“შრომები“№ 2 (2024)
WWW.PAPERS.ETA.EDU.GE/INDEX.PHP/PAPERS

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

კიბერუსაფრთხოების გამოწვევების ანალიზი თანამედროვე სამხედრო კონფლიქტების ჭრილში

ნანი არაბული,[1] რომეო გალდავა,[2] გიორგი კოხრეიძე[3]
DOI: https://doi.org/10.61446/pa.2.2024.8417

აბსტრაქტი

წარმოდგენილ ნაშრომში განხილულია კიბერუსაფრთხოების გამოწვევები თანამედროვე სამხედრო კონფლიქტების კონტექსტში, მათი გავლენა ქვეყნების თავდაცვისუნარიანობაზე და ის ძირითადი მიმართულებები, რომლებიც განსაზღვრავენ წარმატებულ კიბერთავდაცვას. კვლევაში გაანალიზებულია კრიტიკული ინფრასტრუქტურის დაცვის, სახელმწიფო უწყებების უსაფრთხოების, ეკონომიკური უსაფრთხოების, დემოკრატიული პროცესების დაცვისა და სამხედრო უპირატესობის საკითხები კიბერუსაფრთხოების ჭრილში. განსაკუთრებული ყურადღება ეთმობა თანამედროვე კონფლიქტების მაგალითზე კიბერშეტევების სტატისტიკურ ანალიზს, მათ ფორმებს და გავლენას სამხედრო ოპერაციებზე. ნაშრომში შემოთავაზებულია, აგრეთვე, კიბერშენაერთების ორგანიზაციული სტრუქტურის მოდელი, განხილულია მათი თავდაცვითი და შეტევითი ოპერაციების სპეციფიკა, დასაბუთებულია საქართველოში სპეციალიზებული კიბერდანაყოფის შექმნის აუცილებლობა, რაც მნიშვნელოვნად გააძლიერებს ქვეყნის თავდაცვისუნარიანობას.

საკვანძო სიტყვები: კიბერუსაფრთხოება, კიბერუსაფრთხოება და სამხედრო კონფლიქტები, კიბერშეტევები, კიბერშენაერთი, კრიტიკული ინფრასტრუქტურა, თავდაცვისუნარიანობა.

[1] სსიპ - დავით აღმაშენებლის სახელობის საქართველოს, ეროვნული თავდაცვის აკადემიის ბაკალავრიატის ინფორმატიკის მიმართულების ასოცირებული პროფესორი, ტექნიკის მეცნიერებათა დოქტორი
[2] სსიპ - დავით აღმაშენებლის სახელობის საქართველოს, ეროვნული თავდაცვის აკადემიის ბაკალავრიატის ინფორმატიკის მიმართულების ასოცირებული პროფესორი, მათემატიკის დოქტორი
[3] სსიპ - დავით აღმაშენებლის სახელობის საქართველოს, ეროვნული თავდაცვის აკადემიისბაკალავრიატის ინფორმატიკის მიმართულების ასისტენტ პროფესორი, დოქტორანტი

“შრომები“№ 2 (2024)
WWW.PAPERS.ETA.EDU.GE/INDEX.PHP/PAPERS
ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

Analysis of Cybersecurity Challenges in the Context of Modern Military Conflicts

Nani Arabuli,[4] Romeo Galdava,[5] Giorgi Kokhreidze[6]
DOI: https://doi.org/10.61446/pa.2.2024.8417

Abstract

This paper examines cybersecurity challenges in the context of modern military conflicts, their impact on countries' defense capabilities, and the key directions that define successful cyber defense. The research analyzes critical infrastructure protection, government agency security, economic security, protection of democratic processes, and military advantage from a cybersecurity perspective. Special attention is paid to the statistical analysis of cyber-attacks based on modern conflicts, their forms, and impact on military operations. The paper also proposes an organizational structure model for cyber units, discusses the specifics of their defensive and offensive operations, and justifies the necessity of creating a specialized cyber unit in Georgia, which would significantly strengthen the country's defense capabilities.

Keywords: cybersecurity, cybersecurity and military conflicts, cyber-attacks, cyber unit, critical infrastructure, defense capability.

[4] Associate Professor of Bachelor's Program in Informatics of LEPL-David Aghmashenebeli National Defence Academy of Georgia, Doctor of Technical Science
[5]Associate Professor of Bachelor's Program in Informatics of LEPL-David Aghmashenebeli National Defence Academy of Georgia, Doctor of Mathematics
[6] Assistant Professor of Bachelor's Program in Informatics of LEPL-David Aghmashenebeli National Defence Academy of Georgia, PhD Student

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

შესავალი

თანამედროვე სწრაფად ცვალებად ტექნოლოგიურ სამყაროში კიბერუსაფრთხოება წარმოადგენს ეროვნული უსაფრთხოების პოლიტიკის უნიშვნელოვანეს გამოწვევას, რომელიც მოითხოვს მუდმივ მზადყოფნას, ინოვაციურობას და ადაპტაციას.

თანამედროვე სამხედრო კონფლიქტები ახლა ვრცელდება ფიზიკური ბრძოლის ველების მიღმა ვირტუალურ ასპარეზზე, სადაც კიბერშეტევებმა შეიძლება დაარღვიოს, გამორთოს ან თუნდაც გაანადგუროს კრიტიკული ინფრასტრუქტურა და თავდაცვის სისტემები. ამ ცვლილებამ გამოიწვია კიბერუსაფრთხოების ყოვლისმომცველი ზომების გადაუდებელი აუცილებლობა, რადგან მოწინააღმდეგეები სულ უფრო მეტად იყენებენ კიბერ ტაქტიკას სტრატეგიული უპირატესობების მოსაპოვებლად, ჯაშუშობის განსახორციელებლად და ფართო შეფერხების შესაქმნელად.

ქვეყნების უნარი, ეფექტურად დაიცვან თავიანთი ციფრული აქტივები და ინფრასტრუქტურა, 21-ე საუკუნეში გახდა მათი სუვერენიტეტისა და ეროვნული უსაფრთხოების შენარჩუნების აუცილებელი პირობა. ამ კუთხით მნიშვნელოვანია თანამედროვე მსოფლიოში არსებული მდგომარეობა და ის ღონისძიებები, რომლებსაც ისინი ახორციელებენ ამ მიმართულებით. აღნიშნული გამოცდილება უაღესად მნიშვნელოვანია საქართველოსათვის, რადგან იგი მნიშვნელოვნად გააძლიერებს ქვეყნის თავდაცვისუნარიანობას.

ძირითადი ნაწილი

თანამედროვე ეტაპზე კიბერუსაფრთხოება წარმოადგენს ურთულეს გამოწვევას ეროვნული უსაფრთხოების თვალსაზრისით. მსოფლიოში მიმდანარე კონფლიქტებმაც დაადასტურეს აღნიშნული გარემოება, უფრო მეტიც, აღნიშნული ინსტრუმენტის გარეშე წარმოუდგენელია სუვერენიტეტისა და ეროვნული უსაფრთხოების შენარჩუნება. ამ მიმართულებით მნიშვნელოვანია შესწავლილ იქნას თანამედროვე მსოფლიოში არსებული მდგომარეობა და განხორციელებულ იქნას ქმედითი ნაბიჯები კიბერუსაფრთხოების კუთხით, რაც მნიშვნელოვნად გააძლიერებს ქვეყნის თავდაცვისუნარიანობას.

ცნობილია, რომ კიბერუსაფრთხოების კუთხით განსაკუთრებულად მნიშვნელოვანია შემდეგი ძირითადი მიმართულებები:

კრიტიკული ინფრასტრუქტურის დაცვა: თანამედროვე საზოგადოების ფუნქციონირება მნიშვნელოვნად არის დამოკიდებული ციფრულ სისტემებზე. ენერგეტიკა, წყალმომარაგება, ტრანსპორტი, საფინანსო სექტორი და ჯანდაცვა და სხვა - ყველა ეს სფერო იმართება კომპიუტერული ტექნოლოგიებით. კიბერშეტევამ ამ სისტემებზე შეიძლება გამოიწვიოს კატასტროფული შედეგები, დაწყებული ეკონომიკური ზარალით, დამთავრებული ადამიანების სიცოცხლის საფრთხეში ჩაგდებით.

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

სახელმწიფო უწყებების დაცვა: ისინი ინახავენ ქვეყნისათვის უნიშვნელოვანეს, მათ შორის სენსიტიურ ინფორმაციას ციფრულ ფორმატში, რომელიც მოიცავს დიპლომატიურ კომუნიკაციებს, სამხედრო გეგმებს, სადაზვერვო ინფორმაციას და სხვ. ამავე დროს კიბერჯაშუშობა გახდა ერთ-ერთი მთავარი საშუალება სახელმწიფოებისთვის, მოიპოვონ ინფორმაცია თავიანთი მეტოქეების შესახებ.

ეკონომიკური უსაფრთხოება: კიბერდანაშაული და ინდუსტრიული შპიონაჟი სერიოზულ საფრთხეს უქმნის ქვეყნების ეკონომიკურ სტაბილურობასაც. ცნობილია, რომ ინტელექტუალური საკუთრების ქურდობა, ფინანსური თაღლითობა და ბიზნეს-პროცესების შეფერხება იწვევს მილიარდობით ზარალს ყოველწლიურად.

დემოკრატიული პროცესების დაცვა: კიბერშეტევები საარჩევნო სისტემებზე და დეზინფორმაციის კამპანიები სოციალურ მედიაში საფრთხეს უქმნის დემოკრატიულ პროცესებს. ქვეყნები იძულებულნი არიან, გააძლიერონ თავიანთი კიბერუსაფრთხოების შესაძლებლობები, რათა დაიცვან საზოგადოებრივი აზრის ფორმირების პროცესი უცხო ქვეყნების ჩარევისგან.

სამხედრო უპირატესობა: თანამედროვე სამხედრო ოპერაციები მჭიდროდ არის დაკავშირებული ქვეყნების კიბერშესაძლებლობებთან. კიბერიარაღი გახდა სტრატეგიული მნიშვნელობის ინსტრუმენტი, რომელსაც შეუძლია დააზიანოს/გაანადგუროს მოწინააღმდეგის სამხედრო სისტემები ფიზიკური კონტაქტის გარეშე.

საერთაშორისო ურთიერთობები: კიბერსივრცე გახდა ახალი არენა გეოპოლიტიკური დაპირისპირებისთვის. ქვეყნები იყენებენ კიბერშესაძლებლობებს როგორც "რბილი ძალის" ინსტრუმენტს, რათა გაავრცელონ თავიანთი გავლენა და დააზიანონ მოწინააღმდეგეების რეპუტაცია.

კიბერუსაფრთხოების გამოწვევების საპასუხოდ, თანამედროვე ქვეყნები ახორციელებენ მასშტაბურ ინვესტიციებს კიბერუსაფრთხოების სფეროში. ეს მოიცავს სპეციალიზებული კიბერუსაფრთხოების სააგენტოების შექმნას, კიბერშეტევებზე რეაგირების ჯგუფების ფორმირებას და საერთაშორისო თანამშრომლობის გაღრმავებას კიბერდანაშაულთან ბრძოლის მიმართულებით.

ამ რეალობაში, ბრძოლისუნარიანობის თვალსაზრისით, კრიტიკულად მნიშვნელოვანია სამხედრო ობიექტების კიბერუსაფრთხოების მიმართულება, რომელმაც უნდა უზრუნველყოს:

სამხედრო კომუნიკაციების უსაფრთხოება: კრიტიკულად მნიშვნელოვანია დაცული იყოს სამხედრო პერსონალს შორის კომუნიკაცია. კიბერშეტევამ შეიძლება გამოიწვიოს კომუნიკაციის შეფერხება, მწყობრიდან გამოსვლა, მნიშვნელოვანი ინფორმაციის გაჟონვა და სხვ.

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

სამხედრო ინფრასტრუქტურის დაცვა: თანამედროვე სამხედრო ბაზები და ობიექტები იყენებენ "ჭკვიან" სისტემებს, რომლებიც მოწყვლადია კიბერშეტევების მიმართ.
შეიარაღების სისტემების უსაფრთხოება: თანამედროვე შეიარაღება ხშირად შემთხვევაში დაფუძნებულია კომპიუტერულ სისტემებზე და შესაბამისად საჭიროებს დაცვას არასანქცირებული წვდომისგან.

აღნიშნული გამოწვევების გათვალისწინებით ბევრმა ქვეყანამ თავდაცვის მიმართულებით აქტიურად დაიწყო სპეციალიზირებული კიბერშენაერთების შექმნა და განვითარება, რომელიც სპეციალიზირებულია ციფრულ გარემოში ოპერაციების წარმოებაზე. თანამედროვე სამყაროში, სადაც ინფორმაციული ტექნოლოგიები განსაზღვრავს სამხედრო უპირატესობას, აღნიშნული სახის შენაერთების როლი კრიტიკულად მნიშვნელოვანი გახდა.

სხვადასხვა ქვეყნების გამოცდილებიდან გამომდინარე, კიბერშენაერთების ორგანიზაციული სტრუქტურა შეიძლება შემდეგი სახით ჩამოყალიბდეს:

კიბერდაზვერვის განყოფილება/ქვედანაყოფი - საფრთხეების იდენტიფიკაცია და ანალიზი, მოწინააღმდეგის კიბერშესაძლებლობების შეფასება და ტექნოლოგიური ტენდენციების მონიტორინგი;
კიბერთავდაცვის განყოფილება/ქვედანაყოფი - ქსელების და სისტემების მონიტორინგი, უსაფრთხოების ხარვეზების აღმოჩენა და აღმოფხვრა, ინციდენტებზე რეაგირება;
კიბერშეტევების განყოფილება/ქვედანაყოფი - შემტევი კიბეროპერაციების დაგეგმვა და განხორციელება, მავნე პროგრამული უზრუნველყოფის შემუშავება, მოწინააღმდეგის სისტემებში შეღწევის მეთოდების განვითარება;
კვლევისა და განვითარების განყოფილება/ქვედანაყოფი - ახალი ტექნოლოგიების შემუშავება, კიბერშესაძლებლობები განვითარება, უსაფრთხოების ინსტრუმენტების შექმნა.

ტრადიციული შეიარაღებული დანაყოფების მსგავსად, კიბერშენაერთებში უნდა გაიმიჯნოს თავდაცვითი და თავდასხმითი ოპერაციები, კერძოდ:

თავდაცვითი ოპერაციები - ისინი ძირითადად მოიცავენ შემდეგ პუნქტებს:
ა) ქსელების მონიტორინგი
რეალურ დროში თვალყურის დევნება;
ანომალიების დეტექცია;
პროაქტიული საფრთხეების იდენტიფიკაცია.
ბ) ინციდენტებზე რეაგირება
- სწრაფი რეაგირების პროტოკოლები;
- ზიანის შეფასება და შემცირება;
- სისტემების აღდგენა;

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

გ) კრიტიკული ინფრასტრუქტურის დაცვა

- ენერგეტიკული სისტემების უსაფრთხოება;
- სამხედრო კომუნიკაციების დაცვა;
- სტრატეგიული ობიექტების კიბერუსაფრთხოება.

შეტევითი ოპერაციები - ისინი ძირითადად მოიცავენ შემდეგ პუნქტებს:

ა) კიბერშეტევების ორგანიზება

- DDoS შეტევები;
- მავნე პროგრამული უზრუნველყოფის გავრცელება;
- სოციალური ინჟინერია.

ბ) ინფორმაციის მოპოვება

- ელექტრონული დაზვერვა (SIGINT);
- მოწინააღმდეგის სისტემებში შეღწევა;
- კომუნიკაციების არხებში შეღწევა.

გ) კიბერსაბოტაჟი

- მოწინააღმდეგის სისტემების გათიშვა/პარალიზება;
- მონაცემთა განადგურება ან მოდიფიცირება;
- დეზინფორმაციის გავრცელება.

ზემოთქმულიდან გამომდინარე, შეიძლება დავასკვნათ, რომ თანამედროვე ეტაპზე კიბერდანაყოფი წარმოადგენს თანამედროვე სამხედრო ძალების აუცილებელ კომპონენტს, რომელიც უზრუნველყოფს უსაფრთხოებას ციფრულ სივრცეში, რაც საბოლოო ჯამში განსაზღვრავს ქვეყნის უსაფრთხოებას. მისი ეფექტური ფუნქციონირება მოითხოვს მუდმივ განვითარებას, ინოვაციურ მიდგომებს და საერთაშორისო თანამშრომლობას. მომავალში კიბერშენაერთების როლი და მნიშვნელობა კიდევ უფრო გაიზრდება, რაც მოითხოვს მეტ ინვესტიციას, კვალიფიციურ კადრებს და ტექნოლოგიურ განვითარებას.

ამ მოსაზრებას კიდევ უფრო ამყარებს სტატისტიკა, რომელიც წარმოაჩენს როგორც კიბერსშტევების განმახორციელებელ და სამიზნე ქვეყნებს, ასევე განხორციელებული შეტევების რაოდენობას.

სამიზნე ქვეყნები და მათზე განხორციელებული შეტევების რაოდენობა (2022-2023 წწ):

ამ ჩამონათვალში ლიდერობს უკრაინა 1500 შეტევით, რაც გამოწვეულია მიმდინარე კონფლიქტით რუსეთთან.

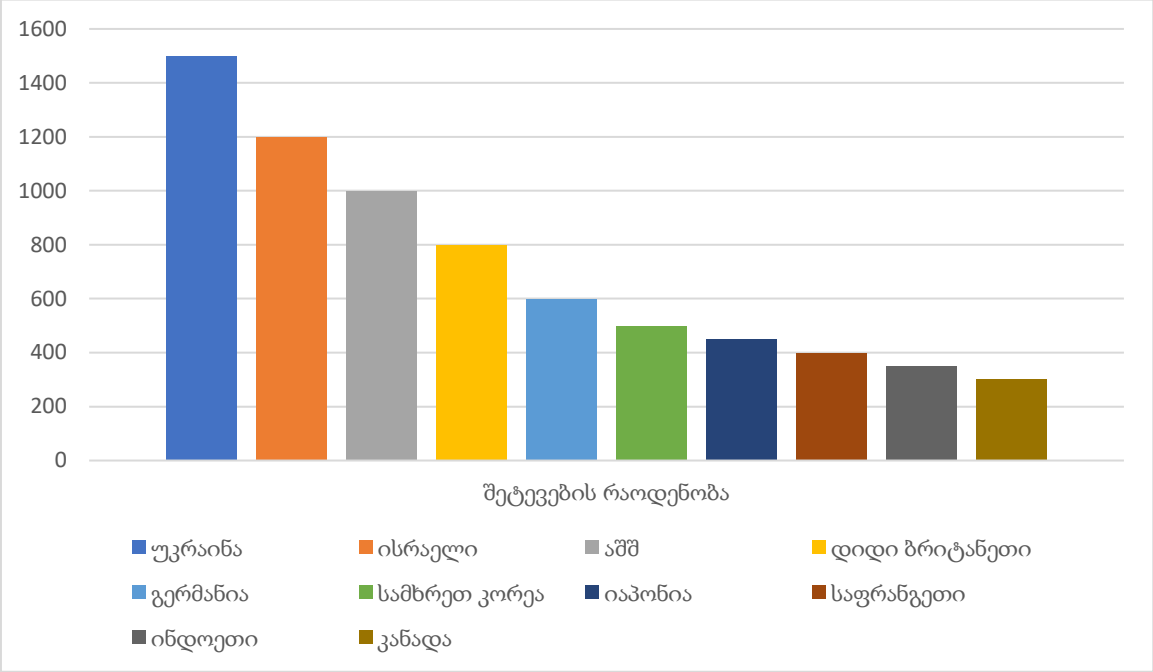
ისრაელი მეორე ადგილზეა 1200 შეტევით, რაც უკავშირდება რეგიონულ დაძაბულობას.

აშშ, გაერთიანებული სამეფო და გერმანია ასევე მაღალ პოზიციებზე არიან, რაც ასახავს მათ, როგორც ხშირ სამიზნეებს გლობალური კიბერშეტევებისთვის.

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

შემტევი ქვეყნები და მათთან ასოცირებული დაჯგუფებები (2022-2023 წწ):

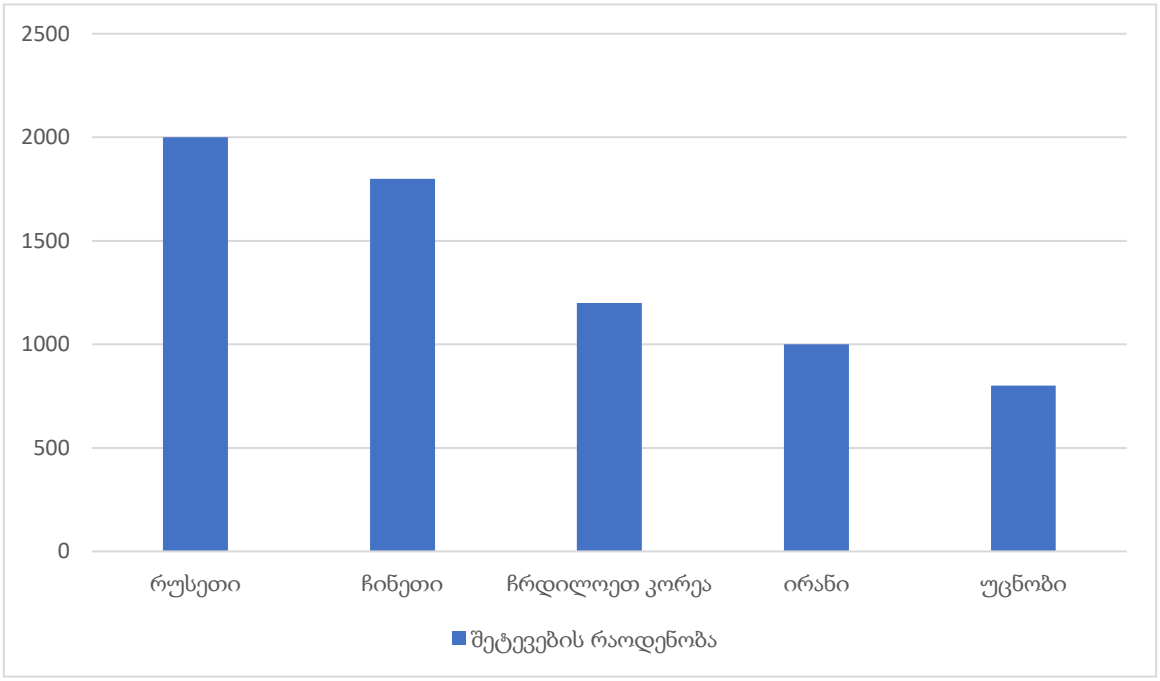
რუსეთი და ჩინეთი ლიდერობენ შეტევების რაოდენობით.
ჩრდილოეთ კორეა და ირანი ასევე მნიშვნელოვან პოზიციებს იკავებენ.
დაჯგუფებებს შორის ლიდერობენ Fancy Bear (რუსეთთან ასოცირებული) და Lazarus Group (ჩრდილოეთ კორეასთან ასოცირებული).



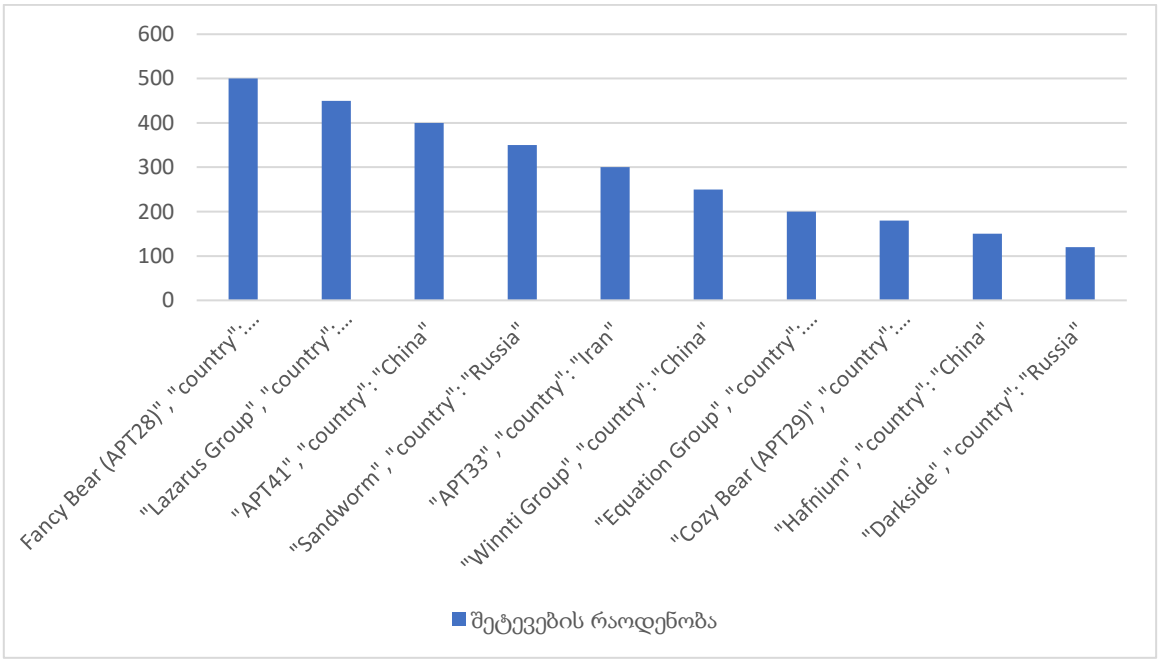
დიაგრამა 1. სამიზნე ქვეყნების სტატისტიკური მონაცემები (2022 – 2023 წწ) [7]

[7] Microsoft Digital Defense Report 2023

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)



დიაგრამა 2. შემტევი ქვეყნების სტატისტიკური მონაცემები (2022 – 2023 წწ) [8]



დიაგრამა 3. სხვადასხვა ქვეყნებთან ასოცირებული შემტევი ორგანიზაციების მონაცემები (2022 – 2023 წწ) [9]

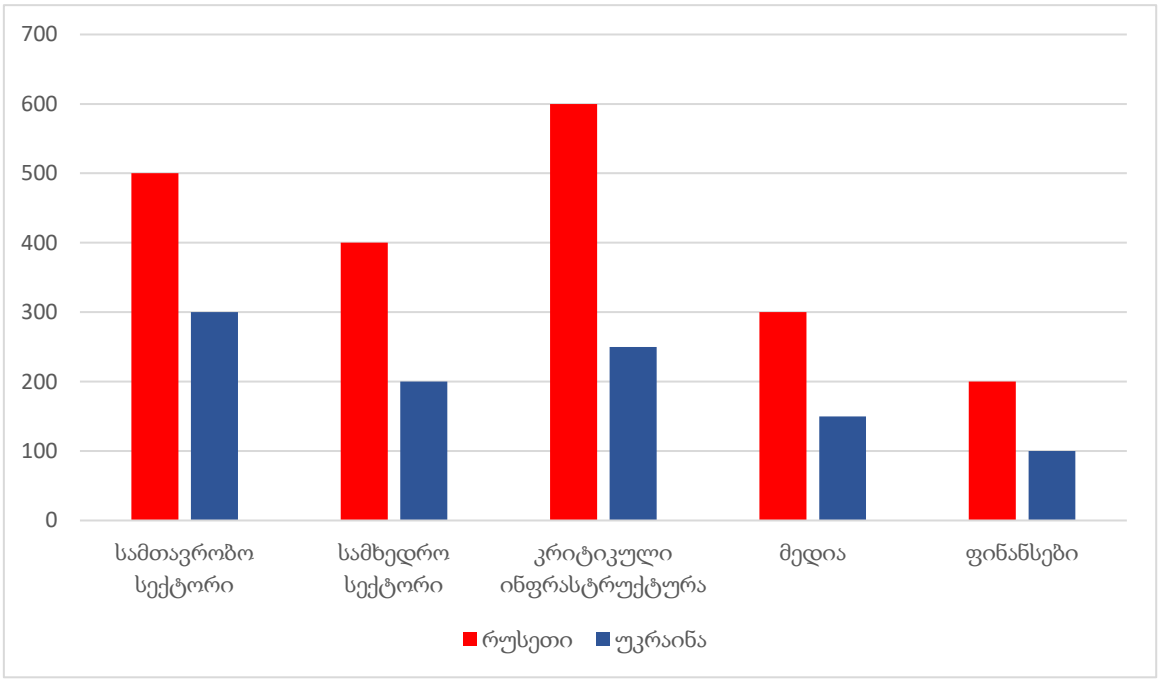
აღნიშნული მიმართულებით განსაკუთრებული ადგილი უჭირავს რუსეთ-უკრაინის კონფლიქტს, რომლის დროსაც არაერთი მსხვილი კიბერშეტევა განხორციელდა, რომლებმაც მნიშვნელოვანი ზარალი მიაყენეს კონფლიქტის მხარეებს. შეიძლება ითქვას, რომ აღნიშნულმა კონფლიქტმა ნათლად წარმოაჩინა თანამედროვე ეტაპზე კიბერუსაფრთხოების მზარდი მნიშვნელობა. მნიშვნელოვანია, რომ ორივე მხარემ კიბერშე-

[8] Check Point Research, Mid-Year Report 2023
[9] CrowdStrike Intelligence Report 2023

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

საძლებლობები გამოიყენა სხვადასხვა მიზნით და ფორმით, როგორც სამხედრო ოპერაციების მხარდაჭერით, ასევე ფსიქოლოგიური ზემოქმედებით.

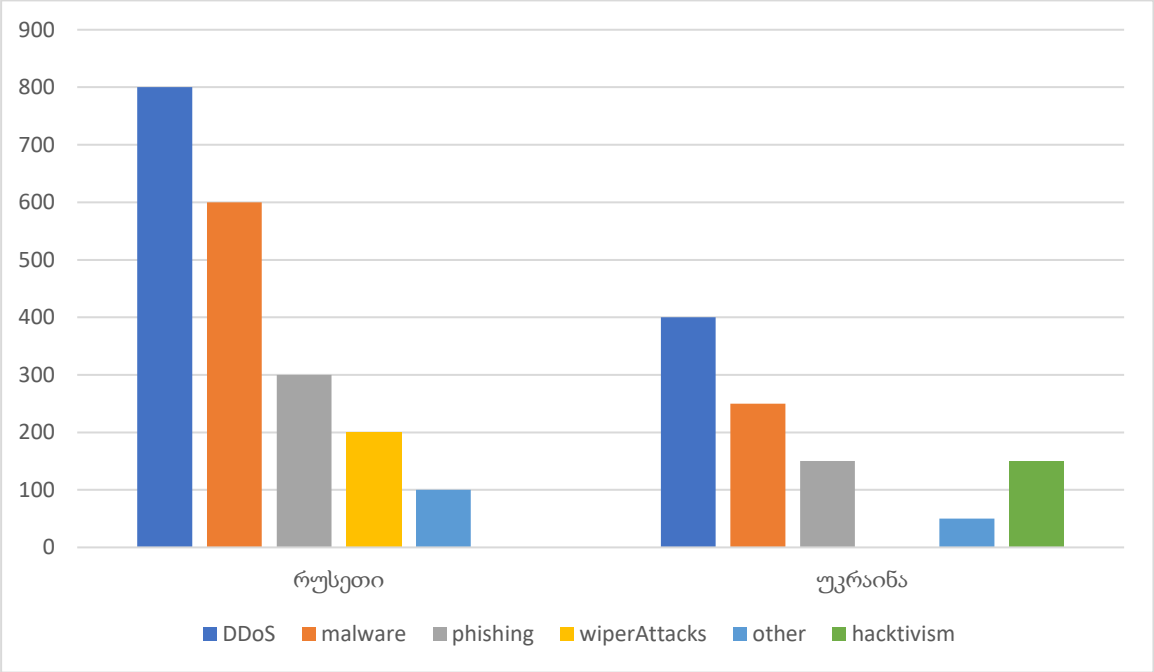
ამ თვალსაზრით ძალზედ მნიშვნელოვანია სტატისტიკური მონაცემები, რომლებიც ასახევან როგორც რუსეთის, ასევე უკრაინის მიერ განხორციელებულ კიბერშეტევებს, მათ სამიზნეებს და ფორმებს.



დიაგრამა 4. რუსეთ-უკრაინის კონფლიქტში განხორციელებული კიბერშეტევების სტატისტიკა (2022 – 2023 წწ)[10]

[10] Recorded Future Intelligence Report 2023

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)



დიაგრამა 5. გამოყენებული შეტევების ფორმების სტატისტიკა[11]

აღნიშნული მონაცემებიდან ირკვევა, რომ რუსეთმა განახორციელა დაახლოებით 2000 მნიშვნელოვანი კიბერშეტევა უკრაინაზე ომის დაწყებიდან. აღსანიშნავია, რომ ეს რიცხვი ასახავს მხოლოდ დოკუმენტირებულ შემთხვევებს და რეალური რაოდენობა შესაძლოა გაცილებით მეტი იყოს. შეტევის ძირეითადი სამიზნეები იყო:

სამთავრობო უწყებები (500 შეტევა, 25%) რუსეთის ერთ-ერთი მთავარი სამიზნე იყო უკრაინის მთავრობის ფუნქციონირების შეფერხება.

სამხედრო ობიექტები (400 შეტევა, 20%) შეტევები მიმართული იყო უკრაინის სამხედრო კომუნიკაციებისა და კომანდირების სისტემების წინააღმდეგ.

კრიტიკული ინფრასტრუქტურა (600 შეტევა, 30%) ენერგეტიკა, წყალმომარაგება და სატრანსპორტო სისტემები იყო ხშირი სამიზნე.

მედია (300 შეტევა, 15%) შეტევები მიზნად ისახავდა ინფორმაციის გავრცელების შეფერხებას და დეზინფორმაციის ხელშეწყობას.

საფინანსო სექტორი (200 შეტევა, 10%) ბანკები და საფინანსო ინსტიტუტები დაზარალდნენ ეკონომიკური დესტაბილიზაციის მცდელობით.

შეტევების განხორციელებისას რუსეთის საოკუპაციო მხარე იყენებდა სხვადასხვა ფორმის შეტევებს:

DDoS შეტევები (800 შეტევა, 40%) ყველაზე ხშირად გამოყენებული მეთოდი, მიმართული ვებ-სერვისების გათიშვისკენ.

[11] Mandiant Special Report 2023

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

მავნე პროგრამული უზრუნველყოფა (600 შეტევა, 30%) რთული ვირუსები და ტროიანები გამოიყენებოდა სისტემებში შეღწევისთვის.

ფიშინგი (300 შეტევა, 15%) მიზნობრივი ფიშინგ-კამპანიები სენსიტიური ინფორმაციის მოპოვების მიზნით.

Wiper-შეტევები (200 შეტევა, 10%) დესტრუქციული პროგრამები, რომლებიც შლიან მონაცემებს და აზიანებენ სისტემებს.

სხვა (100 შეტევა, 5%) მათ შორის სოციალური ინჟინერია და ნულოვანი დღის ექსპლოიტები.

რუსული შეტევებიდან თავისი მაშტაბებით და მნიშვნელობით განსაკუთრებით აღსანიშნავია შემდეგი შეტევები:

ViaSat-ის თანამგზავრული ინტერნეტის მომსახურების გათიშვა ომის დაწყების დღეს, რამაც გავლენა მოახდინა უკრაინის სამხედრო კომუნიკაციებზე.

Industroyer2 მავნე პროგრამის გამოყენების მცდელობა უკრაინის ენერგოქსელის წინააღმდეგ 2022 წლის აპრილში.

მასშტაბური DDoS შეტევები უკრაინის საბანკო სექტორზე 2022 წლის თებერვალში, რუსეთის შეჭრამდე რამდენიმე დღით ადრე.

აღსანიშნავია, აგრეთვე უკრაინისა და მასთან ასოცირებული ქვედანაყოფების საპასუხო შეტევები აგრესორი ქვეყნის მიმართებით. მათ განახორციელეს დაახლოებით 1000 მნიშვნელოვანი კიბერშეტევა რუსეთზე. ეს რიცხვი ნაკლებია რუსეთის შეტევებთან შედარებით, თუმცა რეალურად ასახავს უკრაინის მზარდ კიბერშესაძლებლობებს.

მათი შეტევების სამიზნეს ძირითადად წარმოადგენდა:

სამთავრობო უწყებები (300 შეტევა, 30%) რუსეთის მთავრობის ვებ-გვერდები და შიდა სისტემები.

სამხედრო ობიექტები (200 შეტევა, 20%) მცდელობები, შეეფერხებინათ რუსეთის სამხედრო ლოგისტიკა და კომუნიკაციები.

კრიტიკული ინფრასტრუქტურა (250 შეტევა, 25%) ენერგეტიკა, ტრანსპორტი და სხვა სასიცოცხლო სისტემები.

მედია (150 შეტევა, 15%) რუსული მედია-საშუალებები, პროპაგანდის წინააღმდეგ ბრძოლის მიზნით.

საფინანსო სექტორი (100 შეტევა, 10%) ბანკები და ფინანსური ინსტიტუტები.

ამ შემთხვევაშიც, შეტევებისას გამოყენებულ იქნა სხვადასხვა ფორმები. არსებული სტატისტიკის მიხედვით გვაქვს შემდეგი სურათი:

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

DDoS შეტევები (400 შეტევა, 40%) ფართოდ გამოყენებული მეთოდი რუსული ვებ-რესურსების წინააღმდეგ.

მავნე პროგრამული უზრუნველყოფა (250 შეტევა, 25%) სპეციალიზებული ვირუსები და ტროიანები.

ფიშინგი (150 შეტევა, 15%) მიზნობრივი კამპანიები რუსი თანამდებობის პირების წინააღმდეგ.

ჰაქტივიზმი (150 შეტევა, 15%) საპროტესტო და პროპაგანდისტული აქციები ონლაინ სივრცეში.

სხვა (50 შეტევა, 5%) მათ შორის სოციალური ინჟინერია და ნულოვანი დღის ექსპლოიტები.

უკრაინული მხარის მიერ განხორციელებულ შეტევებში განსაკუთრებულად გამორჩეულია შემდეგი შეტევები:

რუსეთის ცენტრალური ბანკის მონაცემთა ბაზის გატეხვა და კონფიდენციალური ინფორმაციის გამოქვეყნება.

რუსული სახელმწიფო ტელევიზიის სიგნალის დარღვევა და ანტისაომარი მესიჯების გავრცელება.

რუსეთის საგარეო საქმეთა სამინისტროს ვებ-გვერდში შეღწევა და ინფორმაციის მოპოვება.

წარმოდგენილი სტატისტიკური მონაცემების ანალიზის საფუძველზე შეიძლება დავასკვნათ, რომ რუსეთ-უკრაინის კონფლიქტში განხორციელებულმა კიბერშეტევებმა აჩვენა კიბერსივრცის, როგორც თანამედროვე კონფლიქტის მნიშვნელოვანი არეალის როლი. ორივე მხარემ გამოიყენა მრავალფეროვანი ტაქტიკა და ტექნიკა, რამაც გავლენა მოახდინა არა მხოლოდ სამხედრო ოპერაციებზე, არამედ ზოგადად ქვეყნების განვითარებაზე, მათ ეკონომიკაზე, საზოგადოებრივ აზრსა და დიპლომატიურ ურთიერთობებზეც. ეს კონფლიქტი კიდევ ერთხელ უსვამს ხაზს კიბერუსაფრთხოების მნიშვნელობას ეროვნული უსაფრთხოების სტრატეგიებში და აჩვენებს, რომ მომავალში კიბერშესაძლებლობები კიდევ უფრო მნიშვნელოვან როლს ითამაშებს საერთაშორისო კონფლიქტებში.

დასკვნა

თანამედროვე სამყაროში ტრადიციული სამხედრო ოპერაციების პარალელურად, კიბერსივრცე გახდა ახალი საბრძოლო არეალი, რის გამოც ქვეყნები სულ უფრო მეტ ყურადღებას უთმობენ როგორც კიბერუსაფრთხოებას, ასევე კიბერშეიარაღების განვითარებას.

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

ამავე დროს, თანამედროვე სამხედრო ოპერაციები მჭიდროდაა დაკავშირებული ციფრულ ტექნოლოგიებთან. ეს ეხება როგორც საკომუნიკაციო სისტემებს, ასევე თანამედროვე შეიარაღებას. თითქმის ყველა სამხედრო კომპონენტი დამოკიდებულია კომპიუტერულ სისტემასა და ტექნოლოგიაზე. მნიშვნელოვანია, რომ ეს დამოკიდებულება მოიცავს საფრთხეებსაც, რაც თავისთავად ზრდის კიბერუსაფრთხოების გაძლიერების აუცილებლობას.

ამ მიმართულებით აღსანიშნავია, რომ საქართველოს თავდაცვის ძალებში ფუნქციონირებს კიბერუსაფრთხოების ბიურო, რომელიც ახორციელებს თავდაცვის სამინისტროსა და მისი სტრუქტურული ერთეულების კიბერუსაფრთხოებას. თუმცა, არსებული რთული მოვლენების ფონზე, სხვა ქვეყნების მაგალითზე, მიზანშეწონილად მიგვაჩნია საქართველოში სპეციალიზირებული კიბერდანაყოფის შექმნის მიმართულებით მუშაობა, რაც მნიშვნელოვნად გააძლიერებს ქვეყნის თავდაცვისუნარიანობას.

ბიბლიოგრაფია

საქართველოს თავდაცვის სამინისტრო. (2023). "კიბერუსაფრთხოების სტრატეგიული მიმოხილვა."

ნ. არაბული, ა. შეყელაძე, ვ. ადამია, ზ. ცირამუა „კიბერუსაფრთხოების გამოწვევები, კონცეფციები და პრაქტიკა“. გამომცემლობა „სამშობლო“. 2024.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2023). "Cyber Operations in Contemporary Military Conflicts." https://ccdcoe.org/

Microsoft Digital Defense Report (2023). "Global Threat Activity and Cyber Security Trends." Microsoft Security https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Microsoft Digital Defense Report (2024). "Global Threat Activity and Cyber Security Trends." Microsoft Security https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Recorded Future. "Cyber Operations in the Russia-Ukraine War 2022-2023." Intelligence Report, 2023.

Microsoft Digital Defense Report. "Nation State Threats and Targeted Cyberattacks." Annual Security Review, 2023. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Check Point Research. "Cyber Attack Trends: 2023 Mid-Year Report." Global Threat Intelligence, 2023.

Mandiant. "Special Report: Russia-Ukraine Crisis." Cyber Security Analysis, 2023.

CERT-UA. "Ukrainian Computer Emergency Response Team Annual Report 2022-2023." Government Special Communications Service of Ukraine, 2023.

CrowdStrike. "Global Threat Report: Russia-Ukraine Conflict Analysis." Intelligence Report Series,2023.

Mandiant Threat Intelligence Report (2023). "Russia-Ukraine War: A Cyber Warfare Perspective."

ISSN 1512-0708 (PRINT)
ISSN 2587-4837 (ONLINE)

CERT-UA (Computer Emergency Response Team of Ukraine) Reports (2022-2023). "Cyber Attacks Statistics During Russian Invasion."

Council on Foreign Relations. (2023). "Cyber Operations in Military Conflicts: Lessons from Ukraine."

U.S. Cybersecurity & Infrastructure Security Agency (CISA). (2023). "Advisory on Russian State-Sponsored Cyber Operations."

United Nations Institute for Disarmament Research (UNIDIR). (2023). "The Role of Cyber Operations in Modern Military Conflicts."

RAND Corporation. (2023). "The Evolution of Cyber Operations in Modern Warfare."