Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 20-30 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

CYBER ESPIONAGE AND CYBERDIVERSITY - MODERN CHALLENGES OF NATIONAL SECURITY

Irakli Kikishvili
The Ministry Of Internal Affairs Of Georgia, Tbilisi Police Department - Analyst

ABSTRACT. The latest developments (warfare, economic crisis, acute epidemiological situation, etc.) in the recent history indicate that the states are intellectually affected by the intelligence, that points out the importance of the issue. Consequently, it is important to define the information leakage sectors and intelligence aspects related to this process, which serve to develop appropriate self-defense mechanisms and to ensure the state's national security. Internet penetration in modern societies overruled information security issues, therefore increased risk and the need to provide information security.

The role of internet interference in the field of information provision became particularly urgent in the XXI century. Computerization processes significantly simplified the organization of business (and not only business) processes. Simplified communication process, that became an integral part of everyday activity, that seemed to be impossible before, but such technological developments always bring disadvantages: this is a new type of crime - cybercrime and cyber espionage that has become one of the key directions for the intelligence services of countries.

Keywords: National Security, Cybercrime, Cyber War, Cyber Security, Intelligence Activities, Information Security, Information War

რეზიუმე

უახლეს ისტორიაში განვითარებული მოვლენების (საომარი მოქმედებები, ეკონომიკური კრიზისი, მწვავე ეპიდემიოლოგიური ვითარება და სხვა) ანალიზი ცხადყოფს, რომ სახელმწიფოები სადაზვერვო ზემოქმედებას ექვემდებარებიან, რაც საკითხის აქტუალობაზე მიუთითებს. შესაბამისად, მნიშვნელოვანია, განისაზღვროს ინფორმაციის გაჟონვის სექტორები და ამ პროცესთან დაკავშირებული სადაზვერვო ასპექტები, რაც შესაბამისი თავდაცვითი მექანიზმების შემუშავებას და სახელმწიფოს ეროვნული უსაფრთხოების უზრუნველყოფას ემსახურება.

თანამედროვე სოციუმში ინტერნეტის შემოჭრამ გადატრიალება მოახდინა ინფორმაციული უზრუნველყოფის საკითხებში, შესაბამისად, გაიზარდა რისკი და ინფორმაციის დაცვის უზრუნველყოფის საჭიროება. ინტერნეტის როლი ინფორმაციული უზრუნველყოფის თვასაზრისით განსაკუთრებით აქტუალური გახდა XXI საუკუნეში. კომპიუტერიზაციის პროცესებმა მნიშვნელოვნად გაამარტივა საქმიანი (და არამარტო საქმიანი) პროცესების ორგანიზება. გამარტივდა კომუნიკაციის პროცესი, რომელიც ყოველდღიური საქმიანობის შემადგენელი ნაწილი გახდა, რაც მანამდე წარმოუდგენელი იყო, თუმცა ამგვარ ტექნოლოგიურ განვითარებას ყოველთვის აქვს თავისი უარყოფითი მხარე: ეს არის ახალი სახის დანაშაული – კიბერდანაშაული და კიბერშპიონაჟი, რომელიც სახემწიფოთა სპეცსამსახურების საქმიანობის ერთ-ერთი მნიშვნელოვან მიმართულებად იქცა.

საკვანძო სიტყვები: ეროვნული უსაფრთხოება, კიბერშპიონაჟი, კიბერდივერსია, კიბერ უსაფრთხოება, სადაზვერვო საქმიანობა, ინფორმაციული უსაფრთხოება, საინფორმაციო ომი

შესავალი

სახელმწიფოებს შორის უძველესი დროიდან მიმდინარეობს ფარული ინფორმაციული ომი. აშკარად გამოვლენილი დაპირისპირებები კი ამ ომის მხოლოდ გამომჟღავნებას ნიშნავს. თითოეული სახელმწიფოს ძალისხმევა მიმართულია ნებისმიერი ფორმითა და საშუალებით უზრუნველყოს საკუთარი ქვეყნის ეროვნული უსაფრთხოება, რაც სათანადო ინფორმაციული რესურსის ნაკლებობის ფონზე წარმოუდგენელია.

აღნიშნული მიზნით, საომარ და მშვიდობიან პერიოდში სხვადასხვა ქვეყნის სპეცსამსახურები სადაზვერვო საქმიანობას[1] ახორციელებენ, რომელიც საგარეო პოლიტიკის განსაზღვრის და ეროვნული უსაფრთხოების უზრუნველყოფის მიზნით, უცხო ქვეყნების შესახებ ინფორმაციის მოძიებას და დამუშავებას გულისხმობს.[2] შესაბამისად, ინფორმაციული უზრუნველყოფა სადაზვერვო საქმიანობის ძირითად მიმართულებას წარმოადგენს. ინფორმაციულ უსაფრთხოებაზე კონტროლის განმახორციელებელ რგოლს სახელმწიფოში კონტსადაზვერვო, ხოლო საზღვრებს გარეთ სადაზვერვო საქმიანობის განმახორციელებელი ორგანო წარმოადგენს.

[1]საქართველოსკანონის „სადაზვერვოსაქმიანობისშესახებ“ მე-2 მუხლისშესაბამისად - „სადაზვერვოსაქმიანობაარისსაქართველოსეროვნულიინტერესებისწინააღმდეგმიმართულისაგარეოსა ფრთხეებისშესახებინფორ¬მაციისმოპოვება, დამუშავება, ანალიზი, რეალიზაცია, აგრეთვეეროვნულიუსაფრთხოებისადათავდაცვისსფეროებშიქვეყნისსტრატეგიულიკურსისგატარების ათვისხელისშეწყობა“.

[2]*Martin T. BimforT*, Intelligence as a Science, Studies in Intelligence, Vol. 2, No. 2, 1958, 78.

ამგვარად, სადაზვერვო საქმიანობა შეიძლება განისაზღვროსროგორც ღონისძიებათა კომპლექსი, რომელიც პირდაპირ უკავშირდება საიდუმლო და არასაიდუმლო ინფორმაციის მოპოვებას, სათანადო ანალიტიკურ დამუშავებას, გამოყენებას ქვეყნის სასიცოცხლო ინტერესების უზრუნველსაყოფად და კონკურენტ ქვეყანაზე უპირატესობის მისაღწევად.

სამეცნიერო ლიტერატურაში ეროვნულუსაფრთხოებასხშირად სამხედრო ხასიათის დაპირისპირების ხელყოფის ობიექტს უკავშირებენ, თუმცა ეს მხოლოდ მისი შემადგენელი ერთ-ერთი ნაწილია.მისი არსის შემეცნების საშუალებას იძლევა ეროვნული უსაფრთხოების სფეროების იდენტიფიცირება ისეთი, როგორიცაა სამხედრო, ეკონომიკური, ინფორმაციული, დემოგრაფიული, ეთნიკური, გეოსტრატეგიული, **კიბერნეტიკული**, საგარეო უსაფრთხოება. ასევე კვების, ჯანდაცვის, გარემოს დაცვის, ენერგეტიკის, ბუნებრივი რესურსების, კატასტროფის მართვის და გენური ინჟინერიის სფეროები.[3]ეროვნული უსაფრთხოების ხელყოფის ხარისხი თითოეულ სფეროზე მიყენებული ზიანის და არსებული საფრთხის ხარისხის შესაბამისად განისაზღვრება, რომელიც გამოწვეულია როგორც ფიზიკური საომარი მოქმედებებით, ისე სახელმწიფოში მიმდინარე დამაზიანებელი სხვადასხვა პროცესებით[4] (მათ შორის კიბერსივრცეში).

ინფორმაციული უზრუნველყოფის თვალსაზრისით, კიბერსივრცე განსაკუთრებული სადაზვერვო ზემოქმედების წინაშე დგას. როგორც სახელმწიფო, ისე კერძო სექტორში გამოყენებადი ინფორმაციის ელექტრონული მიმოქცევის მაღალი მაჩვენებელი, სადაზვერვო საქმიანობაში კიბერდანაშაულის განსაკუთრებულ მნიშვნელობაზე მიუთითებს, ვინაიდან დაცვის შესაბამისი მექანიზმების არასრულყოფილების ფონზე გაზრდილია სახელმწიფოზე დამაზიანებელი ზემოქმედების როგორც პერსონალური ტიპის, ასევე საიდუმლო ინფორმაციის გაჟონვის რისკი. ყოველივე კი იმაზე მიუთითებს, რომ მზვერავ სახელმწიფოს ექმნება ხელსაყრელი პირობები, მოიპოვოს სადაზვერვო ინფორმაცია, გაეცნოს ობიექტ ქვეყანაში არსებულ ოპერატიულ ვითარებას და დაგეგმოს შესაბამისი სადაზვერვო-ოპერაციული ღონისძიებები.

თავი I. პირადი უსაფრთხოების სადაზვერვო ასპექტები

ინფორმაციის თავისუფალი მიმოქცევის პირობებში, სხვადასხვა ფორმითა და მეთოდით (შანტაჟი, კომპრომეტაცია, მოტყუება და სხვა) ტერორისტული ორგანიზაციები, კრიმინალები[5] და მათ შორის სპეცსამსახურები სასურველი ზეგავლენის განსახორციელებლად ინფორმაციულ ტექნოლოგიებს აქტიურად

[3] *Prabhakaram P.,* NATIONAL SECURITY, New delhi, Taya Mcgraw-Hill, 2008, 66.

[4]სადაზვერვოხასიათის: დივერსია, საზოგადოებრივიაზრისფორმირება, საბოტაჟიდასხვა.

[5]*სვანიძე ვ., გოცირიძე ა.,* კიბერ თავდაცვა, თბილისი, საქართველოს თავდაცვის სამინისტრო, სსიპ-კიბერუსაფრთხოების ბიურო, 2015, 193.

გამოიყენებენ, შესაბამისად ეროვნული უსაფრთხოების წინაშე არსებული საფრთხის მასშტაბები იზრდება.

მიიჩნევენ, რომ ღია წყაროებით მოპოვებული საჯარო ინფორმაცია ისეთივე მნიშვნელოვანი და გამოყენებადია, როგორც სახელმწიფო საიდუმლოებას მიკუთვნებული ინფორმაცია.[6] ამავდროულად, სათანადო საიდუმლო რეჟიმის დაცვის იგნორირების შემთხვევაში, მისი გამოყენებით საიდუმლო ინფორმაციის მოპოვებაა შესაძლებელი, რომლის უზურუნველსაყოფად ინფორმაციის მოპოვების სხვადასხვა ხერხი გამოიყენება. სადაზვერვო შეღწევადობის თვალსაზრისით, განსაკუთრებული ყურადღების ქვეშ სოციალური ქსელებიექცევიან, ვინაიდან ამ სექტორზე კომუნიკაციის პროცესში ინფორმაციის გავრცელების მაღალი რისკი არსებობს (იგულისხმება საჯარო, საიდუმლო და პერსონალური ტიპის მონაცემები). თითოეული მომხმარებელი უამრავ ინფორმაციას ფლობს და ინახავს, რომელიც დაცვის შესაბამისი მექანიზმების არარსებობის პირობებში, კომუნიკაციის პროცესში შესაძლოა გამჟღავნდეს. ამასთანავე, სოციალური ქსელები (შესაბამისი ველების შევსებით) კონკრეტული პიროვნების ფსიქოლოგიური პორტრეტის შესაქმნელად გამოყენებადი მონაცემების შეუფერხებელი მოპოვების საშუალებას იძლევა, რაც სადაზვერვო გადაბირების ერთ-ერთ მნიშვნელოვან პირობას წარმოადგენს.

ამ კუთხით საყურადღებოა, მსოფლიოში ფართოდ გამოყენებადი (სხვადასხვა ქვეყნის პროვაიდერული უზრუნველყოფით) სოციალური ქსელები, რომლებშიც შევსებული შესაბამისი ველები და სხვა სახის ერთი შეხედვით უვნებელი ინფორმაცია, პიროვნების შესახებ ფსიქოლოგიური პორტრეტის შექმნის საფუძველი შეიძლება გახდეს. აღნიშნული ქსელების შესწავლით გამოიკვეთა, რომ მათ გააჩნიათ იდენტური ველები, რომლებიც ქვემოჩამოთვლილი კატეგორიის მონაცემების გამჟღავნებას უზრუნველყოფენ:

- პირადი სახის ინფორმაცია - სახელი და გვარი, დაბადების ადგილი და თარიღი, მისამართი და ფაქტობრივი საცხოვრებელი ადგილი, საკონტაქტო ინფორმაცია, განათლება, სამუშაო გამოცდილება, ოჯახური მდგომარეობა;
- კავშირები - ოჯახის წევრები, მეგობრები, კლასელები და ჯგუფელები სასწავლო დაწესებულებიდან, თანამშრომლები ან სხვა ნიშნით დაკავშირებული პირები. (შეიძლება გამოვყოთ ახლო მეგობრები);
- ინტერესები - სპორტი, მუსიკა, სატელევიზიო გადაცემები, ფილმები, წიგნები, თამაშები, ნახატები და სხვა;
- დამოკიდებულებები, შეხედულებები, კონფლიქტები - კომენტარები, გამოქვეყნებული და მოწონებული გამოთქმები, ე.წ. სტატუსები, კონფლიქტები და მათი ხასიათი, რომელთა ანალიზით შესაძლებელია დადგინდეს პიროვნების დამოკიდებულება კონკრეტული საკითხის ან ობიექტისადმი.

პრაქტიკულად, სახეზეა ვითარება, რომლის დროსაც პიროვნების შესახებ კანონმდებლობით დაცული პერსონალური ინფორმაცია საჯაროდ ხელმისაწვდომი

[6] *Jahankhani H., Lilburn Watson D., Me G., Leonhardt F.,* Handbook of electronic security and digital forensics, World Scientific, 2010, 266.

ხდება. უფრო მეტიც, სოციალური ქსელები საშუალებას იძლევიან დისტანციურად (შენიღბულად), ყოველგვარი დამატებითი ძალისხმევის გარეშე მოპოვებულ იქნეს ისეთი სახის ინფორმაცია, რომლის მოპოვება მთელი რიგი ოპერატიულ-აგენტურული ღონისძიებების განხორციელებას მოითხოვს. შეიძლება ითქვას, რომ ინფორმაციის ტექნიკურ მოწყობილებაში განთავსება სადაზვერვო ინფორმაციის მოპოვების პროცესის ერთ-ერთი ხელშემწყობი ფაქტორია.

ინტერნეტქსელში ჩართული, ტექნიკურ მოწყობილობაში არსებული ინფორმაციის მოპოვება სპეციალურად შექმნილი პროგრამითაა შესაძლებელი, რაც ეროვნული უსაფრთხოების ხელყოფის ალბათობას ზრდის. გამოთქმულ მოსაზრებას ადასტურებს იაპონიაში ტოკიოს პოლიციის თანამშრომლის კომპიუტერიდან პერსონალური მონაცემების გაჟონვის ფაქტი,[7]სადაც სპეციალური პროგრამის გამოყენებით მონაცემების ინტერნეტსივრცეში ანონიმურად გადატანა განხორციელდა. მოპოვებული პერსონალური ინფორმაცია სამართალდამცავი ორგანოების, სპეციალური სამსახურების თანამშრომლების და ზოგადად, სახელმწიფოს კომპრომეტაციის ორგანიზების საშუალებას იძლევა. ამ სადაზვერვო შეღწევადობისათვის ხელსაყრელ პროცესებს ხელს უწყობს საჯარო სექტორში მომსახურე პირების დაუდევარი დამოკიდებულება (საიდუმლო ან კონფიდენციალური) ინფორმაციის დაცვის რეჟიმისადმი.ამ თვალსაზრისით საყურადრებოა „BBC“ იაპონიის თანამშრომლის კომპიუტერიდან ინფორმაციის ინტერნეტსივრცეში გავრცელების ფაქტი[8],რომელიც ირანში ამერიკის შეერთებული შტატების შეიარაღებული ძალების პერსონალის მონაცემებს უკავშირდებოდა. იგი, კუნძულ ოკინავაზე სწავლების სცენარის, სამხედრო-საჰაერო ბაზაზე ტერორისტული შეღწევადობის შემთხვევაში, არსებული საგუშაგოების ფოტოებს, შენობების გეგმების შესახებ ინფორმაციას შეიცავდა.[9]

ამგვარად, კომპიუტერული ვირუსის გამოყენებით მოპოვებული ინფორმაციის მნიშვნელობა განუსაზღვრელია. სადაზვერვო გადაბირების ორგანიზების ხელშემწყობ მონაცემთან ერთად, გავრცელებული ინფორმაციაგამოყენებადია ტერორისტული მიზნებით, რაც სათანადო საიდუმლოების რეჟიმის უგულვებელყოფის შედეგია. შეიძლება ითქვას, რომ ინტერნეტის ქსელზე მიერთებულ ტექნიკურ მოწყობილებაში არსებული ინფორმაცია პრაქტიკულად დაუცველია, რაც იმაზე მიუთითებს, რომ ეროვნული უსაფრთხოება ამ სექტორზე სადაზვერვო შეღწევადობისა და ზეგავლენის თვალსაზრისით დიდი საფრთხის წინაშე დგება.

---

[7] Police secrets leaked by computer virus, Press Releases, SAPHOS, 2006, <https://www.sophos.com/zh-tw/press-office/press-releases/2006/03/jppolice.aspx>, [16.08.2018].

[8]საიდუმლოინფორმაციისგაჟონვაუზრუნველყოფილიიყოკომპიუტერულიპროგრამით (ვირუსით), რომელიცშესაძლებელსხდიდადამოუკიდებლად,
ავტომატურრეჟიმშიგაეცვალადოკუმენტებიინტერნეტისსხვამომხმარებ¬ლებთან.

[9]Данные о составе войск США в Ираке случайно попали в открытый доступ в интернете, NEWSru.com, 30.11.2006, http://www.newsru.com/world/30nov2006/inet.html, [16.08.2018].

მაღალი რისკის შემცველ ობიექტებს წარმოადგენენ ინტერნეტ კომპანიები, რომელთა პროვაიდერულ უზრუნველყოფას უცხო ქვეყნები ახორციელებენ. ასეთი კომპანიების სერვისით (რომელიც თითქმის მთელს მსოფლიოშია ხელმისაწვდომი) უცხო ქვეყნის სპეცსამსახურებს ექმნებათ ხელსაყრელი პირობები აკონტროლონ სადაზვერვო დაინტერესების ობიექტები.

2013 წელს ბრიტანულ და ამერიკულ გაზეთებში გრიფით „სრულიად საიდუმლო“ მასალები გავრცელდა, რომლებიც ამერიკის შეერთებული შტატების ეროვნული უსაფრთხოების სააგენტოს - „NSA“ საიდუმლო პროგრამას „PRISM“-ს უკავშირდება. გავრცელებული მასალებით ირკვევა, რომ ეროვნული უსაფრთხოების სააგენტო საიდუმლო რეჟიმში თანამშრომლობს ისეთ კომპანიებთან, როგორიცაა: „Microsoft“, „Google“, „Yahoo“, „Facebook“, „PalTalk“, „YouTube“, „Skype“, „AOL“, „Apple“,[10] რაც იმაზე მიუთითებს, რომ მთელი მსოფლიოს მასშტაბით ინტერნეტ პროგრამების სერვის-მომხმარებლებიდან მნიშვნელოვანი სადაზვერვო ინფორმაციის მოპოვებაა შესაძლებელი. ინფორმაცის მოპოვება სპეცსამსახურებს პროგრამების პროვაიდერებთან პირდაპირი წვდომით შეუძლიათ. აღნიშნული პროგრამები როგორც ყოველდღიურ ყოფით, ისე საქმიან ურთიერთობებში გამოიყენება, შესაბამისად, სადაზვერვო შეღწევადობის რისკის წინაშე ნებისმიერი მომხმარებელი დგას. პერსონალური მონაცემების ხელმისაწვდომობა ხელსაყრელ პირობას ქმნის ფსიქოლოგიური პორტრეტის შესაქმნელად. ასეთი ინფორმაცია გადაბირების თითქმის ნებისმიერ ეტაპზე გამოყენებადია, როგორც გადაბირების კანდიდატის შერჩევისას, ისე შესწავლისას და დამუშავებისას.

აღსანიშნავია, რომ აღნიშნულ პროგრამებს გამოიყენებენ უმაღლესი პოლიტი-კური თანამდებობის პირები, სამართალდამცავი ორგანოების და სპეციალური სამსახურების თანამშრომლები, რაც იმაზე მიუთითებს, რომ უცხო ქვეყნის სპეცსამსახურებს მათთვის საინტერესო პიროვნების, ფაქტების შესახებ ინფორმაციის მოპოვების დიდი ბერკეტი გააჩნიათ, რაც გადაბირების ორგანიზებისათვის მნიშვნელოვან მაკომპრომეტირებელ მასალას შეიძლება შეიცავდეს.

პრაქტიკურად, ინტერნეტი, როგორც ულევი ინფორმაციის წყარო, მზვერავსა და სადაზვერვო ზემოქმედების უშუალო ობიექტს შორის ერთგვარ დამაკავშირებელ რგოლს წარმოადგენს, რადგან იქ მოხვედრილი ინფორმაცია არ იკარგება. გავრცელებული მასალები კომბინირებული ანალიზის შემთხვევაში მოწინააღმდეგის დაზიანების ხელსაყრელ პირობებს ქმნიან.

[10] *Greenwald G., MacAskill E.,*NSA Prism program taps in to user data of Apple, Google and others, The Guardian, 07.06.2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, [16.08.2018].

თავიII.კრიტიკული ინფრასტრუქტურის წინაშე არსებული სადაზვერვო საფრთხეები

კომპიუტერულ სისტემაში უნებართვო შეღწევით მონაცემების მოპოვება (მოპარვა), მონაცემების შეცვლა, დაზიანება და სხვა მავნე ქმედებები როგორც ინტერნეტის ფიზიკურ მომხმარებლებს, ისე კერძო სექტორს და სახელმწიფო სტრატეგიული მნიშვნელობის ობიექტებს მნიშვნელოვან ზიანს აყენებს.[11] მონაცემების მოპოვებით სადაზვერვო დაინტერესების ობიექტის, მოწინააღმდეგის ელექტრონული ქსელის და მისი შესაძლებლობების წინასწარ სადაზვერვო შესწავლა ხორციელდება. კრიტიკულ ინფრასტრუქტურაზე მიზანმიმართულად განხორციელებული კიბერშეტევა, ინფრასტრუქტურის დაზიანება, საკომუნიკაციო არხების ბლოკირება და პარალიზება სადაზვერვო-ოპერაციული საქმიანობის შემადგენელ ნაწილს წარმოადგენს, შესაბამისად, ეროვნული უსაფრთხოების უსზრუნველსაყოფად კიბერსივრცის კონტრსადაზვერვო ორგანიზება მნიშვნელოვან როლს ასრულებს.

კიბერუსაფრთხოების დიდ მნიშვნელობაზე 2008 წლისრუსეთ-საქართველოს საომარი მოქმედებების დროს, საქართველოს ინტერნეტ სივრცეზე განხორციელებული კიბერ შეტევით გამოწვეული შედეგები[12] მიუთითებს. „საქართველოს ინტერნეტ-სერვერების უმეტესობა მოექცა გარე კონტროლის ქვეშ“[13], რაც იმაზე მიუთითებს, რომ საომარი მოქმედებების მიმდინარეობამდე საკომუნი-კაციო არხების შესაძლებლობების შესახებ სადაზვერვო ინფორმაციის შეგროვება ხორციელდებოდა. შექმნილი ვითარებით შეუძლებელი გახდა კომუნიკაცია როგორც ქვეყნის შიგნით, ასევე საერთაშორისო არენაზე, მათ შორის საქართველოს სახელმწიფო ინტერესებისათვის სასურველი საზოგადოებრივი აზრის მობილიზების უზრუნველყოფის თვალსაზრისით.

საყურადღებოა ის ფაქტიც, რომ ქართულ ინტერნეტგვერდებზე განთავსებული ინფორმაცია შეიცავდა მაღალი რანგის თანამდებობის პირების მადესკრედიტირებელ იმიტირებულ ფოტო-კოლაჟს,[14]რაც ობიექტი ქვეყნის ხელისუფლების წარმომადგენლების ირგვლივ უარყოფითი საზოგადოებრივი განწყობის შექმნის მაპროვოცირებელი გარემოებაა. ამგვარად, სადაზვერვო-ოპერაციული ხასიათის ქმედებებს ელექტრონული კომუნიკაციით მოსარგებლე ობიექტი სახელმწიფოს

[11] *თავდაცვის სამინისტრო,* კიბერუსაფრთხოების საბაზისო კურსი, სსიპ-კიბერუსაფრთხოების ბიურო, 2016, 7-8.

[12] დაზიანდა სამთავრობო საიტები, საკომუნიკაციო სისტემები, სატრანსპორტო კომპანიების და მასობრივი ინფორმაციის საშუალებების, ასევე საქართველოს ეროვნული ბანკის კუთვნილი ინტერნეტ გვერდები. ქართული ინტერნეტ სივრცის მიმართულებით იგზავნებოდა დიდი რაოდენობის ქსელური პაკეტები, რამაც ინტერნეტ არხების გადავსება და ქართული ინტერნეტ სივრცის ბლოკირება გამოიწვია.

[13] *საქართველოში მომხდარ კონფლიქტთან დაკავშირებული ფაქტების დამდგენი დამოუკიდებელი საერთაშორისო მისია,* ანგარიში, ტომი III, 2009, 34.

[14] *Markoff J.,* Before the Gunfire, Cyberattacks, The New York Times, 12.8.2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html>, [16.08.2018].

სტრატეგიული და სასიცოცხლო ობიექტების ხანგრძლივი დროით მწყობრიდან გამოყვანა წარმოადგენს, რომლის მიზანია მოწინააღმდეგე სახელმწიფოს ინტერესებისათვის სასურველი საზოგადოებრივი აზრის მობილიზების ხელშეშლა.

საქართველოს მთავრობის დადგენილება (N14 საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ) კიბერუსაფრთხოების სფეროში სახელმწიფო და კერძო სექტორს შორის თანამშრომლობას ერთ-ერთ ძირითად პირინციპად გამოყოფს.[15] კერძო სექტორზე განხორციელებული კიბერშეტევა მნიშვნელოვან ზიანს აყენებს ეროვნულ უსაფრთხოებას. ამ კუთხით გამორჩეულია კორპორაციული ჯაშუშობის ორგანიზების პროცესი, რომელსაც შესაძლოა სადაზვერვო ხასიათი გააჩნდეს.

საყურადღებოა „McAfee“-ის მიერ გამოვლენილი გლობალური ფინანსური თაღლითური კიბერპროგრამით - „Operation High Roller“ განხორციელებული კიბერშეტევები, რომლის მიზანსაც საბანკო ტრანზაქციების მონიტორინგით და საჭირო საბანკო მონაცემების მოპოვებით საბანკო ანგარიშებიდან ფულადი სახსრების (რამდენიმე მილიარდი) უკანონო მიღება წარმოადგენდა. კიბერშეტევის ობიექტებს ევროპული, ლათინური ამერიკის ქვეყნები და ამერიკის შეერთებული შტატების ათასობით კომერციული ორგანიზაცია და კერძო პირი წარმოადგენდა.[16] გასათვალისწინებელია ის ფაქტიც, რომ ოპერაციიდან მაღალი ფინანსური მოგების გარდა, შესაძლებელი გახდა ისეთი პერსონალური მონაცემების მიღება, რომელთა გამოყენება სადაზვერვო გადაბირებისათვის აუცილებელი ფსიქოლოგიური პორტრეტის შედგენისათვის გამოიყენება.

ამგვარად, სადაზვერვო ორგანიზებით განხორციელებული კორპორაციული ჯაშუშობის შედეგად გადაბირებისათვის აუცილებელი პერსონალური მონაცემების მოპოვებასთან ერთად, შესაძლებელია კონკრეტულ ქვეყანაზე (სახელმწიფო ან კერძო სექტორზე) ეკონომიკური დივერსიის განხორციელება. ამ პროცესმა კომპანიების მასიური გაკოტრება, ამ კომპანიებში დასაქმებული პირების უმუშევრად დატოვება, პროფილიდან გამომდინარე პროდუქციის შექმნის პროცესის შეწყვეტა, საერთაშორისო სარეალიზაციო ბაზრებზე შეღწევადობის პოზიციის დაკარგვა, დაუცველობიდან გამომდინარე არსებული ხელისუფლებისადმი უარყოფითი განწყობების და მისგან მომდინარე მავნე შედეგები შეიძლება გამოიწვიოს.

[15] *საქართველოს მთავრობის დადგენილება N14* საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ, ქ.თბილისი, 13.01.2017, 4.

[16] *Marcus D., Sherstobitoff R.,* Dissecting Operation High Roller, McAfee, Executive Summary, <http://www.mcafee.com/tw/resources/reports/rp-operation-high-roller.pdf>, [16.08.2018].

დასკვნა

ნაშრომში განხილული საკითხების საფუძველზე, შეიძლება დავასკვნათ, რომ სახელმწიფოში და საერთაშორისო არენაზე მიმდინარე პროცესები სრულყოფილ, ობიექტურ და დროულ ინფორმაციულ უზრუნველყოფაზეა დამოკიდებული.

დაცვის სათანადო მექანიზმების არარსებობის ფონზე, სახელმწიფოს ეროვნული უსაფრთხოების განმტკიცების თვალსაზრისით, მნიშვნელოვანი ინფორმაციის გაჟონვის ალბათობა დიდია, რაც სახელწიფოებრივ ინტერესებზე უარყოფით ზეგავლენას ახდენს. ეროვნული უსაფრთხოების წინაშე არსებული საფრთხის მასშტაბების შემცირებისა და კიბერუსაფრთხოებაზე, როგორც ეროვნული უსაფრთხოების ერთ-ერთ სეგმენტზე, მავნე ზემოქმედების თავიდან აცილების მიზნით, მნიშვნელოვანია, განისაზღვროს ინფორმაციის გაჟონვის რისკ-ჯგუფები, რომლის მიხედვითაც:

- ✓ კიბერუსაფრთხოება ეროვნული უსაფრთხოების მნიშვნელოვანი შემადგენელი ნაწილია, რომლის მეშვეობით ობიექტ ქვეყანაში სადაზვერვო ხასიათის იდეოლოგიური ბრძოლის პირობებში, მასობრივი პროტესტის-არეულობის ინსპირირებაა შესაძლებელი;

- ✓ ინტერნეტი, როგორც ულევი ინფორმაციის წყარო, მზვერავსა და სადაზვერვო ზემოქმედების უშუალო ობიექტს შორის, ერთგვარ დამაკავშირებელ რგოლს წარმოადგენს. მონაცემების კომბინირებული ანალიზის შემთხვევაში კი, მოწინააღმდეგის დაზიანების ხელსაყრელ პირობებს იძლევა;

- ✓ სოციალური ქსელები დისტანციურად (შენიღბულად), ყოველგვარი დამატებითი ძალისხმევის გარეშე ისეთი სახის სადაზვერვო ინფორმაციის მოპოვების საშუალებას იძლევიან, რომელთა მოპოვება ოპერატიულ-აგენტურული ღონისძიებების განხორციელებას მოითხოვს;

- ✓ ინტერნეტ პროვაიდერები სადაზვერვო ფუნქციის მატარებელ სახელმწიფო სპეცსამსახურებთან აქტიურად თანამშრომლობენ. შესაბამისად, მომსახურებას დაქვემდებარებული მოქალაქეები, უმაღლესი პოლიტიკური თანამდებობის პირები, სამართალდამცავი ორგანოების და სპეციალური სამსახურების თანამშრომლები, სადაზვერვო შესწავლა-კომპრომეტაციის მაღალი რისკის ობიექტებს წარმოადგენენ;

- ✓ სადაზვერვო საქმიანობის ოპერაციული ქმედებების ერთ-ერთ სახეობას კომპიუტერული მოწყობილობის ვირუსებით ინფიცირებით, ანონიმურად

ინფორმაციის შეკრება წარმოადგენს, რომელიც სადაზვერვო გადაბირების მიზნით, მაკომპრომეტირებელი მასალების მოპოვების საშუალებას იძლევა;

- ✓ სახელმწიფოებს შორის საომარი მოქმედებების დაწყებამდე, მიმდინარეობისას ან მის შემდგომ პერიოდში მოწინააღმდეგის ინტერნეტსივრცის პარალიზება მნიშვნელოვან სადაზვერვო ამოცანას წარმოადგენს. მისი განხორციელება შესაძლებელია „ჰაკერების“ დახმარებით ობიექტი სახელმწიფოს ინტერნეტ ქსელში დიდი რაოდენობის ქსელური პაკეტების გაგზავნა - არხების გადავსებით. აღნიშნული მიმართულებით სახელმწიფოთა შორის საომარი მოქმედებების მიმდინარეობამდე მოწინააღმდეგის საკომუნიკაციო არხების შესაძლებლობების შესახებ სადაზვერვო ხასიათის ინფორმაციის შეგროვება ხორციელდება;

- ✓ საკომუნიკაციო არხების გამოყენებით, მზვერავი ქვეყნის სპეციალური სამსახურები ობიექტი ქვეყნის ხელისუფლების წევრების ირგვლივ მადისკრედიტირებელ იმიტირებულ ფოტო-კოლაჟს ავრცელებენ, რაც სადაზვერვო კუთხით უარყოფითი საზოგადოებრივი აზრის შექმნის მაპროვოცირებელი გარემოებაა;

- ✓ სადაზვერვო-ოპერაციული ხასიათის ქმედებებს ელექტრონული კომუნიკაციით მოსარგებლე ობიექტი სახელმწიფოს სტრატეგიული და სასიცოცხლო ობიექტების (სახელმწიფო და კერძო სექტორი) ხანგრძლივი დროით მწყობრიდან გამოყვანა და მატერიალური ზიანის მიყენება წარმოადგენს, რის შედეგადაც კომპანიების მასიური გაკოტრება, ამ კომპანიებში დასაქმებული პირების უმუშევრად დატოვება, პროდუქციის შექმნის შეწყვეტა, საერთაშორისო სარეალიზაციო ბაზრებზე პოზიციის დაკარგვა, დაუცველობიდან გამომდინარე არსებული ხელისუფლებისადმი უარყოფითი განწყობა და მისგან მომდინარე მავნე შედეგები მიიღწევა.

ბიბლიოგრაფია

1. საქართველოს კანონის „სადაზვერვო საქმიანობის შესახებ“;

2. *Martin T. BimforT*, Intelligence as a Science, Studies in Intelligence, Vol. 2, No. 2, 1958, 78.

3. *Prabhakaram P.,* NATIONAL SECURITY, New delhi, Taya Mcgraw-Hill, 2008, 66.

4. *სვანიძე ვ., გოცირიძე ა.,* კიბერ თავდაცვა, თბილისი, საქართველოს თავდაცვის სამინისტრო, სსიპ-კიბერუსაფრთხოების ბიურო, 2015, 193;

5. *Jahankhani H., Lilburn Watson D., Me G., Leonhardt F.,* Handbook of electronic security and digital forensics, World Scientific, 2010, 266.

6. Police secrets leaked by computer virus, Press Releases, SAPHOS, 2006, <https://www.sophos.com/zh-tw/press-office/press-releases/2006/03/jppolice.aspx>, [16.08.2018].

7. Данные о составе войск США в Ираке случайно попали в открытый доступ в интернете, NEWSru.com, 30.11.2006, http://www.newsru.com/world/30nov2006/inet.html, [16.08.2018].

8. *Greenwald G., MacAskill E.,*NSA Prism program taps in to user data of Apple, Google and others, The Guardian, 07.06.2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, [16.08.2018].

9. *თავდაცვის სამინისტრო,* კიბერუსაფრთხოების საბაზისო კურსი, სსიპ-კიბერუსაფრთხოების ბიურო, 2016, 7-8.

10. *საქართველოში მომხდარ კონფლიქტთან დაკავშირებული ფაქტების დამდგენი დამოუკიდებელი საერთაშორისო მისია,* ანგარიში, ტომი III, 2009, 34.

11. *Markoff J.,* Before the Gunfire, Cyberattacks, The New York Times, 12.8.2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html>, [16.08.2018].

12. *საქართველოს მთავრობის დადგენილება N14* საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ, ქ.თბილისი, 13.01.2017, 4.

13. *Marcus D., Sherstobitoff R.,* Dissecting Operation High Roller, McAfee, Executive Summary, <http://www.mcafee.com/tw/resources/reports/rp-operation-high-roller.pdf>, [16.08.2018].