RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

ანტიდასავლური საინფორმაციო ომის ევროპული პერსპექტივა

ერეკლე იანტბელიძე

165

ექსპერტის აზრი

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

ექსპერტის აზრი

ერეკლე იანტბელიძე

ანტიდასავლური საინფორმაციო ომის ევროპული პერსპექტივა

165

2021

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

„მიუხედავად იმისა, რომ ჩვენს თვალებს არ შეუძლიათ შეაღწიონ მომავლის სიბნელეებში, სამეცნიერო გეოპოლიტიკური ანალიზი საშუალებას გვაძლევს გავაკეთოთ გარკვეული პროგნოზები“.
კარლ ჰაუსჰოფერი, 1942

(Gearóid Ó Tuathail, 2003)

შესავალი

საერთაშორისო პოლიტიკური რეალობის გადასვლა ახალ მულტიპოლარულ პრიზმაში აქტუალობას სძენს გეოპოლიტიკას, როგორც ინტერდისციპლინარული სწავლების ერთ-ერთ მიმართულებას. ციფრული და სამეცნიერო ტექნოლოგიების განვითარებამ ახალ ეტაპზე გადაიყვანა ძალთა ბალანსის ფენომენი და რიგი სახელმწიფოებისა თუ საერთაშორისო სამთავრობო ორგანიზაციებისათვის ტერმინი გეოპოლიტიკა იქცა უსაფრთხოების სტრატეგიის, კულტურული დომინირებისა და დემოკრატიული პროცესების ფლაგმანად. ახალი „გეოპოლიტიკური კომისიის“ პირობებში, ურსულა ფონ დერ ლაიენის სამოქმედო გეგმა ემყარება ორ ძირითად პრინციპს – ევროპის კლიმატურ და ციფრულ ტრანზიციას (European Parliament, 2020). შესაბამისად, ღირებულებათა ომის პირობებში, გეოპოლიტიკა და ციფრული, ტექნოლოგიური განვითარება გახდა ის უმნიშვნელოვანესი კომპონენტები, რომელთა პრიორიტეტად წამოწევასაც ცდილობს ევროკავშირი მსოფლიოს მოწინავე სახელმწიფოებთან (ჩინეთი, ინდოეთი, რუსეთი, თურქეთი) ჭიდილში. როგორც ევროკავშირის ტოპ დიპლომატმა ჯოსეფ ბორელმა განაცხადა, ევროპა არ უნდა გახდეს სხვა დიდი სახელმწიფოების სათამაშო მოედანი და ევროკავშირმა უნდა იტვირთოს გეოპოლიტიკური ლიდერის როლი მსოფლიოში (Barigazzi, 2019). აღსანიშნავია ისიც, რომ ევროპის გეოპოლიტიკურობა ითვალისწინებს სამეზობლო პოლიტიკის განვითარებასა და გრადუალურ გაფართოებას. თუმცა აღმოსავლეთ პარტნიორობის ფორმატში (EaP) ასოცირებულ პარტნიორებს (მოლდოვა, საქართველო, უკრაინა) აქვთ იმაზე მეტი ამბიციაც და მიზნებიც, ვიდრე ღრმა და ყოვლისმომცველი სავაჭრო სივრცის განვითარება (DCFTA) და ასოცირების ხელშეკრულების (AA) სრული იმპლემენტაციაა (European Commission, 2019).

რეგიონალური თვალსაზრისით, რუსეთის მიერ საქართველოს ტერიტორიების ოკუპირება 2008 წლის აგვისტოში, ასევე

2014 წელს ყირიმის ანექსიისა და შეიარაღებული კონფლიქტის წარმოება დონბასის რეგიონში გახდა რუსული ჰიბრიდული ომის მხილების მთავარი წყარო. საპასუხოდ, ევროპის მრავალი სახელმწიფოსათვის რუსეთის მიერ ომის წარმოების არსებული ფორმა აღმოჩნდა განგაშის საბაბი და შიდაპოლიტიკური პოლარიზაციის ერთერთი მთავარი მიზეზი. მაშინ, როდესაც შვედეთი და პოლონეთი ღიად უჭერენ მხარს აღმოსავლეთ პარტნიორებთან უსაფრთხოების კუთხით მჭიდრო თანამშრომლობას, ევროკავშირის სხვა წევრი სახელმწიფოები უარყოფენ ამ მიმართულებით პოლიტიკური პროცესების განვითარებას, მათ შორის, ინკლუზიურობასა და დიფერენციაციას სამეზობლო პოლიტიკის ფორმატში (Gerasimov, 2020). მიუხედავად ამისა, ასოცირებული პარტნიორების გარდა, აზერბაიჯანიც გამოხატავს ევროკავშირთან თანამშრომლობის სურვილს ჰიბრიდული ომის, დეზინფორმაციის, პროპაგანდის დაძლევისა და „რბილი უსაფრთხოების“ (soft security) განვითარების თვალსაზრისით.

ზემოთ აღნიშნული პოლიტიკური მოვლენები და ინტერესთა კონფლიქტი უშუალოდ ევროკავშირის წევრ-სახელმწიფოებში აუცილებელს ხდის გადაიდგას ერთიანი ევროპული ქმედითი ნაბიჯები და შეიქმნას ფუნქციური მექანიზმები (გარდა ევროპის უსაფრთხოების სტრატეგიისა 2020-2024 წწ.) საინფორმაციო და ჰიბრიდული ომის დასაძლევად. შესაბამისად:

- ნაშრომის მიზანია, გაანალიზოს ევროკავშირის როლი ანტიდასავლური, ჰიბრიდული ომის წინააღმდეგ;
- შეაფასოს რუსული პროპაგანდისა და დეზინფორმაციის მნიშვნელობა ევროპული სახელმწიფოების შიდაპოლიტიკურ პროცესებში;
- ახსნას აღმოსავლეთ პარტნიორობის მნიშვნელობა დეზინფორმაციის დაძლევისა და ევროპული უსაფრთხოების განმტკიცებაში.

ევროკავშირი და რუსული „მასკიროვკა (2.0)“

ევროპის არცერთი სახელმწიფოსათვის და არც ევროკავშირისათვის აღარ არის უცხო ის ფაქტი, რომ რუსეთის ფედერაცია ხშირად მიმართავს საბჭოთა გამოცდილებას. მაშასადამე, არც

უსაფრთხოებისა და ჰიბრიდული ომის პირობებში მოხდა საბჭოთა წარსულის უგულებელყოფა. ე.წ. „მასკიროვკის“ დოქტრინა რომელიც აერთიანებდა ტაქტიკურ გათვლებსა და პრინციპებს, ხშირად გამოიყენებოდა წითელი არმიის სამხედრო მოქმედებებში (Elliott, 2018). დღესდღეობით რუსეთმა აღნიშნული კონცეფცია კიდევ უფრო განავითარა თეორიული და პრაქტიკული დანიშნულებით, რასაც დაემატა ახალი სამთავრობო საშუალებების ნუსხა, კერძოდ: მედიით მანიპულირება, ენერგო და საწვავი რესურსებით ვაჭრობა, პოლიტიკური აგიტაცია, კიბერთავდასხმები, ე.წ. სუროგატი სამხედრო ძალების წაქეზება, აგენტების ჩანერგვა და ანტისახელმწიფოებრივი პროცესების პროვოცირება (Roberts, 2015). მნიშვნელოვანია ის ფაქტიც, რომ შემუშავებული დოქტრინა მუდმივი ადაპტაციის პირობებში ცდილობს იპოვოს სახელმწიფოს ის სუსტი მხარეები, რომლებიც საშუალებას მისცემს, მყისიერი რეაგირება მოახდინოს პოლიტიკურ დესტაბილიზაციაზე, საზოგადოებრივი აზრის პოლარიზებასა და რადიკალიზაციაზე (Vowell, 2015).

რუსეთის სამხედრო, პოლიტიკური, ადმინისტრაციული და მედია უწყებები, შეიძლება ითქვას, რომ დახელოვნებული არიან „მასკიროვკის (2.0)“ პრაქტიკაში გატარებით. ამის საპასუხოდ, ევროკავშირს არ გააჩნია ერთიანი, ჰოლისტიკური მიდგომა, რომელიც გადაიქცევა რუსული ანტიდასავლური, ინფორმაციული ომის შემაკავებლად. მეორე მხრივ, უნდა აღინიშნოს 2017 წელს ევროკავშირის კიბერუსაფრთხოების სააგენტოს მიერ შექმნილი Cyber Diplomacy Toolbox და ევროკავშირის ქსელისა და ინფორმაციის უსაფრთხოების სააგენტოს (ENISA) ფუნქციონირება (Pawlak, 2017). არსებული საშუალებებით ხდება შიდა ინსტიტუციონალურ დონეზე უსაფრთხოების ზომების დაცვა და პოტენციური კიბერთავდასხმების თავიდან აცილება. მასშტაბური თვალსაზრისით, ევროკავშირი ჯერჯერობით ძალიან მცირე რაოდენობის ფინანსურ თუ ტექნოლოგიურ რესურსს ხარჯავს, რაც კიდევ უფრო მეტ თავდაჯერებულობას მატებს რუსეთის სპეცსამსახურებს, რათა ძალის დემონსტრირება მოახდინონ დასავლურ სახელმწიფოებში. როგორც ვლადიმერ პუტინის სპეციალური წარმომადგენელი ინფორმაციული უსაფრთხოების საკითხში აღნიშნავს, რუსეთი კიბერგიგანტია, ხოლო ევროკავშირი – პატარა, არარელევანტური, მყეფარე ქოფაკი (Gressel, 2019).

საერთო ევროპული ღირებულებებით გაერთიანებული სახელმწიფოებისა და ინსტიტუტების შეცდომა ისაა, რომ მოკავშირე ქვეყნები ძალიან გვიან მიხვდნენ, როგორც მ. ვაისი და პ. პომერანცევი აღნიშნავენ, „კულტურისა და იდეების შეიარაღებას" (weaponization of culture and ideas) რუსეთის ანტიდასავლური პოლიტიკის ქვეშ (Weiss, 2014). შესაბამისად, 2015 წელს ევროპის საბჭომ გადადგა პირველი ნაბიჯი და ევროპის საგარეო საქმეთა სამსახურის (EEAS) დაქვემდებარებაში შეიქმნა ციფრული პლატფორმა, სახელწოდებით – East StratCom Task Force, რომლის მეშვეობითაც პირველ ეტაპზე მოხდა 4 000-მდე პროპაგანდისტული და დეზინფორმაციული ისტორიების გამოაშკარავება და მათი გასაჯაროება (www.euvsdisinfo.eu) ვებგვერდზე. ასევე 2016 წლის საპარლამენტო რეზოლუციის მიხედვით, ზემოაღნიშნულმა ინსტიტუტმა მიიღო პირველი ბიუჯეტური დაფინანსება 1.1 მილიონი ევროს ოდენობით და პრიორიტეტული გახადა, სოციალური მედია-პლატფორმების (Twitter, Facebook, Instagram) გამოყენებით რუსეთის ანტიდასავლური პროპაგანდის მხილება (European Parliament, 2019). ევროკავშირის მიერ გადადგმულმა ამ კონკრეტულმა ნაბიჯებმა კარგი შედეგი გამოიღო fake news-ის გამოვლენის თვალსაზრისით, თუმცა სახელმწიფოებსა და ევროინსტიტუტებს კიდევ ბევრი აქვთ სამუშაო ციფრული პლატფორმების, კოორდინირებული სტრატეგიისა და მოქალაქეთა ცნობიერების ამაღლების თვალსაზრისით.

საბედნიეროდ, ევროპის უსაფრთხოებისა და თავდაცვის პოლიტიკა მუდმივმოქმედი სტრუქტურული თანამშრომლობის (PESCO) პირობებში ითვალისწინებს მნიშვნელოვანი პროექტების განხორციელებას კიბერუსაფრთხოებისა და კონტრდაზვერვის მიმართულებით. მათ შორის აღსანიშნავია სწრაფი რეაგირებისა და ურთიერთდახმარების პროგრამა კიბერთავდასხმების შემთხვევაში. ასევე, სტრატეგიული მართვისა და კონტროლის (C2) სისტემების გაუმჯობესება კიბერსაფრთხეებსა და ინციდენტებზე რეაგირების თვალსაზრისით (EU Cyber Direct, 2019). მიუხედავად ამისა, "PESCO" თავისი სტრუქტურითა და მიზნებით არის ინტერესთა კონფლიქტის ერთ-ერთი მთავარი საბაბი ევროკავშირის წევრ-სახელმწიფოთა შორის. პოლიტიკოსთა ნაწილი თანამშრომლობის ფორმატს აღიქვამს, როგორც ევროპის სამომავლო უსაფრთხოების გარანტს, ხოლო ტექნოკრატთა მეორე ნაწილი უარყოფს კავშირის შიგნით გარკვეული ტიპის სამხედრო ალიანსის შექმნას. შესაბამისად, არა-

საკმარისი კოორდინაციისა და ღირებულებათა კონფლიქტების პირობებში, ევროკავშირს და მის დაქვემდებარებულ ინსტიტუტებს უჭირთ ეფექტურად გაუმკლავდნენ რუსული „მასკიროვკის (2.0)“ ანტიდასავლურ განზრახვებს.

ევროპული არჩევნები და „სიმართლის ილუზია“

> „თუ სიცრუე ხშირად იბეჭდება, ის ხდება კვაზი სიმართლე. ხოლო თუ ასეთი სიმართლე ხშირად მეორდება, ის ხდება რწმენის საგანი, დოგმა, რის გამოც ადამიანი თავსაც გასწირავს“.
> იზაბელ ბლაგდენი, 1869

(Stafford, 2016).

რუსული ჰიბრიდული ომის გადააზრება ევროპის მასშტაბით, რა თქმა უნდა, ხდება შიდა სახელმწიფოებრივ დონეზეც. დასავლურ სახელმწიფოთა საზოგადოებრივი წრეები ხშირად არიან რუსული დეზინფორმაციული მანიპულირების მსხვერპლნი. სიცრუის აპელირება და ანტიდასავლური რიტორიკა, როგორც წესი, ყოველდღიურად იჩენს თავს. მიუხედავად ამისა, რესურსების მობილიზებას რუსეთის ხელისუფლება, უმეტეს შემთხვევაში, ახდენს წინასაარჩევნო პერიოდის დროს, როდესაც საზოგადოებრივ აზრზე ზემოქმედება ძალიან მარტივია და ემოციური ფონი მაღალია. რუსული „რბილი ძალის“ მექანიზმები მოქმედებენ თითქმის ყველა ევროპულ სახელმწიფოში. მათ შორის აღსანიშნავია საინფორმაციო საშუალებები, კერძოდ: „Sputnik News” და „Russia Today”. რუსეთი მხარს უჭერს ყველა იმ მეთოდს, რომელიც ევროპული პოლიტიკის დესტაბილიზაციას ახდენს, რაც გამოიკვეთა შოტლანდიისა და კატალონიის რეფერენდუმების დროს, ასევე საფრანგეთის „ყვითელი ჟილეტების“ საპროტესტო გამოსვლების პერიოდში (Gressel, 2019).

ევროპულ სახელმწიფოთა გარკვეულმა ნაწილმა რუსული ჰიბრიდული ომის საპასუხოდ გამოყო სპეციალური დანაყოფები და დიპლომატიური წარმომადგენლები, რომლებიც კოორდინირებას უწევენ დეზინფორმაციული საფრთხეების გამოვლენას. ასეთი სახელმწიფოების რიცხვს მიეკუთვნება: ლიეტუვა, ფინეთი, პოლონეთი, შვედეთი და ესპანეთი. რაც შეეხება გერმანიასა და საფრანგეთს, ორივე სახელმწიფო ცდილობს არაპირდაპირი გზით გამოააშკარაოს რუსული ანტიდასავლური ქმედებები, თუმცა ისე, რომ

ამას არ ჰქონდეს პოლიტიკური ხასიათი. უნგრეთის, ავსტრიისა და იტალიის შემთხვევაში, ხელისუფლების წარმომადგენლები პრიორიტეტულად არ აღიქვამენ დეზინფორმაციული ომის საფრთხეებს და თავს იკავებენ კონფრონტაციაში შევიდნენ რუსეთთან, თავდაცვისა და უსაფრთხოების საკითხებთან მიმართებით. გასაკვირი არ არის, რომ დასავლური სამყაროსათვის შოკისმომგვრელი აღმოჩნდა რუსული „ბოტების“, „ტროლებისა“ და „ანგარიშების“ გამოყენება ბრექსიტის რეფერენდუმის დროს. როგორც ორგანიზაცია F-Secure აცხადებს, მოხდა Twitter-ისა და Facebook ანგარიშების გამოყენება დეზინფორმაციული და პროპაგანდისტული ნარატივის გასავრცელებლად (Ellyatt, 2020). ციფრულ დონეზე მოხდა როგორც ევროპული ღირებულებების გაშარჟება, ისე ევროკავშირის სტიგმატიზება. საინტერესოა ის ფინანსური დანახარჯი, რაც რუსეთის ფედერაციამ გაიღო ბრიტანული რეფერენდუმისათვის. როგორც Hanns Seidel Foundation-ის კვლევიდან ირკვევა, საერთო ჯამში, რუსეთმა გაიღო 1 353 000 გირვანქა სტერლინგი, საიდანაც 102 000 დაიხარჯა Facebook-ის ანგარიშებზე, ხოლო 50 000-დან 100 000-მდე – Twitter-ის ანგარიშებზე (Špalková, 2018). ასევე კრემლის დაქვემდებარებაში მყოფმა მედიასაშუალებებმა მოახერხეს ნეგატიური ზეგავლენა მოეხდინათ დაახლოებით 134 მილიონ ამომრჩეველზე, მათ შორის, 11 მილიონ ბრიტანელზე, რომლებიც ცხოვრობენ საზღვარგარეთ.

ერთ-ერთი ყველაზე თვალსაჩინო მაგალითი რუსეთის დეზინფორმაციული ბარიერის გადალახვისა დაფიქსირდა 2017 წელს საფრანგეთში. ემანუელ მაკრონის საპრეზიდენტო საარჩევნო კამპანიის დროს კიბერ და ინფორმაციული თავდასხმის შედეგად, ელექტრონული ფოსტის მეშვეობით გავრცელდა სურათები, ინვოისები და პერსონალური დოკუმენტები, რომლებიც შეიცავდა „Fake" მასალებს საპრეზიდენტო კანდიდატის შესახებ. როგორც სტრატეგიული და საერთაშორისო სწავლების ცენტრის ხელმძღვანელი ჰეზერ ა. კონლი აცხადებს, საფრანგეთის პოლიტიკური ინსტიტუტები მომზადებული შეხვდნენ კიბერთავდასხმებს და სწრაფად მოახერხეს ყალბი მასალების გამოვლენა. ასევე დიდი როლი შეასრულა ფრანგული პოლიტიკური ცენტრალიზაციის პრაქტიკამ (რაც არ უნდა გასაკვირი იყოს!). ინტეგრირებული და ზედამხედველობითი მეთოდების მეშვეობით საფრანგეთის სადაზვერვო სამსახურებმა მოახერხეს ინტერვენციის წყაროს გამოაშკარავება, რამაც ძლიერი

ზეგავლენა ვერ მოახდინა საპრეზიდენტო არჩევნების შედეგებზე (Bulckaert, 2018). მიუხედავად ამისა, რუსეთის ანტიდასავლურმა ინფორმაციულმა პრაქტიკამ ტრანსფორმაცია განიცადა და 2018 წლიდან ფრანგულ საინფორმაციო ველზე ადგილი დაიმკვიდრა Russia Today-მ, რომელიც აუდიენციას არა მხოლოდ ტელევიზიით, არამედ ვებსაიტებისა და სოციალური მედიის გამოყენებით აწვდის ანტიდასავლურ პოლიტიკურ ნარატივს.

ზემოთ განხილული მაგალითების გათვალისწინებით, შეიძლება ითქვას, რომ რუსეთის დეზინფორმაციული სტრატეგია ძალიან მოქნილი და ცვალებადია. მიუხედავად იმისა, რომ ევროკავშირის მოქალაქეებს აქვთ მაღალი პოლიტიკური კულტურა, დეზინფორმაციული ბარიერის გადალახვა ძალიან რთულია და მოითხოვს დიდ მენტალურ და ფსიქოლოგიურ მედეგობას. სიმართლის ილუზიაში გახვევისგან დღესდღეობით არ არის დაზღვეული არც ერთი სახელმწიფო და, მით უმეტეს, ინდივიდი.

აღმოსავლეთ პარტნიორობა და „შეუსრულებელი მისია“

ევროპული პერსპექტივის გათვალისწინებით შეიძლება ითქვას, რომ აღმოსავლეთ პარტნიორობის რეგიონი წარმოადგენს ყველაზე უფრო მყიფე ტერიტორიას ჰიბრიდული საფრთხეების გავრცელების თვალსაზრისით. როგორც Rand Europe-ის კვლევაშია ნაჩვენები, რუსული სოციალური მედიის გავლენის სფეროები ყველაზე მეტად ამ რეგიონში ვრცელდება, რაც გამოწვეულია რიგი კულტურული, ენობრივი, რელიგიური და სოციალურ-ეკონომიკური ფაქტორებით (Todd C. Helmus, 2018). რუსეთის მხრიდან ანტიდასავლური და დეზინფორმაციული პროპაგანდის როლი ახდენს გავლენას როგორც სახელმწიფოთა შიდა, ისე საგარეო პოლიტიკურ პროცესებზე. თვისებრივად სახელმწიფოებს, როგორებიცაა მოლდოვა, საქართველო და უკრაინა, აერთიანებთ მწარე ისტორიული გამოცდილება რუსეთის ფედერაციასთან ურთიერთობისა. ასევე თითოეული სახელმწიფო ოკუპირებულია რუსული და სეპარატისტული ძალების მიერ (მიუხედავად იმისა, რომ დნესტრისპირეთის შემთხვევაში რუსეთი პოტენციურად „შემრიგებლის“ როლს ითავსებს). რელიგიური და ასევე ეთნიკური ბარიერი ქმნის მყარ გარემოს იმისათვის, რომ რუსულმა მედიასაშუალებებმა ზეგავლენა მოახდინონ მოსახლეობის დიდ ნაწილზე და ხელი შეუწყონ საზოგა-

დოებრივი აზრის პოლარიზაციას. მნიშვნელოვანია ის ფაქტიც, რომ ევროკავშირის ასოცირებული პარტნიორები არიან დემოკრატიული ტრანზიციის გზაზე და მოქალაქეების ნდობა სახელმწიფო ინსტიტუტების მიმართ ძალიან დაბალია. ამ და სხვა ელემენტების გათვალისწინებით, აღმოსავლეთ პარტნიორობის რეგიონი წარმოადგენს ერთგვარ ლაბორატორიას რუსული ჰიბრიდული სტრატეგიის მოდერნიზაციისა და წარმატებული ტრანსფორმაციისათვის.

ყოველწლიურად მედიისა და სახელმწიფო ინსტიტუტების მხრიდან ვრცელდება ინფორმაცია რუსული კიბერთავდასხმებისა და ინფორმაციული ინტერვენციის შესახებ სახელმწიფოთა საარჩევნო პროცესებში. ქართულ რეალობაში თავდასხმა მოხდა 2019 წლის 15-17 ოქტომბერს კერძო და საჯარო ვებგვერდებზე, რომელმაც უშუალოდ ვერ გამოავლინა რუსული ან საგარეო სახელმწიფოებრივი ინტერვენცია საქართველოს ინტერნეტსივრცეში, თუმცა კიდევ უფრო მეტად დააფიქრა დასავლური სახელმწიფოები კიბერუსაფრთხოების განვითარების აუცილებლობასა და მნიშვნელობაზე (Kakha Gogolashvili, 2019). გარდა ამისა, 2020 წლის 1 სექტემბერს განხორციელდა კიდევ ერთი კიბერთავდასხმა ლუგარის ლაბორატორიაზე, რომელიც შეფასდა უდიდეს საფრთხედ კოვიდ-19-ის პანდემიის პირობებში (U.S. Embassy in Georgia, 2020). დეზინფორმაციული კამპანია შეეხო მოლდოვას საპარლამენტო არჩევნების დროს. ამ შემთხვევაში Facebook-ის ანალიტიკურმა სამსახურმა გამოავლინა 168 Fake-ანგარიში, რომლებიც, მათი ცნობით, იყო ლოკალური და არანაირი კავშირი არ ჰქონდა რუსეთთან (Gressel, 2019). აღწერილი მაგალითების საფუძველზე შეიძლება ითქვას, რომ აღმოსავლეთ პარტნიორობის რეგიონში რუსეთი იმაზე მარტივად, დაფარულად ახერხებს დეზინფორმაციითა და საზოგადოებრივი აზრით მანიპულირებას, ვიდრე ცენტრალურ და დასავლეთ ევროპულ სახელმწიფოებში. რუსეთის ფედერაციისათვის რეგიონი წარმოადგენს როგორც საგარეო პოლიტიკის გავლენის მთავარ სფეროს, ისე ჰიბრიდული ომის სტრატეგიული გაუმჯობესების მთავარ სივრცეს.

ვინაიდან ევროინსტიტუტებისა და ევროკავშირის წევრსახელმწიფოთათვის რუსულ ჰიბრიდულ ომთან გამკლავება წააგავს ერთგვარ „შეუსრულებელ მისიას“, აუცილებელია იმ რესურსის გამოყენება, რომელიც აქვს აღმოსავლეთ პარტნიორობის რეგიონს. კოორდინირებული სტრატეგიული მიდგომების მეშვეობით შესაძლებელია ანტიდასავლურ ნარატივთან სრულად თუ

არა, ეფექტურად გამკლავება. უმნიშვნელოვანესია, ევროკავშირმა მხარი დაუჭიროს ისეთ ორგანიზაციებსა და ინიციატივებს, როგორიცაა „მედიარეფორმების ცენტრი“ უკრაინაში. ამ ორგანიზაციის მეშვეობით ხორციელდება საგანმანათლებლო პროექტები დასავლური ჟურნალისტური სტანდარტების დასამკვიდრებლად. ასევე ორგანიზაციის მთავარ საკვლევ სფეროში შედის დეზინფორმაცია და პროპაგანდა, რომელიც საერთაშორისო საზოგადოებას სტატიებითა და სტატისტიკური მონაცემებით აცნობს Fake News-ის ნეგატიური დანიშნულებას. ორგანიზაციას აქვს ელექტრონული პლატფორმა (www.stopfake.org), რაც უფრო მეტად ხელმისაწვდომს ხდის საერთაშორისო აუდიტორიისათვის ანტიდასავლური ნარატივის წყაროებისა და ხელოვნურად შეთხზული ისტორიების გამოაშკარავებას (Stop Fake, 2020).

ტექნოლოგიურ პროგრესთან ერთად რადიკალურად შეიცვალა ინფორმაციული ომის დატვირთვაცა და პრინციპებიც. რადგან „რბილი ძალისა“ და პროპაგანდის სტრატეგიულად გამოყენება, შესაძლოა, გაცილებით ეფექტური აღმოჩნდეს, ვიდრე სამხედრო ძალის დემონსტრირება, აუცილებელია, ევროპის თავდაცვისა და უსაფრთხოების სტრატეგიაში განხორციელდეს ცვლილებები აღმოსავლეთის მიმართულებით. რუსული ჰიბრიდული ომის პირობებში, აღმოსავლეთ პარტნიორობის ფორმატის კიბერუსაფრთხოების კუთხით გაფართოება ევროკავშირს აქცევს გავლენიან გეოპოლიტიკურ მოთამაშედ საერთაშორისო მასშტაბით. რეგიონში უსაფრთხოებისა და თავდაცვის სფეროს მიმართულებით თანამშრომლობა ევროკავშირს მისცემს იმის შესაძლებლობას, რომ განავითაროს ტექნოლოგიები და მყისიერი რეაგირება მოახდინოს რუსული ჰიბრიდული ომის ტრანსფორმირებულ ელემენტებზე.

დასკვნა და რეკომენდაციები

შესაძლოა, ვერ მოხერხდეს შეღწევა რუსული ჰიბრიდული ომის სტრატეგიულ სიღრმეებში, თუმცა როგორც კარლ ჰაუსჰოფერი აცხადებს, გეოპოლიტიკისა და, ამ შემთხვევაში, გეოპოლიტიკური ევროპის პირობებში შესაძლოა გვქონდეს რელევანტური პროგნოზი რუსეთის სამომავლო ანტიდასავლური გეგმების შესახებ. კიბერუსაფრთხოების განვითარება და დეზინფორმაციული ბარიერის გადალახვა ითვალისწინებს ჰოლისტიკურ და კონსტრუქციულ

მიდგომას ევროპის კონტინენტზე. კიდევ ერთხელ უნდა გაესვას ხაზი აღმოსავლეთ პარტნიორობის ფორმატის მნიშვნელობას რუსული ანტიდასავლური საინფორმაციო ომის წინააღმდეგ, რადგან აღნიშნული რეგიონი არის რუსული პოლიტიკური და პროპაგანდისტული გავლენების პირველადი სამიზნე. საჭიროა ევროკავშირმა გადადგას ნაბიჯი, როგორც პოლიტიკურ და ციფრულ, ისე დიპლომატიურ ფრონტზე რუსული ჰიბრიდული ომის დასაძლევად. შესაბამისად, აღნიშნული სტრატეგია საჭიროებს სხვადასხვა ტიპის ქმედებებს, როგორც ევროკავშირის წევრი-სახელმწიფოების, ისე აღმოსავლეთ პარტნიორობის ფორმატის წევრი-ქვეყნების მხრიდან:

- ევროკავშირს ესაჭიროება ერთიანი მიდგომა, თუ როგორ განავითაროს აღმოსავლეთ პარტნიორობის ფორმატი. საჭიროა ამ ფორმატის არა განახლება (update), არამედ – განვითარება (upgrade).
- აუცილებელია ინკლუზიურობისა და დიფერენციაციის საბოლოო დანერგვა EaP-ის ფორმატში, რაც ასოცირებულ წევრებს საშუალებას მისცემს მიიღონ მეტი სარგებელი ევროკავშირთან თანამშრომლობით. შესაბამისად, საჭიროა დიფერენციაციის პირობებში შეიქმნას უსაფრთხოებისა და თავდაცვის საერთო ფორმატი, რომელიც მოიცავს ანტიდასავლურ პროპაგანდასთან გამკლავებას, დეზინფორმაციასთან ბრძოლას და კიბერუსაფრთხოების განვითარებას (Gogolashvili, 2018).
- მნიშვნელოვანია, ევროკავშირმა შექმნას საერთო სამართლებრივი სტანდარტი დეზინფორმაციასთან გამკლავების თვალსაზრისით, რაც მოიცავს აღმოსავლეთ პარტნიორების ფორმატში მიღებული სტანდარტების გაზიარებასა და დანერგვას.
- საჭიროა, გაიზარდოს ფინანსური და ტექნიკური დახმარება, როგორც ENISA-ის, ისე Europol-ის, და შეიქმნას ახალი მექანიზმები კიბერუსაფრთხოების განმტკიცებისათვის.
- აუცილებელია ევროკავშირის დიპლომატიური კორპუსის გაძლიერება ახალი „კიბერალიანსის“ ჩამოყალიბების მიზნით, როგორც საერთაშორისო ორგანიზაციებთან (ნატო, გაერო), ისე სტრატეგიულ პარტნიორებთან (აშშ, ავსტრალია, კანადა, იაპონია).

- ევროკავშირის ასოცირებულმა პარტნიორებმა დღის წესრიგში უნდა დააყენონ ციფრული უსაფრთხოებისა და სტრატეგიული თანამშრომლობის საკითხები. ღიად უნდა გამოხატონ მზადყოფნა ევროკავშირთან უსაფრთხოებისა და თავდაცვის კუთხით დაახლოების შესახებ.

* * *

„ჩვენ გრძელი გზა გვაქვს გასავლელი, მაგრამ კიდევ უფრო გაზრდილია იმპულსი, რომ გავაძლიეროთ ჩვენი კოლექტიური შესაძლებლობები უსაფრთხოებისა და თავდაცის სფეროში“.
ჯოსეფ ბორელი, 2020

(European External Action Service, 2020)

ბიბლიოგრაფია

- Barigazzi, J. (2019, 10 19). “Borrell urges EU to be foreign policy ‘player, not the playground.’” Brussels, Belgium. Retrieved from https://www.politico.eu/article/on-foreign-policy-josep-borrell-urges-eu-to-be-a-player-not-the-playground-balkans/
- Bulckaert, N. (2018, 07 17). “How France successfully countered Russian interference during the presidential election.” Paris, France. Retrieved from https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/
- Elliott, J. K. (2018, 06 09). “Theatricality and deception: How Russia uses ‘maskirovka’ to shake the world.” Canada. Retrieved from https://globalnews.ca/news/4260938/russia-strategy-maskirovka-military-politics-putin/
- Ellyatt, H. (2020, 07 21). “UK intelligence report says Russia is a capable cyber actor and its influence is the ‘new normal.’” New York, U.S.A. Retrieved from https://www.cnbc.com/2020/07/21/uk-report-says-russia-meddled-in-scottish-referendum.html
- *EU Cyber Direct*. (2019, 11 20). Retrieved from https://eucyberdirect.eu/: https://eucyberdirect.eu/content_knowledge_hu/cyber-related-pesco-projects/
- European Commission. (2019). *Ursula von der Leyen - Mission letter.* Brussels: European Union. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/president-elect_von_der_leyens_mission_letter_to_oliver_varhelyi.pdf
- European External Action Service. (2020, 06 21). *EEAS Europe*. Retrieved from www.eeas.europe.eu: https://eeas.europa.eu/headquarters/headquarters-homepage/81247/europe-security-and-defence-way-forward_en
- European Parliament. (2019). *Online disinformation and the EU’s response.* Brussels: European Union. Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf
- European Parliament. (2020). *The von der Leyen Commission’s priorities for 2019-2024.* Brussels: European Union. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646148/EPRS_BRI(2020)646148_EN.pdf
- Gearóid Ó Tuathail, S. D. (2003). *The Geopolitics Reader.* New York: Taylor & Francis e-Library. Retrieved from https://frenndw.files.wordpress.com/2011/03/geopol-the-geopolitics-reader.pdf
- Gerasimov, C. (2020). “An Eastern Policy Update, but No Upgrade.” *German Council on Foreign Relations*, 2-9. Retrieved from https://dgap.org/sites/default/files/article_pdfs/DGAP-Policy%20Brief-2020-05.pdf
- Gogolashvili, K. (2018). *www.gfsis.org*. Retrieved from https://www.gfsis.org/files/library/pdf/English-2651.pdf
- Gressel, G. (2019, 06 01). PROTECTING EUROPE AGAINST HYBRID THREATS. Berlin, Germany.

- Kakha Gogolashvili, V. P. (2019). *Hybrid Threats in EaP Countries: Building a Common Response.* Tbilisi, Chisinau, Kyiv, Erevan, Brussels. : Georgian Foundation for Strategic and International Studies.
- Pawlak, E. M. (2017). *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?* Brussels: European Union Institute for Security Studies (EUISS). Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf
- Roberts, J. Q. (2015). "Maskirovka 2.0: Hybrid Threat, Hybrid Response." *Joint Special Operations University*, 1-24. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/1007494.pdf
- Špalková, V. (2018). *INFLUENCE OF RUSSIAN DISINFORMATION OPERATIONS: SPECIFIC EXAMPLES IN DATA AND NUMBERS.* Prague: Hanns Seidel Foundation. Retrieved from https://www.europeanvalues.net/wp-content/uploads/2019/02/Influence-of-Russian-Disinformation-Operations-Specific-examples-in-data-and-numbers.pdf
- Stafford, T. (2016, 10 26). "How liars create the 'illusion of truth.'" London, England. Retrieved from https://www.bbc.com/future/article/20161026-how-liars-create-the-illusion-of-truth
- *Stop Fake*. (2020, 09 04). Retrieved from www.stopfake.org: https://www.stopfake.org/en/main/
- Todd C. Helmus, E. B.-B. (2018). Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. Santa Monika, California, U.S.A: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf
- *U.S. Embassy in Georgia*. (2020, 10 01). Retrieved from www.ge.usembassy.gov: https://ge.usembassy.gov/u-s-embassy-statement-on-september-1-2020-cyberattack-against-georgian-ministry-of-health/?fbclid=IwAR2BRVtUZu8Yrgr2Gj-IrnSBT4al-EBjgLmJG3t-ZmWvZAHYmJca_rLUS4s#.X1FI1L_ovcI.facebook
- Vowell, C. J. (2015). *RealClear Defense* . Retrieved from realcleardefense.com: https://www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html
- Weiss, P. P. (2014). "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money." *The Interpreter*, 14-30. Retrieved from https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf