ინფორმაციული უსაფრთხოების
ხვლევებისა და ანალიზის ცენტრი

კიბერ რეპორტი 2008 - 2010

აგვისტოს მოვლენებიდან დღემდე

დამა ჯაფარიძე

საავტორო უფლებები

ავტორისაგან

მოცემული პუბლიკაცია წარმოადგენს 2008 წლის აგვისტოს რუსეთ-საქართველოს ომის დროს განვითარებული მოვლენების კიბერ ანალიზს, რომელიც ამ მასშტაბითა და ფორმით პირველად იქნა შესწავლილი ლოკალურად. რაოდენ პარადოქსულიც არ უნდა იყოს, ამ მოვლენებზე უცხოური პრესის წარმომადგენლები და ექსპერტები უფრო ბევრს საუბრობენ და მეტ ყურადღებას უთმობენ მათ ვიდრე ჩვენ, საქართველოში. მოცემულ ანგარიშში ასევე იქნება განხილული ის დამოკიდებულება, რომელიც ამ საკითხების მიმართ არსებობს საზოგადოებასა და სხვადასხვა წრეებში; ასევე საკანონდმებლო ხარვეზები ინფორმაციული უსაფრთხოების საკითხებში; ინფრასტრუქტურული პრობლემები და ინფორმაციული ვაკუუმი, რომელიც ომმა შექმნა. სწორედ ამ ინფორმაციული სიცარიელის შესავსებად, საზოგადოების მეტი ინფორმირებისთვის და სათანადო ინსტიტუციური მექანიზმების შექმნის წასახალისებლად ჩამოყალიბდა ორგანიზაცია, რომელიც ამ სფეროში პირველია კავკასიის რეგიონში - ინფორმაციული უსაფრთხოების კვლევებისა და ანალიზის ცენტრი. იგი წარმოადგენს პირველ და დღესდღეობით ერთადერთ ორგანიზაციას საქართველოში, რომელიც უშუალოდ მუშაობს ინფორმაციული უსაფრთხოების საკითხებზე და ნერგავს უამრავ ინოვაციას როგორც კერძო, ისე სახელმწიფო სექტორში.

თემები

კიბერ ომის ქრონოლოგია

2008 წლის აგვისტოს, როდესაც მსოფლიო შოკირებული იყო რუსეთის აგრესიით საქართველოს წინააღმდეგ, ბრძოლის ასპარეზზე გამოჩნდნენ XXI საუკუნის ახალი ტიპის მეომრები, ახალი იარაღითა და კოლოსალური შესაძლებლობებით. მთელი ამ ომის პარალელურად, გაიმართა კიდევ ერთი უმნიშვნელოვანესი ბრძოლა კიბერსივრცესა და მედიაში – კიბერ ომი. სოციალურ ქსელებსა და მედიაში ჰაკერები და სხვადასხვა სპეცსამსახურების თანამშრომლები ყველა რესურსს იყენებდნენ საკუთარი ინტერესების დასაცავად. ეს ყველაფერი ომამდე გაცილებით ადრე დაიწყო. რუსეთი ცდილობდა შესაბამისი ფონი შეექმნა და ამისათვის ყველაზე ეფექტური საშუალებაც გამონახა – სოციალური ქსელები, მედია და ზოგადად ინტერნეტი. ომის პირველი სიმპტომები მალევე ვიგრძენით. მასიური კიბერ შეტევები განოხრციელდა ერთდროულად რამოდენიმე მნიშვნელოვან ობიექტზე.

კიბერ შეტევა განხორციელდა საქართველოს საგარეო საქმეთა სამინისტროს ოფიციალურ პორტალზე. ზიანი სხვა ელექტრონულ რესურსებსაც მიაყენეს. მათ შორის საქართველოს ეროვნული ბანკისა და პრეზიდენტის ვებ-გვერდებს. ჰაკერებმა ასევე სცადეს საქართველოს საკომუნიკაციო და სატრანსპორტო ელექტრონულ ინფრასტრუქტურაზე შეტევა, ისევე როგორც შეტევები ძალოვანი უწყებების ელექტრონულ ინფრასტრუქტურაზე. თუმცა საბედნიეროდ, მათ ვერ შეძლეს ბოლომდე მიეღწიათ მიზნისათვის და გამოეყვანათ მწყობრიდან ქვეყნის სასიცოცხლოდ მნიშვნელოვანი ობიექტები.

კიბერ შეტევები საქართველოს წინააღმდეგ იმგვარად იყო ორგანიზებული, რომ ობიექტები პრიორიტეტების მიხედვით გადანაწილდა და ქრონოლოგიაც პარალელურ მოვლენებს ემთხვეოდა. შეტევის ძირითად ობიექტებს წარმოადგენდნენ:

www.president.gov.ge - საქართველოს პრეზიდენტის ვებ-გვერდი

www.government.gov.ge - საქართველოს მთავრობის ვებ-გვერდი

www.parliament.ge - საქართველოს პარლამენტის ვებ-გვერდი

www.nsc.gov.ge - უშიშროების ეროვნული საბჭოს ვებ-გვერდი

www.constcourt.gov.ge - საქართველოს საკონსტიტუციო სასამართლო

www.supremecourt.ge - საქართველოს უზენაესი სასამრთლო

www.cec.gov.ge - ცენტრალური საარჩევნო კომისია

www.nbg.gov.ge - საქართველოს ეროვნული ბანკი

www.nplg.gov.ge - საქართველოს პარლამენტის ეროვნული ბიბლიოთეკა

www.police.ge - შინაგან საქმეთა სამინისტრო

www.mod.gov.ge - თავდაცვის სამინისტრო

www.mes.gov.ge - განათლების სამინისტრო

www.mfa.gov.ge - საგარეო საქმეთა სამინისტრო

www.iberiapac.ge - დაცული ელექტრონული ფოსტის სერვისი

www.mof.ge - ფინანსთა სამინისტროს ვებ-პორტალი

www.newsgeorgia.ru - ახალი ამბები საქართველოს შესახებ

www.apsny.ge - საინფორმაციო ანალიტიკური პორტალი "Грузия Online"

www.nukri.org - ვებ-გვერდი აფხაზეთის შესახებ

www.opentext.org.ge - ქართული პრესის ელექტრონული არქივი

www.messenger.com.ge - ინგლისურ ენოვანი პოპულარული ქართული ჟურნალი

www.abkhazia.gov.ge - აფხაზეთის ავტონომიური რესპუბლიკის ვებ-გვერდი

www.naec.gov.ge - გამოცდების ეროვნული ცენტრი

www.forum.ge - ერთ-ერთი უმსხვილესი ქართული ფორუმი

www.civil.ge - საინფორმაციო რესურსი

www.presa.ge - ახალი ამბები ქართული პრესიდან

www.rustavi2.com - სამაუწყებლო კომპანია რუსთავი2-ის ვებ-გვერდი

www.news.ge - ინგლისურენოვანი საინფორმაციო პორტალი საქართველოზე

www.interpress.ge - საინფორმაციო პორტალი

www.tbc.ge - თიბისი ბანკის ვებ-გვერდი

www.tbilisiweb.info - საინფორმაციო პორტალი

www.newsgeorgia.ru - ახალი ამბების გვერდი

www.os-inform.com - საინფორმაციო სააგენტო "ოსინფორმი"

www.kasparov.ru - ცნობილი რუსული ოპოზიციური პარტიის ვებ-გვერდი

რათქმაუნდა ეს არ არის სრული სია, თუმცა საკმარისია იმისთვის რომ მივხვდეთ თუ რა დატვირთვა ქონდა რუსულ კიბერ შეტევებს, რომელსაც ზოგი უპასუხისმგებლო ადამიანი უბრალო კომპიუტერულ ხულიგნობად აფასებდა, რომელსაც ვითომდა კავშირი არ ქონდა ომის მოვლენებთან.

ქვეყნის გათიშვის მცდელობა

ამგვარად გაჩნდა ახალი ბრძოლის ველი. ასეთ კრიტიკულ სიტუაციაში, როდესაც მოსახლეობა ყოველ წუთს ელოდა ინფორმაციას. როდესაც ხალხი პანიკამდე მივიდა და წარმოიშვა შიდა დესტაბილიზაციის საშიშროება, სანდო ინფორმაციის ოპერატიულად მიწოდებას განსაკუთრებული მნიშვნელობა ქონდა. საქართველოს საგარეო საქმეთა სამინისტროს ვებ-გვერდის მწყობრიდან გამოსვლის გამო, ქვეყნის მთავარ დიპლომატიურ უწყებას ისღა დარჩენოდა, რომ ვებ-გვერდზე განსათავსებელი ინფორმაცია საინფორმაციო სააგენტოების საშუალებით გაევრცელებინა.

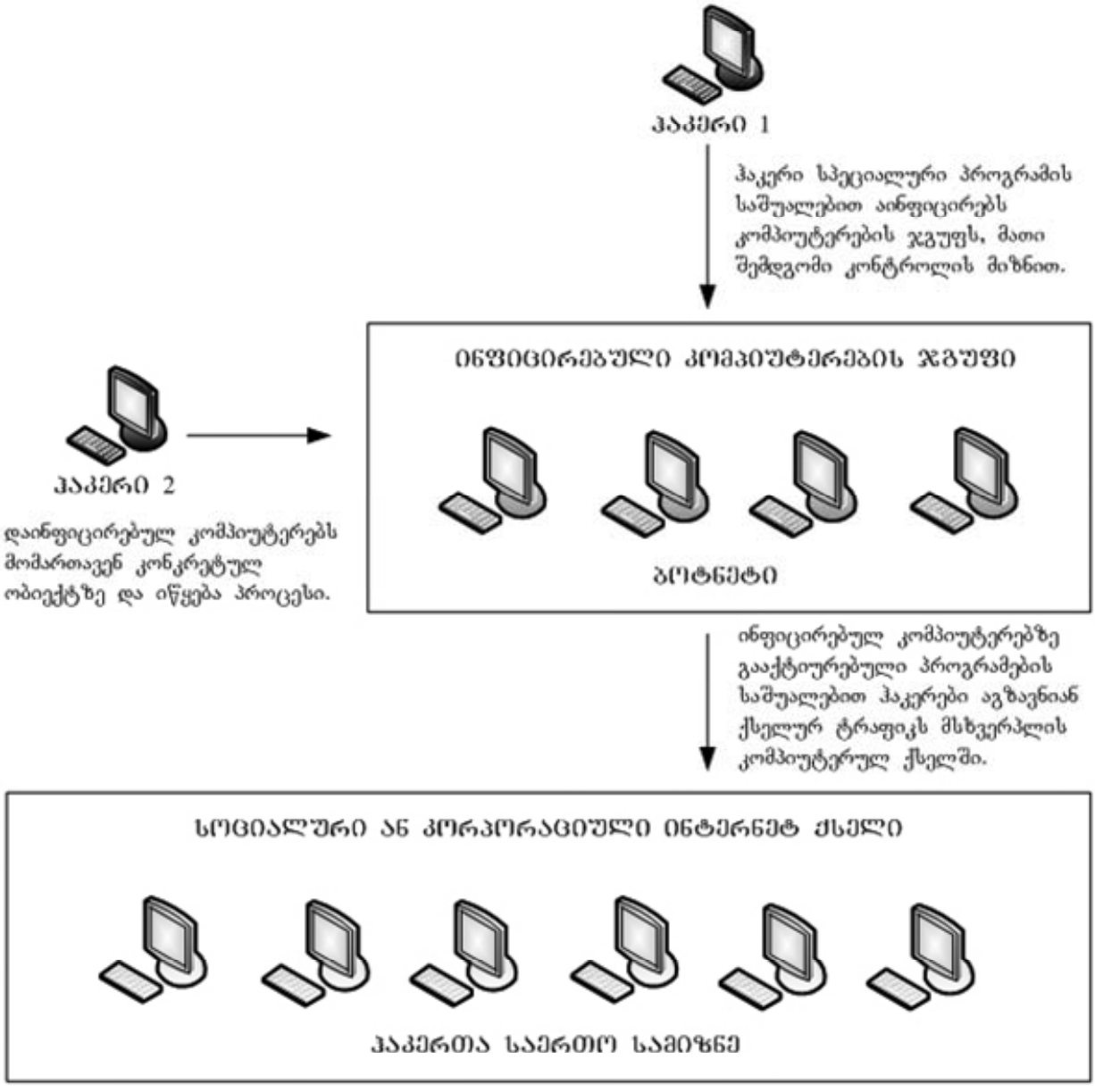
ხარვეზი სამინისტროს ვებ-გვერზე მხოლოდ ორი დღის შემდეგ აღმოიფხვრა, მაგრამ ეს არ ყოფილა ერთადერთი პრობლემა. ამის პარალელურად დაიბლოკა ქართული საინფორმაციო ელექტრონული რესურსები, სოციალური ქსელები და სახელმწიფო დანიშნულების მრავალი ელექტრონული ობიექტი. რუსეთი საკუთარ აგრესიულ მოქმედებებში ფოკუსირებული იყო შეტევებზე ქვეყნის სასიცოცხლო ინფრასტრუქტურის წინააღმდეგ. იგი მთელი ძალებით ცდილობდა "ქვეყანა გაეთიშა".

ეს არ ყოფილა სპონტანური გადაწყვეტილება, რადგან რუსული სპეცსამსახურების კიბერ მოქმედებები კარგად დაგეგმილი სტრატეგიის ნაწილი იყო, რომლის მიხედვითაც მათ უნდა გაენეიტრალებინათ მოწინააღმდეგის ყველაზე საშიში იარაღი – ინფორმაციის გავრცელების საშუალებები. და მართლაც, თუ გავაანალიზებთ იმას თუ როგორ განვითარდა სიტუაცია ნათლად ჩანს, რომ ომის შეჩერება მოხერხდა არა იმდენად სამხედრო ძალით, რამდენადაც ინფორმაციის დროული გაცვლით, რასაც თავისმხრივ მოყვა შემდგომი მხარდაჭერა ქვეყნის გარედან. ეს მხარდაჭერა კიდევ უფრო ძლიერი შეიძლებოდა ყოფილიყო უკეთესი ინფრასტრუქტურა რომ გვქონოდა და უკეთ რომ შეგვძლებოდა ფუნქციონირება ფორს მაჟორულ სიტუაციაში. ასეთი პატარა ქვეყნისთვის სასიცოცხლოდ მნიშვნელოვანია კრიტიკულ სიტუაციებში ინფორმაციის გავრცელების საშუალება, როგორც ქვეყნის შიგნით, ისე მის ტერირტორიებს

გარეთ. სწორედ ამიტომ მათ პრიორიტეტულ მიზანს წარმოადგენდა საჯარო ინსტიტუტების (სამთავრობო, საპარლამენტო, ძალოვანი და სხვა) ინფრასტრუქტურის მოშლა, ასევე მედია და კერძო სექტორის ინფრასტრუქტურის მწყობრიდან გამოყვანა, რათა შექმნილიყო მაქსიმალურად ქაოტური მდგომარეობა. მათ ასევე განახორციელეს შეტევა ქსელურ ინფრასტრუქტურაზე და ამ სერვისების მომწოდებლებზე (ინტერნეტ პროვაიდერები, მობილური და საკომუნიკაციო ოპერატორები). რაც შეეხება კიბერ დაპირისპირებას, რომელშიც რუსეთი კიდევ უფრო არაპროპორციული ძალით დაგვიპირისპირდა ვიდრე ეს სამხედრო ძალებით განახორციელა, მიუხედვად მისი მასშტაბისა განსაკუთრებულ ტექნოლოგიურ ინოვაციურობას ადგილი არ ქონია. მისი მასშტაბურობა იმითაა გამოწვეული, რომ ერთდროულად დიდი რაოდენობის ადამიანური რესურსი იყო მობილიზებული. სწორედაც, რომ ჩვეულებრივი ადამიანები და არა ამ სფეროს სპეციალისტები. რათქმაუნდა იყვნენ ჰაკერებიც და ექსპერტებიც, მაგრამ ისინი ხშირ შემთხვევაში საორგანიზაციო საკითხებს უფრო ითავსებდნენ. ამ რესურსს ჭირდებოდა მართვა. ალბათ იკითხავთ თუ როგორ შეეძლოთ ჩვეულებრივ ადამიანებს ასეთი ოპერაციების ჩატარება – სწორედ ამას მოიცავდა ზემოთ ნახსენები საორგანიზაციო საკითხები. – მთელი საიდუმლო სწორი ტექნოლოგიის შერჩევაშია, რომელიც არსებული სიტუაციის ოპტიმალურ გამოყენებას გულისხმობს. მოდით განვიხილოთ ჩვენი მხარე. ასეა თუ ისე, რუსეთთან შედარებით საქართველოში ბევრად მცირეა ტექნიკური სპეციალისტების რაოდენობა. ეს ბუნებრივიცაა რადგან, რუსეთის მოსახლეობა რაოდენობრივად ბევრად აღემატება ჩვენსას. როგორც ზემოთ აღინიშნა ამ სფეროში არსებული უახლესი ტექნოლოგიური მიღწევები მაინც და მაინც არ გამოყენებულა. ეს იმიტომ, რომ როდესაც საქმე დიდი რაოდენობის ადამიანურ რესურსთან გვაქვს, არსებობს მხოლოდ რამოდენიმე ტექნოლოგიური სტრატეგია, რომელიც ამ რესურსის ოპტიმალურად გამოიყენების საშუალებას იძლევა.

კიბერ დაპირისპირება

კიბერ შეტევის ყველაზე გავცელებული მოდელის მიხედვით ჰაკერების მცირე ჯგუფი ორგანიზებას უწევს მთელ დანარჩენ რესურსს და თითოეულ კომპიუტერს მასში ანიჭებს ცალკეული იარაღის ფუნქციას. ამ სტრატეგიას "ბოტნეტის" შეკვრა ეწოდება.



მსხვერპლის კომპიუტერული ქსელი ავტომატურად ამუშავებს მიღებულ ინფორმაციას და რაკი ეს უკანასკნელი კოლოსალური მოცულობისაა სისტემა იტვირთება, რაც იწვევს საერთო გაუმართაობას.

როგრც წესი კომპიუტერების უმრავლესობა ეკუთვნით ჩვეულებრივ მომხმარებლებს, რომლებსაც ხშირად წარმოდგენაც არ აქვთ რა ხდება მათ კომპიუტერებში. ჰაკერები ახერხებენ ამგვარ კომპიუტერებში შეღწევას და მათში საკუთარი პროგრამის გააქტიურებას. მას შემდეგ რაც პროგრამა გააქტიურდება კომპიუტერზე ის უკვე დამოუკიდებლად იღებს მართვას და ავტონომიური ხდება. ამგვარი პროგრამები შენიღბულად მოქმედებენ. ყველა ეს ცალკეული ინსტრუმენტი მოქცეული ერთ მთლიანობაში დიდი ძალის მქონე იარაღად იქცევა. ტექნოლოგიურად ეს ასე გამოიყურება: რომელიმე ქსელში ხდება კიბერ გაერთიანების შეკვრა, რომელშიც თითოეული კომპიუტერი ახორციელებს არჩეული საერთო ობიექტის მაქსიმალურ დატვირთვას. ანუ ე.წ. გადაჭარბებული "ტრაფიკის" (ქსელური ინფორმაციის) მიწოდებას. მსხვერპლის კომპიუტერს უწყვეტად ეგზავნება დიდი მოცულობის ინფორმაცია, რომელსაც იგი ავტომატურად ამუშავებს და ასე გრძელდება მანამ კომპიუტერი მწყობრიდან გამოვა. ამ სქემის ყველაზე გავრცელებული ოპერაცია Ping-ის გამოყენებაა. ამ დროს, რაც უფრო მეტი კომპიუტერი ახორციელებს ობიექტის ერთდროულ "დაპინგვას", მით მეტად იტვირთება იგი და როდესაც დატვირთვის მაქსიმალურ დონეს აღწევს, სისტემა მწყობრიდან გამოდის. ტექნიკურად "დაპინგვა" არის ძალზედ მარტივი ქსელური ოპერაცია. მისი მეშვეობით როგორც წესი, მოწმდება კავშირი გარკვეულ ქსელურ ობიექტთან. ამ დროს იგზავნება ბიტების გარკვეული რაოდენობა და პასუხის მიხედვით დგინდება კავშირის მდგომარეობა. დაპინგვის პროცედურა ძალიან მარტივია. ცალკეული დაპინგვისას საჭიროა მომხმარებელმა გამოიძახოს სპეციალური პროგრამა "Command Promt", რომელშიც მან შესაბამისი ბრძანება უნდა აკრიფოს. დაახლოებით ასე: ping www.dezinformaciulisaiti.ru (მაგალითი) და დაპინგვის ყოველი ოპერაციის დასრულების შემდეგ, კვლავ გაიმეოროს იგივე ბრძანება მინიმალური ინტერვალით. კომპიუტერის მომხმარებლების უმრავლესობისთვის ეს შეიძლება სირთულეს წარმოადგენდეს. თანაც მისი ერთჯერადი განხორციელება საკმარისი არ არის და მხოლოდ უმნიშვნელო ეფექტს იძლევა. ასეთ დროს საჭიროა პროცესის სრული ავტომატიზება. რისთვისაც იდეალური გადაწყვეტაა მსუბუქი და მარტივი პროგრამების დაწერა, რომლებსაც კიბერ დაჯგუფების წევრებს უგზავნიან და ისინი ააქტიურებენ მას. ერთ-ერთი ასეთი მცირე პროგრამის ფრაგმენტი, რომელიც გამოიყენებოდა კიბერ დაჯგუფებების მიერ აგვისტოს ინფორმაციული ომის დროს:@echo offSET PING_COUNT=50SET PING_TOMEOUT=1000:PINGecho vpingavt rusul serverebsping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% "აქ

რაც შეეხება რუსულ მხარეს, მათ ამას უფრო ორგანიზებული სახე მისცეს და კომპილირებული პროგრამები დაუგზავნეს კიბერ ხულიგნებს. ეს პროგრამაც იგივე ფუნქციას ასრულებდა და ასე გამოიყურებოდა

რეპორტში სპეციალურად მხოლოდ რამოდენიმე კონკრეტული მაგალითია მოყვანილი, ცხადია იყო გაცილებით რთული სქემებიც. ამ და სხვა ოპერაციების უფრო მეტი დეტალიზაცია არ იქნებოდა სწორი თუ გავითვალისწინებთ რა შეიძლება მოყვეს მის ბოროტად გამოყენებას. ჰაკერული ტექნოლოგიები გარკვეულ დონეზე კომპიუტერის დამწყები მომხმარებლებისთვისაც კი გახდა ხელმისაწვდომი. მათაც შეუძლიათ გარკვეული ოპერაციების განხორციელება. საშიში თითქოს არაფერია, მაგრამ როდესაც ასეთი მომხმარებლების დიდ რაოდენობასთან გვაქვს საქმე, იგი უკვე სერიოზულ საფრთხედ განიხილება.

ომი რომელიც პრეცედენტად იქცა

დავიწყოთ დროებით ტექნიკური მხარე და მივუბრუნდეთ კონფლიქტს. მთელი მსოფლიო ჩაება ინფორმაციულ ომში, რომელმაც სოციალური ქსელის ყველა კომპონენტი მოიცვა. მულტიმედია ვიდეო პორტალებით დაწყებული სადისკუსიო ფორუმებით დამთავრებული მიდიოდა გააფთრებული ომი პროპაგანდისტებსა და იმ ადამიანებს შორის, ვისაც სურდა ჯანსაღი, ობიექტური ინფორმაციის მიწოდება მსოფლიოსათვის. დეზინფორმატორების ორგანიზებულობამ განაპირობა ის, რომ ჩვენ წავაგეთ ინფორმაციული ბრძოლა. მიუხედავად იმისა, რომ მასში ყველა ჩაება ვისაც კი წვდომა ქონდა ინტერნეტთან. ყველა თავისებურად ცდილობდა დაეცვა საკუთარი ქვეყნის ინტერესები. ცდილობდნენ ეჩვენებინათ დანარჩენი მსოფლიოსათვის თუ რა ხდებოდა სინამდვილეში - არაპროპორციული დაპირისპირება, უსამართლო აგრესია და რუსეთის ნამდვილი სახე. ჩვენ წავაგეთ ბრძოლა, მაგრამ არა ომი, რადგან ინფორმაციულ ეპოქაში შეუძლებელია დიდ ხანს შენიღბო ტყუილი და ბუნებრივია მოგვიანებით ყველაფერი ცხადი გახდა. ყველა საუბრობდა ამ ომზე, თუმცა ძირითადად პოლიტიკურ და დიმპლომატიურ ჭრილში, რადგან მრავალი ფაქტი მოგვიანებით გახდა ცნობილი და მრავალსაც ანალიზისათვის დრო ჭირდებოდა. სამწუხაროა რომ ჩვენი ქვეყნის დიპლომატიურმა წრეებმა იმ მომენტში ვერ მოახერხეს გამოეყენებინათ ძალიან კარგი შესაძლებლობა მიენიჭებინათ ამ მოვლენებისთვის კიბერ ომის სტატუსიც. რაც არ უნდა დაუჯერებლად ეღერდეს მსოფლიო პრაქტიკაში ეს იყო დღემდე ცნობილი ერთადერთი შემთხვევა, რომელსაც შეიძლებოდა მინიჭებოდა კიბერ ომის

სტატუსი. რათქმაუნდა არსებობს კიბერ კონფლიქტების სხვა მასშტაბური პრეცედენტებიც, როგორც მაგალითად დანიაში 2006 წელს, ესტონეთში 2007-ში, ლიტვაში 2008 წელს და ირანშიც კი 2009 წელს, მაგრამ მათ არ ქონდათ შესაბამისი სამართლებრივი ბაზა, რათა კიბერ ომის სტატუსი მიენიჭებინათ ამ მოვლენებისთვის, რადგან არსებობს მხოლოდ ორი გზა ამისათვის: პირველი არის სწორედ შესაბამისი სამართლებრივი ბაზის ქონა, ხოლო მეორე მყარი არგუმენტაცია. ეს უკანასკნელი კი ჩვენს შემთხვევაში საკმარისად გვქონდა. ამის სამართლებრივი არგუმენტი იყო ის, რომ რუსეთი საქართველოსთან აწარმოებდა რეალურ, კონვენციურ ომს, ხოლო კიბერ ომი, იყო ერთ-ერთი პარალელური პროცესი. ეს არის ერთ-ერთი გამოუყენებელი მომენტი თუ შეიძლება ამას ასე ეწოდოს. პრობლემაც ალბათ ტექნიკური ხასიათის უფრო იყო, რადგან ისევ და ისევ ამ სფეროს სპეციალისტების დეფიციტმა, არასაკმარისმა ინტერესმა ამ საკითხის მიმართ თუ კვალიფიკაციის არ არსებობამ გამოიწვია ის, რომ ვერავინ ურჩია დიპლომატიურ უწყებას სათანადო რეაგირება მოეხდინა ამ კუთხით. ეხლა ეს სამწუხაროდ უკვე დაგვიანებულია. ამგვარი ფაქტები ჩნდება ხანგრძლივი ანალიზის ან უბრალოდ დროის გავლის შემდეგ. დრო გადის, მაგრამ ამ თემისადმი აქტუალობა არ იკარგება. აგვისტოს მოვლენების პასიურ ფაზაში გადასვლიდან დაიწყო ერთგვარი ღია ანალიტიკური ციკლიც.

სულ მალე გამოჩნდა პუბლიკაციები ჩვენი ინფორმაციული ომის შესახებაც.

ერთ-ერთი ასეთი საინტერესო სტატია მოამზადა "Computerworld"-ის ცნობილმა მიმომხილველმა Greg Kaiser-მა, სადაც მან საინტერესო პარალელები გაავლო ესტონეთში მომხდარ ანალოგიურ მოვლენებთან და მოიყვანა სხვადასხვა სააგენტოს მონიტორინგის შედეგები. ესტონეთის შემთხვევა მართლაც ძალიან ახლოს იყო და დღემდე ახლოს არის ჩვენს სიტუაციასთან. ჩვენ ბევრი შეგვიძლია ვისწავლოთ მათგან, რადგან თავად ისინი დღემდე სწავლობენ ჩვენს მაგალითზე. საქართველო-რუსეთს შორის გამართული კიბერ ომი და შემდგომი მოვლენები იქცა ერთ-ერთ ყველაზე აქტუალურ თემად კიბერ უსაფრთხოების საერთაშორისო საექსპერტო წრეებსა და ინსტიტუტებში. დაიწერა უამრავი სტატია, გამოქვეყნდა სხვადასხვა ნაშრომი და სახელმძღვანელო სპეციალურად ამ მოვლენებზე

დაყრდნობით. ეს აქტუალობა აბსოლიტურად ბუნებრივია, რადგან ამგვარი ფაქტები შესანიშნავ მასალას წარმოადგენენ გაანალიზებისათვის და შემდგომი პრევენციული მექანიზმების შესამუშავებლად. უცნაური კი ის არის, რომ ეს აქტუალობა ჩვენი ქვეყნის გარეთ უფრო იყო და არის, ვიდრე მის შიგნით. ჩვენს მაგალითზე სხვები სწავლობენ, ჩვენ კი აქამდე ამაზე ბევრი არაფერი გვითქვამს. სწორედ ეს რეპორტი, გახლავთ თუნდაც ის დაგვიანებული სათქმელი, რამაც უნდა დაგვანახოს ახალი რეალობა. ესტონეთში მომხდარ ცნობილ კიბერ შეტევების მასშტაბი იმის ნახევარიც არ ყოფილა, რაც ჩვენთან მოხდა. ესტონეთი კი ამ ინციდენტების შემდეგ იმდენად დაიხვეწა ამ მიმართულებით, რომ ერთ-ერთ წამყვან ქვეყანად იქცა ინფორმაციული უსაფრთხოების სფეროში. მათ სწორად გაანალიზეს მომხდარი ფაქტები და საპასუხოდ შექმნეს მთელი ინფრასტრუქტურა, ახალი ინსტიტუციური მექანიზმები, დახვეწეს და გადაახალისეს საკანონმდებლო ბაზა, ჩამოაყალიბეს სასწავლო პროგრამები. ერთი სიტყვით მათ ეს გაკვეთილი, მართლაც გაკვეთილად მიიღეს და საშინაო დავალებაც უმაღლეს ქულაზე მოამზადეს.

კიდევ ერთი საინტერესო გამოხმაურება მოყვა ინფორმაციულ ომს გაზეთ “New York Times”-ში, რომელიც კიდევ უფრო მნიშვნელოვანია თუ გავითვალისწინებთ მისი ავტორის ვინაობას - ჯონ მარკოფი. იგი დაკავშირებულია სკანდალური ჰაკერის, კევინ მიტნიკის ისტორიასთან და ერთ-ერთი ყველაზე პოპულარული მიმომხილველია ტექნილოგიურ საკითხებში. ეს მოვლენები თავიდანვე განსაკუთრებით აქტუალური იყო და მრავალი საინტერესო გამოხმაურება მოყვა მსოფლიოს სხვადასხვა წერტილიდან. ამგვარი მასშტაბის ფაქტები იშვიათად ხდება და ამიტომ არსებითად მნიშვნელოვანია მათი დეტალური შესწავლა, უკეთესი თავდაცვითი მექანიზმების შემუშავების მიზნით. სწორედ ამიტომ იყო ეს საკითხი ასეთი აქტუალური. ახლა როცა ომს წარსულ ფორმატში ვაანალიზებთ ცხადი ხდება მრავალი რამ. როგორც ძლიერი მხარეები, ისე სისუსტეები, რომლებზედაც საჭიროა მეტი მუშაობა. ის არაორგანიზებულობა ინფორმაციულ ომში, ის დაბნეულობა ექსტრემალურ სიტუაციაში, რომელიც ქვეყანაში იყო ისედაც მძიმე დროს, არის შედეგი იმისა, რომ არ არსებობდა ინფორმაციული უსაფრთხოების ერთიანი ჩამოყალიბებული პოლიტიკა და შესაბამისი დონის ინფრასტრუქტურა. შესაბამისად არ იყო სათანადო დონეზე განვითარებული ინსტიტუტები რომლებიც ამ პრობლემებს გადაჭრიდნენ. გარდა უსაფრთხოების პოლიტიკისა, მნიშვნელოვანია საზოგადოებრივი აზრიც მის გარშემო. პრობლემებზე ღია საუბარი მათი გადაჭრის საუკეთესო დასაწყისია, ხოლო წარსული შეცდომების დანახვა უკეთესი მომავლის პერსპექტივაა.

ინფორმაციული ომი სოციალურ ქსელებში

აგვისტოს ომის ზუსტად ერთი წლის თავზე მოხდა მორიგი სკანდალი ინტერნეტ სივრცეში. 2009 წლის 7 აგვისტოს განხორციელდა მძლავრი და მასშტაბური შეტევა მსოფლიოს წამყვან სოციალურ ქსელებზე, როგორებიცაა Twitter, Facebook და სხვები. ამ ფაქტმა მსოფლიო აალაპარაკა. რაც მთავარია ეს მოვლენა ისევ და ისევ საქართველოს უკავშირდება. შეტევის ობიექტი პროქართული "ბლოგერი", მეტსახელად "Cyxymu" იყო. მიზეზი კი რუსეთისთვის გამაღიზიანებელი ფაქტების გამოქვეყნება იყო. ექსპერტების აზრით, ეს არ იყო უბრალოდ ჰაკერთა დაჯგუფების მიერ ორგანიზებული, არამედ იგი უფრო წააგავდა სპეცსამსახურის დონეზე განხორციელებულ დივერსიას. ამ ფაქტზე მალევე გაჩნდა მრავალი გამოხმაურება და სხვადასხვა სააგენტოს ანგარიში. ერთ-ერთ ასეთ გამოცემაში კომპანია F-Secure-ის ანალიტიკოსმა მიკო ჰიპონენმა (Mikko Hyponnen) საინტერესო ციტატა მოიყვანა: "სოციალურ ქსელებზე ჰაკერული თავდასხმა ეს იგივეა, სატელევიზიო სადგური რომ დაბომბო, მხოლოდ იმიტომ, რომ მისი რომელიმე წამყვარნი არ მოგეწონათ". რასაც ალბათ ბევრი დაეთანხმება. ალბათ ეს ფაქტი არ დარჩება გამოუძიებელი საერთაშორისო დონეზე და რათქმაუნდა არც უკანასკნელი იქნება. უფრო მეტიც, ყოველდღიურად ხორციელდება ათასობით კიბერ შეტევა და საფრთხის ქვეშ არის ძალზედ სენსიტიური ინფორმაცია და მთელი ინფრასტრუქტურა. ინფორმაციული ომი არასოდეს დამთავრდება, იგი მხოლოდ ტრანსფორმაციას განიცდის და ისეთ ფორმას იღებს, რომელიც ადეკვატურია კონკრეტული მომენტისთვის. ინტერნეტი დინამიური ცნებაა და მუდმივად ვითარდება. ამიტომაც მნიშვნელოვანია, რომ შეგვეძლოს სწრაფი ადაპტირება. 2008 წლის 23 სექტემბერს საქართველოს პრეზიდენტმა, მიხეილ სააკაშვილმა გაეროს გენერალური ასამბლეის 63-ე ყოველწლიურ სხდომაზე განცხადება გააკეთა, სადაც რუსეთის აგრესიაზე საუბრისას აღნიშნა, რომ ეს იყო ერთ-ერთი ყველაზე მასშტაბური კიბერ ომი. ციტატა: "ჩვენ გამოვცადეთ კიბერ ომის პირველი სრულმასშტაბიანი კამპანია, კამპანია, რომელიც მიზნად ისახავდა ჩემი ქვეყნის ეკონომიკის განადგურებასა და გარე სამყაროსთან კომუნიკაციის შესაძლებლობის შეწყვეტას. ეს ძალზე აღმაშფოთებელია, როდესაც ხედავ ტექნოლოგიას, რომელმაც გაგვაერთიანა მთელი მსოფლიო და ასევე დაგვეხმარა კულტურის შეკავშირებაში, და რომელიც იქნა გამოყენებული იმისათვის, რომ ეთნიკური ნიშნის მიხედვით დაყოფილ იქნას ხალხი და გახლეჩილი იქნას ჩვენი მსოფლიო."

სახელმწიფოსთვის ინფორმაციული უსაფრთხოების მძლავრი ინსტიტუტები ისეთივე მნიშვნელოვანია, როგორც ფიზიკური დაცულობა. საჭიროა სწორი ხედვა და პრიორიტეტები, უსაფრთხოება კი მათგან უმთავრესია, რომელსაც ინფორმაციულ ეპოქაში განვითარებული ქვეყნები ახალი მეთოდებით იცავენ.

ორგანიზაციის შესახებ

ინფორმაციული უსაფრთხოების კვლევებისა და ანალიზის ცენტრი წარმოადგენს კავკასიის რეგიონში პირველ და დღესდღეობით ერთადერთ ორგანიზაციას, რომელიც ორიენტირებულია ინფორმაციულ უსაფრთხოებაზე.

აღნიშნული ორგანიზაციის დაფუძნება განაპირობა საქართველო-რუსეთის ომის შემდეგ ქვეყნის წინაშე დამდგარმა ახალმა რეალობამ. როგორც 2008 წლის აგვისტოს ომმა დაგვანახა, ქვეყანაში ფაქტობრივად არ არსებობს საინფორმაციო ომის წარმოებისა და კიბერ-ტერორიზმისგან დაცვის ჩამოყალიბებული მექანიზმები, რაც თანაბრად უქმნის საფრთხეს როგორც საჯარო, ისე კერძო სექტორს. არ არსებობს შესაბამისი საკანონდმებლო ბაზა, სახელმწიფო ინსტიტუტები და მატერიალურ ტექნიკური ინფრასტრუქტურა კიბერ ტერორიზმთან და კომპიუტერულ დანაშაულთან საბრძოლველად. რაც გარდა სახელმწიფოს თავდაცვისუნარიანობისა, ასევე ახდენს მკვეთრ ნეგატიურ გავლენას ქვეყნის ეკონომიკაზე.

უკანასკნელ პერიოდში როგორც კერძო, ისე სახელმწიფო სექტორის ყველა მიმართულებით მიმდინარეობს თანამედროვე ტექნოლოგიების ინტენსიური დანერგვა. რაც უფრო მეტია პროცესების ავტომატიზაციის მასშტაბი მით უფრო რთულია მათი კონტროლი. ასეთ პირობებში, როცა შპიონაჟი და ქვეყნის უსაფრთხოების სხვა გამოწვევები ტექნოლოგიურ ხასიათს იძენენ, ჩნდება ახალი საფრთხეები. შესაბამისად აღნიშნული ინფორმაციის სათანადო დაცვა სასიცოცხლო მნიშვნელობისაა არამხოლოდ სახელმწიფო, არამედ კერძო ორგანიზაციებისთვისაც.

ზემოთ აღნიშნული საფრთხეებისა და გამოწვევების წინააღმდეგ ჩვენი ორგანიზაციის გარშემო შეიკრიბა გამოცდილი პროფესიონალების გუნდი. რაც საშუალებას იძლევა პირველად საქართველოში ჩამოყალიბდეს კიბერ ტერორიზმთან, მეკობრეობასთან, კორპორაციულ შპიონაჟთან და სხვა სახის ტექნოლოგიურ საფრთხეებთან ბრძოლის ინსტიტუციური მექანიზმები.

ორგანიზაციის საქმიანობის შესახებ

ინფორმაციული უსაფრთხოების კვლევებისა და ანალიზის ცენტრი წარმოადგენს უნიკალურ სერვისს როგორც კერძო, ისე სახელმწიფო სექტორისთვის, რომელიც მოიცავს მრავალპროფილიან მომსახურებას:

კადრების რეკრუტირება

სხვადასხვა რგოლის პერსონალის მომზადება (ტრეინინგები);

ინფორმაციული უსაფრთხოების სხვადასხვა ასპექტების აუდიტი და შესაბამისი დასკვნა-რეკომენდაციების მომზადება;

სტანდარტებისა და შიდა პროტოკოლების შემუშავება;

ორგანიზაციული ერთეულების შექმნა საფრთხეების მონიტორინგისა და ინციდენტებზე რეაგირებისთვის;

საკონსულტაციო მომსახურება როგორც IT ინფრასტრუქტურულ საკითხებზე, ისე იურიდიული მხარეზე სხვადასხვა ტიპის IT პროექტებთან დაკავშირებით;

შესაბამისი პროგრამულ-აპარატურული გადაწყვეტილებების შემუშავება, დანერგვა და მიწოდება;

IT აუთსორსინგი, დაცული ჰოსტინგი აშშ-ს სერვერებზე, და სხვა...

ამავდროულად ცენტრის უმთავრეს პრიორიტეტს წარმოადგენს ქვეყნის წინაშე არსებული სხვადასხვა სახის ტექნოლოგიური, გეოპოლიტიკური და სამხედრო გამოწვევების შესწავლა, მათი სრულყოფილი ანალიზი და ამაზე დაყრდნობით საზოგადოებისთვის ამომწურავი და ობიექტური ინფორმაციის დროული მიწოდება, რისთვისაც ინფორმაციული უსაფრთხოების კვლევებისა და ანალიზის ცენტრის ანალიტიკური ჯგუფი პერიოდულად ამზადებს საჯარო პუბლიკაციების სერიას თანამედროვე საფრთხეებისა და გლობალური ტენდენციების შესახებ.

ჩვენ ვართ მაქსიმალურად გახსნილი საკუთარ საქმიანობაში და ვეხმარებით ამ სფეროთი დაინტერესებულ პირებს. ვაძლევთ მათ შესაბამის ცოდნასა და საშუალებებს რათა თავად გახდნენ ნაწილი ამ სისტემის და მონაწილეობა მიიღონ ცენტრის მიერ განხორციელებულ სხვადასხვა პროექტებში.

ჩვენი მიზანია ვითანამშრომლოთ რაც შეიძლება მეტ ორგანიზაციასთან, სახელმწიფო სტრუქტურასთან და საგანმანათლებლო დაწესებულებებთან რათა კიდევ უფრო ეფექტურად ვებრძოლოთ თანამედროვე საფრთხეებს, შევქმნათ საერთო სტანდარტები და ამ სტანდარტების შესრულების ინსტრუმენტები, ავამაღლოთ საზოგადოებრივი ინფორმირების ხარისხი ამ საკითხში და მივაწოდოთ ჩვენი სერვისი მათ, ვისაც ეს ნამდვილად ჭირდება.

ჰებრიტასიის ელექტრონული ვერსია შეგიძლიათ იხილოთ

ინფორმაციული უსაფრთხოების ხვრევებისა და ანალიზის სენტრის ვებ-ჰორტალზე

HTTP://WWW.ISSAC.GE