GFSIS
საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა ქართული ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

52

ახალი გამოწვევა საქართველოს ინტერნეტსივრცისთვის

ვლადიმერ სვანაძე

ექსპერტის აზრი

2016

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

ექსპერტის აზრი

ვლადიმერ სვანაძე

ახალი გამოწვევა საქართველოს ინტერნეტსივრცისთვის

52

2016

პუბლიკაცია დაიბეჭდა ამერიკის შეერთებული შტატების საელჩოს ფინანსური მხარდაჭერით.

რედაქტორი: რუსუდან მარგიშვილი

ტექნიკური რედაქტორი: არტემ მელიქ-ნუბაროვი

ISSN 1512-4835
ISBN 978-9941-0-8512-3

მსოფლიო საზოგადოება დადგა ახალი კიბერსაფრთხის წინაშე, რომელიც მომდინარეობს ისლამური ჰაკერული ჯგუფებიდან და დაჯგუფებებიდან. ამ მხრივ საყურადღებოა, რომ ბოლო წლებში, განსაკუთრებით, სირიაში საომარი მოქმედებებისა და ახლო აღმოსავლეთში ე. წ. „ისლამური სახელმწიფოს“ (ISIS) ასპარეზზე გამოსვლის შემდეგ, ერთიორად გაიზარდა კიბერშეტევების რიცხვი. ამ მიმართულებით განსაკუთრებით აქტიურობენ ჰაკერული დაჯგუფებები „ახლო აღმოსავლეთის კიბერარმია“ (the Middle Eastern Cyber Army - MECA), Fallaga Hackers Team და Cyber Caliphate და, ასევე, „სირიის ელექტრონული არმია“ (SEA), რომელსაც დიდ მხარდაჭერას უწევს „ირანის კიბერარმია“ (ICA).

უახლოეს მომავალში ამგვარი საფრთხის წინაშე აღმოჩნდება საქართველოს ინტერნეტსივრცეც, რომლის საგარეო პოლიტიკა მიმართულია ევროპულ ინსტიტუტებში ინტეგრაციისკენ – ქვეყანა უნდა გახდეს ევროკავშირისა და ჩრდილოეთ ატლანტიკური ალიანსის წევრი. გასულ წელს საქართველომ ხელი მოაწერა ევროკავშირთან ასოცირების ხელშეკრულებას, სადაც ერთ-ერთ პუნქტად ჩადებულია უსაფრთხოების უზრუნველყოფის საკითხები (ევროკავშირთან ასოცირების შესახებ შეთანხმება, მუხლი 1, პუნქტი (ფ)), იქვე მოხსენიებულია ასევე პერსონალურ მონაცემთა დაცვა (ევროკავშირთან ასოცირების შესახებ შეთანხმება, კარი 3, მუხლი 14) და კიბერდანაშაულთან ბრძოლა (ევროკავშირთან ასოცირების შესახებ შეთანხმება, კარი 3, მუხლი 17, პუნქტი (გ)).

ყოველივე ეს გამოიწვევს საქართველოში დასავლური სახელმწიფო ინსტიტუტების, კომპანიების, ახალი მისიებისა და წარმომადგენლობითი ოფისების გახსნას. პროცესი იქნება სულ უფრო მზარდი, რაც, თავის მხრივ, ჩვენი ქვეყნის მიმართ კიდევ უფრო გაზრდის საფრთხეებს როგორც პოტენციურად მოწინააღმდეგე ქვეყნების, ისე ისლამური ფუნდამენტალიზმის მიმდევრების მხრიდანაც. ყოველივეს პარალელურად იზრდება კიბერსაფრთხეებიც.

სტატისტიკური მონაცემებით, საქართველოში 2008-2014 წლებში მომხდარი კიბერშეტევების დიდი რაოდენობა მოდიოდა რუსეთზე (FirEye, 2014), რომლის დროსაც სისტემატურად ხორციელდებოდა კიბერშეტევა შინაგან საქმეთა და საგარეო საქმეთა სამინისტროების, ასევე კავკასიის თემაზე მომუშავე ზოგიერთი არასამთავრობო ორგანიზაციის ვებგვერდებზე.

რუსი ჰაკერების მთავარ სამიზნეს ასევე წარმოადგენდნენ ის ვებგვერდები და პირები, რომლებიც ინტერნეტსივრცეში ქარ-

თულ სახელმწიფოებრიობასა და ინტერესებს იცავენ. მაგალითად, ამ მხრივ საინტერესოა 2009 წლის 6-7 აგვისტოს რუსი ჰაკერების მიერ განხორციელებული კიბერშეტევა პოპულარულ ქართულ სოციალურ ქსელებზე, რომლის მიზეზი ქართველი ბლოგერის – „სოხუმის“ პოლიტიკური შეხედულებები გახდა. 7 აგვისტოს გააქტიურდა კიბერშეტევა და ცხადი გახდა, რომ მას რუსული სპეცსამსახურები ახორციელებდნენ, რომლებიც ბლოკავდნენ ინფორმაციას, რომელსაც ბლოგერი „სოხუმი“ ავრცელებდა და რომელიც აგვისტოს ომის წლისთავს უკავშირდებოდა. უკვე ყველა სპეციალისტი ადასტურებს, რომ შეტევა ვებგვერდებზე რუსეთიდან განხორციელდა და იმდენად კარგად იყო ორგანიზებული, რომ ცალკეული ჰაკერების მოქმედებას გამორიცხავს.

აღსანიშნავია ის გარემოებაც, რომ რუსეთიდან წამოსული კიბერშეტევები ემსახურებოდა ასევე კიბერჯაშუშური გზით ინფორმაციის მოპოვებასა და შეგროვებას საქართველო-შეერთებული შტატების, საქართველო-ევროკავშირისა და საქართველო-ჩრდილოატლანტიკური ალიანსის ურთიერთობებისა და მომავალი საქმიანობის შესახებ.

2015 წელს რუსეთის აქტიურობა საქართველოს კიბერსივრცეში ნაკლებად შეინიშნებოდა, მათი მხრიდან შემოღწევა ოფიციალურად არ დაფიქსირებულა. თუმცა 2015 წლის 21-25 მაისს ქართულ საფინანსო ორგანიზაციებზე განხორციელდა მასობრივი DDoS შეტევა. სულ შეტევაში მონაწილეობდა 300 000-მდე უნიკალური IP მისამართი, 160-ზე მეტი ქვეყნიდან. შეტევის მასშტაბიდან, მომზადების ხარისხიდან და რეგიონისადმი გეოპოლიტიკური ინტერესიდან გამომდინარე, უნდა ვივარაუდოთ, რომ ამ შეტევის უკან რუსეთთან დაკავშირებული ჰაკერული ჯგუფი იდგა. იმის გათვალისწინებით, რომ ასეთი მასშტაბური შეტევა არ იყო ორიენტირებული ფინანსურ ზარალზე, დიდი ალბათობით, იგი მიზნად ისახავდა ყურადღების გადატანას სხვა, შესაძლოა უფრო მეტად ზიანის მომტანი შეტევისაგან.

2015 წლის პირველ ნახევარში ინციდენტების ორგანიზატორებს შორის უკვე გამოჩნდა ისლამური ჰაკერული დაჯგუფებები. კერძოდ, 10 იანვარს ფრანგულ კომპანია „კარფურის“ საქართველოს ფილიალის ვებგვერდზე „ახლო აღმოსავლეთის კიბერარმიამ“ განახორციელა კიბერშეტევა. სხვათა შორის, იმ პერიოდში მოხდა საკმაოდ მასობრივი კიბერშეტევა ფრანგულ კომპანიებსა და მათ წარმომადგენლობით ოფისებზე მთელ მსოფლიოში, სადაც ასევე

ფიგურირებდა „კარფურის“ საქართველოს ფილიალი. ეს ფაქტი იმსახურებს ყურადღებას და განხილული უნდა იყოს, როგორც დასავლური კომპანიის წარმომადგენლობაზე კიბერთავდასხმის პირველი სერიოზული პრეცედენტი ჩვენს ქვეყანაში.

გარდა ამისა, ასევე მნიშვნელოვანია მეორე შემთხვევა, რომელიც 2015 წლის 16 აპრილს ისლამურმა ჰაკერულმა დაჯგუფება „ელ მოჰაჯირმა“ ჩაიდინა „საქართველოს მოსამართლეთა ერთობის“ ვებგვერდზე. კიბერთავდასხმა ატარებდა დაშინებისა და პროპაგანდისტულ ხასიათს.

ასევე განსაკუთრებულ ყურადღებას იმსახურებს მიმდინარე წლის 6 ივლისს ISIS-ის ჰაკერების მიერ განხორციელებული კიბერშეტევა საქართველოს სახელმწიფო მინისტრის აპარატის ევროპულ და ევროატლანტიკურ სტრუქტურებში ინტეგრაციის საკითხების ვებგვერდზე.

მომავალში სულ უფრო გაიზრდება ისლამური ჰაკერული ჯგუფებიდან და დაჯგუფებებიდან მომდინარე მსგავსი ინციდენტების რიცხვი, რაც უნდა განვიხილოთ, როგორც ახალი სერიოზული გამოწვევა საქართველოს ეროვნული უსაფრთხოებისთვის. ამ კონტექსტში გასათვალისწინებელია „იემენის კიბერარმიის“ მიზნები და მისი შესაძლებლობები. ეს არის ახლადშექმნილი ორგანიზაცია, რომლის მიზანია კიბერთავდასხმების გზით შეერთებული შტატებს, ევროკავშირის წევრ ქვეყნებსა და მათ სტრატეგიულ პარტნიორებს შორის არსებული ურთიერთობების შესახებ ელექტრონული მიმოწერის მოპარვა, რომელსაც იგი იმ ქვეყნებიდან ახორციელებს, რომელთა კიბერსივრცე უფრო მოწყვლადი და მგრძნობიარეა. მაგალითისთვის, ივნისის თვეში ორგანიზაციამ განახორციელა კიბერთავდასხმა საუდის არაბეთის საგარეო საქმეთა სამინისტროზე, საიდანაც მოიპარეს შეერთებულ შტატებთან და ევროკავშირთან ელექტრონული მიმოწერის დაახლოებით ათი ათასამდე სტრატეგიული დოკუმენტი. მსგავსი საფრთხის წინაშე ასევე შეიძლება აღმოჩნდნენ საქართველოს სახელმწიფო სუბიექტები.

საქართველოს კიბერსივრცეში 2015 წელს მომხდარი არასანქცირებული შეტევებიდან შეიძლება გამოიყოს შემდეგი ინციდენტები:

- 19 იანვრის კიბერთავდასხმა დიასპორის საკითხებში სახელმწიფო მინისტრის აპარატის ვებგვერდზე;
- 2 თებერვლის მასობრივი კიბერშეტევა ელექტრონულ ფოსტებ-

ზე. კერძოდ, ინტერნეტში გავრცელდა ახალი კომპიუტერული ვირუსი, რომელიც სხვადასხვა ენაზე აგზავნის ელექტრონულ წერილებს, მათ შორის, ქართულ ენაზეც. ვირუსი მსხვერპლს 96 საათს აძლევს, რომ გადაურიცხოს კონკრეტული თანხა, წინააღმდეგ შემთხვევაში, ფაილები სამუდამოდ განადგურდება;

- 5 თებერვლის კიბერშეტევა საქართველოს საგარეო საქმეთა სამინისტროს ოფიციალურ ვებგვერდზე. შედეგად, ამ კიბერშეტევის გამო საქართველოს საგარეო საქმეთა სამინისტრომ მიიღო გადაწყვეტილება აამოქმედოს სამინისტროს ახალი ვებგვერდი, რომელზე მუშაობაც ამ ეტაპზე ნაწილობრივ არის დასრულებული. ჯერ დაუდგენელია კიბერშეტევის წყარო;
- წლის პირველ ნახევარში განხორციელებული რამდენიმე კიბერშეტევა საქართველოს სოფლის მეურნეობის ვებგვერდზე.

შინაგან საქმეთა სამინისტროს ოფიციალური სტატისტიკური მონაცემებით, კიბერდანაშაული საქართველოში ყოველდღიურად მატულობს, თუმცა მოიკლო კიბერდანაშაულის გახსნის პროცენტულმა მაჩვენებელმა. კერძოდ, სამინისტროს მიერ დაფიქსირებული კიბერდანაშაულის რიცხვმა, 2014 წელთან შედარებით, 2015 წლის იანვარ-აგვისტოს მდგომარეობით 11,11%-ით მოიმატა. რაც შეეხება კიბერდანაშაულის გახსნას, 2014 წელს გახსნის მაჩვენებელმა შეადგინა 59,26%, როცა 2015 წლის იანვარ-აგვისტოს მდგომარეობით ის შეადგენს 34,44%-ს.

ზემოთ მოცემული ცნობილი კიბერშეტევების გარდა საქართველოს სხვადასხვა ორგანიზაციასა და კომპანიაზე განხორციელდა კიბერშეტევები. კერძოდ, ორგანიზაცია zona-h-ის მონაცემებით, გასული წლის იანვრიდან ოქტომბრის ჩათვლით საქართველოს კიბერსივრცეში მოხდა 489 სხვადასხვა სახის უკანონო კიბერშემოღწევა. ეს მაჩვენებელი არცთუ დიდია ისეთი ქვეყნებისთვის, როგორიცაა შეერთებული შტატები, დიდი ბრიტანეთი ან ჩინეთი. მაგრამ საქართველოს კიბერსივრცეში ოფიციალურად დაფიქსირებული უკანონო შემოღწევების მოყვანილი რაოდენობა გარკვეულ შეშფოთებას იწვევს. ფაქტობრივად, ქვეყანაში ყოველდღე ხდება კიბერინციდენტი.

საერთაშორისო სისტემაში არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით, საქართველოს უსაფრთხოების პოლიტიკის დაგეგმვა და განხორციელება კიბერუსაფრთხოების

სფეროში განიხილავს საფრთხეებისა და გამოწვევების შემდეგ სამ მიმართულებას:

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

ამ ეტაპზე საქართველოს ხელისუფლება მუშაობს კიბერუსაფრთხოების ახალ სტრატეგიასა და 2016-2018 წლების სამოქმედო გეგმაზე.

გამოყენებული ლიტერატურა

1. ევროკავშირთან ასოცირების შესახებ შეთანხმება, 2014;
2. საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ;
3. საქართველოს კიბერუსაფრთხოების სტრატეგია.
4. United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk, Washington DC:US GAO, 2009;
5. Democratic Governance Challenges of Cyber Security, Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, DCAF 2010, DCAF Horizon 2015 Working Paper Series;
6. www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html;