

## სამხედრო დანაყოფების მართვის საინფორმაციო-ტექნოლოგიური სისტემები

ნანი არაბული<sup>1</sup>, ავთანდილ მიგინეიშვილი<sup>2</sup>, მიხეილ გოგნაძე<sup>3</sup>

<sup>1</sup>საქართველოს ტექნიკური უნივერსიტეტი

<sup>2</sup>ახალი უნივერსიტეტი

<sup>3</sup>საქართველო თავდაცვის ძალების დასავლეთის სარდლობის მე-3 ქვეითი ბრიგადა

### რეზიუმე

თანამედროვე სამხედრო ოპერაციების წარმატება მნიშვნელოვნად არის დამოკიდებული ინფორმაციის სწრაფად შეგროვებასა და ანალიზზე. წარმოდგენილ სტატიაში განხილულია სამხედრო საინფორმაციო-ტექნოლოგიური სისტემების ევოლუცია, არქიტექტურა და ძირითადი კომპონენტები. Network-Centric Warfare მოდელი, AI, IoT და სენსორული ქსელები ქმნიან ბრძოლის ველის ციფრულ ჩარჩოს, რომელიც უზრუნველყოფს რეალურ დროში გადაწყვეტილებების მიღებას. სტრატეგიული, ოპერატიული და ტაქტიკური დონეები ინტეგრირებულია ტექნოლოგიური ინფრასტრუქტურით, რომელიც მოიცავს მონაცემთა ბაზებს, GIS სისტემებს, დაშიფვრის ალგორითმებს და კიბერუსაფრთხოების მექანიზმებს. ავტონომიური სისტემები, დრონები და სამხედრო რობოტები ზრდიან ოპერაციულ მოქნილობას და ამცირებენ ადამიანურ რისკებს. აპლიკაციები ISR ფუნქციებით და მართვის მექანიზმებით აძლიერებენ სიტუაციურ ცნობიერებას. სტატიაში ასევე განხილულია არსებული გამოწვევები და მათი დაძლევის სამომავლო რეკომენდაციები.

**საკვანძო სიტყვები:** სამხედრო საინფორმაციო სისტემები; Network-Centric Warfare; ხელოვნური ინტელექტი (AI); ინტერნეტ ნივთების (IoT) ტექნოლოგია; სენსორული ქსელები.

### 1 შესავალი.

თანამედროვე სამხედრო მოქმედებების ეფექტიანობა მნიშვნელოვნად არის დამოკიდებული ინფორმაციის სწორად შეგროვებასა და სწრაფად დამუშავებაზე. ბრძოლის ველის დინამიკურ პირობებში წამებში მიღებული გადაწყვეტილებები განსაზღვრავს ოპერაციის წარმატებას. სწორედ ამიტომ, ინფორმაციული ტექნოლოგიები სამხედრო სტრატეგიის განუყოფელ ნაწილად იქცა. ციფრული პლატფორმები უზრუნველყოფს ინფორმაციის სწრაფ გადაცემას, რომელიც აუმჯობესებს მონაცემთა ანალიზსა და ქვედანაყოფებს შორის კოორდინაციას.

დღევანდელ მსოფლიოში სამხედრო ტექნოლოგიების განვითარება აღარ არის მხოლოდ ტექნიკური ინოვაციების სფერო, იგი უშუალოდ განსაზღვრავს სახელმწიფოების თავდაცვის უნარიანობას, სტრატეგიულ ავტონომიასა და ეროვნული უსაფრთხოების პოლიტიკას. თანამედროვე კონფლიქტები, იქნება ეს უკრაინაში მიმდინარე ომი, ახლო აღმოსავლეთში ძალთა გადაადგილება თუ აზია-წყნარი ოკეანის რეგიონში მზარდი დაძაბულობა, ცხადად აჩვენებს, რომ ინფორმაციული ტექნოლოგიები გახდა ბრძოლის გადამწყვეტი ფაქტორი. ბრძოლის ველზე წარმატება აღარ ეფუძნება მხოლოდ ფიზიკურ რესურსებსა და შეიარაღებას, გადამწყვეტი მნიშვნელობა აქვს მონაცემების სიზუსტეს, მათ დროულ გადაცემასა და სწორი გადაწყვეტილებების მიღებას.

ინფორმაციული ტექნოლოგიური სისტემები ქმნიან ე.წ. Network-Centric Warfare მოდელს, სადაც თითოეული ჯარისკაცი, სატელიტი, დრონი და სენსორი დაკავშირებულია ერთმანეთთან.

ეს მიდგომა საშუალებას აძლევს მეთაურებს მიიღოს გადაწყვეტილებები არა ინტუიციით, არამედ ზუსტ მონაცემებზე დაფუძნებით. ასეთი სისტემების არქიტექტურა დღეს წარმოადგენს ერთ-ერთ ყველაზე მნიშვნელოვან მიმართულებას მსოფლიოს წამყვანი სახელმწიფოების სამხედრო კვლევით სფეროს. მაგალითად, აშშ, ნატო და იაპონია აქტიურად ატარებენ კვლევებს AI-ზე და 5G-ზე დაფუძნებულ ტაქტიკურ კომუნიკაციებზე, ხოლო რუსეთი და ჩინეთი ქმნიან საკუთარი სამხედრო ციფრულ გარემოს.

საქართველოსთვის ეს თემა არანაკლებ აქტუალურია. რეგიონში არსებული გეოპოლიტიკური გამოწვევები, ჰიბრიდული ომების საფრთხეები და კიბერშეტევების მზარდი სიხშირე ნათლად აჩვენებს, რომ უსაფრთხოების ეფექტიანი სისტემა შეუძლებელია ინფორმაციული ტექნოლოგიების გარეშე. ეროვნული თავდაცვის სისტემაში თანამედროვე IT ინფრასტრუქტურის დანერგვა ზრდის ბრძოლის ველის ცნობიერებას, ამცირებს რეაგირების დროს და ზრდის ოპერაციულ მოქნილობას. კიბერუსაფრთხოების გაძლიერება და ინფორმაციის დაცული გადაცემა კი უზრუნველყოფს სამხედრო კომუნიკაციის საიმედოობას.

სამხედრო საინფორმაციო-ტექნოლოგიური სისტემების შესწავლა და განვითარება არა მხოლოდ აკადემიური ინტერესის საგანია, არამედ პირდაპირ უკავშირდება ქვეყნის თავდაცვისუნარიანობას, რეგიონულ უსაფრთხოებასა და ტექნოლოგიურ პროგრესს. ამ მიმართულებით ინვესტირება წარმოადგენს აუცილებელ ნაბიჯს სახელმწიფოს გრძელვადიანი სტრატეგიული მდგრადობის უზრუნველსაყოფად.

არსებული მოდელების არქიტექტურა

უძველესი დროიდან სამხედრო ქვედანაყოფებს შორის ინფორმაციის მიმოცვლისთვის სხვადასხვა ტექნოლოგია გამოიყენებოდა, რომელიც ეპოქის ტექნიკურ შესაძლებლობებზე იყო დამოკიდებული. თავდაპირველად ეს იყო სიგნალებით, როგორცაა დროშებით, სინათლის სიგნალებითა და მორზეს ანბანით გადაცემული შეტყობინებები. მოგვიანებით, მე-20 საუკუნის დასაწყისში, სამხედრო ქვედანაყოფებში ფართოდ დაიწერა ტელეგრაფი და ფიქსირებული ტელეფონი, რამაც მნიშვნელოვანი ნაბიჯი გადადგა ტაქტიკური კომუნიკაციის მიმართულებით. მეორე მსოფლიო ომისა და ცივი ომის პერიოდში უმთავრეს როლს ასრულებდა ანალოგური რადიოკავშირი, რომელიც საშუალებას აძლევდა სამხედროებს უფრო სწრაფად გადაეცათ ინფორმაცია, თუმცა დაცულობისა და საიმედოობის მხრივ ეს სისტემები სუსტი იყო. ინფორმაციის ნაწილი კვლავ ფიზიკური გზით გადაჰქონდათ (დისკებით, ქაღალდით ან სპეციალური კურიერებით), რაც დიდ დროს მოითხოვდა და დაკარგვის და დაზიანების რისკებს ზრდიდა.

თანამედროვე ეპოქაში, ტექნოლოგიური პროგრესის შედეგად, სამხედრო საინფორმაციო არქიტექტურა რადიკალურად შეიცვალა. ციფრული რადიოკავშირი და Software Defined Radio (SDR) სისტემები უზრუნველყოფს მრავალარხიან, დაშიფრულ და მოქნილ კომუნიკაციას, რომელიც თითქმის შეუძლებელია, რომ მტრის მიერ იქნას აღმოჩენილი. სატელიტური არხები (SATCOM) ქმნიან გლობალურ ქსელს და საშუალებას აძლევს ჯარისკაცს ნებისმიერი ადგილიდან დაუკავშირდეს შტაბს. თუ ადრე ინფორმაციის ნაკადი ძირითადად ცენტრალიზებულ შტაბზე იყო დამოკიდებული, დღეს გაგრძელებულია დეცენტრალიზებული, ქსელურ მოდელზე დაფუძნებული არქიტექტურა, სადაც თითოეულ ქვედანაყოფს შეუძლია მიიღოს და გადასცეს მონაცემები რეალურ დროში.

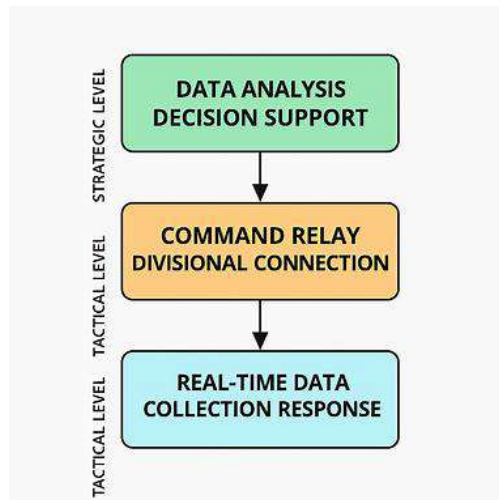
გარდა ამისა, სამხედრო კომუნიკაცია აღარ შემოიფარგლება მხოლოდ ხმოვანი შეტყობინებებით. თანამედროვე სისტემები აერთიანებს ვიდეოს, სურათებს, სენსორების მონაცემებსა

და დრონიდან მიღებულ ინფორმაციას. მობილური ტერმინალები და ტაბლეტები უშუალოდ ჯარისკაცებს აძლევს ბრძოლის ველზე გადაწყვეტილების მისაღებად საჭირო ინფორმაციას. ინტეგრირებულია IoT და სენსორული ქსელები, რომლებიც ავტომატურად აგროვებენ მონაცემებს გარემოს, ტექნიკისა და ჯარისკაცების მდგომარეობის შესახებ.

ძველი არქიტექტურისთვის დამახასიათებელი ნელი და დაუცველი კავშირი შეიცვალა სწრაფი, უსაფრთხო ქსელებით რაც უზრუნველყოფს მოქნილ და დაცულ კომუნიკაციას, რაც სამხედრო ოპერაციებისთვის უმნიშვნელოვანესია.

საინფორმაციო-ტექნოლოგიურ სისტემების არქიტექტურაში გამოყოფენ შრეობრივ და ტექნოლოგიურ სტრუქტურას.

შრეობრივი არქიტექტურა იყოფა შრეობრივ დონეებად და უზრუნველყოფს ეფექტურ მართვას, ოპტიმალურ რეაგირებას და სტრატეგიულ გადაწყვეტილებებს. შრეობრივი არქიტექტურის თითოეული დონე ემსახურება კონკრეტულ მიზანს:



სურ.1. შრეობრივი არქიტექტურა. ნაჩვენებია სტრატეგიული, ოპერატიული და ტაქტიკური დონეები, რომლებიც ერთმანეთთან დაკავშირებულია მონაცემთა ნაკადით

### 1. სტრატეგიული დონე, რომელიც მოიცავს:

მონაცემთა ანალიზის დონეს: გამოიყენება დიდი მოცულობის მონაცემების შესასწავლად, ტენდენციების გამოსავლენად და პროგნოზირების მოდელების შესაქმნელად.

გადაწყვეტილების მხარდაჭერა: BI (Business Intelligence) სისტემები, ML მოდელები და ანალიტიკური პლატფორმები უზრუნველყოფენ ოპტიმალური გადაწყვეტილებების მიღებაში.

დასაყრდენი ინსტრუმენტები: მონაცემთა საწყობები (Data Warehouses), OLAP, AI/ML მოდულები.

### 2. ოპერატიული დონე გამოიყენება ბრძანების ცენტრებისა და ქვედანაყოფების კოორდინაციისთვის. იგი მოიცავს:

კავშირის ქვედანაყოფებთან: უზრუნველყოფს უწყვეტ კომუნიკაციას სხვადასხვა ოპერატიულ ერთეულებს შორის.

ტექნოლოგიურ მხარდაჭერას: API-ები, მიკროსერვისები, სიგნალის გადაცემის პროტოკოლები (მაგ. MQTT, AMQP).

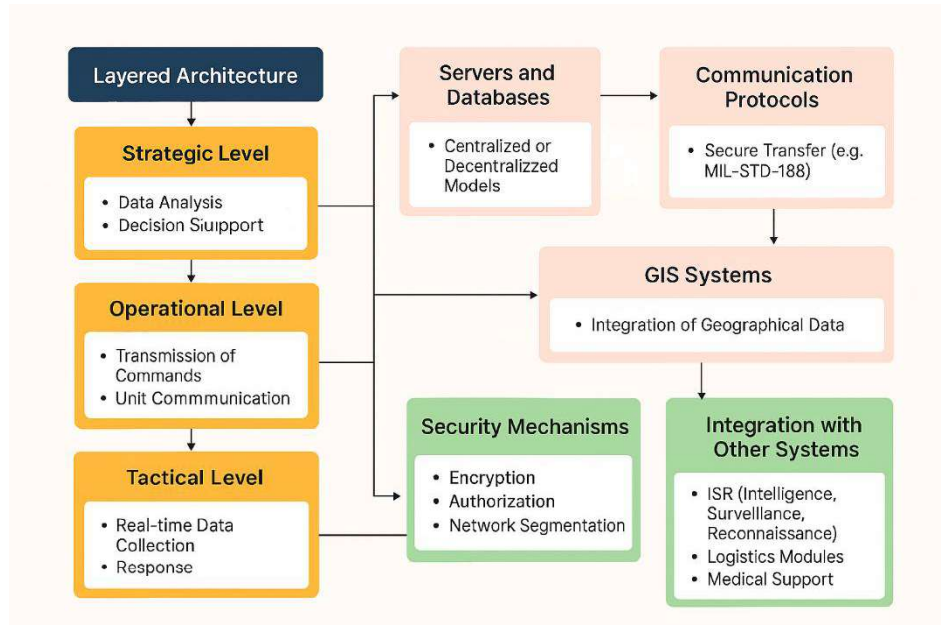
### 3. ტაქტიკური დონე, გამოიყენება მონაცემების შეგროვებისთვის: სენსორები, IoT მოწყობილობები და edge computing პლატფორმები უზრუნველყოფენ სწრაფ მონაცემთა მიღებას.

რეაგირება: ავტომატიზებული ალგორითმები, ალერტების სისტემა და ოპერატიული ინტერფეისები რეაგირებენ კრიტიკულ ცვლილებებზე.

მხარდაჭერა: GIS ინტეგრაცია, ვიდეო მონიტორინგი, დრონების მონაცემები.

ტექნოლოგიური არქიტექტურის მოიცავს:

1. სერვერებს და მონაცემთა ბაზებს, სადაც ხდება ცენტრალიზებული მოდელის სტრუქტურით მონაცემების შენახვა ერთიან მონაცემთა ცენტრში, რაც ამარტივებს მართვას და უსაფრთხოების კონტროლს.



სურ.2. ტექნოლოგიური სტრუქტურის დიაგრამა, სადაც წარმოდგენილია სერვერები, მონაცემთა ბაზები, GIS სისტემები, კომუნიკაციის პროტოკოლები და უსაფრთხოების მექანიზმები.

2. დეცენტრალიზებული მოდელი, რომელიც მონაცემებს ანაწილებს სხვადასხვა ლოკაციებზე, რაც ზრდის სისტემის გამძლეობას და რეაგირების სიჩქარეს.

აღნიშნულ არქიტექტურებში გამოიყენება შემდეგი ტექნოლოგიები: PostgreSQL, MongoDB, Cassandra, Kubernetes, Docker. და კომუნიკაციის პროტოკოლები, როგორებიცაა TLS/SSL, VPN, და სამხედრო სტანდარტები (მაგ. MIL-STD-188). ასევე UDP-დაფუძნებული პროტოკოლები რეალურ დროში კომუნიკაციისთვის. GIS სისტემები გამოიყენება რუკების ვიზუალიზაციისთვის, ობიექტების ლოკაციის განსაზღვრისთვის და ოპერატიული დაგეგმვისთვის, რომლის ძირითადი ფუნქციაა ტოპოგრაფიული ანალიზი, მარშრუტების დაგეგმვა, რისკების ზონირება.

უსაფრთხოების მექანიზმები ერთერთ მნიშვნელოვან ასპექტს წარმოადგენს აღნიშნულ არქიტექტურებში. გადაცემა ხორციელდება შუფრაციის ალგორითმებით AES-256, RSA და ECC ალგორითმებით. ასევე იყენებს ავტორიზაცია და ავთენტიფიკაციის მრავალფაქტორიან არქიტექტურას. ქსელურ სეგმენტაციას: VLAN-ები, Zero Trust არქიტექტურა, firewall-ები და intrusion detection სისტემები (IDS/IPS) და ლოგირება და მონიტორინგის სისტემებს, SIEM სისტემები (მაგ. Splunk, ELK Stack) უსაფრთხოების ინციდენტების დროული გამოვლენისთვის.

სისტემის არქიტექტურა, რომელიც ეფუძნება შერეობრივ მოდელს და ტექნოლოგიურ სტრუქტურას, წარმოადგენს ინტეგრირებულ და მოქნილ ჩარჩოს, რომელიც სრულად პასუხობს თანამედროვე ოპერაციული და სტრატეგიული მოთხოვნებს. მისი მოქნილობა,

ინტეგრირებულობა და რეალურ დროში რეაგირების უნარი ქმნის საფუძველს წარმატებული და ეფექტური ფუნქციონირებისთვის ნებისმიერ გარემოში.

**სამხედრო საინფორმაციო სისტემების ძირითადი კომპონენტები.** სამხედრო საინფორმაციო სისტემები აგებულია რამდენიმე კომპონენტზე, რომლებიც მთლიანობაში უზრუნველყოფენ ინფორმაციის შეგროვებას, გადამუშავებას, მიწოდებასა და გამოყენებას. ქვემოთ წარმოდგენილია ყველა მნიშვნელოვანი კომპონენტი, ფუნქციები, ტექნოლოგიური საფუძველი, რომლებიც აუცილებელია მათი ეფექტური მიმუშავებისთვის.

სამხედრო საინფორმაციო სისტემები აერთიანებს საველე და განვითარების საბრძოლო ავტომატიზაციის სისტემებსა და კომუნიკაციებს, რათა ფუნქციურად დააკავშიროს სტრატეგიული, ოპერატიული და ტაქტიკური შტაბები. სურათი 2 ასახავს სტრატეგიული, ოპერატიული და ტაქტიკური არქიტექტურების ურთიერთკავშირს, რომელიც აერთიანებს მრავალგანაწილებულ ელემენტს ინტეგრირებულ, ურთიერთთავსებად და თანმიმდევრულ ქსელში.

საკომუნიკაციო არხები- საკომუნიკაციო არხები სამხედრო სისტემების ქვაკუთხედი იქნის უზრუნველყოფენ მონაცემთა, ბრძანებების და სიტუაციური მოხსენებების კომპონენტების ერთობლივად გადაცემას. თანამედროვე გარემო მოიცავს:

ტრადიციულ და ციფრულ რადიოს (FM/AM, VHF/UHF, tactical SDR) - მიერთებულია frequency-hopping, ადაპტიური მოდულაცია და end-to-end დამიფრა;

სატელიტური კომუნიკაციები (SATCOM) უზრუნველყოფს გლობალური პოზიციონირების სისტემებს, მაღალი სისწრაფის და დაბალი დაყოვნების მონაცემთა გადაცემას.

IP-ზე დაფუძნებული ქსელები (ბრძოლის ველის LTE/5G ტაქტიკური ქსელები) - შესაძლებელი ხდება მაღალი მოცულობის მონაცემთა (ვიდეო სტრიმები) მიწოდება და QoS კონტროლი;

ოპტიკური და ბოჭკოვანი კავშირები, რომელიც უზრუნველყოფს მაღალ გამტარუნარიანობას.

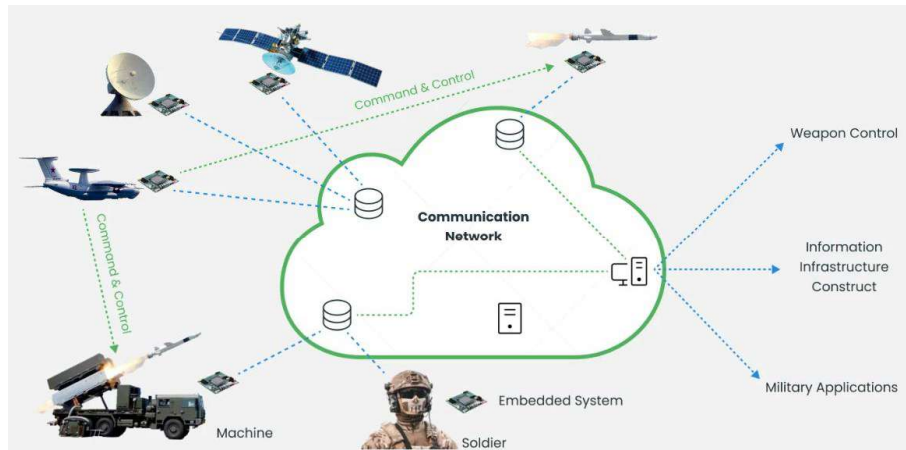
თანამედროვე სამხედრო საინფორმაციო სისტემების განვითარება მჭიდროდ არის დაკავშირებული თანამედროვე ტექნოლოგიებთან, რომლებიც აუმჯობესებენ ინფორმაციის შეგროვებას, ანალიზს და გადაცემას. ხელოვნური ინტელექტი გამოიყენება მონაცემთა სწრაფად დამუშავებისა და ანალიზისთვის. AI-ს მეშვეობით სამხედრო სისტემა შეუძლია:

- ცალკეული საფრთხეების იდენტიფიკაცია და პრიორიტეტიზაცია,
- ოპერატიული გადაწყვეტილებების მხარდაჭერა რეალურ დროში,
- სცენარების სიმულაცია და ოპტიმალური ქმედების გზების რეკომენდაცია.

IoT-ს საშუალებით საბრძოლო ველზე სხვადასხვა სენსორი, კამერა და მოწყობილობა უკავშირდება ერთმანეთს. ეს ქმნის ქსელს, რომელიც აკვირდება ჯარისკაცების, ტექნიკის და გარემოს მდგომარეობას, ავტომატურად აგროვებს მონაცემებს რეალურ დროში, ზრდის ბრძოლის ველის შესახებ ცნობიერებას და ოპერაციული გადაწყვეტილებების ეფექტურობას.

სენსორული ქსელები უზრუნველყოფენ მუდმივ მონიტორინგს, საზღვრების კონტროლსა და მოწინააღმდეგის გადაადგილების გამოვლენას. ისინი ქმნიან მრავალშრიან მონაცემთა ნაკადს, რომელიც ინტეგრირდება მონაცემთა მართვის სისტემებთან, უზრუნველყოფს დროულ რეაგირებას საფრთხეებზე და ოპერაციების უკეთესი კოორდინაციას.

ეს სამი ინოვაცია AI, IoT და სენსორული ქსელები ქმნის საფუძველს სწრაფი, ეფექტური და უსაფრთხო გადაწყვეტილებების მიღებისთვის თანამედროვე საბრძოლო გარემოში.



სურ.3. თანამედროვე სამხედრო კომუნიკაცია

თანამედროვე სამხედრო სტრატეგიაში ავტონომიურ სისტემებს განსაკუთრებული ადგილი უჭირავთ. ისინი მნიშვნელოვნად ამცირებენ ადამიანური რესურსის რისკებს და ზრდიან ოპერაციების ეფექტიანობას.

დრონები გამოიყენება როგორც სადაზვერვო, ასევე შეტევით ოპერაციებში დღესდღეობით ძალიან მნიშვნელოვან ასპექტს წარმოადგენს. სადაზვერვო დრონები აგროვებენ ინფორმაციას ბრძოლის ველზე, აკვირდებიან მტრის გადაადგილებას და აფიქსირებენ ცვლილებებს გარემოში. შეტევითი დრონები აღჭურვილია საბრძოლო საშუალებებით და შეიძლება გამოიყენონ ზუსტი დარტყმებისთვის მიზანზე. დრონების უპირატესობაა მაღალი მანევრირება, დაბალი ხარჯი და რისკის შემცირება სამხედრო პერსონალისთვის.

სამხედრო რობოტები გამოიყენება როგორც ლოჯისტიკურ, ასევე საბრძოლო ამოცანებში. ლოჯისტიკური რობოტები ამარაგებენ ქვედანაყოფებს საბრძოლო მასალით, საკვებით ან მედიკამენტებით რთულ გარემოში. საბრძოლო რობოტები აღჭურვილია სენსორებითა და იარაღით, რაც საშუალებას იძლევა საშიშ ზონებში ადამიანების გარეშე განხორციელდეს ოპერაციები. რობოტიკას შეუძლია ასევე განაღმვისა და ინფრასტრუქტურის აღდგენის ამოცანების შესრულება.

ავტონომიური სისტემების ინტეგრაცია სამხედრო ოპერაციებში ზრდის ოპერატიულ მოქნილობას, ამცირებს ადამიანური დანაკარგების ალბათობას და იძლევა რეალურ დროში ინფორმაციის უფრო ფართო სპექტრის შეგროვების საშუალებას.

კიბერუსაფრთხოება და მდგრადობა სამხედრო IT სისტემებში ერთ-ერთი ყველაზე კრიტიკული მიმართულებაა. ტექნოლოგიების განვითარებასთან ერთად იზრდება საფრთხეებიც, რომლებიც მიზნად ისახავს როგორც მონაცემთა მოპარვას, ისე ოპერაციების შეფერხებას. სამხედრო ინფრასტრუქტურა დაუცველია კიბერშეტევების, მავნე პროგრამების, ფიშინგის და შიდა წყაროებიდან ინფორმაციის გაჟონვის მიმართ.

დაცვის მიზნით გამოიყენება მრავალფენიანი უსაფრთხოების მიდგომა. საკომუნიკაციო არხები სრულად იზიფრება, სამხედრო პერსონალი გადის მრავალფაქტორულ ავთენტიფიკაციას, ქსელები ნაწილდება სეგმენტებად და თითოეულ მათგანს იცავს სპეციალური firewall-ები. გარდა ამისა, არსებობს წინასწარ შემუშავებული გეგმები, რომლებიც განსაზღვრავს როგორ უნდა მოხდეს რეაგირება კიბერინციდენტზე და სისტემების სწრაფი აღდგენა.

ბოლო წლებში დაფიქსირდა არაერთი მაგალითი, რაც ადასტურებს ამ საკითხის მნიშვნელობას. 2010 წელს Stuxnet-მა ირანის ბირთვული ინფრასტრუქტურა სერიოზულად

დააზიანა. 2017 წლის NotPetya-ს მასშტაბურმა შეტევამ სამხედრო ლოჯისტიკის სისტემების შეაფერხა. NATO-ს და ევროპული ქვეყნების თავდაცვის უწყებები არაერთხელ გამხდარან DDOS და ფიშინგ შეტევების სამიზნე.

ამიტომ, თანამედროვე სამხედრო IT სისტემების უსაფრთხოება ეფუძნება არა მხოლოდ ტექნოლოგიურ გადაწყვეტილებებს, არამედ მუდმივ მონიტორინგს, პერსონალის გადამზადებას და სისტემების მდგრადობის უზრუნველყოფას.

აპლიკაციები სამხედრო საინფორმაციო სისტემებში მნიშვნელოვან კონკრეტულ უპირატესობას აძლევს სამხედრო ძალებს და მათ განსაკუთრებული ადგილი უჭირავს ბრძოლის ველის შესახებ ინფორმირებულობასა და რეალურ დროში გადაწყვეტილების მიღებისას. თანამედროვე სისტემები აგროვებს ინფორმაციას სხვადასხვა წყაროდან სადაზვერვო დრონების საშუალებით, დაფარული და ადგილობრივი სენსორებიდან, სატელიტური მონაცემებიდან, შეიარაღებული ქვედანაყოფების რეპორტებიდან, რის შედეგადაც წარმოიქმნება ყოვლისმომცველი, განახლებადი სურათი ბრძოლის ველზე. ეს სიტუაციური ცნობიერება საშუალებას აძლევს ხელმძღვანელობას სწრაფად განსაზღვროს მოწინააღმდეგის პოზიციები, საფრთხეები და ხელმისაწვდომი რესურსები.

აპლიკაციები მოიცავს ასევე კონკრეტულ ოპერაციულ სფეროებს: სადაზვერვო, დაკვირვების და გადაცემა (ISR) ფუნქციებს, სადაზვერვო-ოპერატიულ ინტეგრაციას, მართვისა და კონტროლის მექანიზმებს, ლოჯისტიკური გადაწყვეტილებების ავტომატიზაციას და სამედიცინო ევაკუაციის მიმოხილვას რეალურ დროში. გარდა ოპერაციული ეფექტურობისა, ასეთი სისტემები ამცირებენ შეცდომის ალბათობასა და ოპერაციულ ხარჯებს, რადგან გადაწყვეტილებები მიღება დამოკიდებულია განახლებულ ინფორმაციაზე.

თუმცა რეალურ დროში გადაწყვეტილების მიღების სისტემებთან ერთად მნიშვნელოვან პრობლემებსაც ვხვდებით. ესენია, მონაცემების სიზუსტე და სანდოობა, საკომუნიკაციო დაყოვნება და კიბერუსაფრთხოების რისკები და სხვა. ამიტომ ეფექტური აპლიკაცია არა მხოლოდ ტექნიკურ გადაწყვეტებზე უნდა იყოს აგებული, არამედ მოითხოვს ადამიანის გაძლიერებულ კონტროლს და მკაფიო პასუხისმგებლობის მექანიზმებს.

სამხედრო საინფორმაციო-ტექნოლოგიური სისტემების განვითარებას თან ახლავს არაერთი სირთულე. მთავარი გამოწვევაა კიბერუსაფრთხოება, მოწინააღმდეგე ცდილობს მონაცემთა მოპარვას, სისტემების პარალიზებას ან დეზინფორმაციის გავრცელებას, რაც პირდაპირ მოქმედებს ბრძოლის ველის მართვის ეფექტურობაზე. სირთულეს წარმოადგენს ასევე სხვადასხვა სისტემის ინტეგრაცია. ძველი პლატფორმები ხშირად შეუსაბამოა თანამედროვე ციფრულ არქიტექტურებთან, რის გამოც ინფორმაცია გვიანდება ან იკარგება. მნიშვნელოვანია ადამიანური ფაქტორიც თანამედროვე ტექნოლოგიებთან მუშაობა საჭიროებს მაღალკვალიფიციურ კადრებს, ხოლო მათი მუდმივი გადამზადება დიდ რესურსებს მოითხოვს.

ამიტომ მნიშვნელოვანია პირველ რიგში, ერთიანი სტანდარტების შემუშავება, რათა სხვადასხვა ქვედანაყოფებს შეუფერხებლად შეძლოს მონაცემების გაზიარება. პარალელურად, აუცილებელია კიბერუსაფრთხოების მექანიზმების გაძლიერება მონაცემთა შიფრაცია, ქსელური მონიტორინგი და კიბერშეტევების პრევენციის სისტემები და სპეციალისტების რეგულარული გადამზადება, რადგან ტექნოლოგიები სწრაფად ვითარდება და მათთან ადაპტაცია მუდმივად საჭიროა.

### დასკვნა

სამხედრო IT სისტემების განვითარება მჭიდროდ იქნება დაკავშირებული ხელოვნური ინტელექტის, სენსორული ქსელების და ავტონომიური სისტემების ინტეგრაციასთან.

ბრძოლის ველზე ინფორმაციის შეგროვება და ანალიზი, რომელიც ხორციელდება რეალურ დროში, საშუალებას იძლევა არა მხოლოდ სწრაფად მოხდეს გადაწყვეტილებების მიღება, არამედ წინასწარ მოხდეს საფრთხეების პროგნოზირება.

AI, IoT და სენსორული ქსელები ქმნიან ინტელექტუალურ გარემოს, რომელიც საშუალებას აძლევს სამხედრო ხელმძღვანელობას მიიღოს ზუსტი და დროული გადაწყვეტილებები. ამ სისტემების წარმატებული დანერგვა მოითხოვს ტექნოლოგიურ ინვესტიციებს, კიბერუსაფრთხოების გაძლიერებას და ადამიანური რესურსების მუდმივ გადამზადებას. მხოლოდ ასე იქნება შესაძლებელი თანამედროვე საფრთხეებთან ეფექტური გამკლავება და ეროვნული უსაფრთხოების მდგრადი უზრუნველყოფა.

### გამოყენებული ლიტერატურა:

1. Bistrion, M., & Piotrowski, Z. Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens. *Electronics*, 10(7). 2021.
2. IEEE Communications Society. The Internet of Military Defense Things (IoMDT): State-of-the-Art and Future Directions. *IEEE Internet of Things Magazine*. 2023.
3. IEEE Xplore. Military IoT from Management to Perception: Challenges and Opportunities. 2024.
4. UNIDIR. Artificial Intelligence in the Military Domain and its Implications for International Peace and Security. 2025.
5. Journal of Global Security Studies. Digital Targeting: Artificial Intelligence, Data, and Military Decision-Making. 2024.
6. Quest Journals – JRHSS. AI in Defense: Global Perspectives on Strategic Integration and Future Challenges. 2025.

## Information and Technology Systems for Military Unit Management

Nani Arabuli<sup>1</sup>, Avtandil Migineishvili<sup>2</sup>, Mikheil Gognadze<sup>3</sup>

<sup>1</sup>Georgian Technical University

<sup>2</sup>New University

<sup>3</sup>Commander of the 3rd Infantry Brigade of the Western Command of the Georgian Defense Forces

### Summary

The success of modern military operations largely depends on the rapid collection and analysis of information. This article examines the evolution, architecture, and key components of military information and technology systems. The Network-Centric Warfare model, along with AI, IoT, and sensor networks, forms a digital framework of the battlefield that enables real-time decision-making. Strategic, operational, and tactical levels are integrated through a technological infrastructure that includes databases, GIS systems, encryption algorithms, and cybersecurity mechanisms. Autonomous systems, drones, and military robots enhance operational flexibility and reduce human risks. Applications with ISR functions and control mechanisms strengthen situational awareness. The article also discusses the existing challenges and provides recommendations for their future mitigation.

**Keywords:** Military Information Systems; Network-Centric Warfare; Artificial Intelligence (AI); Internet of Things (IoT) Technology; Sensor Networks.