RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

რუსული „საინფორმაციო კონფრონტაციის“ ძირითადი მიმართულებები და შედეგები 2018 წლის საპრეზიდენტო არჩევნების პროცესში

ანდრია გოცირიძე

115

ექსპერტის აზრი

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

ექსპერტის აზრი

ანდრია გოცირიძე

რუსული „საინფორმაციო კონფრონტაციის“ ძირითადი მიმართულებები და შედეგები 2018 წლის საპრეზიდენტო არჩევნების პროცესში

115

2019

პუბლიკაცია დაიბეჭდა ამერიკის შეერთებული შტატების საელჩოს ფინანსური მხარდაჭერით. გამოცემაში გამოთქმული მოსაზრებები ეკუთვნის ავტორებს და შეიძლება არ ასახავდეს საელჩოს თვალსაზრისს.

ტექნიკური რედაქტორი: არტემ მელიქ-ნუბაროვი

ISSN 1512-4835
ISBN 978-9941-8-0961-3

„ინფორმაციული კონფრონტაცია“ (“Информационное Противоборство”), რომლის ძირითადი შედეგი მიზნობრივი აუდიტორიის ცნობიერების ფორმირება და ქცევის მანიპულირებაა, კრემლისათვის მსოფლიო არენაზე დომინირების ერთ-ერთი მნიშვნელოვანი საშუალებაა. რუსეთის სტრატეგიის ამ ასპექტის არსი დასავლური საზოგადოების წინააღმდეგ ბრძოლაა და ის ფსიქოლოგიური ომის საბჭოურ ტაქტიკას ემყარება. შედეგი – ინფორმაციული უპირატესობა (“Информационное Превосходство”) – ინფორმაციული კონტენტის მოპოვებასა და მისი გავრცელების ტექნიკურ საშუალებებზე კონტროლს გულისხმობს, რაც, არცთუ იშვიათად, ფსიქოლოგიური ოპერაციების მხარდამჭერი კიბერთავდასხმების განხორციელებას მოითხოვს. ამგვარი კიბეროპერაციების მიზანი ინტერესის ობიექტთა ქსელების კომპრომეტაციაა. ამ გზით მოპოვებული ინფორმაცია, დასახული სტრატეგიული ან ტაქტიკური ამოცანიდან გამომდინარე, დაშინების, შანტაჟის, დისკრედიტაციისა ან ფალსიფიკაციის მიზნით გამოიყენება. ხშირად, სასურველი ნარატივის დასანერგად ან განწყობის შესაქმნელად, კიბერშპიონაჟით მოპოვებული ინფორმაციული კონტენტი, თითქოსდა უნებლიე გაჟონვის გზით, ვრცელდება მასმედიით ან სოციალური ქსელებით.

გავრცელებული კონტენტი, ცრუ და ნამდვილი ინფორმაციის ნაზავი, გათვლილია დაბნეულ და დემორალიზებულ სამიზნე აუდიტორიაზე გავლენის მოსაპოვებლად. სამიზნე აუდიტორია კი, დასახული ამოცანიდან გამომდინარე, არის საკუთარი მოსახლეობა, სხვა ქვეყნების მაცხოვრებელთა ესა თუ ის ჯგუფი, თავად რუსეთისა და სამიზნე ქვეყნების პოლიტიკური ელიტა. რუსეთი ცდილობს, ინფორმაციული უპირატესობა მოიპოვოს, საამისოდ ის, ერთი მხრივ, ინფორმაციას ტექნიკურად ამუშავებს, სხვა მხრივ კი, აკონტროლებს შინაარსობრივ მხარესაც. სწორედ ამიტომ აპრობირებული ცნება „კიბერუსაფრთხოება“ რუსულ დოქტრინებსა და კონცეპტუალურ დოკუმენტებში ჩანაცვლებულია ტერმინით „ინფორმაციული უსაფრთხოება“.

რუსული პროპაგანდისტული კონტენტის გავრცელების, „საინფორმაციო კონფრონტაციის“ მნიშვნელოვანი ინსტრუმენტებია რუსული საინფორმაციო საიტები, სატელევიზიო თუ რადიოარხები (მაგალითად, Russia Today da Sputnik News), ბოტები, ტროლები, ოპტიმიზებული საძიებო სისტემები. ხშირია დასავლურ მედიაში ჟურნალისტების მოსყიდვაც. ავტორიტეტული ამერიკელი ექსპერტის მოსაზრებით, „DDoS შეტევა, კიბერშპიონაჟის მაღალგან-

ვითარებული ტექნიკა და ტელევიზია Russia Today საინფორმაციო ომის ურთიერთდაკავშირებული ინსტრუმენტებია“.[1]

ბოლო წლების განმავლობაში რუსეთის საინფორმაციო ომისა და მისგან განუყოფელი დესტრუქციული კიბეროპერაციების მნიშვნელოვანი მიმართულება სახელმწიფოთა დემოკრატიულ ინსტიტუტებსა და სისტემებზე თავდასხმები, საკვანძო პოლიტიკური ფიგურებისა და მმართველობის ფორმების დისკრედიტაციაა. ამ მიზნით, ჩვეულებრივ, კარგად კონსპირირებულ შეფარების ორგანიზაციებს, ფალსე ფლაგ ოპერაციებსა და სხვა ფარულ ღონისძიებებს მიმართავენ. კრემლის მიერ დაარსებულ-დაფინანსებული ან აუთსორსინგის გზით მოზიდული ჰაკერული დაჯგუფებები, სახელმწიფო ინტერესების სრული გათვალისწინებით, გართულებული ატრიბუციის პირობებში აწარმოებენ ფართო სპექტრის კიბეროპერაციებს – DDoS შეტევებს, რთული ფორმის კიბერშპიონაჟსა თუ სადეზინფორმაციო კამპანიებს. პოლიტიკური ფიგურებისა თუ ინსტიტუტების მაკომპრომეტირებელი მასალა ხშირად ქვეყნდება „დამოუკიდებელ“ საინფორმაციო სისტემებში (მაგალითად, WikiLeaks), რომლებიც წყაროს ანონიმურობისა და შენიღბვის დამატებით ღონისძიებებს უზრუნველყოფენ.

დასავლეთის ქვეყნების საარჩევნო პროცესებში ჩარევის მიზნით, მაკომპრომეტირებელი მასალების მოსაპოვებლად წარმართულ რუსულ კიბეოპერაციებში მნიშვნელოვან როლს ასრულებდა რუსულ სპეცსამსახურებთან ასოცირებული ორი ჰაკერული დაჯგუფება – APT 28 (Fancy Bear)[2] და APT 29 (Cozy Bear)[3]. მათ, სხვა გახმაურებული კიბერშეტევების გარდა, პასუხისმგებლობა ეკისრებათ აშშ-ის საპრეზიდენტო არჩევნებისას დემოკრატიული პარტიის სერვერებიდან ინფორმაციის არაავტორიზებულ დაუფლებაზე (ე.წ. DNC Hack). “DNC hack” განიხილება აშშ-ის არჩევნებში ჩარევად, რაც, დემოკრატიული პროცესების რწმენის შესასუსტებლად და კონკრეტული კანდიდატის კომპრომეტაციის მიზნით, სანქცირებული იყო რუსეთის ხელისუფლების უმაღლესი ეშელონების დონეზე.[4]

APT 28 ასევე პასუხისმგებელია ევროპის ქვეყნების თავდაცვის სექტორის საინფორმაციო სისტემებიდან ინფორმაციის მოპარვასა და საქართველოს სახელმწიფო სტრუქტურებისა თუ ჟურნალისტური წრეების წინააღმდეგ 2008-2014 წლებში განხორციელებულ კიბერჯაშუშურ კამპანიაზე. რაც შეეხება APT 29-ს, ამ დაჯგუფების სახელი აშშ-ის სახელმწიფო დეპარტამენტის, თეთრი სახლის, პენტაგონისა და სხვა სახელმწიფო უწყებების სისტემები-

დან არასაიდუმლო ინფორმაციის გაჟონვას უკავშირდება. DNC Hack პროცესში ორივე დაჯგუფება ფიგურირებს: APT 29-ს, არსებული მონაცემებით, დემოკრატიული პარტიის კომუნიკაციის საშუალებებზე, ელექტრონულ ფოსტასა და ჩატის კონტენტზე თითქმის წელიწადი ჰქონდა წვდომა.[5]

დაზვერვის წყაროებისა ან კონტროლირებადი მედიის მეშვეობით არასასურველ კანდიდატთა მაკომპრომეტირებელი ინფორმაციისა ან მათთვის საზიანო დეზინფორმაციის გავრცელების ტრადიცია სათავეს ჯერ კიდევ ცივი ომის დროიდან იღებს. რაც შეეხება არჩევნებში ჩასარევად კიბეროპერაციების გამოყენებას, რუსეთმა ამგვარი პრეცედენტი ჯერ კიდევ უკრაინის კონფლიქტისას შექმნა – 2014 წელს უკრაინის საარჩევნო ინფრასტრუქტურაზე მასირებული შეტევა განხორციელდა.

დაინტერესების ქვეყნების საარჩევნო პროცესებში ჩარევის სტიმულირებისა და შედეგებით მანიპულირებისათვის არსებობს მოქმედი სქემა. მასზე დაყრდნობით, საინფორმაციო სისტემებში გაბნეული და ღია წყაროებიდან გარკვეული პრინციპით ამოკრეფილი ინფორმაცია არჩევნებამდე დიდი ხნით ადრე გროვდება, შემდეგ კი, პოლიტიკური ფიგურებისა ან ინსტიტუტების დისკრედიტაციის მიზნით ვრცელდება. იმავდროულად, ტროლები ყალბი პროფილებით ამკვიდრებენ ცრუ ინფორმაციას. მათ ბლოგებში გარკვეულ თემათა წინასწარ წამოწევით ფეხს იკიდებს რუსული ნარატივი და ვრცელდება ცრუ ინფორმაცია, რაც განაპირობებს სასურველი საზოგადოებრივი აზრის ჩამოყალიბებას. ამ სქემის სისრულეში მოყვანას მნიშვნელოვნად ეხმარება „სასარგებლო იდიოტთა " მიერ გავრცელებული მოცულობითი კომენტარებიც.

ჯერ კიდევ 2011 წელს, რუსეთში ჩატარებული არჩევნების შემდგომ, ფეისბუქში დაგეგმილმა საპროტესტო გამოსვლებმა და „არაბული გაზაფხულის" მოვლენებმა კრემლს ნათლად დაანახა ინტერნეტისა და სოციალური ქსელების ძალა. შიდაპოლიტიკური სტაბილურობის მისაღწევად გაძლიერდა საინფორმაციო სივრცის გაკონტროლებისაკენ მიმართული ღონისძიებები, უკანასკნელ პერიოდში კი ამ სივრციდან ანტირუსული ინფორმაციისა და განწყობის განსადევნად ტროლების ტექნოლოგია გამოიყენეს საერთაშორისო არენაზეც – უკრაინაში, დასავლეთ ევროპასა და აშშ-ში.

2012 წელს ჰაქტივისტურმა დაჯგუფება Anonymous-მა გამოაქვეყნა მტკიცებულებები, რომლებიც ააშკარავებდნენ რუსეთის მთავრობის მიერ, ანტირუსული ინფორმაციის დისკრედიტაციის,

კრემლის მესიჯების ინტერნეტში გავრცელებისა და პროკრემლისტური განწყობების ჩამოყალიბების მიზნით, პროფესიონალი ტროლების ფინანსირების ფაქტებს.[6] ტროლებს ანაზღაურებას უხდიან ანტირუსული სტატიების კომენტირებისათვის, რეჟიმის საწინააღმდეგო ვიდეოების მისამართით გამოხატული ანტიპათიისათვის (ე.წ. dislike-ისთვის), ყალბი ონლაინპროფილების მართვისა და სოციალურ მედიაში ანტირუსული აზრის დევნისათვის. ტროლი ხშირად არაერთ ონლაინპროფილსა და ბლოგს იყენებს. თუმცა რუსული ტროლინგის მიზანი მხოლოდ აუდიტორიის კრემლის სისწორეში დარწმუნება როდია. მანვე უნდა შეუწყოს ხელი მედიის გადავსებას ყალბი შინაარსის კონტენტით, დაბადოს ეჭვი და შიში, გააჩინოს არასტაბილურობის განცდა, ხელი შეუშალოს დემოკრატიული ინტერნეტსივრცის გამოყენებას.

2014 წელს უკრაინის საარჩევნო სისტემაზე განხორციელებული კიბერშეტევებიდან მოყოლებული, კიბეროპერაციებს მეტნაკლები წარმატებით მიმართავდნენ საპრეზიდენტო არჩევნებისას აშშ-სა და საფრანგეთში, ასევე გერმანიის ბუნდესტაგის საარჩევნო პროცესში. დემოკრატიული ქვეყნების საარჩევნო პროცესებში ჩარევათა შემთხვევების განსაზოგადებლად, საინტერესო იქნებოდა, განგვეხილა საქართველოს პრეზიდენტის 2018 წლის საარჩევნო კამპანიის მიმდინარეობა, რუსული „საინფორმაციო კონფრონტაციის“ კვალი და ძირითადი შედეგები. მით უმეტეს, რომ აშშ-ის სადაზვერვო სამსახურების მიერ მომზადებულ სპეციალურ ანალიტიკურ მასალაში გამოთქმული ვარაუდით, მსოფლიოზე საკუთარი გავლენის გასაზრდელად რუსეთი მსგავს ტექნოლოგიებს, დიდი ალბათობით, აშშ-ის მოკავშირე ქვეყნების საარჩევნო პროცესებში ჩასარევადაც გამოიყენებს.[7] ამგვარ ეჭვს ამერიკელი ექსპერტებიც იზიარებენ.[8]

ამ დოკუმენტზე დაყრდნობით, რუსეთის მხრიდან არჩევნებში ჩარევა, გარდა კონკრეტული კანდიდატის რეპუტაციის შელახვისა, მიზნად ისახავდა დემოკრატიული პროცესებისა და, ზოგადად, არჩევნების ინსტიტუტის დისკრედიტაციას. ამასთანავე, გამარჯვებული კანდიდატის იმიჯი იქმნება ისე, თითქოსდა მას მხარს უჭერდეს რუსეთი, რაც აბრკოლებს საერთო-ეროვნული მიზნის გარშემო საზოგადოების კონცენტრაციას, ეს კი, თავის მხრივ, ხელს აძლევს რუსეთს.

გერმანიის კონტრდაზვერვითი ორგანოს ხელმძღვანელი ჰანს-გეორგ მაასენი (2012-2018) უფრო შორს მიდის და საეჭვოდ

მიიჩნევს, რომ აშშ-ის საპრეზიდენტო ან 2016 წელს გერმანიის ბუნდესტაგის არჩევნებისას რუსეთი მხარს უჭერდა რომელიმე კონკრეტულ კანდიდატს.[9] თავად უწყების ანგარიშის თანახმად, ამ შეტევების მთავარი მიზანი დემოკრატიული ინსტიტუტების გრძელვადიანი დისკრედიტაცია და სახელმწიფოს ნებისმიერი მომავალი მეთაურის მხარდაჭერის შესუსტებაა, რაც რუსული გეოპოლიტიკური ინტერესების რეალიზაციას უწყობს ხელს.[10] გერმანიის კონტრდაზვერვის ღია ანგარიშში ყურადღება გამახვილებულია ბუნდესტაგის არჩევნების პროცესში რუსეთთან აფილირებული ჰაკერული დაჯგუფებების მხრიდან არსებულ საფრთხეზეც. იმავე მაასენის მოსაზრებით,[11] გერმანიის არჩევნებისას რუსული დეზინფორმაციული კამპანიის მიზანი იქნება არა რომელიმე ერთი პარტიის მხარდაჭერა, არამედ დემოკრატიულ ინსტიტუტთა ნდობის შესუსტება და მომავალი კანცლერის შიდაპოლიტიკური მხარდაჭერის მინიმუმამდე დაყვანა, რაც შემდგომში, ისევე, როგორც აშშ-ის შემთხვევაში, რუსული საგარეო პოლიტიკისათვის დამატებითი ხეირი იქნება.[12]

საგულისხმოა, რომ არჩევნებისას გერმანიაში, როგორც აშშ-ში, მაკომპრომეტირებელი და სხვა ტიპის სენსიტიური ინფორმაცია ჰაკერებმა კიბერქსელებიდან მათ გამოყენებამდე ბევრად ადრე მოიპარეს: გერმანიაში – 2015 წელს ბუნდესტაგის ქსელებზე განხორციელებული კიბერშეტევებისას, ხოლო აშშ-ის დემკრატიული პარტიის საკომუნიკაციო ქსელებიდან კი – არჩევნებამდე თითქმის 1 წლით ადრე.

თუკი საქართველოს შიდაპოლიტიკური პროცესებით რუსეთის დაინტერესების ხარისხს, ქართული სახელმწიფო თუ კერძო სექტორის ქსელების დაუცველობასა და რუსეთის დესტრუქციულ კიბერაქტორთა წვდომის შესაძლებლობებს გავითვალისწინებთ, ცხადია, საპრეზიდენტო საარჩევნო კამპანიაში რუსული ნარატივის მნიშვნელობა და რუსული გავლენა ცალსახად ყურადსაღებია. ცნობილი ფაქტია, რომ კრემლთან დაკავშირებულ აქტორებს, მათ შორის APT28-ს, დიდხანს ჰქონდა არასანქცირებული წვდომა ქართულ სახელმწიფო, საკომუნიკაციო თუ ბიზნესქსელებზე, რის შედეგადაც, ქართული სამსახურებისათვის უცნობი, სავარაუდოდ, დიდი მოცულობის, სენსიტიური ინფორმაცია წლების განმავლობაში რუსული სპეცსამსახურების ხელში ხვდებოდა.[13] რაც შეეხება ჩვენს არჩევნებს, გარდა იმისა, რომ არსებობდა არალეგალურად მოპოვებული მაკომპრომეტირებელი მასალა, ამა თუ იმ კანდიდატისა ან

მათ მხარდამჭერ პოლიტიკურ ძალთა მოსაზრება-გამონათქვამები ერთობ ფაქიზ თემებსა და პროცესებზე, რომლებიც ხელმისაწვდომი იყო ღია რესურსებსა და სოციალურ ქსელებში, კარგი კონტენტი იყო გასავრცელებლად.

რუსულმა „საინფორმაციო კონფრონტაციამ“ მიზანს მიაღწია. დამოუკიდებლად იმისგან, თუ ვინ გაიმარჯვა არჩევნებში, ამგვარ შეტევათა ფონზე მოვლენები კრემლისათვის რამდენიმე მიმართულებით წარმატებულად განვითარდა, ეს კი ჩვენი სახელმწიფოსათვის არაერთ საფრთხეს შეიცავს:

- რუსეთთან ფარული თუ ღია კავშირის აქცენტირებითა და შესაბამისი კონტენტის ტირაჟირებით მოხერხდა ორივე კანდიდატის მაქსიმალური დისკრედიტაცია. დამკვიდრებული იმიჯის შესაბამისად, არჩეული პრეზიდენტი რუსეთისათვის სასურველ ან მის მიერ მართულ კანდიდატად აღიქმება, რაც მას, პრაქტიკულად, შიდაპოლიტიკურ მხარდაჭერას უკარგავს. ამგვარი იმიჯის გასამყარებლად რუსეთის ოფიციალური პირები საპარლამენტო თუ სამთავრობო დონეზეც კი არ მოერიდნენ შესაბამის განცხადებებს. პრეზიდენტს, რომელიც დაკარგავს სათანადო შიდაპოლიტიკურ მხარდაჭერას, წაერთმევა ლავირების უნარი და შესაძლებლობა, სადეოკუპაციო მოლაპარაკებებისას (თუნდაც მტრულ ძალასთან) აწარმოოს მოქნილი პოლიტიკა;
- იმ კანდიდატის გამარჯვება, რომლის იმიჯიც ოკუპანტთან და მის მხარდაჭერასთან ასოცირდება, აღვივებს ანტაგონისტურ განწყობებს და ხელს უწყობს მაქსიმალურად დიდი საპროტესტო ელექტორატის ჩამოყალიბებას. ამგვარად წარმართულმა კამპანიამ გამოიწვია არჩეული პრეზიდენტის (მიუხედავად ვინაობისა) მიმართ ანტაგონისტურად განწყობილი ოპოზიციის (ამომრჩეველთა 40-45%-ის) ჩამოყალიბება. ამ გარემოებათა გათვალისწინებით, მმართველობის პერიოდში მისი ყურადღება, ნაცვლად სახელმწიფოსათვის მნიშვნელოვან საკითხებზე კონცენტრირებისა, ძირითადად, არსებული წინააღმდეგობის დაძლევას დაეთმობა;
- რუსთთან დაკავშირებულ პერსონად მიჩნეული პრეზიდენტის, უმაღლესი მთავარსარდლის, არსებობა საზოგადოებაში აღძრავს განცდას, რომ ქვეყნის მმართველი წრეები კრემლისადმი ლოიალური ძალებითაა დაკომპლექტებული, ეს კი, თავის მხრივ, პრორუსული ძალებისა და ელიტის ფორმირება-გაძლიერებას განაპირობებს;

- კრემლისადმი ლოიალობის ზრდასა და ეროვნული იდეის უზურპაცია-დისკრედიტაციას ხელს უწყობს მკვეთრად პრორუსული პოლიტიკური ძალების მიერ მეორე ტურის წინ, თითქოსდა ერის კონსოლიდაციის მიზნით, ეროვნული პრობლემატიკით გაჯერებული ხალხმრავალი აქციების გამართვა. შესაძლოა, რუსეთისათვის ეს ერთგვარი სიგნალი აღმოჩნდეს პრორუსული პოლიტიკური ძალების ქვეყნის მმართველობაში ამა თუ იმ ფორმით მონაწილეობისათვის მზადყოფნის შესახებ. გარდა ამისა, ამგვარმა აქციებმა კიდევ უფრო გააღრმავა განცდა, რომ კანდიდატს, არჩეულ პრეზიდენტს, მხარს უჭერენ რუსეთისადმი ლოიალური ძალები, ეროვნულ ძალთა ნიშას კი პრორუსული პარტიები იკავებენ;
- 2008 წლის რუსეთ-საქართველოს ომის ინიციატორის თემის, საერთაშორისო სასამართლოზე ქართველი სამხედროების თითქოსდა გასამართლების საფრთხის წამოწევა სახელმწიფოსათვის უკიდურესად წამგებიან კონტექსტში მოხდა. მოგვიანებით საერთაშორისო საკომუნიკაციო ქსელებში 9 აპრილის თემაზე გავრცელებული მოსაზრებებიც ეროვნული გრძნობების შეურაცხმყოფელი იყო. ამ თემას თავისი კომენტარებით შეხმატკბილებულად და მასშტაბურად გამოეხმაურნენ ტროლები და „სასარგებლო იდიოტები“. გამთიშავი პროპაგანდის აგორებული ტალღა შეეხო არაერთ ავტორიტეტულ ჯგუფს – სამხედრო მოსამსახურეებს, ვეტერანებს, ეკლესიასა და ა.შ.;
- საინფორმაციო სივრცეში კვლავ გაისმა და სადისკუსიოდ იქცა „ომის დაწყების“, „ჰააგის სასამართლოს“, „ფაშისტური, ნაცისტური რეჟიმის“, „ლუსტრაციისა“ და არაერთი სხვა საკითხი, უკიდურესად არასახარბიელო როგორც შიდაპოლიტიკური, ასევე საერთაშორისო თვალსაზრისით. ასეთი დისკუსია, ერთი მხრივ, აღრმავებს გამთიშავ პროცესებს და ართულებს კონსოლიდაციას სახელმწიფოებრივი მნიშვნელობის პრობლემატიკის გარშემო, სხვა მხრივ კი, ლახავს ქვეყნის საერთაშორისო იმიჯს;
- საერთაშორისო დამკვირვებლებისა და სტრატეგიული პარტნიორების ამა თუ იმ შეფასებაში 2012 წლის შემდგომ პირველად გაისმა საარჩევნო სისტემისა და პროცესის კრიტიკა,[14] მოსაზრებები ნეგატიურ საარჩევნო კამპანიაზე, ერთ-ერთი ძალის სასარგებლოდ რესურსების არათანაბარ განაწილებასა და ამომრჩევლის მოსყიდვაზე. მსგავს შეფასებებს,[15] მით უმეტეს, მომავალი საპარლამენტო არჩევნებისას პრობლემის გაღრ-

მავების შემთხვევაში, იმ გათვლით, რომ ევროატლანტიკური ინტეგრაციის პროცესის გაჭიანურება ქვეყნის დემოკრატიის არასათანადო ხარისხს მიეწერება და არა თუნდაც ნატოში გაწევრიანებაზე რუსეთის „ვეტოს“, მოწინააღმდეგე ხელიდან არ გაუშვებს.[1617] ეს ფაქტორი საქართველოს ევროინტეგრაციისადმი სკეპტიკურად განწყობილ ქვეყნებს მოუხსნის დისკომფორტს, რომელსაც დემოკრატიულ საზოგადოებას ევროატლანტიკურ ბლოკში ინტეგრაციაზე რუსული პოზიციის გავლენა უქმნის. მოვლენათა ამგვარი განვითარება გააჩენს პოლიტიკური თუ ეკონომიური არასტაბილურობის განცდას, რაც საინფორმაციო კონფრონტაციის ერთ-ერთი ძირითადი მიზანია;

- სოციალური ქსელებისა და, ზოგადად, კიბერსივრცის ძირგამომთხრელი საქმიანობისთვის გამოყენება, განსაკუთრებით, მეზობლებთან ან/და პარტნიორებთან ურთიერთობისას, „საინფორმაციო კონფრონტაციის“ ერთ-ერთი მიმართულებაა. ამგვარი ქმედებების მიზანი, ჩვეულებრივ, არის ნდობის შესუსტება, სტრატეგიულ პარტნიორებთან ან მეზობელ სახელმწიფოსთან ურთიერთობის გაფუჭება, რაც პოლიტიკურ, სამხედრო, ჰუმანიტარულ თუ სხვა სახის მხარდაჭერას, მოსალოდნელი აგრესიის შემთხვევაში, გაართულებს. ამ მიზნით, ორივე კანდიდატისა და მათი მხარდამჭერების გამოსვლებიდან ამოკრეფილი და ამ ნიშნით დალაგებული ციტატების კომენტირებისას განსაკუთრებული აქცენტი გაკეთდა იმ ინციდენტებსა და გამონათქვამებზე, რომლებიც ეროვნული უმცირესობებით დასახლებულ რეგიონებსა თუ პარტნიორი სახელმწიფოების წარმომადგენლებს შეეხებოდა. ტრადიციული, ხშირად ყოფითი, სამეზობლო დავის სახელმწიფოთაშორისი ურთიერთობების კონტექსტში განხილვა ან ერთაშორისი ურთიერთობის უკიდურესად ნეგატიურ ჭრილში ჩვენება, ტრადიციულად სენსიტიური საკითხების აქცენტირება, უარყოფით კონტექსტში წარმოჩენილი პრობლემატიკის ტირაჟირება სოციალური ქსელებით და შემდგომ ამაზე დისკუსიის გამართვა ტროლების, „სასარგებლო იდიოტების“ თუ სხვა საშუალებათა გამოყენებით, საბოლოო ჯამში, ერთაშორისი ან სახელმწიფოთაშორისი პრობლემაა.

ამრიგად, განსხვავებით აშშ-ის საპრეზიდენტო არჩევნებისა, სადაც, დემოკრატიული პროცესებისა და საარჩევნო სისტემის დისკრედიტაციის მიღმა, რუსეთი აშკარად ერთ-ერთი კანდიდატის კომპრომეტაციის მიზნით მოქმედებდა, საქართველოს საპრეზიდენტო არჩევნებში რუსული ინტერესები კონცენტრირდა ორივე კანდიდა-

ტის მაქსიმალურ დისკრედიტაციაზე, იმ მიზნით, რომ არჩეულმა პრეზიდენტმა ვერ ისარგებლოს შიდაპოლიტიკური მხარდაჭერით ქვეყნისათვის მნიშვნელოვან საკითხების, პირველ რიგში კი, დეოკუპაციისა და ევროატლანტიკური ინტეგრაციის პროცესებთან დაკავშირებული პრობლემების, გადაწყვეტისას. გარდა აღნიშნულისა, პროპაგანდისტული თვალსაზრისით, უკიდურესად ნეგატიურად დამუხტული კამპანიის მთავარი სამიზნე იყო თავად საზოგადოება, რომლის აზრიც, განსაკუთრებით, სენსიტიურ სახელმწიფოებრივ საკითხებზე, უნდა გახლეჩილიყო. საპრეზიდენტო კამპანიისას, სამწუხაროდ, აშკარა იყო პრორუსული განწყობების მქონე პოლიტიკური ელიტების როლის გააქტიურება, თითქოსდა მათი ეგიდით მოსახლეობა ეროვნული იდეის გარშემო გაერთიანდებოდა.

მნიშვნელოვანი პროპაგანდისტული რესურსი დაიხარჯა საიმისოდ, რომ, ნებისმიერი კანდიდატის გამარჯვების შემთხვევაში, არჩეულ პრეზიდენტს რუსეთის მიერ მხარდაჭერილის იმიჯი ჰქონოდა, რაც, ერთი მხრივ, ჩამოაყალიბებდა ანტაგონისტურად განწყობილ დიდ საპროტესტო ელექტორატს, მეორე მხრივ კი – პრორუსულ ელიტას.

მსგავსი ტენდენციები ყურადსაღებია, ვინაიდან კრემლის სასარგებლოდ ცნობიერების ცვლა, პრორუსულ ელიტათა ფორმირების უკიდურესად სახიფათო პროცესი, კრიტიკული მასის ჩამოყალიბების შემთხვევაში, შესაძლებელია, კონვენციური თავდასხმის წინაპირობად და ხელშემწყობ ფაქტორად იქცეს.

მნიშვნელოვანია იმ საპასუხო ნაბიჯების განხილვა, რომელთა მეშვეობითაც მოხერხდება არჩევნებში რუსული მხარის ჩარევის პრევენცია და ნეგატიური ზეგავლენის მინიმიზაცია. განვითარებული კიბერშესაძლებლობებისა და/ან მძლავრი სამხედრო პოტენციალის მქონე სახელმწიფოებს შეუძლიათ საპასუხო ნაბიჯების დეკლარირება, რაც დესტრუქციული კიბერაქტივობებისა თუ არჩევნების შედეგებით მანიპულირებისაგან თავის ასარიდებლად მარჯვე ხერხია. მაგალითად, საფრანგეთსა და გერმანიაში, რომლებმაც საარჩევნო პროცესებში რუსეთის აქტივობას აშშ-ზე უკეთ გაართვეს თავი, სხვა ფაქტორებთან ერთად, პრევენციული ეფექტი სწორედ ასეთმა განცხადებებმა იქონია.[18] საფრანგეთის თავდაცვის მინისტრმა მძლავრი კიბერდანაყოფის ჩამოყალიბებისა და, შესაძლო ჩარევის შემთხვევაში, კიბერშეტევისა თუ კონვენციური პასუხის შესახებ საჯაროდ განაცხადა.[19] მოგვიანებით საგარეო საქმეთა მინისტრმა ისიც დაამატა, რომ საფრანგეთი არც რუსე-

თის მხრიდან და არც რომელიმე სხვა სახელმწიფოსაგან მოითმენდა საარჩევნო პროცესში რაიმე სახის ჩარევას. გაფრთხილება და ერთგვარ სამაგიეროზე მინიშნება შეგვიძლია ამოვიცნოთ გერმანიის კონტრდაზვერვის ხელმძღვანელის, ჰანს-გეორგ მაასენის, განცხადებაშიც, რომელშიც მკაფიოდ ითქვა, რომ რუსეთი დეზინფორმაციული კამპანიისათვის ემზადებოდა და ეს ფსიქოლოგიური ოპერაცია რუსეთის უმაღლესი პოლიტიკური ხელმძღვანელობის მიერ იყო სანქცირებული.[20]

ცხადია, საქართველო, მასშტაბებიდან გამომდინარე, მოკლებულია ამგვარი განცხადებებისა და, მეტადრე, ქმედებების შესაძლებლობას. უფრო მეტიც, არათანაბარი ძალებისა და რუსეთის რეგიონალური ინტერესების გამო, ამგვარი რიტორიკა საფრთხილოცაა. შესაბამისად, საქართველომ პრობლემის გადაწყვეტის შიდასახელმწიფოებრივი გზები უნდა ეძიოს.

მნიშვნელოვანია, შეიქმნას კიბერთავდაცვის ეფექტური მექანიზმი, რომელიც, ტექნიკურ შედეგზე ორიენტირებული კიბერშეტევის შემთხვევაში, უსაფრთხოების უზრუნველყოფასაც შეძლებს და დესტრუქციულ კიბეროპერაციათა საინფორმაციო-ფსიქოლოგიური ეფექტის პრევენციასაც:

- არცთუ უშედეგო იქნება კიბერთავდაცვითი ორგანიზაციების ჩართვა არჩევნებზე ნეგატიური ზეგავლენის პრევენციისათვის გათვალისწინებულ ღონისძიებებში. მოქმედების სავარაუდო არეალი ამგვარად შეიძლება განისაზღვროს: საფრთხეთა იდენტიფიცირება, საფრთხის წყაროების კვლევა, მოსალოდნელი საფრთხისა და დესტრუქციული აქტორების შესახებ მიზნობრივი ჯგუფების ინფორმირება;
- ცნობიერების ასამაღლებლად აუცილებელია, რეგულარული სახე მიეცეს პროაქტიურ კამპანიას მედიის წარმომადგენლებთან, პოლიტიკურ პარტიებსა თუ საარჩევნო პროცესის სხვა მონაწილეებთან. მნიშვნელოვანია, რომ ზემოთ ჩამოთვლილ აქტორებს წინსწრებით მიეწოდებოდეს ინფორმაცია რუსეთის დესტრუქციულ კიბეროპერაციებზე, შესაძლო არხებზე, მოსალოდნელ შედეგებსა თუ ეფექტურ თავდაცვით ღონისძიებებზე;
- კიბერშეტევების შედეგებთან დაკავშირებით, ეფექტურია დროული გასაჯაროებისა და ტრანსპარენტულობის პოლიტიკა. ხშირად, ვითომდა რეპუტაციის მოსაფრთხილებლად, მიყენებული ზიანი, რომელზე დაყრდნობითაც შემდგომში პროპაგანდისტული კონტენტი მზადდება და ვრცელდება, არ საჯაროვდება;

- დეზინფორმაციის ნეგატიური შედეგების გასაბათილებლად საჭიროა სოციალური მედიის გააქტიურება. ამ თვალსაზრისით, მნიშვნელოვანია სამოქალაქო პლატფორმაც – აქტივისტთა ჩართულობა და მოხალისეობრივ საწყისებზე კიბერთავდაცვით ოპერაციებში აქტიური კიბერთავდაცვის არაკრიმინალურ ღონისძიებათა ინტეგრაცია;
- საფრანგეთის პრეცედენტმა ცხადყო, რომ პროდუქტიულია პროპაგანდის დადგენილი არხების (მოცემულ შემთხვევაში, RT-ისა და Sputnik-ის) დროებითი ან გრძელვადიანი გადაკეტვა საკანონმდებლო დონეზე, თუნდაც ერთჯერადი სამართლებრივი აქტებით;
- ინფორმაციის კატეგორიზაცია და საჯარო სამსახურებსა თუ პოლიტიკურ აქტორთა საინფორმაციო სისტემებში საინფორმაციო ტექნოლოგიების უსაფრთხო მოხმარების კულტურის დანერგვა უსათუო აუცილებლობაა. ღია, კონფიდენციალური და სენსიტიური ინფორმაციის გადაცემისას გვერდს ვერ ავუვლით საინფორმაციო არხების დივერსიფიკაციას, ზოგიერთ შემთხვევაში კი, გარდაუვალია ამგვარი ინფორმაციის სრული ამოღება.

ბიბლიოგრაფია

1. “Distributed denial of services attacks (DDoS), advanced [cyber] exploitation techniques and Russia Today television are all related tools of information warfare.” D. J. Smith, ‘How Russia Harnesses Cyberwarfare,’ Defense Dossier, American Foreign Policy Council, Issue 4, August 2012, p. 8, ხელმისაწვდომია 11.12.2018 www.afpc.org/publications/e-journals/cyberspace-the-new-battlefield

2. FANCY BEAR (იგ. APT 28, Sofacy, Pawn Storm), რუსული წარმოშობის კიბერაქტორი, აქტიურია 2000-იანი წლების შუა პერიოდიდან და პასუხისმგებელია საჰაერო სივრცეზე, თავდაცვის და ენერგეტიკის სფეროებზე, სახელმწიფო თუ მედიასექტორზე განხორციელებულ კიბერთავდასხმებზე. თავდასხმების არეალი ფართოა და მოიცავს აშშ-ს, დასავლეთ ევროპას, ირანს, იაპონიას, საქართველოს, მალაიზიასა და სამხრეთ კორეას. ის ცნობილია თავდაცვის სექტორსა და სხვა სამხედრო მიზნებზე განხორციელებული კიბერშპიონაჟის გახმაურებული ფაქტით, რომლის პროფილიც, ფაქტობრივად, ემთხვეოდა რუსეთის სამხედრო დაზვერვის გენერალური შტაბის მთავარი სადაზვერვო სამმართველოს (Главное Разведывательное Управление, GRU) ინტერესთა სფეროს. FANCY BEAR-ის სახელს უკავშირდება გერმანიის ბუნდესტაგსა და ფრანგულ TV5 Monde-ზე 2015 წლის აპრილში განხორციელებული შეტევები. გარდა კიბერშპიონაჟის ზემოაღნიშნული ფაქტისა, მან სახელი გაითქვა კარგად ორგანიზებული ფიშინგშეტევებით.

3. COZY BEAR (იგ. CozyDuke ან APT 29) არის რუსული ჰაკერული დაჯგუფება, რომელმაც ახლო წარსულში განახორციელა წარმატებული კიბერშეტევები თეთრ სახლზე, სახელმწიფო დეპარტამენტსა და აშშ-ის გაერთიანებულ შტაბებზე. გარდა აღნიშნულისა, დაჯგუფების სამიზნეებია თავდაცვისა და ენერგეტიკის სექტორი, საფინანსო და სადაზღვევო სფეროები, ფარმაინდუსტრიული და ტექნოლოგიური კვლევები, მედია და ანალიტიკური ცენტრები. აღწერილია თავდასხმები დასავლეთ ევროპის, ჩინეთის, ბრაზილიის, მექსიკის, იაპონიის, თურქეთისა და შუა აზიის ქვეყნებზე. ის ცნობილია Sprea-Phishing ტექნიკის მიზანმიმართული ფიშინგშეტევებით.

4. Intelligence Community Assessment. Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution. ICA 2017-01D, 6 January 2017.

5. www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

6. www.theguardian.com/world/2012/feb/07/putin-hacked-emails-russian-nashi.

7. Intelligence Community Assessment. Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution. ICA 2017-01D, 6 January 2017.

8. საფრანგეთის საპრეზიდენტო არჩევნებში რუსული ჰაკერული ორგანიზაციის მოქმედების აღწერისას დ. სმიტი ასკვნის: “Russia is indeed conducting a broad integrated strategy to attack western democratic processes. Let us see what unfolds before and after the May 7 French presidential run-off election but Pawn Storm is more than a French affair.” იხ. D. Smith. Pawn Storm: More then a French Affair, www.cyberlightglobal.com/insight-blog/.

9. www.express.co.uk/news/world/993893/Russia-German-election-Merkel.

10. Bundesministerium des Inners. Verfassungsschutzberricht 2016. SPIONAGE UND SONSTIGE NACHRICHTENDIENSTLICHE AKTIVITÄTEN.

11. www.reuters.com/article/us-germany-election-russia-idUSKBN19P1FK.

12. www.dw.com/ru/берлин-знает-чего-ждать-от-хакеров-из-рф-во-время-выборов/a-39540359.

13. Fire eye special report, 2014. APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? об. www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

14. www.state.gov/r/pa/prs/ps/2018/11/287714.htm.

15. www.amerikiskhma.com/a/interview-with-rasa-jukneviciene/4671137.html?fbclid=IwAR0ocHfc5MLNAs7ETHZh4g3BJeusOF5JUCz8FgZGK5zNRsWCIkY0FtQhdRc.

16. www.russian.rt.com/world/news/578141-gosdep-gruziya-vybory-narusheniya.

17. www.apsny.ge/2018/pol/1544637855.php?utm_source=dlvr.it&utm_medium=facebook&fbclid=IwAR2hl_983a7CdGCxYguIv1qka1w__7O4xidhFBrbBpyf2glotWS1OfqrwsQ.

18. Mika Aaltola, Safeguarding democratic elections against cyber-enabled autocratic meddling. The Finnish Institute of International Affairs. FIIA Briefing Paper 226, November 2017.

19. Jean-Baptiste Jeangène Vilmer. Successfully Countering Russian Electoral Interference. CSIS Brief. June 2018.

20. "We recognize this as a campaign being directed from Russia. Our counterpart is trying to generate information that can be used for disinformation or for influencing operations. Whether they do it or not is a political decision." (Quoted by Reuters (4 May 2017). Germany challenges Russia over cyberattacks, www.reuters.com/article/us-germany-security-cyber-russia/germany-challenges-russia-over-alleged-cyberattacks-idUSKBN1801CA (14.12.2018).