Artilleriya Sistemlərinin Rəqəmsal Kriminalistika Əsasında Effektiv İdarə Olunması

Yaşar Hüseynov
Milli Müdafiə Universiteti, Naxçıvan Hərbi Kolleci, Naxçıvan, Azərbaycan
yasar.huseynov@mmu.edu.az

***Xülasə*— Müasir artilleriya sistemlərinin effektiv idarə olunması üçün təkcə atəş gücü deyil, həm də rəqəmsal təhlükəsizlik və əməliyyat şəffaflığı vacibdir. Rəqəmsal kriminalistika loq fayllarının təhlili, icazəsiz əmrlərin aşkarlanması və sistem bütövlüyünün auditi vasitəsilə bu sahədə effektiv həll yolu təklif edir. Tətbiq olunan metodlar sayəsində həm hadisələrdən sonra dəqiq araşdırma, həm də real-vaxt rejimində anomaliyaların qarşısının alınması mümkün olur. Nəticədə, rəqəmsal kriminalistika əsasında qurulan idarəetmə modeli artilleriya bölmələrinin döyüş hazırlığını və kiber dayanıqlığını əhəmiyyətli dərəcədə artırır.**

***Açar sözlər*— *rəqəmsal kriminalistika; artilleriya sistemləri; loq analizi; icazəsiz əmrlər; sistem auditi; kibertəhlükəsizlik*.**

I. GİRİŞ

Müasir artilleriya sistemlərinin döyüş effektivliyi onların avtomatlaşdırılmış idarəetmə sistemləri, sensor şəbəkələri və dəqiq naviqasiya modulları ilə inteqrasiya dərəcəsi ilə birbaşa bağlıdır. Bu rəqəmsal transformasiya artilleriya bölmələrinə daha yüksək sürət, dəqiqlik və məhv etmə qabiliyyəti təmin etsə də, eyni zamanda yeni təhlükəsizlik boşluqları və idarəetmə çağırışları yaradır.

Ənənəvi artilleriya idarəetmə strategiyaları adətən döyüş taktikası, atəş planlaması və fiziki təhlükəsizlik üzərində cəmləşmişdir. Lakin süni intellekt və avtomatlaşdırılmış qərar qəbuletmə sistemlərinin artması ilə rəqəmsal infrastrukturun özü də bir döyüş meydanına çevrilmişdir.

Son illərdə rəqəmsal kriminalistika, informasiya təhlükəsizliyi və hadisələrə cavab tədbirləri sahəsində əldə edilən nailiyyətlər bu metodların hərbi sistemlərə tətbiqinin zəruriliyini ortaya qoymuşdur. Artilleriya sistemlərində yaranan loq faylları, sensor məlumatları və potensial kiber hücumları, proqram səhvlərini və ya daxili sui-istifadə hallarını aşkar etmək üçün qiymətli rəqəmsal sübutlar kimi çıxış edir.

Belə bir kontekstdə rəqəmsal kriminalistika metodlarının artilleriya sistemlərinin effektiv idarə olunmasına inteqrasiyası təkcə texniki bir yenilik deyil, həm də əməliyyat təhlükəsizliyi və döyüş hazırlığı üçün strateji zərurətdir.

Bu məqalədə rəqəmsal kriminalistikanın əsas prinsipləri ilə artilleriyanın idarəetmə proseslərinin sintezi araşdırılacaq. Real-vaxt rejimində anomaliyaların aşkarlanması, sistem bütövlüyünün yoxlanılması və hadisələrdən sonra dəqiq araşdırma mexanizmlərinin təmin edilməsi yolları təhlil ediləcəkdir.

II. ARTİLLERİYA SİSTEMLƏRİNDƏ RƏQƏMSAL İZLƏR VƏ LOQ FAYLLARIN STRUKTURU

Müasir artilleriya sistemləri, özüyeriyən artilleriya qurğuları (ÖAQ), yaylım atəşli reaktiv sistemlər (YARS) və əks-artilleriya radar stansiyaları daxil olmaqla, getdikcə daha çox rəqəmsal idarəetmə blokları, sensor inteqrasiyası və şəbəkə mərkəzli əlaqə protokolları ilə təchiz edilir [1]. Bu sistemlərin gündəlik əməliyyatları nəticəsində çoxsaylı rəqəmsal izlər, avtomatik qeydə alınan loq faylları yaranır. Rəqəmsal kriminalistika baxımından bu loq faylları hadisə sonrası araşdırmalar, anomaliyaların aşkarlanması və sistem bütövlüyünün təsdiqlənməsi üçün əsas sübut mənbəyidir.

Artilleriya sistemlərində rast gəlinən loq faylları funksional olaraq dörd əsas kateqoriyaya bölünür:

- əmr loqları (atəş əmrləri, hədəflərin koordinatları, istifadəçi ID),
- sensor loqları (radarlar, termal kameralar və akustik mənbələrdən əldə olunan məlumatlar),
- sistem loqları (əməliyyat sistemi hadisələri, xəta mesajları)
- şəbəkə loqları (IP trafiki, komanda-nəzarət kanalları).

Bu loq növlərinin hər biri həm real-vaxt rejimində monitorinq, həm də hadisə sonrası dəlillərin analizi üçün potensial sübutlar daşıyır [2].

Loq faylları adətən vaxt nişanı (timestamp), mənbə identifikatoru (source ID), hadisə tipi (event type) və məlumat sahəsi (data field) olmaqla dörd əsas komponentdən ibarət standart quruluşa malikdir. Kriminalistika baxımından ən kritik məqam vaxt nişanlarının dəqiqliyi və mənbə identifikatorlarının dəyişməzliyidir. Vaxt sinxronlaşdırılması pozulmuş sistemlərdə hadisələrin ardıcıllığını bərpa etmək çətinləşir və sübutların etibarlılığı sual altına düşür ki, bu da öz növbəsində rəqəmsal dəlillərin əsas prinsiplərindən biridir.

Praktikada loq toplanması bir sıra çətinliklərlə üzləşir:

- yüksək intensivlikli atəş dövrlərində böyük məlumat həcmi,
- məxfilik tələbləri səbəbindən bəzi məlumatların şifrələnməsi və ya silinməsi,
- təcrübəli hakerlər tərəfindən loqların saxtalaşdırılması riski.

Bu problemlərin həlli üçün "hiper zaman xətti" (hyper timeline) konsepsiyası ənənəvi "düz" zaman xəttini

DOI: 10.25045/forensic.gov.2026.60

genişləndirərək, yalnız vaxt nişanlarına deyil, həm də məlumat bazalarındakı ardıcıllıq nömrələri və loq fayllarındakı sətir nömrələri kimi dolayı zaman məlumatlarına əsaslanan yanaşma mühüm həll yolu kimi çıxış edə bilər.

Azərbaycan kontekstində bu sahədə aparılan tədqiqatlar məhduddur. Müdafiə Sənayesi Nazirliyi və müvafiq institutlar arasında əməkdaşlıq çərçivəsində hərbi sistemlərdə rəqəmsal təhlükəsizlik üzrə bəzi işlər aparılsa da, artilleriya sistemlərinin kriminalistik analizinə dair Azərbaycanda nəşr edilmiş akademik mənbələrə hələlik rast gəlinmir. Bu sahə gələcək tədqiqatlar üçün açıq və perspektivli bir istiqamətdir.

III. RƏQƏMSAL KRİMİNALİSTİKA METODLARININ TƏTBİQİ: REAL-VAXT VƏ POST-İNSİDENT ANALİZ

Rəqəmsal kriminalistika metodlarının artilleriya sistemlərinə tətbiqi iki əsas istiqamətdə həyata keçirilir:

- real-vaxt kriminalistikası (live forensics)
- hadisə sonrası analiz (post-incident forensics).

Bu iki yanaşma bir-birini tamamlayır və sistemin həm cari təhlükələrə qarşı qorunmasını, həm də baş vermiş hadisələrin dəqiq araşdırılmasını təmin edir [3].

Real-vaxt rejimində analiz artilleriya sisteminin normal fəaliyyəti zamanı loq fayllarının davamlı izlənilməsi və anomaliyaların ani aşkarlanmasıdır. Bu yanaşma, icazəsiz əmrlərin, qeyri-adi sensor məlumatlarının və ya şəbəkə trafikindəki anormal dəyişikliklərin dərhal identifikasiyasına imkan verir. Real-vaxt kriminalistikasının ən mühüm üstünlüyü ondan ibarətdir ki, hücum anında müdaxilə etmək və zərərin yayılmasının qarşısını almaq mümkün olur [2].

Real-vaxt analizinin texniki cəhətdən həyata keçirilməsi üçün adətən üç komponent tələb olunur:

- loq toplama aqreqatorları;
- anomaliyaların aşkarlanması alqoritmləri;
- əvvəlcədən müəyyən edilmiş cavab tədbirləri.

Bununla belə, real-vaxt kriminalistikasının tətbiqi ilə bağlı ciddi çətinliklər də mövcuddur. Əsas problem böyük həcmli məlumat axınının real-vaxtda emalı üçün yüksək hesablama resursları tələb olunmasıdır. Bundan əlavə, bəzi hərbi sistemlərdə məxfilik tələbləri səbəbindən loq məlumatlarının real-vaxtda sistemdənkənar ünvanlara təhlil üçün göndərilməsi məhdudlaşdırılır [2].

Hadisə sonrası analiz isə arzuolunmaz hadisə baş verdikdən sonra loq fayllarının dərindən tədqiq edilməsidir. Bu mərhələdə mütəxəssislər vaxt nişanlarını ardıcıllığa salır, silinmiş və ya zədələnmiş loqları bərpa edir, hadisənin zəncirini addım-addım qururlar. Post-insident analizin ən mühüm vəzifəsi, hadisənin texniki nasazlıq, operator xətası, qəsdən törədilmiş müdaxilə və ya icazəsiz əmrlər nəticəsində baş verdiyini müəyyən etməkdir [3].

Post-insident analizin tipik mərhələləri bunlardır:

- məlumatların toplanması, bərpası və təmizlənməsi,
- vaxt ardıcıllığının qurulması,
- hadisə zəncirinin rekonstruksiyası
- hüquqi və hərbi qiymətləndirmə.

Artilleriya kontekstində ən çətin mərhələ adətən vaxt ardıcıllığının bərpasıdır, çünki müxtəlif sensorlar və komanda sistemləri arasında vaxt sinxronlaşdırılması çox vaxt qeyri-kafi olur. Bu problemin həlli üçün "zaman lövbərləri" (time anchors) və "əsas (dayaq) hadisələr" (anchoring events) konsepsiyalarından istifadə edilə bilər.

Hər iki yanaşmanın effektivliyi üçün loq fayllarının bütövlüyü və dəyişməzliyi kritik əhəmiyyət daşıyır. Əgər loq faylları haker tərəfindən dəyişdirilə bilirsə, nə real-vaxt monitorinqi, nə də post-insident analiz etibarlı nəticə verə bilməz. NATO-nun Döyüş Meydanı Rəqəmsal Kriminalistikası üzrə rəsmi hesabatında bu problemə xüsusi diqqət yetirilir və sübut zəncirinin (chain of custody) qorunması üçün standart prosedurlar təklif edilir [2].

Müasir tədqiqatlarda loq bütövlüyü probleminin həlli üçün müxtəlif yanaşmalar təklif edilməkdədir. Vaxt nişanlarının düzgünlüyünün yoxlanılması üçün "hiper zaman xətti" (hyper timeline) metodu ənənəvi "düz" zaman xəttini genişləndirərək, yalnız vaxt nişanlarına deyil, həm də məlumat bazalarındakı ardıcıllıq nömrələri və loq fayllarındakı sətir nömrələri kimi dolayı zaman məlumatlarına əsaslanır.

IV. EFFEKTİV İDARƏETMƏYƏ TÖHFƏLƏR VƏ ÇƏTİNLİKLƏR

Rəqəmsal kriminalistika metodlarının artilleriya sistemlərinə inteqrasiyası idarəetmənin effektivliyini bir neçə mühüm istiqamətdə artırır. Bu töhfələr təkcə texniki deyil, həm də təşkilati, əməliyyat və strateji səviyyələri əhatə edir [2].

Birinci istiqamət - döyüş hazırlığının yüksəldilməsi: loq fayllarının davamlı təhlili vasitəsilə potensial nasazlıqlar və konfiqurasiya səhvləri vaxtında aşkarlanaraq aradan qaldırıla bilir. Bu, sistemin döyüş meydanına çıxmazdan əvvəl tam hazır vəziyyətdə olmasını təmin edir [1].

İkinci istiqamət - komanda və nəzarət strukturlarında şəffaflıq: Hər bir atəş əmrinin kim tərəfindən, nə vaxt və hansı əsaslarla verildiyi dəqiq izlənilir. Bu, daxili sui-istifadə hallarının qarşısını alır, eyni zamanda əməliyyatlardan sonra hesabatlılığı gücləndirir. Mancini, Monti və Panico qeyd edir ki, döyüş meydanında rəqəmsal sübutların məhkəmədə texniki və hüquqi dəyəri getdikcə artır və bu, artilleriya sistemlərində dəqiq loq qeydiyyatının vacibliyini vurğulayır [3].

Üçüncü istiqamət - sistemin kiber dayanıqlığının artırılması: Real-vaxt rejimində anomaliyaların aşkarlanması, hücum anında müdaxilə etməyə və mümkün zərərlərin qarşısının alınmasına imkan verir. NATO-nun Döyüş Meydanı Rəqəmsal Kriminalistikası hesabatında [2] qeyd olunur ki, xüsusi əməliyyatlar zamanı rəqəmsal kəşfiyyat və sübut toplanması əməliyyatların uğuru üçün kritik əhəmiyyət daşıyır.

Dördüncü istiqamət - təlim və kadr hazırlığının təkmilləşdirilməsi: Toplanmış loq məlumatları operatorların tipik səhvlərini, sistemin zəif nöqtələrini və təlim prosesindəki boşluqları aşkar etmək üçün istifadə edilə bilər [3].

Beşinci istiqamət - hüquqi və əməliyyat auditinin asanlaşdırılması: Müharibə qanunlarının pozulması, döyüş cinayətləri və ya sivil itkilərlə bağlı iddialar araşdırılarkən, forensik (kriminalistik) cəhətdən etibarlı loq qeydləri mühüm

dəlil rolunu oynayır [3].

Bununla belə, bu yanaşmanın tətbiqi ilə bağlı ciddi çətinliklər də mövcuddur. Bu çətinliklərin tanınması və həlli yollarının işlənilməsi, kriminalistik idarəetmənin real artilleriya sistemlərində tətbiqi üçün vacibdir.

Vaxt sinxronlaşdırılması problemləri. Sistem saatının təhrif edilməsi, təbii sürüşmə (clock drift) və ya sistem nasazlıqları səbəbindən qeydə alınan vaxt nişanları real hadisə vaxtlarını əks etdirməyə bilər. Bu problemin həlli üçün "zaman lövbərləri" (time anchors) konsepsiyası təklif edilir ki, bu da məlum vaxtlarda baş vermiş xarici hadisələrdən (məsələn, GPS siqnalları və ya şəbəkə sorğuları) istinad (dayaq) nöqtələri kimi istifadə etməyi nəzərdə tutur.

Məlumatların bərpası problemləri. Şifrələnmiş, zədələnmiş və ya qəsdən silinmiş logların bərpası hər zaman mümkün olmur. Xüsusilə təcrübəli kiber təcavüzkarlar izlərini gizlətmək üçün loq fayllarını dəyişdirir, silir və ya şifrələyirlər [2].

Standartlaşmanın olmaması. Hazırda artilleriya sistemləri istehsalçıdan asılı olaraq müxtəlif loq formatları, vaxt nişanı standartları və saxlanma protokollarından istifadə edir. Bu sahədə vahid standart yaratmağa cəhd göstərsə də, tam inteqrasiya hələ də tamamlanmamışdır [1]. Bu müxtəliflik, xüsusilə müştərək əməliyyatlarda kriminalistik analizi çətinləşdirir.

Kadr çatışmazlığı. Rəqəmsal kriminalistika üzrə mütəxəssislər artıq mülki sektorda çatışmazlıq təşkil edir. Hərbi sistemlərin özəlliklərini də bilən mütəxəssislər tapmaq isə daha da çətindir. Mancini və həmmüəllifləri [4] qeyd edirlər ki, bu problem xüsusi əməliyyatlar qüvvələrində daha kəskin şəkildə özünü göstərir.

Məxfilik və əməliyyat təhlükəsizliyi ilə balans. Loq fayllarının ətraflı toplanması və saxlanması, həm də özlüyündə təhlükəsizlik riski yarada bilər. Əgər loq məlumatları düşmən əlinə keçərsə, bu, artilleriya sisteminin taktiki üsulları və həssas yerləri haqqında dəyərli kəşfiyyat məlumatı verə bilər [2].

NƏTİCƏ

Rəqəmsal kriminalistika artilleriya sistemlərinin idarə olunmasında artıq sadəcə "hadisələrdən sonra araşdırma aparan" bir köməkçi alət deyil. Bu tədqiqat göstərir ki, kriminalistik metodların real-vaxt rejimində inteqrasiyası artilleriya idarəetmə sistemlərini passiv dəlil bazalarından aktiv müdafiə mexanizmlərinə çevirə bilər. Başqa sözlə, gələcəyin artilleriya sistemləri yalnız atəş gücünə deyil, həm də öz rəqəmsal mühitini qorumaq və loq məlumatlarının bütövlüyünü təmin etmək qabiliyyətinə malik olmalıdır.

Burada irəli sürülən ən mühüm yenilik **"**kriminalistik idarəetmə dövrü" konsepsiyasıdır**:**

- real-vaxt monitorinqi
- anomaliyaların aşkarlanması
- avtomatik bloklama
- post-insident yoxlamaları
- sistemin öyrənməsi
- sistemin özünü təkmilləşdirməsi.

Bu qapalı dövr olmadan artilleriya sistemləri rəqəmsal mühitdəki döyüş meydanında passiv qalır.

Təəssüf ki, hazırkı hərbi doktrinalarda loq faylları çox vaxt köməkçi texniki məlumatlar kimi qiymətləndirilir. Bu münasibət dəyişməlidir. Artilleriya sistemlərinin rəqəmsal izləri, döyüş sursatı qədər strateji dəyərə malikdir. Bir sursat bir hədəfi məhv edir, bir loq isə bütöv bir sistemin xilas olmasına səbəb ola bilər.

Gələcək tədqiqatlar aşağıdakı istiqamətlərdə aparılmalıdır:

- süni intellektin kriminalistik analizə tam inteqrasiyası,
- blokçeyn əsaslı paylanmış loq idarəsi,
- taktiki səviyyədə yüngül real-vaxt kriminalistika agentlərinin işlənilməsi.

Ən əsası isə, bu sahədə vahid beynəlxalq standartın - məsələn, "Beynəlxalq Kriminalistika Artilleriya Protokolu"nun yaradılması zəruridir. Bu protokol olmadan, müxtəlif sistemlərin loq formatlarının uyğunsuzluğu səbəbindən müştərək əməliyyatlarda kriminalistik analiz praktiki olaraq qeyri-mümkün olacaqdır.

Nəticə etibarilə, rəqəmsal kriminalistika gələcəyin artilleriya sistemlərinin təhlükəsiz və etibarlı idarə edilməsinin əsas komponentlərindən biri kimi qiymətləndirilməlidir.

ƏDƏBIYYAT

[1] STANAG 4537: NATO Armaments Ballistic Kernel (NABK) and Other Shareable Fire Control Software. NATO Standardization Office, 2005.

[2] T. Väisänen, C. Braccini, M. Sadlon, H. Bahşi, A. Panico, K. van der Meij, et al., Battlefield Digital Forensics: Digital Intelligence and Evidence Collection in Special Operations. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016.

[3] L. V. Mancini, A. Monti, and A. Panico, "SOF on trial: The technical and legal value of battlefield digital forensics in court," Lecture Notes in Computer Science, vol. 10717, pp. 9–26, 2017.

[4] S. Khan, A. Divakaran, and H. S. Sawhney, "Weapon identification across varying acoustic conditions using an exemplar embedding approach," in Proc. SPIE Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies, vol. 7666, p. 76662B, 2010.

Effective Management of Artillery Systems Based on Digital Forensics

Yashar Huseynov
National Defense University, Nakhchivan Military College,
Nakhchivan, Azerbaijan
yasar.huseynov@mmu.edu.az

Abstract- The effective management of modern artillery systems requires not only firepower but also digital security and operational transparency. Digital forensics—through log file analysis, detection of unauthorized commands, and system integrity auditing—offers a robust solution in this field. The applied methods enable both accurate post-incident investigations and real-time prevention of anomalies. As a result, a management model based on digital forensics significantly enhances the combat readiness and cyber resilience of artillery units.

Keywords- digital forensics; artillery systems; log analysis; unauthorized commands; system auditing, cybersecurity.