Hərbi İdarəetmədə Rəqəmsal Transformasiya Və Kibertəhlükəsizlik

Elvin Qurbani
Milli Müdafiə Universiteti, Bakı, Azərbaycan
elvinqurbani.mmu@gmail.com

***Xülasə*— Tədqiqat işində müasir rəqəmsal transformasiya şəraitində hərbi idarəetmə sistemlərinin modelləşdirilməsi prinsipləri və kibertəhlükəsizlik məsələləri araşdırılmışdır. Məqalədə kritik informasiya infrastrukturlarının qorunması, süni intellektə əsaslanan qərar qəbuletməyə dəstək sistemləri və hərbi idarəetmə sistemlərində yaranan kiberdayanıqlılığın təmin olunması problemləri təhlil edilmişdir.**

Açar sözlər*— *hərbi idarəetmə, rəqəmsallaşma, modelləşdirmə, kibertəhlükəsizlik, şəbəkə-mərkəzli müharibə, süni intellekt.

I. GİRİŞ

Müasir hərbi inkişaf "Müdafiə 4.0" mərhələsinə qədəm qoymuşdur. Bu dövr dördüncü sənaye inqilabının, yəni "Sənaye 4.0" konsepsiyasının nailiyyətlərinin hərbi sahəyə tətbiqidir. Rəqəmsal texnologiyaların, süni intellektin, avtomatlaşdırılmış idarəetmə sistemlərinin, pilotsuz platformaların və şəbəkə rabitəsinin inkişafı müasir silahlı münaqişələrin təbiətini kökündən dəyişdirib. Son müharibələrin və lokal münaqişələrin təhlili göstərir ki, bu dövrün əsas xüsusiyyəti qarşıdurmanın nəticəsinin artıq getdikcə fiziki güc, silahların miqdarı və ordunun ölçüsü ilə deyil, informasiya üstünlüyü, məlumatların emal sürəti və qərar qəbuletmənin effektivliyi ilə müəyyən edilməsidir [1]. Bugünkü mühitdə informasiya əhəmiyyətinə görə silah, enerji və insan resursları ilə müqayisə edilə bilən strateji bir gücə çevrilir. Cədvəl 1-də ənənəvi və müasir rəqəmsal yanaşmalar arasındakı fərqlər, həmçinin yeni dövrün tələbləri müqayisə edilir.

CƏDVƏL I. ƏNƏNƏVİ YANAŞMA VƏ MÜASİR RƏQƏMSAL YANAŞMA ARASINDAKI FƏRQLƏR

Xüsusiyyət	Ənənəvi Yanaşma	Rəqəmsal Dövr
Əsas Güc Faktoru	Fiziki güc, silah sayı və ordunun ölçüsü.	İnformasiya üstünlüyü, məlumatın emal sürəti.
Qərar Qəbuletmə	Sərt iyerarxiya və ardıcıl əmr ötürülməsi.	Real-vaxt rejimində təhlil və sürətli reaksiya.
Texnoloji Fokus	Mexaniki silahlar və insan resursları.	Sİ, pilotsuz platformalar, bulud texnologiyaları.
Əsas Resurs	Yanacaq, sursat və canlı qüvvə.	İnformasiya və rəqəmsal infrastruktur.
Koordinasiya	Bölmələr arası statik əlaqə.	Bütün qoşun növləri arasında davamlı rəqəmsal əlaqə.

Rəqəmsal transformasiya hərbi idarəetmədə qərar qəbuletmə müddətini əhəmiyyətli dərəcədə azaldır. Ağıllı sistemlərin inteqrasiyası sayəsində idarəetmə sistemi əməliyyat vəziyyətini real-vaxt rejimində təhlil edə, müxtəlif bölmələrin hərəkətlərini tez bir zamanda əlaqələndirə və ortaya çıxan təhdidlərə dərhal reaksiya verə bilir. Nəticədə, ordunun əməliyyat çevikliyi və operativliyi əhəmiyyətli dərəcədə artır. Eyni zamanda, rəqəmsal texnologiyaların aktiv tətbiqi silahlı qüvvələri yeni, görünməz təhdidlərin, yəni (nəticələri ənənəvi hərbi zərbələrdən az dağıdıcı olmayan) kibertəhdidlərin mərkəzinə çəkir.

Bu gün kiberməkan quru, dəniz və hava ilə yanaşı, tam hüquqlu müharibə növü hesab olunur. Müasir ordular getdikcə informasiya sistemlərindən, şəbəkə rabitəsindən, peyk naviqasiyasından, bulud texnologiyalarından və avtomatlaşdırılmış idarəetmə mərkəzlərindən asılıdır. Bu, ciddi risklər yaradır, çünki rəqəmsal infrastrukturdakı hər hansı bir zəiflik düşmən tərəfindən rabitəni pozmaq, idarəetməni və nəzarəti pozmaq, məlumatları təhrif etmək və ya kritik hərbi sistemləri tamamilə sıradan çıxarmaq üçün istifadə edilə bilər. Beləliklə, ordunun rəqəmsal asılılığı eyni zamanda həm üstünlük, həm də potensial zəifliyə (təhlükəyə) çevrilir.

II. HƏRBİ İDARƏETMƏNİN RƏQƏMSALLAŞDIRILMASI ZƏRURƏTİ

Hərbi idarəetmə və nəzarət sistemlərinin rəqəmsallaşdırılması artıq alternativ inkişaf istiqaməti deyil, milli təhlükəsizliyin təmin edilməsi üçün zəruri şərtdir. Ciddi iyerarxiya və statik struktur üzərində qurulmuş ənənəvi idarəetmə modellərindən fərqli olaraq, müasir hərbi əməliyyatlar çeviklik, uyğunlaşma və yüksək cavabdehlik tələb edir. Klassik idarəetmə və idarəetmə sistemləri tez-tez sürətlə dəyişən mühitlərdə effektiv fəaliyyət göstərə bilmir.

Müasir silahlı qüvvələr şəbəkə texnologiyalarından, avtomatlaşdırılmış məlumatların təhlili sistemlərindən və ağıllı idarəetmə və nəzarət platformalarından istifadə etmədən effektiv fəaliyyət göstərə bilməz. Lakin bu transformasiya zamanı kibertəhlükəsizlik məsələləri ikinci dərəcəli hesab olunarsa, ordu düşmənin ən həssas hədəfinə çevrilə bilər. İnformasiya axını pozularsa və ya rəqəmsal infrastruktur təhlükəyə məruz qalarsa, hətta yüksək texnologiyalı silahlar belə effektivliyini itirir.

Müasir münaqişələrdə kompüter şəbəkələrini və texniki sistemləri qorumaqla kifayətlənmək mümkün deyil. Ötürülən məlumatların təhlükəsizliyini, onun məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək eyni dərəcədə vacib bir vəzifəyə çevrilir [2]. Məlumatın tutulması, dəyişdirilməsi və ya təhrif edilməsi səhv idarəetmə qərarlarına, bölmələr arasında koordinasiyanın pozulmasına və döyüş meydanında kritik vəziyyətlərin yaranmasına səbəb ola bilər. Bu səbəbdən informasiya təhlükəsizliyi yalnız qorunmanın texniki

DOI: 10.25045/forensic.gov.2026.70

aspektlərini deyil, həm də təşkilati, kriptoqrafik və strateji aspektləri əhatə etməlidir.

Buna görə də, müasir hərbi sistemləri layihələndirərkən və modelləşdirərkən təhlükəsizlik arxitekturası inkişaf tamamlandıqdan sonra tətbiq edilmək əvəzinə, sistemin özü ilə eyni vaxtda yaradılmalıdır. Bu yanaşma, təhlükəsizlik mexanizmlərinin sistemə həyat dövrünün bütün mərhələlərində inteqrasiya olunduğu "Təhlükəsizlik dizayn mərhələsindən" (Security by Design) prinsipinə uyğundur. Bu prinsipin tətbiqi dizayn mərhələsindəki zəiflikləri minimuma endirir, infrastrukturun kiberhücumlara qarşı dayanıqlığını artırır və aktiv informasiya müharibəsi şəraitində belə hərbi sistemlərin davamlı işləməsini təmin edir.

Müasir hərbi elmdə uzaqdan idarə olunan ağıllı texnologiyaların istifadəsi xüsusi rol oynayır. Pilotsuz uçuş aparatlarının, robot sistemlərinin, elektron müşahidə sistemlərinin və süni intellekt elementlərinin istifadəsi daimi məlumat mübadiləsi və real-vaxt rejimində məlumatların emalı tələb edir. Bu cür sistemlərin effektiv işləməsi üçün ordunun bütün qoşun növləri arasında davamlı rəqəmsal koordinasiya tələb olunur. Məlumat ötürülməsində və ya rabitədə hər hansı bir gecikmə əməliyyatın nəticəsinə mənfi təsir göstərə və taktiki üstünlüyün itirilməsinə səbəb ola bilər.

III. Hərbi İdarəetmə Sistemlərinin Modelləşdirilməsi və İnteqrasiyası

Sürətli rəqəmsal transformasiya kontekstində hərbi sektorda intellektual informasiya texnologiyalarının, avtomatlaşdırılmış idarəetmə sistemlərinin və şəbəkə qarşılıqlı əlaqə platformalarının tətbiqi ilə bağlı fundamental dəyişikliklər baş verir. Müasir hərbi idarəetmə modeli artıq ənənəvi idarəetmə və nəzarət sistemi ilə məhdudlaşmır. Bu gün o, vahid informasiya məkanında fəaliyyət göstərən bir-biri ilə əlaqəli rəqəmsal, informasiya və təşkilati komponentlərin mürəkkəb sistemini təşkil edir. Buna görə də, hərbi idarəetmə sistemlərinin modelləşdirilməsi və inteqrasiyası milli təhlükəsizliyin və müdafiə qabiliyyətinin təmin edilməsində əsas vəzifəyə çevrilir.

Rəqəmsal transformasiya kontekstində müasir hərbi idarəetmə modeli idarəetmənin davamlılığını, davamlı rabitəni, əməliyyat məlumatlarının emalını və silahlı qüvvələrin koordinasiyasını təmin edən bir neçə vacib elementin birləşməsi kimi qəbul edilməlidir. Beynəlxalq təcrübədə bu cür sistemlərin əsasını C4ISR (Komanda, Nəzarət, Rabitə, Kompüterlər, Kəşfiyyat, Müşahidə və Kəşfiyyat) sistemləri təşkil edir. Bu konsepsiya rabitə, hesablama texnologiyaları, kəşfiyyat platformaları və məlumatların təhlili alətlərini vahid hərbi əməliyyatların idarəetmə şəbəkəsinə birləşdirən inteqrasiya olunmuş bir sistemdir.

C4ISR müasir müdafiə sistemlərində əsas rol oynayır və dövlətlərin, hərbi strukturların, kritik infrastruktur müəssisələrinin və bütövlükdə cəmiyyətin əməliyyat sabitliyini təmin edir. Şəbəkə texnologiyalarından və avtomatlaşdırılmış informasiya emalından istifadə etməklə hərbi idarəetmə müxtəlif mənbələrdən real-vaxt rejimində alınan müvafiq məlumatlara əsasən qərarlar qəbul edə bilir. Bu, təhdidlərə cavab sürətini əhəmiyyətli dərəcədə artırır, hədəf aşkarlanması ilə qərar qəbuletmə arasındakı vaxtı azaldır və bölmələr arasında daha dəqiq koordinasiyanı təmin edir [3].

Dünya ölkələri hazırda C4ISR-də texnoloji üstünlük uğrunda fəal şəkildə mübarizə aparırlar, çünki bu sahədə liderlik strateji milli üstünlük kimi qəbul edilir. Hərbi idarəetmə və idarəetmə sistemlərində innovasiyaları effektiv şəkildə tətbiq edə bilən dövlətlər informasiya məkanına hakim ola və yüksək səviyyədə müdafiə qabiliyyətini təmin edə bilirlər. Müasir müharibədə qələbə getdikcə silahların miqdarı ilə deyil, məlumatları tez bir zamanda əldə etmək, təhlil etmək və istifadə etmək qabiliyyəti ilə müəyyən edilir.

Şəbəkə əsaslı yanaşma müasir hərbi idarəetmə sistemlərində xüsusi əhəmiyyət kəsb edir. Şəkil 1-də onun əsas ideyası təsvir edilmişdir bütün hərbi bölmələri orqanizmin "sinir sistemi" kimi fəaliyyət göstərən vahid informasiya şəbəkəsinə birləşməsini izah edir.

Təqdim edilən model daxilində hərbiçilər, pilotsuz uçuş aparatları, raket buraxıcıları, peyk müşahidə sistemləri və komanda mərkəzləri vahid rəqəmsal məkanın elementləri kimi fəaliyyət göstərir. Bu, ani məlumat mübadiləsini, sinxronlaşdırılmış hərəkətləri və artan əməliyyat səmərəliliyini təmin edir.

Şəkil 1. Şəbəkə əsaslı hərbi idarəetmə və qarşılıqlı əlaqə modeli

Şəbəkə əsaslı idarəetmə və idarəetmə modeli ciddi iyerarxiyaya və ardıcıl əmr ötürülməsinə əsaslanan ənənəvi hərbi strukturlardan əhəmiyyətli dərəcədə fərqlənir. Bugünkü döyüş mühitində hərbi əməliyyatların dinamikası yüksək reaksiya sürəti, uyğunlaşma və fərdi bölmələrin əlahiddə olmasını tələb edir. Məlumat gecikmədən alınmalı və qərarlar mümkün qədər tez qəbul edilməlidir. Məhz buna görə də rəqəmsal şəbəkələr və ağıllı sistemlər müasir hərbi arxitekturanın təməlinə çevrilir.

Rəqəmsal sistemlərin idarə olunmasında klassik hərbi iyerarxiya texnoloji iyerarxiya ilə tamamlanmalıdır. Əvvəllər əsas diqqət komandirlər və bölmələr arasında idarəetmə səlahiyyətlərinin bölüşdürülməsinə yönəlmişdisə, bu gün informasiya təhlükəsizliyi mütəxəssisləri, məlumat analitikləri, şəbəkə infrastrukturu administratorları və rəqəmsal platforma operatorları da mühüm rol oynayırlar. Müasir idarəetmə modelləri təşkilati və texnoloji mexanizmlərin vahid sistemə inteqrasiyasını tələb edir.

Beynəlxalq təcrübədə COBIT 5 və ISO 27001 kimi informasiya idarəetməsi və kibertəhlükəsizlik standartlarından geniş istifadə olunur. Bu standartlar informasiya resurslarının idarə edilməsi, risklərin qiymətləndirilməsi və kritik infrastrukturun qorunması üçün sistemli bir yanaşma təmin edir. Onların hərbi təşkilatlarda tətbiqi informasiya təhlükəsizliyinin

idarə edilməsi proseslərinin rəsmiləşdirilməsinə, personalın məsuliyyətlərinin müəyyən edilməsinə və rəqəmsal mühitin xarici təsirlərə qarşı dayanıqlığının artırılmasına imkan verir [4].

Silahlı qüvvələrin rəqəmsal strukturunda CISO (Baş İnformasiya Təhlükəsizliyi Zabiti) və SOC (Təhlükəsizlik Əməliyyatları Mərkəzi) kimi elementlər xüsusi rol oynayır. Bu cür strukturların mövcudluğu informasiya riskləri üzərində mərkəzləşdirilmiş nəzarəti, şəbəkə fəaliyyətinin monitorinqini və kiber insidentlərin vaxtında aşkarlanmasını təmin edir. Bundan əlavə, hərbi təşkilatın hər bir zabiti və işçisi rəqəmsal məsuliyyətlərini başa düşməli və informasiya ilə işləyərkən kibertəhlükəsizlik tələblərinə riayət etməlidir.

Ordunun rəqəmsal transformasiyası kontekstində kibertəhlükəsizliyin əhəmiyyəti əsas prioritetlərdən biridir. 2026-cı il kiberhücumların artıq yalnız məlumatları hədəf almadığı, əksinə, kritik infrastrukturu, vacib xidmətləri, eləcə də qlobal təchizat zəncirlərini getdikcə daha çox təhlükə altına aldığı kritik bir məqama çatır. Bu zəifliklər hibrid təhdidlər və xarici texnologiyalardan artan geosiyasi asılılıqlarla daha da artır [5]. Müasir hərbi idarəetmə və nəzarət sistemləri getdikcə daha çox şəbəkələşdiyindən potensial zəiflik nöqtələrinin sayını əhəmiyyətli dərəcədə artır. Hərbi rabitə, GPS peyk sistemləri, enerji şəbəkələri, logistika bazaları, bulud platformaları və avtomatlaşdırılmış idarəetmə mərkəzləri vahid kiber informasiya sisteminin (CIS) bir hissəsidir. Hətta bir elementdəki pozuntu bütün hərbi infrastruktur üçün ciddi nəticələrə səbəb ola bilər. Kiberhücum hərbi rabitəni pozarsa, naviqasiya sistemlərini sıradan çıxararsa və ya məlumat ötürmə kanallarını bloklayarsa, hətta ən qabaqcıl silahlar belə yararsız hala düşə bilər. Rəqəmsal müharibədə silahların effektivliyi birbaşa informasiya mühitinin sabitliyindən asılıdır. Müasir raketlər, dronlar və idarəetmə sistemləri proqram təminatı və rəqəmsal rabitə vasitələrindən istifadə edərək işləyir, buna görə də onların iş prinsipi kibertəhlükəsizlik səviyyəsindən çox asılıdır.

Rəqəmsal transformasiya mühitində Qabaqcıl Davamlı Təhdidlər (APT) kiberhücumları xüsusi bir təhlükə yaradır. Ənənəvi viruslardan və ya kütləvi hücumlardan fərqli olaraq, APT hücumları yüksək dərəcədə gizlilik, sistemdə uzunmüddətli mövcudluq və dəqiqlik ilə xarakterizə olunur. Hücumçular illərlə infrastruktur daxilində aşkarlanmadan, məlumat toplayaraq, sistem arxitekturasını öyrənərək və hücum üçün şərait hazırlayaraq qala bilərlər [6]. Kritik anda bu cür mexanizmlər rabitəni pozmaq, komandanlığı və nəzarəti pozmaq və ya strateji əhəmiyyətli obyektləri sıradan çıxarmaq üçün aktivləşdirilə bilər.

APT təhdidlərinin təhlükəsi həm də onların müasir təhlükəsizlik alətləri ilə belə çətin aşkarlanmasıdır. Bu, şəbəkə fəaliyyətinin daimi monitorinqini, istifadəçi davranışının təhlili sistemlərinin istifadəsini və rəqəmsal infrastrukturdakı anomaliyaları aşkar etmək üçün süni intellekt texnologiyalarından istifadəni tələb edir.

Hərbi idarəetmə və nəzarətdə yalnız məlumatın məxfiliyi deyil, həm də onun bütövlüyü vacibdir. Hakerlər məlumatların kiçik bir hissəsini belə dəyişdirə bilirlərsə, bu, fəlakətli nəticələrə səbəb ola bilər. Hədəf koordinatlarını təhrif etmək, nəqliyyat vasitələrinin marşrutlarını dəyişdirmək, kəşfiyyat məlumatlarını saxtalaşdırmaq və ya yalan məlumatların yayılması idarəetmə və idarəetmə sisteminə xələl gətirə və əməliyyatın uğursuzluğuna səbəb ola bilər.

Rəqəmsal mühitdə dezinformasiya müasir müharibənin ən təhlükəli vasitələrindən birinə çevrilir. İnformasiya manipulyasiyası təkcə texniki sistemlərə deyil, həm də hərbi qulluqçuların, komandirlərin və mülki əhalinin psixoloji vəziyyətinə təsir göstərə bilər. Buna görə də, kibertəhlükəsizlik yalnız şəbəkələri və serverləri qorumaqla yanaşı, ötürülən məlumatların həqiqiliyini də təmin etməlidir.

Süni intellekt (Sİ) texnologiyalarının hərbi sahəyə aktiv inteqrasiyası əlavə mürəkkəblik yaradır. Sİ rəqəmsal ordu üçün bir növ "beyin"ə çevrilir və məlumatların təhlili, avtomatlaşdırılmış qərar qəbuletmə, təhdidlərin proqnozlaşdırılması və muxtar sistemlərin idarə olunması kimi funksiyaları yerinə yetirir. Bununla belə, Sİ özü də hücum hədəfinə və potensial zəifliyə çevrilir.

Ən təhlükəli təhdidlərdən biri "zəhərlənmiş məlumatlar"dır. Bu halda, hücum edənlər qəsdən maşın öyrənmə alqoritmlərinin təlim nümunələrinə yalan və ya təhrif olunmuş məlumatlar daxil edirlər. Nəticədə, Sİ səhv qərarlar qəbul etməyə başlayır: düşmən hədəflərini tanımır, dost qüvvələri səhvən təhdid kimi müəyyən edir və ya əməliyyat vəziyyətini səhv təhlil edir. Bu cür manipulyasiyalar real döyüş vəziyyətlərində ağır nəticələrə səbəb ola bilər.

Beləliklə, kibertəhlükəsizlik problemi proqram təminatı və şəbəkə infrastrukturunun ənənəvi qorunmasından daha geniş anlayış olması fikri bir daha öz təsdiqini tapır. O, strateji kəşfiyyat, hərbi planlaşdırma və milli təhlükəsizlik səviyyəsinə yüksəlir. Müasir ordu təkcə fiziki qarşıdurmaya deyil, həm də informasiya və kiberməkanda müharibəyə hazır olmalıdır.

Rəqəmsal dövrdə hərbi idarəetmə və nəzarət sistemlərinin modelləşdirilməsi bir çox amili nəzərə almalıdır: şəbəkə arxitekturasının dayanıqlığı, rabitə kanallarının qorunması, süni intellektin təhlükəsizliyi, məlumatların saxlanmasının etibarlılığı və sistemin qismən infrastruktur pozuntusu ilə belə işləmə qabiliyyəti. Bu, texnoloji, təşkilati və strateji təhlükəsizlik tədbirlərini birləşdirən hərtərəfli yanaşma tələb edir.

Buna görə də, müasir informasiya texnologiyalarının hərbi sahəyə inteqrasiyası kibertəhlükəsizlik mexanizmlərinin eyni vaxtda inkişaf etdirilməsini tələb edir. Yalnız etibarlı təhlükəsizlik sistemi ilə rəqəmsal transformasiya ordunun effektivliyini artıra, idarəetmə və nəzarətin sabitliyini təmin edə və müasir münaqişələrdə dövlətin strateji üstünlüyünü qoruya bilər.

IV. Azərbaycanın Milli Kibertəhlükəsizlik Ekosistemi – Həlli Yolları və Sintez

Azərbaycan rəqəmsal transformasiya yolunda həm hərbi, həm də mülki sektorda güclü kiber-qalxan formalaşdırır.

Prezident İlham Əliyevin təsdiqlədiyi "İnformasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası" ölkənin rəqəmsal gələcəyinin yol xəritəsidir. Strategiya Kritik informasiya infrastrukturu (Kİİ) obyektlərində təhlükəsizlik risklərinin daim müəyyənləşdirilməsini və xaricdən texnoloji asılılığın

minimuma endirilməsini hədəfləyir [7].

Dövlət Təhlükəsizliyi Xidmətinin (DTX) nəzdində yaradılmış Milli Kibermərkəz və Kibertəhlükəsizlik Əməliyyatları Mərkəzi ölkənin strateji sistemlərinə real-vaxt rejimində mərkəzləşmiş nəzarəti həyata keçirir [8]. Gələcəkdə ölkənin bütün kritik informasiya sistemlərində müasir arxitektura və topologiya formalaşdırılması nəzərdə tutulur ki, bu da hərbi idarəetmənin dayanıqlılığını artıracaqdır.

Artıq ölkədə kritik informasiya infrastrukturu obyektlərinin reyestri yaradılmışdır. Reyestrin operatoru olan Milli Kibermərkəz bu sistemlərə dair həm ümumi, həm də xüsusi təhlükəsizlik tələblərini müəyyən edir [9]. Bu, hərbi idarəetmə sistemlərinin modelləşdirilməsində vahid dövlət standartlarının tətbiqinə imkan verir.

Kiberdayanıqlı hərbi idarəetmə sistemi üçün müdafiə strategiyası çoxlaylı və dərindən müdafiə prinsiplərinə əsaslanaraq, şəbəkədən tutmuş tətbiq kodlarına qədər bütün səviyyələri əhatə etməlidir. Bu sistemin səmərəliliyi üçün hərbi personalın kiber-məkanın riskləri barədə məlumatlandırılması, kiber-mədəniyyətin formalaşdırılması şərtdir [10]. Eyni zamanda, hərbi qurğuları idarə edən SCADA sistemləri üçün xüsusi izolyasiya edilmiş şəbəkələr (air-gapping) və zədəli kodların aşkarlanması üçün dinamik analiz metodları tətbiq olunmalıdır. Xarici texnoloji asılılığın aradan qaldırılması məqsədilə yerli məhsulların yaradılması və onların laboratoriya şəraitində sınaqdan keçirilməsi prioritet olmalıdır.

Bundan əlavə, milli kibertəhlükəsizlik ekosisteminin effektiv fəaliyyəti üçün dövlət–özəl sektor əməkdaşlığının gücləndirilməsi xüsusi əhəmiyyət daşıyır. Müasir dövrdə kibertəhdidlər yalnız dövlət qurumlarını deyil, enerji, nəqliyyat, rabitə, bank və digər strateji sahələri də əhatə etdiyindən təhlükəsizlik tədbirlərinin vahid koordinasiya altında həyata keçirilməsi vacibdir. Çünki, 2019-cu ildən bəri mövcud və ortaya çıxan təhdidlərin ümumi dəsti xeyli dəyişib. Müasir hücumlar tez-tez həyati əhəmiyyətli əməliyyatları və sənaye şəbəkələrini pozur və sərhədlərarası koordinasiyada struktur qüsurları aşkar edir. Bu məqsədlə informasiya mübadiləsi mexanizmlərinin yaradılması, milli kiber mərkəzlərin imkanlarının genişləndirilməsi, həmçinin dövlət qurumları ilə özəl şirkətlər arasında operativ məlumat paylaşımının təmin olunması zəruridir.

Eyni zamanda informasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin formalaşdırılması kompleks təşkilati prosesdir. Bu proses əməkdaşlarda təhlükəsiz davranış vərdişlərinin, zəruri bilik və bacarıqların formalaşdırılmasını, təhlükəsizlik qaydalarına əməl edilməsini və insidentlərə düzgün reaksiya verilməsini əhatə edir. İnformasiya texnologiyalarının sürətli inkişafı kibertəhlükəsizlik üzrə maarifləndirmə tədbirlərinin davamlı şəkildə yenilənməsini və müasir təhdidlərə uyğunlaşdırılmasını zəruri edir [7].

Belə inteqrasiya olunmuş yanaşma kibercinayətkarlıq, hibrid təhdidlər və dövlət səviyyəli kiberhücumlara qarşı daha çevik müdafiə sisteminin formalaşdırılmasına şərait yaradır.

Eyni zamanda, süni intellekt və böyük verilənlər (Big Data) texnologiyalarının kibertəhlükəsizlik sahəsində tətbiqi gələcək hərbi idarəetmə sistemlərinin əsas istiqamətlərindən biri hesab olunur. Süni intellekt əsaslı təhlükə aşkarlama sistemləri müasir kibertəhlükəsizlikdə həlledici rol oynayır. Onlar maşın təlimi və dərin təlim alqoritmlərindən istifadə edərək milyonlarla hadisəni bir neçə millisaniyə ərzində təhlil edir, bu da ənənəvi alətlərlə müqayisədə təhdidləri yüz dəfələrlə daha sürətli müəyyən etməyə imkan verir. Bu texnologiyalar xüsusilə hərbi əməliyyatların idarə edilməsində qərar qəbuletmə sürətini artırır və insan faktorundan yaranan riskləri minimuma endirir. Bununla yanaşı, süni intellekt sistemlərinin özlərinin də kiberhücum hədəfinə çevrilməsi ehtimalı nəzərə alınmalı, onların təhlükəsizlik auditləri və etibarlılıq testləri mütəmadi şəkildə aparılmalıdır.

Milli kibertəhlükəsizlik potensialının gücləndirilməsində insan kapitalının inkişafı da mühüm rol oynayır. Ali təhsil müəssisələrində kibertəhlükəsizlik ixtisaslarının genişləndirilməsi, hərbi təhsil sistemində kiberəməliyyatlara dair xüsusi hazırlıq proqramlarının tətbiqi və beynəlxalq təcrübənin öyrənilməsi ölkənin müdafiə qabiliyyətinin artırılmasına xidmət edir. Xüsusilə kiberməkan üzrə yüksək ixtisaslı mütəxəssislərin hazırlanması, milli proqram təminatı və kriptoqrafik həllərin yaradılması Azərbaycanın rəqəmsal suverenliyinin təmin olunması baxımından strateji əhəmiyyət daşıyır.

Beləliklə, Azərbaycanın milli kibertəhlükəsizlik ekosistemi yalnız texnoloji müdafiə vasitələrinin inkişafı ilə deyil, həm də institusional idarəetmə, insan resurslarının hazırlanması və yerli innovasiya potensialının gücləndirilməsi ilə kompleks şəkildə formalaşdırılır. Bu yanaşma gələcəkdə rəqəmsal transformasiya şəraitində dayanıqlı və təhlükəsiz hərbi idarəetmə modelinin qurulmasına mühüm zəmin yaradır.

NƏTİCƏ

21-ci əsrdə rəqəmsal transformasiya silahlı qüvvələrin inkişafının əsas istiqamətlərindən birinə çevrilmişdir. Süni intellekt, avtomatlaşdırılmış idarəetmə sistemləri, şəbəkə texnologiyaları və böyük verilənlərin tətbiqi hərbi idarəetmədə qərar qəbuletmə sürətini artırır, əməliyyat koordinasiyasını gücləndirir və informasiya üstünlüyünün əldə olunmasına şərait yaradır. Müasir hərbi əməliyyatlarda uğur artıq yalnız fiziki resurslarla deyil, məlumatın emal sürəti, operativ informasiya mübadiləsi və rəqəmsal sistemlərin dayanıqlılığı ilə müəyyən olunur. Bu baxımdan, rəqəmsal texnologiyalar müasir ordunun əsas strateji komponentinə çevrilmişdir.

Lakin rəqəmsallaşmanın genişlənməsi ilə kibertəhdidlərin miqyası da artır. Hərbi rabitə sistemlərinin sıradan çıxarılması, məlumatların saxtalaşdırılması, SCADA və C4ISR infrastrukturlarına müdaxilə, eləcə də süni intellekt alqoritmlərinin manipulyasiyası dövlətin milli təhlükəsizliyi üçün ciddi risklər yaradır. Müasir müharibələrdə kiberməkan artıq ənənəvi döyüş meydanı ilə paralel fəaliyyət göstərən strateji qarşıdurma sahəsinə çevrilmişdir. Buna görə də kibertəhlükəsizlik hərbi idarəetmənin əlavə texniki elementi deyil, onun əsas dayaqlarından biri kimi qiymətləndirilməlidir.

Tədqiqat göstərir ki, rəqəmsal hərbi idarəetmə sistemlərinin effektiv fəaliyyəti "Təhlükəsizlik dizayn mərhələsindən" prinsipinin tətbiqindən, çoxlaylı müdafiə mexanizmlərinin qurulmasından və kritik informasiya infrastrukturunun davamlı monitorinqindən birbaşa asılıdır. Şəbəkələrin seqmentləşdirilməsi, air-gapping yanaşmaları, dinamik analiz

metodları və süni intellekt əsaslı təhlükə aşkarlama sistemləri müasir ordunun kiberdayanıqlılığının təmin edilməsində mühüm rol oynayır. Eyni zamanda, insan amili təhlükəsizliyin ən həssas nöqtələrindən biri olaraq qalır. Buna görə də hərbi personalın kibertəhlükəsizlik üzrə davamlı təlimlərə cəlb olunması, kiber-mədəniyyətin formalaşdırılması və yüksək ixtisaslı mütəxəssislərin hazırlanması xüsusi əhəmiyyət daşıyır.

Azərbaycanın milli kibertəhlükəsizlik strategiyası və Milli Kibermərkəzin fəaliyyəti ölkədə vahid rəqəmsal təhlükəsizlik ekosisteminin formalaşdırılması istiqamətində mühüm addımdır. Yerli texnologiyaların inkişafı, milli proqram təminatı və kriptoqrafik həllərin yaradılması rəqəmsal suverenliyin təmin olunmasına xidmət edir. Beləliklə, müasir rəqəmsal ordu yalnız texnoloji üstünlüklə deyil, həm də güclü kibertəhlükəsizlik infrastrukturu, peşəkar insan resursları və dayanıqlı idarəetmə modeli ilə formalaşır. Bu yanaşma Azərbaycan Ordusunun həm fiziki döyüş meydanında, həm də kiberməkanda strateji üstünlüyünü təmin edən əsas amillərdən biri kimi çıxış edir.

ƏDƏBİYYAT

[1] "Məlumatlar Atəş Gücü Kimi: Məlumat Üstünlüyünün Müharibə Konsepsiyası Kimi Araşdırılması" https://smallwarsjournal.com/2025/08/15/data-superiority-modern-warfare/

[2] Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası. "İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi aspektləri" fənni üzrə mühazirələr toplusu. Bakı, 2024.

[3] C4ISR rəhbərliyi ilə missiyanın irəliləməsi. https://www.baesystems.com/en-us/who-we-are/electronic-systems/

[4] "İnformasiya Təhlükəsizliyi Rolları və İdarəetmə İerarxiyası (COBIT 5 təhlili)", Azad Məmmədov, 2022.

[5] "Avropa Birliyi Kibertəhlükəsizlik Agentliyi" -nin (ENISA) 2026-ci il üçün təklif etdiyi Kibertəhlükəsizlik Qanunu. https://www.ga-alliance.eu/en/eu-cybersecurity-act-proposal/

[6] Advanced Persistent Threats (Qabaqcıl Davamlı Təhdid Qrupları) https://cert.az/news/2024/etx-advanced-persistent-threats

[7] Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası. (Sərəncam № 4060, 28 avqust 2023).

[8] "Haqqımızda: Milli Kibermərkəzin fəaliyyət istiqamətləri", DTX rəsmi bülleteni, 2023.

[9] "Kritik informasiya infrastrukturu obyektləri yeni növ kiberhücumların əsas hədəflərindədir", NCSC elmi məqaləsi, mart 2025.

[10] Mahmudova R.Ş., "Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində beynəlxalq təcrübənin analizi", İnformasiya cəmiyyəti problemləri, 2022, №1.

Digital transformation and Cybersecurity in Military Management

Elvin Qurbani
National Defense University, Baku, Azerbaijan
elvinqurbani.mmu@gmail.com

Abstract - This study investigates the principles of modeling military management systems and the associated cybersecurity challenges in the context of modern digital transformation. The paper analyzes issues related to the protection of critical information infrastructures, artificial intelligence-based decision support systems, and the provision of cyber resilience in military management systems.

Keywords - digital transformation; military education; distance learning; management; artificial intelligence; simulation.