რუსეთ-უკრაინის ტექნოლოგიური ომი

თორნიკე ზედელაშვილი
პოლიტიკის მეცნიერების დოქტორი, იუსტიციის სამინიტროს
ციფრული მმართველობის სააგენტოს, ინფორმაციული
უსაფრთხოების დეპარტამენტის თანამშრომელი,
ინტერნეტგამოცემა „ლიდერის“ დამფუძნებელი,
კავკასიის საერთაშორისო უნივერსიტეტის მოწვეული ლექტორი.
ელ-ფოსტა: thomaszedelashvili@gmail.com
ORCID: 0000-0003-2630-1779

აბსტრაქტი: შავიზღვისპირეთი წარმოადგენს პრიორიტეტულ რეგიონს, სადაც ფიგურირებს ექვსი ქვეყანა – რუსეთი, თურქეთი, უკრაინა, რუმინეთი, ბულგარეთი და საქართველო. რა თქმა უნდა, ამ ქვეყნებიდან ყველაზე დიდ გავლენას შავიზღვისპირეთზე ახდენს რუსეთი, შემდეგ თურქეთი. შესაბამისად, რუსეთ-უკრაინის ომი დიდ პოლიტიკურ, ეკონომიკურ და სოციალურ რისკებს აჩენს როგორც სამხრეთ კავკასიაში, ასევე მთელ შავიზღვისპირეთში. მით უფრო, როცა მსოფლიო იმყოფება ტექნოლოგიური მიღწევების ისეთ ფაზაში, როცა აქტიურად მიდის საუბარი ჯარისკაცების რობოტებით ჩანაცვლებაზე. გარკვეულწილად ეს უკვე მუშაობს, ექსპერტები აღნიშნულ ომს უწოდებენ ტექნოლოგიურ ომს, ეს კი მის ხანგრძლივობაზეც ახდენს გარკვეულ ზეგავლენას. შავიზღვისპირეთის ქვეყნებს სჭირდებათ ახალი ტექნოლოგიური დაცვა. რუსეთ-უკრაინის ომის კოლოსალურ ზარალში თანამედროვე ტექნოლოგიების გამოყენებას დიდი წვლილი შეაქვს – დაიღუპა უამრავი ადამიანი და განადგურდა ინფრასტრუქტურა. ეს დაპირისპირება დიდი დოზით მოიცავს კიბერშეტევებს, დეზინფორმაციას, ეკონომიკურ ზეწოლას, ჰიბრიდული ომის კომპონენტებს. ახალი არ გახლავთ, თანამედროვე ტექნიკას უკრაინა იღებს ამერიკის შეერთებული შტატებიდან, ჩრდილოატლანტიკური ალიანსიდან, ევროკავშირიდან, დიდი ბრიტანეთიდან, გერმანიიდან, საფრანგეთიდან, პოლონეთიდან და სხვა ევროპული ქვეყნებიდან. ახალი ტექნოლოგიების გამოყენება, როგორიცაა კიბერომის წარმოება, ხელოვნური ინტელექტის გამოყენება, შეიძლება ითქვას, გავლენას უკვე ახდენს გეოპოლიტიკასა და საომარ მოქმედებებზე პოტენციური სარგებლით, ერთი მხრივ ზარალის შემცირებით თავდაცვითი მიმართულებით, ხოლო მეორე მხრივ თავდასხმის შემთხვევაში ზარალის გაზრდით, დეტალური სამიზნე ინფორმაციის მიწოდებით და ლოჯისტიკურ საკითხებში დახმარებით. ასევე, ***AI*** გამოიყენება საინფორმაციო-ფსიქოლოგიური ომი წარმოების დროს. მაღალი აქტივობით მუშაობს ხელოვნური ინტელექტის ტექნოლოგიები კიბერთავდასხმებში, რაც მეტად საშიშ რელობას ქმნის.

საკვანძო სიტყვები: ხელოვნური ინტელექტი; კიბერშეტევები; კიბერომი; შავიზღვისპირეთი; ტექნოლოგიები; დეზინფორმაცია; ჰიბრიდული ომი.

* * *

(Cyberattacks);
სოციალური მედია (Social Media);
დრონები (Drones);
თანამგზავრები (Satellites);
ტელეკომები საზღვრების გარეშე (Télécoms Sans Frontières – TSF);
ელექტრონული ბრძოლა – ომი (Electronic warfare);
სამომხმარებლო ტექნოლოგია და აპლიკაციები (Consumer technology and applications);
VR და 3D ჰოლოგრამები (VR & 3D holograms),

მათ შორის, უახლესი ტექნოლოგიები, პლატფორმები ხელოვნური ინტელექტის მიმართულებით, რაც ეხმარება სხვადასხვა გადაწყვეტილებების მიღებასა და განხორციელებაში – ***„RZ-500***

თავდასხმითი დრონი, სადაზვერვო დრონი PD-1 / PD-2, Hunter RSVK-M2 უპილოტო სამხედრო მანქანები, საზენიტო სარაკეტო სისტემა Stugna-P, ST-35 Silent Thunder მოძრავი საბრძოლო თვითმფრინავი" (Kryvenko P.)

საარტილერიო სარაკეტო სისტემები

რუსეთმა გამოიყენა სხვადასხვა ტიპის საარტილერიო და სარაკეტო სისტემები – სარაკეტო გამშვებები, ***ჰაუბიცები,*** ბალისტიკური რაკეტები და სხვა. გამოიყენა უკრაინის კონტროლირებად ტერიტორიებზე სამიზნეების დაბომბვის მიზნით. უკრაინის კომუნიკაციების სამსახურის განცხადებით, 2022 წლის ოქტომბრის მონაცემებით, 4000-ზე მეტი საბაზო სადგური, 60000 კმ. ოპტიკურ-ბოჭკოვანი ხაზი და 18 სამაუწყებლო ანტენა არის განადგურებული, დაზიანებული ან მოპარული.

ამერიკის შეერთებულ შტატებში წარმოებული ***Javelin-ის*** ტანკსაწინააღმდეგო საბრძოლო მასალის გამოყენება უკრაინელებს საქმეს უადვილებთ. ასევე ეხმარება ამერიკული ტექნოლოგიური კომპანიის – ***Palantir-ის*** პროგრამული უზრუნველყოფა, უკვე შესაძლებელია რუსული ტანკებისა და არტილერიის მიზანში მარტივად ამოღება. იგი ხელს უწყობს კომერციული თანამგზავრებიდან და სოციალური მედიის არხებიდან არმიის პოზიციების ვიზუალურ ჩვენებას და შემდგომ ხდება მათი განადგურება. თერმული გამოსახულების ტექნოლოგია აადვილებს ციფრული დამიზნების შესაძლებლობებს.

ხელოვნური ინტელექტი (AI)

უკრაინა ხელოვნური ინტელექტის ტექნოლოგიების დიდ ნაწილს იყენებს თავდაცვისთვის. ხელოვნური ინტელექტის მიმართულებით მომუშავე უკრაინულმა კომპანია ***Primer-მა*** შეცვალა თავისი კომერციული ***AI-ის*** მქონე ხმის ტრანსკრიფციისა და თარგმანის სერვისები, რათა ქვეყანას შესაძლებლობა ჰქონოდა, რუსული საკომუნიკაციო ქსელების მონაცემები დაემუშავებინა.

რუსეთ-უკრაინის კონფლიქტი შეიძლება ჩაითვალოს პირველ ომად, სადაც ხელოვნური ინტელექტის მოწინავე ტექნოლოგიებია გამოყენებული – მაგალითად, სახის ამოცნობის პროგრამული უზრუნველყოფა. ცნობილია, რომ *„2022 წლის მარტში უკრაინის თავდაცვის სამინისტრომ დაიწყო ამერიკული კომპანია **Clearview AI-ის** მიერ შექმნილი ახალი გამოსახულებისა და სახის ამომცნობი პროგრამა, რომელიც ხელოვნურ ინტელექტზეა დაფუძნებული და ამით ადგენენ დაღუპული ჯარისკაცების ვინაობას, ასევე რუსი თავდამსხმელების ვინაობას"* (Fontes R.).

რუსეთ-უკრაინის ომში კომპანია ***Palantir-ის*** დახმარებით გამოიყენება ხელოვნურ ინტელექტზე დაფუძნებული ხელსაწყო სახელწოდებით ***MetaConstellation,*** ეს ინსტრუმენტი საშუალებას იძლევა, უკრაინას და მის მოკავშირეებს წვდომა ჰქონდეთ კომერციულ მონაცემებზე. პრაქტიკამ აჩვენა, რომ კომერციულ კომპანიებს ბევრი სასარგებლო ინფორმაცია გააჩნიათ – მაგალითად, *„ოპტიკური გამოსახულება, სინთეზური დიაფრაგმების რადარის გამოსახულება – აღნიშნული გულისხმობს ციდან გადაღების კადრებს; თერმული გამოსახულება, რომელიც გულისხმობს საარტილერიო და სარაკეტო ცეცხლის აღმოჩენის საშუალებას. ცნობილია, რომ აღნიშნული მონაცემების წყაროებია სხვადასხვა სამეცნიერო ინსტიტუტები, რომლებიც ატარებენ ატმოსფერულ კვლევებს – მაგალითად: **Airbus, Capella, Maxar** და სხვა"* (re-russia.net).

აღნიშნულმა კომპანიამ *„დაახლოებით 40-მდე კომერციული თანამგზავრის მიერ შეგროვებული მონაცემები შეაფასა"* (re-russia.net), ამან უკრაინის მხარეს საშუალება მისცა რელიეფის სურათების მიღებისა, რაც გულისხმობს სამ კვადრატულ მეტრამდე ფოკუსს. ასევე, უკრაინელ ოფიცრებს საშუალება აქვთ, გამოიყენონ კომპიუტერული ტაბლეტები, რათა მარტივად და რეალურ დროში მოხდეს იმ ინფორმაციის მიწოდება, რაზეც ზევით ვისაუბრეთ. ამ შემთხვევაში ანალიტიკოსები ერთადერთ პრობლემად ასახელებენ მაღალი ხარისხის ინტერნეტის ხელმისაწვდომობას.

Palantir-ის აღმასრულებელი დირექტორი ***ალექს კარპი (Alex Karp)*** ამბობს, რომ *„გამოყენებული ხელოვნური ინტელექტის ტექნოლოგია პატარა ქვეყნების კონკურენტულ უპირატესობას ცვლის დიდი ქვეყნების წინააღმდეგ"* (Fontes R.).

კიბერშეტევები

რუსეთმა კიბერსივრცეში პირველი შეტევები ომის დაწყებამდე განახორციელა, ეს იყო ***DDoS-ს*** შეტევები. რუსმა ჰაკერულმა დაჯგუფებებმა გამოიყენეს უკრაინის სამთავრობო უწყებების სისტემების წინააღმდეგ ცნობილი *„ტროას ცხენის“* მავნე პროგრამა, რომელსაც ***Microsoft-მა*** უწოდა ***„FoxBlade“*** (ქართულად შეიძლება გადავთარგმნოთ როგორც „მელიას ბასრი დანის პირი'', რაც გულისხმობს იმას, რომ რუს თავდამსხმელებს სურდათ ინტერნეტკავშირის გათიშვა, უკრაინის მართვის და კონტროლის ცენტრების პარალიზება).

Microsoft-ის ანგარიშში ვკითხულობთ, რომ ამას აკვირდებოდნენ ამერიკის შეერთებული შტატების ეთიკური ჰაკერები, სხვადასხვა ჯგუფები. უკრაინამ სწრაფი მოქმედებების ხარჯზე შეძლო თავის დაცვა – ტექნოლოგიურმა სტრუქტურებმა სწრაფად გაანაწილეს ციფრული ინფრასტრუქტურა საჯარო *„ღრუბლოვანი“* მეხსიერების ობიექტებზე, რომლის მონაცემთა ცენტრები განთავსებულია ევროპის სხვადასხვა ქვეყნებში. ***Microsoft-ი*** აცხადებს, რომ აღმოაჩინეს რუსეთის მიერ დაქირავებული ჰაკერული ჯგუფების უკანონო შეჭრის მცდელობა 42 ქვეყანაში, რომელიც მოიცავდა 128 ორგანიზაციის სისტემას.

ჰაქტივისტურმა დაჯგუფება *„ანონიმუსმა“* ამ ომში უკრაინას დაუჭირა მხარი და საპასუხო კიბეშეტევებით უპასუხა რუსეთის ფედერაციას, რამაც გამოიწვია სამთავრობო სისტემების, სხვადასხვა ტელეარხებისა და ვიდეოპლატფორმების შეფერხებით მუშაობა. *„ანონიმუსმა“* მოიპოვა რუსი აგენტების სია, რომლის ნაწილიც გაასაჯაროვა. თუმცა დიდი ნაწილი ჯერ კიდევ საიდუმლოდ რჩება. ასევე, ამ კიბერომში ჩართულია უკრაინის IT არმია, რომელსაც უკრაინის მთავრობა უჭერს მხარს. 2022 წლის პირველ ნახევარში დაზიანდა და განადგურდა უკრაინის ბოჭკოვანი ქსელის 22 პროცენტი, დაფიქსირდა 1350 მძლავრი კიბერთავდასხმა. 2022 წლის მეორე ნახევარში დაფიქსირდა 2194 მძლავრი კიბერშეტევა, ზარალს ჯერ კიდევ ითვლიან.

2022 წლის 16 თებერვალს დაიბლოკა თითქმის ყველა სამთავრობო სტრუქტურის ვებ-საიტი. რუსეთი ღიად ითხოვს: ნატო არ უნდა გაფართოვდეს აღმოსავლეთ ევროპისკენ, ამ ორგანიზაციის წევრები ვერ გახდებიან უკრაინა და საქართველო. რუსეთმა კატეგორიულად მოითხოვა, ამერიკის შეერთებულმა შტატებმა და ევროპამ გადახედონ ბრიუსელის სამიტზე მიღებულ გადაწყვეტილებას და უკან წაიღონ აღმოსავლეთ ევროპის მიმართულებით გაფართოების სტრატეგია. რუსეთს აქვს დიდი შესაძლებლობები კიბერომის თვალსაზრისით და არაერთი მოვლენა ადასტურებს ამას, მაგრამ მის შესაძლებლობებსაც აქვს ზღვარი. ნატომ გამოაქვეყნა კომუნიკე, სადაც ჩაიწერა, ბუქარესტის 2008 წლის გადაწყვეტილება ძალაში რჩება. კომუნიკეში ხაზგასმით არის აღნიშნული, რომ *„საქართველო და უკრაინა ალიანსის წევრები აუცილებლად გახდებიან“*. (საქართველოს საზოგადოებრივი მაუწყებელი) ბუქარესტის სამიტზე მიღებული გადაწყვეტილება ვერ მოინელა რუსეთმა.

Cisco-ს ცნობით, *„მასირებული კიბერთავდასხმები განხორციელდა 2022 წლის 15 თებერვალს, მეორე კი 24 თებერვალს. ამის შემდეგ* ***CISA-მ*** *და* ***FBI-მ*** *17 მარტს ერთობლივი კიბერუსაფრთხოების რეკომენდაციები გამოაქვეყნეს, მათ მოუწოდეს აშშ-ისა და საერთაშორისო სატელიტური კომუნიკაციის ქსელის პროვაიდერების მომხმარებლებს* ***(SATCOM),*** *იყვნენ მზადყოფნაში შესაძლო საფრთხეებთან დაკავშირებით. აღნიშნული გაფრთხილება მოყვა 24 თებერვლის კიბერშეტევებს, როდესაც განხორციელდა თავდასხმები* ***Viasat-სა*** *და* ***KA-SAT-ზე,*** *რამაც შეაფერხა ფართოზოლიანი თანამგზავრული ინტერნეტი უკრაინასა და ევროპის სხვა ქვეყნებში“*. (Cisco Annual Report) მსოფლიო მასშტაბით ყველა სახელმწიფო უნდა იყოს მზადყოფნაში – სხვადასხვა აქტორები, რომლებიც გამოირჩევიან ჰაკერული თაღლითური და ინფრასტრუქტურის დამაზიანებელი თავდასხმებით, ცდილობენ, სარგებელი ნახონ – რუსეთ-უკრაინის კონფლიქტი გამოიყენონ ერთგვარ ინსტრუმენტად. მაგალითად, ახალი ამბების, დეზინფორმაციის გავრცელება, შემოწირულობების მოთხოვნა მავნე ბმულებით, დახმარების ფონდების სახელებით და ყალბი ვებ-მისამართებით ან ლტოლვილთა მხარდაჭერის ყალბი ვებ-გვერდებით და სხვა.

უკრაინის სახელმწიფო სპეციალური კომუნიკაციების სამსახურმა (State Special Communications Service of Ukraine) გამოაქვეყნა ანგარიში ომის დროს რუსეთის კიბერთავდასხმებისა და კიბერსტრატეგიის შესახებ, სადაც ხაზგასმით არის ნათქვამი:

„24 ნოემბერს რუსეთმა დაიწყო ძლიერი კიბერშეტევები უკრაინის კრიტიკულ ინფრასტრუქტურაზე, კერძოდ, ენერგეტიკულ ობიექტებზე, რათა მომხდარიყო ელექტროენერგიის მიწოდების შეზღუდვა. რუსეთის ფედერაციამ კიბერთავდასხმებთან ერთად პარალელურ რეჟიმში ასევე განახორციელა წერტილოვანი დაბომბვა“. (cyberscoop.com)

როგორც აღვნიშნეთ, ამ კიბერშეტევებში ჩართულები არიან სხვადასხვა ჰაკრეული დაჯგუფებები სხვადასხვა დონეზე. როდესაც რუსეთი უკრაინაში შეიჭრა და წამოიწყო კონვენციური ომი, ამას წინ უძღვოდა ტრადიციული კიბერთავდასხმები, რაც დღემდე გრძელდება. არსებობს ჰაკტივისტური დაჯგუფება სახელწოდებით – ***„ანონიმური სუდანი“ (Anonymous Sudan).*** ექსპერტების მტკიცებით, იგი არის ბოროტი ჰაკერებით დაკომპლექტებული რუსული ჯგუფი, რომელიც პირდაპირ კავშირშია რუსულ ჰაკტივისტურ დაჯგუფება ***Killnet-თან.*** ამ ჰაკერულ დაჯგუფებას გაცხადებული აქვს, რომ რუსეთ-უკრაინის ომში მხარს რუსეთის ფედერაციას უჭერს, ამიტომ ხშირად უკრაინის საწინააღმდეგოდ მოქმედებს.

„ანონიმურმა სუდანმა“ და ***Killnet-მა*** 2023 წლის მარტში ერთობლივადაც ბევრ კიბერთავდასხმებზე აიღეს პასუხისმგებლობა, მათ შორის ლატვიის სამთავრობო უწყებებზე, ნასას სისტემებზე, უკრაინის სისტემებზე. როგორც ცალ-ცალკე, ასევე ერთობლივად განახორციელეს ***DDoS*** შეტევები საფრანგეთის საავადმყოფოებზე, უნივერსიტეტებზე, აეროპორტებზე, იუსტიციისა და შინაგან საქმეთა სამინისტროების სისტემებზე.

Killnet-ის სამიზნეები აშშ-ის გარდა ყველა ის ქვეყანა აღმოჩნდა, რომელიც ამა თუ იმ ფორმით დახმარებას უწევს უკრაინას. ჰაქტივისტურმა დაჯგუფებამ თებერვალში კიბერთავდასხმები დაიწყო ამერიკის შეერთებული შტატების ათზე მეტ საავადმყოფოზე *(Stanford Health, Michigan Medicine, Duke Health და Cedar-Sinai და სხვა).* (research.checkpoint.com) ოქტომბერში ***DDoS*** შეტევები განახორციელა ამერიკის შეერთებული შტატების რამდენიმე აეროპორტზე *(ლოს-ანჯელესის საერთაშორისო აეროპორტი, ჩიკაგოს ოჰარის საერთაშორისო აეროპორტი, ჰარტსფილდ-ჯექსონ ატლანტას საერთაშორისო აეროპორტი და ა.შ.),* (research.checkpoint.com) რამაც გამოიწვია ფრენების შეჩერება და პარალიზება.

Killnet-მა 2022 წლის აპრილში სრულად გადაიტანა ყურადღება რუსეთის გეოპოლიტიკური ინტერესების მხარდასაჭერად. მისი განცხადებით, *„550-ზე მეტი კიბერთავდასხმა განახორციელეს, აქედან 45 თავდასხმა იყო უკრაინის სისტემებზე, რაც მთლიანი თავდასხმების 10 პროცენტზე ნაკლებია“* (research.checkpoint.com).

ერთ-ერთი *„სამიზნე იყო* ***ილონ მასკის*** *ფართოზოლიანი სატელიტური ქსელი* ***Starlink-ი,*** *რომელზეც განახორციელეს კიბერთავდასხმები, რის შედეგადაც 18 ნოემბერს ბევრი მომხმარებელი ჩიოდა, რომ ისინი რამდენიმე საათის განმავლობაში ვერ ახერხებდნენ თავიანთ ანგარიშებზე შესვლას. აღნიშნული კიბერშეტევების განხორციელებაში სხვადასხვა დაჯგუფებებიც იყვნენ ჩართულები – მაგალითად, ჰაკერული დაჯგუფება* ***Radis, Halva, Anonymous Russian*** *და სხვა“.* (Bracken B.) ***Killnet-მა*** 17 ნოემბერს *„კიბერთავდასხმები განახორციელა თეთრი სახლის ვებ-გვერდზე, რომელსაც დაარქვა „სატესტო შეტევის 30 წუთი“.* (Bracken B.) ამერიკის შეერთებული შტატების ეროვნული კიბერუსაფრთხოების სააგენტოს დირექტორი ***რობ ჯოისი (Rob Joyce)*** ამბობს:

„მათ სამიზნეს წარმოადგენს დახურული წრიული სატელევიზიო კამერები, რომლებსაც ადგილობრივი ხელისუფლება და კერძო ბიზნესი იყენებს გარემოს მონიტორინგისთვის, ჩვენ ვაკვირდებით რუსი ჰაკერების შესვლას საჯარო ვებკამერებში, რაც ყველასთვის ხელმისაწვდომია, თუმცა რუსი ჰაკერები ასევე ამას იყენებენ და უყურებენ დახმარების მიმწოდებელ კოლონებსა და მატარებლებს, ჩვენ ვიცით, რომ რუსები ასევე აკვირდებიან ლოჯისტიკურ სატრანსპორტო კომპანიებს, რათა მეტი გაიგონ უკრაინაში იარაღის მიწოდების შესახებ“ (theguardian.com).

უკრაინაში რუსეთის მიერ წამოწყებულმა ომმა დაანგრია არა მხოლოდ რუსეთის უძლეველობის მითი სამხედრო თვალსაზრისით, ასევე კიბერომის თვალსაზრისითაც. ომის დაწყებისთანავე რუსეთში ჰაკერებმა გატეხეს ვიდეოპლატფორმები – ***Wink*** და ***IVI***, რუსეთის რამდენიმე არხზე სერიალების ნაცვლად ეთერში გაუშვეს უკრაინაში დაბომბვების შესახებ *„ნასტოიაშჩეე ვრემიასა“* და *„დოჟდის“* ვიდეოები. ომის კადრების რუსულ არხებზე გაშვების შესახებ ***„ანონიმუსმა“ „ტვიტერზე“***

დაწერა და ვიდეოც გაავრცელა. ***„ანონიმუსმა“,*** რომელიც თავისუფალი, არაცენტრალიზებული ჰაკერული ორგანიზაციაა და აერთიანებს ე.წ. *ჰაკტივისტებს,* გამოაქვეყნა განცხადება, რომ მათ შეაღწიეს რუსეთის უსაფრთხოების სისტემებში და გამოიტანეს რუსეთის აგენტების სიები, რასაც ეტაპობრივად გამოაქვეყნებდნენ სახელმწიფოების მიხედვით.

კიბერსაფრთხეების ანალიტიკოსებმა შეადგინეს კიბერჯგუფების ცხრილი, რომლებიც რუსეთ-უკრაინის კონფლიქტში არიან ჩართულები, ანალიზის გაკეთების საშუალებას გვაძლევს კიბერსაფრთხეების ლანდშაფტის შესაფასებლად. რუსეთის მხრიდან დაფინანსებულმა ***მოწინავე საფრთხის ჯგუფებმა (APT)*** გამოავლინეს უნარი, შეინარჩუნონ მუდმივი, ამოუცნობი, გრძელვადიანი წვდომა და უნებართვო წვდომა ქსელებში, ლეგიტიმური სერტიფიკატების გამოყენებით. ისინი წარმოადგენენ კიბერშეტევების ყველაზე მაღალ რისკს, როგორებიც არიან: „***APT28, Turla, Gamaredon, Energetic Bear, APT29, Sandworm*** *და სხვა“.*

სოციალური მედია

რუსეთ-უკრაინის ომი არის ომი, სადაც ყველაზე მეტი დოზით გამოიყენება ინტერნეტი, სადაც ვრცელდება უამრავი ინფორმაცია და დეზინფორმაცია, ტექსტობრივი, ფოტო თუ ვიდეოს სახით. აქტიურად გამოიყენება სხვადასხვა სოციალური ქსელებისა და სოციალური მედიის პლატფორმები. სოციალურ ქსელებში და მედიაში აქტივობა დიდია – ოჯახის წევრები, მეგობრები აქვეყნებენ პოსტებს, ცნობებს, ვიდეო-ფოტო მასალას, ეკონტაქტებიან ნაცნობებს, მეგობრებს, ოჯახის წევრებს, რათა შეატყობინონ მათი უსაფრთხოებისა და ადგილმდებარეობის შესახებ, რომ ისინი ცოცხლები არიან. ცნობილია, რომ ბევრმა მსხვილმა ტექნოლოგიურმა კომპანიამ გარკვეულწილად შეზღუდა რუსული მედიასაშუალებების პროპაგანდა, დეზინფორმაციის გავრცელება. შეიზღუდა ასევე პოსტების ხილვადობა „ფეისბუკსა'' და „ტვიტერზე''.

დრონები

რუსეთმა და უკრაინამ ომში გამოიყენეს ბევრად მეტი უპილოტო საფრენი აპარატი, ვიდრე სხვა ომებში გამოყენებულა. დრონები მეტად ეფექტური აღმოჩნდა დაზვერვისა და მეთვალყურეობისთვის. უკრაინელმა სამხედროებმა ასევე გამოიყენეს დრონები მტრის პოზიციების დასაზვერად და დასამიზნებლად ზუსტი მართვადი საბრძოლო იარაღის გამოყენებით. ცნობილია, რომ უკრაინის მხრიდან ხშირად გამოყენებული უპილოტო საფრენი მოწყობილობები არის ძალიან მარტივი, ჩვეულებრივი კომერციული დრონები, რაშიც ინტეგრირებულია მაღალი გარჩევადობის კამერები, რომლებიც დაკავშირებულია სმარტფონებთან.

მაგალითად, თურქული თვითმფრინავი ***Bayraktar TB2*** ატარებს ლაზერით მართვად ბომბებს, რომელიც მიზანში იღებს მანქანებს, საჯარისო დაჯგუფებებს, სამხედრო ბაზებს. არსებობს ამერიკული წარმოების ***Switchblade*** და რუსული წარმოების ***Lantset,*** ესენია ე.წ. *კამიკაძე დრონები. მათი* ტარება შეუძლია ერთ ადამიანს ზურგჩანთითაც კი. მათში ჩაშენებულია ქობინები, რაც გულისხმობს, რომ სამიზნეს ეჯახება და ფეთქდება.

იქიდან გამომდინარე, რომ რუსეთ-უკრაინის ომში უპრეცედენტოდ გაიზარდა დრონების გამოყენება, ორივე მხარემ შეიმუშავა კონტრ-დრონების სისტემები, მტრის უპილოტო საფრენი აპარატების აღმოსაჩენად და ლიკვიდაციისთვის. მაგალითად, უკრაინული მხარე იყენებს ანტი-დრონის სისტემებს, როგორიცაა თურქული წარმოების ***KARGU.*** მას შეუძლია აწარმოოს მონიტორინგი და გაანადგუროს სამიზნეები.

თანამგზავრები

რაც შეეხება თანამგზავრებს, უკრაინაში რუსეთის შეჭრის შემდეგ *5000* ***Starlink-ის*** ფართოზოლიანი თანამგზავრები უკრაინას ინტერნეტით უზრუნველყოფენ. ეს გადამწყვეტი საკითხი იყო მოქალაქეებისა და მთავრობის დასახმარებლად, რათა ქვეყანა კავშირზე ყოფილიყო და უკეთესად მომხდარიყო კოორდინაცია. დღემდე ფუნქციონირებს დაახლოებით *25 000* ***Starlink*** ტერმინალი უკრაინის თავდაცვისა და კავშირის დასახმარებლად.

ტელეკომები საზღვრების გარეშე (TSF)

ეს არის მსოფლიოში პირველი არასამთავრობო ორგანიზაცია, რომელიც ფოკუსირებულია საგანგებო სიტუაციების რეაგირების ტექნოლოგიებზე. ამ ორგანიზაციის მიზანია, ააშენონ სწრაფი რეაგირების საკომუნიკაციო ცენტრები მსოფლიო მასშტაბით. ***TSF-ის*** ჯგუფებმა შეძლეს, გადაუდებელი სატელეკომუნიკაციო აღჭურვილობით უკრაინაშიც და უკრაინის ფარგლებს გარეთაც, ლტოლვილების დახმარება. ცნობილია, რომ რუსეთის შეჭრის შემდეგ უკრაინა რვა მილიონზე მეტმა ადამიანმა დატოვა. მათ თავშესაფარი მოითხოვეს სხვადასხვა ქვეყანაში, ექვს მილიონზე მეტი ადამიანი დევნილი გახდა ქვეყნის შიგნით. ეს არის უკრაინის მოსახლეობის *32* პროცენტი.

ელექტრონული სისტემებით ბრძოლა (ომი)

რუსეთ-უკრაინის ომში მნიშვნელოვანი საკითხი იყო ***ელექტრონული ბრძოლის (EW)*** სისტემების გამოყენება. ამაშიც იგულისხმება კომუნიკაციების, სარადარო და სხვა ელექტრონული სისტემების შეფერხება.

თებერვალში, სანამ რუსეთი ომს დაიწყებდა, ტექნოლოგიური კომპანია ***HawkEye 360-ის*** თანამშრომლებმა კომერციული თანამგზავრების საშუალებით, რომელიც გულისხმობს ***გლობალური ადგილმდებარეობის სისტემას (GPS)***, დააფიქსირეს საზღვრის დარღვევა უკრაინა-ბელორუსის საზღვართან, ჩერნობილის ჩრდილოეთით, უპილოტო საჰაერო თვითმფრინავებმა გადაკვეთეს საზღვარი, რომლებიც მოძრაობდნენ ლუგანსკისა და დონეცკის რეგიონში. უკრაინელმა სამხედროებმა ელექტრონული ბრძოლის სისტემები გამოიყენეს რუსული კომუნიკაციებისა და ***GPS*** სიგნალების დასაბლოკად, რამაც უზრუნველყო საკომუნიკაციო ინფრასტრუქტურის დაცვა.

ელექტრონული ომის სისტემები არის ტექნოლოგიების ნებისმიერი კონფიგურაცია, რომელიც შექმნილია და აგებულია ერთ ან რამდენიმე საჰაერო, სახმელეთო, საზღვაო ან კოსმოსურ პლატფორმაზე, სამხედრო ან სადაზვერვო მისიების შესასრულებლად.

სამომხმარებლო ტექნოლოგია და აპლიკაციები

2020 წელს ამოქმედდა მობილური აპლიკაცია და ონლაინ პორტალი ***Diia,*** რომელიც იყო ტრადიციული სამთავრობო სისტემა, იგი გამოიყენებოდა ლიცენზირების ნებართვების გასანახლებლად, პარკირების ბილეთების საყიდლად, რომელიც ომის დაწყების შემდეგ გადაკეთდა ისე, რომ მშვიდობიან მოქალაქეებს საშუალება ჰქონდეთ, ატვირთონ სურათები გეოლოკაციის კოორდინატებით, რუსეთის სხვადასხვა სამხედრო აქტივობების შესახებ, ან გაავრცელონ ინფორმაცია საეჭვო ადამიანების შესახებ.

მაგალითად, 2022 წლის მარტში დაიწყო ფუნქციონირება უსაფრთხო ჩათის (სასაუბრო) სისტემა ***eVorog-მა (eEnemy),*** რომლის გამოყენებაც ***„ტელეგრამზეა“*** შესაძლებელი, იგი საშუალებას აძლევს მშვიდობიან მოსახლეობას, გააზიარონ უამრავი ინფორმაცია ჯარების აქტივობისა და გადაადგილების შესახებ. ჩათის სისტემამ სმარტფონის მქონე უკრაინელი მოქალაქეები ციფრული წინააღმდეგობის მებრძოლებად აქცია – ადამიანები ერთ სივრცეში იკრიბებიან და აწარმოებენ სამხედრო დაზვერვას.

ვირტუალური რეალობის სისტემები (VR) და 3D ჰოლოგრამები

ომისთვის საწვრთნელად უკრაინელმა სამხედროებმა გამოიყენეს ***ვირტუალური რეალობის სასწავლო სისტემები (VR)***, რომელშიც იგულისხმება საბრძოლო სცენარების სიმულაციები, ჯარისკაცების ტაქტიკისა და პროცედურების მოსამზადებლად. ამ ტიპის წვრთნებმა ჯარისკაცებს საშუალება მისცა, ევარჯიშათ უსაფრთხო და კონტროლირებად გარემოში, სანამ ისინი უშუალოდ გავიდოდნენ ფრონტის ხაზზე.

2022 წლის ივნისში ვოლოდიმირ ზელენსკიმ ***ARHT Media-ს 3D ჰოლოგრაფიული ტექნოლოგიის*** საშუალებით 200 000-ზე მეტ ტოპ ტექნიკურ მეწარმეს, ინვესტორსა და კორპორატიულ ლიდერს მიმართა ევროპის შვიდ მთავარ ტექნოლოგიურ ღონისძიებაზე.

აქვე აუცილებლად ხაზი უნდა გავუსვათ ხელოვნური ინტელექტის კომპონენტების გამოყენების პრობლემურ საკითხებს კონვენციური ომის დროს. სამხედრო სისტემებში ხელოვნური ინტე-

ლექტის გამოყენების ერთ-ერთ პრობლემას წარმოადგენს დაუცველობა სპეცშეტევების მიმართ, ანუ იმ შეტევების მიმართ, რომელიც უშუალოდ მიმართულია აპარატურის პროგრამული უზრუნველყოფის წინააღმდეგ – მონაცემების შეყვანის დროს უმნიშვნელო ცვლილებამაც კი შეიძლება გამოიწვიოს ინფორმაციის დამუშავების არასწორი შედეგები, რაც ბრძოლის პროცესში შეიძლება კატასტროფული აღმოჩნდეს. კაცობრიობა მიისწრაფვის ისეთი სამყაროსკენ, სადაც ახალი ტექნოლოგიები შეცვლის ძველ, სტანდარტულ ომს, ტექნოლოგიური ხელმისაწვდომობის საშუალებით გადაასხვაფერებს ომის დინამიკას.

ექსპერტები უკვე ალაპარაკდნენ იმაზე, რომ შესაძლოა, რუსეთ-უკრაინის ომი იყოს ხელოვნური ინტელექტის და ზოგადად ახალი ტექნოლოგიების გამოცდის ერთგვარი პერიოდი – გარდა იმისა, რაც ჩამოვთვალეთ, დაიტესტოს ხელოვნური ინტელექტის კომპონენტების ახალი ტექნოლოგიური გამოგონებები. ახალი ტექნოლოგიების კომპონენტების გამოყენება კონვენციური ომის პროცესზე კი ახდენს ზეგავლენას, მაგრამ მთლიანობაში მაინც ვერ განსაზღვრავს. როგორ შეიძლება შეცვალოს ომის მთლიანი არსი ახალმა ტექნოლოგიებმა და ხელოვნური ინტელექტის კომპონენტების განვითარებამ?

მაგალითად შეგვიძლია მოვიყვანოთ ფაქტი, რომელიც 1988 წელს მოხდა: *„ამერიკის შეერთებული შტატების საზღვაო ძალების კრეისერმა სახელწოდებით **Aegis-მა** შეცდომით ჩამოაგდო ირანული სამგზავრო თვითმფრინავი, რადგან საბრძოლო ინფორმაციის ცენტრში ტაქტიკური მოქმედების ოფიცერმა ინფორმაცია არასწორად შეაფასა, მას სხვადასხვა მონაცემებზე დაყრდნობით ეგონა, რომ ეს იყო მტრულად განწყობილი ირანული სამხედრო თვითმფინავი. შედეგად 300-მდე მშვიდობიანი მოქალაქე დაიღუპა“* (Stavridis J.).

ამ შემთხვევაში შეგვიძლია ვივარაუდოთ, იმ დროისთვის ხელოვნური ინტელექტის სისტემები ხელმისაწვდომი თუ იქნებოდა, რომელიც შეძლებდა დიდი რაოდენობით მონაცემების გაანალიზებას, რა თქმა უნდა, გამოავლენდა, რომ ეს იყო სამოქალაქო თვითმფრინავი და ადამიანები გადარჩებოდნენ. ხელოვნურ ინტელექტს სხვადასხვა კონკრეტულ მომენტში შეუძლია მოგვცეს დეტალური და სტრატეგიული ინფორმაცია, რაც გადაწყვეტილების მიმღებთ აძლევს საშუალებას, გამოიყენონ ზუსტი იარაღი.

მაღალ ტექნოლოგიურ მიღწევებში გათვითცნობიერებულ ადამიანებს აღელვებთ ერთი ყველაზე მნიშვნელოვანი საკითხი – რაც უფრო იხვეწება, იარაღი ყოველდღიურად უფრო ჭკვიანი ხდება და ამავე დროს მარტივდება სიცოცხლის მოსპობა. შესაბამისად, წამყვანი ქვეყნები მუშაობენ რეგულაციების შემუშავებაზე, რათა დადგინდეს ნორმები. ამ თემას სერიოზულად უდგება ნატო, ევროკავშირი, ამერიკის შეერთებული შტატები, დიდი ბრიტანეთი და სხვა ევროპული ქვეყნები.

მსოფლიოში არსებობენ აგრესორი ქვეყნები *(როგორიც არის რუსეთი)* და არსებობენ ჰაკერულ-ტერორისტული დაჯგუფებები, რომლებიც ტექნოლოგიურ მიღწევებს ითვისებენ ავი ზრახვებისთვის. ამჟამად ძალიან სწრაფად იზრდება ტექნოლოგიური მიღწევები, როგორც ვირტუალურ სივრცეში, ასევე რეალურ სივრცეში, მათ შორის ხელოვნური ინტელექტის კომპონენტების გამოყენებით, ამას უფრო ამძაფრებს ის გეოპოლიტიკური ვითარება, რაც მსოფლიო მასშტაბით შეიქმნა და კონკრეტულად შეიძლება ვთქვათ შავი ზღვისპირეთში. ეს ფაქტობრივად გამოიწვია რუსეთის აგრესიამ უკრაინის წინააღმდეგ. 2022 წლის 24 თებერვლიდან დიდი დრო გავიდა, რუსეთის არმია კვლავაც განაგრძობს სუვერენული სახელმწიფოს მთელ ტერიტორიაზე სახმელეთო, საავიაციო ოპერაციებსა და კიბერთავდასხმებს.

დასკვნა

ჩვენ არ ვიცით, ომი კიდევ რამდენ ხანს გაგრძელდება. მართალია, უკრაინას ინტენსიურად ეხმარებიან მოწინავე ქვეყნები, მაგრამ ანალიტიკოსების მტკიცებით, ეს საკმარისი არ არის. რაც ხდება რეალური ომის პირობებში, თითქმის იგივე ხდება ვირტუალური ომის პირობებშიც, ანუ ინტერნეტსივრცეში. ამ ორი მოვლენის განხილვა განყენებულად შეუძლებელია. უკრაინას სჭირდება უახლესი ტექნოლოგიებით აღჭურვილი თავდაცვითი სისტემები არა მხოლოდ იარაღის სახით, არამედ ახალი ტექნოლოგიების თვალსაზრისით. საჭიროა დიდი ყურადღება, აღჭურვა, დაკვირვება, შესწავლა და მოქმედება.

დღეს რუსეთის ხელისუფლება ხშირად ახსენებს ბირთვულ იარაღს. ყველამ ვიცით, რომ ეს იქნება სრული კატასტროფა კაცობრიობისთვის. არ არის გამორიცხული, ამ შემთხვევაშიც მხოლოდ შეშინების მიზნით წამოწყებულ პროპაგანდასთან გვქონდეს საქმე, მაგრამ ვიცით რა რუსეთის ხასიათი და ბუნება, ვერ ვენდობით, კრემლი ნამდვილად არის ამაზე წამსვლელი. ამიტომ მთელი მსოფლიო ვალდებულია, წინ აღუდგეს რუსულ აგრესიას – ნატომ, ევროკავშირმა, ამერიკის შეერთებულმა შტატებმა უნდა შეიმუშაონ ეფექტური პროგრამები, სადაც დეტალურად იქნება გაწერილი უკრაინის დახმარება. ფაქტობრივად, ყველა წამყვანმა ქვეყანამ თავისი გადამწყვეტი სიტყვა უნდა თქვას და ეს საქმითაც გამოხატოს. ბოლო დროს იმაზეც დაიწყეს საუბარი, რომ ეს ომი აუცილებლად უნდა დასრულდეს და საკითხები გადაწყდეს მრგვალ მაგიდასთან. ბუნებრივია, როდისღაც ყველა ომი სრულდება, მაგრამ ამ შემთხვევაში არსებობს დილემა – რუსეთი უკან არ იხევს, არ თმობს დაპყრობილ ტერიტორიებს, უკრაინის ხელისუფლება არ თმობს, რასაკვირველია, არ აღიარებს ოკუპირებულ ტერიტორიებს, მაშ რანაირად უნდა დასრულდეს ომი შავი ზღვის რეგიონში? ამ ეტაპზე შეგვიძლია ვივარაუდოთ, რომ არსებული მდგომარეობა დაკონსერვდება და შემდეგ ნებისმიერ დროს ომი განახლდება, ყოველ შემთხვევაში, სიტუაცია იქნება მუდამ ფეთქებადი. ალბათ ბევრი რამ იქნება დამოკიდებული, როგორ ჩაივლის არჩევნები ამერიკის შეერთებულ შტატებში და ვინ მოვა ხელისუფლებაში. თუმცა, ვინც არ უნდა გადაიბაროს ძალაუფლება, რუსეთ-უკრაინის ურთიერთობას მაინც ვერ დაათბობს და ვერ დაუბრუნებს პირვანდელ მდგომარეობას, როგორც უკვე აღვნიშნე, არსებული მდგომარეობა შეიძლება გაიყინოს და ამას ეწოდოს ომის დასრულება. ამ ეტაპზე სხვა მოცემულობა არ არსებობს. აქვე უნდა აღინიშნოს, რომ არც ევროკავშირში და არც აშშ-ის ადმინისტრაციაში ოფიციალური პირები ომის დასრულებაზე არ საუბრობენ, ისინი მობილიზებულნი არიან, რომ უკრაინას უნდა გაეზარდოს დახმარება. ეს ცუდია თუ კარგი, ამას უახლოესი მომავალი გვიჩვენებს.

ბიბლიოგრაფია:

Bracken B. *„Killnet Gloats About DDoS Attacks Downing Starlink“, darkreading.com.* 2022 წლის 29 november. 2025 წლის 10 01.

Cisco Annual Report. *Reimagining the future of connectivity*. Research. USA: Cisco, 2022.

cyberscoop.com. *„Ukraine warns of ‘massive cyberattacks’ coming from Russia on critical infrastructure sites“*. 2022 წლის 26 08. 2025 წლის 10 01.

Fontes R., Kamminga J.,. *„Ukraine A Living Lab for AI Warfare“, nationaldefensemagazine.org,*. 2023 წლის 24 03. 2025 წლის 10 01.

Kryvenko P. *„Artificial Intelligence in the Russian-Ukrainian war“, newgeopolitics.org.* 13 june 2022. 10 january 2025.

re-russia.net. *„A natural ally: Artificial intelligence is becoming an increasingly important tool in warfare, but it requires access to an extensive civilian digital infrastructure“*. 2023 წლის 14 04. 2025 წლის 10 01.

research.checkpoint.com. *„The New Era of Hacktivism – State-Mobilized Hacktivism Proliferates to the West and Beyond“*. 2022 წლის 29 08. 2025 წლის 10 01.

Stavridis J. *„The Russia-Ukraine war may become a testing ground for AI“, livemint.com.* 2023 წლის 01 jun. 2025 წლის 10 01.

theguardian.com. *„Russian hackers ‘target security cameras inside Ukraine coffee shops“*. 2023 წლის 11 04. 2025 წლის 10 01.

theguardian.com, Russian hackers ‘target security cameras inside Ukraine coffee shops“. თ. გ.

საქართველოს საზოგადოებრივი მაუწყებელი. *„ბრიუსელის სამიტი და ნატოს კომუნიკე“, 1tv.ge,*. 2021 წლის 14 06. 2025 წლის 10 01.