი და საკითხი მოითხოვს საერთაშორისო თუ რეგიონალურ მიდგომას.

კრებულში მოცემული ნაშრომები განკუთვნილია როგორც მოცემული დარგის სპეციალისტებისთვის, ისე იმ დაინტერესებული პირებისთვის, რომლებსაც სურთ ამ მიმართულებით შეიძინონ გარკვეული ცოდნა.

რეცენზია

ვლადიმერ სვანაძის ნაშრომზე „კიბერსივრცე და კიბერუსაფრთხოების ახალი გამოწვევები“

ინტერნეტის შემქმნელები ვერასდროს წარმოიდგენდნენ, რომ ინტერნეტტექნოლოგიების მზარდი განვითარება წარმოშობდა ისეთ მასშტაბურ სისტემათა სისტემას, რომლის უსაფრთხოება ესოდენ მნიშვნელოვან გამოწვევად გადაიქცეოდა. ამ ახალმა მეცნიერულმა მიღწევამ ბევრ სიკეთესთან ერთად, ასევე წარმოშვა ახალი საფრთხეები და საბრძოლო სივრცის ახალი ველი. ყოველდღიურად ხდება კიბერდანაშაული ინდივიდების, სხვადასხვა ბიზნესისა თუ მთავრობის წინააღმდეგ. დღეს, კიბერთავდასხმები წარმოადგენს საფრთხეს, რომლის წინააღმდეგაც ეროვნული უსაფრთხოების ექსპერტები ეძიებენ უფრო ეფექტურ, თანმიმდევრულ კიბერპოლიტიკას, ქმნიან სტრატეგიულ დოკუმენტებს და თავდაცვის მეთოდებს. წარმოდგენილი კრებული, რომელიც ავტორის მიერ შექმნილ ნაშრომთა სრულ სიას წარმოადგენს ვრცლად მიმოიხილავს კიბერსაფრთხეების წარმოშობის წყაროებს, თავდასხმის ტიპებს და ამ საფრთხეებთან ბრძოლის სტრატეგიებსა და ტაქტიკებს. ამ თვალსაზრისით ავტორი მკითხველს სთავაზობს სხვადასხვა ქვეყნების გამოცდილებას. ავტორი ასევე განიხილავს კიბერსაფრთხეებთან საბრძოლველად არსებული საერთაშორისო კონვენციების, შეთანხმებების და თანამშრომლობის მნიშვნელობას, რადგანაც კიბერომის, კიბერტერორიზმის, კიბერკრიმანის წინააღმდეგ ბრძოლა მეგობარი ქვეყნების მთავრობების ერთიანი ძალისხმევის, რესურსისა და გამოცდილების გაზიარების გამოყენებითაა შესაძლებელი. ავტორი თავის ნაშრომში ასევე მიმოიხილავს ამ თვალსაზრისით საკანონმდებლო ბაზის საერთაშორისო სტანდარტებთან შესაბამისობის მნიშვნელობას.

კრებულში მნიშვნელოვანი ყურადღება ეთმობა ახალი ინფორმაციული სივრცის გლობალურ მნიშვნელობას, მის დადებით და უარყოფით ფაქტორებს. მასში ფართოდაა გაანალიზებული სოციალური მედიის როლი, რომელსაც თავისი მნიშვნელობით და გავლენით დღეს მეხუთე ხელისუფლებასაც კი უწოდებენ.

კრებული, **„კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“** უდავოდ გამოირჩევა თავისი აქტუალობით და მნიშვნელობით. მასში თანმიმდევრულად და ძირეულადაა განხილული არსებული პრობლემატიკა. ის უთუოდ დიდ დახმარებას გაუწევს მკითხველს ძირეული ინმფორმაცია მიიღოს კიბერ და ინფორმაციული სივრციდან მომდინარე ახალ გამოწვევებზე.

ხათუნა მშვიდობაძე

სოციალურ მეცნიერებათა დოქტორი

რეცენზია

ვლადიმერ სვანაძის ნაშრომზე „კიბერსივრცე და კიბერუსაფრთხოების ახალი გამოწვევები“

თანამედროვე სამყაროში, ისე როგორც განვითარებულ, ასე განვითრებად ქვეყნებში საზოგადოების ლექსიკაში მყარად დამკვიდრდა ტერმენები: კიბერსივრცე, ინფორმაციული ომი, ინფორმაციული უსაფრთხოება, კიბერდანაშაული, კიბერშეტევა, კიბერუსაფრთხოება და შესაბამისი კანონმდებლობა. თუმცა აღსანიშნავია, რომ საქართველოში კიბერსუსაფრთხოების საკითხის შესწავლა საწყის ეტაპზეა და ამ მიმართულებით კვლევები და სამეცნიერო ლიტერატურა ჯერ კიდევ მიუწვდომელია. ჩვენი ქვეყანა 2008 წელს მასირებული კიბერშეტევის მსხვეპლი გახდა, რამაც კიდევ ერთხელ ხაზი გაუსვა საქართველოსთვის კიბერუსაფრთხოებისა და ინფორმაციული უსაფრთხოების დარგში ეროვნული სტრატეგიისა და სამოქმედო გეგმის შექმნის აუცილებლობას.

ამ მიმართულებით, განსაკუთრებით მნიშვნელოვანია ქვეყანაში შესაბამისი კანონდმებლობის შექმნა, რომელიც შესაძლებელს გახდის სხვადასხვა სახელმწიფო და არასახელმწიფო ორგანიზაციების თანამშრომლობას ქვეყნის ინფორმაციული სივრცისა და ქსელის დაცვაზე.

ავტორს თავის ნაშრომში კარგად აქვს განხილული კიბერუსაფრთხოების საფუძვლები, მისი უზრუნველყოფის კომპონენტები და სხვადასხვა ქვეყნების, საერთაშორისო ორგანიზაციების გამოცდილება. ავტორის აზრით, მნიშვნელოვანია, რომ გლობალიზაციასა და ინფორმაციული ტექნოლოგიების სწრაფი ზრდის პირობებში აუცილებელია სახელმწიფოს სისტემა იყოს მოქნილი. ასევე მნიშვნელოვანია, ქვეყანამ განსაზღვროს ამ სფეროში არსებული საფრთხეები, რათა ქვეყანამ მოახდინოს დროული პრევენცია და თავიდან იქნას აცილებული კიბერშეტევები საქართველოს ინფორმაციულ ქსელებზე და საერთოდ ინფრასტრუქტურაზე.

ავტორის მიერ გაანალიზებულია კიბერშეტევის შესაძლო დამკვეთები და ორგანიზატორები და გამოყოფილია ჯგუფები, მაგალითად ჰაკერები, კრიმინალები, კერძო სექტორი და პოლიტიკური მიზნით განხორციელებული კიბერშეტევები. აღნიშნული დანაშაული უშუალოდ უკავშირდება ახალი ინფორმაციული ტექნოლოგიების განვითრებას.

ავტორის აზრით, ინფორმაციული ტექნოლოგიებისა და კიბერსივრცის განვითარება ყოველთვის ერთი ნაბიჯით წინ არის ვიდრე ქვეყნის კანონმდებლობა ან ეროვნული სტრატეგია, სამოქმედო გეგმა. მისი აზრით მნიშველოვანია, რომ ქვეყანაში მუდმივად უნდა ხდებოდეს მის გარშემო არსებული სიტუაციის შესწავლა, კანონმდებლობის ანალიზი და პოლიტიკის სრულყოფა, რათა ქვეყანა ნებისმიერ გამოწვევას მომზადებული დახვდეს.

ამ მიმართულებით, ქართულ ენაზე ფაქტიურად არ არსებობს აკადემიურ დონეზე ჩატარებული კვლევები და ჩემი აზრით, ავტორის მიერ მომზადებული ნაშრომები იქნება ერთ - ერთი პირველი, რომელიც დადებით როლს შეასრულებს ქვეყანაში კიბერსივრცის შესწავლისა და სწორი ანალიზის განვითარების მიმართულებით. ნაშრომები შეიძლება გამოიყენონ როგორც დარგის სპეციალისტებმა, ისე სხვა დაინტერესებულმა პირებმა.

გელა კვაშილავა

ეკონომიკურ მეცნიერებათა კანდიდატი

მარტი, 2012 წელი

სოციალური მედია და ეროვნული უსაფრთხოება

შესავალი

მასობრივი ინფორმაციის საშუალებას ყოველთვის შეეძლო გარკვეული დადებითი თუ უარყოფითი როლი ეთამაშა ნებისმიერი ქვეყნის ეროვნული უსაფრთხოების საკითხებში და მასზე გარკვეული ზეგავლენა ექონია, მთავარი იყო მხოლოდ რა მიმართულებით? ვინ და საიდან? და როგორ გამოიყენებდა ტრადიციულ მედია საშუალებებს.

XXI საუკუნის დასაწყისის ბოლო ათწლეულში ძალზედ პოპულარული და გამოყენებადი გახდა სოციალური მედიით სარგებლობა. შეიცვალა საშუალებები, ხოლო მიზნები და ამოცანები, ისევე როგორც ზემოთ მოცემული კითხვები, იგივე დარჩა. ეროვნულ უსაფრთხოებაზე ისევ ისეთი გავლენა აქვს მედია საშუალებებს, როგორც ტრადიციულ მედიას, მხოლოდ ყოველივე ეს დროში დაჩქარდა, უფრო სწრაფად ხდება მოვლენათა განვითარება და გავრცელება.

სოციალურმა მედიამ თავისი არსებობა დაიწყო XXI საუკუნეში აშშ - ში, და მას აქეთ ვითარდება გეომეტრიული პროგრესიით. 2010 წლის მონაცემებით, სოციალური მედიის მომხმარებელმა შეადგინა დაახლოებით ორი მილიარდი, პლანეტის მთლიანი მოსახლეობის თითქმის მესამედი.

განვითარების პირველ ეტაპზე, 2000 – 2005 წლებში, სოციალური მედია გავრცელებული იყო მაღალი ტექნოლოგიების მქონე ქვეყნებში, სადაც

დემოკრატიულობის ინდექსის ნიშნულის მაჩვენებელი საკმაოდ მაღალ დონეზე არის. 2005 წლიდან სოციალური მედია საშუალება გავრცელებას იწყებს შედარებით დაბალგანვითარებულ ქვეყნებში, სადაც დემოკრატიულობის ინდექსის მაჩვენებელი შედარებით დაბალია, ზოგან კი საერთოდ არ არსებობს. ეს ფაქტი ძალზედ აისახება არა მარტო ქვეყნის ეროვნულ უსაფრთხოებაზე, არამედ რეგიონალურ და ხშირ შემთხვევაში საერთაშორისო უსაფრთხოებაზე.

ტრადიციულად სოციალურ მედიაში იგულისხმება ისეთი ცნობილი სოციალური ქსელები, როგორებიც არის Facebook, LinkedIn, MySpace, Twitter, YouTube, Flickr, WordPress, Blogger, Typepad, LiveJournal, Wikipedia, Wetpaint, Wikidot, Second Life, Del.icio.us, Digg, Reddit, Lulu.

სოციალური ქსელების მომხმარებელთა რაოდენობა დღითიდღე იზრდება. მის სწრაფ გლობალურ გავრცელებას ხელს უწყობს სოციალური მედიისთვის დამახასიათებელი, მომხმარებლისთვის მნიშვნელოვანი ისეთი საშუალებები, როგორიც არის ოპერატიულობა, ინფორმაციის სწრაფი გადაცემა და ორმხრივი კომუნიკაციის შესაძლებლობა, იაფფასიანობა და ა. შ. მომხმარებელთა მუდმივი ზრდა.

თუმცა სოციალურ მედიას გააჩნია როგორც დადებითი ისე უარყოფითი მხარეები. მისი არასწორი მიმართულებით გამოყენებამ შეიძლება ცუდი გავლენა იქონიოს ქვეყნის ეროვნულ უსაფრთხოებაზე. თუმცა ამავე დროს სოციალურ მედიას შეუძლია დადებითი ეფექტის მოტანა ქვეყნისთვის, მისი საშუალებით შესაძლებელია სტრატეგიული თუ ტაქტიკური მიზნების მიღწევა, საფრთხეებზე მუშაობა და მათი დროული პრევენცია.

სოციალური მედია ძალზედ სწრაფად ვითარდება, და აუცილებელია მისი საშუალებით გეო - პოლიტიკურ, გეო - ეკონომიკურ, თუ სხვა სახის პროცესებზე მუდმივი მონიტორინგი სახელმწიფოს მხრიდან. მთლიანობაში, კომპლექსურად ეს პროცესი საშუალებას მოგვცემს თავიდან ავიცილოთ საგარეო საფრთხეები და მათი გავლენა საშინაო მოვლენებზე. შეიძლება ითქვას, რომ სოციალურ მედიას საკმაოდ წარმატებით იყენებენ საერთაშორისო დამნაშავე ჯგუფები, მათ შორის ტერორისტული

ორგანიზაციები. თავისი მიზნების მისაღწევად, სოციალურ მედიას თავის ინტერესებში გამოყენებას არ ერიდებიან აგრეთვე პოტენციურად მოწინააღმდეგე ქვეყნები და ალიანსები.

აუცილებელია ვიცოდეთ, როგორ და რამდენად შეუძლია სოციალურ მედიას გაუწიოს დახმარება სახელმწიფოს აღკვეთოს საფრთხეები და დაიცვას სტრატეგიული ინტერესები. აუცილებელია სწორად იქნას გამოყენებული სოციალური მედიის შესაძლებლობა, თუმცა აქვე გასათვალისწინებელია ის გარემოება, რომ არ უნდა დაირღვეს მომხმარებლის, როგორც პიროვნების უფლებები.

საქართველოში სოციალურ მედიას რატომღაც სწავლობენ და იჩემებენ საკითხის კომპეტენტურობას ჟურნალისტები, როცა ეს თემა თავისი აქტუალობიდან, შინაარსიდან და დატვირთულობიდან გამომდინარე წარმოადგენს საერთაშორისო ურთიერთობის, საერთაშორისო უსაფრთხოების კვლევის საგანს.

სანამ მთავარი საკითხის განხილვას დავიწყებდეთ, ნათელი წარმოდგენის შექმნისთვის, ორიოდე სიტყვით შევეხოთ სოციალური მედიის განსაზღვრებას, მის დეფინიციას, განსხვავებას ტრადიციულ მედიასთან და სოციალური ქსელების მომხმარებლის კატეგორიებს. აგრეთვე, საუბარი იქნება ინფორმაციული ომის შესახებ და ამ ომში სოციალური მედიის როლსა და ადგილზე.

სოციალური მედიის განსაზღვრება და შედარება ტრადიციულ მედიასთან

რა არის ზოგადად სოციალური მედია? თითქმის ათი წელი გავიდა მას შემდეგ, რაც ინტერნეტში გაჩნდა სოციალური მედია, და როგორც წესი მსგავსი სიახლეები ელვის სისწრაფით ვრცელდება. ფაქტიურად სოციალური მედიის გავრცელებამ და გამოყენებამ აშკარად გაუსწრო მისი შესწავლის პროცესს, რაც გახდა ძირითადად მიზეზი ოპონენტთა შორის მწვავე დებატებისა და აზრთა სხვადასხვაობისა.

შეიძლება ითქვას, რომ საკითხი ბოლომდე შესწავლილი არ არის, ჯერ არ ჩატარებულა საკმარისი კვლევები და მის შესახებ ერთიანი ჩამოყალიბებული აზრი არ

არსებობს, შესაბამისად სოციალური მედიის დეფინიციაც ზოგად ხასიათს ატარებს. მაგალითად, the US Congressional Research Service (CRS) ანალიტიკოსი ბრუს ლინდსი სოციალურ მედიას განსაზღვრავს შემდეგნაირად: „ტერმინი სოციალური მედიის შესახებ განეკუთვნება ინტერნეტ - ბმულებს, რომლებიც იძლევა ადამიანთა შორის ურთიერთობის საშუალებას, რესურსებისა და ინფორმაციის ერთობლივ გამოყენებას. სოცილური მედია თავისთან მოიცავს სადისკუსიო ფორუმებს, ბლოგებს, ჩათებს, YouTube channels, LinkedIn, Facebook და Twitter. სოციალურ მედიასთან დაშვება შეიძლება მივიღოთ კომპიუტერის დახმარებით, აგრეთვე სმარტფონების, ფიჭური კავშირისა და მობილური ტელეფონების მოკლე ტექსტური შეტყობინების საშუალებით“.

სტრატეგიული კომუნიკაციების ექსპერტი და Oklahoma State University პროფესორი ბობი ლუისი სოცილურ მედიას განსაზღვრავს, როგორც „ბლოგების, YouTube, Flickr, MySpace და Facebook ისეთ ინტერნეტ - საშუალებას, რაც ჩვეულებრივ ადამიანს საშუალებას აძლევს შექმნას კონტენტი, რომელსაც გაუზიარებს მსოფლიო აუდიტორიას. მოცემული საშუალებების ინტერაქტიულმა ხასიათმა შეცვალა მასიური საინფორმაციო საშუალებების ცალმხრივი გავრცელებიდან ორმხრივი დიალოგისკენ“.

როგორც ზემოთ არის აღნიშნული, სოციალური მედიის ზუსტი განსაზღვრების შესახებ ერთი ჩამოყალიბებული აზრი არ არსებობს, და ამაზე შეჩერება ცოტა შორს წაგვიყვანდა, მხოლოდ ბოლოში მოვიშველიებ სკონსულტაციო ფირმა Burston – Marsteller ვერსიას სოციალური მედიის აღწერის შესახებ, კერძოდ „ეს არის გადართვა, სადაც ადამიანები აკეთებენ ახალ აღმოჩენებს, კითხულობენ და უზიარებენ ერთმანეთს ახალ ამბებს, ინფორმაციასა და კონტენტებს, მათ შორის წერით, ვიდეო, ფოტო და აუდიო“.

მოკლედ შეგვიძლია ვთქვათ, რომ სოციალური მედია ეს არის კიბერ სივრცეში მიღწევადი კავშირისა და კომუნიკაციის საშუალება, რომელიც ოპერატიულად ფუნქციონირებს ტექნოლოგიური მოწყობილობების ბაზაზე (ინტერნეტი, მობილური ტელეფონები, კომპიუტერები და სხვა) და გააჩნია პროგრამული უზრუნველყოფის (Facebook, Twitter, MySpace, LinkedIn, YouTube, etc.) პლატფორმა. ყოველივე აღნიშნულის დახმარებით მომხმარებლებს შეუძლიათ:

- ერთმანეთთან ურთიერთობა;
- სხვადასხვა სახის კონტენტების (ვიდეო, ფოტო, აუდიო, და სხვა) გაზიარება;
- ქსელური გაერთიანებების შექმნა (პროფესიული, რელიგირი, კულტურული, ნაცნობები, პოლიტიკური და ა. შ.);
- სოციალური იდენტურობის განსაზღვრა და განვითარება.

სოციალურ მედიას, ტრადიციული მასიური საინფორმაციო საშუალებებისგან განსხვავებით, გააჩნია მომხმარებელთა შორის ძალზედ მაღალი დონის ინტერაქტიული ურთიერთდამოკიდებულება. ტრადიციული მედია საშუალებები არის ინფორმაციის ცალმხრივად გამავრცელებელი, როცა სოციალური მედიის მომხმარებლები არიან როგორც ინფორმაციის მიმღებნი, ისე მისი შემქმნელნი და გამავრცელებელნი.

ტრადიციული და სოციალური მედიის შედარებისას, ეს უკანასკნელი არის უფრო დინამიური, პირადი და ინტერაქტიული. აგრეთვე მას ახასიათებს ოპერატიულობა და ინფორმაციულობის გავრცელების სისწრაფე მთელს მსოფლიოში, მისთვის მიუღებელია დრო და სივრცე, ის მარტივი და იაფია. სოციალური მედიის გამოყენებისას მომხმარებელს ვირტუალურ სივრცეში შეუძლია შექმნას, გააქტიუროს და მართოს თავისი პირადი პროფილი, დაიმკვიდროს თავისი ადგილი არარეალურ სამყაროში.

სოციალური მედიის მომხმარებელი

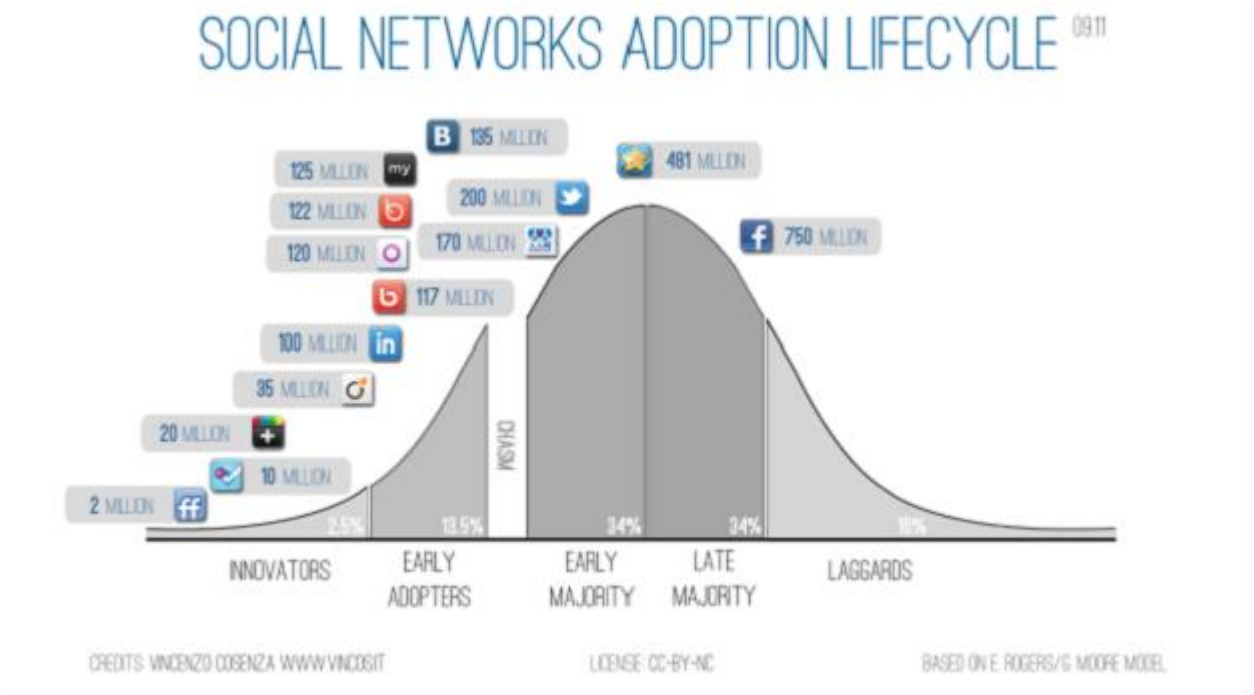
სოციალური მედიის მომხმარებლები შეიძლება დაიყოს რამოდენიმე კატეგორიად. პირველ რიგში ესენი არიან ჩვეულებრივი პიროვნებები, რომლებიც იყენებენ სოციალური მედიის ისეთ საშუალებებს, როგორიც არის ინფორმაციისა და კონტენტის გაცვლა - გაზიარება, კომუნიკაცია, პიროვნული იდენტურობის ამაღლება სოციალური ქსელის გამოყენებით. ფაქტიურად სოციალური მედია ცალკეულ პირებს საშუალებას აძლევს დაიკმაყოფილოს თითქმის ყველა თავისი მოთხოვნა, ფიზიოლოგიურის (ჭამა, სმა, ძილი) გარდა. ეს კი ზრდის მომხმარებლის დამოკიდებულებას სხვადასხვა სოციალურ ქსელებზე, ხშირ შემთხვევაში, ასეთ დამოკიდებულებას სპეციალისტები უკვე ადარებენ ალკოჰოლზე, ნარკოტიკულ ნივთიერებაზე, ყავაზე დამოკიდებულებას.

2011 წლის სტატისტიკის მიხედვით სოციალური მედიის მომხმარებელია:

- ინტერნეტის მომხმარებლის 75%, რომელთაც გააჩნიათ თავიანთი პროფილი;
- დაახლოებით 40% - ს აქვს მობილურიდან წვდომის საშუალება, რომელსაც იყენებენ აქტიურად;
- 55 წელს გადაცილებულები იყენებენ მხოლოდ საკუთარ კომპიუტერს;
- ქალები უფრო ხშირად იყენებენ სოციალურ მედიას ვიდრე მამაკაცები;
- სოციალური ქსელების აქტიური მომხმარებლის ასაკია 18 – 35 წელი.

ჰააგის სტრატეგიული კვლევების ცენტრის მონაცემებით, სულ უფრო იზრდება სოციალური მედიის შეღწევა ჩვენს ყოველდღიურ ცხოვრებაში, და როგორც მოსალოდნელია უახლოეს მომავალში კიდევ უფრო გაიზრდება. საზოგადოებრივ ცხოვრებაში სოციალური შეღწევადობის დონის სწრაფი გაზრდა დამოკიდებულია რამოდენიმე ფაქტორზე, რომელთაგან მთავარ როლს თამაშობს ქსელში დაშვების სიმარტივე და ნდობის უფრო მაღალი ხარისხი. ეს ფაქტორები კიდევ უფრო იზრდება და შესაბამისად გაიზრდება სოციალური ქსელების მომხმარებელთა რიცხვი.

ქვემოთ გრაფიკზე მოცემულია სოციალური ქსელების სიცოცხლის ციკლი, რაც პირდაპირპროპორციულად არის დამოკიდებული სოციალური ქსელის მომხმარებელთა რაოდენობაზე.



წყარო: *ალფონსო მონტაგნესე*

ცალკეულ პირებს შეუძლიათ გამოიყენონ სოციალური ქსელი არა მარტო პირადი მიზნებისთვის, არამედ სხვა ინტერესებშიც, მაგალითად, თავის თანამოაზრეებთან ერთად შექმნან ჯგუფი მათთვის საინტერესო სფეროში. სოციალურ ქსელში შექმნილი ჯგუფი არის პოტენციური მომხმარებელი და მას ფაქტიურად, მართავს ჯგუფის ერთი ან რამოდენიმე წევრი, ყველა მასში გაერთიანებული პირის სახელით. ხშირ შემთხვევაში, სოციალური ქსელის ჯგუფები ემსახურება მცირე წრის პირად ინტერესებს, რომელიც შეიძლება იყოს როგორც ყოფითი, ისე საზოგადო. უკვე გაჩნდა სპეციალისტების გაფრთხილება მომხმარებლისადმი სოციალურ ქსელებთან მუშაობის პროცესში მეტი ყურადღებისა და სიფრთხილის გამოჩენის შესახებ.

სოციალური მედია და ინფორმაციული ომი

სანამ სოციალური მედიის როლსა და ადგილზე ვისაუბრებდეთ ინფორმაციულ ომში, ვნახოთ რა არის ინფორმაციული ომი, რა მეთოდებს იყენებენ და რა ძირითადი მახასიათებლებით გამოირჩევა?

ამერიკის შეერთებული შტატების თავდაცვის დეპარტამენტის განსაზღვრებით, Information War (IW) ანუ როგორც მას ეძახიან აგრეთვე Information Operations (IO) - ეს არის ქმედება მიმართული საკუთარი ინფორმაციული სისტემის შენარჩუნებისკენ, რათა არ მოხდეს არასასურველი შეღწევა გარედან, ქვეყნის თავდაცვისუნარიანობის დარღვევის მიზნით. ამავდროულად, ეს არის ქმედება, რომელიც მიმართულია მოწინააღმდეგის საინფორმაციო სისტემის პარალიზებისკენ, ამ უკანასკნელზე უპირატესობის მოპოვების მიზნით.

თუმცა არსებობს კიდევ სხვა სახის განმარტება, კერძოდ IW/IO მოიხსენიებენ, როგორც მოწინააღმდეგე ან სხვა ქვეყნის მოსახლეობასა და სამხედრო მოსამსახურეებზე, ინფორმაციის გავრცელების გზით, ფსიქოლოგიურ ზემოქმედებას, პოლიტიკური და სამხედრო უპირატესობის მოპოვების მიზნით. ასეთი განსაზღვრებით IW/IO ხშირად მოიხსენიებენ, როგორც „ინფორმაციულ - ფსიქოლოგიურ ომს“.

IW/IO წარმოების დროს ძირითად მეთოდად გამოიყენება დეზინფორმაციის გავრცელება, ან ვრცელდება საჭირო კონტექსტის შემცველი ინფორმაცია. მსგავსი მეთოდები საშუალებას იძლევა შეცვალოს საზოგადოებრივი აზრი ამა თუ იმ მოვლენებზე.

IW/IO წარმოებას ძირითადად ახასიათებს:

- ინფორმაციული ზემოქმედება შეიძლება განხორციელდეს როგორც ინფორმაციული ბუმის ფონზე, ისე ინფორმაციული ვაკუუმის დროს;
- საშუალებად გამოიყენება ტრადიციული და სოციალური მედია საშუალებები, აგრეთვე ფოსტა და ჭორები;

- ინფორმაციული ზემოქმედება შეიცავს დამახინჯებულ ფაქტებს და ობიექტს ემოციურ ფონზე თავს ახვევს გამავრცელებლისთვის მისაღებ ინფორმაციას;
- ინფორმაციული ზემოქმედების ობიექტებად ითვლება როგორც მოსახლეობა მთლიანად, ისე ინდივიდები. ინდივიდუალური ზემოქმედების ობიექტებად მიჩნეულია ქვეყნის მმართველი პირები (პრეზიდენტი, პრემიერ - მინისტრი, მინისტრები, პოლიტიკოსები, სახელმწიფო თუ საზოგადო მოღვაწეები, კომპანიების ტოპ - მენეჯერები და ა. შ.) და მისი ძირითადი მიზანია მიაღებინოს მათ სასურველი გადაწყვეტილება. ხოლო მოსახლეობის შემთხვევაში, ხდება ცნობიერებაზე მასიური ზემოქმედება, რაც ფსიქოთერაპიის ანალოგად შეიძლება იქნეს მიჩნეული;
- ინფორმაციული ზემოქმედების დროს არ არის აუცილებელი ფსიქოაქტიური საშუალებების გამოყენება (შანტაჟი, დაშინება, ფიზიკური ზემოქმედება, მოსყიდვა და ა. შ.), თუმცა შეიძლება ღონისძიების კომპლექსურად ჩატარება.

IW/IO წარმოების დროს აქტიურად გამოიყენება სოციალური მედია საშუალებები. მისი გამოყენებისას ორგანიზებული ჯგუფები ცდილობენ მოიპოვონ თავიანთ მოწინააღმდეგეზე უპირატესობა, გახდნენ უფრო კონკურენტუნარიანები.

სოციალური მედია შეიძლება გახდეს IW/IO ეფექტური ინსტრუმენტი, ვინაიდან ის თავის მომხმარებელს აძლევს საშუალებას:

1) სტრატეგიული და ტაქტიკური თვალსაზრისით იძლევა მნიშვნელოვან შედეგებს:
- მოქმედებს დომეინის ფარგლებში (კიბერ სივრცე), განსხვავებით ტრადიციული სამხედრო სახეობებისგან (სახმელეთო, საზღვაო, საჰაერო);
- ზომებსა და მასშტაბებში, განსხვავებით ტრადიციული ომის წარმოებისგან;
- ობიექტებად სამხედროების გარდა მიღებულია აგრეთვე სოციალური საზოგადოება (ეთნიკური, რელიგიური, პროფესიული და კულტურული);

2) შესაძლებელია მიზნის მიღწევა მინიმალური ფინანსური დანახარჯებით;
3) მნიშვნელოვანი შედეგების მიღწევა ყოველგვარი კონტროლისა და მონიტორინგის, აგრეთვე გამოძიების შესძლებლობის ჩატარების გარეშე;
4) ასიმეტრიული კონფლიქტების მართვა, კერძოდ, ზემოქმედება ხდება მცირე და საშუალო ჯგუფებზე, როცა რეალური სამიზნე არის უფრო დიდი დაჯგუფება ან მთლიანად სახელმწიფო.

ინფორმაციული ომის წარმოებას სოციალური მედია საშუალებების გამოყენებით, შეიძლება გააჩნდეს სხვადასხვა ნიშანი, დამოკიდებული ორგანიზებული ჯგუფის ხასიათზე (ტერორისტული ან დანაშაულებრივი ჯგუფი, სახელმწიფო, კომპანია და ა. შ.) და მათ წინაშე დასახულ ამოცანაზე. მოცემული შეიძლება დაიყოს შემდეგნაირად:

1) კიბერ - ომი (კიბერ - შეტევა) - „სახელმწიფოს - ერის მოქმედება მიმართული სხვა სახელმწიფოს კომპიუტერულ ქსელში შესაღწევად, ამ უკანასკნელისთვის ზიანის მიყენების ან საერთოდ მწყობრიდან გამოყვანის მიზნით“ (Richard Clarke, USA national security expert) ანუ სხვა სიტყვებით, რომ ვთქვათ ეს არის შეტევითი ღონისძიებების კომპლექსი, რომელიც ხორციელდება კიბერ სივრცეში ერთი ან რამდენიმე სახელმწიფოს მიერ, და მიმართულია სხვა სახელმწიფოს ან საერთაშორისო დონის არასახელმწიფო სუბიექტის წინააღმდეგ;
2) კიბერ - ტერორიზმი, რაც გამოიყენება ტერორისტული ორგანიზაციების მიერ კიბერ სივრცეში და მიმართულია ქვეყნის ეროვნული უსაფრთხოების წინააღმდეგ;
3) ანტი კიბერ - ტერორიზმი, გამოიყენება ტერორისტული ორგანიზაციების წინააღმდეგ და ხორციელდება კიბერ სივრცეში;
4) კიბერ - დანაშაული, გამოიყენება სხვადასხვა დამნაშავე ან ტრანსნაციონალური ჯგუფების მიერ, რომლის დროსაც კიბერ სივრცის გამოყენებით ხდება ქურდობა, ინფორმაციის მოპარვა, თაღლითობა და ა. შ.

მათი ობიექტები შეიძლება იყოს როგორც ცალკეული პირები, ისე მსხვილი კომპანიები. მისი მიზანია ეკონომიკური მოგების მიღება;

5) ანტი კიბერ - დანაშაული, ეს მოიცავს სახელმწიფოს სამართალდამცავების ან კერძო პირებისა და კომპანიების მხრიდან დაცვით ღონისძიებებს მიმართულს კიბერ დამნაშავეების წინააღმდეგ.

აქ შეიძლება აღინიშნოს ის გარემოება, რომ სპეციალისტები და ექსპერტები ცალკე საკითხად გამოყოფენ კიბერ - შეტევას, და განასხვავებენ მას კიბერ - ომისგან. თუმცა უნდა აღინიშნოს ისიც, რომ ხშირ შემთხვევაში ძალზედ ძნელია განასხვავო კიბერ - ომი კიბერ - შეტევისგან, ჯერ ფაქტიურად, დადგენილი არ არის ზღვარი მოცემულ ორ მცნებას შორის, და არ არის კონკრეტულად განსაზღვრული ის კრიტერიუმები, რომლითაც უნდა შეფასდეს ან ერთი, ან მეორე ქმედება.

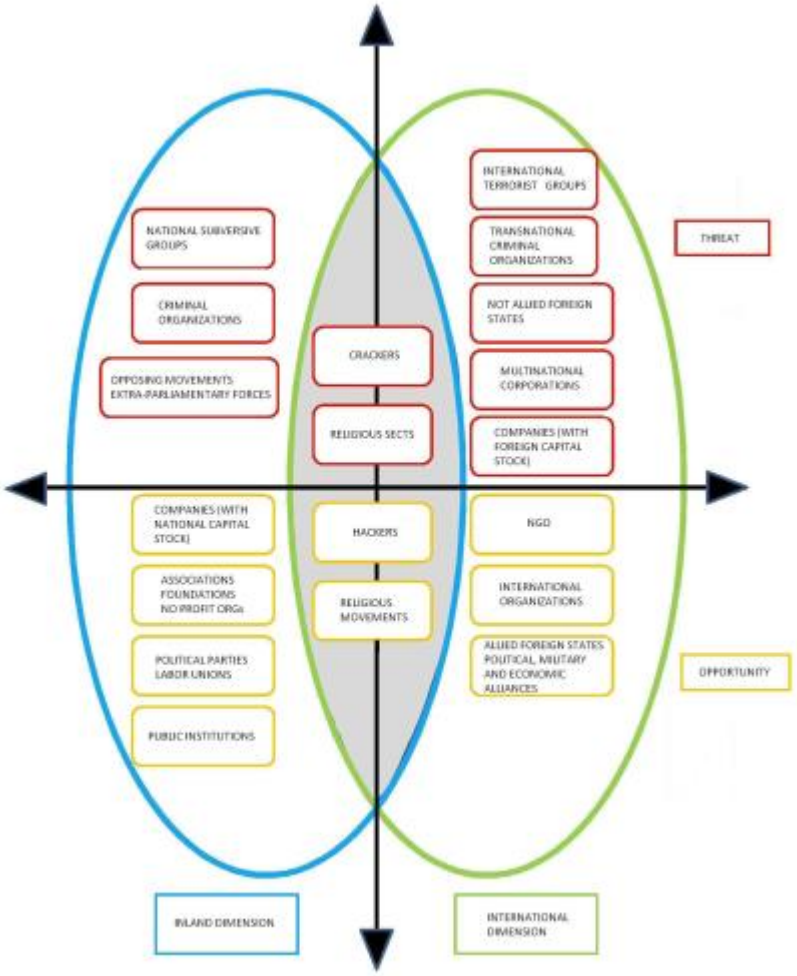
სოციალური მედია შეიძლება გამოყენებულ იქნას ადგილობრივი და საერთაშორისო დამნაშავე ჯგუფების მიერ, რომელიც პირდაპირ უქმნიან საფრთხეს ეროვნულ უსაფრთხოებას. ასეთ ჯგუფებად მოიაზრებიან:

- ეროვნული დივერსიული ჯგუფები (მარქსისტულ - ლენინური დაჯგუფებები, ანარქისტები);
- ეროვნული და ტრანსნაციონალური დამნაშავე ჯგუფები (მაფია, იაკუძა, ტრიადა, კამორა);
- ტერორისტული ორგანიზაციები;
- მულტინაციონალური კომპანიები თავისი ფინანსური საშუალებებით;
- კომპანიები საგარეო კაპიტალით;
- ექსტრა საპარლამენტო ოპოზიციური ჯგუფები (მემარჯვენე ექსტრემისტები, ქსენოფობიური ჯგუფები);
- რელიგიური სექტები;
- ჰაკერთა დაჯგუფებები;
- სხვა სახელმწიფოსი და ეროვნული სამხედრო - პოლიტიკური, აგრეთვე ფინანსური გაერთიანებები;

- ასოციაციები, ფონდები, არაკომერციული ორგანიზაციები;
- არასამთავრობო და საერთაშორისო ორგანიზაციები;
- პოლიტიკური ორგანიზაციები და პროფკავშირები;
- სახელმწიფო დაწესებულებები.

სოციალური მედია საშუალებები ვითარდება სწრაფად და ის ვრცელდება მთელს მსოფლიოში, სადაც კი არის ინერნეტ წვდომა. ეს ფაქტი საშუალებას იძლევა ჩამოყალიბდეს და შეიქმნას კიდევ ახალი ტიპისა და თავისი საქმიანობით განსხვავებული უცნობი დაჯგუფებები, რომელთა რეალური მიზნები და მისწრაფებები გარკვეულ დრომდე ცნობილი არ არის, და შესაძლებელია ის იყოს გარკვეული საფრთხის შემცველი, რომლის შესწავლას სჭირდება გარკვეული დრო. ყოველივე ეს აშკარად უარყოფითად აისახება ეროვნულ უსაფრთხოებაზე. ამიტომ ეს თემა არის მუდმივი კვლევისა და შესწავლის საგანი. აგრეთვე, შეიძლება ითქვას, რომ საჭიროა მუდმივი მონიტორინგი სოციალურ მედიაზე, თუმცა არ უნდა დაირღვეს პიროვნების უფლებები და ჯდებოდეს კონსტიტუციით განსაზღვრულ ფარგლებში.

ქვემოთ მოყვანილი სქემა აჩვენებს თუ როგორ შეიძლება ცალკეულმა ჯგუფებმა იქონიონ დადებითი ან უარყოფითი გავლენა ეროვნულ უსაფრთხოებაზე.



წყარო: *ალფონსო მონტაგნესე*

ეროვნული უსაფრთხოება

სანამ კონკრეტულად საფრთხეებზე დავიწყებდეთ საუბარს, ორიოდე სიტყვით ვთქვათ თუ რას წარმოადგენს ეროვნული უსაფრთხოება, რას მოიცავს და რის დაცვას უზრუნველყოფს, აგრეთვე რომელი სახელმწიფო სტრუქტურები ახორციელებენ ეროვნული უსაფრთხოების დაცვას?

არსებობს ეროვნული უსაფრთხოების ბევრი განმარტება, რომელთაგან წარმოგიდგენთ რამოდენიმე ვარიანტს, კერძოდ:

1. ეროვნული უსაფრთხოება - ეს არის პიროვნების, საზოგადოებისა და სახელმწიფოს სასიცოცხლოდ მნიშვნელოვანი ინტერესების დაცვა გარე და შიდა საფრთხეებისგან, ქვეყნის სტაბილური განვითარების უზრუნველყოფა;
2. ეროვნული უსაფრთხოება - ეს არის ერის შესაძლებლბა, არსებული მდგომარეობის საბაზისო ღირებულებებისთვის მინიმალური საფრთხის მიყენების გათვალისწინებით, მოთხოვნილებების დაკმაყოფილება აუცილებელი თვითდამკვიდრებისა და თვითგადარჩენისთვის;
3. ეროვნული უსაფრთხოება - ეს არის სტაბილურობა, რომელიც შეიძლება შენარჩუნებულ იქნას ხანგრძლივი პერიოდის განმავლობაში, ამავდროულად, წინასწარ შეფასდეს და გამოვლინდეს არსებული საფრთხეები, მათი დროული ნეიტრალიზაციის მიზნით;
4. ეროვნული უსაფრთხოება - ეს არის სახელმწიფო სტრატეგიისა და მიზნების ოფიციალურად მიღებული შეხედულებების ერთობლიობა, რომელიც უზრუნველყოფს პიროვნების, საზოგადოებისა და სახელმწიფოს დაცვას პოლიტიკური, ეკონომიკური, სოციალური, სამხედრო, ინფორმაციული, ტექნოგენური, ეკოლოგიური ან სხვა ხასიათის გარე და შიდა საფრთხეებისგან, არსებული რესურსებისა და შესაძლებლობების გათვალწნებით.

მოყვანილი განმარტებების გათვალისწინებით ეროვნული უსაფრთხოება თავისთან მოიცავს და შედგება შემდეგი კომპონენტებისგან:

- სახელმწიფო უშიშროება:
- საზოგადოებრივი უსაფრთხოება;
- ტექნოგენური უსაფრთხოება;
- ეკოლოგიური უსაფრთხოება;
- პოლიტიკური უსაფრთხოება;
- სამხედრო უსაფრთხოება;
- ეკონომიკური უსაფრთხოება;
- ენერგეტიკული უსაფრთხოება;

- ინფორმაციული უსაფრთხოება;
- პიროვნების უსაფრთხოება.

ეროვნული უსაფრთხოების უზრუნველყოფა - ეს არის პოლიტიკური, ეკონომიკური, სოციალური, სამხედრო, ჯანდაცვისა და სამართალდაცვითი ღონისძიებების ერთობლიობა, მიმართული ერის ნორმალური ცხოვრების უზრუნველყოფისკენ და შესაძლო საფრთხეების დროული პრევენციისკენ. მის მთავარ ამოცანად შეიძლება ჩაითვალოს მოქალაქის სტაბილური ეკონომიური მდგომარეობის ჩამოყალიბება, დაცვა და მისი კეთილდღეობის განვითარება სხვა ქვეყნის მოქალაქეებთან მიმართებაში.

ეროვნული უსაფრთხოების უზრუნველყოფა თავისთან მოიცავს:

- სახელმწიფო და საზოგადოებრივი წყობის დაცვას;
- სუვერენიტეტისა და ტერიტორიული დაურღვევლობის უზრუნველყოფას;
- ერის პოლიტიკური და ეკონომიკური დამოუკიდებლობის უზრუნველყოფას;
- ერის ჯანმრთელობის უზრუნველყოფას;
- საზოგადოებრივი წესრიგის დაცვას;
- დანაშაულებასთან ბრძოლას;
- ტექნოგენური უსაფრთხოების უზრუნველყოფასა და სტიქიური უბედურებისგან დაცვას.

ეროვნული უსაფრთხოების დაცვაში კომპლექსურად ჩართულია სახელმწიფოს ყველა არსებული რესურსი, თუმცა მის დაცვას ძირითადად უზრუნველყოფს არმია, დაზვერვისა და კონტრ - დაზვერვის სამსახურები, სამართალდამცავი და ჯანდაცვის სტრუქტურები.

ეროვნული უსაფრთხოებისთვის სოციალური მედიის გამოყენებით შექმნილი საფრთხე

სოციალურ მედიას შეიძლება გააჩნდეს როგორც დადებითი ისე უარყოფითი ეფექტი ქვეყნის ეროვნულ უსაფრთხოებაზე. რაც უფრო მაღალია ქვეყნის ინფორმატიზაციის დონე, მით მაღალია საფრთხის შემცველი რისკ - ფაქტორები, მიმართული ქვეყნის სტრატეგიული ინტერესებისა და მიზნების წინააღმდეგ. მსაგავსი საფრთხეები ეროვნულ უსაფრთხოებას შეიძლება შეექმნას სოციალური მედიის გამოყენებით.

ტერორისტული ორგანიზაციები

სოციალური მედია საშუალებებს სულ უფრო აქტიურად გამოიყენებს ტერორისტული ორგანიზაციები. ამ გზით წარმოებს ინფორმაციის გაცვლა და კომუნიკაცია, იდეოლოგიის გავრცელება, დაქირავების პროცესი და ტრენინგები.

დღესდღეისობით ყველაზე აქტიურად სოციალური მედიის საშუალებებს გამოიყენებს ისლამისტურ - ჯიჰადისტური ტერორისტული ორგანიზაციები. მაგალითად, ალ - ქაედას მიერ ხშირად გამოიყენება Facebook - სა და YouTube - ს არხები „ისლამის მებრძოლთა“ დაქირავებისთვის და ფუნდამენტური ისლამის იდეოლოგიის გავრცელებისთვის, აგრეთვე, ცდილობს სულ უფრო მეტი მომხრე შეიძინოს, განსაკუთრებით დასავლეთში. გარდა ამისა, სოციალური ქსელები აქტიურად გამოიყენება ტერორისტულ ორგანიზაციებს შორის ინფორმაციისა და რჩევების გასაცვლელად.

სოციალური მედია საშუალებებით, და ზოგადად ინტერნეტით ტერორისტული ორგანიზაციები ავრცელებენ ექსტრემისტულ მასალებსა და იდეებს, რაც მათ საშუალებას აძლევს მოახდინონ რეკრუიტმენტი, ყოველგვარი შუამავლის გარეშე.

ამის გარდა, სოციალური მედია საშუალებები გამოიყენება პროპაგანდისტული მიზნების მისაღწევად, კერძოდ, გაავრცელონ ინფორმაცია და შესაბამისი მასალები წარმატებულად ჩატარებული ტერორისტული ღონისძიებების შესახებ, რითაც თესავენ მოსახლეობაში პანიკას. აგრეთვე, ვრცელდება სხვადასხვა ხასიათის დეზინფორმაციული

მასალები და ინფორმაცია ტერაქტის ჩატარების შესახებ, რომლის მიზანს ასევე წარმოადგენს პანიკა. ამ დროს მოსახლეობის გარდა, სავარაუდო თავდასხმის ობიექტს შეიძლება წარმოადგენდეს კონკრეტული პირი, ფინანსური ინსტიტუტები, პოლიტიკური ორგანიზაციები ან მსხვილი კომპანიები.

აშშ - ს კვლევითი სამსახურების ვარაუდით, ზოგიერთი ტერორისტული ორგანიზაციების მხრიდან სოციალური მედიის გამოყენება ხდება მიზანმიმართული ტყუილის გავრცელება სტიქიური უბედურების დროს ან მისი დამთავრებისთანავე, რათა ზედმეტად უარყოფითად იქნას წარმოჩენილი ზემოქმედება, და ქვეყნის მხრიდან დაგვიანებული რეაქცია.

აშშ - ს არმიის განცხადებით, სოციალური მედია საშუალებები ზოგიერთი ტერორისტული ორგანიზაციის მიერ შეიძლება გამოყენებულ იქნას კომპიუტერული და მობილური ტექნიკის მიზანმიმართული დაზიანებისკენ. პროპაგანდისტული მასალების გავრცელების გარდა, სოციალური ქსელის საშუალებით, ძირითადად Facebook - სა და YouTube - ს არხების გამოყენებით, იგზავნება სპეციალურად დავირუსებული პროგრამები, რომელსაც მწყობრიდან გამოჰყავს მომხმარებლის ტექნიკა.

ყველაზე უფრო კარგად და წარმატებულად სოციალური მედიის გამომყენებლად შეიძლება ჩაითვალოს ალ - ქაედა, კერძოდ, ანვარ ალ - ავლაქი, რომელმაც შეიმუშავა მთელი სტრატეგია ინტერნეტის საშუალებით სასურველი ინფორმაციის გავრცელებისთვის, პროპაგანდისთვისა და დაქირავებისთვის. ის მოკლეს 2011 წლის 30 სექტემბერს, იემენში, აშშ - სადაზვერვო სამსახურების სპეციალურმა ძალებმა. ანვერ ალ - ავლაქის „წარმატებულ“ იდეოლოგიურ ოპერაციად შეიძლება ჩაითვალოს აშშ - ს არმიის მაიორის ნადილ ჰასანის მიერ, ალ - ავლაქის სოციალური ქსელით გავრცელებული პროპაგნდის ზემოქმედებით, 13 ამერიკელი სამხედროს მკვლელობა და 43 - ს დაჭრა, რომელიც მოხდა აშშ - ში, სამხედრო ბაზაზე, ერაყში გამგზავრების წინ. ნადილ ჰასანი პროფესიით იყო ფსიქოლოგი და სამხედროებს უტარებდა ფსიქოლოგიური მომზადების კურსებს.

კრიმინალური ორგანიზაციები

კრიმინალური ორგანიზაციები, თავიანთი არაკანონიერი საქმიანობის განხორციელებისთვის, სოციალურ მედია საშუალებებს იყენებენ მხოლოდ მხარდაჭერის მიზნით. ასეთი არაკანონიერი საქმიანო შეიძლება იყოს ან ინფორმაციის გავრცელება (მაგალითად, საბავშვო პორნოგრაფია, ვირუსების გავრცელება, პიროვნების პირადი ინფორმაციის მოპარვა და სხვა) ან ტრადიციული საქმიანობა (მაგალითად, ნარკოტიკების კონტრაბანდა, ტრეფიკინგი, ფულის გათეთრება, მოპარული დოკუმენტების გადაცემა, კორპორატიული შპიონაჟი).

კრიმინალური დაჯგუფებები შეიძლება იყოს ერთ ადგილას, ლოკალურად თავმოყრილი ადამიანთა ჯგუფი, რომლებიც ერთმანეთს პირადად იცნობენ, ან მსოფლიოს სხვადასხვა კუთხეში გაბნეული პირები, რომლებსაც ერთმანეთთან მხოლოდ ვირტუალური შეხება გააჩნიათ. ასეთი ჯგუფები იმართება ე. წ. მოდერატორების მიერ, რომლებიც აღჭურვილნი არიან განსაკუთრებული მმართველობითი უფლებებით, მათ შეუძლიათ გააგდონ ნაკლებად აქტიური წევრები, ან „დააწინაურონ“ კარგი შედეგის მაჩვენებლები.

სოციალურ მედიაში კრიმინალური ქსელი სულ უფრო ფართოვდება და სულ უფრო მასშტაბურ ხასიათს იძენს.

ომი

NATO - ს მიერ ჩატარებული კვლევების მიხედვით, მომავალში კონფლიქტები წარმოიქმნება იმ გარემოში, რომელსაც ახასიათებს საინფორმაციო და საკომუნიკაციო უახლესი ტექნოლოგიების, მათ შორის სოციალური მედია საშუალებების აქტიური გამოყენება.

სამხედრო ოპერაციების ჩატარების დროს პარალელურად წარმოებს მხარდამჭერი ღონისძიებები სოციალური მედია საშუალებებით. მაგალითად, ისრაელსა და ლიბანს შორის მომხდარი ბოლო ორი კონფლიქტი. 2006 წელს, მეორე კონფლიქტის დროს, ჰეზბოლამ ჩაატარა რამოდენიმე IW ოპერაცია სოციალური მედია საშუალებით, კერძოდ,

YouTube - ს გამოყენებით გამოაქვეყნეს რამოდენიმე მათთვის სასურველი ვიდეო და ფოტო მასალა, რის საპასუხოდ ისრაელმა მომავალი კონფლიქტების პერიოდში, იგივე სოციალური მედიის გამოყენებით გაუშვა კონტრ - ინფორმაციები.

საპროტესტო მოძრაობები და რევოლუციები

ახალი ტექნოლოგიები, და კერძოდ, სოციალური მედია საშუალებები ძალზედ მნიშვნელოვან, და ხშირ შემთხვევაში, გადამწყვეტ როლსაც თამაშობს საპროტესტო მოძრაობებსა და რევოლუციების ორგანიზებაში. ასეთ შემთხვევაში რევოლუციური ჯგუფების მიერ სოციალური ქსელები გამოიყენება მასობრივი გამოსვლებისთვის, მათი კოორდინაციისათვის და მოქმედების სტიმულირებისათვის, აგრეთვე, საპროტესტო გამოსვლების ტაქტიკური და ოპერატიული მართვის მიზნით.

თუ გავითვალისწინებთ იმ გარემოებას, რომ სოციალური მედია სულ უფრო სწრაფად ვითარდება, მაშინ დაბეჯითებით შეიძლება ითქვას, რომ შესაბამისად გაიზრდება საპროტესტო გამოსვლებისა და რევოლუციების რაოდენობა. Stratfor - ის ანალიტიკოსების განცხადებით, სოციალური მედია წარმოადგენს ინსტრუმენტს, რომელიც რევოლუციურ ჯგუფებს საშუალებას აძლევს შეამცირონ დანახარჯები ღონისძიების ორგანიზებაზე, მონაწილეობაზე, დაქირავებასა და ტრენინგზე.

ტუნისსა და ეგვიპტეში საპროტესტო გამოსვლების შესწავლისას გაირკვა, რომ:

- პროტესტში მოსახლეობის სტიმულირებასა და მართვაში, ძალზედ გაიზარდა სოციალური მედიის როლი;
- მობილურ ტელეფონთან ერთად, გაიზარდა მოქმედების სისწრაფე და გავრცელების არეალი;
- სიიაფის გამო, რევოლუციურ მოძრაობას საშუალება აქვს იმოქმედოს უფრო ავტონომიურად, ის საერთოდ არ არის დამოკიდებული საგარეო ფინანსებზე;
- ნაკლებად ან საერთოდ არ იზღუდება ცენზურისგან;

- საპროტესტო გამოსვლები და რევოლუციური ცვლილებები ხდება იმ ქვეყნებში, სადაც სახელმწიფოს ან კერძო კომპანიების მხრიდან არის მკაცრი ცენზურა ტრადიციულ მედია საშუალებებზე. ამ დროს სოციალური მედია საშუალება მოსახლეობისთვის წარმოადგენს ბრძოლის უნიკალურ შესაძლებლობას არსებულ რეჟიმთან, აგრეთვე თავიანთი სიტყვის თავისუფლებისა და უფლებების დაცვაში.

სახელმწიფო მოხელეების მიერ სოციალური მედიის არასწორი გამოყენება

სულ უფრო ხშირია სოციალური მედიის საშუალებით კონფიდენციალური და საიდუმლო მასალების გამოქვეყნება, რაც სერიოზულ ზიანს აყენებს ეროვნულ უსაფრთხოებას. გამოხატვისა და კომუნიკაციის თავისუფლება უნდა გაჩერდეს იქ, სადაც საქმე ეხება კონფიდენციალურობის შემცველ მასალებს. სახელმწიფო სტრუქტურები თავიანთ საქმიანობაში სულ უფრო აქტიურად იყენებენ სოციალურ მედიას, რომლის დროსაც არ არის გამორიცხული უნებურად საიდუმლო მასალის გავრცელება. ამიტომ, რისკების შემცირების მიზნით აუცილებელია სახელმწიფო ჩინოვნიკების მუდმივი ინფორმირება სოციალური ქსელის სწორად გამოყენებასა და უსაფრთხოების კულტურის ამაღლებაზე.

ეროვნული უსაფრთხოების დაცვის შესაძლებლობები

სოციალური მედია საშუალებები სახელმწიფო სტრუქტურების მიერ, ეროვნული უსაფრთხოების დაცვის მიზნით, შეიძლება გამოყენებული იქნას, როგორც თავდაცვით ისე თავდასხმით საშუალებად. კერძოდ, თავდაცვით ღონისძიებებში იგულისხმება პროფილაქტიკა, გაფრთხილება, კრიზისების მართვა, პროპაგანდასთან ბრძოლა, ხოლო თავდასხმითი მოქმედებები თავისთან მოიცავს ზემოქმედებას, პროპაგანდასა და ტყუილს.

სოციალური მედიის მუდმივი მონიტორინგი სადაზვერვო სამსახურების მხრიდან საშუალებას იძლევა მოპოვებულ იქნას წინმსწრები ინფორმაციები ეროვნული

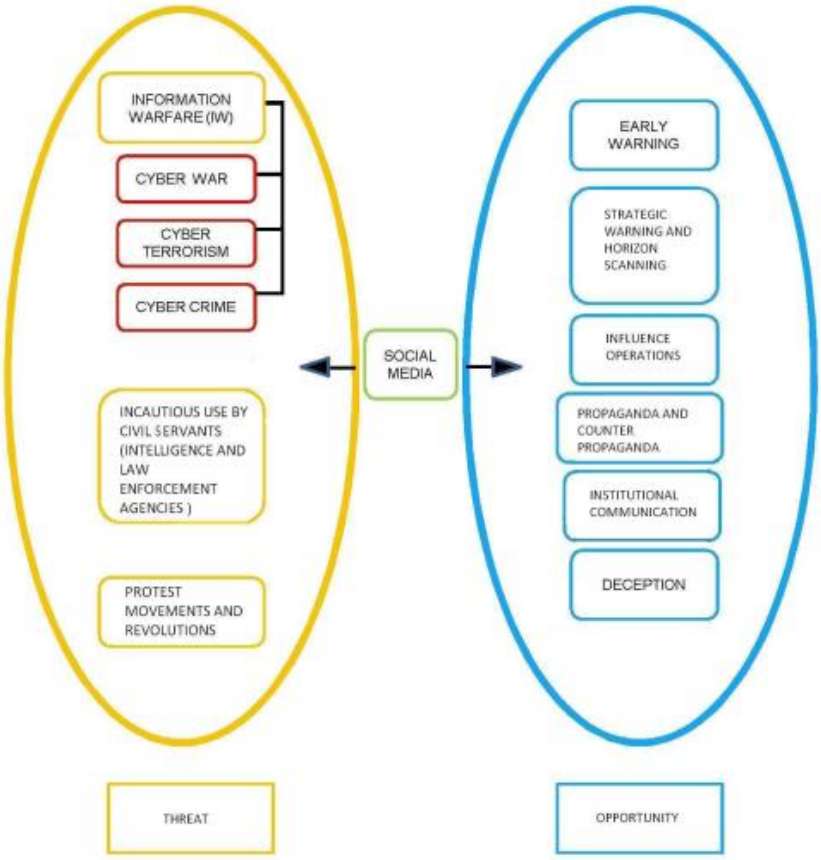
უსაფრთხოებისთვის შემცველი არსებული და მომავალი საფრთხეების შესახებ, და დროულად იქნას აღკვეთილი.

მონიტორინგის მუდმივი პროცესი ასევე იძლევა საშუალებას განისაზღვროს მოკლე-, საშუალო- და გრძელვადიანი პოლიტიკური, ეკონომიკური და სამხედრო პერსპექტივები, მოხდეს მოვლენათა ზუსტი შეფასება და გაკეთდეს მაქსიმალურად სწორი დასკვნები.

ეროვნული უსაფრთხოების სტაბილურობა ბევრად არის დამოკიდებული საერთაშორისო უსაფრთხოების შემადგენელ თითოეულ ცალკეულ კომპონენტზე. დღეს მსოფლიოში ერთ - ერთ მთავარ და ძირითად კომპონენტად განიხილება სწორედ კიბერსივრციდან მომდინარე საფრთხეები იქნება ეს კიბერ ომი თუ კიბერ შეტევა, ან სხვადასხვა სახის კიბერ დანაშაულება, რომლებმაც შესაძლოა სერიოზული საფრთხის წინაშე დააყენოს ეროვნული უსაფრთხოება და ქვეყნის სტრატეგიული ინტერესები. ამიტომ მსგავსი საფრთხეების პრევენციისა და რისკების შემცირების მიზნით, აუცილებელია მსხვილი მოთამაშე დიდი სახელმწიფოების მხრიდან გადადგმული იქნას შესაბამისი ნაბიჯები ურთიერთანამშრომლობისკენ, რითაც დაცული იქნება კიბერსივრცეში მოქმედების გარკვეული ბალანსი.

შეერთებულ შტატებსა და რუსეთს შორის უკვე დასასრულს უახლოვდება ორმხრივი მოლაპარაკებები, რაც ხელს შეუწყობს კიბერსივრცეში საფრთხეების შემცირებას, გამჭვირვალობასა და ურთიერთკოორდინაციას. კიბერსივრციდან მომდინარე საფრთხეები, ისევე როგორც ბირთვული საფრთხე, შეყვანილი იქნება დაცული კავშირის არხში, რომლის საშუალებითაც მოხდება ერთმანეთის გაფრთხილება და ინფორმაციის გაცვლა. ეს ხელს შეუწყობს მომხდარი ფაქტის მართებული სურათის წარმოსახვას და გამორიცხავს ე. წ. „ტყუილი განგაშის“ თემას, სადაც შესაძლოა ჩართული იყოს მესამე მოქმედი პირი ან არ მოხდეს ერთმანეთის შეცდომაში შეყვანა, რამაც შესაძლოა გამოიწვიოს საბრძოლო მოქმედებების დაწყება ან სხვა დიდი კატასტროფა, მათ შორის ბირთვული ომიც.

მსგავსი შეთანხმება არის წინგადადგული ნაბიჯი პირველ რიგში ორი ქვეყნის ეროვნული უსაფრთხოების დაცვის საკითხში, და შემდეგ მთელი მსოფლიოს საერთაშორისო უსაფრთხოებაში. ვინაიდან მოლაპარაკება ხდება ორ დიდ სახელმწიფოს შორის, რომლებიც დიდი, შეიძლება გადამწყვეტ როლს თამაშობენ მსოფლიო უსაფრთხოების საკითხში.

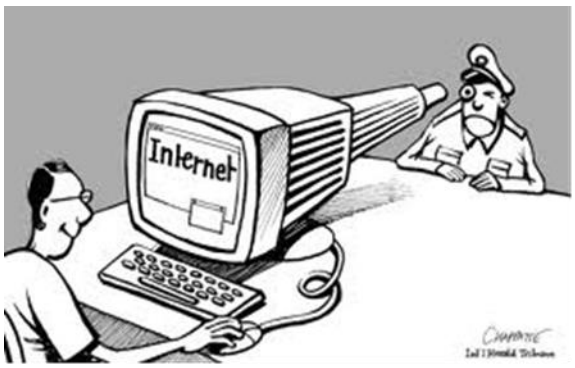


წყარო: *ალფონსო მონტაგნესე*

გამოყენებული ლიტერატურა

1. LINDSAY B. R., (2011), Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Congressional Research Service, Washington, DC;
2. LEWIS B. K., (2010), Social Media and Strategic Communication: Attitudes and Perceptions Among College Students, Public Relations Jouurnal vol. 4, New York;
3. BURSON - MARSTELLER, (2010), Social Media Check-up: a Burson – Marsteller Evidence – Based Tool, New York;
4. US DEPARTMENT OF DEFENSE, (2011), Department of Defense Strategy for Operatung in Cyberspace, Arligton Country, VA;
5. US GOVERNMENT, (2010), National Security Strategy 2010, Washington, DC;
6. CLARKER A., (2010), Cyber War: The Next Threat to National Security and What to do About it, Harper Collins, New York;
7. BURSON – MASTELLER, (2011), The Global Social Media Check – up 2011, New York;
8. http://www.hcss.nl
9. THE HAGUE CENTRE FOR STRATEGIC STUDIES, (2011), Social Networking – The security shakedown of shared information, Future Issue n. 11/2011, The Hague;
10. http://www.vincos.it
11. http://www.nmincite.com
12. http://www.bbc.co.uk
13. INTELLIGENCE AND NATIONAL SECURITY ALLIANCE, (2011), Cyber Intelligence: setting the landscape for an emerging discipline, Arlington, VA
14. NATO Allied Command Transformation, (2009), Multiple Futures Project – Navigating Towards 2030, Norfolk;
15. PAPIC M., NOONAN S., (2011), Social Media as a Tool for Protest, STRATFOR, Austin, TX;

16. WEINBERG S., (2011), The Spy Who Tweeted Me: Intelligence Wants to Monitor Social Media, Wired, San Francisco;
17. Capt. CC ALFONSO MONTAGNESE, (2012), Impact of Social Medea on National Security, Centro Militare di Studi Strategici;
18. თამთა კახაძე, კიბერუსაფრთხოება და XXI საუკუნის გამოწვევა, გაზეთი „24 საათი“, 7 ნოემბერი, 2011 http://24saati.ge/index.php/category/news/2011-11-07/21449;
19. ლონდონის კონფერენცია კიბერსივრცის შესახებ, ჟურნალი „ტაბულა“ 17 ოქტომბერი, 2011 http://www.tabula.ge/article-6058.html;
20. Ellen Nakashima, In U.S. – Russia deal, nuclearcommunication system may be used for cybersecurity, The Washington Post, 26 April, 2012;
21. Ellen Nakashima, U.S. Web site covering China scandal disputed by cyberattack, The Washington Post, 21 April, 2012;
22. Ellen Nakashima, Cyber-intruder sparks massive federal response – and debate over dealig with threats, The Washington Post, 9 December, 2011.



აპრილი, 2012 წელი

სოციალური ქსელები - დემოკრატია თუ უსაფრთხოება?

ინტერნეტის სწრაფმა განვითარებამ სათავე დაუდო უზარმაზარი ეკონომიკური და სოციალური შესაძლებლობების შექმნას. 2012 წლის მონაცემებით, სოციალური მედიის მომხმარებელმა ორ მილიარდზე მეტი შეადგინა, პლანეტის მთლიანი მოსახლეობის თითქმის მესამედი. არსებული გამოკვლევებითა და დაკვირვებით, ინტერნეტ ქსელის გაფართოება პირდაპირპროპორციულად აისახება მთლიანი შიდა პროდუქტის გლობალურ მაჩვენებელზე, რაც ხელს უწყობს კონკურენციის ზრდასა და ახალი ბაზრების შექმნას. ინტერნეტ სივრცეში მსოფლიო მასშტაბით წარმოებული კომერცია გულისხმობს რვა ტრილიონ აშშ დოლარის წლიურ ბრუნვას, ხოლო კიბერდამნაშავეთა მიერ მიყენებული ფინანსური ზარალი წელიწადში ერთ ტრილიონ აშშ დოლარს აღწევს. ინტერნეტ ქსელის მომხმარებელთა რიცხვი ყოველდღიურად იზრდება (მაგალითად, Google - ს ყოველდღიურმა მომხმარებელმა ერთ მილიარდს მიაღწია) და მისმა სწრაფმა განვითარებამ წარმოშვა ისეთი სერიოზული პრობლემები, რომლებიც ინტერნეტის გამოყენების დადებითი ნაწილის უპირატესობის მნიშვნელობას საგრძნობლად ამცირებს და საფრთხეს უქმნის კიბერსივრცის შესაძლებლობების სრულ გამოყენებას. ფაქტიურად, განვითარებულ ქვეყნებს გააჩნიათ ინფორმაციული ტექნოლოგიების ინოვაციური მომავლის შესაძლებლობა, მაგრამ ამავდროულად ისინიც და მთელი მსოფლიოც დგას საფრთხის წინაშე, რომ ყოველ ნოუ ჰაუს ასევე შეუძლია დიდი ზიანის მოტანა.

ახალი ინფორმაციული ტექნოლოგიები საკმაოდ დიდ შესაძლებლობებს აძლევს კრიმინალურ სამყაროსა და ტერორისტულ ორგანიზაციებს. მათ მიერ სოციალური

ქსელების გამოყენებით წარმოებს მოტყუება, დაშანტაჟება, იდეების მოპარვა, იდეოლოგიის გავრცელება, კორპორატიული თუ სამრეწველო შპიონაჟი და ა. შ. ინფორმაციული ტექნოლოგიების მიღწევები ასევე ბოროტად გამოიყენება რეპრესიული ხელისუფლებისა და ავტორიტარული რეჟიმების მხრიდანაც. კერძოდ, ისინი ზღუდავენ თავიანთ მოქალაქეთა უფლებებს, კრძალავენ სიტყვის თავისუფლებას და ხელს უშლიან სხვისთვის ადვილად ხელმისაწვდომი ინფორმაციის გავრცელებას. მაგალითად, რუსეთში საპრეზიდენტო არჩევნების წინა პერიოდში ოპოზიციური ძალების პარალიზების მიზნით, ხელისფულების მხრიდან მათ ბლოგებზე განხორციელდა კიბერშეტევები. ხოლო თურქეთში, ასევე არჩევნების პერიოდში დროებით დაიხურა Facebook - სა და სხვა სოციალურ ქსელებზე წვდომის შესაძლებლობა. კიბერსივრცეში ახალი ტექნოლოგიების შექმნამ ასევე წარმოშვა „კიბერ ომის“ ცნება, რაც თავისთან მოიცავს სახელმწიფოებისა და ალიანსების მხრიდან ერთმანეთისთვის ინფრასტრუქტურის განადგურების და მაქსიმალური ზიანის მიყენებას.

სოციალური ქსელებიდან მომდინარე საფრთხეებს დიდი ზიანის მიყენება შეუძლია მსოფლიო ცივილიზებული სამყაროსთვის და ისინი პირდაპირ ემუქრებიან ეროვნულ თუ საერთაშორისო უსაფრთხოებას. ამიტომ ცივილიზებული მსოფლიო ცდილობს შეინარჩუნოს ინტერნეტის უზარმაზარი შესაძლებლობები, არ შეფერხდეს ინფორმაციული ტექნოლოგიების ინოვაციური განვითარება, არ დაირღვეს ადამიანის უფლებები და ამავდროულად, ყოველივე ამის ფონზე მაქსიმალურად იყოს დაცული უსაფრთხოება თავის ყველა დონეზე.

უსაფრთხოების უზრუნველყოფაზე ფიქრისას მუდმივად ვაწყდებით გარკვეულ შეუთავსებლობას, რაც თავის მხრივ წარმოშობს დილემურ კითხვას - უფრო მეტი დემოკრატია თუ სათანადო უსაფრთხოება? ანუ სად მთავრდება დემოკრატიული პრინციპები და საიდან იწყება უსაფრთხოება, იქნება ეს ეროვნული თუ საერთაშორისო? ყოველი ქვეყნის ხელისუფლების საზრუნავს წარმოადგენს მოცემულ ორ ცნებას შორის სწორი არჩევანის გაკეთება და მათ შორის გარკვეული ბალანსის დამყარება.

ავტორიტარული მმართველობის ქვეყნებში, ხელისუფლება ცდილობს თავის კონტროლს დაუქვემდებაროს სოციალურ ქსელებზე მომხმარებლის წვდომა და მისი აქტიურობა. თუმცა უნდა ითქვას, რომ დემოკრატიულ ქვეყნებშიც წარმოიშვა მსგავსი პრობლემები, განსაკუთრებით „არაბული გაზაფხულის“, „დავიკავოთ უოლსტრიტისა“ და ლონდონში მასიური გამოსვლების შემდეგ. ყოველივე ორგანიზებული იყო ბლოგერების მიერ სოციალური ქსელების საშუალებით. ყველა გამოსვლამ გამოიწვია დასავლეთის დიდი შეშფოთება და შიში იმისა, რომ საპროტესტო აქციებს უფრო მასშტაბური ხასიათი არ მიეღო, არ გადაზრდილიყო პოლიტიკურში და არ ყოფილიყო გამოყენებული ულტრა - მემარცხენე ოპოზიციური ძალების მიერ.

ფაქტიურად, დასავლეთი აღმოჩნდა სერიოზული პრობლემის წინაშე. კერძოდ. სოციალური ქსელები, რომლებიც საზოგადოების ძალიან დიდ ნაწილს მოიცავს, კარგად გამოიყენება დესტაბილიზაციის მიზნებისთვის, შიდა პოლიტიკური, ეკონომიური თუ სოციალური ტემპერატურის კონტროლისთვის. ამის გამო სოციალური ქსელების სწორად გამოყენების გზებს მსოფლიოს მთელი საზოგადოება ეძებს. ხელისუფლების მხრიდან სოციალურ ქსელებზე მონიტორინგის განხორციელება და კონტროლის დაწესება გარკვეულწილად ადამიანის უფლებების დარღვევად აღიქმება, როცა არდაწესებამ შეიძლება წარმოშვას სერიოზული საფრთხეები. ეს ფაქტი კი ერთგვარი დილემის წინაშე აყენებს ამა თუ იმ ქვეყნის მთავრობებს, რომლებიც ცდილობენ პრობლემა თავისებურად მოაგვარონ, რაც ხშირ შემთხვევაში უშედეგოდ მთავრდება. მაგალითად, დიდი ბრიტანეთის პრემიერ - მინისტრის დევიდ ქემერონის მხრიდან გაკეთებულმა განცხადებამ სოციალურ ქსელებზე სახელმწიფო კონტროლისა და მონიტორინგის დაწესების შესახებ საზოგადოებრიობის დიდი უკმაყოფილება გამოიწვია და დემოკრატიული პრინციპებიდან გამომდინარე, მთავრობაც იძულებული იყო წასულიყო დათმობებზე.

ამერიკელი მეცნიერების კვლევები აჩვენებს, რომ სოციალური ქსელების კონტროლი საკმაოდ იოლი ყოფილა, რაც პირდაპირ კავშირშია თავად ქსელის სტრუქტურასთან და მის ჰომოგენურობასთან. სოციალური ქსელის საშუალებით

სასურველი შედეგის მისაღწევად, აუცილებელია ქსელის მხოლოდ 20 პროცენტ მომხმარებელში საჭირო ინფორმაციის გავრცელება. თუმცა უნდა აღინიშნოს, რომ ამ მეთოდითაც გარკვეულწილად იზღუდება პიროვნების თავისუფალი არჩევანისა და ნების გამოხატულობის საშუალება. ფაქტიურად, სოციალური ქსელის მეშვეობით მომხმარებელს გარკვეული ფორმით მიეწოდება ისეთი ინფორმაცია, რაც პირდაპირ კავშირშია მისაღები შედეგის დადგომასთან და იწვევს შენთვის სასურველი მიზნის მიღწევას, რაშიც ქსელის მომხმარებელი, მისდაგაუცნობიერებლად „გეხმარება“. ესეც შეიძლება მიჩნეულ იქნას სოციალურ ქსელებზე კონტროლის დაწესების ერთ - ერთ მეთოდად.

საკმაოდ რთული გადასაწყვეტია პრობლემა დაკავშირებული ადამიანის როგორც სოციალური ქსელების მომხმარებლის უფლებებთან. ეს უფლება ადამიანს მინიჭებული აქვს კონსტიტუციით, სხვადასხვა ქარტიებითა და საერთაშორისო აქტებით, მისი ხელყოფა კი დემოკრატიულობის პრინციპებიდან გამომდინარე ყოვლად დაუშვებელია. მის დარღვევას ან თუნდაც ნაწილობრივ შეზღუდვას ერიდება დემოკრატიულობის ინდექსის მაღალი თუ საშუალო ნიშნულის მაჩვენებელი ყველა ქვეყნის ხელისუფლება, რადგან ეს მისთვის პოლიტიკურად აშკარად წამგებიანი ნაბიჯი იქნება. ამიტომაც პოლიტიკური ლიდერები სოციალური ქსელების არასწორი გამოყენების პროცესს ხშირ შემთხვევაში უკავშირებენ ეროვნულ და საერთაშორისო უსაფრთხოებას, ქვეყნის სტრატეგიულ ინტერესებს, რაც ხშირად ხდება ხელისუფლების მხრიდან სოციალურ ქსელებზე არასანქცირებული ფარული მონიტორინგისა და კონტროლის განხორციელების მცდელობის მიზეზი. სწორედ აქ სრულდება დემოკრატია და იზღუდება მისი ფასეულობები. თუმცა ასევე მნიშვნელოვანია იმის გათვალისწინება, რომ უნდა ამაღლდეს სამოქალაქო ცნობიერება დაკავშირებული ქვეყნის უსაფრთხოების საკითხებთან და მოქალაქეთა მხრიდან სოციალური ქსელების სწორად გამოყენებასთან, რათა არ მოხდეს ქვეყნის სტრატეგიული ინტერესებისათვის რაიმე სახის ზიანის მიყენება.

ნოემბერი, 2014 წელი

ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები და რეკომენდაციები. საქართველოს კიბერუსაფრთხოების სტრატეგია

შესავალი

გარკვეული პერიოდის განმავლობაში, საზოგადოებრივი კეთილდღეობა და ეკონომიკური სტაბილურობა ეყრდნობოდა გადაცემის ქსელების მონაცემებისა და გამოთვლითი მომსახურების გამართულ მუშაობას, რომლის სანდოობის მაჩვენებელი საკმაოდ დიდი იყო. საერთო მოხმარების ინფორმაციული სისტემების ფუნქციონირებაზე დიდი გავლენა აქვს ისეთ ფაქტორებს, როგორებიც არის ინტერნეტზე შეტევა (attack), ფიზიკური ზემოქმედების შედეგად მიყენებული დარღვევები, პროგრამული და აპარატული უზრუნველყოფის მწყობრიდან გამოსვლა, ადამიანის როგორც მომხმარებლის მიერ მუშაობის პროცესში დაშვებული შეცდომები. ჩამოთვლილი ფაქტორები ნათლად აჩვენებს იმ გარემოებას, თუ რამდენად არის დამოკიდებული თანამედროვე საზოგადოება ინფორმაციული სისტემების სტაბილურ მუშაობაზე. მოცემულს ნათლად ასახავს კიბერუსაფრთხოების გერმანული სტრატეგია, კერძოდ: „კიბერსივრცეზე დაშვების უზრუნველყოფა, ასევე ინფორმაციის კონფიდენციალობა და სანდოობა კიბერსივრცეში გახდა ერთერთი მნიშვნელოვანი პრობლემა 21 - ე საუკუნეში. ამიტომ კიბერსივრცის დაცვა ხდება მთავარი ამოცანა სახელმწიფოს, ეკონომიკისა და საზოგადოების, როგორც ქვეყნის, ისე საერთაშორისო დონეზე“[1].

ევროკომისიის ზოგიერთ შეხვედრაზე[2] არაერთხელ განიხილებოდა და ამჟამადაც აქტიურად განიხილება ქსელისა და ინფორმაციული უსაფრთხოების მნიშვნელობა. ამ მიზნით, ასევე აქტიური განხილვის საგანია ერთიანი ევროპული ინფორმაციული სივრცის შექმნა.

[1] გერმანიის სტრატეგია, გვ. 1
http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

[2] მაგალითად, COM/2005/0229 final “i2010 – A European Information Society for growth and development”; COM/2006/251 “A Strategy for a Secure Information Society”; COM/2010/245 final/2 “A Digital Agenda for Europe”; COM/2009/149 on Critical Information Infrastructure Protection

ევროკომისიის ბოლო შეხვედრებზე მიღებული ნორმატიული და სამართლებრივი აქტები[3] ინფორმაციული ინფრასტრუქტურის (CII – Critical Information Infrastructure Protection) დაცვის შესახებ, გვთავაზობს პრაქტიკულ ზომებსა და რეგულაციებს ქსელების საერთო მოხმარების უსაფრთხოებისა და სანდოობის თაობაზე.

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

ევროკავშირის წევრ - ქვეყნებში კიბერუსაფრთხოების უზრუნველყოფის გაუმჯობესებისა და კოორდინირებული მუშაობის, ასევე, საერთო პოლიტიკის შემუშავების მიზნით, შექმნილია სპეციალური სააგენტო European Union Agency for Network and Information Security – ENISA[4].

ENISA ამუშავებს სპეციალურ სახელმძღვანელოს Good Practice Guide[5], რომელიც წარმოადგენს ევროკავშირის წევრი ქვეყნების მხარდამჭერ დოკუმენტს მათი მხრიდან კიბერუსაფრთხოების სახელმწიფო პოლიტიკის შემუშავების მთავარ მისიაში. მოცემული სახელმძღვანელო ევროკავშირის თითოეული წევრი ქვეყნისთვის იძლევა

[3] DIRECTIVE 2009/140/EU
[4] http://www.enisa.europa.eu/
[5] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

რეკომენდაციებსა და არსებულ მოწინავე პრაქტიკას კიბერუსაფრთხოების სტრატეგიის შემუშავებასა და დანერგვაში.

წინამდებარე დოკუმენტში მოკლედ არის განხილული ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოებისა და ზოგადად ევროკავშირის ინტერნეტის უსაფრთხოების სტრატეგიები, მასთან დაკავშირებული საკითხები და არსებული ვითარება. საკითხის მიმართ დიდი ინტერესიდან გამომდინარე, ქვემოთ განხილულია ასევე შეერთებული შტატების, კანადისა და იაპონიის კიბერუსაფრთხოების სტრატეგიის ძირითადი მიმართულებები. დოკუმენტში ასევე მოცემული არის სტრატეგიების საერთო მახასიათებლები, განსხვავებები, დასკვნა, რეკომენდაციები და წარმოდგენილია საქართველოს კიბერუსაფრთხოების პოლიტიკისა და სტრატეგიის მიმართულებები.

ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები

კიბერუსაფრთხოების პირველი სტრატეგია შემუშავებულ იქნა ამერიკის შეერთებულ შტატებში 2000 წლების დასაწყისში. შეერთებული შტატები გახდა ის ქვეყანა, რომელმაც დაიწყო კიბერუსაფრთხოების აღქმა, როგორც სახელმწიფო მნიშვნელობის საკითხი. 2003 წელს შეერთებულ შტატებში გამოქვეყნდა კიბერსივრცის უსაფრთხოების ეროვნული სტრატეგია (National Strategy to Secure Cyberspace)[6]. მოცემული დოკუმენტი წარმოადგენს უფრო ფართო ეროვნული უსაფრთხოების უზრუნველყოფის სტრატეგიის ნაწილს (National Strategy for Homeland Security), რომელიც შეიქმნა 2001 წლის 11 სექტემბრის ტერორისტული შეტევის პასუხად.

შემდგომ წლებში ევროპაში მთელი მასშტაბით დაიწყო ღონისძიებებისა და სტრატეგიების შემუშავება, რომელიც ემსახურებოდა კიბერუსივრცის დაცვის საკითხს. 2005 წელს გერმანია იღებს ინფორმაციული ინფრასტრუქტურის დაცვის სახელმწიფო გეგმას (National Plan for Information Infrastructure Protection - NPSI)[7]. მომავალ წელს შვედეთის მთავრობა ამუშავებს შვედეთში ინტერნეტის უსაფრთხოების გაძლიერების

[6] http://www.dhs.gov/files/publications/editorial_0329.shtm
[7] http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf

სტრატეგიას (Strategy to improve Internet Security in Sweden). ესტონეთმა თავისი კიბერუსაფრთხოების სტრატეგიის შემუშავება დაიწყო 2007 წელს რუსეთის მხრიდან ქვეყანაზე განხორციელებული მასიური კიბერშეტევის შემდეგ და 2008 წელს ევროკავშირის წევრ - ქვეყნებს შორის გახდა პირველი, რომელმაც გამოაქვეყნა კიბერუსაფრთხოების სახელმწიფო სტრატეგია[8]. ამის შემდეგ ევროკავშირის და უშუალოდ წევრი ქვეყნების მიერ გატარებულ იქნა მთელი რიგი ღონისძიებები და ჩატარდა დიდი სამუშაოები კიბერსივრცის უსაფრთხოების უზრუნველყოფის მიმართულებით. შედეგად, ევროკავშირის ათამდე წევრმა ქვეყანამ გამოაქვეყნა თავისი კიბერუსაფრთხოების სახელმწიფო სტრატეგია. ზოგიერთი წევრი ქვეყანა ამ დროისთვის არის სტრატეგიის დამუშავების სტადიაზე, რომლებიც ახლოსაა დასრულებასთან და მალე გამოქვეყნდება. ასევე აღსანიშნავია ის გარემოებაც, რომ ევროკავშირის რამოდენიმე წევრ - ქვეყანას გააჩნია არაოფიციალური ან არაფორმალური სტრატეგიები.

ქვემოთ განხილულია კიბერუსაფრთხოების სტარტეგიების მოკლე აღწერილობა. კერძოდ:

- ✓ **ესტონეთი** - კიბერუსაფრთხოების სტრატეგია ქვეყანამ მიიღო 2008 წელს. ესტონეთი დიდ მნიშვნელობას ანიჭებს თავისი კიბერსივრცის დაცვას და ამახვილებს ყურადღებას ინფორმაციული სისტემების უსაფრთხოებაზე. სარეკომენდაციო ღონისძიებები ატარებს სამოქალაქო ხასიათს და ეფუძნება სამართლებრივ რეგულაციებს, სწავლებასა და თანამშრომლობას;
- ✓ **ფინეთი** - ფინეთის მიერ კიბერუსაფრთხოების სტრატეგია მიღებულია 2008 წელს და მას საფუძვლად უდევს კიბერუსაფრთხოების გაგება როგორც ეკონომიკური ხასიათის პრობლემა, რომელიც მჭიდრო კავშირშია ქვეყნის ინფორმაციული სისტემებისა და საზოგადოების განვითარებასთან;
- ✓ **სლოვაკეთი** - ინფორმაციული უსაფრთხოების უზრუნველყოფა განიხილება როგორც საზოგადოების ნორმალური ფუნქციონირებისა და განვითარების აუცილებელი პირობა. ამიტომ სტრატეგიის მიზანს

[8] http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

წარმოადგენს ინფორმაციის დაცვის მჭიდრო ფუნდამენტი. სტრატეგია მიმართულია როგორც საფრთხის გაუვნებელყოფაზე, ისე ამისთვის საჭირო საშუალებების მზადყოფნასა და გაძლიერებაზე. სტარტეგია სლოვაკეთმა შეიმუშავა 2008 წელს;

- ✓ **ჩეხეთის რესპუბლიკა** - კიბერუსაფრთხოების სტრატეგიის ძირითადი მიმართულება თავისთან მოიცავს ინფორმაციული და საკომუნიკაციო სისტემების მოწყვლადი ადგილების დაცვას, ასევე რისკებისა და მოსალოდნელი საფრთხეების მაქსიმალურ შემცირებას. სტრატეგია ძირითადად ფოკუსირდება ინფორმაციულ სისტემებზე თავისუფალი დაშვების პრობლემებზე, ასევე ქვეყნის კიბერსივრცის მთლიანობასა და მონაცემთა კონფიდენციალობის დაცვაზე. სტრატეგია შემუშავდა 2011 წელს და ის კარგად არის ჰარმონიზირებული ჩეხეთის რესპუბლიკის სხვა სამართლებრივ - ნორმატიულ აქტებთან;
- ✓ **საფრანგეთი** - კიბერუსაფრთხოების სტრატეგია ქვეყნის ხელისუფლებამ მიიღო 2011 წელს, რომელიც ორიენტირებულია ინფორმაციული სისტემების შესაძლებლობებზე და ის წინ უნდა აღუდგეს კიბერსივრცეში არსებულ ისეთ მოვლენებს, რაც უარყოფითად მოქმედებს ინფორმაციის დაშვებაზე, მთლიანობასა და კონფიდენციალობის დაცვაზე. საფრანგეთი თავის სტრატეგიაში ძირითად აქცენტს აკეთებს ტექნიკური საშუალებებით ინფორმაციის დაცვაზე, კიბერდანაშაულებებთან ბრძოლასა და კიბერდაცვის გაძლიერებაზე;
- ✓ **გერმანია** - ქვეყნის კიბერუსაფრთხოების სტრატეგიას, რომელიც შემუშავებულ იქნა 2011 წელს, საფუძვლად უდევს კრიტიკული ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფა. ქვეყანა ძირითადად კონცენტრირებულია კიბერშეტევის დროულ გამოვლენაზე, გაუვნებელყოფასა და სამართლებრივ დევნაზე, ასევე ინფორმაციული და საკომუნიკაციო ტექნოლოგიების (ICT) მოწყობილობების მწყობრიდან გამოსვლის გაუვნებელყოფაზე, რომელიც გამოწვეულია შემთხვევითი

ფაქტორებით. ეს უკანასკნელი განსაკუთრებით ეხება კრიტიკულად მნიშვნელოვან ინფორმაციულ სისტემებს. სტრატეგიაში ასევე მოცემულია ანალიზი, რომელიც საშუალებას იძლევა განისაზღვროს დამატებითი ღონისძიებები მიმართული ინფორმაციული და საკომუნიკაციო ტექნოლოგიების (ICT) სისტემების დაცვაზე. სტარტეგიაში ასევე განსაზღვრულია მცირე და საშუალო ბიზნესის კიბერსივრცეში დაცვის უზრუნველყოფითი ღონისძიებები;

- ✓ **ლიტვა** - ქვეყანა ორიენტირებულია იმ მიზნებისა და ღონისძიებების განსაზღვრაზე, რომელიც მიმართულია ელექტრონული ინფორმაციის განვითარებაზე, ასევე კიბერსივრცეში კონფიდენციალობის დაცვაზე, დაშვებასა და მთლიანობაზე. გარდა ამისა, ლიტვის სტრატეგია უზრუნველყოფს კიბერსივრცეში პერსონალური მონაცემების, სატელეკომუნიკაციო ქსელის, ინფორმაციული სისტემისა და კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურის დაცვას კიბერშეტევებისა და უსაფრთხოების დარღვევისგან. სტრატეგიაში, რომელიც მიღებული იყო 2011 წელს, განსაზღვრულია ღონისძიებები, რომელთა რეალიზაცია იძლევა კიბერსივრცეში მუშაობის სრულყოფილი უსაფრთხოების გარანტიებს;
- ✓ **ლუქსემბურგი** - კიბერუსაფრთხოების სტრატეგია მიღებულ იქნა 2011 წელს. მოცემული სტრატეგია აცნობიერებს იმ საფრთხეებს, რომლებიც არსებობს კიბერსივრცეში და ამის გათვალისწინებით, გამოყოფილია საზოგადოებრივი და ეკონომიკური უსაფრთხოება. სტრატეგიაში ასევე აღნიშნულია ინფორმაციული და საკომუნიკაციო ტექნოლოგიების მნიშვნელობა ეკონომიკური ზრდისთვის, ცალკეული მოქალაქეებისთვისა და ზოგადად მთელი საზოგადოებისთვის. სტრატეგია მუშაობს შემდეგი ხუთი მიმართულით - ძირითადი ინფორმაციული ინფრასტრუქტურის დაცვა და დროული რეაგირება ინციდენტებზე; სამართლებრივ - ნორმატიული ბაზის მოდერნიზაცია; საერთაშორისო თანამშრომლობა; სწავლება და ინფორმირება; სტანდარტების დახვეწა;

- ✓ **ჰოლანდია** - ქვეყანა ერთის მხრივ მიისწრაფვის ინფორმაციული და საკომუნიკაციო სისტემების უსაფრთხო და სანდო ფუნქციონირებისკენ, და მეორეს მხრივ, აღიარებს ინტერნეტ სივრცის თავისუფლებისა და გამჭვირვალობის აუცილებლობას. 2011 წელს მიღებულ სტრატეგიაში აღსანიშნავი და მნიშვნელოვანია კიბერუსაფრთხოების განსაზღვრება, რომლის მიხედვით „კიბერუსაფრთხოება - ეს არის ინფორმაციული და საკომუნიკაციო სისტემების დაცულობა არასწორი ექსპლუატაციისგან, რომელმაც შეიძლება უარყოფითი გავლენა იქონიოს ინფორმაციული და საკომუნიკაციო სისტემებზე დაშვებასა და სანდოობაზე, ასევე რისკის ქვეშ დააყენოს სისტემებში არსებული ინფორმაციის კონფიდენციალობა და მთლიანობა“;
- ✓ **დიდი ბრიტანეთი** - გაერთიანებული სამეფოს მიდგომა ასევე მიმართულია კიბერუსაფრთხოების განვითარებაზე. სტრატეგიის მთავარი მიზანია გაიყვანოს დიდი ბრიტანეთი მოწინავე პოზიციებზე ინფორმაციული და სატელეკომუნიკაციო ტექნოლოგიების სფეროში ინოვაციების, ინვესტიციებისა და ხარისხიანი მომსახურების მიხედვით. ასევე მთლიანად ისარგებლოს კიბერსივრცის ყველა უპირატესობებითა და მიღწევებით. 2011 წელს შემოღებული სტრატეგია ასახავს მაქსიმალური რისკების შემცირებას დამნაშავეთა (მათ შორის ტერორისტების) და სხვა სახელმწიფოთა მხრიდან კიბერშეტევების მიმართ, რაც მიმართულია კიბერსივრცეში თითოეული მოქალაქის, საზოგადოებისა და ეკონომიკის უსაფრთხოებისკენ.

ევროკავშირის არაწევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები - შეერთებული შტატები, კანადა და იაპონია

როგორც ზემოთ იყო აღნიშნული, აქ მოკლედ იქნება განხილული ევროკავშირს არაწევრი ქვეყნების - შეერთებული შტატების, კანადისა და იაპონიის კიბერუსაფრთხოების სტრატეგიების მთავარი და მნიშვნელოვანი მიმართულებები. გარდა ამისა, აღსანიშნავია ის გარემოებაც, რომ ბევრ ქვეყანას უკვე აქვს გამოქვეყნებული თავისი სტრატეგიები ამ მიმართულებით. მაგალითად, კიბერუსაფრთხოების

სტრატეგიები გააჩნია ინდოეთს, ავსტრალიას, ახალ ზელანდიას, კოლუმბიას და სხვა ქვეყნებს. ეს ფაქტი ნათლად მოწმობს, რომ კიბერსივრცის დაცვა აღიარებულია მთავარ პრობლემურ საკითხად მთელს მსოფლიოში.

ამერიკის შეერთებული შტატები

2011 წლის მაისში[9] შეერთებულმა შტატებმა გამოაქვეყნა თავისი სტრატეგია კიბერსივრცის დაცვაზე. სტრატეგიას საფუძვლად უდევს მთავრობას, საერთაშორისო პარტნიორებსა და კერძო სექტორს შორის თანამშრომლობის მოდელი, სადაც აღწერილია მთელი რიგი ღონისძიებები, რომლებიც აუცილებელია გატარდეს შემდეგი შვიდი მიმართულებით:

- ეკონომიკა - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ღია და ლიბერალური ბაზარი;
- ეროვნული ქსელის დაცვა - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა;
- სამართალებრივი მხარე - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება;
- სამხედრო სფერო - უსაფრთხოების თანამედროვე გამოწვევებზე მზადყოფნა;
- სამთავრობო ინტერნეტის ქსელი - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება;
- საერთაშორისო განვითარება - უსაფრთხოების ორგანიზება, საერთაშორისო კომპეტენციების განვითარება და ეკონომიკური აყვავება;
- თავისუფლება ინტერნეტში - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა.

კანადა

[9] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

2010 წელს[10] გამოქვეყნებული კიბერუსაფრთხოების სტრატეგია ეფუძნება სამ ძირითად მიმართულებას:

- სამთავრობო სისტემების დაცვა;
- თანამშრომლობა ფედერალური მთავრობის გარეთ არსებული მთავარი კიბერ - სისტემების დაცვის მიზნით;
- კიბერსივრცეში კანადის მოქალაქეთა უსაფრთხოების უზრუნველყოფა.

პირველ მიმართულებაში იგულისხმება როლებისა და პასუხისმგებლობის მკვეთრი გამიჯვნა, ფედერალურ დონეზე კიბერ - სისტემების უსაფრთხოების გაძლიერება და კიბერუსაფრთხოების სფეროში მთავრობის ინფორმირების ამაღლება. მეორე მიმართულება ეს არის სახელმწიფო დონის საპარტნიორო პროექტები კერძო და კრიტიკული ინფრასტრუქტურის სექტორების მონაწილეობით. ბოლო, მესამე მიმართულება განსაზღვრავს ბრძოლას კიბერდანაშაულებებთან და ონლაინ სივრცეში კანადის მოქალაქეთა დაცვას. აქვე აგრეთვე განხილულია პერსონალური მონაცემების დაცვის პრობლემა.

<u>იაპონია</u>

იაპონიის კიბერუსაფრთხოების სტრატეგია, რომელიც გამოქვეყნდა 2010 წლის მაისის თვეში[11], შეიძლება დაიყოს რამოდენიმე მთავარ მიმართულებად, კერძოდ:

- მასიური კიბერშეტევების წინააღმდეგ ბრძოლა და ამ პროცესზე პასუხისმგებელი ორგანოს გაძლიერება;
- ინფორმაციული უსაფრთხოების სფეროში ცვლილებებზე ადვილი ადაპტირების პოლიტიკის გატარება;

[10] http://publications.gc.ca/site/eng/379746/publication.html
[11] http://www.nisc.go.jp/eng/

- ინფორმაციული უსაფრთხოების აქტიური პოლიტიკის უპირატესობა პასიურებთან მიმართებაში.

იაპონიის კიბერუსაფრთხოების სტრატეგიაში აღწერილი მიმართულებები ასევე მოიცავს:

- ინფორმაციული და საკომუნიკაციო ტექნოლოგიების რისკების მართვას საზოგადოების უსაფრთხო ცხოვრების უზრუნველყოფის მიზნით;
- პოლიტიკის დანერგვა, რომელიც ხელს შეუწყობს სახელმწიფო უსაფრთხოების გაძლიერებას, კიბერსივრცეში კრიზისების მართვის გაუმჯობესება, რაც წინააღმდეგობაში არ მოვა ინფორმაციული და საკომუნიკაციო სისტემების გამოყენების პოლიტიკასთან, რომელსაც საფუძვლად უდევს სოციალური და ეკონომიკური მოღვაწეობა;
- სამნაწილიანი პოლიტიკა, სადაც კომპლექსურად განიხილება ეროვნული უსაფრთხოების, კრიზისების მართვისა და პიროვნებისა და საზოგადოების დაცვის პრობლემა. განსაკუთრებით, აქტიურად განიხილება პიროვნებისა და საზოგადოების ინფორმაციული უსაფრთხოების უზრუნველყოფა;
- ინფორმაციული უსაფრთხოების პოლიტიკა, რომელიც არ ეწინააღმდეგება ეკონომიკური ზრდის პოლიტიკას და მოდის მასთან თანხვედრაში;
- საერთაშორისო თანამშრომლობა და ალიანსების შექმნა.

ევროკავშირის ინტერნეტის უსაფრთხოების სტრატეგია

ამ მომენტისთვის ევროკავშირს არ გააჩნია კიბერუსაფრთხოების საერთო სტრატეგია. თუმცა 2012 წლის[12] ევროკავშირის კომისიის სამუშაო პროგრამაში დამტკიცებულია, რომ კომისია შეიმუშავებს ევროკავშირისთვის ინტერნეტის უსაფრთხოების სტრატეგიას. მოცემული სტრატეგიის შემუშავებას თავის თავზე იღებს DG CONNECT (DG INFOSO)[13] - ს მთავარი დირექტორატი. პროექტის მიზნები მდგომარეობს შემდეგში:

[12] COM (2011) 777 final VOL.1/2 http://ec.europa.eu/atwork/peogrammes/docs/cwp2012_en.pdf
[13] http://ec.europa.eu/dgs/connect/en/content/dg-connect

- ძირითადი რისკებისა და პრობლემების პარალელურად გამოვლინდეს ეკონომიკური და გეოპოლიტიკური შესაძლებლობები;
- მოხდეს შედარება მზადყოფნის ხარისხისა და პოლიტიკური ყურადღების და მესამე ქვეყნების ინტერნეტის უსაფრთხოების პრობლემებს შორის;
- აღინიშნოს ძირითადი და მნიშვნელოვანი პრობლემები, რომლებიც მოითხოვს დაუყოვნებლივ გადაწყვეტას;
- შეფასდეს მიმდინარე და დაგეგმილი ღონისძიებები, აგრეთვე აღინიშნოს ის პრობლემური ზონები, რომლებზეც ევროკავშირმა უნდა გაამახვილოს ყურადღება[14].

კიბერუსაფრთხოების სტრატეგია და ინტერნეტის უსაფრთხოების სტრატეგია - ეს არის ორი ერთმანეთისგან განსხვავებული თემა, თუმცა მათ გააჩნიათ ბევრი საერთოც. მაგალითად, შესაბამისი სამთავრობო მოდელის განსაზღვრა და შეთავაზება, რომელიც მიმართულია კიბერსივრცეში ინციდენტების გაუვნებელყოფაზე და მათ წინააღმდეგ ბრძოლაზე.

DG CONNECT - ის მთავარი დირექტორატის ძირითად ამოცანას წარმოადგენს გლობალურ პოლიტიკურ კონტექსტში სწორად დაალაგოს არსებული და დაგეგმილი ღონისძიებები. ინტერნეტის უსაფრთხოების პრობლემის მიმართ კომპლექსური და სტრუქტურული მიდგომის მიზნით, დირექტორატი ევროკავშირს ასევე უმზადებს და აწვდის მომავალ სამოქმედო გეგმას[15]. პროექტის რეალიზაციისთვის მარტო DG CONNECT - ის მთავარი დირექტორატის კომპეტენცია საკმარისი არ არის. ამიტომ მოცემულ თემაზე მიმდინარეობს კომპლექსური და კოორდინირებული მუშაობა ევროკავშირის სხვა კომისიებთან მჭიდრო თანამშრომლობით[16].

[14] COM(2011) 777 final VOL.2/2 http://ec.europa.eu/atwork/programmes/docs/cwp2012_annex_en.pdf

[15] ROADMAP: Proposal on a European Strategy for Internet Strategy http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

[16] SPEECH/12/204 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204

არაერთხელ იქნა აღნიშნული ის გარემოება, რომ აუცილებელია მიღწეულ იყოს კოორდინირებული და კომპლექსური მუშაობა, რის შესახებაც საუბარია 2011 წლის ENISA - ს დოკუმენტში „კიბერუსაფრთხოება: მომავალი გამოწვევები და შესაძლებლობები“[17] და ლორდთა პალატის მიერ პარლამენტში საბჭოზე გაკეთებულ მოხსენებაში ევროკავშირის შიდა უსაფრთხოების სტრატეგიის შესახებ[18].

ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიების საერთო პრინციპები და რეკომენდაციები

კიბერუსაფრთხოების განსაზღვრების შესახებ შეთანხმება საერთაშორისო დონეზე არ არსებობს[19]. ყოველ ქვეყანაში კიბერუსაფრთხოების, კიბერსივრცის, კიბერდანაშაულისა და მასთან დაკავშირებული მთავარი ტერმინების განსაზღვრება შეიძლება მკვეთრად განსხვავდებოდეს ერთმანეთისგან. ასევე განსხვავდება თითოეული ქვეყნის მიდგომა კიბერუსაფრთხოების სტრატეგიის შედგენის მიმართ. მიუხედავად იმისა, რომ საერთაშორისო თანამშრომლობის მნიშვნელობას აღიარებს ყველა ქვეყანა, მაინც საერთო მთავარი ტერმინებისა და ერთიანი ე. წ. „ენის“ არარსებობა ძალზედ ართულებს თანამშრომლობას საერთაშორისო დონეზე.

<u>საერთო პრინციპები</u>

როგორც წესი, ყოველი ქვეყნის კიბერუსაფრთხოების სტრატეგიებს მაინც გააჩნიათ საერთო პრინციპები, რომელიც შეიძლება შემდეგნაირად ჩამოყალიბდეს:

- ✓ სახელმწიფო მოდელისა და პოლიტიკის შემუშავება, რომელიც მიმართულია კიბერუსაფრთხოების უზრუნველყოფაზე;
- ✓ სახელმწიფო პარტნიორობაზე დაფუძნებული შესაბამისი მექანიზმის განსაზღვრა, რომელიც კერძო და სახელმწიფო სექტორის დაინტერესებულ

[17] http://www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities
[18] http://www.publications.parliament.uk/pa/ld201012/ldselect/ldeucom/149/149.pdf
[19] H. Luiijf, K. Besseling, M Spoelstra, P. de Graaf, Ten National Cyber Security Strategies: a comprasion, CRITIS 2001 – 6th International Conference on Critical Information Infrastructures Security, September 2011

მხარეებს საშუალებას აძლევს განიხილონ და დაამტკიცონ პოლიტიკა დაკავშირებული კიბერუსაფრთხოების პრობლემებთან;

- ✓ აუცილებელი პოლიტიკისა და მექანიზმების რეგულაციების დაგეგმვა და განსაზღვრა, როლების, უფლებებისა და პასუხისმგებლობის მკვეთრი გამიჯვნა კერძო და სახელმწიფო სექტორისთვის;
- ✓ საერთაშორისო დონეზე თანამშრომლობა ინფორმაციის გაცვლაზე კიბერდანაშაულის შესახებ და ამისთვის აუცილებელი საკანონმდებლო ბაზის არსებობა. ეს საშუალებას იძლევა განხორციელდეს თანამშრომლობა საერთაშორისო დონეზე. მაგალითად, ჰოლანდია[20] და საფრანგეთი[21] აძლიერებენ თავიანთ საკანონმდებლო ბაზას მიმართულს კიბერდანაშაულის, გამოძიებისა და სამართლებრივი დევნის შესახებ;
- ✓ კრიტიკული ინფორმაციის ინფრასტრუქტურის (CII – Critical Information Infrastructure Protection) განსაზღვრა. მათ შორის ძირითადი აქტივების, მომსახურებისა და ურთიერთდამოკიდებულების განვითარება;
- ✓ მზადყოფნის ამაღლება, ინციდენტებზე რეაგირების დროის მაქსიმალურად შემცირება, დაზიანებული კრიტიკული ინფორმაციის ინფრასტრუქტურის (CII – Critical Information Infrastructure Protection) დროული აღდგენისა და დაცვის მექანიზმების გეგმის შემუშავება. ორგანიზაციული სტრუქტურების ინტეგრაციის აუცილებელი განსაზღვრა, რომელთა ვალდებულებებში შედის ამაღლებული მზადყოფნის საშუალებების, დაცვის მექანიზმებისა და დაზიანებული ინფრასტრუქტურის დროული აღდგენის გეგმების დამუშავება, დანერგვა და ტესტირება;
- ✓ რისკების სახელმწიფო მართვის მიმართ სისტემური და ინტეგრირებული მიდგომის შემუშავება;

[20] ჰოლანდიის სტრატეგია, გვ. 12
[21] საფრანგეთის სტრატეგია, გვ. 8

- ✓ ინფორმაციული პროგრამების მიზნების განსაზღვრა და აღნიშვნა, რომელიც მიმართულია შესთავაზოს მომხმარებელს ქცევისა და მუშაობის ახალი მოდელები;
- ✓ საერთაშორისო თანამშრომლობა არამარტო ევროკავშირის წევრ - ქვეყნებს შორის, არამედ იმ ქვეყნებთანაც, რომლებიც არ შედიან ევროკავშირში;
- ✓ კომპლექსური კვლევების ჩატარება და პროგრამების განვითარებაზე მუშაობა, რომელიც მიმართულია კიბერსივრცის უსაფრთხოების პრობლემების გადაჭრაზე. ინტელექტუალური რესურსების განვითარება;
- ✓ განათლების ახალი პროგრამების აუცილებლობა, რომელიც მიმართულია ინფორმაციული და საკომუნიკაციო ტექნოლოგიების სპეციალისტებისა და სხვა საჭირო ადამიანური რესურსების მომზადებაზე, გადამზადებასა და პროფესიულ განვითარებაზე კიბერუსაფრთხოების სფეროში. ასევე ტრენინგებისა და სხვა მოკლე სასწავლო კურსების ჩატარების აუცილებლობა, რომელიც ანვითარებს მომხმარებლის უნარ - ჩვევებს. მაგალითად, გაერთიანებული სამეფოს[22] კიბერუსაფრთხოების სტრატეგიაში აქტიურად არის განხილული ინფორმაციული უსაფრთხოების სპეციალისტების საგანმანათლებლო პროგრამების განვითარება, რომელიც ხელს შეუწყობს კიბერუსაფრთხოების სანდო და პროფესიული ფუნდამენტის შექმნას.

<u>რეკომენდაციები</u>

გარემოში, სადაც მუდმივად ვითარდება, თავს იჩენს და განიცდის ევოლუციას კიბერსაფრთხეები, ევროკავშირის წევრი ქვეყნები, რომლებიც მუდმივად აწყდებიან ახალ გამოწვევებსა და გლობალურ საფრთხეებს კიბერსივრცეში, მიიღებენ დიდ სარგებელს მოქნილი და ოპერატიული კიბერუსაფრთხოების სტრატეგიის არსებობის შემთხვევაში.

[22] გაერთიანებული სამეფოს სტრატეგია, გვ. 29

კიბერდანაშაულის ტრანსსასაზღვრო ხასიათი წევრ - ქვეყნებს იძულებულს ხდის მჭიდროდ ითანამშრომლონ ერთმანეთთან და ზოგადად საერთაშორისო დონეზე. მსგავსი თანამშრომლობა აუცილებელია არამარტო კიბერშეტევისთვის ეფექტური მომზადებისთვის, არამედ მათზე დროული რეაგირებისთვის. ამიტომ კიბერუსაფრთხოების მიმართ სახელმწიფო სტრატეგიის მიდგომა უნდა იყოს კომპლექსური.

ამ მიზნით, ევროკავშირი, მასში შემავალი წევრი ქვეყნების მიმართ იძლევა ზოგად რეკომენდაციებს, კერძოდ:

მოკლევადიანი პერიოდისთვის

- ✓ დაპროექტდეს, შეფასდეს და მხარი დაეჭიროს კიბერუსაფრთხოების სახელმწიფო სტრატეგიას. ასევე ის ღონისძიებები, რომლებიც აუცილებელია გატარდეს სტრატეგიის ჩარჩოში;
- ✓ მკვეთრად უნდა განისაზღვროს მოქმედების არეალი, სტრატეგიის მიზნები და თავად ტერმინი „კიბერუსაფრთხოება“;
- ✓ უნდა დარწმუნდნენ, რომ კიბერუსაფრთხოებაზე პასუხისმგებელი სახელმწიფო ორგანოს მიერ შემუსავებული წინადადებები და რეგულაციები, იქნება განხილული და მიღებული;
- ✓ სტრატეგიაში უნდა იქნას გათვალისწინებული სამეცნიერო საზოგადოების, სამრეწველო და ეკონომიკური წარმომადგენლებისა და სამოქალაქო ინტერესები;
- ✓ კიბერუსაფრთხოების კოორდინირებული და შეთანხმებული ხასიათის გარანტირებული თანამშრომლობის მიზნით, წევრმა ქვეყნებმა უნდა ითანამშრომლონ ერთმანეთთან, აგრეთვე მათ მჭიდრო ურთიერთობა უნდა გააჩნდეს ევროკავშირის კომისიასთან;
- ✓ აუცილებელია აღიარებული იქნას ის გარემოება, რომ კიბერსივრცე და კიბერუსაფრთხოება მუდმივად განიცდის განვითარებას, და ამიტომ

სტრატეგია მუდმივად მოითხოვს რედაქტირებასა და გადახედვას, რათა ის შესაბამისობაში იქნას მოყვანილი ახალ გამოწვევებთან;

- ✓ აუცილებელია გავითვალისწინოთ ის ფაქტი, რომ მუდმივად არსებული რისკები და ახალი საფრთხეები საშუალებას იძლევა განვითარდეს და გაუმჯობესდეს ინფორმაციული სისტემები სახელმწიფო, კერძო და სამოქალაქო სექტორებისთვის;
- ✓ აუცილებელია თავიდან იქნას არიდებული გატარებული ღონისძიებების დუბლირება და ფოკუსირება გაკეთდეს ახალ პრობლემებსა და გამოწვევებზე;
- ✓ აუცილებელია, რომ სტრატეგია შესაბამისად იქნას გამოყენებული და მოქმედებდეს ეროვნული და ევროპული უსაფრთხოების დონის ამაღლებაზე;
- ✓ მხარი უნდა დაეჭიროს ევროკავშირის კომისიას ინტერნეტის უსაფრთხოების სტრატეგიაზე მუშაობის, შექმნისა და იმპლიმენტაციის საკითხში.

გრძელვადიანი პერიოდისთვის

- ✓ მომავალში მთლიანად ევროკავშირისთვის საერთო მიზნების მიღწევისა და ფორმულირების მიზნით, აუცილებელია შემუშავდეს და შეთანხმდეს „კიბერუსაფრთხოების“ საერთო განსაზღვრება და მასთან დაკავშირებული ტერმინოლოგია;
- ✓ აუცილებელია გათვალისწინებული იქნას ის გარემოება, რომ ევროკავშირისა და მისი წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები არ უნდა ეწინააღმდეგებოდეს საერთაშორისო საზოგადოების მიზნებს და ადამიანის უფლებებს, თუმცა ამავდროულად, გლობალურ დონეზე მხარს უნდა უჭერდეს კიბერუსაფრთხოების პრობლემებთან ბრძოლას.

კიბერუსაფრთხოების სტრატეგიის რეალიზაციისთვის აუცილებელია კერძო და სახელმწიფო სექტორების ერთმანეთთან მჭიდრო თანამშრომლობა, რომელიც სახელმწიფო და ზოგადად ევროკავშირის დონეზე, უნდა განხორციელდეს ინფორმაციის გაცვლის საშუალებებით, მოწინავე ტექნოლოგიებისა და პრაქტიკული ცოდნის გაზიარებით, აგრეთვე სამეცნიერო წრეების ერთმანეთთან დაახლოებითა და პრობლემაზე ერთობლივი მუშაობით.

როგორც ზემოთ იყო აღნიშნული, ENISA ევროკავშირის კომისიისა და წევრი ქვეყნებისთვის სტრატეგიის შექმნის მიზნით, შეიმუშავებს სპეციალურ სახელმძღვანელოს (Good Practices Guide). მოცემული სახელმძღვანელო შეიცავს რეკომენდაციებსა და მოწინავე პრაქტიკას კიბერუსაფრთხოების სახელმწიფო სტრატეგიის დაპროექტებისთვის, დანერგვისა და მხარდასაჭერად. ის არის სასარგებლო ინსტრუმენტი და პრაქტიკული რჩევები იმ პირებისთვის, ვინც არის სტრატეგიის დაპროექტებაზე პასუხისმგებელი ან ჩართულია ამ პროცესში. სახელმძღვანელო მუშავდება მთელი ევროპის მასშტაბით კერძო და სახელმწიფო სექტორიდან დაინტერესებული მხარეების მონაწილეობითა და ხელშეწყობით. სახელმძღვანელოს დამუშავებაში ასევე მონაწილეობას იღებენ ის საერთაშორისო ექსპერტები, რომლებიც აწარმოებენ ENISA - ს რეკომენდაციების შუალედურ ანალიზს.

საქართველოს კიბერუსაფრთხოების სტრატეგია, პოლიტიკა და გამოწვევები

2008 წლის აგვისტოში, საქართველო - რუსეთის ომის დროს, რუსეთის მხრიდან განხორციელდა მასიური კიბერშეტევა საქართველოს ინტერნეტ სივრცეზე, რის შედეგადაც გარკვეული პერიოდი პარალიზებული იყო ქვეყნის სამთავრობო და კერძო სექტორის ვებ - გვერდები, შეუძლებელი იყო დაკავშირება გარე სამყაროსთან. საქართველოს კიბერუსაფრთხოების სტრატეგიის შესავალ ნაწილში ვკითხულობთ, რომ „2008 წლის აგვისტოში რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად აჩვენა, რომ საქართველოს ეროვნული უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების

უზრუნველყოფის გარეშე. რუსეთ - საქართველოს ომის დროს, რუსეთის ფედერაციამ საქართველოს წინააღმდეგ სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, განახორციელა მიზანმიმართული და მასირებული კიბერშეტევები. აღნიშნულმა კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საზღვაო და საჰაერო სივრცეების დაცვა“[23]. ეს კიბერშეტევა ბევრი საერთაშორისო ექსპერტის მიერ შეფასდა როგორც „ინფორმაციული/კიბერ ომი“ საქართველოს წინააღმდეგ, რასაც ქვეყანა მოუმზადებელი შეხვდა, არ არსებობდა საჭირო რესურსები, გამოცდილება და შესაბამისად საქართველომ კიბერშეტევის მოგერიება ვერ შეძლო. შედეგად ქვეყანა აღმოჩნდა სერიოზული საერთაშორისო ინფორმაციული ვაკუუმის წინაშე. პრობლემა გადაიჭრა ქვეყნის უცხოელი სტრატეგიული პარტნიორების, კერძოდ ესტონელების ჩარევის შემდეგ, რის შედეგადაც შეჩერებული და თავიდან აცილებული იქნა მთლიანი ინფრასტრუქტურის განადგურება.

2008 წლის აგვისტოს ომისა და მისი შედეგების გათვალისწინებით, რაც უკავშირდებოდა ქვეყნის დაუცველ კიბერსივრცეს, საქართველოს ხელისუფლებამ დაიწყო სამართლებრივ - ნორმატიულ ბაზაზე მუშაობა მოცემული მიმართულებით, რის შედეგად 2013 წლის მაისში გამოქვეყნდა საქართველოს კიბერუსაფრთხოების სტრატეგია, რომელიც „წარმოადგენს „ეროვნული უსაფრთხოების მიმოხილვის“ პროცესის ფარგლებში შექმნილი კონცეპტუალური და სტრატეგიული დოკუმენტების პაკეტის ნაწილს. შესაბამისად, აღნიშნული სტრატეგია ეფუძნება „საქართველოს საფრთხეების შეფასების 2010 – 2013 წ.წ. დოკუმენტს“ და „საქართველოს ეროვნული უსაფრთხოების კონცეფციას““[24].

<u>საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ</u>

[23] საქართველოს კიბერუსაფრთხოების სტრატეგია, გვ. 1
[24] საქართველოს კიბერუსაფრთხოების სტრატეგია, გვ. 1

კიბერუსაფრთხოების სტრატეგიის გამოქვეყნებას წინ უძღოდა 2012 წლის ივნისში[25] კანონის „ინფორმაციული უსაფრთხოების შესახებ“ გამოქვეყნება. მოცემული კანონის მიზანია „ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება - მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები“[26].

კანონში „ინფორმაციული უსაფრთხოების შესახებ“ მოცემულია ტერმინთა განმარტებები, რომლის თანახმად ინფორმაციული უსაფრთხოება ეს არის „საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას“[27]. იქვე განმარტებულია კრიტიკული ინფორმაციული სისტემა და ის სუბიექტები[28], რომელთა ქვეყნის კიბერსივრცეში დაცვა აუცილებელი პირობაა ეროვნული უსაფრთხოების უზრუნველსაყოფად.

კანონი ასევე იძლევა კიბერსივრცის, კიბერშეტევისა და კომპიუტერული ინციდენტების საინტერესო განსაზღვრებას. კერძოდ:

„კიბერსივრცე - სივრცე, რომლის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვისათვის, შეცვლისათვის და გაცვლისათვის;

კიბერშეტევა - ქმედება, როდესაც ელექტრონული მოწყობილობა ან/და მასთან დაკავშირებული ქსელი ან სისტემა გამოიყენება კრიტიკულ ინფორმაციულ სისტემაში

[25] http://www.economy.ge/uploads/kanonmdebloba/kavshirgabmuloba/informaciuli_usafrtxoeba.pdf
[26] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 1
[27] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 1
[28] კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხა განსაზღვრულია საქართველოს პრეზიდენტის 2013 წლის 11 მარტის № 157 ბრძანებულებით https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1867646&lang=ge

შემავალი სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით;

კომპიუტერული ინციდენტი - ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას“[29].

კანონში განსაზღვრული და ზოგადად ჩამოყალიბებულია ის პრიორიტეტული საფრთხეები[30], რომლებიც შეიძლება თან ახლდეს კიბერუსაფრთხოებას, კერძოდ:

„ა) კიბერშეტევა, რომელიც საფრთხეს უქმნის ადამიანთა სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას;

ბ) კიბერშეტევა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული სისტემების წინააღმდეგ;

გ) კიბერშეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურსებს ან/და საკუთრების უფლებას;

დ) სხვა ნებისმიერი ქმედება, რომელიც, მისი ხასიათიდან, მიზნიდან, წყაროდან, მოცულობიდან ან რაოდენობიდან ან მისი აღკვეთისათვის საჭირო რესურსების ოდენობიდან გამომდინარე, კრიტიკული ინფორმაციული სისტემის ნორმალური ფუნქციონირებისათვის საკმარისი საფრთხის შემცველია“.

კანონი ასევე საინტერესოა იმ თვალსაზრისით, რომ ის განსაზღვრავს კიბერუსაფრთხოებაზე პასუხიმგებელ და მაკოორდინირებელ სახელმწიფო ორგანოს. კერძოდ, კანონის მე - 3 თავში „კიბერუსაფრთხოების უზრუნველყოფა“ ვკითხულობთ, რომ „საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, ასევე ინფორმაციული უსაფრთხოების

[29] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 1, 2
[30] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7

კოორდინაციისკენ მიმართულ სხვა, მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE“[3132]. მოცემული ჯგუფის მოვალეობებში შედის კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა, კომპიუტერული ინციდენტების ანალიზი, აღრიცხვა, მათი დროული გამოვლენა, რეაგირება და კოორდინაციის უზრუნველყოფა და სხვა. ასევე, ჯგუფი პასუხისმგებელია მოცემულ სფეროში ცნობიერების ამაღლებაზე, საგანმანათლებლო პროცესზე და სხვა[33]. კანონში ასევე ასახულია კრიტიკული ინფორმაციული სისტემის სუბიექტის მხრიდან პასუხისმგებელი პირის განსაზღვრის აუცილებელი ვალდებულება, კერძოდ „კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული სისტემების უსაფრთხოების პრაქტიკული უზრუნველყოფისათვის (კომპიუტერული უსაფრთხოების სპეციალისტი)“[34].

საქართველოს კიბერუსაფრთხოების სტრატეგია

საქართველოს კიბერუსაფრთხოების სტრატეგია გამოქვეყნდა 2013 წლის 20 მაისს[35], საქართველოს პრეზიდენტის 2013 წლის 17 მაისის №321 ბრძანებულების მიღების თანახმად. მოცემული დოკუმენტი შემუშავდა საქართველოს ეროვნული უშიშროების საბჭოსთან არსებული ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი საუწყებათაშორისო კომისიის მიერ

[31] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7

[32] 2013 წლის 24 დეკემბერს კანონში ინფორმაციული უსაფრთხოების შესახებ შევიდა ცვლილებები, რომლის თანახმად თავდაცვის სამინისტროში შეიქმნა კიბერუსაფრთხოების ბიურო, რომელიც პასუხისმგებელია თავდაცვის სფეროში კიბერსივრცის დაცვის უზრუნველყოფაზე, მეტი ინფორმაცია შეგიძლიათ იხილოთ https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2162943

[33] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7, 8

[34] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 9, გვ. 8

[35] https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1923932

და ის წარმოადგენს არამარტო სტრატეგიას, არამედ მასში მოცემულია ასევე ამ სტრატეგიის განხორციელების 2013 – 2015 წ.წ. სამოქმედო გეგმაც[36].

„საქართველოს კიბერუსაფრთხოების სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს სამოქმედო გეგმებს და ამოცანებს. სტრატეგიაზე დაყრდნობით, საქართველოს ხელისუფლება გაატარებს ღონისძიებებს, რომლებიც ხელს შეუწყობს სახელმწიფო ორგანოების, კერძო სექტორისა და სამოქალაქო საზოგადოების კიბერსივრცეში დაცულად ფუნქციონირებას, ელექტრონული ოპერაციების უსაფრთხო განხორციელებას და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებლად მოქმედებას“[37].

სანამ სტრატეგიის განხილვაზე გადავიდოდეთ, ვნახოთ კანონში „ინფორმაციული უსაფრთხოების შესახებ“ თუ როგორი განსაზღვრება აქვს იმ ძირითად საკითხებს, რაც უშუალო კავშირშია კუბერუსაფრთხოების უზრუნველყოფასთან. კერძოდ:

„კრიტიკული ინფორმაციული სისტემა - ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის“[38] და „კრიტიკული ინფორმაციული სისტემის სუბიექტი - სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის“[39].

საქართველოს ეროვნული უსაფრთხოების კონცეფცია კიბერსივრცის დაცვის უზრუნველყოფასა და ზოგადად კიბერუსაფრთხოებას განიხილავს, როგორც ქვეყნის

[36] საქართველოს კიბერუსაფრთხოების სტრატეგია, დანართი №2
[37] საქართველოს კიბერუსაფრთხოების სტრატეგია, გვ. 1
[38] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 2
[39] იქვე, დანარჩენი ტერმინოლოგია იხილეთ საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ http://www.economy.ge/uploads/kanonmdebloba/kavshirgabmuloba/informaciuli_usafrtxoeba.pdf

უსაფრთხოების ერთ - ერთ ძირითად შემადგენელ ნაწილსა და მის მნიშვნელოვან მიმართულებას. კიბერსივრცის დაცვასა და კიბერუსაფრთხოების უზრუნველყოფაზე ბევრად არის დამოკიდებული ქვეყნის შემდგომი ეკონომიკური სტაბილურობა და სოციალური განვითარება. მოცემული მიზნის მისაღწევად, სტრატეგია განიხილავს შემდეგი თანამშრომლობის მნიშვნელოვან პრინციპებს[40]:

- საქართველოს მთავრობის ერთიანი მიდგომა;
- თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის;
- აქტიური საერთაშორისო თანამშრომლობა;
- ინდივიდუალური პასუხისმგებლობა;
- ადეკვატური ზომები.

სტრატეგიის მთავარი მიზანია კიბერშეტევის ან სხვა ქმედებების საზიანო შედეგები და რისკები მაქსიმალურად იქნას შემცირებული და უმოკლეს დროში მოხდეს დაზიანებული ინფორმაციული ინფრასტრუქტურის სრული აღდგენა. ყოველივე ამას ემატება კრიტიკული ინფორმაციული სისტემების მდგრადობისა და დაცულობის ამაღლება, ასევე დროული პრევენცია.

გლობალური ინტერნეტ სივრცის მუდმივი განვითარება და მასთან დაკავშირებული არსებული საფრთხეები, საქართველოს კიბერსივრცესა და შესაბამისად კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემის გამართულ ფუნქციონირებას მუდმივად ახალი გამოწვევების წინაშე აყენებს. სტრატეგიის თანახმად, ინფორმაციული სისტემის კრიტიკულობა და კიბერუსაფრთხოების მდგრადობა განისაზღვრება ისეთი კრიტერიუმებით, როგორიცაა მოსალოდნელი მატერიალური ზარალის სიმძიმე და მასშტაბები, ინფორმაციული სისტემის აუცილებლობა სახელმწიფოსა და საზოგადოების ნორმალური ფუნქციონირება, სისტემის მომხმარებელთა რაოდენობა და კიბერუსაფრთხოების სათანადო დონის უზრუნველყოფა საჭირო რესურსებით.

[40] საქართველოს კიბერუსაფრთხოების სტრატეგია, გვ. 2

საერთაშორისო სისტემაში არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით, საქართველოს უსაფრთხოების პოლიტიკის დაგეგმვა და განხორციელება განიხილავს კიბერუსაფრთხოების სფეროში შემდეგ საფრთხეებსა და გამოწვევებს:

- კიბერომი ან/და კიბერშეტევა, რომელიც მიმართულია პოტენციური მოწინააღმდეგის მხრიდან საქართველოს მთლიანი კიბერსივრცის დაზიანებისა და მწყობრიდან გამოყვანისკენ. ამასთან, ქვეყანა კვლავ დგას მასიური კიბერშეტევის საფრთხის წინაშე;
- კიბერტერორიზმი, რომელმაც კრიტიკულ ინფორმაციულ ინფრასტრუქტურაზე კიბერშეტევით შეიძლება მნიშვნელოვანი ზიანი მიაყენოს ქვეყნის ეროვნულ უსაფრთხოებას;
- კიბერსივრცის გამოყენებით ჩადენილი სხვა ქმედებები, რომელმაც შეიძლება ზიანი მიაყენოს კრიტიკული ინფორმაციული ინფრასტრუქტურის ცალკეულ სუბიექტებს, რაც გამოიწვევს ეკონომიური, სოციალური თუ სხვა სფეროს ფუნქციონირების უარყოფით შედეგებს.

სტრატეგიაში განხილულია ასევე საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიმართულებები:

- კვლევა და ანალიზი;
- ახალი საკანონმდებლო - ნორმატიული ბაზა;
- კიბერუსაფრთხოების უზრუნველყოფის ინსტიტუციური კოორდინაცია;
- საზოგადოებრივი ცნობიერების ამაღლება და საგანამანმათლებლო ბაზის ჩამოყალიბება;
- საერთაშორისო თანამშრომლობა.

ძალზედ მნიშვნელოვანია, რომ კიბერუსაფრთხოების და მასთან დაკავშირებული ქმედებები, იქნება ეს სამართლებრივი და ნორმატიული აქტები, სხვადასხვა ინიციატივები, რეკომენდაციები, ინსტრუქციები, ასევე კიბერსივრცეში მიმდინარე

პროცესები, ემყარებოდეს კვლევებსა და ანალიზს, რომელიც უზრუნველყოფს არამარტო კიბერუსაფრთხოების პოლიტიკის ეფექტიანობასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემის ნორმალურ ფუნქციონირებას, არამედ ასევე დადებითად აისახება მთლიანად ეროვნული უსაფრთხოების პოლიტიკაზე.

სტრატეგიის მიხედვით, კვლევა და ანალიზი აუცილებელია განხორციელდეს შემდეგი მიმართულებებით:

- სხვა ქვეყნების საუკეთესო პრაქტიკის შესწავლა და გამოცდილების გაზიარება;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტების იდენტიფიცირების კრიტერიუმებისა და სტანდარტების კვლევა;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის მდგრადობის ანალიზი;
- კიბერუსაფრთხოების სფეროში რეგიონში არსებული პრობლემატიკის შესწავლა;
- კიბერუსაფრთხოების განმსაზღვრელი სტანდარტების შემუშავება მათი შემდგომი დანერგვის მიზნით;
- საქართველოს კიბერსივრცის წინაშე მდგარი საფრთხეების და რისკების გამოვლენაზე წინადადებების პერიოდული მომზადება.

მიუხედავად მსოფლიოში არსებული ახალი გამოწვევებისა, საფრთხეებისა და პოტენციური მოწინააღმდეგების არსებობისა, დღევანდელი მდგომარეობით საქართველოს კიბერუსაფრთხოების სფეროში არ გააჩნია ეროვნული კანონმდებლობა. აუცილებელი და მნიშვნელოვანია საკანონმდებლო ბაზის შექმნა, რომელიც შესაბამისობაში იქნება მოსული საერთაშორისო სტანდარტებთან და ხელს შეუწყობს მოცემული სფეროს განვითარებას.

სტარტეგიის მიხედვით, სამართლებრივი ბაზის შექმნისა და მისი სრულყოფისათვის აუცილებელია გატარდეს შემდეგი ღონისძიებები:

- ინფორმაციული უსაფრთხოების შესახებ საკანონმდებლო აქტების ინიცირება;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის განმსაზღვრელი და მისი კიბერუსაფრთხოების უზრუნველმყოფი ნორმატიული ბაზის შექმნა;
- კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის ფუნქციონირების სამართლებრივი უზრუნველყოფა;
- ევროპის საბჭოს 2001 წლის „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირების შედეგად აღებული ვალდებულებების შესრულება;
- იმ ორგანოს ან ორგანოთა საკანონმდებლო დონეზე იდენტიფიცირება, რომელთა უფლებამოსილებაში შევა ინფორმაციული უსაფრთხოების პოლიტიკის განსაზღვრა და მაკოორდინირებელი ფუნქციის განხორციელება;
- კიბერუსფრთხოებასთან დაკავშირებული კრიზისული სიტუაციების დროს მოქმედების სარეზერვო გეგმების და პროცედურების გაწერა.

იმისთვის, რომ კიბერუსაფრთხოებამ და მასთან დაკავშირებულმა პროცესებმა ეფექტური გავლენა მოახდინოს ქვეყნის ეროვნულ უსაფრთხოებაზე და იმუშაოს ერთიან სისტემად, აუცილებელია უწყებათაშორისი საკოორდინაციო მექანიზმის შექმნა, გაძლიერება და სახელმწიფო და კერძო სექტორების მჭიდრო თანამშრომლობა.

ამ მიზნით, სტრატეგიაში მოცემულია შემდეგი ღონისძიებების გატარების აუცილებლობა:

- კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შემდგომი განვითარება;
- მაღალტექნოლოგიური დანაშაულის (კიბერდანაშაული) საერთაშორისო საკონტაქტო პუნქტის 24/7 შემდგომი განვითარება;
- კიბერდანაშაულის საქმეებზე საექსპერტო დახმარების ჯგუფის (დანაყოფი) განსაზღვრა;

- სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის ფორმატისა და მექანიზმების ჩამოყალიბება.

კიბერუსაფრთხოების სფეროში რისკების შემცირება და კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა ბევრად არის დამოკიდებული საზოგადოებაში ცნობიერების ამაღლებაზე, შესაბამისი სპეციალისტების მომზადებასა და მათი პროფესიული დონის ამაღლებაზე, ასევე სგანმანათლებლო ბაზის შექმნა და სასწავლო პროცესის სწორად წარმართვა.

სტრატეგიის მიხედვით მოცემული პროცესი უნდა წარიმართოს შემდეგი ღონისძიებების გატარებით:

- კიბერუსაფრთხოების სფეროში საზოგადოებრივი ცნობიერების ამაღლებისა და საგანმანათლებლო პროგრამების შექმნა;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის სუბიექტების და სხვა დაინტერესებული ორგანიზაციების კადრებისა და ტექნიკური პერსონალის გადამზადება ინფორმაციული უსაფრთხოების საერთაშორისო და ეროვნული სტანდარტების შესწავლისათვის;
- კიბერდანაშაულის ექსპერტების სპეციალიზებული ტრენინგები ელექტრონული მტკიცებულებების (კიბერკრიმინალისტიკის) დარგში;
- კიბერუსაფრთხოების სფეროში სამეცნიერო - კვლევითი პროექტების ხელშეწყობა;
- კვლევითი ლაბორატორიის შექმნა.

კიბერუსფრთხოების სრულყოფილი უზრუნველყოფისათვის აუცლებელია არამარტო ქვეყნის შიგნით მოხდეს კოორდინირებული მუშაობა, არამედ აუცილებელია საერთაშორისო თანამშრომლობის მუდმივი განვითარება როგორც საერთაშორისო ორგანიზაციებთან, ისე ცალკეულ ქვეყნებთან, რათა მოხდეს მათი გამოცდილების გაზიარება, გადმოტანა და მორგება ჩვენს რეალობას.

სტარტეგიაში მოცემულია ის ღონისძიებები, რომლებიც უნდა გატარდეს საერთაშორისო თანამშრომლობის განვითარებისათვის, კერძოდ:

- კიბერუსაფრთხოების საკითხებზე საერთაშორისო ურთიერთობების განმტკიცება ამ სფეროში მომუშავე საერთაშორისო ორგანიზაციებთან (OECD, EU, OSCE, CoE, UN, ITU)[41] და სახელმწიფო ორგანოებთან;
- კიბერუსაფრთხოების სფეროში საერთაშორისო ინიციატივებში აქტიური მონაწილეობის მიღება და ამ ინიციატივების რეგიონის მასშტაბით მხარდაჭერა;
- სხვა ქვეყნების CERT - ებთან კიბერუსაფრთხოების სფეროში ორმხრივ და მრავალმხრივ ფორმატებში თანამშრომლობის ინიცირება.

საქართველოს კიბერუსაფრთხოების სტრატეგია არის გარდამავალი დოკუმენტი და მისი განხორციელების ვადებია 2013 – 2015 წლები, რისთვისაც შექმნილი არის სპეციალური სამოქმედო გეგმა[42] და მის განხორციელებაზე თავისი კომპეტენციის ფარგლებში პასუხისმგებელი უწყებები: საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო და საქართველოს CERT; საქართველოს შინაგან საქმეთა, იუსტიციისა და საგარეო საქმეთა სამინისტროები; საქართველოს ეროვნული უშიშროების საბჭოს აპარატი. სტრატეგიის სამოქმედო გეგმაში ასევე გათვალისწინებულია საერთაშორისო დახმარება კვლევითი ლაბორატორიის შექმნასა და ელექტრონული მტკიცებულებების (კიბერკრიმინალისტიკის) სფეროში, კიბერდანაშაულის ექსპერტების სპეციალიზებული ტრენინგების ორგანიზებაში.

[41] The Organisation for Economic Co-operation and Development (OECD) http://www.oecd.org/
The European Union (EU) http://europa.eu/
The Organization for Security and Co-operation in Europe (OSCE) http://www.osce.org/
The Council of Europe (CE) http://www.coe.int/web/portal/home
The United Nations (UN) http://www.un.org/
The International Telecommunication Union (ITU) http://www.itu.int/en/Pages/default.aspx
[42] საქართველოს კიბერუსაფრთხოების სტრატეგია, დანართი №2
https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1923932

რეზუმე

ნაშრომში მოკლედ, ზოგად ფორმებში არის განხილული ევროკავშირის წევრი ქვეყნებისა და შეერთებული შტატების, კანადისა და იაპონიის კიბერუსაფრთხოების სტრატეგიები, მათი პოლიტიკა და ძირითადი მიმართულებები. ასევე აქვე არის წარმოდგენილი თავად ევროკავშირის საერთო პოლიტიკა და მიდგომა ინტერნეტის უსაფრთხოების მიმართ. ფაქტიურად, ევროკავშირს არ გააჩნია ერთიანი კიბერუსაფრთხოების სტრატეგია, ის შემოიფარგლება მხოლოდ ცალკეული რეკომენდაციების გაცემით წევრი ქვეყნების მისამართით. თუმცა ამ ეტაპზე მიმდინარეობს აქტიური მუშაობა ევროკავშირის კიბერსივრცის დაცვის ერთიანი პოლიტიკის შემუშავებაზე. წევრი ქვეყნები ინდივიდუალურად ახორციელებენ და ზრუნავენ საკუთარი კიბერსივრცის დაცვაზე. მიუხედავად ამისა, ყოველი წევრი ქვეყნის კიბერუსაფრთხოების სტრატეგიებს მაინც გააჩნიათ საერთო პრინციპები, რაც მოკლევადიანი და გრძელვადიანი პერიოდის რეკომენდაციებთან ერთად, ასევე არის წარმოდგენილი წინამდებარე ნაშრომში.

საქრთველოსთვის სულ უფრო აქტუალური ხდება საკუთარი კიბერსივრცის დაცვის უზრუნველყოფა. ნაშრომში წარმოდგენილია ქვეყნის კიბერუსაფრთხოების სტრატეგიის პრინციპები, ძირითადი მიმართულებები, პოლიტიკა და სამოქმედო გეგმა. ასევე მოკლედ არის განხილული კანონი „ინფორმაციული უსაფრთხოების შესახებ“. ფაქტიურად, რუსეთის მხრიდან 2008 წლის აგვისტოში, ომის დროს განხორციელებული მასიური კიბერშეტევის შემდეგ, ქვეყნის ხელისუფლების მხრიდან გადაიდგა გარკვეული ნაბიჯები ქვეყნის კიბერსივრცის დაცვის შექმნისა და გაძლიერების მიმართულებით. თუმცა ამ სფეროში მაინც არსებობს გარკვეული ხარვეზები, კერძოდ ამ დრომდე არ არსებობს ერთიანი მაკოორდინირებელი სტრუქტურული ერთეული, არ არის შექმნილი ეროვნული კანონმდებლობა, ძალზედ დაბალია საზოგადოების ცნობიერება ამ სფეროს მიმართ და არ არსებობს შესაბამისი საგანმანათლებლო პროგრამები, არ ტარდება სამეცნიერო - კვლევითი სამუშაოები, არ არის შექმნილი ლაბორატორია და ა. შ.

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

დეკემბერი, 2014 წელი

კიბერსაფრთხეების წარმოშობის წყაროები და სახეობები. კიბერსაფრთხეებთან მებრძოლი სუბიექტები

შესავალი

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

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

ქვემოთ განხილულია კიბერსაფრთხეები და მათი სახეობები, რომლებიც ემუქრება კიბერსივრცეს და ზოგადად ინფორმაციული ინფრასტრუქტურის სისტემების მთლიანობას. ასევე ნაჩვენებია წარმოშობის ის წყაროები, საიდანაც მომდინარეობს

მოცემული კიბერსაფრთხეები. ნაშრომის მეორე ნაწილში განხილულია ის საერთაშორისო და რეგიონალური დონის სუბიექტები, რომლებიც ებრძვიან კიბერსაფრთხეებს და ცდილობენ დაიცვან კიბერსივრცე და ინფორმაციული ინფრასტრუქტურის სისტემები კიბერდამნაშავეთა ხელყოფისგან.

კიბერსაფრთხეების წარმოშობის წყაროები და სახეობები

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

კიბერსაფრთხეების წარმოშობის წყაროებს წარმოადგენენ როგორც სახელმწიფო და კერძო სექტორის წარმომადგენლები, ისე სხვადასხვა სახისა და ნიშნით შექმნილი ორგანიზაციები და ფიზიკური პირები. შეერთებული შტატების კონტროლის პალატის მასალების[43] მიხედვით, კიბერსაფრთხეების წარმოშობის წყაროები შეიძლება დავაკვალიფიციროთ შემდეგნაირად, კერძოდ:

- ✓ **სახელმწიფო** - უცხოეთის ქვეყნების სადაზვერვო სამსახურები კომპიუტერულ ტექნოლოგიებს იყენებენ ინფორმაციის შეგროვებისა და ჯაშუშობისთვის. მსგავსი ქმედებები სადაზვერვო სამსახურების მხრიდან შეიძლება მიმართული იყოს როგორც მეგობარი, ისე მოწინააღმდეგე ქვეყნების მიმართ, ან არასახელმწიფო სუბიექტების წინააღმდეგ. სახელმწიფო თავისი სადაზვერვო სამსახურების გამოყენებით, ახორციელებს კიბერშეტევებს პოტენციური მოწინააღმდეგე

[43] United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009)

სახელმწიფოების მიმართ დეზინფორმაციის, დესტაბილიზაციის, დაშინების ან ფართომასშტაბიანი კიბერომის წარმოების მიზნით. ასევე საყურადღებოა ის გარემოება, რომ ხშირად ხდება პიროვნების უსაფრთხოებისა და უფლებების დარღვევა. კერძოდ, სახელმწიფოს სპეციალურმა სამსახურებმა შეიძლება მიმართონ ისეთ ქმედებებს, რომელთა გამოყენებითაც ხდება მოქალაქეთა პერსონალური მონაცემების გადაჭერა, მოპარვა და გამოყენება. მსგავსი ქმედებები ხშირ შემთხვევაში ხდება სასამართლოს შესაბამისი ორგანოების სანქციისა და სწორი დემოკრატიული კონტროლის გარეშე;

- ✓ **კორპორაციები, კომპანიები** - დაკავებულნი არიან სამრეწველო/კორპორაციული ჯაშუშობითა და/ან დივერსიული საქმიანობით, რაშიც ისინი ხშირად იყენებენ ჰაკერებსა და ორგანიზებულ დამნაშავეთა ჯგუფებს. კომპანიების, კორპორაციებისა და კერძო სექტორის სხვა წარმომადგენლებს ასევე შეუძლიათ დაარღვიონ ადამიანის უფლებები პიროვნების პერსონალური მონაცემების შეგროვებისა და ანალიზის გზით, ან ზოგ შემთხვევაში მოცემული მონაცემების სახელმწიფო ორგანოებთან ან სხვა დაინტერესებულ პირებთან გაცვლით;
- ✓ **ჰაკერები** - იყო დრო როცა ჰაკერების მხრიდან ქსელებში არასანქცირებული შეღწევა ან პროგრამების გატეხვა დაკავშირებული იყო ჰაკერთა საზოგადოებაში ავტორიტეტის მოპოვებასთან ან წვრილმან ჰულიგნობასთან. დღესდღეისობით სურათი კარდინალურად არის შეცვლილი, კერძოდ ჰაკერთა უმრავლესობის ქმედება ატარებს კრიმინალურ ხასიათს. ადრე თუ ჰაკერებისთვის ქსელის გატეხვისათვის საჭირო იყო კომპიუტერული ტექნოლოგიების სფეროში სპეციალური უნარ - ჩვევების ცოდნა, როცა ამჟამად საკმარისია ინტერნეტიდან შესაბამისი ინსტრუქციებისა და პროტოკოლების გადმოქაჩვა და მათი გამოყენება შერჩეულ საიტზე კიბერშეტევის ორგანიზებისთვის. ამის გამო, კიბერშეტევის განხორციელება მომხმარებლისთვის გახდა უფრო ადვილად

ხელმისაწვდომი. ჰაკერთა მომსახურეობით სარგებლობენ არამარტო კორპორაციები და კომპანიები, არამედ სადაზვერვო ან სხვა სახის სპეციალური სამსახურებიც;

- ✓ **ჰაკტივისტები** - ტერმინი „ჰაკტივიზმი“ (hacktivism) წარმოიშვა ორი სიტყვის „Hack“ და “Activism” შეერთებით და ის აღნიშნავს სოციალური პროტესტის გამოხატვის ახალ მოვლენას, რომელიც წარმოადგენს თავისებურ სინთეზს რაღაცის მიმართ გამოხატული პროტესტის სოციალური აქტიურობისა და ჰაკერობის, რომელიც მიმართულია გარკვეული ვებ - გვერდების ან საფოსტო სერვისების წინააღმდეგ. თავიანთი პოლიტიკური მიზნების მისაღწევად, ჰაკტივისტები მიისწრაფვიან დააზიანონ ან საერთოდ მწყობრიდან გამოიყვანონ ზოგიერთი ვებ - გვერდი;
- ✓ **კიბერ დივერსანტები ქსელის უკმაყოფილო მომხმარებელთა რიცხვიდან** - ზოგადად, უკმაყოფილო მომხმარებლები წარმოადგენენ სერიოზულ საფრთხეს, ვინაიდან ისინი კარგად იცნობენ სისტემის მუშაობის პრინციპებს და შეუძლიათ თავიანთი ეს ცოდნა გამოიყენონ დესტრუქციული მიზნებისთვის. მაგალითად, სისტემის დასაზიანებლად ან კონფიდენციალური ინფორმაციის მოსაპარად. შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) მონაცემებით, სისტემის მომხმარებლებისა და გარე წყაროების მხრიდან კიბერშეტევის ორგანიზების შესაძლებლობის ერთმანეთთან შეფარდება შეადგენს 2:1;
- ✓ **ტერორისტები** - ცდილობენ ინფრასტრუქტურის მნიშვნელოვანი ობიექტები გამოიყვანონ მწყობრიდან, საერთოდ გაანადგურონ ან გამოიყენონ თავიანთი მიზნებისთვის. მათი ქმედება სერიოზული საფრთხის ქვეშ აყენებს ქვეყნების ეროვნულ უსაფრთხოებას, იწვევს ადამიანთა მასიურ მსხვერპლს, ასუსტებს ეკონომიკას, ასევე ზიანს აყენებს საზოგადოების მორალურ მდგომარეობასა და ამცირებს მათ სანდოობას ხელისუფლების მიმართ. ყველა ტერორისტული ორგანიზაცია და დაჯგუფება არ ფლობს საკმარის ცოდნასა და ტექნიკურ საშუალებებს

ეფექტური კიბერშეტევის განხორციელებისთვის, თუმცა არსებობს თეორიული დაშვება, რომ მათ მიიღონ მსგავსი ცოდნა და შესაძლებლობა, ან დახმარებისთვის მიმართონ ორგანიზებული დანაშაულის წარმომადგენლების მომსახურებას;

- ✓ **ბოტნეტი** - ინტერნეტ - ბოტი[44] ბოტნეტში წარმოადგენს პროგრამას, რომელიც ფარულად არის დაყენებული მსხვერპლის/ობიექტის კომპიუტერულ მოწყობილობაში, რაც დამნაშავეს/ბოროტმოქმედს საშუალებას აძლევს დავირუსებული კომპიუტერის რესურსების გამოყენებით, შეასრულოს გარკვეული ქმედებები. ჰაკერების ეს სახეობა თავისი პროგრამებით ავირუსებენ კომპიუტერების დიდ რაოდენობას, რომელთა რესურსებსაც შემდეგ იყენებენ კიბერშეტევის კოორდინირებისთვის, ასევე „სპამის“ გასაგზავნად, ფიშინგისთვის და სხვა მავნე ქმედებისთვის. მსგავსი სახის ქსელები წარმოადგენენ არალეგალური ვაჭრობის ობიექტს;
- ✓ **ფიშერები** - ეს არის ფიზიკური პირები ან პატარა დაჯგუფებები, რომლებიც იყენებენ ფიშინგის ტექნოლოგიებს[45] პერსონალური რეკვიზიტების მოპარვისა და ფასიანი ინფორმაციების გადაყიდვის მიზნით. თავიანთი მიზნების მისაღწევად ფიშერები ხშირად იყენებენ „სპამებს“ და ჯაშუშურ პროგრამებს;
- ✓ **სპამერები** - ფიზიკური ან იურიდიული პირები, რომლებიც მასიურად აგზავნიან არამოთხოვნილ ელექტრონულ ფოსტას დაფარული ან მცდარი ინფორმაციით, რომლის მიზანია ფიშინგითა და ჯაშუშური პროგრამების გამოყენებით კონკრეტულ ორგანიზაციებზე კიბერშეტევის განხორციელება;

[44] Internet bot - ეს არის სპეციალური პროგრამა, რომელიც ავტომატურად და/ან მიცემული დავალების თანახმად, ასრულებს იგივე მოქმედებებს, რასაც ჩვეულებრივი მომხმარებელი

[45] Phishing - ინტერნეტ სივრცეში მაქინაციების სახეობა, რომლის მიზანს წარმოადგენს კონკრეტული მომხმარებლის კონფიდენციალური მონაცემების - ე. წ. Login - სა და პაროლის, მიღება

- ✓ **ჯაშუშური და მავნე პროგრამების შემქმნელები** - ფიზიკური ან იურიდიული პირები, რომლებსაც გააჩნიათ დანაშაულებრივი ზრახვები კომპიუტერების მომხმარებლებზე კიბერშეტევის განსახორციელებლად;
- ✓ **პედოფილები** - ეს კატეგორია სულ უფრო აქტიურად იყენებს ინტერნეტს საბავშვო პორნოგრაფიის გასავრცელებლად, ასევე სოციალური ქსელებისა და ინტერნეტ ჩათების გამოყენებით, პოტენციური მსხვერპლების გასაცნობად.

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

შეერთებული შტატების კონტროლის პალატის იგივე მასალებში განხილულია ასევე კიბერსაფრთხეების სახეობები, კერძოდ:

<u>მონაცემთა მთლიანობა</u>

კიბერშეტევების დროს შეიძლება გამოყენებული იყოს ჰაკერული მეთოდები, რომლის მიზანია მონაცემთა მთლიანობის განადგურება ან მათი დამახინჯება და ცვლილებების შეტანა. ქვესახეობები:

- *პროპაგანდა და დეზინფორმაცია* - უცხოეთის სახელმწიფოების ტერიტორიებზე მმართველი რეჟიმების დესტაბილიზაციის მოწყობის, პოლიტიკური პროცესების ან კომერციული საქმიანობის შედეგებზე გავლენის მოხდენის მიზნით, არასწორი მონაცემების შეყვანა/გავრცელება ან არსებულ მონაცემებში ცვლილებების შეტანა;
- *დაშინება* - ვებ - გვერდებზე შეტევების განხორციელების მიზანია მომხმარებლის (როგორც სახელმწიფო მოხელის, ისე ფიზიკური ან იურიდიული პირის) იძულება წაშალოს ან შეცვალოს საიტის შინაარსი /პოლიტიკა;

- *განადგურება* - უცხო სახელმწიფოებისთვის ან კონკურენტებისთვის ზარალის ან მავნებლობის მიყენების მიზნით, მონაცემების მუდმივი და მიზანმიმართული განადგურება. კერძოდ, მსგავსი შეტევები შეიძლება განხორციელდეს უფრო მასშტაბური კონფლიქტის დროს არსებული სხვა მოქმედებების პარალელურად.

<u>დაშვება</u>

სისტემაზე განხორციელებული კიბერშეტევის შედეგად, სისტემის ლეგიტიმურ მომხმარებელს ექმნება ისეთი პირობები, რომ მას არ შეუძლია სისტემაში შესვლა და აღარ აქვს დაშვება სისტემის მიერ შემოთავაზებულ რესურსებზე, ან ასეთი დაშვება არის გართულებული. ქვესახეობები:

- საგარეო ინფორმაცია - განხორციელებული შეტევები, რომლის შედეგად შეუძლებელია სახელმწიფო და კერძო სექტორის სერვისებზე ღია დაშვება. კერძოდ, მასიური საინფორმაციო საშუალებებისა და სახელმწიფო თუ კერძო სტრუქტურების საინფორმაციო საიტები;
- შიდა ინფორმაცია - სახელმწიფო და კერძო სექტორის ქსელზე ლოკალური შეტევის განხორციელება. მაგალითად, ლოკალური შეტევები ენერგეტიკული და სატრანსპორტო მართვის სისტემებზე, ელექტრონული ბანკინგის საიტებზე, ოპერატიული მმართველობის სისტემებზე, კორპორატიული სერვისების ელექტრონულ ფოსტაზე, სამაშველო სამსახურებსა და ა. შ.

<u>კონფიდენციალობა</u>

კიბერშეტევების სამიზნე შეიძლება იყოს კონფიდენციალური ინფორმაციის წყაროები[46] და ის ძირითადად ხორციელდება დანაშაულის მიზნით. ქვესახეობები:

[46] კიბერშეტევის მსხვერპლნი ხშირად ხდებიან კონფიდენციალური ინფორმაციის მატარებელი სახელმწიფო მოხელეები და მსხვილი კორპორაციების მთავარი ფიგურები. კერძოდ, ხდება არამარტო

- *ჯაშუშობა* - კორპორაციების, კომპანიებისა და ფირმების მხრიდან ინფორმაციის მოპოვება თავისი კონკურენტების მიმდინარე და მომავალი საქმიანობის შესახებ. ჯაშუშურ საქმიანობაში სახელმწიფოს მონაწილეობა, რომელიც მიმართულია უცხო ქვეყნებისა და ფიზიკური თუ იურიდიული პირების წინააღმდეგ;
- *პერსონალური მონაცემების მოპარვა* - ფიშინგის ან მსგავსი ანალოგიური შეტევების განხორციელება, რომლის მიზანია მოტყუების გზით მომხმარებელი იძულებული გახადოს აცნობოს თავისი პერსონალური მონაცემები, მაგალითად საბანკო ანგარიშები. ვირუსების დაგზავნა, რომლებიც მომხმარებლის პერსონალური კომპიუტერიდან აკეთებს მონაცემთა კოპირებასა და ჩატვირთვას;
- *„პიროვნების მოპარვა“* - იგულისხმება მომხმარებლის პერსონალური რეკვიზიტების მოპარვა. ტროიანი და მსგავსი პროგრამები გამოიყენება პირადი მონაცემების მოსაპარად;
- *ინფორმაციის მოძიება საერთაშორისო ქსელში* - სხვადასხვა სახის ინფორმაციის, კერძოდ, პერსონალური მონაცემების მოპოვების მიღების მიზნით, გამოიყენება ღია წყაროებიდან ინფორმაციის მოპოვების ტექნოლოგიები;
- *მაქინაციები* - ხშირად ხორციელდება სპამის გამოყენებით, რომელიც ვრცელდება ელექტრონული ფოსტის საშუალებით. მსგავსი მაქინაციის ყველაზე ცნობილი სახეობა არის ე. წ. „ნიგერიული წერილები 419“[47]. აქვე შეიძლება განვიხილოთ მაქინაციების ის სქემები, რომლებიც

კონფიდენციალური ინფორმაციის მოპარვა, არამედ ასევე წარმოებს მსგავსი პირების პერსონალური ინფომაციის ხელყოფა, მათი მომავალში შანტაჟის მიზნით

[47] „ნიგერიული წერილები 419“ (Scam 419) - მაქინაციის გავრცელებული სახეობა, რომელიც განვითარდა ელექტრონული ფოსტის მასიური დაგზავნის გაჩენის შემდეგ. სახელწოდება მიიღო იმის გამო, რომ განსაკუთრებულად განვითარდა ნიგერიაში, სადაც ჯერ ლოკალური, ხოლო შემდეგ საერთაშორისო მასშტაბები მიიღო. აღსანიშნავია, რომ ეს არსებობდა ინტერნეტის გჩენამდე და მისი გავრცელება ხდებოდა ჩვეულებრივი საფოსტო მომსახურებით, ხოლო ახალი ტექნოლოგიებისა და ინტერნეტის გაჩენასთან ერთად „ნიგერიულმა წერილებმა 419“ მსოფლიო მასშტაბები მიიღო.

მომხმარებლებს სთავაზობს არარსებულ სერვისებსა და საქონელზე წინასწარ გადახდას.

კიბერსაფრთხეებთან მებრძოლი სუბიექტები

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

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

საერთაშორისო დონეზე კიბერსაფრთხეებთან ბრძოლის თაობაზე მიღებულია ისეთი მნიშვნელოვანი სამართლებრივი აქტები, როგორებიცაა გაეროს გენერალური ასამბლეის 2000 წლის 4 დეკემბრის №55/63[48] და 2001 წლის 19 დეკემბრის №56/121[49]

[48] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
[49] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

რეზოლუციები „დანაშაულებრივი მიზნებით ინფორმაციული ტექნოლოგიების გამოყენებასთან ბრძოლა“, 2008 წლის 1 – 2 აპრილს, სტრასბურგში მსოფლიო კონფერენციაზე “თანამშრომლობა კიბერდანაშაულის წინააღმდეგ”[50] მიღებული დოკუმენტი „კიბერდანაშაულობასთან ბრძოლის სფეროში სამართალდამცავი ორგანოებისა და ინტერნეტ - პროვაიდერების ერთობლივი მუშაობის ძირითადი პრინციპები“[51]. რეგიონალურ დონეზე უნდა აღინიშნოს ევროსაბჭოს რეკომენდაციები №R[89]9 “კომპიუტერულ დანაშაულებთან ბრძოლა”[52].

კიბერდანაშაულობასთან ბრძოლის ერთერთ ძირითად სუბიექტად მოიაზრება ქსელის მომხმარებელი. ამიტომ აუცილებელია მათი ჩართვა საგანმანათლებლო ღონისძიებებში, რომლებიც დაეხმარება მომხმარებელს უფრო კარგად გაერკვნენ ისეთ საკითხში, როგორიცაა კომპიუტერული მაქინაციები, პირადი რეკვიზიტების მოპარვა, ინტერნეტში არსებული დანაშაულებები, ინტერნეტის ეთიკა და სხვა.

ქვემოთ მოცემულია ზოგიერთი ძირითადი სუბიექტი, რომლებიც მონაწილეობენ კიბერსაფრთხეებთან ბრძოლაში, კერძოდ:

საერთაშორისო და რეგიონალური ორგანიზაციები

- აზია - წყნარი ოკეანის ეკონომიკური თანამშრომლობის სამუშაო ჯგუფი ტელეკომუნიკაციებსა და ინფორმაციებში[53];
- ქსელებისა და ინფორმაციული უსაფრთხოების ევროპული სააგენტო[54];

[50] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_IF08-d-concl1c.pdf
[51] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf
[52] http://www.oas.org/juridico/english/cyber_links_coe.htm
[53] http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx
[54] http://www.enisa.europa.eu/

- ნატო - ს კიბერნეტიკული დაცვის მოწინავე მეთოდების გაერთიანებული ცენტრი[55];
- სამხრეთ - აღმოსავლეთის ქვეყნების ასოციაცია[56];
- ეკონომიკური განვითარებისა და თანამშრომლობის ორგანიზაცია[57];
- კომპიუტერულ ქსელებში საგანგებო სიტუაციებზე ოპერატიული რეაგირების ჯგუფი[58];
- ინტერნეტის მართვის ფორუმი[59];
- ელექტროკავშირის საერთაშორისო გაერთიანება[60];
- ინტერნეტის საზოგადოება[61];
- სახელებისა და ნომრების მინიჭების ინტერნეტ - კორპორაცია[62];
- სამოქალაქო ინიციატივა ინტერნეტ - პოლიტიკა „მერიდიანი“[63];
- დიდი რვიანის ლიონის ჯგუფი, მაღალი ტექნოლოგიების სფეროში დანაშაულებების ქვეჯგუფი, გაერო, ევროსაბჭო.

არასამთავრობო ორგანიზაციები[64]

- უფლებათა დამცავი ორგანიზაციები[65];
- სხვადასხვა ფონდები[66];

[55] https://ccdcoe.org/
[56] http://www.asean.org/
[57] http://www.oecd.org/
[58] https://www.csirt.org/
[59] http://www.intgovforum.org/cms/
[60] http://www.itu.int/en/Pages/default.aspx
[61] http://www.internetsociety.org/
[62] https://www.icann.org/
[63] http://meridianprocess.org/default.aspx
[64] მოცემულია რამოდენიმე ძირითადი და აღიარებული ორგანიზაცია
[65] Human Rights Watch http://www.hrw.org/; საერთაშორისო ამნისტია http://www.amnesty.org/; Reporters Without Borders http://en.rsf.org/
[66] The World Wide Web Foundation http://webfoundation.org/; The Shadowserver Foundation https://www.shadowserver.org/wiki/pmwiki.php

- ანალიტიკური ცენტრები[67].

დარგობრივი ორგანიზაციები

- ანტიფიშინგური სამუშაო ჯგუფი[68];
- ფუნქციონალურ საკითხებში დომეინის სახელების სამსახურების კვლევითი - ანალიტიკური ცენტრი[69];
- სისტემებში შეტყობინებების გადაცემის მავნებლობასთან ბრძოლის სამუშაო ჯგუფი[70];
- ინტერნეტში უსაფრთხოების გაძლიერების დარგობრივი კონსორციუმი[71];
- ელექტრონიკისა და ელექტროტექნიკის ინჟინრების ინსტიტუტი[72];
- სატრანსპორტო ორგანიზაციები[73];
- სხვა დარგობრივი ორგანიზაციები, რომლებიც დაკავშირებულია კრიტიკული ინფრასტრუქტურის მართვასთან.

სახელმწიფო

- საგარეო და შინაგან საქმეთა სამინისტროები, ტრანსპორტის, ფინანსთა და იუსტიციის სამინისტროები, სადაზვერვო და სხვა სპეციალური სამსახურები, პოლიციის სამმართველოები/დეპარტამენტები, ოპერატიული უსაფრთხოების სამმართველოები/დეპარტამენტები, კიბერუსაფრთხოების საკითხებში სპეციალური სამმართველოები/დეპარტამენტები;
- ელექტრონულ ინციდენტებზე რეაგირების კომპიუტერული ჯგუფები (CERT)[74].

---

[67] The Center for Strategic and International Studies (CSIS) http://csis.org/; http://www.rand.org/
[68] http://www.antiphishing.org/
[69] https://www.dns-oarc.net/
[70] https://www.maawg.org/
[71] http://www.icasi.org/
[72] https://www.ieee.org/index.html
[73] მაგალითად, აეროპორტებისა და საჰაერო გადაზიდვების მართვის უსაფრთხოების უზრუნველყოფის ორგანიზაციები
[74] მაგალითად, საქართველოს იუსტიციის სამინისტროს სსიპ „მონაცემთა გაცვლის სააგენტო“ http://www.cert.gov.ge/

კერძო სექტორი

- ინტერნეტში უსაფრთხოების უზრუნველყოფის სპეციალური კომპანიები;
- პროგრამული უზრუნველყოფის შემქნელები/დეველოპერები;
- სისტემების, სერვერების, მოწყობილობების მწარმოებლები;
- ჰოსტინგ - პროვაიდერები;
- კომპანიები, რომლებიც ეწევიან საქონლით ვაჭრობას ინტერნეტში.

ფიზიკური პირები

პერსონალური კომპიუტერების მფლობელები და მომხმარებლები.

რეზუმე

წინამდებარე ნაშრომში ნაჩვენებია ის კიბერსაფრთხეები, მათი წარმოშობის წყაროები და სახეობები, რომლებიც საფრთხეს უქმნიან და ემუქრებიან ინტერნეტის სივრცეს როგორც გლობალურ, ისე ლოკალურ დონეზე, რაც სერიოზულ სირთულეებს უქმნის ეროვნულ და საერთაშორისო უსაფრთხოების პრინციპებს.

ფაქტიურად, კიბერსივრცე დღესდღეისობით არსებული მდგომარეობით ნაკლებად დაცულია, რასაც ხელს უშლის სახელმწიფო და კერძო სექტორებს შორის ნაკლები კომუნიკაცია და იმ განსვავებული მოტივაციის, ინტერესებისა და მიზნების არსებობა, რაც ახასიათებს თითოეულ სექტორს. ყოველივეს ემატება ის გარემოებაც, რომ ტექნოლოგიური განვითარების პარალელურად ვითარდება ასევე კიბერდანაშაულებები, ვინაიდან ისინი ყოველი ნოუ ჰაუს აქტიური მომხმარებლები არიან.

მოცემულ პრობლემაში დიდი მნიშვნელობა ენიჭება არამარტო საერთაშორისო თუ რეგიონალურ დონეზე მიღებულ რეზოლუციებსა და რეკომენდაციებს, ან/და კიბერსაფრთხეებთან მებრძოლ სუბიექტებს, არამედ ასევე პიროვნების ფაქტორს როგორც ქსელისა და პერსონალური კომპიუტერული მოწყობილობის მომხმარებელს, რომლისთვისაც მოცემულ სფეროში ცნობადობის ამაღლება, საგანმანათლებლო პროგრამების მიწოდება და ინტერნეტის ეთიკის ნორმების გამომუშავებაში ხელშეწყობა

აუცილებელი პირობაა ყოველი ხელისუფლებისთვის და საერთაშორისო ორგანიზაციებისთვის, რაც მაქსიმალურად შეამცირებს რისკებს როგორც გლობალურ, ისე ლოკალურ ინტერნეტ სივრცეში.

გამოყენებული ლიტერატურა

1) Democratic Governance Challenges of Cyber Security, Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, DCAF 2010, DCAF Horizon 2015 Working Paper Series http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf; http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security;

2) United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009) http://www.nsi.org/pdf/reports/Information%20Security%20-%20Cyber%20Threats.pdf

დეკემბერი, 2014 წელი

კიბერუსაფრთხოების სფეროში არსებული ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურების მოკლე აღწერა. საქართველოში არსებული სუბიექტები

შესავალი

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

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

ნაშრომში განხილულია ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურები დაკავშირებული კიბერუსაფრთხოებასთან და ის საერთო პრინციპები, რომლებიც გააჩნიათ და ახასიათებთ სხვადასხვა ქვეყნების სახელმწიფო თუ კერძო სუბიექტებს მოცემულ სფეროში. აქვე წარმოდგენილია საქართველოში არსებული ის სუბიექტები, რომლებიც პასუხისმგებელნი არიან კომპიუტერული ქსელებისა და კიბერსივრცის, ასევე პერსონალური მონაცემების დაცვაზე და ებრძვის კიბერდანაშაულს როგორც ლოკალურ ისე საერთაშორისო დონეზე.

ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურების მოკლე მიმოხილვა

ქვემოთ მოცემული მასალა ქმნის გარკვეულ წარმოდგენას კიბერუსაფრთხოების სფეროში არსებული სახელმწიფო სუბიექტების შესახებ. კერძოდ, აქ მოკლედ არის განხილულია ევროკავშირის ზოგიერთი წევრი ქვეყნისა და სხვა ქვეყნების იმ სახელმწიფო სუბიექტების ორგანიზაციული სტრუქტურა, ფუნქციები და უწყებრივი დაქვემდებარებულობა, რომლებიც პასუხისმგებელნი არიან თავიანთ ქვეყნებში უზრუნველყონ კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვა და კიბერუსაფრთხოება, გაატარონ ყველა ის საჭირო ღონისძიებები, რომლებიც საშუალებას იძლევა მაქსიმალურად იყოს დაცული ინტერნეტის სივრცე, მონაცემთა ბაზები და მოქლაქეთა პერსონალური ინფორმაცია, ასევე ეფექტურად აწარმოონ ბრძოლა კიბერდანაშაულის წინააღმდეგ. კერძოდ, განხილულ ქვეყნებს განეკუთვნება:

- **ესტონეთი** - კიბერუსაფრთხოების სტრატეგია გამოქვეყნდა 2008 წელს. მოცემულ დოკუმენტში[75] აღწერილია სახელმწიფოში კიბერუსაფრთხოების სფეროში არსებული ვითარება და განსაზღვრავს ეროვნულ პოლიტიკას მოცემული მიმართულებით. ქვეყანაში არ არსებობს ერთიანი სახელმწიფო ორგანო, რომელიც პასუხისმგებელი იქნებოდა კიბერსივრცის დაცვის უზრუნველყოფაზე. ამ პროცესში უშუალოდ მონაწილეობს რამდენიმე სამინისტრო და მათი ქვედანაყოფი. ინფორმაციული უსაფრთხოების

[75] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

უზრუნველყოფაში მთავარი როლი ეკუთვნის ეკონომიკისა და კავშირგაბმულობის სამინისტროს (MEAC)[76]. სამინისტროს დაქვემდებარებაში არის ცენტრალური აღმასრულებელი ხელისუფლების ორი ორგანო, რომლებიც ახდენენ კიბერუსაფრთხოების სახელმწიფო პოლიტიკის რეალიზაციას. ეს ორგანოებია: ინფორმაციული სისტემების სახელმწიფო დეპარტამენტი (RISO)[77], რომელიც არის მთავარი მაკოორდინირებელი ორგანიზაცია ინფორმაციისა და საკომუნიკაციო ტექნოლოგიების სფეროში (ICT)[78], და ესტონეთის ინფორმატიკის ცენტრი (RIA)[79], რომელიც პასუხისმგებელია მთლიანი ქსელის უსაფრთხოების უზრუნველყოფაზე, კრიტიკული ინფორმაციული ინფრასტრუქტურის სახელმწიფო სუბიექტების ტექნიკურ უსაფრთხოებაზე, ასევე სახელმწიფო ორგანიზაციების ინტერესებიდან გამომდინარე მონაცემთა გადაცემის სისტემის დამუშავება და მართვა. მოცემული ცენტრის შემადგენლობაში ფუნქციონირებს ესტონეთის საგანგებო სიტუაციებზე რეაგირების ოპერატიული ჯგუფი (CERT)[80]. უშუალოდ კრიტიკული ინფრასტრუქტურის დაცვასა (CIIP) და კიბერუსაფრთხოებას უზრუნველყოფს შინაგან საქმეთა და თავდაცვის სამინისტროების სპეციალური სტრუქტურული ერთეულები. ორივე სამინისტრო პასუხისმგებელია ქვეყნის შიდა უსაფრთხოებასა და კრიზისების მართვაზე. საფოსტო და საბაზრო ელექტრონული კავშირის მომსახურების სფეროს კოორდინირებას უწევს კავშირგაბმულობის ეროვნული საბჭო. სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობისთვის შეიქმნა პროექტი „კომპიუტერული უსაფრთხოება 2009“, რომელიც მიმართულია ინფორმაციული უსაფრთხოების გაძლიერებისკენ;

[76] https://www.mkm.ee/en
[77] http://www.riso.ee/en/
[78] Information and Communication Technology
[79] https://www.ria.ee/en/
[80] https://www.ria.ee/cert-estonia

- **დიდი ბრიტანეთი** - 2009 წელს[81] მიღებული კიბერუსაფრთხოების სტრატეგია ხაზს უსვამს კიბერუსაფრთხოების უზრუნველყოფის საკითხთან კომპლექსური მიდგომის აუცილებლობას, რომლის რეალიზაციაში უნდა მონაწილეობდნენ სახელმწიფო სუბიექტები, მრეწველობის ყველა დარგის წარმომადგენლები, სამოქალაქო საზოგადოებრივი ორგანიზაციები და საერთაშორისო პარტნიორები. სტრატეგია ითვალისწინებს ორი ახალი ორგანიზაციის შექმნას[82]. პირველ რიგში ეს არის მინისტრთა კაბინეტის სტრუქტურაში შემავალი კიბერუსაფრთხოების სამმართველო (OCS)[83], რომელიც უზრუნველყოფს სტრატეგიულ ხელმძღვანელობასა და უწყებათაშორის დონეზე შეთანხმებულ მოქმედებას. ის იქნება ასევე დაკავებული კიბერდანაშაულის შესახებ საკოორდინაციო საქმიანობით. ამასთან ერთად გამოყენებული იქნება არსებული შესაძლებლობები, რომელიც გააჩნია თავდაცვის სამინისტროს, სადაზვერვო სამსახურებს და პოლიციას (ლონდონის პოლიციის ელექტრონულ დანაშაულებებთან ბრძოლის განყოფილება, ინტერნეტის ქსელის დაცვისა და ბავშვთა ექსპლუატაციის წინააღმდეგ ქმედებების ცენტრი, ასევე განსაკუთრებით საშიში და ორგანიზებული დანაშაულის სააგენტო). მეორე, ეს არის კიბერუსაფრთხოების ოპერატიული ცენტრი (CSOC), რომელიც ფუნქციონირებს სახელმწიფო კავშირგაბმულობის შტაბის[84] ბაზაზე ქ. ჩელტენჰემში. ეს არის ახალი ცენტრი, სადაც თავმოყრილია სხვადასხვა უწყებების არსებული ფუნქციები კიბერსივრცის მდგომარეობის მონიტორინგისა და ღონისძიებების კოორდინაცია ექსტრემალურ რეაგირებაზე. ცენტრი ასევე გააკეთებს ანალიზს იმ საფრთხეებზე, რომელიც ემუქრება დიდი ბრიტანეთის კომპიუტერულ ქსელებსა და მათ მომხმარებლებს, გამოიმუშავებს შესაბამის

[81] 2011 წელს მოხდა სტრატეგიის განახლება https://www.cpni.gov.uk/advice/cyber/cir/
[82] ორივე ორგანიზაციამ დაიწყო ფუნქციონირება 2010 წელს
[83] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
[84] http://www.gchq.gov.uk/Pages/homepage.aspx

რეკომენდაციებსა და საინფორმაციო სახელმძღვანელოებს. ეროვნული ინფრასტრუქტურის დაცვის ცენტრის (CPNI)[85] შემადგენლობაშია კომპიუტერების დახმარების სასწრაფო სამსახური (CERT Service)[86];

- **შვედეთი** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებში მონაწილეობას იღებს ბევრი ორგანიზაცია. 2009 წელს შვედეთის თავდაცვის სამინისტროსთან არსებულ სამოქალაქო თავდაცვის სააგენტოს (MSB)[87] დაევალა 2010 წლის იანვრამდე წინადადებების მომზადება კომპიუტერულ ქსელებში დანაშაულებების აღკვეთის თაობაზე. გადაწყდა სააგენტოს შემადგენლობაში შექმნილიყო კიბერუსაფრთხოების ეროვნული ოპერატიული საკოორდინაციო ცენტრი, რომელიც უწყებათაშორის დონეზე, გაუწევდა კოორდინაციას ერთობლივ ღონისძიებებს და შეასრულებდა ცენტრალური ელემენტის როლს კრიზისული მენეჯმენტის სისტემაში. ამ პროცესში მთავარი როლი ეკუთვნის ასევე თავდაცვის სამინისტროსთან არსებულ საგანგებო სიტუაციების სააგენტოს (SEMA)[88]. გარდა ამისა, სამოქალაქო თავდაცვის სააგენტოს (MSB) ხელმძღვანელობით, არსებობს ინფორმაციული უსაფრთხოების სფეროში ერთობლივი ოპერაციების ჯგუფი (SAMFI)[89],

[85] http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx
[86] https://www.cpni.gov.uk/advice/cyber/cir/
[87] https://www.msb.se/en/
[88] The Swedish Emergency Management Agency (SEMA) co-ordinates the work to develop the preparedness of Swedish society to manage serious crises. SEMA works together with municipalities, county councils and government authorities, as well as the business community and several organizations, to reduce the vulnerability of society and improve the capacity to handle emergencies. The Swedish Emergency Management Agency (SEMA) supports the bodies responsible for emergency management, especially county administrative boards and municipalities, which have a special role with overall geographic area responsibility. SEMA should be able to give support to other public actors, i.e. municipalities, county councils and government authorities. SEMA does not have an operative role and does not take over any responsibility from other authorities. The support that SEMA is able to provide in the event of a crisis may include advice and expert support within areas such as crisis communication and management methodoligy. SEMA should also assist the Government Offices with updated situation reports. To carry out this task, the authority has an established network of county administrative boards, central authorities and others that may be affected by or have knowledge of an emergency situation. SEMA also co-ordinates the planning, resource allocation, follow-up and evaluation of work within the area of crisis management. Furthermore, SEMA collects knowledge through horizon scanning, strategic analyses and research to develope sociaty's emergency management.
[89] http://rib.msb.se/Filer/pdf/26177.pdf

სადაც შედიან შვედეთის შეიარაღებული ძალების, რადიოტექნიკური თავდაცვის ეროვნული სამსახური (FRA)[90], ფოსტისა და ტელეკომუნიკაციის ეროვნული სააგენტო (PTS)[91] და პოლიციის ეროვნული დეპარტამენტის წარმომადგენლები. უწყებათაშორისო თანამშრომლობის ფარგლებში, მინისტრთა კაბინეტის დონეზე ტარდება სპეციალური სამუშაოები მიმართული საგანგებო სიტუაციების სააგენტოს (SEMA) რეკომენდაციებსა და კრიტიკული ინფორმაციული ინფრასტრუქტურის ეროვნული სისტემის მოდერნიზირებაზე. რაც შეეხება სახელმწიფოსა და კერძო სექტორის პარტნიორულ დონეზე თანამშრომლობას, აქ ხორციელდება საგანგებო სიტუაციების სააგენტოს (SEMA) მიერ მომზადებული ისეთი ინიციატივები და პროექტები, როგორებიცაა მოცემულ სფეროში სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის გაღრმავების, „სამრეწველო უსაფრთხოების დელეგაციისა“ (NSD) და „ინფორმაციის დამუშავების საზოგადოების“ (DFS) პროექტები;

- **ფინეთი** - აქ კიბერუსაფრთხოება განიხილება, როგორც მონაცემთა უსაფრთხოების პრობლემა, აგრეთვე როგორც ეკონომიკური პირობა, რომელიც მჭიდროდ არის დაკავშირებული ქვეყნის ინფორმაციული საზოგადოების განვითარებასთან. კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საკითხებით დაკავებულია შემდეგი სამი სახელმწიფო ორგანო: ტრანსპორტისა და კავშირგაბმულობის სამინისტროს შემადგენლობაში არსებული კავშირგაბმულობის რეგულირების სამსახური (FICORA)[92], რომელიც ხელს უწყობს ინფორმაციული საზოგადოების განვითარებას და ეწევა ტექნიკური საკითხებისა და სტანდარტიზაციის რეგულირებას; მეორე, საგანგებო სიტუაციების ეროვნული სააგენტო (NESA)[93] , ეწევა კრიტიკული ინფორმაციული ინფრასტრუქტურის

[90] http://www.fra.se/snabblankar/english.10.html
[91] http://www.pts.se/en-GB/
[92] https://www.viestintavirasto.fi/en/
[93] http://www.nesa.fi/

საფრთხეებისა და რისკების შეფასებასა და ანალიზს; და მესამე, სახელმწიფო ადმინისტრაციასთან არსებული მონაცემთა უსაფრთხოების მთავარი სამმართველო (VAHTI)[94], რომელიც ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით ამუშავებს პრინციპებისა და პრაქტიკულების სახელმძღვანელოებს. გარდა ამისა, მოცემულ სფეროში სახელმწიფოსა და კერძო სექტორს შორის პარტნიორული ურთიერთობის მიზნით შექმნილია შემდეგი სამი ორგანიზაცია საგანგებო სიტუაციების ეროვნული საბჭო (NESC), ინფორმაციული საზოგადოების საკითხთა საკონსულტაციო საბჭო და ფინეთის ინფორმაციული საზოგადოების განვითარების ცენტრი (TIEKE)[95];

- **ნიდერლანდები** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და კიბერუსაფრთხოების უზრუნველყოფის მაკოორდინირებელ ორგანოს წარმოადგენს შინაგან საქმეთა და სამეფო საქმეთა სამინისტრო. გარდა ამისა, ამ სამინისტროში არსებული კრიზისების ეროვნული ცენტრი კურირებს სხვა უწყებების საქმიანობას, ასევე საერთაშორისო პოლიტიკასა

[94] The Government Information and Cyber Security Management Board (VAHTI), appointed by the Ministry, is responsible for Government cooperation, steering and development efforts in this area. VAHTI sets all the main policy guidelines for information and cyber security in central government. Different administrative branches and levels of administration are represented in VAHTI.
A Government Resolution on the development of information security in central government was issued on 26 November 2009. The Resolution provides guidance to central government in developing information security as an integral part of leadership, expertise, risk management and administrative development and functions. VAHTI's effective cooperation, steering and development of information security in central government will be reinforced. The present Government has discussed the earlier government resolutions and made a decision that this resolution is to be kept in force.
VAHTI guidelines and instructions are also important reference materials for the public authorities, local government, the private sector and civil society. In addition, the results of the work are used in such international information security forums as the OECD and the EU. VAHTI publications are considered to be of high quality in international comparison.
The role and tasks of VAHTI in the development, coordination, cooperation and steering of government information and cyber security have been further developed and strengthened. VAHTI deals with all significant central government information and cyber security guidance and policy matters.
VAHTI has received several awards for improving information security in Finland. The latest OECD report on the development of the global information security culture makes several references to the operations and results of VAHTI.

[95] http://www.tieke.fi/display/English/Home

და კრიზისების მართვას.ინფორმაციული უსაფრთხოების დაცვით ღონისძიებებში ასევე მონაწილეობს საერთო დაზვერვისა და უსაფრთხოების სამსახური (AIVD)[96];

- **გერმანია** - კრიტიკული ინფრასტრუქტურის უსაფრთხოების ეროვნული სტრატეგია განსაზღვრავს მთავრობის მიზნებსა და ამოცანებს მოცემულ სფეროში, რომელიც თავის მხრივ ასახულია ინფორმაციული ინფრასტრუქტურის უსაფრთხოების სახელმწიფო პროგრამაში (NPSI). კიბერუსაფრთხოების საკითხებში მთავარი როლი ეკუთვნის შინაგან საქმეთა სამინისტროსთან არსებულ ინფორმაციული უსაფრთხოების ფედერალურ სააგენტოს (BSI), რომელიც სამოქალაქო თავდაცვისა და საგანგებო სიტუაციების ფედერალურ სააგენტოსთან (BBK), კრიმინალური პოლიციის ფედერალურ სააგენტოსთან (BKA), ფედერალურ პოლიციასთან (BPOL) და ფედერალური ინსტიტუტების ტექნიკური მხარდაჭერის სამსახურთან ერთად ახორციელებს შეფასებასა და ანალიზს, ასევე ფორმულირებას უკეთებს კიბერსივრცის დაცვის კონცეფციას. კრიტიკული ინფრასტრუქტურის დაცვის მიზნით და ამ მიმართულებით კოორდინირებული მოქმედებისთვის შექმნილი არის სამუშაო ჯგუფი (AG KRITIS)[97]. სტრატეგიის შემუშავებისა და მისი შემდგომი რეალიზების საქმიანობა მიმდინარეობს კოორდინირებულად სხვა ფედერალურ სამინისტროებთან, სააგენტოებთან და სამსახურებთან ერთად (ეკონომიკისა და ტექნოლოგიის სამინისტრო, ფედერალური კანცლერის ადმინისტრაცია, იუსტიციის, საგარეო საქმეთა და თავდაცვის ფედერალური სამინისტროები, ელექტრონული ქსელების ფედერალური სააგენტო). გარდა ამისა, წარმოებს კონსულტაციები კერძო სექტორის სტრატეგიულ პარტნიორებთან;

[96] https://www.aivd.nl/english/
[97] file:///C:/Users/Admin/Downloads/doc_263_259_en.pdf

- **საფრანგეთი** - კრიტიკული ინფრასტრუქტურის დაცვაზე მთელი პასუხისმგებლობა ეკისრება პრემიერ - მინისტრის ადმინისტრაციასთან არსებულ ეროვნული თავდაცვის გენერალურ სამდივნოს (SGDN). ქვეყანაში კიბერუსაფრთხოება ამავდროულად განიხილება როგორც მაღალტექნოლოგიური დანაშაულის საკითხი და როგორც პრობლემა, რომელიც ხელს უშლის და ეწინააღმდეგება ინფორმაციული საზოგადოების ნორმალურ განვითარებას. მოცემულ სფეროში დანაშაულის გამოძიებაზე პასუხისმგებელი ორგანოებია 2000 წლის მაისში შექმნილი ინფორმაციისა და საკომუნიკაციო ტექნოლოგიების სფეროში დანაშაულთან ბრძოლის ცენტრალური ოფისი (OCLCTIC) და სასამართლო პოლიციის მთავარი სამმართველოს ეკონომიკური და ფინანსური საგამოძიებო განყოფილება. 2009 წლის ივლისის თვეში, თავდაცვის სამინისტროში შეიქმნა ინფორმაციული სისტემების უსაფრთხოების ეროვნული სააგენტო (Anssi)[98], რომელიც პასუხისმგებელია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და კიბერუსაფრთხოების უზრუნველყოფაზე. გარდა ამისა, ასევე ფუნქციონირებს ინფორმაციული სისტემების უსაფრთხოების უწყებათაშორისი კომისია (CISSY). სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობის ფარგლებში შექმნილია ინფორმაციული ტექნოლოგიების სტრატეგიული საკონსულტაციო საბჭო (CSTI), რომელიც აერთიანებს სახელმწიფო ჩინოვნიკებს, ბიზნესისა და საწარმოთა მაღალი მმართველი რგოლისა და სამეცნიერო წრეების წარმომადგენლებს;
- **ნორვეგია** - სამოქალაქო თავდაცვისა და კრიზისების მართვის სამმართველო (DSB) არის მთავარი მაკოორდინირებელი ორგანიზაცია, რომელიც პასუხისმგებელია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვითი საქმიანობის უზრუნველყოფაზე. სამმართველო იმყოფება იუსტიციისა და პოლიციის სამინისტროს

[98] http://www.ssi.gouv.fr/en/

დაქვემდებარებაში. ინფორმაციისა და ქსელების კავშირის უსაფრთხოება თავმოყრილია სახელმწიფო მართვისა და რეფორმების სამინისტროში. თავდაცვის სამინისტრო პასუხიმგებელია მხოლოდ სამხედრო კომპიუტერულ ქსელზე. ტრანსპორტისა და კავშირგაბმულობის სამინისტრო პასუხს აგებს კავშირგაბმულობის სექტორზე, ასევე ინფორმაციული ქსელების უსაფრთხოების ასპექტებზე. ნორვეგიის ეროვნული უსაფრთხოების სამსახური (NSA) კოორდინირებას უწევს კომპიუტერული ქსელების უსაფრთხოების უზრუნველყოფის ღონისძიებებს. ინფორმაციული უსაფრთხოების საკითხთა სახელმწიფო საკოორდინაციო საბჭო (KIS) უფლებამოსილი არ არის მიიღოს გადაწყვეტილებები, თუმცა ის უწევს კონსულტაციებს სამინისტროებსა და უწყებებს იმ საკითხებში, რომლებიც დაკავშირებულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვასა და კიბერუსაფრთხოებასთან. მის შემადგენლობაში შედის ექვსი სამინისტრო, პრემიერ - მინისტრის აპარატი და ათამდე სხვადასხვა სამმართველო;

- **ავსტრია** - ქვეყანაში არ არსებობს ერთიანი მაკოორდინირებელი ორგანო, რომელიც პასუხისმგებელი იქნება კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებზე. ყოველი სამინისტრო და უწყება თავად ახორციელებს საკუთარი უსაფრთხოების ღონისძიებებს მიმართულს საგარეო კიბერშეტევებსა მონაცემთა არასანქცირებული გამოყენების გაუვნებელყოფაზე. კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას ახორციელებს შინაგან საქმეთა სამინისტროს (BMI)[99] ზოგიერთი ქვედანაყოფი, კერძოდ, აწარმოებს მონავემთა უსაფრთხოების უზრუნველყოფასა და ბრძოლას კიბერდანაშაულებასთან. კრიმინალური პოლიციის ფედერალური სამმართველოს საზოგადოებრივი უსაფრთხოების მთავარ სამმართველოსთან ფუნქციონირებს ბავშვთა

[99] http://www.bmi.gv.at/cms/bmi/_news/bmi.aspx

პორნოგრაფიის გავრცელების საწინააღმდეგო საინფორმაციო ცენტრი. სახელმწიფო დაცვისა და ტერორიზმთან ბრძოლის ფედერალური სააგენტო (BVT)[100] პასუხს აგებს პიროვნებისა და ობიექტების უსაფრთხოების საკითხებზე. თავდაცვის სამინისტროს მეორე სამმართველო აწარმოებს თავის საქმიანობას ინფორმაციული ომის ყველა მიმართულებით და ამასთანავე მჭიდროდ თანამშრომლობს სპეციალურ სამსახურებთან. ერთერთი არის Abwehramt[101], რომელსაც გააჩნია ელექტრონული თავდაცვის სპეციალური დეპარტამენტი. ტრანსპორტის, ინოვაციებისა და ტექნოლოგიების სამინისტრო (BMVIT)[102] პასუხისმგებელია სახელმწიფო ინფორმაციული ინფრასტრუქტურის უსაფრთხოებაზე. იგივე სამინისტრო უწევს კოორდინაციას უსაფრთხოების სფეროში სამეცნიერო კვლევებისა და განვითარების ეროვნულ პროგრამებს. კიბერუსაფრთხოების სფეროში არსებული სახელმწიფო პროგრამების[103] გათვალისწინებით, ავსტრიაში კიბერუსაფრთხოება ძირითადად განიხილება მონაცემთა დაცვის ფარგლებში;

- **პოლონეთი** - კრიტიკული ინფორმაციული ინფრასტრუქტურასა და მის უსაფრთხოებაზე პასუხისმგებელია სახელმწიფო ორი უწყება. კერძოდ, მეცნიერებისა და უმაღლესი განათლებისა და შინაგან საქმეთა და ადმინისტრაციის სამინისტროები. მთავარი სუბიექტი და ერთადერთი მაკოორდინირებელი ორგანო, რომელიც მონაწილეობს სამეცნიერო - ტექნიკური სახელმწიფო პოლიტიკის ყველა სტრატეგიის შემუშავებასა და

[100] The Federal Office for the Protection of the Constitution and Counterterrorism (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, "BVT") is an Austrian police organization that acts as a domestic intelligence agency. It is tasked with the protection of constitutional organs of the Republic of Austria and their ability to function. The agency was created from the Austrian State police, as well as various special task forces targeting organized crime and terrorism that were under the direction of the Directorate General for Public Security (Generaldirektion für die öffentliche Sicherheit, "GDföS"), which itself is a department of the Federal Ministry of the Interior. The BVT publishes the Verfassungsschutzbericht, an annual report on the status of the protection of the constitution

[101] ავსტრიის საგარეო დაზვერვა

[102] http://www.bmvit.gv.at/en/

[103] ელექტრონული მთავრობის პროგრამა, ინფორმაციული უსაფრთხოების სახელმწიფო პროგრამა, მოქალაქის ელექტრონული ინტელექტუალური ბარათის შექმნის საპილოტე პროგრამა

განსაზღვრაში დაკავშირებული კრიტიკული ინფორმაციული ინფრასტრუქტურისა და მისი უსაფრთხოების უზრუნველყოფასთან, არის მეცნიერებისა და უმაღლესი განათლების სამინისტრო. ეს სამინისტრო ამუშავებს სტრატეგიულ რეკომენდაციებს ყველა დანარჩენი სამინისტროსა და უწყებებისთვის, ასევე უზრუნველყოფს სახელმწიფო კომპიუტერული ქსელების თავსებადობას. შინაგან საქმეთა და ადმინისტრაციის სამინისტრო პასუხს აგებს სახელმწიფო კომპიუტერულ ინფრასტრუქტურაზე, სახელმწიფო სატელეკომუნიკაციო და ინფორმაციული ქსელების მართვის სისტემებზე;

- **შვეიცარია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით დაკავებულია რამოდენიმე ორგანიზაცია. ამ სფეროში ერთერთი მთავარი ორგანიზაცია არის ინფორმაციული ტექნოლოგიების ფედერალური სტრატეგიული ქვედანაყოფი (FSUIT)[104]. მოცემული ორგანიზაცია არის ფინანსთა ფედერალური დეპარტამენტის სტრუქტურულ შემადგენლობაში და ის ამუშავებს ინფორმაციულ უსაფრთხოებაში ინსტრუქციებს, მეთოდოლოგიასა და პროცედურებს, ასევე კურირებას უწევს ინფორმაციული უზრუნველყოფის სპეციალურ სამუშაო ჯგუფს (SONIA) და ინფორმაციული უსაფრთხოების საკითხთა საინფორმაციო - ანალიტიკურ ცენტრს (MELANI)[105], რომელიც ახორციელებს კიბერდანაშაულთან ბრძოლის საკოორდინაციო ჯგუფის საქმიანობას (KOBIK)[106]. ორივე ეს ქვედანაყოფი იმყოფება პოლიციის ფედერალური სამმართველოს (FEDPOL)[107] უწყებრივ დაქვემდებარებაში. ინფორმაციული ტექნოლოგიების, ქსელებისა და ტელეკომუნიკაციების ფედერალური სამმარტველო (FOITT)[108] ასევე წარმოადგენს ფინანსთა ფედერალური

[104] http://www.isb.admin.ch/index.html?lang=en
[105] http://www.melani.admin.ch/?lang=en
[106] https://www.cybercrime.admin.ch/kobik/en/home.html
[107] https://www.fedpol.admin.ch/fedpol/en/home.html
[108] http://www.bit.admin.ch/index.html?lang=en

დეპარტამენტის სტრუქტურულ ქვედანაყოფს და პასუხისმგებელია ოპერატიულ დონეზე ინფორმაციული ტექნოლოგიების ფედერალური სისტემების უსაფრთხოებასა და ექსტრემალურ მზადყოფნაზე. ინფორმაციული უსაფრთხოების სფეროში ასევე მოქმედებს ეკონომიკური რესურსების ფედერალური უწყების შემადგენლობაში არსებული ინფორმაციული და სატელეკომუნიკაციო ინფრასტრუქტურის სამმართველო, სამოქალაქო თავდაცვის ფედერალური სამმართველო (FOCP)[109] და ინფორმაციულ ქსელებში საგანგებო სიტუაციებზე რეაგირების სახელმწიფო ჯგუფი. სამხედრო კომპიუტერული ქსელების უსაფრთხოებაზე პასუხისმგებელია შეიარაღებული ძალების სამეთაურო მხარდაჭერის სამსახური (FUB)[110]. შვეიცარიის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პოლიტიკის რეალიზებაში დიდ როლს თამაშობს სახელმწიფო და კერძო სექტორს შორის არსებული საპარტნიორო ურთიერთობა;

- **რუსეთი** - ინფორმაციული უსაფრთხოების სფეროში მთავარ ორგანიზაციებად ითვლება უშიშროების საბჭო, უშიშროების ფედერალური სამსახური (ФСБ), დაცვის ფედერალური სამსახური, ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური და ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტრო. თითოეულ ორგანიზაციულ უწყებას გააჩნია თავისი კომპეტენციის ფარგლები და დაკისრებული პასუხისმგებლობა. კერძოდ, უშიშროების საბჭო განსაზღვრავს ინფორმაციულ სფეროში რუსეთის ეროვნულ ინტერესებს, ობიექტებს, სუბიექტებსა და სხვა რესურსებს, რომლებიც უნდა იყოს დაცული, ასევე კოორდინირებას უწევს ინფორმაციული უსაფრთხოების სტრატეგიის დამუშავებას. უშიშროების ფედერალური სამსახური (ФСБ)[111]

[109] http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/das_babs.html
[110] http://www.vtg.admin.ch/internet/vtg/en/home/schweizerarmee/organisation/fub.html
[111] http://www.fsb.ru/

პასუხისმგებელია რუსეთის ფედერაციის უსაფრთხოებასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის უზრუნველყოფაზე. კონტრდაზვერვის სამსახური[112] ფუნქციონირებს კომპიუტერული და ინფორმაციული უსაფრთხოების სამმართველო. იგივე უშიშროების ფედერალური სამსახური (ФСБ) აწარმოებს ინფორმაციული უსაფრთხოების სფეროში სახელმწიფოს სამეცნიერო - ტექნიკური პოლიტიკის დაგეგმვასა და რეალიზებას, უზრუნველყოფს კომპიუტერული ქსელების კრიპტოგრაფიულ და საინჟინრო - ტექნიკურ დაცვას, იცავს სახელმწიფო საიდუმლოებასა და კავშირგაბმულობის ყველა სახეობას. დაცვის ფედერალური სამსახურის შემადგენლობაშია ინფორმაციისა და სპეციალური კავშირების სამსახური, რომელმაც 2003 წლის შემდეგ აიღო იმ ფუნქციების დიდი ნაწილი, რომელიც ადრე შედიოდა ინფორმაციისა და სამთავრობო კავშირების ფედერალური სააგენტოს (ФАПСИ)[113] კომპეტენციაში. ФАПСИ - ს დანარჩენი ფუნქციები გადანაწილდა შეიარაღებული ძალების გენერალური შტაბის, უშიშროების ფედერალური სამსახურისა (ФСБ) და დაცვის სამსახურს შორის. ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური იმყოფება თავდაცვის სამინისტროს დაქვემდებარებაში. მოცემული სამსახურის კომპეტენციის ფარგლებში შედის უცხოეთის სახელმწიფოების ტექნიკურ ჯაშუშობასთან ბრძოლა, საიდუმლო ინფორმაციის დაცვა და კომპიუტერული ქსელებისა და სისტემების უსაფრთხოების უზრუნველყოფა. ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტრო რეალიზებას უკეთებს სახელმწიფო პოლიტიკასა და ახორციელებს ზედამხედველობას კავშირგაბმულობის სექტორში;

[112] სტრუქტურულად შედის უშიშროების ფედერალურ სამსახურში (ФСБ)
[113] http://www.agentura.ru/dossier/russia/fso/specvyaz/

- **კანადა** - კომპიუტერულ ქსელებში საგანგებო სიტუაციებზე ოპერატიული რეაგირების ცენტრი (CCIRC)[114] ახორციელებს მონიტორინგსა და კონსულტირებას დაკავშირებულს კიბერსაფრთხეებისგან დაცვით საკითხებს, ასევე სახელმწიფო დონეზე კოორდინირებას უწევს ნებისმიერი საგანგებო სიტუაციებზე რეაგირების ოპერატიულ ღონისძიებებს, რომლებიც პირველ რიგში უკავშირდება კრიტიკული ინფორმაციული ინფრასტრუქტურის სახელმწიფო ობიექტებს. მოცემულ ღონისძიებებში ჩართული არის სხვადასხვა სახელმწიფო უწყება, მათ შორისაა კანადის ცხენოსანთა სამეფო პოლიცია, კავშირგაბმულობის უსაფრთხოების სააგენტო და უშიშროებისა და დაზვერვის სამსახური. 2010 წელს სახელმწიფომ ბოლო ათი წლის განმავლობაში მესამედ მიიღო კიბერუსაფრთხოების ეროვნული სტრატეგია;
- **ავსტრალია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვითი საკითხებით დაკავებულია კიბერუსაფრთხოების ოპერატიული მართვის ცენტრი, რომელიც შეიქმნა 2009 წელს კიბერუსაფრთხოების სახელმწიფო სტრატეგიის ფარგლებში და შედის თავდაცვის სამინისტროს კავშირგაბმულობის სამმართველოს შემადგენლობაში (DCD). ცენტრის საშტატო განაკვეთი დაკომპლექტებულია შეიარაღებული ძალების, სამხედრო დაზვერვის სამსახურის, ფედერალური პოლიციის, უშიშროებისა და დაზვერვის სამსახურების სპეციალისტებით. ცენტრი მთავრობას უწევს კონსულტაციას დაკავშირებულს კიბერსაფრთხეებისგან ქვეყნის დაცვაზე, ასევე ცოდნის, გამოცდილებისა და სადაზვერვო მონაცემების ინტეგრაციის გზით, უზრუნველყოფს კოორდინირებულ საქმიანობას. თუმცა ცენტრის საქმიანობა და მასთან დაკავშირებული საკითხები მთლიანობაში გასაიდუმლოებულია;

[114] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

- **იაპონია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და ინფორმაციული უსაფრთხოების უზრუნველყოფის სფეროში მთავარ მოქმედ პირს წარმოადგენს მინისტრთა კაბინეტის სამდივნო. მის სტრუქტურულ შემადგენლობაში ფუნქციონირებს ინფორმაციული ტექნოლოგიების განვითარების სტრატეგიის საბჭო, სადაც შედის 20 ავტორიტეტული ექსპერტი. 2005 წელს მინისტრთა კაბინეტის სამდივნოს სტრუქტურაში შეიქმნა ინფორმაციული უსაფრთხოების პოლიტიკის საბჭო (ISPC) და ინფორმაციული უსაფრთხოების ეროვნული ცენტრი (NISC), რომლებსაც დღეს უკავიათ წამყვანი ადგილი ეროვნული პოლიტიკის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში. ინფორმაციული უსაფრთხოების პოლიტიკის საბჭო (ISPC) წარმოადგენს მთავარ სახელმწიფო ორგანოს უსაფრთხოების პოლიტიკისა და სტრატეგიის მოდერნიზაციისა და დამუშავების საკითხებში. საბჭოს ხელმძღვანელობს მინისტრთა კაბინეტის სამდივნოს უფროსი და ის შედის ინფორმაციული ტექნოლოგიების სტრატეგიულ შტაბში, სადაც ასევე შედიან სხვადასხვა სამინისტროებისა და კერძო სექტორის წარმომადგენლები. ინფორმაციული უსაფრთხოების ეროვნული ცენტრი (NISC) წარმოადგენს ინფორმაციული ტექნოლოგიების უსაფრთხოების საკითხებში აღმასრულებელი ხელისუფლების ცენტრალურ ორგანოს. მინისტრთა კაბინეტის სამდივნო მოქმედებს ეკონომიკის, ვაჭრობისა და მრეწველობის სამინისტროს (METI)[115], ეროვნული პოლიციის სააგენტოს (NPA)[116] და შინაგან საქმეთა და კომუნიკაციების სამინისტროს მხარდაჭერით. ინფორმაციული ტექნოლოგიების სტრატეგიული შტაბის ხელმძღვანელობით, METI ახორციელებს ინფორმაციული პოლიტიკის დაგეგმვასა და რეალიზებას, ასევე დაკავებულია ელექტრონული ვაჭრობის საკითხებით, მონაცემთა დაცვით, ინფორმაციული ტექნოლოგიების

[115] http://www.meti.go.jp/english/
[116] http://www.npa.go.jp/english/index.htm

სფეროში კვლევებითა და განვითარებით. ეროვნული პოლიციის სააგენტო (NPA) უზრუნველყოფს კომპიუტერულ და ქსელურ უსაფრთხოებას, ასევე აწარმოებს კიბერდანაშაულებების საგამოძიებო საქმიანობას. ამ მიზნით, სააგენტოს ფარგლებში მოქმედებს მაღალტექნოლოგიური დანაშაულებების სამმართველო (HTCTD), რომელიც ებრძვის მსხვილმასშტაბიან კომპიუტერულ ინციდენტებს, ასევე უფლებამოსილია განახორციელოს მოკვლევა და დაკავება. სამმართველოს ერთერთ ქვედანაყოფს წარმოადგენს ტექნიკური მხარდაჭერის მობილური ჯგუფი, რომელიც განლაგებულია ქვეყნის მთელ ტერიტორიაზე და იმყოფება კიბერსარდლობის ცენტრის დაქვემდებარებაში. სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობის ფარგლებში მოქმედებს ფინანსების დაცვის, ტექნიკური ექსპლუატაციის, ანალიზისა და რეაგირების ცენტრი (CEPTOAR), რომლის მთავარი მიზანია სახელმწიფო და კერძო სუბიექტებს შორის ინფორმაციის გაცვლის გაუმჯობესება;

- **კორეის რესპუბლიკა** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებს ახორციელებს ყველა სახელმწიფო ორგანიზაცია და მათი სტრუქტურული ქვედანაყოფები. მოცემულ სფეროში ყველა სამინისტროსი და უწყების საქმიანობას კოორდინაციას უწევს კიბერუსაფრთხოების ეროვნული ცენტრი (NCSC)[117], რომელიც მუშაობს დაზვერვის ეროვნული სამსახურის (NIS)[118] ეგიდით. გარდა ამისა, კიბერუსაფრთხოების ეროვნული ცენტრი (NCSC) კიბერსაფრთხეებთან ბრძოლაში აერთიანებს კერძო, საჯარო და სამხედრო სექტორებს, ცენტრი ასევე წარმოადგენს კიბერშეტევების გამოვლენის, გაუვნებელყოფისა და კიბერსაფრთხეებზე ოპერატიული რეაგირების საკითხებში აღმასრულებელი ხელისუფლების ცენტრალურ ორგანოს. კიბერდანაშაულის პროფილაქტიკურ და საგამოძიებო საქმიანობის

[117] http://service1.nis.go.kr/eng/intro/NCSCInfo.jsp
[118] http://eng.nis.go.kr/svc/index.do

კოორდინაციას აწარმოებს გენერალური პროკურატურის სპეციალური სგამოძიებო ორგანო. ელექტრონიკისა და ტელეკომუნიკაციის სამეცნიერო - კვლევითი ინსტიტუტი (ETRI)[119] ახორციელებს შესაბამისი ტექნოლოგიების განვითარებასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებს. მოცემულ სფეროში ინტერნეტისა და სატელეკომუნიკაციო ქსელის უსაფრთხოების კულტურის ფორმირებაზე პასუხისმგებელია ასევე სახელმწიფო მართვისა და უსაფრთხოების სამინისტრო (MOPAS)[120], კავშირგაბმულობის კომისია, ცოდნისა და ეკონომიკის სამინისტრო, ინფორმაციული უსაფრთხოების სააგენტოს (KISA)[121] შემადგენლობაში არსებული ინტერნეტის უსაფრთხოების ცენტრი (KrCERT/CC)[122]. KISA - ში შედის აგრეთვე ინფორმაციული ინფრასტრუქტურის დაცვის განყოფილება, რომელიც შედგება კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვითი ღონისძიებების დაგეგმვის, კრიტიკული ინფრასტრუქტურის უსაფრთხოების მართვისა და სერტიფიკაციის ჯგუფებისგან. ინფორმაციული უსაფრთხოების ეროვნული ალიანსი (NISA), სადაც გაერთიანებულია 22 სახელმწიფო ორგანიზაცია, 17 საწარმოს[123] ინფორმაციული უსაფრთხოების სამსახურების ხელმძღვანელი პირები, ასევე სპეციალისტები სამრეწველო და სამეცნიერო წრეებიდან, წარმოადგენს სახელმწოფოსა და კერძო სექტორებს შორის პარტნიორობას, რომელიც მიმართულია ინფორმაციის გაცვლის გზით, ინფორმაციული უსაფრთხოების ამაღლებასა და განვითარებაზე.

[119] https://www.etri.re.kr/eng/main/index.etri
[120] http://www.iclei.org/
[121] http://www.kisa.or.kr/eng/main.jsp
[122] http://eng.krcert.or.kr/krcert_cc/welcome.jsp
[123] ინფორმაციული ქსელების სახელმწიფო კომპანიები და ოპერატორები

საქართველოში არსებული სუბიექტები

საქართველოში არ არსებობს ერთიანი ორგანო, რომელიც კოორდინაციას გაუწევს ქვეყნის კიბერსივრცის დაცვასა და უზრუნველყოფს კიბერუსაფრთხოებასთან დაკავშირებულ ღონისძიებებს სამინისტროებსა და უწყებებს შორის. განხორციელებულმა საკონსტიტუციო ცვლილებებმა და უშიშროების საბჭოს ალტერნატიული ორგანოს უსაფრთხოებისა და კრიზისების მართვის საბჭოს შექმნამ გამოიწვია მოცემული საკითხის დროებით ღიად დატოვება. კერძოდ, უშიშროების საბჭომ, რომელმაც თავის დროზე შეიმუშავა კიბერუსაფრთხოების სტრატეგია, და რომლის ფარგლებშიც უნდა ყოფილიყო კიბერსივრცის დაცვის საკითხებზე მომუშავე უწყებათაშორისი კომისია[124], თავისი ფუნქციები მოცემულ სფეროში გადასცა უსაფრთხოებისა და კრიზისების მართვის საბჭოს, სადაც ჯერჯერობით ამ მიმართულებით წინსვლა არ არის. მიუხედავად ამისა, კანონში „ინფორმაციული უსაფრთხოების შესახებ“ განსაზღვრულია კიბერუსაფრთხოებაზე პასუხიმგებელი და მაკოორდინირებელი სახელმწიფო ორგანო. კერძოდ, კანონის მე - 3 თავში „კიბერუსაფრთხოების უზრუნველყოფა“ ვკითხულობთ, რომ „საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, ასევე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ სხვა, მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE“[125]. მოცემული ჯგუფის მოვალეობებში შედის კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა, კომპიუტერული ინციდენტების ანალიზი, აღრიცხვა, მათი დროული გამოვლენა, რეაგირება და კოორდინაციის უზრუნველყოფა და სხვა. ასევე,

[124] კომისიაში შედიოდა ყველა სამინისტროსა და უწყებების წარმომადგენლები
[125] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7

ჯგუფი პასუხისმგებელია მოცემულ სფეროში ცნობიერების ამაღლებაზე, საგანმანათლებლო პროცესზე და სხვა[126].

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

- მოცემული სამინისტროებიდან ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემებისა და სუბიექტების დაცვაზე პასუხისმგებელია იუსტიციის სამინისტროს სსიპ „მონაცემთა გაცვლის სააგენტო“[127], სადაც ასევე გაერთიანებულია ზემოთ ნახსენები კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE. სააგენტო ასევე განსაზღვრავს ინფორმაციული უსაფრთხოების პოლიტიკას[128], კოორდინაციასა და მონიტორინგს უწევს სამინისტროებსა და უწყებებში ინფორმაციული უსაფრთხოების მიმართულებით გასატარებელ ყველა ღონისძიებას. მონაცემთა გაცვლის სააგენტო ასევე აქტიურად თანამშრომლობს საერთაშორისო დონეზე, კერძოდ ევროკავშირის წევრ ქვეყნებთან და ნატო - ს შესაბამის სტრუქტურულ ერთეულებთან. გარდა ამისა, სააგენტო წარმატებით ახორციელებს E – Governmant[129] სისტემის დანერგვის პროცესს;

---

[126] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7, 8

[127] http://dea.gov.ge/uploads/legal_acts/1/monacemta%20gacvlis%20saaagento_geo.pdf

[128] http://dea.gov.ge/uploads/legal_acts/8/Inf._Security.pdf

[129] E-government (short for electronic government, also known as e-gov, Internet government, digital government, online government, or connected government) consists of the digital interactions between a citizen and their government (C2G), between governments and government agencies (G2G), between government and citizens (G2C), between government and employees (G2E), and between government and businesses/commerce (G2B). Essentially, e-government delivery models can be briefly summed up as (Jeong, 2007):
G2G (government to governments)
G2C (government to citizens)
G2E (government to employees)

- 2014 წლის თებერვალში[130] თავდაცვის სამინისტროს ფარგლებში შეიქმნა სსიპ „კიბერუსაფრთხოების ბიურო“[131], რომლის მიზანია კიბერდანაშაულთან ბრძოლის ერთიანი სახელმწიფო პოლიტიკის განხორციელება, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა, ბიუროს კომპეტენციას მიკუთვნებული სფეროს მარეგულირებელი კანონმდებლობის შემუშავება და სრულყოფა და კანონმდებლობით დადგენილი სხვა საქმიანობის განხორციელება. ბიუროს ძირითადი საქმიანობა წარიმართება ინფორმაციული და კომუნიკაციების ტექნოლოგიების დეპარტამენტის მიერ, რომლის სტრუქტურული ერთეულებია: პროექტების მართვის სამმართველო; კომპიუტერულ ინციდენტებზე რეაგირების საკოორდინაციო სამმართველო CSIRT/CC); კომპიუტერულ ინციდენტებზე რეაგირების სამმართველო (CSIRT); კომპიუტერულ ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილება;
- ინტერნეტ - სივრცეში კიბერდანაშაულების გამოვლენას, აღკვეთას, მოკვლევით და საგამოძიებო საქმიანობას, ასევე საჭიროების შემთხვევაში დაკავებას, ახორციელებს შინაგან საქმეთა ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველო[132]. გარდა ამისა, შინაგან საქმეთა სამინისტროში საექსპერტო–კრიმინალისტიკური მთავარი სამმართველოს შემადგენლობაში ჩამოყალიბდა კომპიუტერულ–ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც უშუალოდ ახორციელებს ციფრული მტკიცებულებების

G2B (government to businesses)

[130] https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2235212&lang=ge

[131] კიბერუსაფრთხოების ბიუროს მიზნები და ფუნქციების დიდი ნაწილი წარმოადგენს მონაცემთა გაცვლის სააგენტოს მიზნებისა და ფუნქციების ანალოგიას, რაც ყოვლად დაუშვებელია, ვინაიდან მოხდება მოცემულ სფეროში უწყებრივი ფუნქციების აღრევა და სამუშაო პროცესის წარმართვა პარალელურ რეჟიმში

[132] 2012 წელს საქართველო შეუერთდა კიბერდანაშაულთან ბრძოლის შესახებ ევროსაბჭოს კონვენციას. ამავე წელს შსს-ს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო, რომელსაც ევალება კიბერ სივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია.

პირველად მოპყრობასა და მათ შემდგომ ექსპერტიზას. სამინისტროს შემადგენლობაში ასევე ფუნქციონირებს ოპერატიულ - ტექნიკური დეპარტამენტი, რომელიც ახორციელებს სამინისტროში ინოვაციური ინფორმაციული ტექნოლოგიების, ციფრული სატელეკომუნიკაციო სისტემების დანერგვას და ოპერირებას, აღნიშნულ სფეროებში სხვა სახელმწიფო დაწესებულებების კონსულტირებას, სამინისტროსა და მისი სტრუქტურული ქვედანაყოფების სატელეკომუნიკაციო უზრუნველყოფას და კანონმდებლობით დადგენილი წესის შესაბამისად, საგამოძიებო ღონისძიებების განხორციელების შედეგად მოპოვებული ციფრული მტკიცებულებების საექსპერტო - კრიმინალისტიკურ გამოკვლევას.

რეზუმე

ნაშრომში მოკლედ, ზოგად ფორმებში არის განხილული ევროკავშირის ზოგიერთი წევრი ქვეყნისა და სხვა ქვეყნების სუბიექტები, რომლებიც პასუხისმგებელნი არიან კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვასა და კიბერუსაფრთხოების მიმართულებით აუცილებელი ღონისძიებების განხორციელებაზე. კიბერსივრცეში არსებული საფრთხები და რისკები არცთუ ისე დიდი ხნის წინ წარმოიშვა, თუმცა ინტერნეტისა და ტექნოლოგიების სწრაფმა განვითარებამ, დადებითი პროცესების პარალელურად, გამოიწვია ასევე კიბერდანაშაულის სწრაფი ზრდა. კიბერსივრცეში საფრთხეების მაქსიმალური შემცირების მიზნით, მსოფლიო საზოგადოებამ დაიწყო ორგანიზაციული სტრუქტურული ერთეულების შექმნისა და განვითარების პროცესი, რაც პირდაპირ კავშირშია ახალი ტექნოლოგიებისა და კიბერდანაშაულის ზრდასთან, მის ახალ გამოვლინებებთან. ფაქტიურად, მოცემულ სფეროში მუდმივად მიმდინარეობს და ვითარდება ინსტიტუციონალიზმის პროცესი.

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

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

გამოყენებული ლიტერატურა

1) Democratic Governance Challenges of Cyber Security, *Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler*, DCAF 2010, DCAF Horizon 2015 Working Paper Series http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf; http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security;
2) კანონი „ინფორმაციული უსაფრთხოების შესახებ“, 19/06/2012 http://www.economy.ge/uploads/kanonmdebloba/kavshirgabmuloba/informaciuli_usafrtxoeba.pdf;
3) საჯარო სამართლის იურიდიული პირის – კიბერუსაფრთხოების ბიუროს დებულების დამტკიცების შესახებ, *საქართველოს თავდაცვის მინისტრის ბრძანება №8*, 2014 წლის 6 თებერვალი https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2235212&lang=ge

დეკემბერი, 2014 წელი

საერთაშორისო და რეგიონალური დონის ღონისძიებები მიმართული კიბერსივრცის დაცვაზე

შესავალი

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

ქვემოთ წარმოდგენილია ის საერთაშორისო და რეგიონალური დონის ორგანიზაციები, რომლებიც ცდილობენ სხვადასხვა გზებით წინ აღუდგნენ კიბერადანაშაულსა და უზრუნველყონ კიბერსივრცის დაცვა. ევროსაბჭოს, ევროკავშირის, გაერო - ს, ნატო - სა თუ სხვა წარმოდგენილი ორგანიზაციების ფარგლებში წარმოებს საქმიანობა კიბერუსაფრთხოების თემებზე.

ევროპის საბჭო

2001 წლის 23 ნოემბერს ბუდაპეშტში ხელი მოეწერა კიბერდანაშაულთან ბრძოლის ევროპულ კონვენციას (CETS 185)[133], რომელიც ძალაში შევიდა 2004 წლის 1 ივლისს. კონვენცია მომზადდა ევროპის საბჭოს ფარგლებში კანადის, შეერთებული შტატების, იაპონიისა და სამხრეთ აფრიკის რესპუბლიკის მონაწილეობით. დღესდღეისობით ეს

[133] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

კონვენცია არის მოცემულ სფეროში ერთადერთი აღიარებული იურიდიული დოკუმენტი, რომელიც მიღებულია საერთაშორისო დონეზე და ის არის ღია ყველა დაინტერესებული ქვეყნისთვის. ასევე საინტერესოა კონვენციაზე დამატებით მიღებული პროტოკოლი (CETS 189)[134] კომპიუტერულ ქსელებში ქსენოფობიისა და რასიზმის ნიადაგზე ჩადენილი დანაშაულების შესახებ, რომელსაც ხელი მოეწერა 2003 წლის იანვარში და ძალაში შევიდა 2006 წლის მარტის თვეში.

კონვენცია ხელმომწერ ქვეყნებს ავალდებულებს შექმნან სამართლებრივ - ნორმატიული ბაზა აუცილებელი კიბერდანაშაულის პრობლემის ეფექტური გადაწყვეტისთვის. ასევე ყველა ხელმომწერი ქვეყანა თავის თავზე იღებს ერთმანეთისთვის დახმარების აღმოჩენას კიბერდამნაშავეთა სამართლებრივი დევნისა და ინციდენტების გამოძიების საკითხში. ევროპული კონვენცია არის ერთერთი პირველი საერთაშორისო დოკუმენტი, სადაც განსაზღვრულია და კლასიფიცირებულია კიბერდანაშაული. კერძოდ, შემოსულია ინტერნეტ სივრცეში არასანქცირებული შეღწევისა და რესურსების არაკანონიერი გადაჭერის განსაზღვრება, კომპიუტერულ სისტემებსა და ინფორმაციის მატარებელზე არაკანონიერი ჩარევა, მოწყობილობის არასამართლებრივი გამოყენება, კომპიუტერული მაქინაციები. კონვენციის მოქმედება ასევე ვრცელდება საბავშვო პორნოგრაფიასა და საავტორო უფლებების დარღვევაზე. დოკუმენტში განსაზღვრულია კომპიუტერული დანაშაულების ეფექტური გამოძიების ინსტრუმენტები და მათთან ბრძოლა. კონვენციის მოქმედფება ვდრცელდება ყველა დანაშაულზე, რომელიც ჩადენილია კომპიუტერულ სისტემებში, ასევე ელექტრონული საშუალებებით შეგროვილი ნებისმიერი მტკიცებულებები.

ამ ეტაპზე კონვენცია რატიფიცირებულია ევროკავშირის ყველა ქვეყნისა და შეერთებული შტატების მიერ, და ხელმოწერილია ორმოცდაექვსი ქვეყნის მიერ[135]. ხუთ ქვეყანას მიეცა რეკომენდაცია და გაუკეთდა შეთავაზება მიუერთდეს კონვენციას[136].

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

[135] ევროკავშირის წევრი ქვეყნები, კანადა, იაპონიია, სამხრეთ აფრიკის რესპუბლიკა და ნატო - ს ყველა წევრი ქვეყანა

[136] ჩილე, კოსტა - რიკა, დომინიკის რესპუბლიკა, მექსიკა და ფილიპინები

ისეთმა დიდმა ქვეყნებმა, როგორებიცაა ჩინეთი და რუსეთი უარი თქვეს ხელი მოეწერათ კონვენციაზე და მიერთებოდნენ მას[137]. ევროპული კონვენცია გამოიყენება როგორც სახელმძღვანელო და ცნობარი მსოფლიოს ასზე მეტი ქვეყნის სტანდარტული ან ტიპიური საკანონმდებლო ბაზისათვის. გარდა ამისა, კონვენცია მხარს უჭერს ყველა სხვა ორგანიზაციას, რომლებიც იყენებენ მას თავიანთი გადაწყვეტილების მიღებაში. ეს ორგანიზაციებია ევროპის კავშირი, ამერიკის სახელმწიფოთა ორგანიზაცია (OAS)[138], ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია (OECD)[139], აზია - წყნარი ოკეანის ეკონომიკური თანამშრომლობის ორგანიზაცია (APEC)[140], ინტერპოლი[141], ასევე კერძო სექტორის წარმომადგენლები.

მიუხედავად იმისა, რომ მოცემულ კონვენციას აქვს ფართო საერთაშორისო აღიარება, ზოგიერთი ქვეყანა მაინც ამტკიცებს, რომ კონვენცია ითვალისწინებს კიბერდანაშაულის აღსაკვეთად საჭირო არასაკმარის ზომებს, და რამაც შეიძლება დიდი ზიანი მიაყენოს ეროვნულ უსაფრთხოებას. პირველ რიგში, კონვენცია კომპიუტერულ ქსელზე განხორციელებულ შეტევას განიხილავს როგორც კერძო და სახელმწიფო საკუთრების წინააღმდეგ ჩადენილ დანაშაულს, და არა როგორც ეროვნული უსაფრთხოების საფრთხეს. მეორე, კონვენცია ერთმანეთისგან არ ანსხვავებს შეტევებს ჩვეულებრივი კომპიუტერული ქსელებსა და კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტებს შორის, ისევე როგორც ფართომასშტაბიან და ლოკალურ შეტევებს შორის.

თუმცა კონვენცია წარმოადგენს სტანდარტულ დოკუმენტს, რომელიც წარმოადგენს საერთაშორისო კანონმდებლობის ძალზედ მნიშვნელოვან შემადგენელ ნაწილს. მასში მოცემულია იურიდიული და ტექნიკური ნორმების ოპტიმალური კომპლექსი, რომელიც შეიძლება გამოყენებულ იქნას ამ სფეროში საერთაშორისო

[137] აღნიშნული კონვენცია საქართველოსთან მიმართებაში ძალაში შევიდა 2012 წლის პირველი ოქტომბრიდან. შედეგად, საქართველო გახდა კონვენციის 34-ე წევრი სახელმწიფო
[138] Organization of American States http://www.oas.org/en/
[139] Organization for Economic Co-operation and Development http://www.oecd.org/
[140] Azia – Pacific Economic Cooperation http://www.apec.org/
[141] Interpol http://www.interpol.int/

თანამშრომლობის გაფართოებაზე დამატებითი შეთანხმებების დამუშავების მიზნით. გამომდინარე, რომ კიბერდანაშაულს, კიბერტერორიზმსა და კიბერომს გააჩნიათ ბევრი საერთო ნიშანი და მახასიათებელი, კონვენცია ნებისმიერ კიბერშეტევაზე, მიუხედავად მათი მოტივაციისა, ითვალისწინებს, რომ მასზე ხელმომწერმა ქვეყნებმა პასუხისმგებელი უწყებების მოთხოვნაზე უნდა დააკავონ და გადასცენ ყველა კიბერდამნაშავე სამართალდამცავ ორგანოებს, მიუხედავად იმისა, განიხილებიან თუ არა ისინი საკუთარ ქვეყნებში როგორც დამნაშავეები, ტერორისტები ან კიდევ პატრიოტები.

ევროპული კავშირი

ევროკავშირი წარმოადგენს ინფორმაციული უსაფრთხოების სფეროში საერთაშორისო დონეზე არსებულ მთავარ სუბიექტს. ამავდროულად, ევროკავშირი დიდ ყურადღებას უთმობს ისეთ საკითხებს, როგორიც არის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვა, ინფორმაციული საზოგადოების ფორმირება და ინფორმაციული დაცვა. ევროკავშირმა დაიწყო სამეცნიერო - კვლევითი და სხვა სახის პროგრამების რეალიზება, რომელიც უკავშირდება ინფორმაციული რევოლუციის ასპექტებსა და განათლებაზე, ბიზნესზე, ჯანდაცვასა და კავშირგაბმულობაზე მათ გავლენას.

2004 წლის 20 ოქტომბერს[142] ევროკავშირის კომისიის მიერ მიღებული კომუნიკე კრიტიკული ინფრასტრუქტურის დაცვაზე იძლევა კრიტიკული ინფრასტრუქტურისა და მისი ობიექტების განსაზღვრებას, ასევე ადგენს კრიტერიუმებს იმ ობიექტების მიმართ, რომლებიც შეიძლება წარმოიშვას მომავალში. 2005 წლის ნოემბერში[143] ევროკავშირის კომისიის მიერ მიღებულია კრიტიკული ინფრასტრუქტურის დაცვის ევროპული პროგრამა „მწვანე წიგნი“, სადაც განსაზღვრულია ევროკავშირის მოქმედების მიმართულებები მოცემულ სფეროში. 2008 წელს ევროკავშირის კომისია შეუდგა

[142] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm
[143] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

პროექტის რეალიზებას, რომელიც მიმართულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საერთო სტრატეგიის გამომუშავებაზე.

ქვემოთ მოცემულია ევროკავშირის კომისიის სხვა პროექტები და სტრატეგიები:

- ევროკავშირის კომისიის დაკვეთით, ელექტრონული კავშირის ინფრასტრუქტურის შეღწევადობისა და საიმედოობის პრობლემების კვლევების ჩატარება (ARECI)[144];
- პროექტი „კრიტიკული ინფრასტრუქტურის საფრთხეების შეტყობინების ინფორმაციული ქსელი“ (CIWIN)[145];
- 2004 წლის მარტში შეიქმნა და 2005 წლის სექტემბერში, კუნძულ კრეტაზე დაიწყო ფუნქციონირება ქსელური და ინფორმაციული უსაფრთხოების ევროპულმა სააგენტომ (ENISA)[146]. სააგენტოს მიზანია ევროკავშირის ფარგლებში ელექტრონული ქსელების უსაფრთხოების მაღალი დონის მიღწევა;
- ტელემეტრიის ტრანსევროპული სამთავრობოთაშორისო სამსახური (TESTA)[147]. ეს არის სამთავრობოთაშორისო კავშირის ქსელი, რომელიც მოქმედებს მხოლოდ ევროკავშირის ფარგლებში. ის არ არის ჩართული ინტერნეტ - სივრცეში და სხვადასხვა უწყების თანამდებობის პირებს ერთმანეთთან ურთიერთობისას, ინფორმაციის დაზიანებისა და გადინების თავიდან აცილების საშუალებას აძლევს;

ინფორმაციული უსაფრთხოების სფეროში ევროკავშირის სამეცნიერო - კვლევითი პროექტები:

[144] The Availability and Robustness of Electronic Communications Infrastructures file:///C:/Users/Admin/Downloads/StudyFinalReport.pdf
[145] The Critical Infrastructure Warning Information Network https://ciwin.europa.eu/Pages/Home.aspx
[146] The European Union Agency for Network and Information Security https://www.enisa.europa.eu/
[147] The European Software Testing Awards http://www.softwaretestingawards.com/

- ინფორმაციული საზოგადოების ტექნოლოგიები (პროექტები FP6[148] და FP7[149]);
- უსაფრთხოების პრობლემების ევროპული სამეცნიერო - კვლევითი პროგრამა (ESRP)[150];
- კრიტიკული ინფორმაციული ინფრასტრუქტურის პრობლემების სამეცნიერო - კვლევითი საკოორდინაციო პროექტი (CI2RCO)[151];
- ინფრასტრუქტურისა და პროექტირების არქიტექტურა[152].

ინფორმაციული უსაფრთხოების საკითხებში ევროკავშირიოს სამართლებრივ - ნორმატიული ბაზა:

- მონაცემთა დაცვის დირექტივა (1995 წელი)[153];
- ელექტრონული ხელმოწერის დირექტივა (1999 წელი)[154];
- ელექტრონულ კავშირების სფეროში კონფიდენციალობის დაცვის დირექტივა (2002 წელი)[155];
- ჩარჩო დირექტივა (2002 წელი)[156];
- ინფორმაციულ სისტემებზე შეტევის საბჭოს ჩარჩო გადაწყვეტილება (2005 წელი)[157];
- მონაცემთა შენახვის დირექტივა (2006 წელი).

[148] http://ec.europa.eu/research/fp6/index_en.cfm
[149] http://ec.europa.eu/research/fp7/index_en.cfm
[150] http://www.statewatch.org/Targeted-issues/ESRP/security-research.html
[151] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/security/ci2rco-executive-summary_en.pdf
[152] http://www.service-architecture.com/articles/cloud-computing/infrastructure_as_a_service_iaas.html
[153] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 24 October 1995 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[154] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 13 December 1999 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML
[155] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm
[156] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm
[157] http://europa.eu/legislation_summaries/information_society/internet/l33193_en.htm

უსაფრთხოებისა და ექსტრემალური რეაგირების ფორუმი (FIRST)[158]

ფორუმი დაფუძნდა 1990 წელს და წარმოადგენს ინფორმაციული უსაფრთხოების სფეროში ინციდენტებზე ექსტრემალური რეაგირების სპეციალისტების მსოფლიოში არსებულ ერთადერთ საერთაშორისო ფორუმს. ეს ორგანიზაცია წარმოადგენს ქსელებში ექსტრემალური რეაგირების სფეროში მსოფლიოში აღიარებულ ლიდერს და აერთიანებს ოპერატიული რეაგირების ჯგუფებს, რომლებიც მუშაობენ სხვადასხვა უწყებრივ დონეებზე, როგორც სახელმწიფო ისე კერძო სექტორში, მათშორის საგანმანათლებლო დაწესებულებებში. ფორუმის საქმიანობა მიმართულია ინციდენტების აღკვეთის გაძლიერებასა და კოორდინირებულ თანამშრომლობაზე, ასევე სწრაფი რეაგირების სფეროში შესაძლებლობების გაძლიერებაზე. ფორუმი მის წევრებსა და ზოგადად საზოგადოებას შორის ინფორმაციისა და გამოცდილების გაცვლის საშუალებას იძლევა.

დიდი რვიანი (Group of Eight – G8)

დიდი რვიანი 1995 წლიდან მოყოლებული სულ უფრო მეტ აქტიურ მონაწილეობას იღებს იმ საკითხების გადაწყვეტაში, რომლებიც უკავშირდება კიბერდანაშაულს, ინფორმაციულ საზოგადოებას, კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას. 1995 წელს ჰალიფაქსის სამიტზე[159] შეიქმნა უფროს ექსპერტთა ჯგუფი, რომელსაც დაევალა შეეფასებინა და გაანალიზებინა არსებული საერთაშორისო შეთანხმებები, ასევე ორგანიზებულ დანაშაულთან ბრძოლის მექანიზმები. მოცემულმა ჯგუფის მიერ ჩატარებული სამუშაოს შედეგად, შემუშავდა ორმოცი ოპერატიული რეკომენდაცია, რომლებიც დამტკიცებულ იქნა 1996 წელს დიდი რვიანის ლიონის სამიტზე. ამ დროდან მოყოლებული ლიონის ჯგუფი გახდა მუდმივმოქმედი მრავალფუნქციური ორგანო, რომლის შემადგენლობაში შევიდა მთელი რიგი სპეციალური სამუშაო ჯგუფები. 2001 წლიდან, ტერორიზმთან დაკავშირებულ საკითხებზე, ლიონის ჯგუფის სხდომები მიმდინარეობს ერთობლივად რომის ჯგუფთან.

[158] The Forum of Incident Response and Security Teams http://www.first.org/
[159] http://www.chebucto.ns.ca/Current/HalifaxSummitG7/

კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში დიდი რვიანის მუშაობის მიღწევად შეიძლება ჩაითვალოს, პარიზში 2000 წელს[160] ჩატარებული კონფერენცია, სადაც მონაწილეობას იღებდა როგორც სახელმწიფო ისე კერძო სექტორი. კონფერენცია მიეძღვნა სახელმწიფოსა და კერძო სექტორს შორის უსაფრთხოებისა და კიბერსივრცის სფეროში სანდოობის ამაღლების განვითარება. კონფერენციის მიზანი იყო მარალტექნოლოგიური დანაშაულისა და ინტერნეტ - სივრცის არაკანონიერი გამოყენების ირგვლივ მსჯელობა და გადაწყვეტილების მიღება. დიდი რვიანის წევრი ქვეყნები პარიზის კონფერენციაზე შეთანხმდნენ კიბერდანაშაულთან ბრძოლის კონკრეტულ და გამჭვირვალე პრინციპებზე, რომლებიც მიმართულია ახალი „უსაფრთხოების კულტურის“ შექმნაზე, საერთაშორისო თანამშრომლობის გააქტიურებაზე, ასევე მონიტორინგისა და კომპიუტერულ ქსელებში საფრთხის შეტყობინების სფეროში არსებული მოწინავე გამოცდილების გაზიარებაზე. კონფერენციაზე ასევე მიღწეული იყო შეთანხმება ერთობლივი სასწავლო კურსების ჩატარებაზე, რომელმაც უნდა გამოავლინოს ქსელებში საგანგებო ინციდენტებზე რეაგირების სამსახურების მომზადების მზადყოფნა, აგრეთვე საფრთხეების შესახებ შეატყობინოს სხვა ქვეყნების მთავრობებს. კონფერენციაზე სულ მიღებული იქნა თერთმეტი პრინციპი, რომლებიც დახმარებას გაუწევს სახელმწიფოებს კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში შექმნას და გაატაროს ეფექტური ეროვნული პოლიტიკა.

კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პრინციპების ძირითადი ელემენტები აისახა, 2004 წელს გაეროს 78 - ე ასამბლეაზე მიღებულ №58/199 რეზოლუციაში[161] „კიბერუსაფრთხოებისა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის გლობალური კულტურის შექმნაზე“.

[160] https://www.ciret.org/conferences/paris-2000/
[161] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაცია (NATO)

2002 წელს, მას შემდეგ რაც 1990 წლების ბოლოს ბალკანებზე სამხედრო ოპერაციის დროს განხორციელდა ქსელური შეტევები, ალიანსმა შეიმუშავა და გაუშვა კიბერ - დაცვის საკუთარი პროგრამა. ალიანსის ხელმძღვანელობამ გაითვალისწინა „ბალკანეთის გაკვეთილები“, და 2002 წელს პრაღის სამიტზე[162] ნატო - ს წევრი ქვეყნების ლიდერები შეთანხმდნენ კიბერნეტიკული თავდაცვის პროგრამის შემუშავებასა და ინფორმაციულ ქსელებში ინციდენტებზე რეაგირების საკუთარი ჯგუფის (NCIRC)[163] შექმნაზე. ჯგუფის საკოორდინაციო ცენტრი განთავსებულია ბრუსელში, ნატო - ს შტაბ - ბინაში, ხოლო ალიანსის სამეთაურო ოპერაციების მართვის შტაბში[164] ორგანიზებულ იქნა NCIRC - ს ტექნიკური ცენტრი. მოცემული სტრუქტურის შექმნით, ალიანსმა გადაწყვიტა მთელი რიგი სირთულეები დაკავშირებული კიბერუსაფრთხოების საკითხებთან. კერძოდ, ნატო - ს კომპიუტერულ ქსელებში არასანქცირებული შეღწევისა და სხვა მავნებლობების აღმოჩენა და განეიტრალება, ასევე ქსელების კრიპტოგრაფიული დაცვის ეფექტური მართვის უზრუნველყოფა.

გარდა ამისა, ალიანსის ექსპერტები უზრუნველყოფენ კომპიუტერულ ქსელებში საფრთხის წარმოქმნის საწინააღმდეგო ტექნიკურ ღონისძიებების, ასევე შეიმუშავებენ უსაფრთხოების უზრუნველყოფის რეჟიმსა და კომპიუტერულ დანაშაულებების გამოძიების მეთოდოლოგიას. ამის პარალელურად, ტალინში შეიქმნა ალიანსის კომპიუტერული თავდაცვის სფეროში მოწინავე გამოცდილების გაცვლის ცენტრი (CCDCOE)[165], ნატო - მ ასევე დააფუძნა კიბერ - თავდაცვის ღონისძიებების მართვის სპეციალური ორგანო (CDMA)[166], რომელმაც ფუნქციონირება დაიწყო 2008 წელს. ამ

[162] http://www.nato.int/docu/comm/2002/0211-prague/

[163] Computer Incident Response Capability https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf

[164] ქ. მონსი, ბელგია

[165] Cooperative Cyber Defense Centre of Exelllence https://ccdcoe.org/tallinn-manual.html

[166] The Cyber Defense Management Authority (CDMA): The Authority was called upon to initiate and coordinate response to cyber attacks against allied member states, and NATO itself. CDMA was Created and was operational in mid-2008. It was a big step in NATO Cyber Defense because it helps member states improve their own cyber security. Rapid-Reaction Teams (RRT's) are also being created and will be available to member states in order to help them counter cyber attacks and will be available for immediate deployment http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events

უკანასკნელის ფუნქციებში შედის ალიანსის კომპიუტერულ ქსელზე შეტევის შემთხვევაში „კიბერ - თავდაცვის ოპერატიული და ეფექტური ღონისძიებების“ ორგანიზება და კოორდინაცია. 2009 წელს სტრასბურგის სამიტზე[167] ნატო - ს წევრმა ქვეყნებმა ვალდებულება აიღეს დააჩქარონ კიბერ - თავდაცის თანამედროვე საშუალებების შეძენა, გახადონ კიბერდაცვა ალიანსის განუყოფელ ნაწილად, განავითარონ საერთაშორისო თანამშრომლობა არამარტო ნატო - ს წევრ - ქვეყნებს შორის, არამედ ასევე პარტნიორ ქვეყნებთან. ალიანსი ასევე ახორციელებს მხარდამჭერ პროგრამებს მიმართულს წევრი და პარტნიორი ქვეყნების კიბერუსაფრთხოების ეროვნული პოლიტიკის განვითარებისა და კიბერ - საფრთხეებზე ექსტრემალური რეაგირების ჯგუფის შექმნისკენ.

კრიტიკული ინფრასტრუქტურის დაცვა არის ალიანსის ძირითადი მიმართულება ასევე სამოქალაქო თავდაცვის დაგეგმვის სფეროში. ამ სფეროში ღონისძიებების გატარების აუცილებლობაზე ნატო - ს ფარგლებში არაერთი დოკუმენტია მიღებული, სადაც ასახულია სამოქალაქო თავდაცვის დაგეგმვის პრინციპები, რომლებიც შემუშავდა წევრი ქვეყნების შესაბამისი უწყებებისთვის. გარდა ამისა, გეგმის ახალ რედაქციაში კიბერ - საფრთხეების ჭრილში, მოცემულია სამოქალაქო თავდაცვის საგანგებო სიტუაციების ისეთი მიმართულებები როგორიცაა ქიმიური, ბიოლოგიური და ატომური იარაღის გამოყენების წინააღმდეგ. ნატო - ს სამოქალაქო თავდაცვის დაგეგმვის მთავარი კომიტეტი და მისი რვა განყოფილება და კომიტეტი აგრძელებს კრიტიკული ინფრასტრუქტურის დაცვის ფუნქციონალური ასპექტების შესწავლას. ამის შედეგად, მუშავდება შესაბამისი რეკომენდაციები დაგეგმვის ყველა სახეობის მიმართულებით, რასაც ახორციელებს სათანადო განყოფილებები და კომიტეტები.

2007 წლის ნატო - ს საპარლამენტო ასამბლეაზე წარმოდგენილ სპეციალურ მოხსენებაში, ასევე ალიანსის კრიტიკული ინფრასტრუქტურის დაცვის საკითხებზე მომზადებულ სხვა ანგარიშებში (173 DSCFC 09 E bis)[168] განსაზღვრულია ნატო - ს წევრი

[167] http://www.nato.int/cps/en/natolive/news_52837.htm
[168] http://www.nato-pa.int/default.asp?SHORTCUT=1782

ქვეყნებისა და მთლიანად ალიანსის კრიტიკული ინფრასტრუქტურის დაცვის საერთო პრინციპები. ისინი განსაზღვრავენ სხვადასხვა ნორმებს, მათ მსგავსებასა და სხვაობას, ასევე კრიტიკული ინფრასტრუქტურის დაცვის დარგობრივი სტრატეგიების განვითარებისა და რეალიზაციის სფეროში განსაზღვრავენ სუბიექტებს თავისი ფუნქციებით, სადაც აგრეთვე შედის ენერგეტიკა, სამოქალაქო ავიაცია და საზღვაო პორტების უსაფრთხოება.

ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია (OECD)

ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციას გააჩნია დიდი გამოცდილება კომპიუტერული ქსელებისა და სისტემის უსაფრთხოების, მათ შორის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საკითხებზე სტრატეგიული რეკომენდაციების შემუშავებაში. ორგანიზაცია დიდ ყურადღებას უთმობს ასევე მავნებლური პროგრამული უზრუნველყოფის გამოყენებით ჩადენილ კიბერდანაშაულთან ბრძოლას. ორგანიზაცია ამზადებს ანალიტიკურ ანგარიშებს, სტატისტიკურ მონაცემებსა სტრატეგიულ რეკომენდაციებს, რომელთა საფუძველზეც სახელმწიფო და კერძო სექტორს შეუძლიათ შეიმუშავონ ეფექტური სტრატეგია საკუთარი ინფორმაციული უსაფრთხოების გაძლიერებაზე, საზოგადოებაში აამაღლონ ცნობადობის დონე ინტერნეტ - სივრცის უსაფრთხოების მნიშვნელობაზე და ხელი შეუწყონ კიბერუსაფრთხოების კულტურის განვითარებას. ორგანიზაციის ყველა წევრი ქვეყანა თანხმდება, რომ კრიტიკული ინფრასტრუქტურის დაცვა, მისი უსაფრთხო ფუნქციონირება და სანდოობა არის მნიშვნელოვანი ინტერნეტ - სივრცეში კანონიერი ვაჭრობისთვის, პერსონალური მონაცემების დაცვისა და უსაფრთხო საბანკო ოპერაციებისთვის. სწორედ ამიტომ, ორგანიზაციის ინფორმაციული უსაფრთხოებისა და კონფიდენციალობის სამუშაო ჯგუფი (WPISP)[169] აქტიურად მუშაობს ამ სფეროში საერთაშორისო დონეზე შეთანხმებული მიდგომის მიმართულებით, რომელიც ითვალისწინებს კომპიუტერულ ქსელებში ნდობის გაძლიერების მიზნით პოლიტიკის

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

შემუშავებას. გარდა ამისა, ინფორმაციული, კომპიუტერული და საკომუნიკაციო პოლიტიკის კომიტეტი აკეთებს საერთო პრინციპების ანალიზს, რომელიც საფუძვლად უდევს ელექტრონულ ეკონომიკას, ინფორმაციულ ინფრასტრუქტურასა და საზოგადოებას.

გაერთიანებული ერების ორგანიზაცია (UN)

გაეროს 80 - იანი წლების ბოლოს დაიწყო კრიტიკული ინფორმაციული ინფრასტრუქტურის საკითხების განხილვა, თუმცა ფორმალური ზომების დანერგვა დაიწყო მხოლოდ ბოლო პერიოდში. ორგანიზაციის მიერ მის ფარგლებში მიღებულია მთელი რიგი ინიციატივები მიმართული კოორდინირებული მოქმედების გასაუმჯობესებლად. კერძოდ, ეს არის რამოდენიმე რეზოლუცია, მსოფლიო სამიტები ინფორმაციული საზოგადოების საკითხებზე (WSIS), გაეროს ზოგიერთი სტრუქტურის პროექტები.

გლობალურ ციფრულ სივრცეში საერთაშორისო ინფორმაციული უსაფრთხოების გაძლიერების მიზნით, გაეროს განიარაღების კვლევითმა ინსტიტუტმა (UNIDIR) ჩაატარა მთელი რიგი სემინარები. თავის მხრივ, გაეროს ნარკომანიასთან და დანაშაულთან ბრძოლის სამმართველო სისტემატურად ატარებს სწავლებებს, რომლის მიზანია შეთანხმებული და კოორდინირებული მიდგომა კიბერდანაშაულის პრობლემებთან.

2000 და 2001 წლების დეკემბერში გაეროს გენერალური ასამბლეის 55 - ე და 56 - ე სესიებზე მიღებულ იქნა №55.63 და №56/121 რეზოლუციები „ინფორმაციული ტექნოლოგიების დანაშაულებრივ გამოყენებასთან ბრძოლაზე“. 2002 წლის დეკემბერში გაეროს გენერალური ასამბლეის 57 - ე სესიამ მიიღო რეზოლუცია №57/239 „კიბერუსაფრთხოების გლობალური კულტურის შექმნაზე“. 2003 წლის დეკემბერში გაეროს გენერალური ასამბლეის 58 - ე სესიაზე მიიღეს რეზოლუცია №58/199 „კიბერუსაფრთხოების გლობალური კულტურის შექმნასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვაზე“. ამ რეზოლუციის დანართში ფორმულირებულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის

თერთმეტი პრინციპი. შემდეგ წლებში გაეროს გენერალური ასამბლეა რეგულარულად იღებდა რეზოლუციებს „საერთაშორისო უსაფრთხოების კონტექსტში ინფორმაციული და სატელეკომუნიკაციო სფეროს განვითარებაზე“. 2005 და 2006 წლებში ასევე მიღებულ იქნა ორი რეზოლუცია ინფორმაციული საზოგადოების საკითხებზე გაეროს მსოფლიო სამიტების შედეგების შესახებ.

სერიოზული და მნიშვნელოვანი მოვლენა იყო, 2001 წელს გაეროს ეკონომიკური და სოციალური საბჭოს თხოვნის საფუძველზე ინფორმაციული და საკომუნიკაციო ტექნოლოგიების საკითხებზე გაეროს მიზნობრივი ჯგუფის შექმნა. ამ ჯგუფმა მიიღო უფლებამოსილება გაუწიოს საერთაშორისო საზოგადოების ძალისხმევას მობილიზება დეკლარაციის „ათასწლეულის განვითარების მიზნებზე“ იმ ნაწილს რეალიზაცია, რომელიც ეხება ინფორმაციული და საკომუნიკაციო ტექნოლოგიების განვითარებას. 2004 წლის აპრილში ნატო - ს შტაბ - ბინაში, სამიზნე ჯგუფის მიერ ორგანიზებული იყო სემინარი თემაზე „ინფორმაციული უსაფრთხოების სფეროში უსაფრთხოების საკითხები და პოლიტიკა“. 2005 წელს სამიზნე ჯგუფმა გამოაქვეყნა პრაქტიკული სახელმძღვანელო თემაზე „ინფორმაციის დაუცველობა - კიბერსაფრთხეებისა და კიბერუსაფრთხოების „გამოუკვლევი ტერიტორიების“ ათვისების გაკვეთილები“. მოცემულ პრაქტიკულ სახელმძღვანელოში ნაჩვენებია ისეთი ახალი და სერიოზული საერთაშორისო კიბერსაფრთხეები, როგორებიც არის კიბერჰულიგნობა, კიბერტერორიზმი, კიბერომი და კიბერდანაშაული.

ინფორმაციული საზოგადოების საკითხებზე გაეროს მსოფლიო სამიტის მსვლელობისას მონაწილე ქვეყნების ლიდერებმა დაავალეს ელექტროკავშირების საერთაშორისო გაერთიანებას კიბერუსაფრთხოების სფეროში კოორდინაცია გაუწიოს საერთაშორისო მოქმედებებს. თავის მხრივ, 2007 წლის მაისში ელექტროკავშირების საერთაშორისო გაერთიანების ინიციატივით შეიქმნა კიბერუსაფრთხოების გლობალური პროგრამა (GCA), რომელმაც უნდა გამოიმუშავოს გაზრდილი კიბერსაფრთხეების წინააღმდეგ მიმართული ღონისძიებების, პრინციპებისა და მექანიზმების კოორდინირებული მოქმედების საერთო კომპლექსი. პროგრამის რეალიზების მიზნით

შეიქმნა უმაღლესი დონის ექსპერტთა ჯგუფი, სადაც შედიან კიბერუსაფრთხოების სფეროში მსოფლიოში აღიარებული ასამდე სპეციალისტი, რომლებიც წარმოადგენენ კვლევით ინსტიტუტებსა და სამეცნიერო წრეებს, სახელმწიფო და კერძო სექტორს, სამრეწველო საზოგადოებებს, საერთაშორისო ორგანიზაციებს. 2007 და 2008 წლების განმავლობაში, ელექტროკავშირების საერთაშორისო გაერთიანების მიერ ჩატარდა დიდი სამუშაოები უსაფრთხოების არქიტექტურის სტანდარტიზაციაზე, კავშირის არხების კოდირების მეთოდოლოგიის შემუსავებაზე, ინფორმაციული სისტემების უსაფრთხოების მართვასა და ქსელების მომხმარებლის ავტორიზაციაზე. გარდა ამისა, მომზადდა ინფორმაციული და საკომუნიკაციო ტექნოლოგიების უსაფრთხოების სტანდარტების „გზამკვლევი“, რომელიც წარმოადგენს მონაცემთა ელექტრონულ ბაზას, რომელიც შეიცავს ინფორმაციული და საკომუნიკაციო ტექნოლოგიების უსაფრთხოების უკვე არსებულ სტანდარტებს, ასევე საერთაშორისო ნორმებსა და სტანდარტებზე მომუშავე ძირითადი ორგანიზაციების პროექტების ჩამონათვალს.

მსოფლიო ბანკის ჯგუფი (WB)

კომპიუტერული დანაშაულებები და ელექტრონულ ქსელებში არასანქცირებული შეღწევა დიდ ზიანს აყენებს ფინანსურ სექტორს. იმის გათვალისწინებით, რომ სულ უფრო იზრდება ფინანსური ინფორმაციის შენახვისა და გადაცემის მოცულობა, კომპიუტერული დამნაშავეებისთვის ასევე ადვილი ხდება ქსელებში არასანქცირებული შეღწევა და თავიანთი მავნებლური ქმედებების განხორციელება. ამიტომ მსოფლიო ბანკის ჯგუფმა ბოლო პერიოდში განახორციელა მთელი რიგი ღონისძიებები მიმართული ინფორმაციული უსაფრთხოების უზრუნველსაყოფად, განსაკუთრებით ეს ეხება განვითარებად ქვეყნებს.

გლობალური ინფორმაციული - საკომუნიკაციო ტექნოლოგიების დეპარტამენტი[170] უწევს დახმარებას განვითარებად ქვეყნებს ინფომაციული და საკომუნიკაციო ტექნოლოგიების განვითარებაში, ასევე უზრუნველყოფას მსოფლიო ბანკის ჯგუფის

[170] http://www.worldbank.org/en/topic/ict

ძირითადი დეპარტამენტების საქმიანობას, რომელიც ეხება ინფორმაციული - საკომუნიკაციო ტექნოლოგიების სფეროში კვლევების ჩატარებას, პოლიტიკის განსაზღვრას, ინვესტიციებსა და სხვადასხვა პროგრამების განხორციელებას.

2003 წელს გამოიცა „კომპიუტერული უსაფრთხოების ცნობარი“[171], სადაც განხილულია მოწინავე გამოცდილება და რეკომენდაციები ინფორმაციული უსაფრთხოების უზრუნველყოფაში, რომელიც გამოადგება ყველა ქვეყანას, მიუხედავად მათი ტექნიკური შესაძლებლობების დონისა. ეს რეკომენდიციები მოცემულია შესაბამის ვებ - გვერდზე და ახალი ტექნოლოგიებისა და მეთოდიკის გამოჩენასთან ერთად, მუდმივად ხდება მისი განახლება.

2002 წლის ივნისში მსოფლიო ბანკმა გამოაქვეყნა სპეციალური მოხსენება „ელექტრონული უსაფრთხოება: ფინანსური ოპერაციების არსებობასთან ერთად რისკების შემცირება“[172]. ეს დოკუმენტი არის პუბლიკაციების ციკლის გაგრძელება, სადაც ელექტრონული ქსელების უსაფრთხოება განიხილება როგორც ერთერთი ძირითადი პირობა ელექტრონული გადახდების ბაზრის ეფექტური ფუნქციონირებისთვის.

2004 წლის იანვარსა და მაისში გამოვიდა შემდეგი პუბლიკაცია სახელწოდებით „ტექნოლოგიური რისკების საკონტროლო სია“[173], სადაც მოცემულია ელექტრონული უსაფრთხოების ოცდაათამდე დონის აღწერა, ასევე განხილულია ის რისკები, რომლებიც უკავშირდება ქსელების ინფრასტრუქტურის პროგრამულ უზრუნველყოფას. ყოველი მოცემული დონისთვის გათვალისწინებულია რისკების მართვის, კიბერდაზვერვისა და ინტელექტუალური ცენტრალიზებული მართვის ღონისძიებები; დაშვებისა და ავტორიზაციის კონტროლი; ქსელთაშორისი დაცვა და კონტენტის ფილტრაცია; შეღწევის აღმოჩენისა და ანტივირუსული სისტემები; კოდირების საშუალებები და მოწყვლადობის

[171] Information Technology Security Handbook http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2004/09/30/000160016_20040930112655/Rendered/PDF/300750PAPER0eSecurity.pdf

[172] Electronic Security: Risk Mitigation in Financial Transactions - Public Policy Issues https://openknowledge.worldbank.org/bitstream/handle/10986/19261/multi0page.pdf?sequence=1

[173] Technology Risk Checklist http://archive.rdec.gov.tw/public/Data/851413535571.pdf

ტესტირება; სისტემური ადმინისტრირების ღონისძიებები; შეღწევის შემთხვევაში ექსტრემალური ღონისძიებების გეგმები. 2005 წელს გამოვიდა კიდევ ორი დოკუმენტი[174] დაკავშირებული ელექტრონული გადახდების სისტემების უსაფრთხოებასთან, სადაც განხილულია საფრთხეები, რომლებიც მოდის ბოტ - ქსელებისგან, აგრეთვე კიბერსივრცეში ფულის გათეთრების პრობლემები.

ინსტიტუტის „აღმოსავლეთი - დასავლეთის“ გლობალური კიბერუსაფრთხოების ინიციატივა (WCI)[175]

2007 წელს ინსტიტუტის „აღმოსავლეთი - დასავლეთი“ ამერიკულმა ჯგუფმა „სტრატეგიული დიალოგები“, გენერალ ჯეიმს ჯონსონის[176] ხელმძღვანელობით, კიბერუსაფრთხოების სფეროში საერთაშორისო თანამშრომლობის თაობაზე ჩაატარა შეხვედრების სერია ჩინეთისა და რუსეთის ხელმძღვანელ პირებთან. ეს შეხვედრები გაგრძელდა კიდევ უფრო მაღალ დონეზე, რომლის დროს გამართულმა დისკუსიებმა გამოავლინა შეერთებული შტატების, ჩინეთისა და რუსეთის საერთო აღშფოთება არასახელმწიფო სუბიექტების სწრაფად მზარდი შესაძლებლობები, რომლებსაც შესწევთ უნარი დიდი ზიანი მიაყენოს მსოფლიო ეკონომიკას და საფრთხის ქვეშ დააყენოს როგორც თითოეული ქვეყნის ეროვნული უსაფრთხოება ისე დიდი საფრთხე შეუქმნას საერთაშორისო და რეგიონალურ უსაფრთხოებას. შეხვედრების შედეგად, თითოეულმა ქვეყანამ გადახედა კიბერუსაფრთხოების საკითხების შეფასებას, ხოლო შეერთებულმა შტატებმა კიბერსაფრთხეებს მისცა ატომური საფრთხის ტოლფასი შეფასება.

დღეს ინსტიტუტის „აღმოსავლეთი - დასავლეთი“ ხელმძღვანელობით, გლობალური კიბერუსაფრთხოების ინიციატივის ფარგლებში მიმდინარეობს აქტიური თანამშრომლობა შეერთებული შტატების, რუსეთსა და ჩინეთს შორის. ამ თანამშრომლობას უკვე შეუერთდნენ ევროკავშირისა და დიდი ოცეულის ქვეყნები, ასევე

[174] http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/CyberSecurity.pdf

[175] World Cyber Initiative http://www.ewi.info/cyber

[176] ევროპაში ნატო - ს გაერთიანებული შეიარაღებული ძალების ყოფილი უმაღლესი მთავარსადრდალი, ამჟამად შეერთებული შტატების ეროვნული უსაფრთხოების მრჩეველი

კერძო სექტორის, პროფესიული ასოციაციებისა და საერთაშორისო ორგანიზაციების წარმომადგენლები.

გლობალური კიბერუსაფრთხოების ინიციატივის საკონსულტაციო ჯგუფს სათავეში ჩაუდგა "Deloitte" კიბერინოვაციების ცენტრის დირექტორი გენერალი ჰარრი რეიდუედჯი. ეს ჯგუფი სთავაზობს პრობლემის გადაჭრას შემდეგ ორ დონეზე: (1) სანდოობის ამაღლება კიბერუსაფრთხოების კონკრეტული პრობლემის ერთობლივი თანამშრომლობისა და გადაწტვეტილების მიღების გზით, სადაც ჩართული არიან ორი ან ორზე მეტი ქვეყნის ექსპერტთა ჯგუფები; და (2) საზოგადოებრივი პროცესის ინიცირება, რომელიც საშუალებას იძლევა გადაიდგას პირველი ნაბიჯები კიბერსივრცეში საერთაშორისო უსაფრთხოების პოლიტიკის რეალიზების მიმართულებით, როგორც ეს უკვე არსებობს საზღვაო, საჰაერო და კოსმოსური სივრცისთვის. მეორე მიმართულებით საქმიანობა, ინსტიტუტის „აღმოსავლეთ - დასავლეთი" ეგიდით, დაიწყო 2010 წლის მაისში, როცა კიბერუსაფრთხოების საკითხების მსოფლიო პირველი სამიტის ფარგლებში „კიბერ - 40"[177] - ის 200 - მდე ლიდერი შეიკრიბა დალასში (აშშ). ეს სამიტი გახდა უმაღლეს დონეზე სახელმწიფოსა და კერძო სექტორს შორის საპარტნიორო მოძრაობის შექმნის პირველი მცდელობა, რომელიც ეძღვნება კრიტიკული ინფრასტრუქტურის[178] კიბერდაცვის საკითხებს.

[177] დიდ ოცეულთან ერთად გაერთიანებულია კიბერსივრცის კიდევ მსოფლიოს ოცი წამყვანი ქვეყანა

[178] აქ, კრიტიკულ ინფრასტრუქტურაში შედის საფინანსო სექტორი, ენერგეტიკა, სატელეკომუნიკაციო და ძირითადი სახელმწიფო უწყებები და სამსახურები

„ჰორიზონტი 2015“[179]

ბოლო დროს სულ უფრო მეტი ყურადღება ექცევა სამხედრო, უსაფრთხოებისა თუ დაცვის კერძო ორგანიზაციების ჩართვას უსაფრთხოების სექტორის რეფორმირებისა და მართვის პროცესებში. ამ თემაზე უკვე არსებობს დიდი რაოდენობის პუბლიკაციები და მასალა, თუმცა არცთუ ისე ბევრ ნაშრომშია განხილული მოცემული სუბიექტების როლის დიდი მნიშვნელობა სახელმწიფო თუ კერძო სექტორის უსაფრთხოების უფრო ფართო პრობლემების მართვასთან დაკავშირებით. უახლოეს წლებში უნდა მოხდეს ანალიტიკური კვლევების ჩარჩოების გაფართოება და უსაფრთხოების სექტორის რეფორმირებისა და მართვის ახალი მიდგომების შემუშავება. დროა უკვე უარი ვთქვათ მოძველებულ „სახელმწიფო მართვის ერთიან“[180] მიდგომაზე, სადაც მხოლოდ სახელმწიფო სექტორის უწყებები და სამსახურები მონაწილეობენ. აუცილებელი ხდება პრობლემის მიმართ სისტემური მიდგომა, რომელიც უსაფრთხოების სექტორს განიხილავს როგორც ერთიან ორგანიზმს, ხოლო პრობლემის გადაჭრის მასშტაბები სცილდება არსებულ სახელმწიფო ჩარჩოებს და მოიცავს ასევე კერძო თუ საერთაშორისო ორგანიზაციებსაც.

პროექტი „ჰორიზონტი 2015“ ერთმანეთში აერთიანებს დაინტერესებულ სახელმწიფო და არასახელმწიფო სტრუქტურების წარმომადგენლებს, რომელთა შორის იმართება თემატური მრგვალი მაგიდები. ყოველი მსგავსი მრგვალი მაგიდის შემდეგ იქმნება მოცულობითი სამუშაო დოკუმენტი, რომელიც შეიცავს პრობლემის მოკლე აღწერილობას, თეორიულ და პრაქტიკულ საკითხებს, კონტროლისა და ზედამხედველობის მექანიზმებს, რაც ზრდის გამჭვირვალობასა და დემოკრატიულ მმართველობას მთლიანად. თუმცა ეს დოკუმენტები არ იძლევა საკითხის გადაჭრას,

[179] პროექტი ინიცირებულია ორგანიზაცია „შეიარაღებულ ძალებზე დემოკრატიული კონტროლის“ (DCAF) http://www.dcaf.ch/ მიერ 2010 წელს, სადაც ერთ ერთ მნიშვნელოვან პრობლემად განხილულია კიბერუსაფრთხოება http://www.dcaf.ch/Project/Horizon-2015

[180] იგივეა, რაც ცენტრალიზებული მმართველობა, რომლის დროსაც ესა თუ ის პრობლემა გადაიჭრება არა ცალკეული უწყებების მიერ, არამედ მთლიანად სახელმწიფო დონეზე. მსგავსი მიდგომა წარმოიქმნა ამ სფეროში რეფორმირების პირველ ეტაპზე და ამჟამად წარმოადგენს ნაკლებად ეფექტურ საშუალებას, ამიტომ აუცილებელია დაიწყოს რეფორმირების მეორე ეტაპი, რაც მოიცავს ასევე კერძო სექტორის ჩართულობას

ისინი უფრო წამოჭრიან პრობლემას და საფუძველს უდებს სამეცნიერო კვლევების განვითარებას. ანალოგიური პროცესი მიმდინარეობს ასევე კიბერუსაფრთხოების თემების განხილვისას, როცა ასევე მიიღება შესაბამისი დოკუმენტები[181].

რეზუმე

ზემოთ მოკლედ განხილული იყო ევროკავშირის, ევროსაბჭოს, გაეროს, ნატოს, დიდი რვიანისა და სხვა საერთაშორისო თუ რეგიონალური დონის ორგანიზაციების ფარგლებში მიღებული გადაწყვეტილებები, რეკომენდაციები, დირექტივები და რეზოლუციები კიბერუსაფრთხოებაზე, რომელმაც უნდა უზრუნველყოს კიბერსივრცის დაცვა და კიბერდანაშაულთან ბრძოლის ეფექტურობა როგორც საერთაშორისო თუ რეგიონალურ, ისე ეროვნულ დონეებზე.

იანვარი, 2015 წელი

[181] file:///C:/Users/Admin/Downloads/OnCyberwarfare-Schreier.pdf

პარიზის ტერაქტი და ახალი გამოწვევები კიბერსივრცეში

პარიზში, 7 იანვარს ფრანგულ სატირულ ყოველკვირეულ ჟურნალზე Charlie Hebdo - ზე განხორციელებულ ტერაქტს წინ უძღოდა საკმაოდ მასირებული ჰაკერული კიბერშეტევების სერია ფრანგულ კიბერსივრცეზე. ჰაკერების მხრიდან შეტევის ობიექტები გახდნენ როგორც სახელმწიფო ისე კერძო სექტორის და ასევე იმ უცხოური კომპანიების ვებ - გვერდები, რომელთა საქმიანობა სხვადასხვა ფორმით უკავშირდება საფრანგეთსა და ფრანგულ კომპანიებს. კიბერშეტევების რიცხვი კიდევ უფრო გაიზარდა ტერაქტის შემდეგ. კერძოდ, 15 იანვარს abc NEWS, ფრანგი ოფიციალური პირების განცხადებებზე დაყრდნობით, ავრცელებს ინფორმაციას, რომ 7 იანვრის შემდეგ ჰაკერული თავდასხმა განხორციელდა 19, 000 ფრანგულ ვებ - გვერდზე, რაც არ მომხდარა არასდროს და არის პირველი შემთხვევა საფრანგეთის ისტორიაში. იგივე abc NEWS - ის ინფორმაციით, მხოლოდ ბოლო 24 საათის განმავლობაში განხორციელდა დაახლოებით 1, 000 - ზე მეტი შეტევა. ფრანგული ოფიციოზის განცხადებით, ჰაკერულ თავდასხმაში ეჭვმიტანილ ჰაკერულ დაჯგუფებებს შორის არიან: „ახლო აღმოსავლეთის კიბერ არმია“ (the Middle Eastern Cyber Army - MECA), Fallaga Hackers Team და Cyber Caliphate. აღსანიშნავია, რომ ამ უკანასკნელმა 12 იანვარს ერთმანეთის მიყოლებით განახორციელა რამოდენიმე კიბერშეტევა აშშ - ს ცენტრალური სარდლობის Twitter - ისა და YouTube - ს ანგარიშებზე.

აღსანიშნავია, რომ საქართველოს ინტერნეტ - სივრცეც და ქართული დომეინიც იქცნენ ჰაკერების შეტევის ობიექტებად. კერძოდ, 10 იანვარს ფრანგული ჰიპერმარკეტის Carrefour - ის ოფიციალური ვებ - გვერდი http://carrefour.com.ge/ დაჰაკერებული იქნა „ახლო აღმოსავლეთის კიბერ არმიის“ (the Middle Eastern Cyber Army - MECA) მიერ. ვებ - გვერდის გატეხვასთან დაკავშირებით შსს-მ გამოძიება სისხლის სამართლის კოდექსის 284-ე მუხლის 1-ელი ნაწილით დაიწყო, რაც კომპიუტერულ ინფორმაციასთან არამართლზომიერ შეღწევას გულისხმობს. აქვე შეიძლება ავღნიშნოთ, რომ საქართველოს კანონმდებლობა კერძო კომპანიებს არ ავალდებულებს ითანამშრომლონ სახელმწიფოს შესაბამის უწყებებთან, ამ შემთხვევაში იუსტიციის სამინისტროს „სსიპ მონაცემთა გაცვლის სააგენტოსთან“, ინტერნეტ - სივრცის დაცვის საკითხებში, ეს არის მხოლოდ

ნებაყოფლობითი კერძო კომპანიების მხრიდან სურვილის შემთხვევაში, რაც არის ყოვლად მიუღებელი, გამომდინარე, რომ რისკის ქვეშ დგება ქვეყნის კრიტიკული ინფრასტრუქტურა, ობიექტები და ინტერნეტის ნებისმიერი მომხმარებელი. ეს კი პირდაპირ კავშირშია ქვეყნის ეროვნული უსაფრთხოების სენსიტიურ საკითხებთან.

ბოლო წლებში, განსაკუთრებით სირიაში საომარი მოქმედებებისა და ახლო აღმოსავლეთში ე. წ. „ისლამური სახელმწიფოს“ (ISIS) ასპარეზზე გამოსვლის შემდეგ, ერთი - ორად გაიზარდა კიბერშეტევების რიცხვი. ამ მიმართულებით, განსაკუთრებით აქტიურობენ ზემოთ მოცემული ჰაკერული დაჯგუფებები „ახლო აღმოსავლეთის კიბერ არმია“ (the Middle Eastern Cyber Army - MECA), Fallaga Hackers Team და Cyber Caliphate, ასევე „სირიის ელექტრონული არმია“ (SEA).

„სირიის ელექტრონული არმია“ (the Syrian Electronic Army SEA), რომელსაც ასევე ხშირად უწოდებენ „სირიის კიბერ არმიას“ (the Syrian Cyber Army) სირიის პრეზიდენტის ბაშარ ალ - ასადის მხარდაჭერით სარგებლობს. ეს არის არაბულ სამყაროში პირველი ვირტუალური საჯარო არმია (http://sea.sy/index/en), რომლის სამიზნეებია ქვეყნის პოლიტიკური ოპოზიციის წარმომადგენლებისა და დასავლური ვებ - გვერდები. „სირიის ელექტრონული არმიის“ (the Syrian Electronic Army SEA) ჰაკერული თავდასხმის ობიექტები არის BBC News, the Associated Press, National Public Radio, CBC News, Al Jazeera, Financial Times, The Daily Telegraph, The Washington Post, სირიის სატელიტური მაუწყებელი Orient TV და al-Arabia TV. ასევე მობილურის სხვადასხვა VoIP აპლიკაციები, მათშორის Viber და Tango. აღსანიშნავია ისიც, რომ „არმიამ“ განახორციელა არაერთი კიბერშეტევა აშშ - ს პრეზიდენტის ბარაქ ობამასა და თეთრი სახლის, ასევე Human Rights Watch - ის ვებ - გვერდებზე. „სირიის ელექტრონული არმია“ (the Syrian Electronic Army SEA) ამ ეტაპზეც აგრძელებს აქტიურ ჰაკერულ საქმიანობას.

სრულიად უცნობ ჰაკერულ დაჯგუფებას წარმოადგენს „ახლო აღმოსავლეთის კიბერ არმია“ (the Middle Eastern Cyber Army - MECA), რომელიც ასპარეზზე გამოჩნდა გასული 2014 წლის 23 სექტემბერს, როცა მან განახორციელა ჰაკერული თავდასხმები აშშ - ს კიბერსივრცეზე. არ არსებობს არავითარი ინფორმაცია იმის შესახებ, თუ ვინ შეიძლება

იდგეს MECA - ს უკან. თუმცა შეიძლება ითქვას, რომ ეს შეიძლება იყოს როგორც რომელიმე ტერორისტული დაჯგუფება ან სახელმწიფო, ისე კერძო პირი. 15 იანვრის მონაცემებით, „ახლო აღმოსავლეთის კიბერ არმიამ“ (the Middle Eastern Cyber Army - MECA) განახორციელა მასიური შეტევა ნიდერლანდების ვებ - გვერდებზე.

The National Interest - ის ინფორმაციით, Cyber Caliphate უკავშირდება ე. წ. „ისლამური სახელმწიფოს“ (ISIS). თუმცა მის შესახებ ბევრი რამ ცნობილი არ არის. მაგრამ ზოგიერთის ვარაუდით, მოცემული ჰაკერული დაჯგუფების ერთერთი ლიდერი არის ბრიტანელი Junaid Hussain, რომელიც ერთხელ იყო უკვე დაპატიმრებული გაერთიანებული სამეფოს ყოფილი პრემიერ - მინისტრის ტონი ბლერის Gmail - ის ანგარიშის დაჰაკერების გამო. ის ასევე დაკავშირებული იყო ჰაკერთა ჯგუფთან Team Poison, რომელთა მტკიცებით, მათ აქვთ არასანქცირებული წვდომა Blackberry - სა და NATO - ს ქსელებთან, ასევე გაერთიანებული არიან “Anonymous” - თან, საბანკო ანგარიშებზე შეღწევის მიზნით. სხვა წყაროების მიხედვით, Junaid Hussain ახორციელებს ციფრული სფეროს ექსპერტების გადაბირებას სირიისა და ე. წ. „ისლამური სახელმწიფოსთვის“ (ISIS). მოცემული მიმართულების ანალიზი ნათლად აჩვენებს, რომ Cyber Caliphate არის სწრაფად მზარდი ჰაკერული ორგანიზაცია და ექპერტებს მიაჩნიათ, რომ მისი შესაძლებლობები უახლოეს მომავალში გაცილებით დიდი იქნება. ბოლო ერთ თვეში Cyber Caliphate - მა ორჯერ დააჰაკერა Albuquerque Journal - ის, New Mexico’s Mountain View Telegraph - ისა და მერილანდის WBOC 16 TV - ს ვებ - გვერდები, ასევე Twitter. როგორც ზემოთ იყო აღნიშნული, Cyber Caliphate - მა 12 იანვარს ერთმანეთის მიყოლებით განახორციელა რამოდენიმე კიბერშეტევა აშშ - ს ცენტრალური სარდლობის Twitter - ისა და YouTube - ს ანგარიშებზე.

ბოლო დროს კიბერსივრცეში განვითარებული მოვლენები ნათლად აჩვენებს, რომ სულ უფრო აქტიურად ხდება ჰაკერული დაჯგუფებების გამოყენება ტერორისტული ორგანიზაციებისა და მათთან ასოცირებული კერძო პირების მიერ, წარმოებს მათი არასანქცირებული შეღწევა და ჰაკერული თავდასხმები სახელმწიფო თუ კერძო სექტორის ვებ - გვერდებზე, რაც პირდაპირ საფრთხეს უქმნის როგორც ცალკეულ

ორგანიზაციებსა და მომხმარებლებს, ისე მთლიანად საერთაშორისო, რეგიონალურ თუ ეროვნულ უსაფრთხოებას. ვითარებას კიდევ უფრო ართულებს ის გარემოება, რომ დანაშაულებრივ ქმედებებში გამოიყენება უახლესი კომპიუტერული და პროგრამული ტექნოლოგიების მიღწევები.

ერთი - ორი სიტყვით, Charlie Hebdo არის ფრანგული სატირული ყოველკვირეული ჟურნალი, რომელიც ასახავს კარიკატურებს, რეპორტაჟებს, პოლემიკებსა და ხუმრობებს, რომელთაც ნონ - კონფორმისტული სტილი აქვთ. აქვეყნებს სტატიებს რელიგიის, პოლიტიკის, კულტურისა და სხვა საკითხების შესახებ. ჟურნალი დაარსდა 1970 წელს როგორც ჟურნალ „ჰარა-კირის“ მემკვიდრე, რომელიც საფრანგეთის მთავრობამ 1969 წელს დახურა შარლ დე გოლის შესახებ უხამსი კარიკატურების ბეჭდის გამო. ჟურნალი გამოდის ყოველ ოთხშაბათს და მისი ტირაჟი შეადგენდა დაახლოებით 50 ათას ეგზემპლარს. ჟურნალი ცნობილი გახდა წინასწარმეტყველ მუჰამედის კარიკატურებთან დაკავშირებული სკანდალით 2006 წელს, როდესაც იმავე წლის თებერვალში გამოქვეყნდა მუჰამედის კარიკატურები, რომელმაც ფართო პროტესტი გამოიწვია მუსლიმურ სამყაროში. ამის შემდეგ რედაქცია მუდმივად ღებულობდა თავისი მისამართით მუქარას. თუმცა ყველაფრის მიუხედავად, გამომცემლობის ყველაზე ცნობილი კარიკატურისტები აგრძელებდნენ თავიანთი ნახატების გამოქვეყნებას, რომელიც მიმართული იყო მსოფლიოს სხვადასხვა ადგილებში მოღვაწე რელიგიური ფანატიკოსების წინააღმდეგ. პირველი ტერორისტული შეტევა გამომცემლობაზე განხორციელდა 2011 წელს, როცა ნოემბერში ჟურნალმა „შარლი ებდომ“ გამოუშვა ნომერი სახელწოდებით „შარიათ ებდო“. ჟურნალის ეს ნომერი გავრცელდა 400, 000 ეგზემპლარით და ტუნისელი ისლამისტების გამარჯვებას მიეძღვნა. ნომრის გამოსვლისთანავე ღამით რედაქციის შენობა მთლიანად დაიწვა, ვინაიდან უცნობმა პირებმა შენობას დაუშინეს ბოთლები ცეცხლგამჩენ ნივთიერებებთან ერთად. ინციდენტის შედეგად არავინ არ დაშავებულა.