ტერორისტული ორგანიზაციების კიბერშესაძლებლობები

TRC GCSD

ტერორისტული ორგანიზაციების კიბერშესაძლებლობები

ავტორი: ანდრო გოცირიძე

ანდრო გოცირიძე - კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის CYSEC დამფუძნებელი. თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს დირექტორი 2014 -2017 წწ, გენერალური ინსპექტორი 2012-2014 წწ. სხვადასხვა დროს მუშაობდა თავდაცვის სამინისტროსა და სადაზვერვო სამსახურების ხელმძღვანელ თანამდებობებზე, 2008-2012 წლებში იყო სს „პრივატბანკისა“ და სს „ბანკი კონსტანტას“ უსაფრთხოების დეპარტამენტის უფროსი. მისი უშუალო მონაწილეობით დამუშავდა ეროვნული და თავდაცვის სამინისტროს კიბერუსაფრთხოების პოლიტიკა და სტრატეგიები, საფუძველი ჩაეყარა კიბერრეზერვის პროექტს და სამშვიდობო მისიებში დაჭრილი ჯარისკაცების კიბერუსაფრთხოების სფეროში ტრენერებად ინტეგრაციას, დაინერგა კიბერცნობიერების ამაღლების მრავალკომპონენტიანი სისტემა.

კითხულობს ლექციებს BTU, შავი ზღვის საერთაშორისო და კავკასიის უნივერსიტეტებში, ასევე GFSIS (რონდელის ფონდი)-ის, საგარეო საქმეთა სამინისტროს დიპლომატიური ინსტიტუტისა და მედიის განვითარების ფონდის მიერ ორგანიზებულ სხვადასხვა პროექტებში. არის 2015-16 წ. NATO PFPC მიერ შექმნილი Cyber Security Generic Reference Curriculum თანაავტორი.

ტერორისტული ორგანიზაციების კიბერშესაძლებლობები

კომპიუტერის, ქსელის და საინფორმაციო ტექნოლოგიების საშუალებით განხორციელებული ქმედება, რომელიც მიზნად ისახავს ხელი შეუშალოს ჯგუფის, ორგანიზაციის ან სახელმწიფოს პოლიტიკურ, სოციალურ თუ ეკონომიკურ საქმიანობას ან ახდენს ფიზიკური ძალადობის და შიშის პროვოცირებას და მოტივირებულია ტრადიციული ტერორისტული იდეოლოგიებით, კვალიფიცირდება, როგორც კიბერტერორისტული ქმედება.[1]

აშშ-ის გამოძიების ფედერალური სამსახურის განსაზღვრებით, კიბერტერორიზმი ეწოდება კომპიუტერული სისტემებზე, პროგრამებზე, მონაცემებსა და ინფრომაციაზე განზრახ, პოლიტიკურად მოტივირებული თავდასხმას, რაც გამოიწვევს ძალადობას არასამხედრო სამიზნეების მიმართ.[2]

NATO - ს განსაზღვრებით, კიბერტერორიზმი არის კომპიუტერის ან საკომუნიკაციო ქსელის მეშვეობით განხორციელებული იდეოლოგიურად მოტივირებული კიბერშეტევა, რომლის მიზანია მნიშვნელოვანი განადგურების ან შეფერხების გამოწვევით შიშის დათესვა ან საზოგადოების დაშინება[3].

ტერორისტული დაჯგუფების ან ექსტრემისტულად განწყობილ პირთა მიერ კომპიუტერული ქსელებისა და ელექტრონული სერვისების კონფიდენციალურობაზე, ერთიანობასა და ხელმისაწვდომობაზე ზემოქმედებისკენ მიმართული შეტევები ძირითადად მოიცავს კომპიუტერულ ქსელების დაზიანების, სერვისის შეფერხების და კომპიუტერული ქსელის ან არასანქცირებული წვდომის შედეგად ქსელიდან მიღებული ინფორმაციის ტერორისტული მიზნებით გამოყენების მცდელობებს.

დღეისათვის ყველაზე ძლიერ და შესაბამისად, საფრთხისშემცველ კიბერტერორისტულ დაჯგუფებას წამოადგენს Cyber Chaliphate, რომელიც ტერორისტულ ორგანიზაცია დაეშთან ასოცირდება. მისი ერთ ერთი ლიდერი, არაბული წარმოშობის, დიდი ბრიტანეთის მოქალაქე ჯუნაიდ ჰუსეინი იგივე აბუ ჰუსეინ ალ-ბრიტანი (*Abu* Hussain *al Britani*), 2015 წელს ქ. რაკაში დაიღუპა დრონით განხორციელებული შეტევისას. დაჯგუფების დეკლარირებული მიზანია მასიური კიბერშეტევების განხორციელება აშშ-

---

[1] Defining cyber terrorism. Ruben Tuitel. Per concordiam - journal of european security and defense issues, vol. 7, issue 2, 2016. ISSN 2166-322x (print) ISSN 2166-3238 (online)

[2] *Centre of Excellence Defence Against Terrorism, ed. (2008). Responses to Cyber Terrorism. NATO science for peace and security series. Sub-series E: Human and societal dynamics, ISSN 1874-6276.* ***34****. Amsterdam: IOS Press. p. 119. ISBN 9781586038366. Retrieved 2018-07-22. The Federal Bureau of Investigations has the following definition of cyber terrorism: Any 'premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents.'*

[3] *Centre of Excellence Defence Against Terrorism, ed. (2008). Responses to Cyber Terrorism. NATO science for peace and security series. Sub-series E: Human and societal dynamics, ISSN 1874-6276.* ***34****. Amsterdam: IOS Press. p. 119. ISBN 9781586038366. Retrieved 2018-07-22. The current NATO Definition of cyber terrorism is: 'A cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.'*

სა და ანტიტერორისტული კოალიციის წევრი ქვეყნების სახელმწიფო და კერძო ინფრასტრუქტურაზე.

გახმაურებული კიბერშეტევებს მიეკუთვნება აშშ-ს ცენტრალური სარდლობის „Twitter“-ის და „Youtube“-ის ანგარიშების გატეხვა, ასევე თავდასხმა გამომცემლობა Newsweek-ზე. დაჯგუფების შეტევები არ ატარებს ეკონომიკურ ხასიათს, მათი მიზანია პროპაგანდისტული საქმიანობა, ინფორმაციის მოპოვება და მნახველთა დიდი რაოდენობის მქონე ვებ-გვერდებზე ჯიჰადისტური მოწოდებების (მათ შორის მუქარის შემცველი) გამოქვეყნება, ასევე სოციალური მედიის საშუალებით მიმდევართა რეკრუტინგი. სოციალური მედიისადმი ყურადღებას ის ფაქტიც ადასტურებს, დაეშს ათიათასობით ინგლისურენოვანი მიმდევარი ჰყავს Twitter-ზე. ასევე აქტიურად გამოიყენება სპეციალური მედია პლატფორმები პოტენციურ ახალწვეულებზე მიმართვის მიზნით.

დაეშის მიერ საქმიანობისას დაშიფვრის ტექნოლოგიების გამოყენება შესაბამის სამსახურებს ადექვატური რეაგირების შესაძლებლობებს უზღუდავს. ითვლებოდა, რომ დაჯგუფების ყველაზე წარმატებული და გახმაურებული კიბერშეტევა იყო ფრანგულ მაუწყებელ TV5 Monde-ზე განხორციელებული მრავალფაზიანი შეტევა. არც მანამდე და არც მერე ორგანიზაციას ამ მასშტაბის შეტევა არ განუხორციელებია, **თუმცა, როგორც ზემოთ არის აღნიშნული, განხორციელებული კიბერშეტევის ხელწერისა და მავნე კოდებში კირილიცის ელემენტების შემცველობის ფაქტებზე დაყრდნობით თითქმის უტყუარად დადგენილია, რომ ეს შეტევა რუსული სპეცსამსახურების false flag ოპერაციას წარმოადგენდა, რაც დროში დაემთხვა ფრანგულ-რუსული ურთიერთობების გაუარესებას**. [4]

ზემოაღნიშნულის გათვალისწინებით, არსებობს ვარაუდი, რომ CyberCaliphate არ წარმოადგენს ორგანიზებულ ჰაკერულ დაჯგუფებას, ხოლო მასთან ასოცირებული შეტევები დაეშის იდეების გამტარებელი ცალკეული მაღალკვალიფიციური ჰაკერების ან მცირე ჯგუფების განხორციელებულია. ვერ გამოვრიცხავთ, რომ CyberCaliphate წარმოაადგენდეს შენიღბვის საშუალებას, ერთგვარ შირმას რუსული სპეცსამსახურებისთვის, რომლების მისი სახელით ახორციელებენ საკუთარ ინტერესებს.

კიბერსივრცეს აქტიურად იყენებს 2002 წლიდან ნიგერიაში მოქმედი ტერორისტული დაჯგუფება ბოკო ჰარამი, რომელიც სოციალურ ქსელებსა და თანამედროვე კომუნიკაციის სხვა სისტემებში მუშაობს რეკრუტირების, პროპაგანდისა და ფინანსების მოზიდვის მიზნით. ამ ორგანიზაციას ეკისრება პასუხისმგებლობა ათასობით უდანაშაულო მოქალაქის მკვლელობაზე, ქ. აბუჯაში გაეროს შტაბ-ბინის დანგრევასა თუ ქ. ჩიბოკში (ნიგერია) სკოლის მოსწავლეების გატაცებაზე. მისი მოქმედება ვრცელდება ჩადსა და კამერუნზეც.

ტერორისტული ორგანიზაციები, ჰეზბოლა, ჰამასი, ალ კაიდა, დაეში აგძელებენ ინტერნეტის გამოყენებას სადაზვერვო ინფორმაციის მოსაპოვებლად, ფონდების

[4] Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. Report, 2017. ხელმისაწვდომია www.dia.mil/Military-Power-Publications

მოსაძიებლად, რეკრუტირებისათვის, პროპაგანდის გასავრცელებლად და სხვა ქმედებებისათვის. მსგავსი მიზნებით იყენებს ინტერნეტ-ტექნოლოგიებს თალიბანიც. ჰეზბოლა და ჰამასი საკუთარ კიბერაქტივობებს ახლო აღმოსავლეთის რეგიონზე ავრცელებენ, დაეშის კიბერდანაყოფები კი გამუდმებით ცდილობენ შემდგომი ტერაქტების განსახორციელებლად მოიპოვონ სენსიტიური ინფორმაცია ანტიტერორისტული კოალიციის წევრი სახელმწიფოების მოქალაქეებზე, განსაკუთრებით კი სამხედრო პერსონალზე, რათა მათზე თავდასხმის შედეგად გამოწვეულმა მღელვარებამ და შიშმა აიძულოს მთავრობა, დატოვოს კოალიციის რიგები ან შეწყვიტოს სამხედრო ოპერაციები ტერორისტული ორგანიზაციების წინააღმდეგ. თუ გავითვალისწინებთ, რომ საქართველოში ამგვარი სენსიტიური ინფორმაციის დიდი მასივები სახელმწიფო შესყიდვების კანონმდებლობიდან გამომდინარე, კერძო ბიზნესის ხელშია, ცხადი ხდება სახელმწიფო და კერძო სექტორების თანამშრომლობის აუცილებლობა კიბერუსაფრთხოების უზრუნველსაყოფად.

არსებული ვითარების შეფასებით, ტერორისტული დაჯგუფებები დღესდღეობით არ ფლობენ მნიშვნელოვანი ზიანის გამოსაწვევად საკმარის კიბერსაშუალებებს. მსოფლიოში ყველაზე ხშირად განხორციელებული კიბერტერორისტული შეტევის ფორმა არის დაუცველი ვებ-გვერდებისა და სოციალური მედიისათვის ზიანის მიყენება. საქართველოს კიბერსივრცეში ვებ-გვერდების დაზიანების მიზნით განხორციელებული ე.წ. Defacement[5] შეტევების სამიზნეს ძირითადად შედარებით მოწყვლადი, სუსტად დაცული ვებგვერდები წარმოადგენს. როგორც წესი, აღნიშნული სახის შეტევა მხოლოდ მცირე შეფერხებებს იწვევს.

სუსტად დაცული ვებ-გვერდების დაზიანების სიმარტივის არასწორად აღქმის გამო, ტერორისტული ორგანიზაციების კიბერშესაძლებლობები მედიის და საზოგადოების მხრიდან ხშირად გადაჭარბებულადაა შეფასებული. მითუმეტეს, საქართველოში დაუცველი ვებ-გვერდების რაოდენობა კერძო სექტორსა თუ სახელმწიფო დაწესებულებებში დიდია ერთის მხრივ ცნობიერების არასათანადო დონისა და მეორეს მხრივ, არასაკმარისი ფინანსური რესურსის გამო. მაგალითაად, რამდენიმე წლის წინ ერთ ერთ არასაკმარისად დაცულ ჰოსტინგ-პროვაიდერზე განხორციელებულმა რუსული სამხედრო დაზვერვის არცთუ მაღალტექნოლოგიურმა შეტევამ, ათასობით ქართული საიტის, მათ სორის საქართველოს პრეზიდენტის, საერთო სასამართლოების, ადგილობრივი თვითმმართველობებისა და არასამთავრობო სექტორის ვებგვერდების დროებითი შეფერხება გამოიწვია, რამაც საერთაშორისო რეზონანსი ჰპოვა[6]. ისევ ზემოაღნიშნულ ტენდენციას რომ დავუბრუნდეთ, მას ხელს უწყობს საკუთარი

[5] Defacement - კიბერშეტევის სახეობა, რომელიც იწვევს ვებგვერდის ან საიტის ვიზუალის შეცვლას. ხშირად გამოიყენება ტერორისტული ორგანიზაციების მიერ პროპაგანდისტული მოწოდებების გასავრცელებლად.

[6] **Georgian Companies and Government Entities**: a 2018 spearphishing campaign targeting a major media company, 2019 efforts to compromise the network of Parliament, and a wide-ranging website defacement campaign in 2019. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

კიბერშესაძლებლობების გაზვიადება ექსტრემისტულად განწყობილი ჰაკერების მხრიდან რეპუტაციის ამაღლებისა თუ ფსიქოლოგიური ზემოქმედების მიზნით. ამასთან, ზოგიერთი დაჯგუფების მიერ განხორციელებულლი კიბერშეტევა არასწორადაა მიკუთვნებული კიბერტერორისტულ თავდასხმებს და მათ ამგვარ იდეოლოგიასთან საერთო არაფერი აქვთ. მაგალითად 2015 წლის იანვარში მალაიზიის ავიახაზების ვებ-გვერდის დაზიანება კიბერხალიფატის სახელით LizardSquard-ის ჰაკერული დაჯგუფების მიერ იყო ორგანიზებული და სრულიად მოკლებული იყო იდეოლოგიურ საფუძველს.

მოსალოდნელია, რომ ახლო მომავალში, ტერორისტული დაჯგუფებები სავარაუდოდ ისევ კონვენციურ შეტევებს მიანიჭებენ უპირატესობას, როგორც მნიშვნელოვანი ზიანისა თუ შიშის გამომწვევი ამ ეტაპზე მათ ხელთ არსებული ერთადერთი მექანიზმს. რეალურია კიბერსივრცის გამოყენება ტერორისტული ორგანიზაციების მხრივ სადაზვერვო ინფორმაციის მოპოვების, ფინანსური თაღლითობის, პროპაგანდისტული მიზნებით ან რეკრუტირებისათვის. ზემოთქმულის ნათელი მაგალითია ახლო წარსულში რადიკალური ისლამის მიმდევარი ორგანიზაციების მიერ დაწყებული მასშტაბური, მრავალპლატფორმიანი კამპანია სოციალურ ქსელებში, რომელსაც ათასობით ონლაინ მხარდამჭერი მიუერთდა მსოფლიოში და საქართველოშიც. სოციალური მედია საშუალებას იძლევა გავრცელდეს პროპაგანდა მაქსიმალურად ფართო მასებში და მოზიდულ იქნას ახალი ძალები ტერორისტული საქმიანობისათვის. ტერორისტული ორგანიზაციების მხრიდან უახლოეს პერიოდში მოსალოდნელი შეტევები ძირითადად ვებ-გვერდების დაზიანებითა და სერვისების გათიშვით შემოიფარგლება. უპირველეს ყოვლისა ასეთი შეტევები ხორციელდება ანტიტერორისტული კოალიციის წევრი ქვეყნების საქართველოში განთავსებულ ინფრასტრუქტურაზე (ბიზნესი, დიპლომატიური წარმომადგენლობები და სხვა), რომელთა ზოგიერთი პროდუქტიც, სავსებით შესაძლებელია სახელმწიფოსთვის კრიტიკულ სერვისს წარმოადგენდეს.

აღნიშნულ მოსაზრებას ადასტურებს სუპერმარკეტ კარფურის ქსელზე განხორციელებული კიბერშეტევა, რომელიც „Charlie Hebdo“-ს მოვლენების გამოძახილი იყო საქართველოში.

2015 წლის დასაწყისში „ახლო აღმოსავლეთის კიბერარმიამ“ (MECA) სოციალურ ქსელში გამოაქვეყნა განცხადება, რომ ისინი ფრანგულ ვებგვერდებზე კიბერთავდასხმებს განახორციელებდნენ. აღნიშნული შეტევები ფრანგული ჟურნალის მიერ გამოქვეყნებულ კარიკატურებს ეხებოდა ისლამის თემაზე. ”MECA-ს” თავდასხმაში მოხვდა ფრანგულ-ქართული ჰიპერმარკეტის, ”კარფურის” ვებგვერდიც. თავდამსხმელების მიერ შეცვლილი პირველი გვერდი გარკვეული მოკლე დროით ჯიჰადისტურ მოწოდებებს ავრცელებდა, ასევე, შეფერხება იყო კლიენტთა მომსახურების სფეროშიც.

ეს შეტევა მნიშვნელოვანი ზიანის გარეშე იქნა დაძლეული, თუმცა დაუცველ ან სუსტად დაცულ მნიშვნელოვან ობიექტზე ასეთი მარტივი თავდასხმაც კი შესაძლოა არაპროპორციული ზიანის მომტანი იყოს სახელმწიფოსთვის[7].

როგორც უკვე აღინიშნა, დღესდღეობით, ტერორისტული ორგანიზაციების მხრიდან ისეთი კიბერშეტევის განხორციელების ალბათობა, რომელსაც მასობრივი ზიანის ან მსხვერპლის გამოწვევა შეუძლია, ძალზედ დაბალია. მათი კიბერშესაძლებლობები მხოლოდ ელექტრონული სერვისების და ვებ-გვერდების დროებით, ლოკალურ დაზიანებისთვისაა საკმარისი. თუმცა, გაცილებით სერიოზული იქნება საფრთხე, თუკი თავიანთი კიბერშესაძლებლობების არსებითად გასაუმჯობესებლად, ტერორისტული ორგანიზაციები ითანამშრომლებენ რომელიმე განვითარებული კიბერშესაძლებლობების მქონე სახელმწიფოსთან, ელიტარულ კრიმინალურ ჰაკერებთან ან მოახდენენ სპეციალისტების რეკრუტირებას. თუმცა, ტერორისტულ ორგანიზაციასთან თანამშრომლობა სახელმწიფოთათვის პოლიტიკური რისკის შემცველია, ამასთან სახელმწიფოთა კიბერშესაძლებლობები ისედაც შეზღუდულია. ასევე, ჯერჯერობით ნაკლებად შეინიშნება ექსტრემისტებს და კრიმინალურ კიბერ აქტორებს შორის თანამშრომლობის ფაქტები. მიუხედავად აღნიშნულისა, ტერორისტული დაჯგუფებები კვლავ განაგრძობენ კიბერშესაძლებლობების განვითარებას, რამაც შესაძლოა გაზარდოს მათგან მომდინარე საფრთხეები. ყურადსაღებია, რომ რუსეთი ამგვარი თანამშრომლობის პირველ პრეცენდენტს იძლევა, რაც ერთიორად ზრდის მაღალტექნოლოგიური ტერორისტული კიბერშეტევის განხორციელების საფრთხეს.

მხედველობიდან არ უნდა გამოგვრჩეს ის გარემოება, რომ თუკი თუნდაც ერთი წლის წინ კონვენციური შეტევები ტერორისტული ორგანიზაციების მხრიდან რეალური ზიანისა და შიშის გამომწვევ ერთადერთ მექანიზმს წარმოადგენდა, დღეისათვის კიბერშეტევების განხორციელების ალბათობა სავარაუდოდ გაიზრდება, რაც რამდენიმე ფაქტორითაა განპირობებული:

- უკვე განხორციელებული შეტევები, მიუხედავად იმისა, ვინ იდგა რეალურად ამ შეტევების უკან, აღქმულ იქნა წარმატებულად, რაც ამგვარი თავდასხმების ეფექტურობის განცდას ქმნის;
- სახეზეა კომპიუტერულ სისტემებში უკეთესად გარკვეული ექსტრემისტების თაობა და ორგანიზაციები ეცდებიან მათი ცოდნის გამოყენებას ტერორისტული მიზნების მისაღწევად;
- სირია-ერაყის ტერიტორიაზე ტერორისტული ორგანიზაციების კონვენციური ძალების მიერ განცდილი მარცხი, ასევე გაზრდილი უსაფრთხოების ზომები ტერორისტული აქტების წინააღმდეგ, ამ ორგანიზაციებს დიდი ალბათობით კიბერთავდასხმების განხორციელებისკენ უბიძგებს.

[7] ვ. სვანიძე. პარიზის ტერაქტი და ახალი გამოწვევები საქართველოში. ვ.სვანიძე, ა. გოცირიძე. „კიბერ თავდაცვა; კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები“. საქართველოს თავდაცვის სამინისტრო, თბილისი, 2015წ. გვ. 210-214

- ავღანეთიდან კოალიციის ჯარების გამოსვლისა და ტალიბანის რეჟიმის რესტავრაციის პროცესში, მათ ხელში აღმოჩნდა ამერიკული ჯარის კუთვნილი გარკვეული კიბერშესაძლებლობები და მონაცემთა ბაზები[8], რომელთა გამოყენებაც შესაძებელია სამომავლო კიბერშეტევების ან ტერორისტული აქტების დასაგეგმად.

რთულია გამოვრიცხოთ, რომ ზოგიერთ ტერორისტულ დაჯგუფებას მართლაც აქვს ბევრად განვითარებული შესაძლებლობები მათ „მფარველ“ სახელმწიფოებთან ურთიერთობის გამო და ბოლო დროს სამხედრო დაპირისპირებისას განცდილი მარცხის გამო, მსგავსი დაჯგუფებების მისწრაფება, განახორციელონ კიბერშეტევა, რომელიც სერიოზულ ზარალს გამოიწვევს, გაზრდილია.

[8] არსებობს მონაცემები, რომ ტალიბანის მებრძოლებმა ხელში ჩაიგდეს Handheld Interagency Identity Detection Equipment (HIIDE) მოწყობილობა, რომელიც შეიცავს ცენტრალიზებულ მონაცემთა ბაზებზე დაშვების მქონე პერსონალის თვალის რქოვანის და თითის ანაბეჭდებს, ასევე მათ ბიოგრაფიულ მონაცემებს. მართალია, ეს ვერ უზრუნველყოფს ამ ბაზებზე ტალიბანის წევრტა წვდომას, მაგრამ მნიშვნელოვან მონაცემებს სეიცავს სამომავლო ტერაქტების განსახორციელებლად.